ROYAUME DU MAROC
Université Mohammed V - RABAT -
جامعة محمد الخامس – الرباط –
Faculté des sciences
كلية العلوم
CENTRE D'ETUDES DOCTORALES - SCIENCES ET TECHNOLOGIES

N° d'ordre **3112**

THESE

En vue de l'obtention du : ***DOCTORAT***

Structure de Recherche : Laboratoire de Recherche Informatique et Télécommunications.
Discipline : Sciences de l'ingénieur.
Spécialité : Informatique et Télécommunications.

Présentée et soutenue le : 23/06/2018 par :

Meryam El MOUHTADI

Recherche et Indexation de l'Image Biométrique par Contenu Multimédia. Application à l'Empreinte Digitale.

JURY

Rachid OULAD HAJ THAMI	*PES, Université Mohammed V de Rabat, ENSIAS, Rabat, Maroc*	*Président*
Benayad NSIRI	*PES, Université Mohammed V de Rabat, l´Ecole Normale Supérieure de l'Enseignement Technique, Rabat*	*Rapporteur*
Mohammed EL HASSOUNI	*PH, Université Mohammed V de Rabat, Faculté des Lettres et des Sciences Humaines, Rabat, Maroc*	*Examinateur*
Mohammed EL HAJ TIRARI	*PH, Institut National de Statistique et d'Economie Appliquée, Rabat, Maroc*	*Examinateur*
Sanaa El FKIHI	*PH, Université Mohammed V de Rabat, ENSIAS Rabat, Maroc*	*Directeur de Thèse*
Youness TABII	*PH, Université Abdelmalek Essaadi, ENSA de Tétouan, Maroc*	*Rapporteur*

Année Universitaire : 2017/2018

أَيَحْسَبُ الْإِنسَانُ أَلَّن نَّجْمَعَ عِظَامَهُ ③

بَلَىٰ قَادِرِينَ عَلَىٰ أَن نُّسَوِّيَ بَنَانَهُ ④

(سورة القيامة الآيات 3-4)

Chapitre

0 Avant-Propos

Les travaux présentés dans ce rapport ont été réalisés dans le cadre de mon doctorat effectué au sein du Laboratoire de Recherche en Informatique et Télécommunications (**LRIT**), à la Faculté des Sciences de Rabat, Université Mohammed V de Rabat, sous la direction du Professeur **El FKIHI Sanaa**.

Je remercie,tout d'abord, bien vivement aussi mon directeur de thèse, madame **El FKIHI Sanaa** (PH à L'École Nationale Supérieure d'Informatique et d'Analyse des Systèmes de Rabat), pour sa confiance, son encadrement et son soutien continuel. Qu'elle trouve ici l'expression de ma gratitude pour ses précieux conseils et toute l'aide qu'elle m'a procuré durant l'élaboration de ce travail.

Aussi je dois des remerciements particuliers au profeseur **Rachid OULAD HAJ THAMI** (PES à l'École Nationale Supérieure d'Informatique et d'Analyse des Systèmes de Rabat), pour l'honneur qu'il me fait en présidant mon jury de thèse.

J'adresse également mes remerciements au professeur **Nsiri BENAYAD** (PH à l´École Normale Supérieure de l'Enseignement Technique de Rabat), d'avoir bien voulu être rapporteur et de faire partie de mon jury de thèse.

J'adresse également mes remerciements au professeur **Mohammed EL HAJ TIRARI** (PH à Institut National de Statistique et d'Economie Appliquée), d'avoir bien voulu être rapporteur et de faire partie de mon jury de thèse.

J'adresse également mes remerciements au professeur **Youness TABII** (PH à l'Université Abdelmalek Essaadi, ENSA de Tétouan), d'avoir bien voulu être rapporteur et de faire partie de mon jury de thèse.

Je remercie bien vivement aussi professeur **Mohammed EL HASSOUNI** (PH à la Faculté des Lettres et des Sciences Humaines de Rabat) pour avoir accepté dêtre membre de mon jury en tant qu'examinateur.

Mes remerciements vont enfin à toute personne qui a contribué de près ou de loin à l'élaboration de ce travail.

Chapitre 0

Remerciement

A la mémoire de mon père, une pensée à lui qui n'a pas vu l'aboutissement de mes objectifs et mon travail, mais je sais qu'il en aura été très fier de sa fille.

A ma chère mère, ma raison de vivre et l'étoile qui m'illumine, tous les mots ne sauraient exprimer ma gratitude et ma reconnaissance pour ton dévouement et tes sacrifices. Je te dédie cette thèse comme fruit de ton dévouement et l'expression de mon profond amour.

Je remercie spécialement toute la famille ***ADIB****, du plus grand au plus petit, pour la chaleur et l'amour, ils ont toujours été à mes côtés pour me soutenir et m'épauler. Mes chers oncles en or, mes chères tantes d'amour, mes bijoux de cousins et cousines, puissiez-vous trouver dans ce travail le témoin de mon affection et estime..*

Mes remerciement vont également à la famille ***ElMOUHTADI****, à mes gentilles tantes et adorables cousines, merci pour votre soutien permanent. veuillez trouver dans ce travail l'expression de mon respect le plus profond et mon affection la plus sincère.*

A mes amis de ***coeur****, Meryam, Youssef, Reda, Atmane, Imane, Ibtihal, ... ,la liste est longue, vous êtes à moi les frères et soeurs que la vie m'a offert, vous partagerez toujours une partie de ma vie et de mon coeur. Merci pour les bons moments qu'on a passé ensemble, de votre soutien et de votre serviabilité.*

A mes collègues du laboratoire ***LRIT*** *et de la faculté des sciences. Merci pour les beaux moments partégées ensmble durant ces années d'études.Je vous souhaite une vie pleine de réussite, de santé et de bonheur.*

Mes remerciements vont aussi à tout les personnes qui, avec cette question récurrente, «quand est-ce que tu la soutiens cette thèse ? », bien qu'angoissante en période fréquente de doutes, m'ont permis de ne jamais dévier de mon objectif final.

Chapitre 0

Résumé

Dans un monde technologiquement croissant, l'augmentation du nombre des appareils, de téléphones intelligents, et des instances de stockage et prise d'image, est allée de pair avec l'accroissement de l'information biométrique de l'individu.

Faciliter l'accès, l'utilisation fluide et surtout assurer la sécurité des modèles biométriques stockés sont des problèmes qui demeurent critiques. Ainsi que se suscite le regain d'intérêt pour des recherches progressives et, à terme, pour la mise en oeuvre de solutions technologiques. Ces dernières doivent assurer la confidentialité du flux des images biométriques, la pertinence de la recherche dans les grandes bases de données biométrique, et la rapidité de la reconnaissance. Nous croyons que ces contraintes constituent les trois sommets du triangle de pertinence des algorithmes de reconnaissance biométrique. Ainsi que le défi est de trouver le moyen d'équilibrer les dites contraintes. C'est la perspective suivie dans cette thèse.

L'identification par empreinte digitale a gagné le marché de la sécurité biométrique et est présente dans les nouvelles technologies reposant sur une authentification de l'individu par image. Étant une intéressante piste d'application, c'est ainsi que s'enflamme considérablement le besoin en algorithmes de recherche et d'indexation de l'empreinte digitale qui soient à la fois précis en termes de reconnaissance, de rapidité et surtout la tolérance à toutes sorte de menaces. Dans ce contexte, nous avons contribué dans la recherche et l'indexation des empreintes digitale par la proposition de deux approches. La première, appelée HDT, pour la mise en place d'un pertinent algorithme d'indexation fondé sur la transformation hiérarchique des caractéristiques locaux par triangulation. Une deuxième approche, vise l'accélération de la méthode proposée pour la rapidité du système de reconnaissance d'empreinte digitale en se basant sur l'intérêt de la région points singuliers. Nous avons également évalué la sécurité de l'approche de reconnaissance proposée par un scénario d'attaque biométrique par altération de l'empreinte digitale.

Mots clés : *empreinte digitale ; recherche et indexation ; contenu multimédia ; biométrique ; triangulation Delaunay ; reconnaissance*

Chapitre

0

Abstract

In a technologically growing world, the growth of devices, smart phones, and storage imaging instances has gone hand in hand with the growth of individuals' personal information.

Facilitate the access, the fluid use and especially the security of a user identity are the primary factors that led to progressive research for the implementation of technological solutions ensuring the confidentiality and security of used images flow, the relevance of searching images in large databases, and the speed of search.
These last three constraints forms the three peaks of a relevance triangle of image recognition algorithms. The main challenge of the algorithms is to find the best way to equilibrate this constraints..

Fingerprint identification has won the biometric security market and is present in new technologies based on image-based authentication of the individual (biometric maps, fingerprint access systems, the new Iphone Touch ID functionality, ...). Its reliability and relevance have made it a distinguished solution to represent an individual regarding its unique characteristics. Being an interesting application track, thus ignite the need for fingerprint retrieval and indexing algorithms which are precise in terms of recognition, efficiency, speed and above tolerable to all kinds of threats and attacks.

In this thesis we contribute in the fingerprints retrieval and indexing. In order to find the best method for indexing fingerprints and defining the uniqueness of digital information in large databases while meeting the three main constraints and finding the right combination that equilibrate relevance, speed and security of the system. We will search, define, and implement a new feature-based indexing algorithm to better represent and index the fingerprint. while exploiting the tracks of scientific advances in the field of image indexing and retrieval.

Keywords : *Fingerprint ; retrieval and indexing ; multimedia content ; biometric ; Delaunay triangulation ; recognition.*

TABLE DES MATIÈRES

Chapitre

0

Liste des acronymes

DT	*Delaunay triangulation*
HDT	*Hierarchical Delaunay Triangulation*
SDT	*Simple Delaunay Triangulation*
FAR	*False Accept Rate*
FRR	*False Reject Rate*
SPHTD	*Singular point with hierarchical Delanay triangulation*

Liste des figures

Liste des tableaux

Chapitre

1 Introduction

Sommaire

1.1 Contexte général

Cette thèse s'intéresse à l'indexation et à la recherche de l'image dans des bases de données volumineuses par son contenu multimédia. L'indexation consiste à extraire, représenter et organiser efficacement le contenu des documents d'une base de données et ce afin de faciliter au mieux la recherche d'informations.

Les empreintes digitales sont choisîtes en étant le domaine d'application le plus adéquat à nos attentes. Les bases de données contenant des empreintes digitales, sont de plus en plus croissantes avec la numérisation et l'informatisation des systèmes de sécurité, ainsi que l'augmentation des applications d'authentification par empreintes digitales. L'identification des empreintes digitales est couramment employée dans la dernière décennie. En commençant par des utilisations personnelles : des authentifications au Smartphone, accès au bâtiments,..., jusqu'aux utilisations à grande échelle : la médecine légale à l'appui des enquêtes criminelles, les systèmes biométriques, comme les dispositifs d'identification civils et commerciales et d'autres identification des individus par données biométriques.

L'objectif principal de l'indexation des empreintes digitales est de trouver la meilleure solution afin de répondre aux contraintes de reconnaissance formant les trois sommets du triangle de reconnaissance biométrique : la pertinence, la rapidité et la sécurité (Figure 1.1) :

- *La pertinence* remporte la préoccupation majeure de tout système de reconnaissance biométrique, elle désigne le facteur principal de valorisation de sa fonctionnalité. Un système pertinent est un système qui répond sans erreur et avec efficacité à toute requête d'interrogation. Bien évidement, le taux d'erreur de reconnaissance n'est pas négligeable tant qu'on utilise des informations qui peuvent changer de caractéristiques, falsifier ou

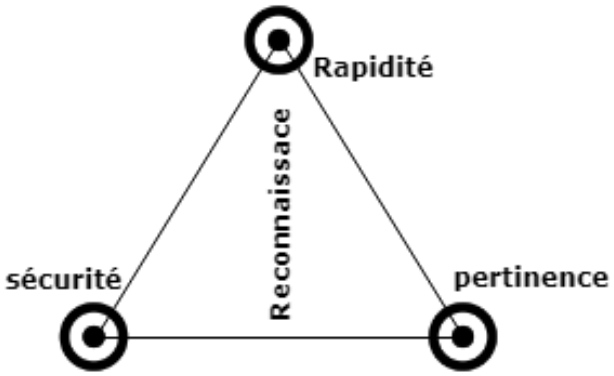


FIGURE 1.1 – Triangle de reconnaissance

attaquer par l'environnement extérieur.

- *La rapidité* est une vérité qui s'accorde avec la croissance de la technologie de nos jours. La pertinence du système de reconnaissance est importante, mais si le système est assez lent, on finira par accepter les failles du système que de rester une heure devant une porte pour rentrer.

- *La sécurité* désigne dans ce sens la confidentialité des données biométriques stockées dans la base de donnée. Ainsi que la capacité du système à savoir si le porteur de l'empreinte est l'utilisateur lui même ou du malveillant qui a falsifié, refait ou copié l'image de l'empreinte. Un utilisateur a besoin non seulement d'un accès rapide et correct mais aussi que ses données biométriques soient bien conservées.

De ce fait, on peut affirmer que les empreintes digitales sont un bon moyen de reconnaissance d'un individu, et elles ont bénéficié d'une étude approfondie depuis plus d'un siècle. Cependant, en faisant preuve d'ingéniosité, on s'aperçoit qu'elles ne sont pas à l'abri de la falsification. C'est ainsi que s'impose la question : ***Quelles sont les bonnes techniques permettant d'équilibrer les trois contraintes ?***

1.2 Problématique et contributions

Dans la littérature, plusieurs travaux sont proposés pour développer des systèmes de reconnaissance d'empreintes digitales en se basant sur plusieurs méthodes d'indexation. Généralement, les algorithmes de reconnaissance visent l'un des trois axes suivants : (i) la réalisation d'algorithmes rapides pour la reconnaissance des empreintes digitales, et sont adaptés pour des systèmes d'authentification des individus par empreintes digitales. Ces approches sont en générale forts pour la vérification mais pas trop pour l'identification des individus dans les grandes bases de données. (ii) D'autres approches se focalisent sur la pertinence du système d'identification, ils proposent des taux d'erreur très petits mais dans un temps assez long qu'on ne peut pas l'appliquer à des systèmes d'authentification à temps réel. (iii) Il existe des algorithmes qui prennent en considération à la fois le temps

et la pertinence. Ces systèmes sont certainement intéressants sauf qu'ils ne gèrent pas le côté sécuritaire du système proposé, on ne trouve pas des renforcements face à des altérations de l'empreinte digitale par un attaquant malveillant voulant accéder aux données personnel d'un utilisateur ou le remplacer.

Cependant, il n'existe pas de méthodologie de reconnaissance intégrant à la fois les trois différentes contraintes de reconnaissance d'empreintes digitales, c'est ainsi que se crée les principaux objectifs de cette thèse. Notre but concerne la proposition d'un système complet de reconnaissance des empreintes digitales qui assure la bonne reconnaissance avec un temps de calcul raisonnable tout en garantissant la sécurité face aux attaques des malévoles. Ces objectifs ont été atteints via trois contributions :

La première contribution consiste à définir le principe de transformations affines des descripteurs de l'empreinte, qui influencent sur la qualité d'un système de recherche d'empreinte digitale. En utilisant les avantages des caractéristiques locaux de l'empreinte digitale nous avons proposé un modèle d'indexation fiable en termes de reconnaissance selon les deux modalités, identification et vérification. Le modèle d'indexation proposée dans cette approche garantit largement la robustesse à toutes formes de transformations affines tout en gardant la pertinence du résultats.

La deuxième contribution de cette thèse se focalise sur l'amélioration de la méthode d'indexation proposée, qui vise particulièrement la validation da la rapidité de l'approche développée, il présente la deuxième problématique de cette thèse. Nous proposons dans cette partie une combinaison de la méthode d'indexation par triangulation des descripteurs ; proposée dans la première contribution ; et les performances des points singuliers des empreintes digitales. Nous avons également étudier l'amélioration du système proposé dans le sens de la pertinence et de la rapidité.

Quant à la troisième contribution, qui complète le triangle de reconnaissance biométrique, nous proposons ; dans un travail collaboré avec une thèse soutenu au sein de notre laboratoire ; l'évaluation de la sécurité de notre système biométrique face aux attaques de trace qui se base sur l'utilisation des images altérées du vrai utilisateur. Dans cette contribution nous présentons l'application d'une attaque biométrique par altération de l'image originale, sur le système de reconnaissance basée sur l'indexation proposée au début de ce mémoire, après avoir définir les différents types d'attaque biométrique adaptés à l'empreinte digitale et les différentes méthode de protection des systèmes biométrique. Notre système d'indexation a prouvé ses avantages en étant une pertinente méthode de protection de l'empreinte digitale robuste aux attaques par altération.

Finalement, les différentes contributions que nous avons proposé, ont été réalisées de manière à équilibrer, à la fois, les trois dites contraintes, comme l'illustre la Figure 1.2.

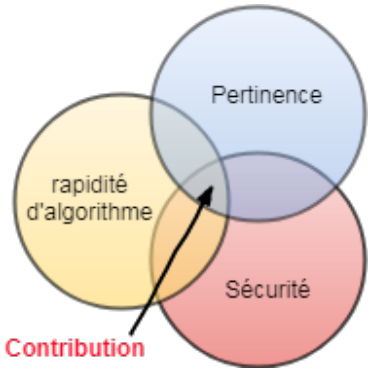


FIGURE 1.2 – L'espace de contribution de cette thèse.

1.3 Organisation du mémoire

Ce manuscrit de thèse est composé de six parties essentielles qui sont présentées de la manière suivante :

L'introduction qui présente le problème de l'indexation des empreintes digitales dans des bases de données volumineuses. Elle décrir également le besoin des systèmes de reconnaissance de l'empreinte digitale qui sont à la fois pertinents, rapides et sécurisés, clarifier le contexte du travail et la contribution de la thèse. Cette partie donne aussi le plan d'organisation de la thèse.

Le chapitre 2 est consacré à l'introduction de la notion de l'empreinte digitale, ses caractéristiques, les processus de traitement de l'image d'empreinte digitale, et un état de l'art sur les méthodes d'indexation.

Le chapitre 3 présente la première contribution de cette thèse. Il définie premièrement les différents problèmes de la recherche d'une image d'empreintes digitales et les transformations qui peuvent l'atteindre. Ensuite, il décrit d'une façon détaillée l'approche proposée comme méthode d'indexation des empreintes digitales.

Le chapitre 4 contient la deuxième contribution de notre thèse, il propose la combinaison des caractéristiques globales de l'empreinte digitale avec la méthode de la première contribution pour améliorer l'aspect de rapidité de la reconnaissance.

La chapitre 5 touche à l'étude de la sécurité du système de reconnaissance, en présentant la méthode d'indexation présentée au début de la thèse comme une méthode de protection biométrique, prêtant un niveau de sécurité considérable au système de reconnaissance.

La dernière partie conclut le mémoire en résumant les principaux résultats obtenus, elle expose également les perspectives et les travaux futures.

1.4 Liste des papiers

Journaux internationaux :

- Elmouhtadi, Meryam. Elfkihi, Sanaa. et Driss, Aboutajdine. (2017).Fingerprint Identification Based Hierarchical Triangulation. Journal of Information Processing Systems.

- Elmouhtadi, Meryam. Lafkih, Maryam. et Elfkihi, Sanaa. (2017). Biometric protection approach based on fingerprint hierarchical identification. International Journal of Applied Engineering Research, 12(21) :11007-11014.

Book Chapter :

- Elmouhtadi, Meryam. Elfkihi, Sanaa. et Driss, Aboutajdine. (2018). Fingerprint identification using hierarchical matching and topological structures. Studies in Computational Intelligence ; Book Volume 730.

Conférences internationales :

- Elmouhtadi, Meryam. El Fkihi, Sanaa. et Aboutajdine, Driss.(2015).Hierarchical Triangulation Based Fingerprint Identification. Mediterranean Conference on Information and Communication Technologies, MedICT 2015 ; Saidia ; Morocco.

- Elmouhtadi, Meryam. Aboutajdine, Driss. et El Fkihi, Sanaa.(2015). Fingerprint indexing based barycenter triangulation. 3rd IEEE World Conference on Complex Systems, WCCS 2015 ; Marrakech ; Morocco.IEEE.

- Elmouhtadi, Meryam. El Fkihi, Sanaa. et Aboutajdine, Driss.(2016). Improving fingerprint matching using Delaunay triangulation features. International Conference on Big Data and Advanced Wireless Technologies, BDAW 2016 ; Blagoevgrad ; Bulgaria. ACM. ***(Best Paper Award)***.

- Elmouhtadi, Meryam. El Fkihi, Sanaa. et Aboutajdine, Driss.(2016). Fingerprint identification using hierarchical matching and topological structures. 2nd International Conference on Advanced Intelligent Systems and Informatics, AISI 2016 ; Cairo ; Egypt. ***(Best Paper and Presentation Award)***.

- Elmouhtadi, Meryam. El Fkihi, Sanaa. et Aboutajdine, Driss.(2016). Fingerprints indexing algorithms based on multiple characteristics. 4th IEEE International Colloquium on Information Science and Technology, CiSt 2016 ; Tangier-Assilah ; Morocco.

Conférences nationales :

-Journées **URAC'29** 2013 :Elmouhtadi, Meryam. El Fkihi, Sanaa. et Aboutajdine,

Driss.Indexation et Recherche par contenu multimédia appliqué aux empreintes digitales (État de l'art).

-**JDTIC** Journées Doctorales en Technologies de l'Information et de la Communication 2013 :Elmouhtadi, Meryam. El Fkihi, Sanaa. et Aboutajdine, Driss. Indexation et Recherche des Empreintes digitales

-**JDTIC** Journées Doctorales en Technologies de l'Information et de la Communication 2014 : Elmouhtadi, Meryam. El Fkihi, Sanaa. et Aboutajdine, Driss. Indexation des empreintes digitales : Etat de l'art

-Journées **URAC'29** 2015 :Elmouhtadi, Meryam. El Fkihi, Sanaa. et Aboutajdine, Driss. Indexation et Recherche par contenu multimédia : Indexation des empreintes digitales.

Concours :

- Participation au concours MT180s (Ma thèse en 180 secondes), laboratoire de Recherche en Informatique et Télécommunications (LRIT). ***(Premier prix)***

Chapitre

2 RECHERCHE DE L'IMAGE PAR CONTENU : TRAITEMENT DE L'EMPREINTE DIGITALE

Sommaire

L'étude des systèmes biométriques, en générale, appartient à beaucoup de domaines tel que l'histoire, la biologie, les mathématiques. Elles intéressent aussi bien les scientifiques que la police et les juristes. Le choix de la technologie biométrique que le client souhaite mettre en place dépend fortement de la pertinence, le taux d'erreur et le temps de réponse. Ces conditions font l'objet du problème d'identification, qui fait référence à son tour aux différentes méthodes de traitement de l'image et d'extraction du contenu pertinent permettant de représenter l'image par son contenu. Cependant, les systèmes de reconnaissance d'image à base des empreintes digitales sont les plus matures et conviennent à un grand nombre de demandes de reconnaissance.
Dans ce chapitre, nous allons étudier la reconnaissance biométriques à base des em-

preintes digitales. Nous introduisons d'abord l'histoire des empreintes, nous présentons leurs caractéristiques, ensuite nous allons explorer l'état de l'art du processus de reconnaissance des empreintes digitales et les méthodes de traitement d'image utilisées.

2.1 Généralités

2.1.1 Historique

Les empreintes digitales humaines ont été découvertes sur des artefacts archéologiques et des objets historiques voire figure 2.1. Bien que ces résultats prouvent que les personnes avant ont utilisé des empreintes digitales pour certains objectifs, ce n'est qu'à la fin du XVI^e siècle que les études scientifiques d'empreintes digitales ont été initiées Lee *et al.* (2001). En 1686, **Marcello Malpighi**, professeur d'anatomie à l'Université de Bologne, avait noté la présence de crêtes papillaires, de spirales et de boucles dans les dessins des empreintes humaine. Henry Fauld, en 1880 (Berry et Stoney (2001)), fut le premier à suggérer scientifiquement l'individualité des empreintes digitales basée sur le principe de l'observation empirique. En même temps, Herschel (Lambourne (1984)) a affirmé qu'il avait pratiqué la reconnaissance d'empreintes digitales pendant environ 20 ans. À la fin du XIX^e siècle, Francis Galton Galton *et al.* (1909) a mené une vaste étude sur les empreintes digitales ; jusqu'au 1888, où il a introduit pour la première fois la notion des minuties qui représentent les caractéristique pour des besoins d'appariement des empreintes digitales. Une autre avancée importante a été faite en 1899 par Edward Henry, qui a établi le fameux **"Système d'Henry"** qui propose une classification des empreintes digitales selon la forme du dessin Hong et Jain (1999).

Au début du vingtième siècle, la reconnaissance des empreintes digitales a été formellement acceptée comme une méthode d'identification valide et est devenue une routine standard en médecine légale Lee *et al.* (2001). Des agences d'identification d'empreintes digitales ont été créées dans le monde entier et des bases de données criminelles sur les empreintes digitales ont été établies ; par exemple, la division d'identification d'empreintes digitales du FBI qui a été développée, en 1924, avec une base de données de 810 000 cartes d'empreintes digitales.

Avec la rapide expansion de la reconnaissance des empreintes digitales dans la criminalistique, les bases de données d'empreintes digitales opérationnelles sont devenues si importantes, ce qui a rendu l'identification manuelle des empreintes digitales irréalisable ; par exemple, le nombre total de cartes d'empreintes digitales dans la base de données d'empreintes digitales du FBI dépasse largement 200 millions et ne cesse de croître. Avec des milliers de demandes reçues quotidiennement, même avec une équipe de plus de 1 300 experts en empreintes digitales, ils restent incapables de fournir des réponses rapides à ces demandes. À partir du début des années 1960, le FBI, Home Office au Royaume-Uni et le département de police de Paris ont commencé à investir dans le développement de systèmes automatiques d'identification des empreintes digitales SAID : ***système automatisé d'identification dactyloscopique***) connu par **AFIS***(automatic fingerprint*

identification systems) .

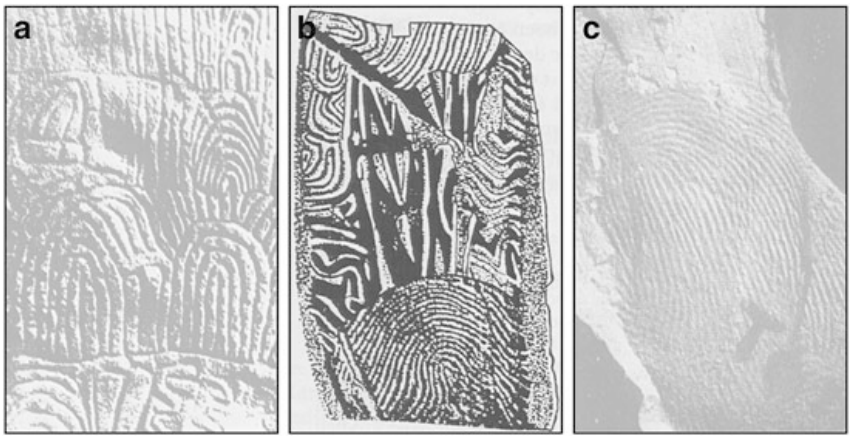


FIGURE 2.1 – Les premiers artefacts d'empreintes digitales trouvés :(a)Sculptures néolithiques ;(b)Empreinte sur une pierre ;(c)Une impression sur une lampe palestinienne (400 après JC)

Aujourd'hui, la technologie de reconnaissance automatique des empreintes digitales s'est rapidement développée au-delà des applications médico-légales. D'un côté, avec le visage, l'empreinte digitale reste toujours la principale modalité biométrique pour les documents électroniques (passeport électronique, visas, cartes d'identité, etc.) utilisés pour faire respecter le passage des frontières et la sécurité des citoyens. D'autre part, grâce à un très bon compromis performance / coût, les systèmes biométriques basés sur les empreintes digitales deviennent très populaires et sont déployés dans un large éventail d'applications commerciales telles que l'authentification des ordinateurs et smartphone, le contrôle d'accès physique, et les guichets automatiques.

2.1.2 Capteurs : types et vulnérabilité

Avant d'entamer le processus de reconnaissance d'empreintes digitales, la construction de l'image d'empreinte digitale est une étape importante autant qu'elle influence sur la performance des systèmes de reconnaissance. Auparavant, les empreintes digitales étaient obtenues en roulant un doigt encré d'ongle à ongle sur un papier. Cependant, de nos jours, de nombreux capteurs sont disponibles permettant d'acquérir l'image en se basant sur les principes de l'optique, de la grandeur capacitive, de la pression ou des capteurs thermiques (Figure 2.2). Ils produisent une image numérique de l'empreinte digitale, généralement composée de valeurs de niveaux de gris de 8 bits, numérisées à 500 dpi.

Les capteurs ont rendu le processus d'acquisition beaucoup plus convivial car ils ne nécessitent qu'une simple pression du doigt sur le capteur. Cependant, la tâche d'un algorithme d'identification d'empreinte digitale est devenue plus compliquée puisque les images tactiles simples (également appelées images dab) contiennent une partie beaucoup plus petite de l'empreinte entière. Par conséquent, moins de points caractéristiques sont présents, les points singuliers, qui caractérisent le centre de l'empreinte digitale, peuvent

se trouver en dehors de la zone capturée, et deux images peuvent se chevaucher pour une très petite partie. Enfin, les algorithmes doivent être adaptés, de préférence, au capteur spécifique utilisé car différents capteurs fournissent des images du même doigt avec des caractéristiques différentes, ce qui augmente le taux de variation intra-classe et rend l'appariement plus difficile.

Dans le but de limiter le chevauchement de différentes impressions d'une empreinte digitale ; des chercheurs comme Ratha *et al.* (1998) et Zhou *et al.* (2001) ; ont proposé d'appliquer une procédure dite mosaïquage. Elle consiste à enrouler le doigt sur un capteur d'empreintes digitales qui capture une séquence d'images. Ces images sont facilement combinées en une seule image plus grande pour but d'acquérir le maximum d'informations. D'autres méthodes, comme dans Jain et Ross (2002),ont été proposés pour construire une image d'empreinte digitale composée à partir de plusieurs impressions prises à différents moments. Dans ce cas, l'enregistrement est beaucoup plus difficile puisque les paramètres d'enregistrement ne sont pas connus à l'avance.

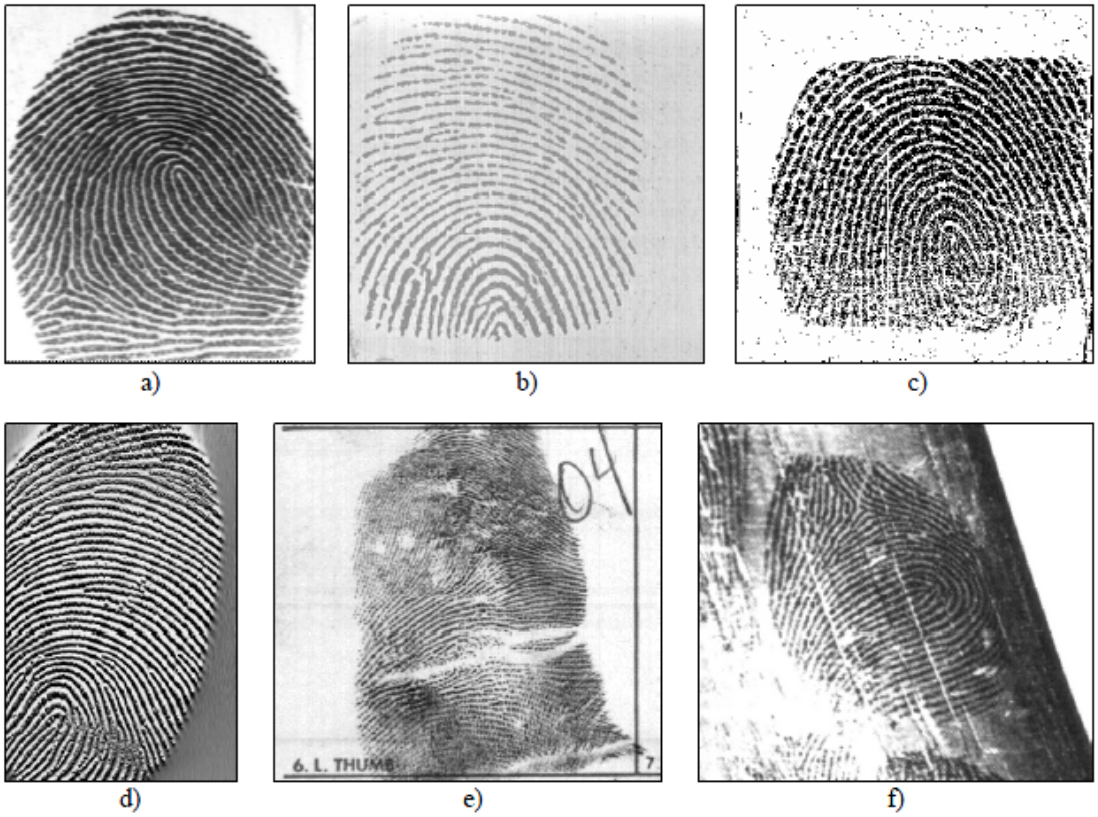


FIGURE 2.2 – Exemple d'image d'empreintes digitales acquises par : (a) Un scanner optique FTIR (b) Un scanner capacitive (c) Un scanner piézoélectrique (d) Un scanner thermique (e) Une impression à l'encre sur papier (f) Une prise de scène de crime

Enfin, la qualité et les caractéristiques de l'image d'empreintes digitales dépendent fortement du type de capteur d'empreintes digitales utilisé, ce qui affecte directement les performances du système de reconnaissance.

C'est dans ce contexte que s'impose la nécessité d'utiliser les algorithmes d'indexation, le prétraitement et le post-traitement, le processus permettant de faciliter l'appariement indépendamment du capteur utilisé et aux conditions d'acquisitions. C'est donc l'un des objectifs principaux de cette thèse, par contre la technologie des capteurs d'empreintes digitales elle-même n'est pas abordée dans cette thèse.

2.2 Processus de la reconnaissance biométrique

L'authentification biométrique est essentiellement une reconnaissance qui fait l'objet d'une identification personnelle consistant à déterminer l'authenticité d'une caractéristique physiologique ou comportementale spécifique possédée par un utilisateur. Le but principal des systèmes de reconnaissance biométrique est de définir une conception pratique permettant d'identifier la personne d'une façon unique. Comme montre la Figure 2.3, on se trouve face à deux modules fondamentaux de l'authentification :

(1). L'enrôlement.

(2). L'identification ou la verification.

Le module d'enrôlement consiste à créer une image représentatif de l'individu dans le système biométrique. Généralement dans la biométrie, pendant cette phase, le paramètre biométrique d'un individu est d'abord analysé par un lecteur biométrique pour produire une représentation numérique brute de la caractéristique. Spécifiquement le capteur des empreintes numérise le bout du doigt et retourne une image à niveau de gris ; ce qui fait l'objet de l'image d'empreinte digitale.

Par la suite et afin de faciliter l'appariement des images selon un système donné, la représentation de l'image acquise doit subir quelques transformations afin d'éliminer toute information inutile et faciliter son stockage. Et donc, les empreintes digitales sont généralement traitées par un processus d'extraction de caractéristiques importantes qu'on nommera le prétraitement, ce qui va générer un modèle représentatif de l'empreinte et par conséquent moins coûteux en terme de stockage. Ce modèle peut être stocké dans la base de données centrale.

Selon l'application souhaitée, la biométrie peut être utilisée dans l'un des deux modes : vérification ou identification. Bien que les technologies biométriques mesurent des caractéristiques différentes de manière très différente, tous les systèmes biométriques commencent par une phase d'inscription dite enrôlement suivie d'une étape de correspondance qui peut utiliser soit la vérification, soit l'identification.

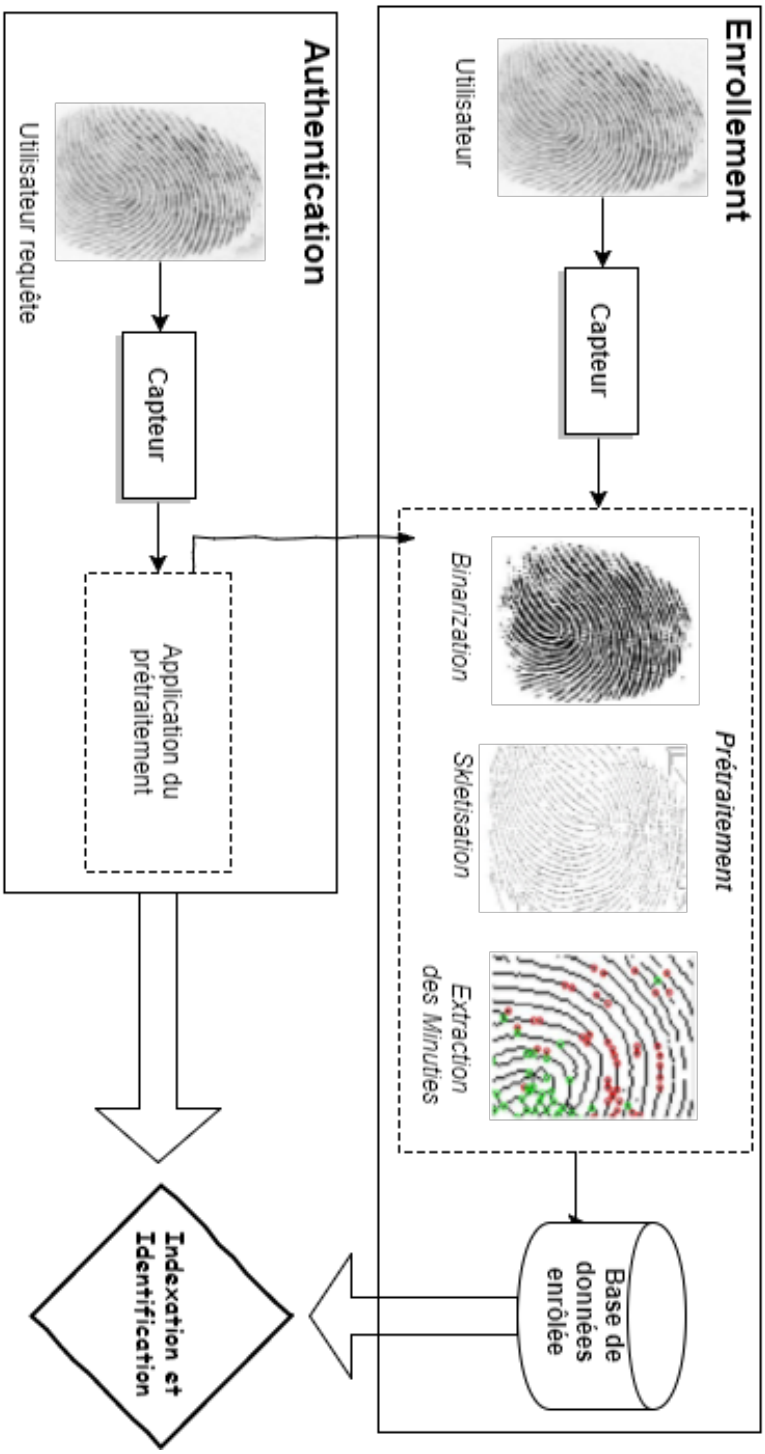


FIGURE 2.3 – Processus de reconnaissance des empreintes digitales.

2.2.1 L'enrôlement

Lors de l'enrôlement, un système biométrique est formé pour identifier une personne spécifique. La personne fournit d'abord un identifiant, tel qu'une carte d'identité. La biométrie est liée à l'identité spécifiée sur le document d'identification. La personne présente ensuite le dispositif biométrique (par exemple, l'empreinte digitale, la main ou l'iris) à un dispositif d'acquisition. Selon la Figure 2.4, les caractéristiques distinctives sont localisées et un ou plusieurs échantillons sont extraits, codés et stockés en tant que modèle de référence pour des utilisations futures.

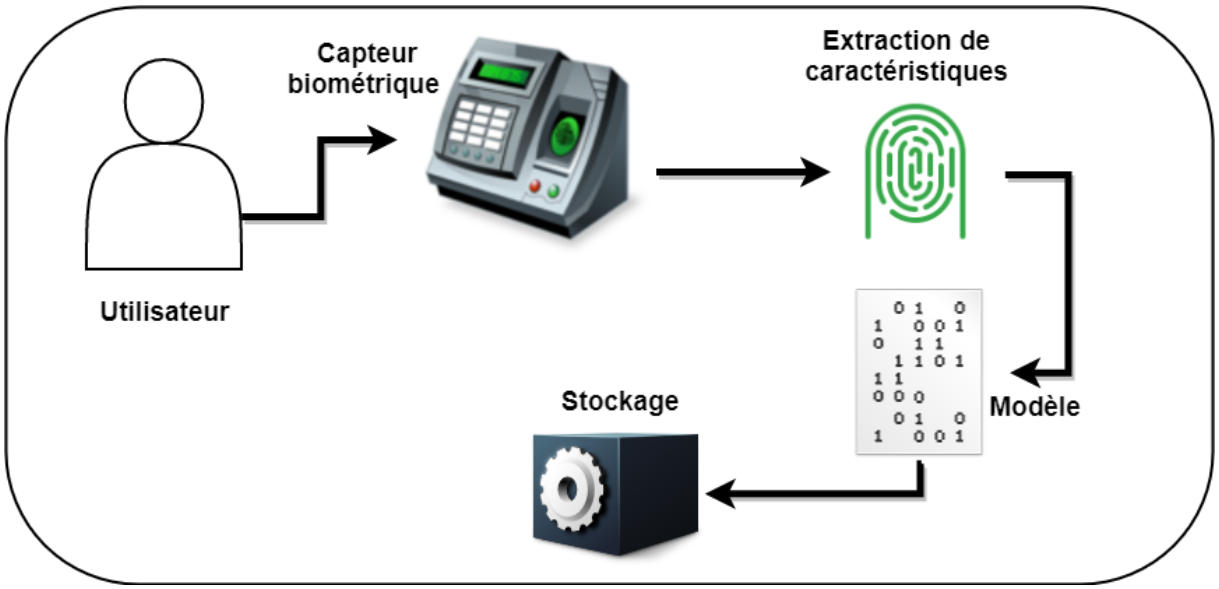


FIGURE 2.4 – Processus de l'enrôlement d'une empreinte digitale.

Selon la technologie, l'échantillon biométrique peut être recueilli sous la forme d'une image, ou d'un enregistrement de mesures dynamiques connexes. La taille du modèle varie en fonction du fournisseur et de la technologie. Les modèles peuvent être stockés à distance dans une base de données centrale ou dans un lecteur biométrique lui-même ; leur petite taille permet également le stockage sur des cartes à puce ou des jetons.

La qualité du ou des modèles enrôlés est essentielle au succès global de l'application de reconnaissance d'empreinte digitale. Ceci revient essentiellement à la qualité du capteur utilisé et aux paramètres de la capture.

2.2.2 Vérification

Dans les systèmes de vérification, l'étape après l'enrôlement consiste à vérifier qu'une personne est ce qu'elle prétend être (c'est-à-dire la personne qui possède déjà son propre modèle dans la base de données enrôlé). Une fois que l'individu fournit son identifiant qui fait référence à son empreinte déjà inscrite, le système génère un modèle après avoir appliqué le prétraitement de l'image reçu. Le système compare ensuite le modèle d'essai

avec le modèle de référence de cette personne, pour but de déterminer si le modèle d'essai et les modèles stockés de la personne correspondent. (voir Figure2.5)

La vérification est souvent appelée appariement 1 : 1 (un-à-un). Les systèmes de vérification peuvent contenir des bases de données allant d'une dizaine à des millions de modèles inscrits, leurs avantages est qu'ils fournissent des décisions plus exactes, puisqu'on est sure que la personne existe déjà dans la base de données, en plus de leur rapidité quand on compare un individu seulement avec son modèle.

L'une des applications les plus courantes de la vérification est un système qui oblige les employés à authentifier leurs identités revendiquées avant de leur accorder l'accès à des bâtiments sécurisés, à des authentifications par smartphone ou par ordinateurs.

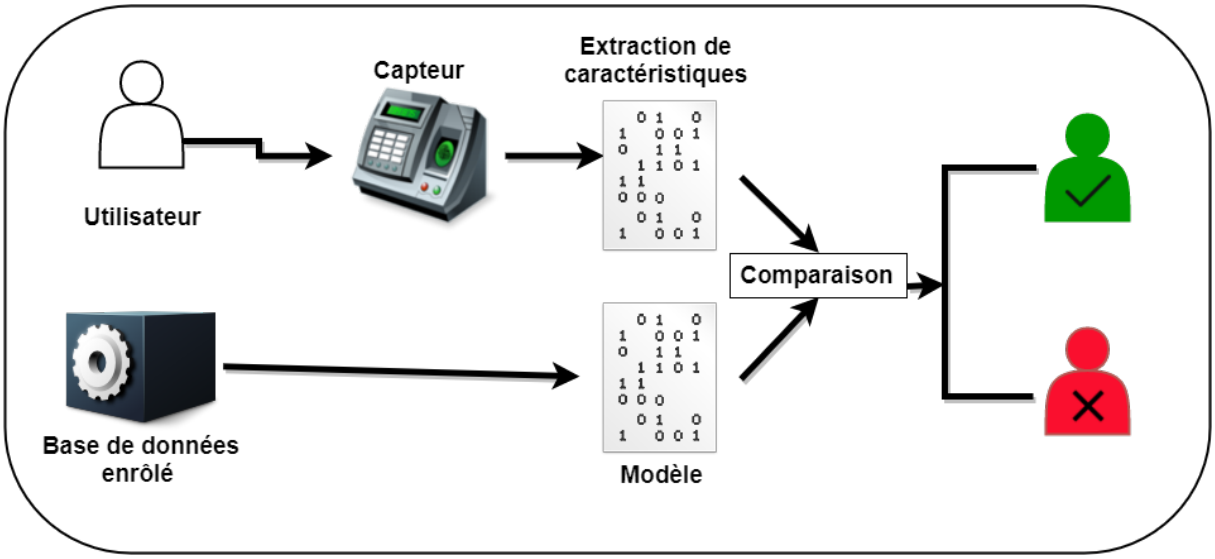


FIGURE 2.5 – Processus de la vérification d'une empreinte digitale.

2.2.3 Identification

Dans les systèmes d'identification, l'étape après l'inscription consiste à identifier la personne. Contrairement aux systèmes de vérification, aucun identifiant n'est fourni et donc on ne possède pas une référence de son empreinte enrôlée. Pour trouver la correspondance, au lieu de localiser et de comparer le modèle de référence de la personne à sa présentation, on compare son empreinte aux modèles de référence stockés de tous les individus enrôlés dans le système, Figure2.6.

Les systèmes d'identification sont appelés appariement 1 : M (un-à-M, ou un-à-plusieurs) parce que la biométrie d'un individu est comparée à plusieurs modèles biométriques dans la base de données du système. Il existe deux types de systèmes d'identification : positif et négatif.

- Les systèmes d'identification positive sont conçus pour s'assurer que les données biométriques d'un individu sont inscrites dans la base de données. Le résultat attendu d'une recherche est une bonne correspondance.

- Les systèmes d'identification négative sont conçus pour s'assurer que les informations biométriques d'une personne ne sont pas présentes dans une base de données. Le résultat attendu d'une recherche est une non-correspondance. De tels systèmes sont utilisés dans les listes des personnes recherchés, le résultat d'identification de l'empreinte digitale assure à toute autre personne ne figurant pas dans la liste un simple passage, sauf en cas de correspondance le système envoie une réclamation aux autorités par exemple.

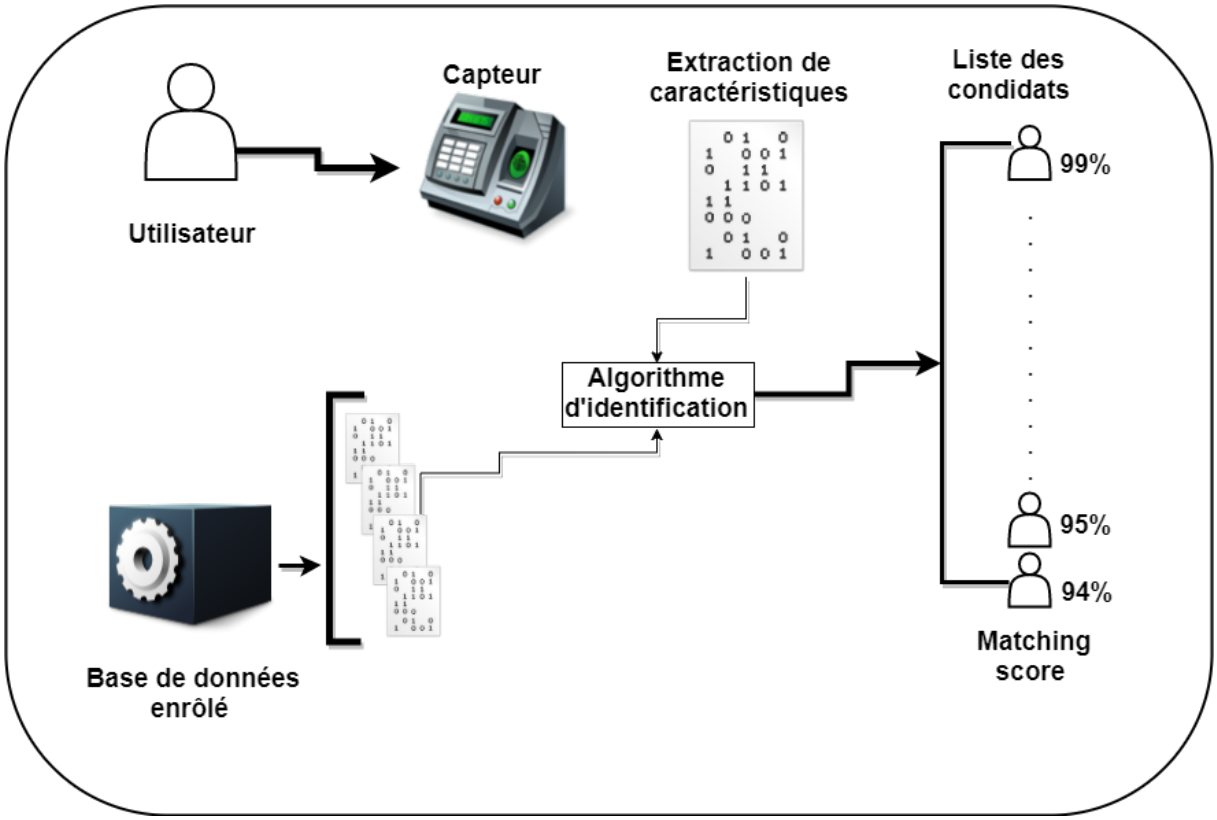


FIGURE 2.6 – Processus de l'identification d'une empreinte digitale.

Les systèmes d'identification sont généralement lents car ils font recours à la comparaison de tous les modèles disponibles dans la base de données. Ils sont généralement connu par la complexité de calcul et le temps de recherche élevé. La raison pour laquelle, des recherches sur la reconnaissance de l'empreinte digitale comme paramètre biométrique, ont partagé le même défi, celui de réduire la complexité de l'identification.

La réduction du temps de recherche et de complexité reviennent principalement à la nature des caractéristiques prises en compte dans la création du modèle. Ceci dit que le choix des caractéristiques influence sur la qualité du système de reconnaissance, identification ou verification. La différence entre un système et un autre réside dans de la manière d'utilisation et manipu-

lation des caractéristiques de l'empreinte digitale pour fournir le modèle de référence, c'est alors ce qu'on appel l'indexation. Ceci fera l'objet principal de cette thèse.

2.3 Caractéristiques de l'empreinte digitale

Parmi tous les systèmes biométriques, les empreintes digitales ont le plus haut niveau de fiabilité et ont été largement utilisées par les experts médico-légaux dans les enquêtes criminelles. Une empreinte digitale se réfère à l'écoulement des modèles de crête papillaires dans la pointe du doigt comme figuré dans l'image 2.7. L'écoulement de la crête présente des anomalies dans les régions locales du bout du doigt, et c'est la position et l'orientation de ces anomalies qui sont utilisées pour représenter et faire correspondre les empreintes digitales.

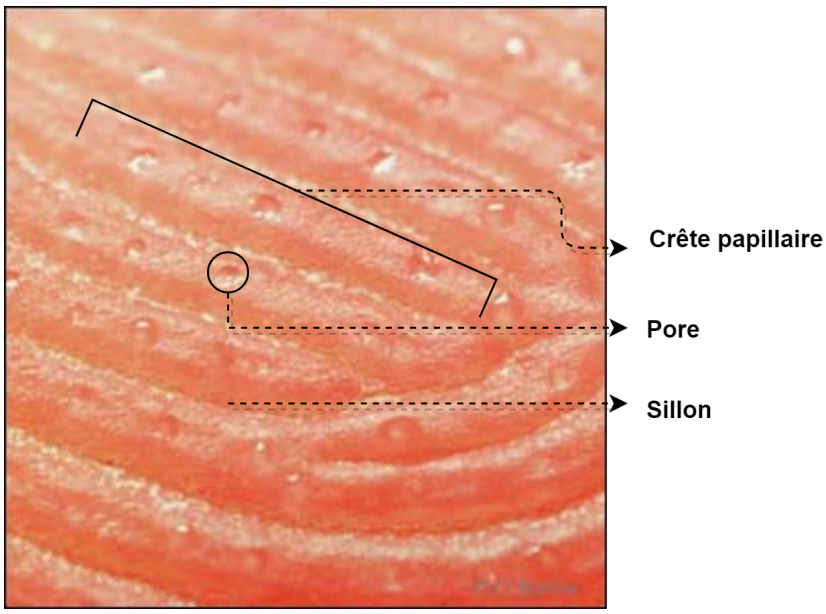


FIGURE 2.7 – L'anatomie de la peau du doigt.

Bien que n'étant pas scientifiquement établi, les empreintes digitales sont considérées comme uniques chez les individus et entre les doigts du même individu. Les dessins digitaux ont trois caractéristiques principales :

✾ **Ils sont individuels** : il est admis que tous les êtres humains possèdent des dessins digitaux différents. Les jumeaux monozygotes ont aussi des empreintes digitales différentes. Même les jumeaux identiques ayant un ADN similaire, sont censés avoir des empreintes digitales différentes.

✾ **Ils sont immuables** : le dessin digital ne change pas depuis sa formation lors de la vie intrautérine jusqu'à sa destruction lors de la putréfaction du corps.

✽ **Ils sont inaltérables** : les dessins digitaux prennent leurs origines dans les couches profondes du derme et lorsque survient une destruction superficielle de l'épiderme, les dessins digitaux se reforment à l'identique lors de la cicatrisation. En revanche, les destructions plus profondes du derme ou certaines maladies de peau peuvent détruire durablement les dessins digitaux.

L'unicité d'une empreinte digitale est déterminée par le relief topographique de la crête et la présence de certaines anomalies de crête nommées minuties. Généralement, la structure d'empreintes digitales est classée en deux catégories : les caractéristiques globales et locales.

✽ Les caractéristiques globales sont les points singuliers : Ogive et delta, obtenus aux points où les arêtes changent d'orientation, ce qui influence largement sur le champs directionnelle. Ils déterminent la structure topologique et le type d'empreinte digitale. Leurs positions et leurs nombres d'occurrence dans l'empreinte, permettent de définir une classification de l'empreinte digitale en six classes principales proposées par Henry comme montré dans la Figure 2.8.

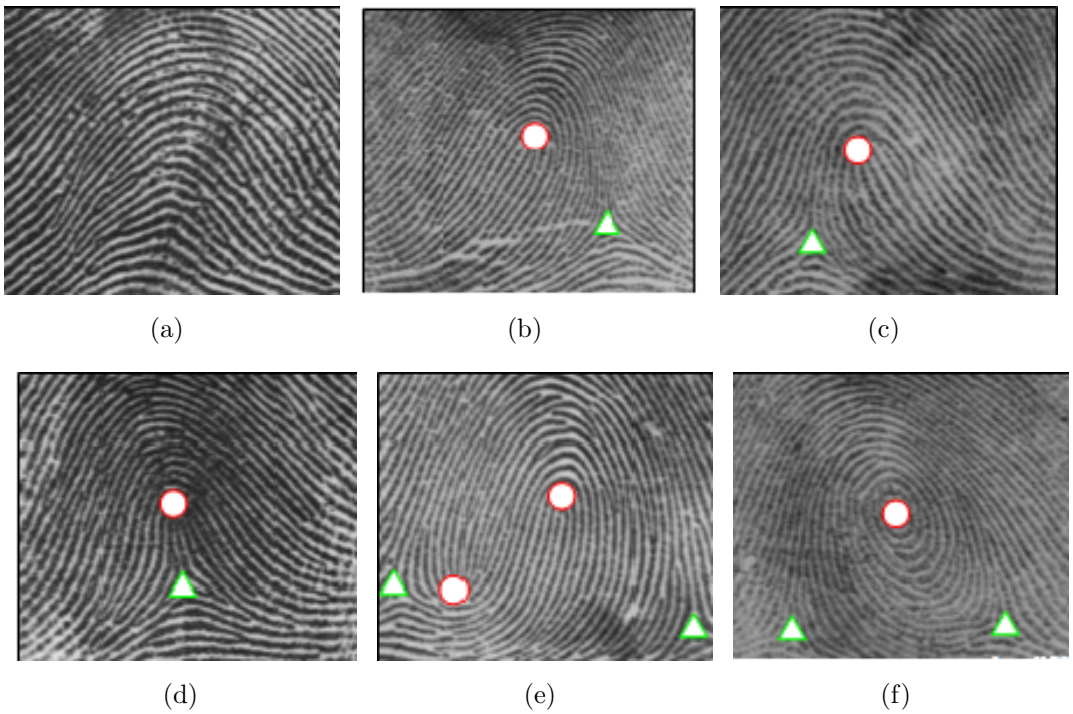
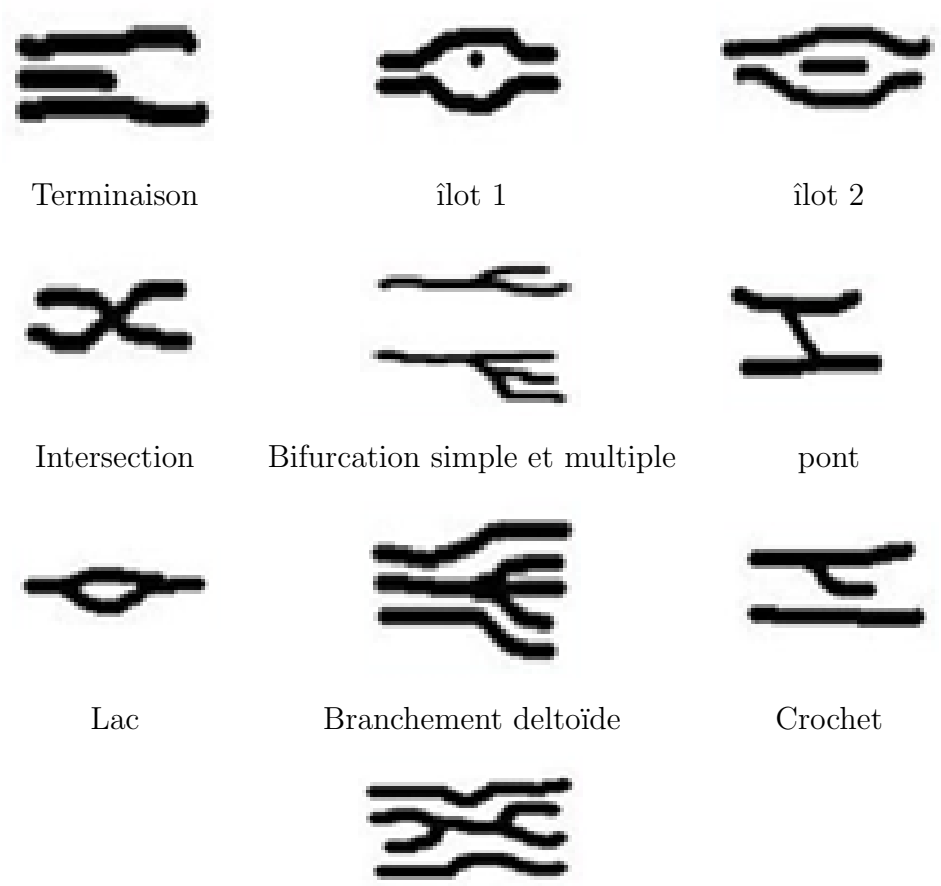


FIGURE 2.8 – les classes d'Henry : (a) Arc ; (b) leftloop ; (c) rightloop ; (d) Arc tendu ; (e) Double ogive ; et, (f) Ogive.

✽ Les caractéristiques locales appelées minuties (voir les figures dans 2.4.3), représentent la forme de l'intersection des arrêts de crêtes. En littérature, il existe dix formes de minuties, tandis que les méthodes d'indexation n'utilisent que deux types de minuties, les terminaisons et les bifurcations, car toutes les autres formes sont représentées par une multiplication de bifurcations ou de terminaisons. Ces deux modèles créent l'unicité de

l'individu ainsi que leurs positions dans l'empreinte digitale est considérée comme un facteur déterminant de différenciation.

Typiquement, la configuration globale définie par la structure de crête est utilisée pour déterminer la classe de l'empreinte digitale, tandis que la distribution des points de minutie est utilisée pour correspondre et établir la similarité entre deux empreintes digitales.



Terminaison	îlot 1	îlot 2
Intersection	Bifurcation simple et multiple	pont
Lac	Branchement deltoïde	Crochet
Branchement opposé		

TABLE 2.1 – Les différents types de caractéristique locaux : minuties

Les systèmes d'identification automatique des empreintes digitales, s'appuient sur l'utilisation de l'indexation basée sur la transformation des caractéristiques locales, sur la classification par les caractéristiques globales ou par la combinaison des deux types de caractéristiques. Dans cette thèse nous allons (i) étudier la performance de travailler par des caractéristiques locales depuis une nouvelle approche d'indexation, (ii) montrer l'avantage des points singulier globaux (iii) et étudier l'amélioration par la méthode hybride.

2.4 Extraction des caractéristiques

L'extraction des caractéristiques de l'empreinte digitale permet de restreindre l'application des méthodes d'indexation des images. En partant d'une image contenant des informations multiples à grande échelle, vers un nombre précis de descripteurs numériques portant des informations propres à l'empreinte digitale et facilitant l'application du processus d'indexation.

Un processus de prétraitement est nécessaire avant l'extraction des différents descripteurs de l'empreinte digitale, ainsi que l'image reçue depuis le capteur numérique doit être nettoyée afin de garder que l'information utile. Nous détaillons les étapes du processus dans les sections qui suivent.

2.4.1 Binarisation

Du à l'environnement de l'acquisition, à la qualité du capteur et à la résolution au niveau de gris, une quantité de l'information inutile s'ajoute à l'image d'empreinte digitale résultante. Cette information est représentée dans les pixels bruités, des pixels manquants et parfois des taches de particules glissées dans le capteur lors de l'acquisition. Dans ces conditions, il est important de dériver la forme des crêtes et d'enlever les pixels de fond, ainsi que l'information qui pourraient être extraites d'une empreinte scannée doit être simplement binaire afin de faciliter les traitements.

Le but de la binarisation (le seuillage) d'images à niveaux de gris est de séparer les pixels de l'image en deux classes, la première représente les pixels qui appartiennent au fond, et la seconde représente ceux appartenant à l'objet (crêtes de l'empreinte).
L'approche la plus simple est la segmentation par seuillage adaptatif ou global. Cependant, le problème dans la réalisation de la binarisation est que toutes les images d'empreintes digitales n'ont pas les mêmes caractéristiques de contraste, de sorte qu'un seul seuil d'intensité utilisant un seuillage global ne peut pas être appliqué. Certaines approches, comme Ratha *et al.* (1996), utilisent le fait qu'il existe une différence significative dans les amplitudes de variation des niveaux de gris le long et à travers les crêtes.

La méthode largement utilisée est la segmentation développée par Otsu ; Otsu (1979) et Sezgin *et al.* (2004a) ; Il consiste à maximiser la variance interclasse définie comme une somme pondérée des variances des deux classes (équation (2.1)), et plus cette variance est grande, plus le seuil va segmenter correctement l'image. Cette méthode a montré de bons résultats. Dans la Figure2.9 nous présentons la différence entre les deux approches de segmentation, seuillage global et Otsu.

$$\sigma^2 = \omega_0(t)\omega_0^2(t) + \omega_1(t)\omega_1^2(t). \tag{2.1}$$

Avec ω_0 , ω_1 représentent les probabilités des deux classes séparées par un seuilt, et ω_0^2 , ω_1^2 sont les variances de ces deux classes.

(a) (b)

(c)

FIGURE 2.9 – La différence de segmentation. (a) Empreinte d'origine ; (b) Binarisation par seuillage globale ; et, (c) Binarisation par la méthode d'Otsu.

2.4.2 Squelettisation

La notion de squelettisation a été introduite la première fois par Blum en 1967 dans Blum (1967), tout simplement le squelette prend le médiane de l'objet et son épaisseur ne dépasse pas un seul pixel, donc il permet de faire une description de l'objet, le squelette facilite beaucoup les traitements dans le domaine de l'imagerie et précisément il est présent dans la reconnaissance de l'empreinte digitale,du fait qu'il représente les crêtes épaisses en une ligne d'un seul pixel, qui facilite l'extraction des points minuties et les repérer par un point de l'espace 2D. Les avantages de squelette sont :

⇛ **L'invariance** : le squelette de l'objet est invariant aux transformations linéaires.

⇛ **L'homotopie** : il garde la connexité de l'objet, le squelette et l'objet ont le même nombre des composantes connexes.

⇛ **La réversibilité** : à partir de squelette on peut construire l'objet initial.

⇛ **L'épaisseur** : en général un pixel suffit aux intersections où il est parfois nécessaire d'ajouter un pixel pour garder la connexité.

Dans la littérature, il existe plusieurs méthodes qui peuvent être groupées en quatre grandes catégories :

— **Amincissement topologique** : consiste à enlever au fur et à mesure les pixels du contour de la forme, tout en préservant ses caractéristiques topologiques. En effet cette méthode commence du contour initial de l'objet, étudie la connexité de chaque pixel du contour dans un voisinage, et retire ceux dont la suppression n'influence pas sur la topologie de l'objet. Ces points sont enlevés soit successivement, soit en parallèle, ou encore à l'aide d'opérations morphologiques. Le squelette est obtenu en érodant itérativement les couches frontières de l'objet. Ces méthodes permettent d'avoir un squelette homotope à l'objet par construction, mince et géométriquement représentatif mais pas forcément centré. Kong et Rosenfeld ont ajouté cette notion de préservation de la topologie à la définition du squelette dans Kong et Rosenfeld (1989).

— **Carte de distance** : Consiste à associer à chaque point de la forme sa distance au point le plus proche du contour comme a démontré Attali et Thiel (1993). Les maxima locaux de la carte de distance représentent les points du squelette. L'extraction du squelette se fait en deux étapes :

⇛ **Étape 1** : recherche de l'axe médian grâce aux maxima locaux de la carte de distance. Ce sous-ensemble est fin, mais généralement non connexe ;

⇛ **Étape 2** : recherche des configurations de voisinage dans la carte de distance afin de retrouver des lignes de crête ou des arêtes de la surface associée, ou encore des chemins (ou cluster) qui vont connecter l'ensemble des maxima locaux dans le but de rendre le sous-ensemble connexe.

Le squelette résultant n'est pas nécessairement homotope ni nécessairement fin mais il est centré.

— **les simulations de propagation de feu de prairie** : Xia (1989) basées sur le principe de prairie couverte de façon homogène d'herbe sèche. Au départ, tous les points qui constituent le contour sont enflammés simultanément. Le feu se propage de manière homogène et à vitesse constante. Les points de rencontre des différents fronts enflammés constituent le squelette.

— **Diagramme de Voronoï (ou méthode continue)** : Attali *et al.* (1995) ; consiste à choisir des points discrets sur le contour continu de l'objet. Le squelette représente un sous-graphe du diagramme de Voronoï de ces points, entièrement contenu dans l'objet. Cette méthode est basée sur les points du contour de l'image, ce qui représente une petite quantité de données. Le squelette obtenu est connecté,

topologiquement équivalent à l'objet, plus centré et fin. Cependant, cette méthode peut poser des problèmes en ce qui concerne la complexité des algorithmes et les temps de calculs qui sont énormes.

La méthode de squelettisation utilisée dans ce mémoire est basée sur l'algorithme de base de (Zhang et Suen (1984), est considérée comme une méthode rapide et parallèle. La majorité des algorithmes récents l'utilise vu la qualité du squelette générée (Parker (2010)).

La sélection de cet algorithme est dû au besoin de construire un squelette de l'empreinte digitale mince, qui respecte le chevauchement des crêtes papillaires ainsi que leurs formes. Un exemple d'application de la méthode Zhang est illustré dans la Figure2.10.

(a)

(b)

FIGURE 2.10 – Squelettisation : (a) Empreinte originale ; (b) Empreinte squelettisée par la méthode de Zhang.

2.4.3 Extraction des minuties

Les minuties sont les motifs les plus utilisés pour la comparaison d'empreintes digitales, depuis les travaux initiaux. Elles constituent la principale information des empreintes digitales. Étymologiquement, le terme se réfère à des "petits détails". En pratique, il s'agit de la dénomination des discontinuités des crêtes d'un motif d'empreinte digitale. L'extraction des minuties d'une empreinte digitale suppose donc, simultanément, l'extraction d'une localisation suffisamment précise des crêtes. L'extraction la plus générale des minuties consiste à distinguer les terminaisons (ridge ending) et les croisements (bifurcations) ; illustrées dans la Figure 2.11.

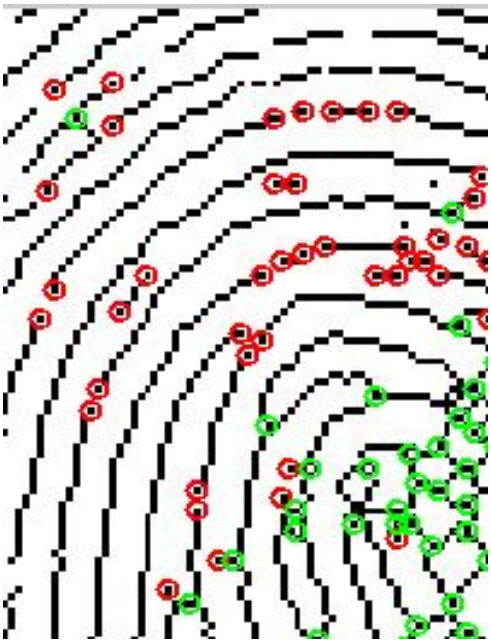
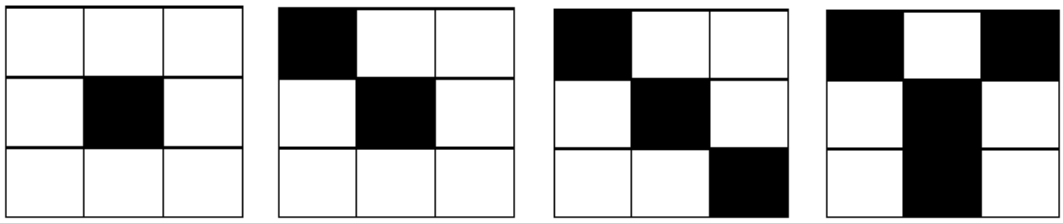


FIGURE 2.11 – L'extraction des minuties par la méthode CR : Bifurcation en vert, et terminaison en rouge

Les bifurcations et les terminaisons sont les caractéristiques les plus significatives de l'empreinte digitale. Dans la plupart des approches, l'extraction faite en divisant l'empreinte digitale squelettisée en blocs. Alain de Boer *et al.* (2001) considère que la bifurcation est identifiée par l'intersection de trois pixels voisins, alors qu'une terminaison est un pixel ayant un seul voisin. Pour améliorer la certitude et la qualité des minuties extraites, ainsi que de diminuer le nombre de fausses extractions, des approches telles qu'Arcelli MuñOz-BriseñO *et al.* (2013), ont valoriser la méthode du Cross Number **(CN)** calculé à partir de nombres de voisins sur un bloc de huit pixels avec :

— CN = 0 : Pixel isolé, non pris en compte ;
— CN = 1 : Minutie de type terminaison ;
— CN = 2 : Les minuties n'existent pas ;
— CN = 3 : Minutie de type Bifurcation ;



CN = 0	CN = 1	CN = 2	CN = 3

TABLE 2.2 – Les connectivité possibles autour d'un pixel.

Cependant, l'extraction des minuties n'est pas authentique en raison du traitement de l'image et du bruit dans l'image d'empreinte digitale. Alors que l'erreur des minuties manquantes ou ajoutées existe toujours.

2.4.4 Orientation

Le champ d'orientation d'une image d'empreinte digitale représente l'orientation locale des structures de crêtes et est calculé sur une grille régulière dans l'empreinte digitale. Dans la littérature, diverses méthodes démontrées par Liu *et al.* (2007a), Ratha *et al.* (1996) et Kumar *et al.* (2016) ont été développées pour estimer l'orientation déposée. Le DF ou champs d'orientation ; comme illustré dans la Figure 2.12; est généralement utilisé pour extraire le point singulier comme étant un descripteur global pour une méthode d'indexation basée sur la classification de l'empreinte ou l'appariement global.

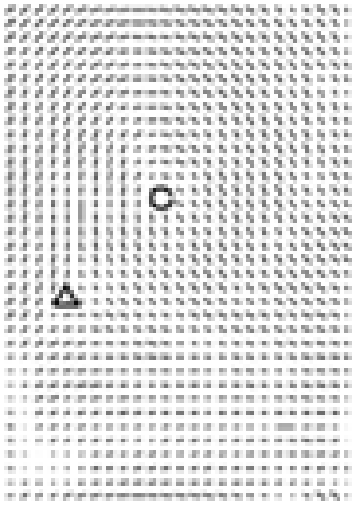


FIGURE 2.12 – Exemple de champs d'orientation (DF)

2.4.5 Mesures des performances

Généralement, les performances du système biométrique peuvent être évaluées en considérant les principales valeurs suivantes :

(1). La Taille de la base de données.

(2). La vitesse du système biométrique.

(3). La précision sur la reconnaissance d'un utilisateur.

La performance de reconnaissance est évaluée en utilisant deux indices d'erreur : le **FAR** , le pourcentage de faux utilisateurs acceptés, et le **FRR**, le pourcentage de vrais utilisateurs refusés.

Le taux **FAR** ***(False accept rate)*** ; calculé selon l'équation 2.2; est la probabilité que le système autorise de manière incorrecte une personne non autorisée qu'on notera **Imposter**, en raison de l'appariement incorrect de l'entrée biométrique avec le modèle enrôlé comme l'illustre la Figure 2.13. Le FAR est normalement exprimé en pourcentage suivant sa définition.

$$FAR = \frac{number\ of\ accepted\ imposter}{total\ number\ of\ imposters} \tag{2.2}$$

$$FRR = \frac{number\ of\ rejected\ genuine}{total\ number\ of\ genuine} \tag{2.3}$$

Le taux de **FRR** ***(false reject rate)*** ; calculé selon l'equation 2.3; est la probabilité que le système rejette de manière incorrecte l'accès à une personne autorisée **Genuine**, en raison de l'échec de l'appariement de l'entrée biométrique avec un modèle enrôlé, comme l'illustre la Figure 2.14.

Dans un système biométrique idéal, ces pourcentages seraient tous les deux nuls. Malheureusement, le système idéal n'existe pas et il faudra donc choisir un compromis entre les valeurs **FAR** et **FRR**, le grand défi de différentes approches de reconnaissance biométrique est de maintenir ces deux index à la baisse.

Pour évaluer le pourcentage global d'erreur du système, on utilise l'**EER** ***(Equal Error Rate)***, défini comme le pourcentage lorsque le **FAR** et le **FRR** sont égaux comme montré dans la Figure2.15. Dans un système biométrique, il faut définir une valeur de seuil en plus d'une mesure de ressemblance pour établir la comparaison de deux données biométriques et donner la décision finale. Si le taux de comparaison mesurée dépasse la valeur du seuil, le système reconnaîtra l'identité de l'utilisateur sinon il le rejette dans le cas échéant. Naturellement, l'administrateur du système biométrique, lorsqu'il établit une valeur seuil, choisit un compromis entre la probabilité de fausses acceptations (permettant l'accès à la mauvaise personne) et les faux rejets (refusant l'accès à la bonne personne).

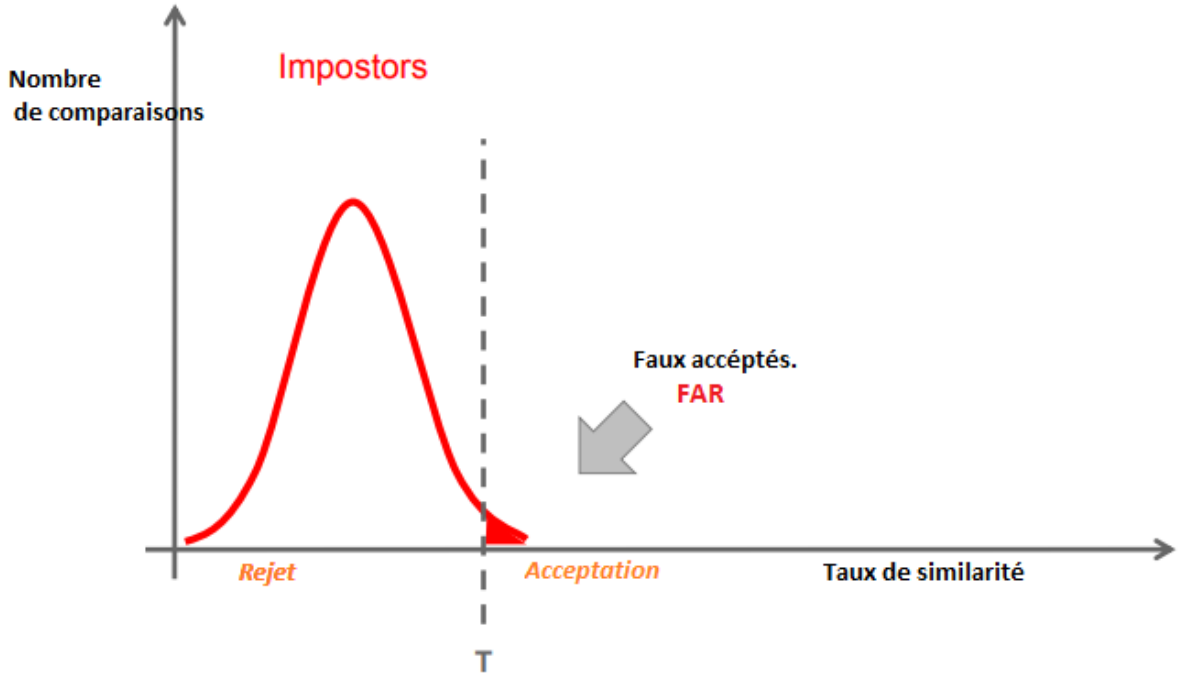


FIGURE 2.13 – L'intervalle de définition de **FAR** selon un seuil T.

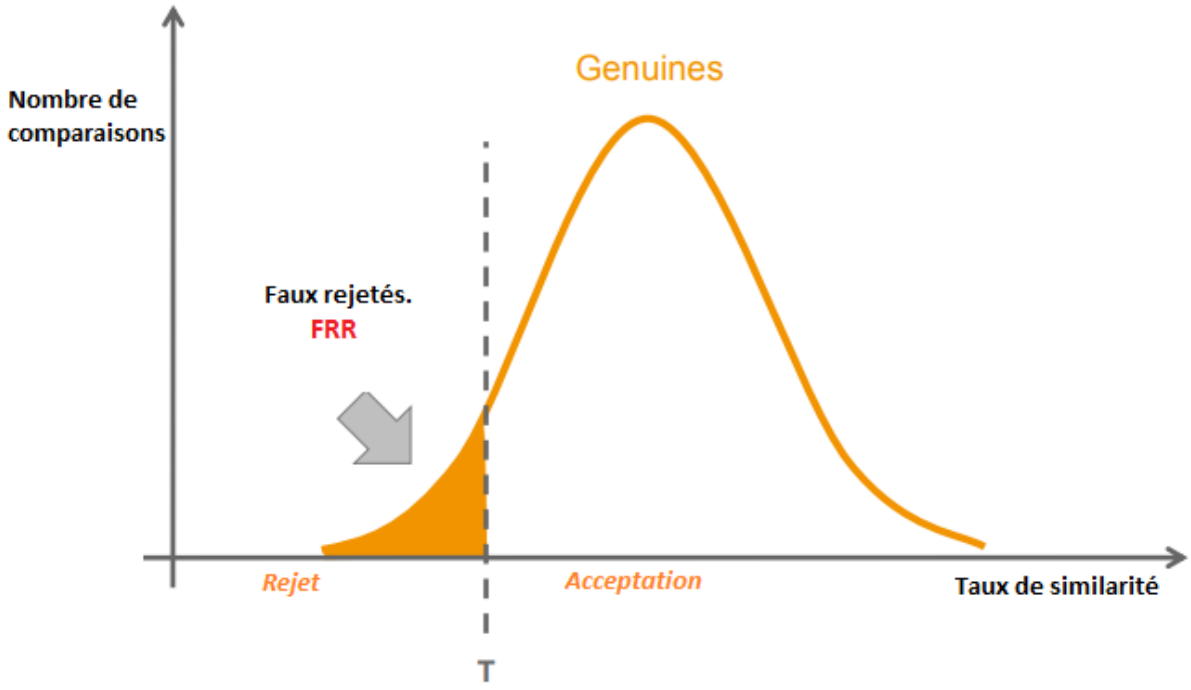


FIGURE 2.14 – L'intervalle de définition de **FRR** selon un seuil T.

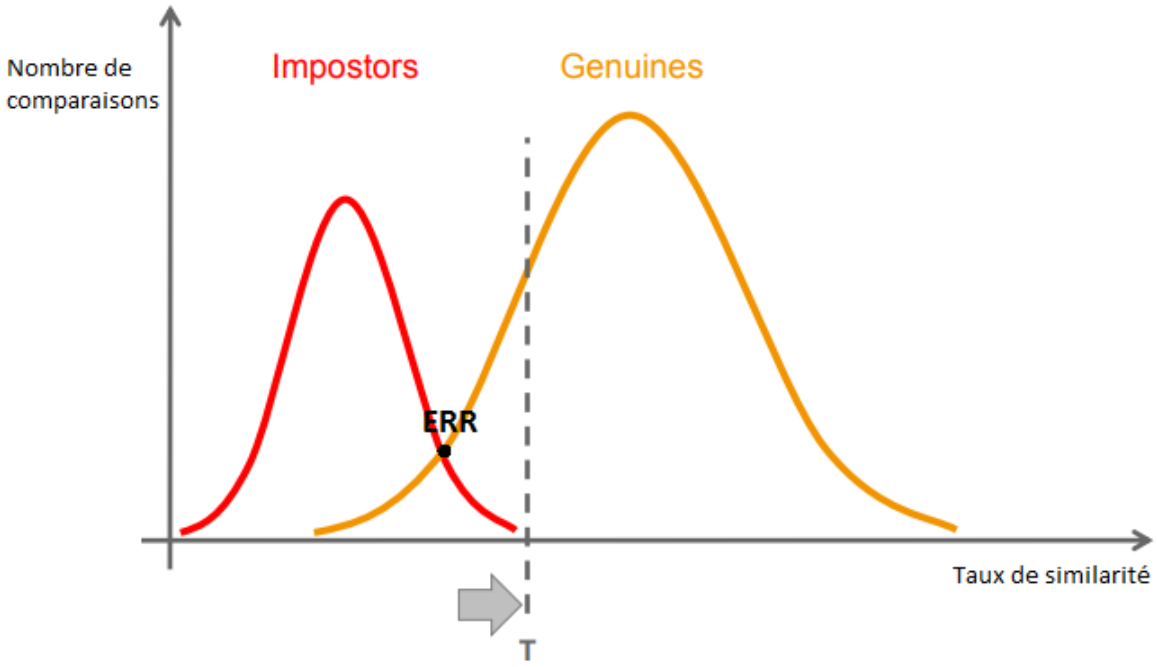


FIGURE 2.15 – L'intervalle de définition du point d'équilibre **ERR**.

Les **FAR** et **FRR** dépendent beaucoup des caractéristiques biométriques utilisées et de la mise en oeuvre technique de la solution biométrique. En outre, le **FRR** dépend fortement de la personne, un **FRR** personnel peut être déterminé pour chaque individu. Le **FRR** peut également augmenter en raison de conditions environnementales lors de l'acquisition ou d'une utilisation incorrecte, par exemple lors de l'utilisation de doigts sales sur un lecteur d'empreintes digitales. Tandis que l'erreur du FAR revient généralement à la performance des caractéristiques utilisées comme méthode d'indexation. Finalement, les systèmes biométriques représentent l'évaluation d'un système par la courbe **ROC** ***(Receiver Operating Characteristics)***, définissant la proportionnalité entre le **FAR** et **FRR** selon les différentes valeurs du seuil T.

2.5 Méthodes d'indexation et de reconnaissance

L'appariement (matching) d'empreintes digitales consiste à comparer et à calculer l'indice de similarité, puis à générer un score de correspondance de deux empreintes digitales pour les procédures de vérification ou d'identification. Cet indice est calculé sur la base

d'une méthode d'indexation, qui est le principal défi de la reconnaissance des empreintes digitales. De nombreuses approches d'indexation ont été proposées dans la littérature, comme résumé dans **?**, divise les algorithmes d'appariement d'empreintes digitales par index en deux classes différentes : (i) les méthodes d'indexation basées sur la corrélation et (ii) les méthodes basées sur les minuties.

✾ **Les méthodes d'indexation basées sur la corrélation** : calculent la correspondance de deux empreintes digitales superposées, en recherchant la corrélation à partir de pixels dans les deux images selon les différents alignements, indépendamment de leurs formes ou de leurs caractéristiques. Les approches basées sur la corrélation sont faciles à implémenter. Cependant, en raison de la nature de la peau, ces méthodes ne sont pas robustes aux problèmes majeures de la variation de l'image d'empreinte digitale, car les déplacements de pixels rendent deux impressions du même doigt très différentes. Les conditions de la peau au moment de détection et le contraste/luminosité peuvent influencer sur les caractéristiques d'empreintes digitales.

✾ **Les méthodes basées sur les caractéristiques des minuties extraites** : ont montré un résultat encourageant, car elles sont robustes aux transformations affines de l'image ou à certaines contraintes de qualité lors de la détection. Le principe de ces méthode repose sur l'utilisation des points minuties comme indice de l'indexation, comme les coordonnées, l'orientation, le nombre des bifurcations et terminaison, ou alors leurs transformations comme la triangulation des points extraites, la transformation en d'autres formes géométriques et graphe (exp : coquille proposé par Moujahdi *et al.* (2014)).

Dans cette thèse nous allons nous intéresser aux méthodes basées sur la triangulation des points minuties comme indice principal de comparaison des empreintes digitales.

2.5.1 Algorithmes d'indexation basées sur la triangulation.

La triangulation est un outil efficace dans le traitement d'un ensemble de données dispersées. Les points minutiae étant dispersés sur la carte, il faut un moyen de localisation pour conserver leur structure topologique. La triangulation des minuties a connu un grand progrès dans les algorithmes d'appariement et d'indexation.

Dans une méthode d'appariement, Liu *et al.* (2005) a produit des triangles partant du point central de l'image d'empreinte digitale, formant un arc avec le plus proche pour compléter tous les points minutiae. Cette méthode a donné de bons résultats en termes de complexité $\mathbf{O(xlogx)}$. de Boer *et al.* (2001) et Bebis *et al.* (1999), ont utilisé la triangulation de Delaunay, elle consiste à générer le plus grand nombre possible de triangles avec les points de minuties générés. La multiplication des triangles a été choisie afin d'augmenter la pertinence de l'indexation et de l'identification puisque la triangulation ne prend pas en compte la nature des minuties ou la taille de l'image, car elle utilise des traits très importants et fiables.

Le problème deBebis *et al.* (1999) et de Boer *et al.* (2001), est que le nombre de triangles générés peut créer un point négatif pour ce genre d'algorithmes, car il peut s'agir d'une fausse minutie donc de faux triangles, ce qui diminue la qualité de l'algorithme. C'est pourquoi certaines approches sont proposées pour réduire le nombre de triangles générés, mais ce n'est pas aussi fiable qu'il peut éliminer les points utiles. D'autres approches comme Liang *et al.* (2006), sont basées sur les caractéristiques formées par les triangles obtenus, comme les longueurs d'arc, les clous ou les triangles de surface.

2.5.2 Algorithmes basés sur la classification

Un certain nombre d'approches de classification des empreintes digitales ont été développées pour accélérer le processus de recherche dans les grandes bases de données ; un benchmark a été proposé par Galar *et al.* (2015). Bien que les méthodes d'indexation basées sur les minuties et leurs caractéristiques donnent de bons résultats, cela n'est pas évident dans le cas de la difficulté d'extraire des minuties, ce qui est dû à des images de pièces très bruyantes ou manquantes. Sur la base de ce principe, les approches de classification ont été basées sur l'estimation de la forme générale définie par Henry, tout en exploitant le champ d'orientation de l'image.

Nous présentons dans la table 2.5.2 une synthèse des approches d'indexation des empreintes digitales, selon les différentes étapes de reconnaissance.

les étapes de reconnaissance	Algorithme			Jain et Pankanti (2000)	MuñOz-BriseñO *et al.* (2013) et Liu *et al.* (2005)	Khodadoust et Khodadoust (2017)	Liang *et al.* (2006)	Assogba et Ali (2011) et Galar *et al.* (2015)
Prétraitement	Orientation			X			X	X
	Squelettisation			X	X		X	X
	Binarisation			X	X	X	X	
Caractéristiques utilisée pour l'indexation	Minuties			X	X	X	X	
	Classification			X	X	X	X	
	Points singuliers			X				X
	Triangulation				X	X		
	Orientation			X			X	X
Matching	matching	Basée sur les minuties	global					X
			local	X	X		X	
		Caractéristiques géométriques des crêtes		X				X
	Triangulation				X	X	X	

TABLE 2.3 – Tableau récapitulatif des différentes approches d'indexation de l'empreinte digitale.

2.6 Conclusion

Dans ce chapitre, nous avons présenté les différents descripteurs de l'empreinte digitale ainsi que les méthodes d'indexation et de création du modèle index. Basée sur le processus de l'indexation, nous avons présenté aussi les méthode de prétraitement ainsi que recenser les meilleures algorithmes de skeletisation, binarization et extraction de minuties adaptées au traitement de l'image d'une façon générale, et au images de l'empreinte digitale plus spécifiquement.

Nous allons détailler dans le chapitre 3 quelles transformations de caractéristiques locales nous allons considéré comme paramètre d'indexation afin d'y appliquer le processus de reconnaissance. Elles sont susceptibles de s'adapter à des méthodes d'identification et de vérification des empreintes digitales, qui permettront alors de remplir la contrainte de la performance et la pertinence, ce qui fera l'objet principal du prochain chapitre.

Chapitre

3 Indexation des empreintes digitales basée sur la triangulation hiérarchique

Sommaire

Comme déjà présenté dans la partie précédente, la reconnaissance des empreintes digitales est l'une des techniques biométriques les plus populaires utilisées dans l'identification et la vérification automatique des données personnelles. Les méthodes de reconnaissance sont basées essentiellement sur l'utilisation des points caractéristiques extraites pour créer le modèle de référence pour indexer l'image dans la base de données à enroulé. Le problème majeur des méthodes d'indexation est la robustesse aux transformations de l'image requête ce qui diminue la pertinence du système. Quelles sont les meilleures caractéristiques à exploiter et comment peut-on contribuer pour augmenter la pertinence de reconnaissance ?.

3.1 Introduction

Les méthodes de reconnaissance de l'empreinte digitale s'appuient sur l'utilisation de ses caractéristiques pour des fins de comparaison. L'indexation des empreintes digitales

est considérée comme un véritable défi dans cette piste de recherche. Elle représente un moyen permettant de représenter l'image de l'empreinte d'une façon numérique, simple, et fiable tout en respectant les caractéristiques garantissant l'unicité de l'empreinte digitale.

Dans ce chapitre nous allons présenter une nouvelle méthode d'indexation basée sur l'utilisation des minuties comme caractéristique locale de l'empreinte et l'application de la triangulation de Delaunay d'une façon hiérarchique comme méthode de transformation des caractéristiques extraites. La Figure 3.1 présente un aperçu général de l'approche proposée que nous détaillerons dans ci-après et qui fait l'objet de notre article Elmouhtadi *et al.* (2018b).

Le but de cette approche est d'assurer le bon emplacement des triangles de Delaunay appariés, ce qui signifie que les minuties correspondantes figurent bien dans le même emplacement dans les deux images comparées. Les points forts de cette approche sont résumée comme suit :

— L'utilisation de triangles comme paramètre d'appariement assure la robustesse au zoom de l'image car les triangles conservent la même proportionnalité des paramètres en cas de changement de dimensions.

— La robustesse à la rotation dans le cas d'une image de test pivotée ; les résultats de l'identification resteront inchangés.

— En utilisant seulement les points minuties comme caractéristiques extraites, notre approche est robuste aussi à la qualité d'image, car nous n'utilisons pas la totalité du contenu de l'image d'empreinte digitale.

— L'utilisation de la méthode de triangulation de manière hiérarchique garantit que les minuties trouvées similaires ont la même structure géographique et les mêmes coordonnées dans les deux images. Cela augmente la performance et la pertinence du système.

3.2 Prétraitement de l'empreinte

Comme nous l'avons déjà mentionné dans le chapitre précédant, l'image acquise par les capteurs d'empreintes digitales contient toujours du bruit, du contraste, des pixels manquant et d'autres rajoutés. Ceci impose l'application du prétraitement afin d'éliminer toute information menant à diminuer la performance des descripteurs en premier lieu et par la suite la performance de la méthode d'indexation appliquée.

Dans cette partie, nous allons commencé par l'application du processus de prétraitement avant d'extraire les minuties qui seront classées par la suite dans un vecteur de terminaisons et de bifurcations. Plus précisément, nous allons appliquer la binarisation

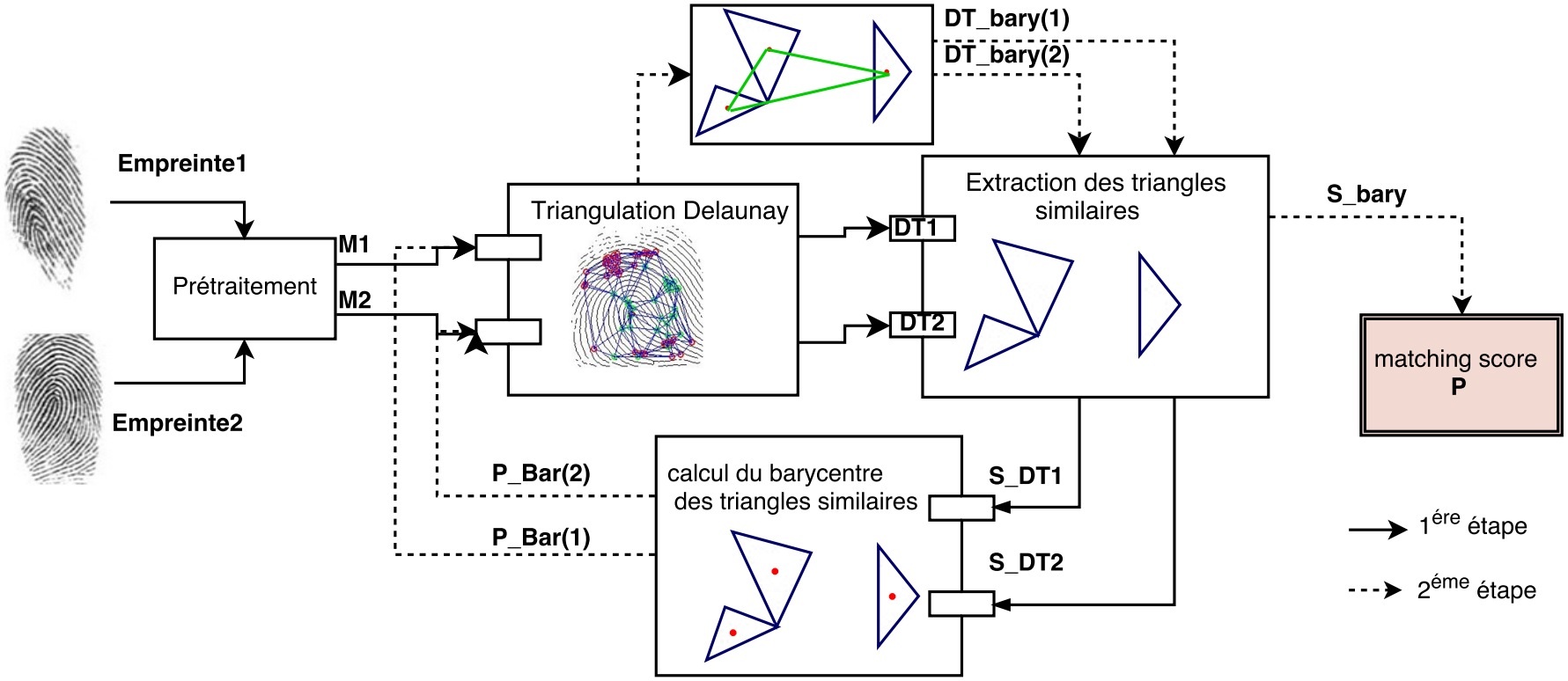


FIGURE 3.1 – Vue d'ensemble de l'approche proposée.

d'Otsu (Sezgin *et al.* (2004a) et Otsu (1979)), l'approche de squelette de Zhang comme démontré en Parker (2010) et TISSE *et al.* (2001)), puis la méthode basée sur le Cross Number pour l'extraction des points minuties MuñOz-BriseñO *et al.* (2013)). Toutes ces méthodes ont été présentées dans le chapitre précédent.

3.3 Transformation des descripteurs.

En fonction du vecteur minuties obtenu, nous générons des triplets par ces points minuties. L'approche de Delaunay triangulation sera appliquée dans le but de générer l'ensemble de tous les triangles possibles sur la totalité de l'empreinte digitale. Ces triangles représentent les descripteurs de l'image de l'empreinte digitale. Alors, pour tout ensemble de points minuties $\boldsymbol{M}$, on associe $\boldsymbol{DT}$ le vecteur de triangles Delaunay correspondant. Pour chaque triangle, comme illustré dans la Figure3.2, nous conservons les indices suivant :

- les minuties M_1 , M_2 et M_3 representant les trois sommets du triangle.
- les longueurs des trois côtés a, b et c.
- les trois angles intérieurs du triangle $\triangle_{M_1M_2M_3}$, que nous notons α_1, α_2 et α_3. Nous calculons les valuers de ces trois angles par le théorème d'Al-Kashi qui permet de déduire les angles intérieurs d'un triangle en fonction des longueurs de ses côtés, selon les equations (3.1) (3.2) (3.3).

$$\alpha_1 = \arccos\left(\frac{a^2 + b^2 - c^2}{2ab}\right) \tag{3.1}$$

$$\alpha_2 = \arccos\left(\frac{c^2 + b^2 - a^2}{2bc}\right) \tag{3.2}$$

$$\alpha_3 = \arccos\left(\frac{a^2 + c^2 - b^2}{2ac}\right) \tag{3.3}$$

Dans le cas normal, la reconnaissance des indices décrivant un triangle est assez suffisante pour juger de la ressemblance de deux triangles, chose qui est impossible à considérer pour le traitement d'images et spécialement dans le traitement des empreintes digitales. Une contrainte qui résulte d'un simple changement au niveau des pixels et conduit à un changement de points d'intérêts, les minuties, suivi par une transformation de leur nature et leur nombre. Ceci génère deux ensembles de minuties tout à fait différents pour une empreinte digitale prise deux fois par exemple. Alors, nous serons face à une production

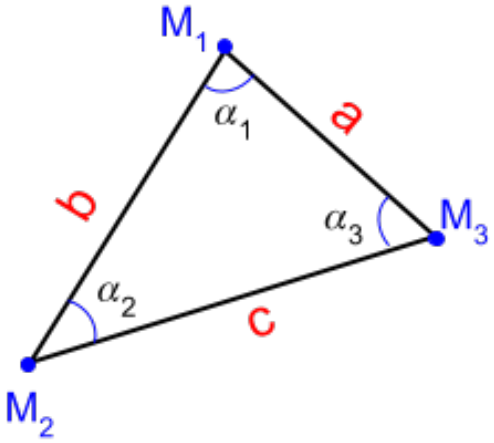


FIGURE 3.2 – Exemple des caractéristiques réservées pour chaque triangle.

de deux ensembles de triangles différents, qui implique un indexe faible et un taux d'appariement faible ce qui implique le rejet d'un utilisateur authentique. Nous détaillerons par la suite toutes les contraintes de transformations.

3.4 Les contraintes de transformations

Historiquement, l'acquisition des empreintes digitales s'est généralement faite sur des surfaces planes, feuilles de papiers ou capteurs optiques. L'acquisition d'empreintes digitales en trois dimensions, par capture photo ou vidéo de doigts sans contact avec un capteur, commence à se répandre. Néanmoins à l'heure actuelle une grande part des bases de données d'empreintes digitales est constituée des images à acquisition plane en deux dimensions.

Nous ferons donc ici l'hypothèse que les empreintes digitales analysées se présentent en deux dimensions, et à échelle unique. Cette particularité fait que l'image de l'empreinte digitale est fortement vulnérable à toutes les transformations linéaires affines dans l'ensemble $\mathbf{M}$ des points minuties.

En plus de la certitude, le défi principale de toutes les méthodes de matching basées sur les triplets de minuties est généralement focalisé sur la tolérance des problèmes de transformations affines sur l'ensemble des caractéristiques linéaires dans une image d'empreinte digitale (Elmouhtadi *et al.* (2016)). Ce changement est principalement dû à la nature de la peau humaine, dont l'élasticité peut causer un déplacement des pixels représentants les minuties. D'autre part la luminosité et la résolution du capteur peuvent changer la nature et les coordonnées d'un pixel representant une minutie.

Pour chaque triangle de $\triangle_{M_1M_2M_3}$ obtenu par la triangulation Delaunay $\mathbf{DT}$ des points minuties, nous notons les cas de transformations linéaire suivants :

3.4.1 Translation de minuties

Considérant comme première contrainte, le taux d'erreur retourné par les algorithmes d'extraction des minuties, et la deuxième contrainte porte sur la différence du choix de l'approche d'extraction par les différents systèmes d'indexation. Pour deux exécutions distinctes d'une seule contrainte ou par concaténation des deux contraintes précédentes, de la superposition de deux ensembles de minuties **M** de la même image résulte un changement d'une ou plusieurs minuties qui peuvent changer de coordonnées en se déplaçant vers les pixels des voisinages. Ceci pose un véritable problème pour une indexation basée sur la triangulation vu qu'une petite translation affine changera les paramètres du triangle.
La Figure3.3 illustre un exemple de translation du point minutie M_1 ; nous obtenons alors un nouveau triangle $\triangle_{M'_1 M'_2 M'_3}$. L'intolérance de ce problème produit un score de matching très faible ce qui diminue la qualité des systèmes d'indexation.

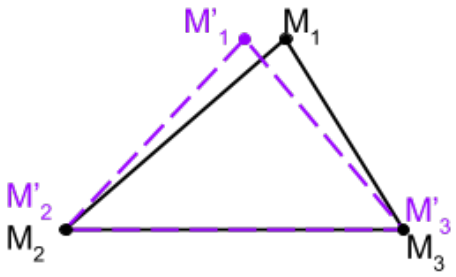


FIGURE 3.3 – Dilatation des minuties .

3.4.2 L'empreinte miroir

L'image d'empreinte requise pourras être reflétée dans le cas d'une reconstitution de l'image, ou bien par les méthodes de prélèvement de traces sur des espaces planes, ce qui donne une empreinte reflétée comme effet miroir (figure3.4). Par conséquent les minuties extraites dans l'image requête n'auront pas le même emplacement comme dans l'image référence de la base de données. Aussi, les triangles obtenus par la Delaunay triangulation auront des paramètres différents dans les deux empreintes.

Ce type de transformations diminue le taux de ressemblance car les deux images sont considérées différentes, et la décision du système peut prendre la valeur de rejet.

3.4.3 Rotation

Si l'on fait abstraction des distorsions non linéaires de la surface du doigt, parmi les raisons majeurs pour lesquelles une image d'empreinte digitale change d'orientation, nous notons (i) la diversité des capteurs selon la qualité et les caractéristiques techniques,

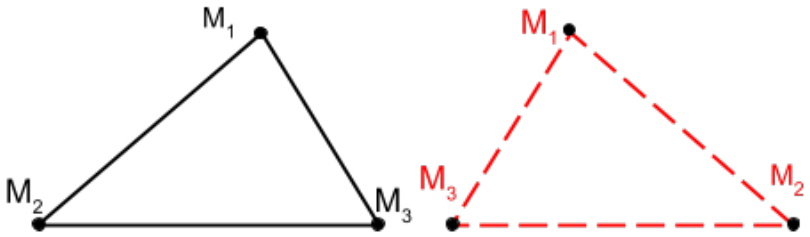


FIGURE 3.4 – Exemple de transformation miroir.

(ii) les conditions de prises ainsi que les protocoles de prises adaptés, (iii) l'origine de l'image, si elle est construite d'après une scène de crime ou bien prise directement du doigt. Ce changement signifie que la transformation affine superposant deux acquisitions d'une même image d'empreinte digitale est atteinte aussi à une rotation affine ; ceci explique que l'orientation des minuties est complètement différente pour la même image, et par conséquent l'obtention de deux triangles $\triangle_{M_1M_2M_3}$ et $\triangle_{M'_1M'_2M'_3}$ (figure3.5) dans le cas de la triangulation des minuties.

Le calcul de l'angle de rotation est une étape importante qui s'est présentée dans un grand nombre de méthodes d'indexation des empreintes digitales. Selon le protocole et l'objectif principal de la méthode d'indexation, l'étape d'extraction de l'angle varie entre le post-traitement et le prétraitement.

- **post-traitement** : Le calcul de l'angle de l'orientation sert à superposer globalement deux images, ce qui permet d'identifier la correspondance des caractéristiques locales, et bien évidement donner la décision de similarité d'une façon globale.

- **prétraitement** : Dans le cas de prétraitement l'angle de rotation consiste spécialement à extraire l'orientation des points caractéristiques, afin d'identifier le type de ces points.

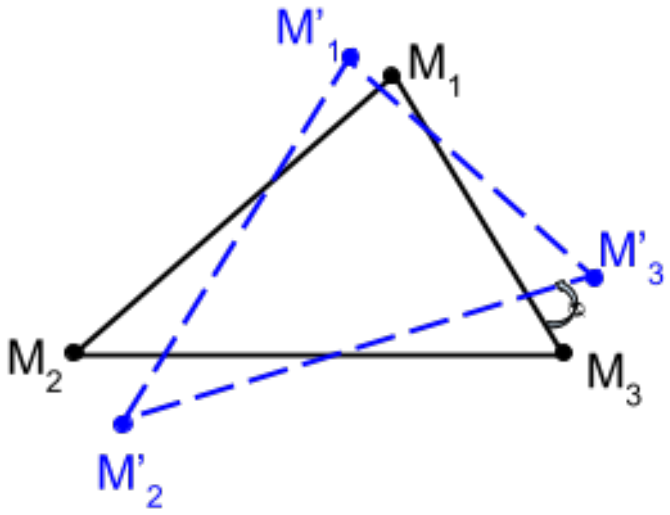


FIGURE 3.5 – Transformation de triplet des minuties par rotation .

3.4.4 Zoom

Comme nous l'avons présenter, la différence dans les capteurs des empreintes digitales ainsi que les conditions de captures fassent que les images obtenues seront de différentes dimensions. cela fait l'objet d'une transformation de zoom en avant ou en arrière.

Dans ce cas les méthodes basées sur la triangulation des minuties semble les plus performantes vu que les triangles gardent les mêmes proportionnalités des paramètres en cas de changement de dimensions, la Figure 3.6 présente une illustration de zoom.

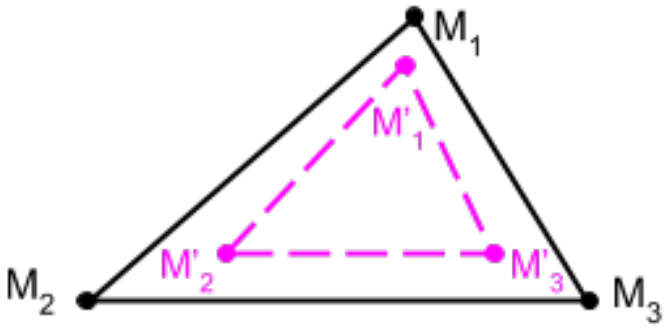


FIGURE 3.6 – Deux triangles similaires de longueurs proportionnelles .

3.5 Comparaison des triangles

Les algorithmes de reconnaissance des empreintes digitales reposent essentiellement sur la comparaison des caractéristiques propres à l'empreinte digitale considérée comme clé primaire selon la méthode utilisée. L'utilisation des triangles dans les méthodes basées

sur la triangulation comme principale caractéristique extraite va restreindre la comparaison à l'ensemble des triangles extraits et aux caractéristiques propres du triangle. Dans cette partie, nous décrivons la méthode de comparaison adaptée pour deux ensembles de triangles.

En appliquant la Delaunay triangulation pour la triangulation des minuties extraites dans une image requête (Empreinte 1) et une image d'utilisateur (Empreinte 2), pour chaque image requête représentée par l'ensemble des triangles $\triangle_{M_{1i}M_{2i}M_{3i}}; (i = \{1..n\})$ avec n est le nombre totale des triangles générés dans DT, nous conservons les paramètres suivants :

- Les minuties $Req(M_1, M_2, M_3)$.
- Les Mesures angulaires $Req\theta(\cos\theta_1, \cos\theta_2, \cos\theta_3)$.
- Tout en considérant une distance euclidienne entre deux points par (3.4).
  Nous conservons la matrice Md_req (3.6) des distances d_{min}, d_{mid} et d_{max} qui représentent respectivement les distances minimales, moyennes et maximales des trois cotés du triangle.

$$d(P_i, P_j) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \tag{3.4}$$

- $Mreq\theta$: la matrice des mesures angulaires pour chaque triangle obtenu (équation (3.5)).

Le choix du cosinus est principalement fondée sur le fait que les mesures angulaires des triangles peuvent changer de valeurs pour tout déplacement des minuties par quelques pixels.

Les mesures trigonométriques (3.1)(3.2) et (3.3), agissent de façon à tolérer les petits déplacements négligeables de minuties, et par conséquent les sommets des triangles. Alors, nous ne manquerons pas de combiner deux triangles avec des coordonnées légèrement déplacées.

$$Mreq\theta = \begin{pmatrix} Req\theta_1 \\ \vdots \\ Req\theta_n \end{pmatrix} = \begin{pmatrix} \cos\theta_{11} & \cos\theta_{12} & \cos\theta_{13} \\ \vdots & \vdots & \vdots \\ \cos\theta_{n1} & \cos\theta_{n2} & \cos\theta_{n3} \end{pmatrix} \tag{3.5}$$

$$Md\_req = \begin{pmatrix} d_{min1} & d_{mid1} & d_{max1} \\ \vdots & \vdots & \vdots \\ d_{minn} & d_{midn} & d_{maxn} \end{pmatrix} \tag{3.6}$$

La méthode de comparaison des empreintes digitales diffère selon l'approche utilisée et les descripteurs clés choisis. Généralement la comparaison entre deux empreintes digitales est basée sur l'appariement des descripteurs locaux au premier plan. Une autre étape de comparaison basée sur la cohérence globale des deux images d'empreintes digitales est présente dans quelques algorithmes. Or celle-ci est obligatoirement précédée par un appariement des descripteurs locaux et elle n'est nécessaire que pour une vérification globale et l'appui de l'étape précédente.

En tenant en compte nos descripteurs locaux représentés par l'ensemble $\triangle_n$ des triangles extraits et leurs caractéristiques calculées, nous considérons une empreinte digitale de test définie par les mêmes paramètres utilisés dans l'image requête (voir la Figure 3.7), nous notons pour chaque élément de l'ensemble $\triangle_m$ des triangles générés dans l'image de test, avec m est le cardinal des triangles :

- les points minuties : $Temp(M'_1, M'_2, M'_3)$.
- les paramètres angulaires : $Temp_\varphi(\cos\varphi_1, \cos\varphi_2, \cos\varphi_3)$ (équation (3.7)).
- les distances des trois côtés $d'_{min}, d'_{mid} et d'_{max}$, respectivement triés dans la matrice Md_{temp}.

$$Mtemp_\varphi = \begin{pmatrix} Temp_{\varphi 1} \\ \vdots \\ Temp_{\varphi m} \end{pmatrix} = \begin{pmatrix} \cos_{\varphi 11} & \cos_{\varphi 12} & \cos_{\varphi 13} \\ \vdots & \vdots & \vdots \\ \cos_{\varphi m1} & \cos_{\varphi m2} & \cos_{\varphi m3} \end{pmatrix} \tag{3.7}$$

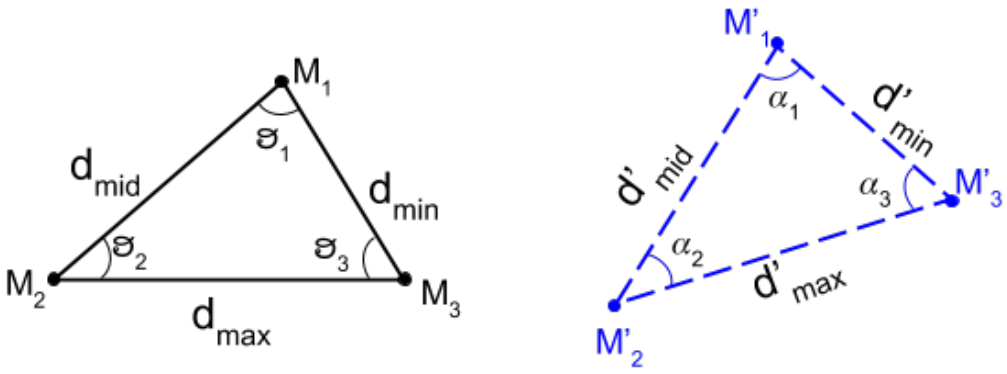


FIGURE 3.7 – Mesures des triangles pour un exemple de rotation affine.

Dans une première étape, nous cherchons les triangles similaires en se basant sur l'extraction de la similarité angulaire dans les deux images (image de test et template), comme montré dans l'algorithme 3.1.

Algorithme 3.1 Extraction des triangles similaires.

pour tout $Req\theta_i$ de $Mreq_\theta$ **faire**
  pour tout $Temp\varphi_j$ de $Mtemp_\varphi$ **faire**
    si $ismember(Req\theta_i, Temp\varphi_j) = (1, 1, 1)$ **alors**
      $S\_Req\theta_i \leftarrow Req\theta_i$
      $S\_Temp\varphi_j \leftarrow Temp\varphi_j$
    finsi
  fin pour
fin pour

Afin d'améliorer la certitude de la similarité trouvée, nous considérons les mesures proportionnelles de distances des trois côtés pour chaque deux triangles trouvés similaires. Cette approche permet de tolérer les transformations affines et le zoom puisque les angles et la proportion des côtés ne changent pas si on considère une transformation de zoom, changement de taille ou déplacement négligeable de minuties.

Comme détaillé dans l'algorithme 3.2, nous calculons les distances des trois côtés et la proportionnalité. Pour chaque triplet $Req(M_1, M_2, M_3)$ et $Temp(M_1, M_2, M_3)$ correspondent respectivement, à $S\_Req\theta_i$ et $S\_Temp\varphi_j$, avec MT est la matrice des triangles appariés.

Algorithme 3.2 Mesures de similarité entre triangles.

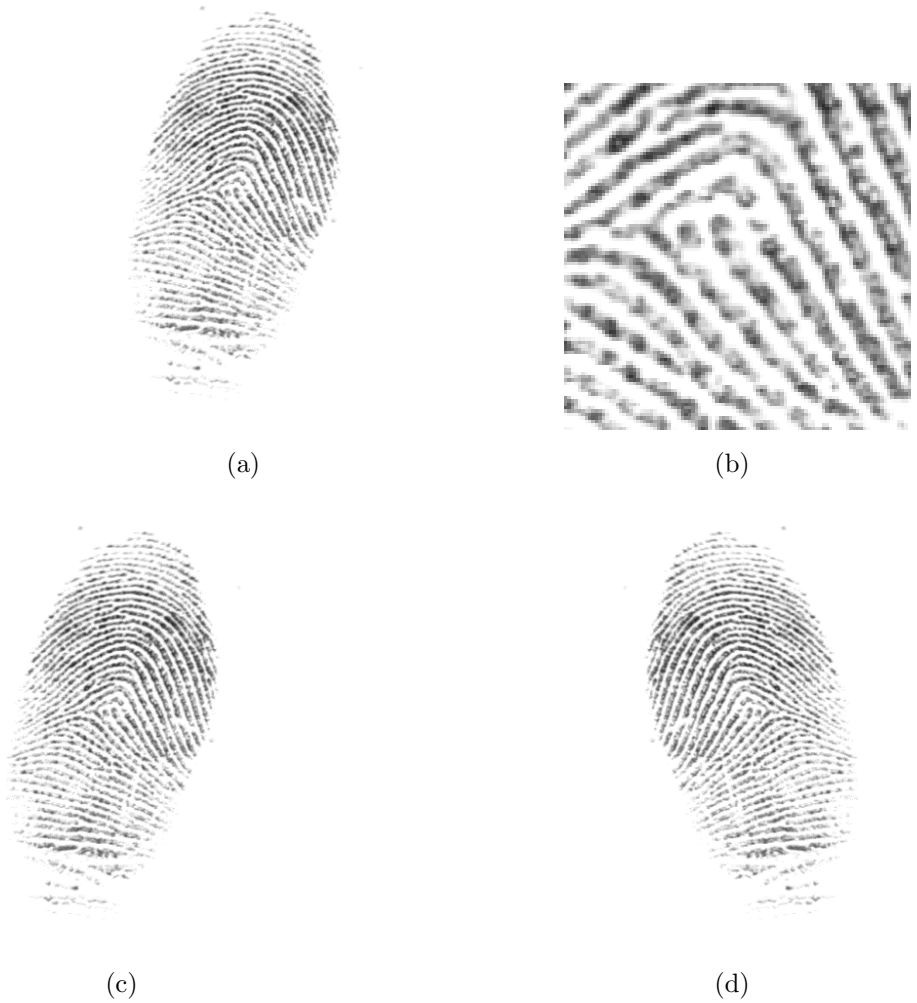
pour tout Md_req correspondante à $S\_Req_\theta i$ **faire**
  pour tout Md_temp correspondante à $S\_temp\varphi j$ **faire**
    si $\frac{d_{maxi}}{d'_{maxj}} = \frac{d_{midi}}{d'_{midj}} = \frac{d_{mini}}{d'_{minj}}$ **alors**
      $Tri_{sim} \leftarrow 1$ et $MT \leftarrow [Req_i]$
    sinon
      $Tri_{sim} \leftarrow 0$
    finsi
  fin pour
fin pour

Finalement, pour obtenir le score de matching, nous calculons la probabilité des triangles trouvés similaires (équation (3.3)), avec :

$|MT|$: est le nombre de triangles trouvés similaires.
$card(Req_i)$: est le cardinal des triangles générés par la Delaunay triangulation.

$$P_{match} = \frac{|MT|}{card(Req_i)} \tag{3.8}$$

Pour un simple test de vérification, nous considérons un ensemble d'empreintes digitales de la base de donnés DB1_B de FVC2004. En comparant la version transformée à l'empreinte digitale d'origine comme le montre la Figure3.8, les résultats du tableau 3.1 montrent la moyenne des taux d'appariement des images considérées selon les différentes transformations. Cela signifie dans un premier temps que notre méthode tolère les transformations majeurs qui réduisent l'efficacité des systèmes de reconnaissance. Ensuite, nous notons que le temps de traitement moyen pour chaque empreinte digitale est d'environ $0,098s$, sur une machine avec processeur Intel®Core™$i5-3230M$.
Ensuite, on peut admettre l'hypothèse que le matching basé sur les triplets donne de meilleurs résultats en terme de complexité.



(a) (b)

(c) (d)

FIGURE 3.8 – Les différents cas de transformations : (a) Image originale $DB1/101\_5$; (b) Zoom ; (c) Rotation avec $\alpha = 20°$; et, (d) Transformation miroir.

	Rotation	Zoom	Miroir
P_{match}	100%	92%	100%

TABLE 3.1 – Résultats de matching pour les différentes transformations.

3.6 Delaunay Triangulation Hiérarchique (HDT)

Nous présentons dans cette section notre approche proposée HDT pour triangulaion Delaunay hiérarchique.

3.6.1 Approche du Barycentre

Après avoir appliquer la Delaunay Triangulation dans une image requête DT1 et une image de test DT2, nous conservons les triangles trouvés similaires dans la matrice Similar_DT (calculer par les méthodes présentées dans le chapitre précédent).

Le problème qui se pose dans cette comparaison, c'est que nous risquons de trouver des triangles similaires, mais de base ils ne sont pas formés par les mêmes points minuties. En effet, même s'il existe une transformation homothétique entre deux triangles cela ne garantit pas qu'ils sont vraiment similaires puisqu'ils peuvent être dans deux positions différentes dans les deux empreintes digitales comparées. Pour faire face à ce problème et prendre en considération l'emplacement des triangles similaires, l'étape suivante de notre méthode consiste à extraire le barycentre de chaque triangle donné dans la matrice Similar_DT.

Comme montré dans les équations (3.9) et (3.10), le barycentre est calculé en utilisant la moyenne des points sommet M_1, M_2, et M_3 pour chaque triangle $\triangle_i(M_1, M_2, M_3)$ dans Similar_DT. Avec $M_1(x, y), M_2(x, y), M_3(x, y)$ les coordonnées des sommets (minuties). Nous conservons les résultats des barycentres calculés dans le vecteur $P_{bar}(x_{center}, y_{center})$.

$$x\_center = \frac{\sum_{i=1}^{3} M_{ix}}{3} \tag{3.9}$$

$$y\_center = \frac{\sum_{i=1}^{3} M_{iy}}{3} \tag{3.10}$$

Afin de conserver la structure topologique des minuties, nous appliquons la triangulation Delaunay DT_bary des points sauvegardés dans le vecteur P_bar, puis nous mesurons la similarité entre DT_bary_1 de l'empreinte digitale d'entrée et DT_bary_2 de l'empreinte digitale comparée.

Pour chaque trois triangles semblables, nous générons un nouveau triangle tel que ses sommets sont les points barycentres des trois triangles à partir de P_bar. Ensuite, nous cherchons à nouveau la similarité dans le nouvel ensemble des triangles généré, par les points de barycentre.

Cette triangulation hiérarchique permettra d'améliorer la décision de similarité des

triangles Delaunay trouvés similaires dans la première phase et garantira que les triangles sont bien localisés de la même façon dans les deux empreintes. Et par conséquent, les minuties portées par ces triangles ont aussi le même emplacement géométrique dans les deux images, ce qui augmente la pertinence du système d'identification.

3.6.2 Mesures de score

Pour obtenir le score de similarité en cas de verification et d'identification, nous calculons la probabilité **P** de matching à partir du nombre de triangles dans chaque étape de l'approche, équations (3.11), (4.10) et (3.13).

Les valeurs obtenues pour P_1 et P_2 comprises entre 0 et 1 sont considérées comme valeurs probabilistes, d'où le choix du produit des deux scores est plus convenable que leurs moyenne afin de réduire les scores à 0.

$$P_1 = \frac{|SDT|}{|DT|} \tag{3.11}$$

$$P_2 = \frac{|S\_bary|}{|DT\_bary|} \tag{3.12}$$

$$P = P_1 * P_2 \tag{3.13}$$

Nous notons :

|DT| : Cardinal de triangles obtenus dans la première étape par Delaunay triangulation.
|SDT| : Cardinal de triangles similaire dans la première comparaison.
|DT_bary| : Cardinal de triangles Delaunay générés à partir des points barycentres.
|S_bary| : Cardinal de triangles similaires dans la deuxième comparaison.

3.7 Expérimentations et résultats

Pour évaluer la performance de l'approche hiérarchique proposée, nous utilisons l'ensemble de données DB1_B de la base de données FVC2004 disponible sur Maio *et al.* (2004). FVC2004 DB1 et DB2 contiennent 880 empreintes digitales, de qualité variable, à partir de 110 doigts distincts (c'est-à-dire que chaque personne est représentée par 8 impressions). Trois scanners différents et un générateur synthétique SFinGE ont été utilisés pour collecter les empreintes digitales de cette base de données (voir Tableau 3.2).

Afin de clarifier les étapes de l'indexation par **HDT**, nous procédons par l'exemple de comparaison de deux empreintes digitales issues de la base de données DB1_1 de FVC2004. Les figures 3.9(a) et 3.9(b) représentent les descripteurs de l'image de l'empreinte, générés

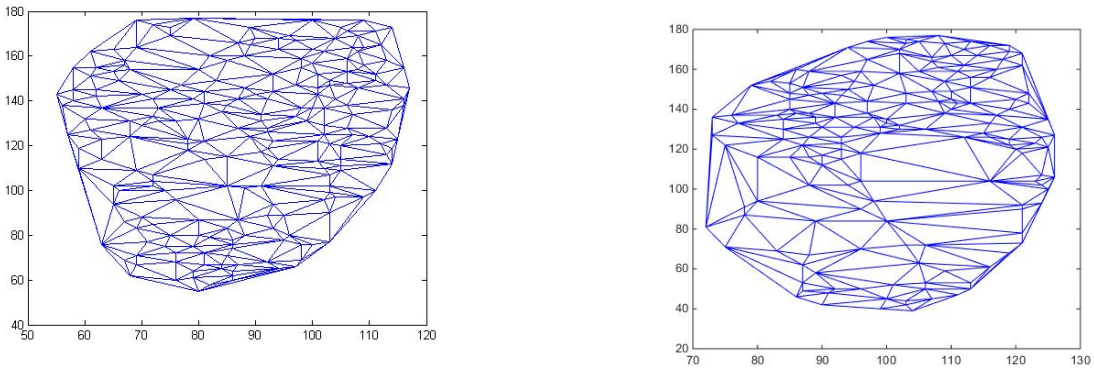
	Technologie	Image	Resolution
DB1	Optical Sensor (CrossMatch V300)	640 × 480	500 dpi
DB2	Optical Sensor (Digital Persona U.are.U 4000)	328×364	500 dpi
DB3	Thermal Sweeping Sensor (Atmel FingerChip)	300× 480	512 dpi
DB4	Synthetic Generator (SFinGe v3.0)	288×384	About 500 dpi

TABLE 3.2 – Base de données FVC2004

par la triangulation Delaunay des points minuties extraits pour une image utilisateur et image de test. La phase suivante décrite dans la Figure3.10 consiste à extraire les triangles similaires tout en se basant sur l'algorithme 3.2 présenté avant.

Nous éliminons par la suite tout triangle non similaire dans le but de garder l'information utile comme montré sur la Figure3.11.

Nous faisons suivre l'approche proposée par l'extraction du point barycentre dans la Figure 3.12, puis la deuxième phase de la hiérarchie par la triangulation des points barycentres dans la Figure3.13.

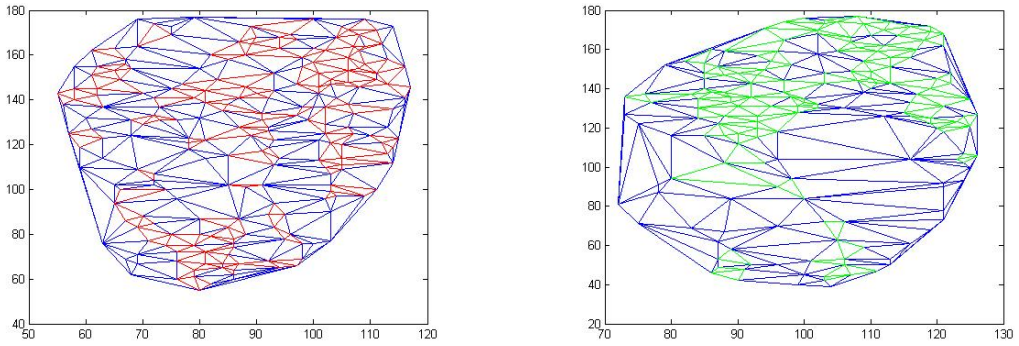


(a) (b)

FIGURE 3.9 – Application de la Delaunay triangulation sur l'ensemble des minuties extraites : (a) DT1 Empreinte utilisateur ; et , (b) DT2 Empreinte de test.

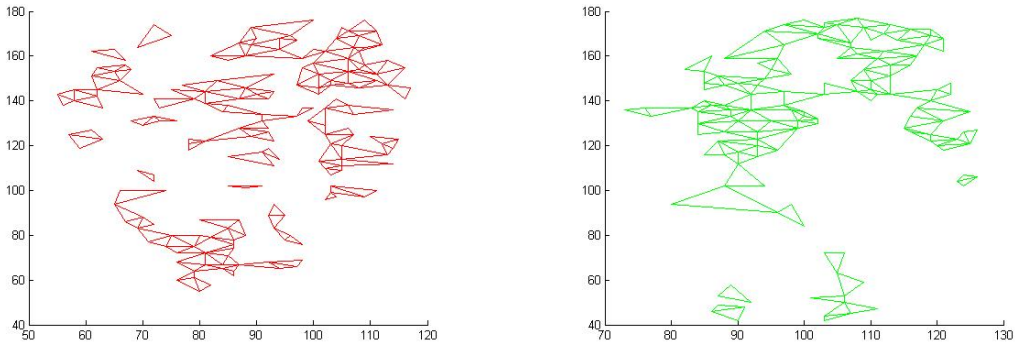
D'après le protocole d'expérimentation de FVC décrit par Bhatnagar et Kumar (2009), des expériences ont été menées pour évaluer la performance de notre approche prposée sur la base de données DB1_B. Nous avons adapté la mesure de la performance pour la vérification et l'identification en calculant le taux de fausse correspondance (**FAR**) et le taux de faux rejets **(FRR)**, pour un seuil t allant de 0 à 1.

Pour chaque empreinte digitale de la base de données, nous réalisons les étapes du prétraitement puis nous calculons, selon l'approche proposée, le score de similarité correspondant aux comparaisons avec les autres impressions du même doigt pour obtenir la variation intraclasse qui permettra de définir le taux **FRR**(équation 3.14). Dans ce cas chaque empreinte de test est considérée comme "propre".



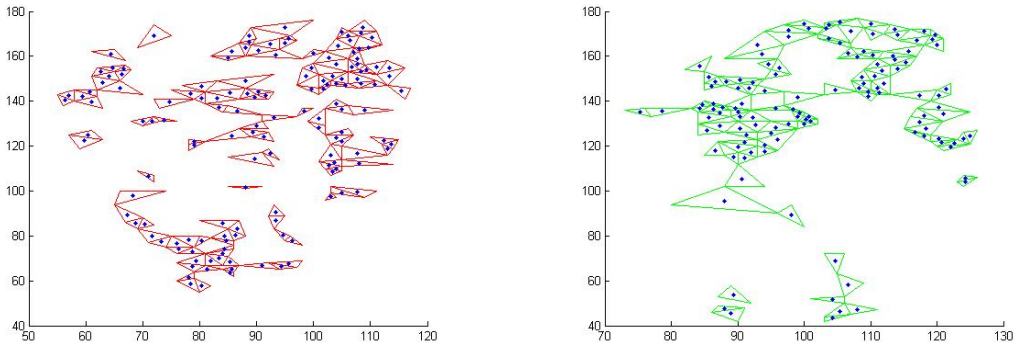
(a) (b)

FIGURE 3.10 – Calcul des triangles similaires : (a) Empreinte utilisateur ; et , (b) Empreinte de test.



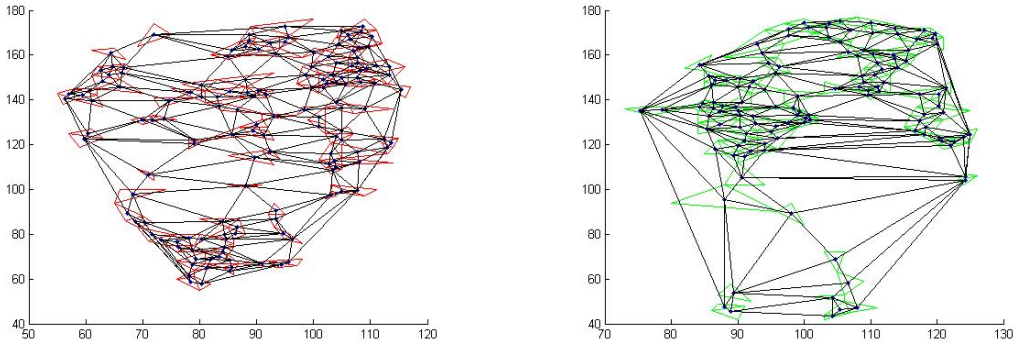
(a) (b)

FIGURE 3.11 – Extraction des triangles similaires : (a) S_DT1 ; et , (b) S_DT2.



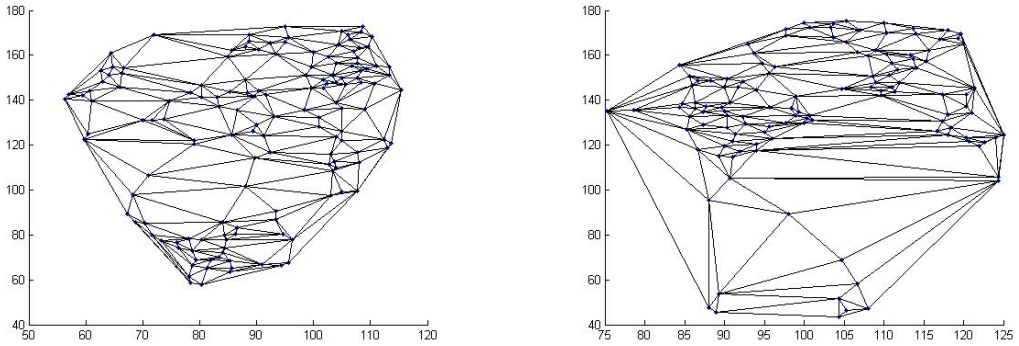
(a) (b)

FIGURE 3.12 – Calcul du barycentre des triangles trouvés similaires : (a) Empreinte utilisateur P_Bar(1) ; et , (b) Empreinte de test P_Bar(2).



(a) (b)

FIGURE 3.13 – Triangulation des barycentre : (a) DT_Bary(1) ; et , (b) DT_Bary(2).



(a) (b)

FIGURE 3.14 – Extraction des triangles similaires : (a) *S_bary* d'empreinte utilisateur ; et , (b) *S_bary* de l'empreinte test.

Une deuxième mesure est faite pour obtenir le score des faux acceptés **FAR** (équation 3.14), en comparant chaque empreinte digitale avec l'ensemble des autre images dans la base de données. Dans ce cas chaque empreinte de test est considérée comme "imposteur".

Nous résumons alors les performances en :

$$FRR = \frac{nombre\ des\ propres\ rejetes}{nombre\ total\ des\ propres} \tag{3.14}$$

$$FAR = \frac{nombre\ des\ imposteurs\ acceptes}{nombre\ total\ des\ imposteurs} \tag{3.15}$$

La cause essentielle de faux rejets dans la triangulation Delaunay revient généralement au bruit d'acquisition, aux transformations affines ou tout simplement à l'erreur de l'extraction des points minuties. Ces faux rejets peuvent être compensés lors de la phase d'acquisition par le grand nombre de triangles générés, permettant de consolider les points minuties manquantes dans une partie de l'image, par d'autres minuties d'une autre partie.

Puisque le nombre des faux acceptés se comporte différemment vis-à-vis de celui des faux rejetés, vu que notre méthode **HDT** élimine à chaque étape de la hiérarchie les candidats à faible score ou à score qui tend vers zéro, à la fin de l'expérimentation un nombre important des candidats rejetés.

Pour valider la performance de la méthode **HDT**, nous procédons à la visualisation et l'expérimentation de l'appariement en identification avec la triangulation Delaunay simple, dont les scores de comparaison ou d'identification sont basés seulement sur la comparaison des triangles obtenus dans la première triangulation.

La courbe **ROC** de la Figure3.15 *(Receiver Operating Characteristic)* représente les performances de la méthode proposée en comparaison avec la simple correspondance de Delaunay (**SDM**), en calculant les mesures FAR (False Acceptation Rate) et **FRR** (False Reject Rate). Les expériences sont effectuées sur DB1_1 à partir de FVC2004.

Nous observons que les performances obtenues en taux de faux acceptés vs les faux rejets sont effectivement assez faibles pour l'indexation par simple Delaunay triangulation (**SDM**). Donc nous pouvons déjà noter, à ce stade, que les meilleures performances sont obtenues avec l'indexation basée sur la triangulation hiérarchique **(HDT)**. Ce constat vérifie que la méthode de triangulation hiérarchique propose un taux de précision assez important tout en exploitant la totalité de l'information extraite de l'empreinte digitale, et renforce la pertinence des systèmes de comparaisons basés sur les triplets.

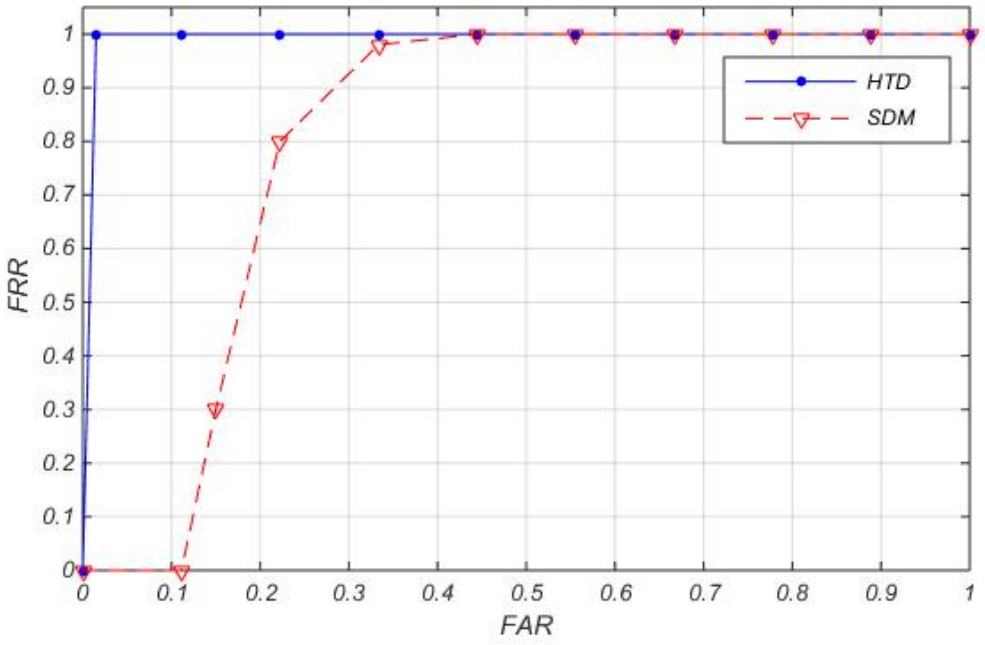


FIGURE 3.15 – La courbe **Roc**

La Figure3.16 et le tableau 3.3 montrent que notre approche est plus précise par rapport aux méthodes utilisant uniquement la triangulation de Delaunay. En effet, nous obtenons une similarité de 100% seulement pour l'image de la requête (I10) en utilisant notre méthode proposée et pour toutes les autres empreintes digitales non similaires nous obtenons 0% comme taux de similarité. Dans le cas contraire, lorsque l'appariement Delaunay est utilisé, de nombreux taux de détection erronées (taux non égaux à 0%) sont déterminés.

En outre, cette dernière approche donne deux images pertinentes avec des taux de similarité égaux à 100%, ce qui provoque des erreurs dans l'étape de vérification et d'identification.

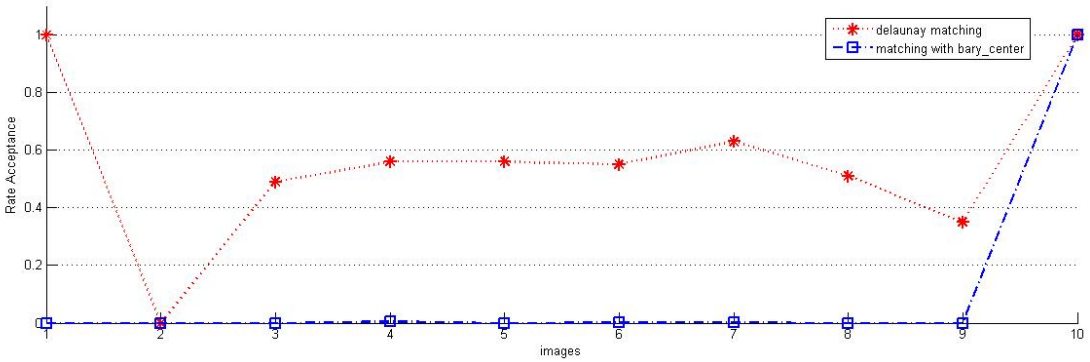


FIGURE 3.16 – Taux d'acceptation.

Image comparée	Méthode proposée	Simple Delaunay
I1	0%	100%
I2	0%	0%
I3	0%	49%
I4	0%	56%
I5	0%	56%
I6	0%	55%
I7	0%	63%
I8	0%	51%
I9	0%	35%
I10	100%	100%

TABLE 3.3 – Taux de similarité de l'image requête (I10) et quelques images de la base de données

3.8 Conclusion

A l'issue de ce chapitre, suite à une revue de l'état de l'art des principaux algorithmes de comparaison, d'identification et de récupération d'empreintes digitales nous avons procédé au développement d'une nouvelle méthode d'indexation d'empreintes digitales basée sur les minuties comme caractéristiques locales et leur triangulation. En particulier, nous avons proposé d'utiliser la triangulation de Delaunay d'une façon hiérarchique et une méthode d'indexation basée sur les triangulation de caractéristiques locales extraite de l'image.

Nous avons introduit la notion de barycentre afin d'assurer la localisation géométrique des triangles similaires respectivement des minuties similaires. Comme ces dernières peuvent être sensible à toute transformation homothétique qui ne garantit pas la position du triangle dans une empreinte digitale, nous introduisons le barycentre des triangles comme alternative afin de s'assurer qu'au moins trois triangles adjacents sont correctement situés dans l'empreinte considérée. Ainsi les résultats des expériences ont montré une amélioration significative.

L'utilisation des caractéristiques locales et leurs transformation se justifie par deux raisons majeures : D'abord, la robustesse aux requêtes de mauvaise qualité et au transformations affines, car la comparaison par triangulation nécessite un grand nombre d'appariement de triangles pour être fiables, donc de disposer d'une grande quantité d'information fiable en requête. Ensuite, les caractéristiques locales offrent la possibilité d'une indexation locale, c'est-à-dire sans avoir besoin d'indexer l'image totale de l'empreinte digitale.

Dans le chapitre suivant, nous allons étudier l'efficacité de combiner le principe de triangulation et la notion de barycentre. Nous avons utilisé d'autres caractéristiques géométriques de l'empreinte digitale d'une manière hiérarchique et en boucle jusqu'à l'obtention de triangles similaires inchangés dans le but de l'accélération de recherche et la minimisation du coût.

Chapitre

4 Indexation de l'empreinte digitale par combinaison du point singulier et transformation des minuties

Sommaire

Parmi les méthodes d'indexation et de comparaison d'empreintes digitales décrites jusque-là, les critères de choix prioritaires étaient la robustesse au bruit et aux transformations affines, ainsi que la pertinence des résultats de reconnaissance. Or que, dans ce chapitre, nous allons discuter la possibilité d'accélérer le processus d'indexation et de comparaison pour des fins utiles en temps de recherche et de coûts. En utilisant d'autres descripteurs de l'empreinte digitale, nous allons présenter une amélioration de la méthode d'indexation ***HDT*** *proposée afin de joindre le facteur de rapidité à sa pertinence.*

4.1 Introduction

Parmi les méthodes d'indexation et de comparaison d'empreintes digitales décrites jusque-là, les critères de choix prioritaires étaient la robustesse au bruit et aux transformations affines, mais aussi la possibilité d'accélérer le processus d'indexation et de comparaison pour des fins utiles en temps de recherche et de coûts.

L'indexation basée sur les minuties comme caractéristiques locaux et leur transformation par la Delaunay triangulation semble une bonne prestation pour une recherche pertinente, ainsi que l'utilisation de la méthode **HDT** mis en force l'efficacité du système

de recherche. Or que l'efficacité des systèmes biométriques est non proportionnelle à la complexité de l'algorithme de reconnaissance utilisé. Ce qui rend la méthode HDT complexe suite à l'utilisation hiérarchique et récursive des minuties et triangles générés par la Delaunay.

Dans ce chapitre, nous optons pour l'exploitation des avantages précisés dans les caractéristiques locaux et l'indexation par **HDT**. Par la combinaison de ces deux facteurs et les caractéristiques globaux d'une empreinte digitale, nous présentons une méthode de minimisation de la complexité tout en gardant l'efficacité et la pertinence de la méthode de recherche.

A l'issue de ce chapitre, nous présentons une nouvelle méthode basée sur l'extraction du point singulier, qui représente le point central de l'image, en utilisant l'orientation des points minuties pour les localiser, nous allons se focaliser sur un bloc de 100 × 100 pixels autour du point singulier extrait Elmouhtadi *et al.* (2018a). Le bloc sélectionné représente un intervalle contenant les minuties de haute qualité dont la probabilité de les perdre est faible pour tout type de transformation, car l'aquisition de l'image de l'empreinte digitale est généralement focalisée sur le centre du doigt, et la probabilité qu'un individu ne dépose pas le centre de son doigt dans le capteur est très peu probable, par rapport au manque des parties loin du centre.

Dans un deuxième lieu, nous appliquerons la triangulation de Delaunay hiérarchique **HDT** des points minuties comme méthode de comparaison des deux blocs d'images.

Les points forts de cette méthode sont résumés en :

- Se limiter à l'étude de la région du point singulier implique la réduction des minuties traitées lors de l'appariement, et par conséquent la réduction des triplets générés, ce qui implique une réduction du temps et de la complexité.

- La localisation du point singulier au centre de l'image le rend robuste à la perte de l'information utile en cas de contour manquant chose qui augmente les performances de reconnaissance.

- La robustesse au zoom vu l'utilisation de la transformation des caractéristiques locaux en triplets tout en ignorant la disposition de l'image intégrale.

- Le changement d'orientation de l'image requête n'affecte pas les résultats d'identification. Cela approuve la performance de l'utilisation de la triangulation.

- La considération du barycentre des triangles similaires dans la HDT, assure que les triangles pertinents trouvés sont situés aux mêmes endroits dans les deux impressions comparées.

- ✾ La considération d'un petit bloc de l'image accélère d'avantage la méthode d'indexation par rapport à l'utilisation de l'image totale.

4.2 Extraction du point singulier

Les points singuliers, le Core et le delta ; sont les caractéristiques globales les plus importantes d'une empreinte digitale, elles déterminent également la structure topologique. La zone ponctuelle singulière définie comme une région où la courbure de la crête est supérieure à la normale et où la direction de la crête change rapidement. Un point singulier Core est défini comme le point central d'une région ogive, et un point delta est le centre de régions triangulaires où trois directions différentes se rencontrent.

Dans la littérature, plusieurs approches ont été basées sur l'extraction du point singulier comme caractéristique globale de l'empreinte digitale Bazen et Gerez (2002) et Zhou *et al.* (2009). Le point singulier, core ou delta, est considéré comme un descripteur global qui pourra être utile pour :(i) déterminer la classification de l'image selon le classement d'Henry Hong et Jain (1999), (ii) estimer l'orientation globale de l'empreinte digitale, et (iii) servir comme indexe pour la vérification et l'identification.

Dans la plupart des méthodes existantes, l'extraction du point singulier est généralement basée sur l'estimation de la directivité *(orientation field)* des crêtes papillaires pour obtenir la représentation de l'images à champ directionnel à noter Liu *et al.* (2007a) et Ratha *et al.* (1996).

4.2.1 Méthode du Poincaré

L'index de Poincaré est l'un des plus pratiques et simples algorithmes utilisés dans la détection des caractéristiques globales d'une empreinte digitale en se basant sur l'orientation. Comme démontré par Wang *et al.* (2002), Liu (2010) et Awad et Baba (2012), le Poincaré est considéré comme une méthode très sensible au bruit et aux variations du niveau de gris de l'image requête. Il consiste à détecter les cores et les deltas présents dans l'empreinte, en divisant une image en plusieurs blocs et en calculant l'orientation de chaque strie. Ensuite, les blocs qui contiennent les points singuliers seront détectés. Ces points permettent la classification des empreintes en catégorie selon leur motif général. La Figure4.1 montre le calcul de l'index de Poincaré avec un voisinage de $N = 8$ pixels autour du pixel [i,j] appartenant respectivement (de gauche à droite) à une zone singulière en core, et delta.

Le core est défini comme un point où l'orientation dans un voisinage local autour d'un point représente une tendance semi-circulaire. Le delta est défini comme un point dans le champ d'orientation où le voisinage local autour d'un point forme trois secteurs et l'orientation dans chaque secteur représente une tendance hyperbolique. L'index de

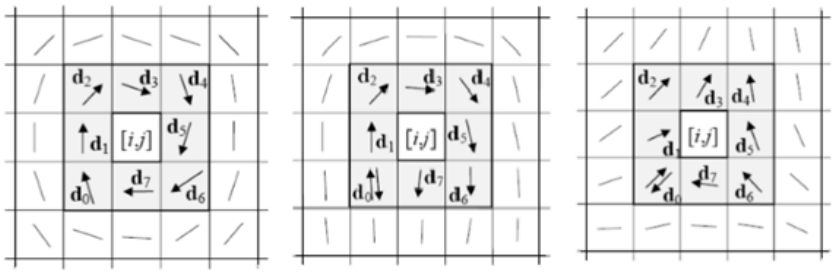


FIGURE 4.1 – L'index de Poincaré calculé avec un voisinage de N= 8 pixels autour du point [i,j].

Poincaré est alors calculé par les équations (4.1), (4.2) et (4.3), en passant par les pixels du bloc de 0 à N-1 dans le sens inverse des aiguilles d'une montre.

$$poincare(x,y) = \frac{1}{2\pi}\sum_{k=0}^{N-1}\nabla(k) \tag{4.1}$$

Où :

$$\nabla(k) = \begin{cases} \delta k & |\delta k| < \frac{\pi}{2} \\ \delta k + \pi & \delta k < -\frac{\pi}{2} \\ \pi - \delta k & \delta k > \frac{\pi}{2} \end{cases} \tag{4.2}$$

$$\delta(k) = \theta(x_{(k+1)modN}, y_{(k+1)modN}) - \theta(x_k, y_k) \tag{4.3}$$

Cependant, dans notre approche nous nous intéressons seulement au point singulier de type Core dans le but de détecter le centre d'une empreinte digitale en tant que région importante, en fait, quelle que soit la position du doigt sur le capteur, nous obtiendrons le centre de l'empreinte dans l'image requise, contrairement au delta qui peut être manqué dans une mauvaise position lors de l'impression ou dans le cas d'une image reconstituée.

4.2.2 Méthode du Gradient

La méthode basée sur le gradient pour la detection du point Core a été adoptée par de nombreuses approches comme Zhou *et al.* (2009). Le gradient a montré de très importants résultats pour la detection du point singulier, tout en gardant la robustesse face à la qualité d'image faible et aux bruyantes impressions des empreintes digitales. Il s'appuie sur l'estimation de l'orientation de l'image par la dérivée de chaque pixel dans les directions x et y pour obtenir le vecteur gradient (4.4).

$$GI(x,y) = \begin{bmatrix} G_x I(x,y) \\ G_y I(x,y) \end{bmatrix} = \begin{bmatrix} \frac{\partial_I(x,y)}{\partial_x} \\ \frac{\partial_I(x,y)}{\partial_y} \end{bmatrix} \tag{4.4}$$

Du fait que les points singuliers sont les points où le champ d'orientation est discontinu, l'orientation joue un rôle essentiel dans l'estimation du point Core sur une image d'empreinte digitale.

Nous calculons l'estimation de l'orientation en se basant sur le calcul du gradient des composantes $G_xI(x,y)$ et $G_yI(x,y)$ pour une fenêtre de $W(3,3)$ autour du pixel (x,y) (4.4). Le calcul du gradient au niveau de chaque pixel, permet de définir l'angle moyenne orthogonale à l'orientation de la crête pour chaque changement d'intensité de pixel.

Désormais, nous avons besoin d'un autre mécanisme pour affiner le champ d'orientation afin d'éliminer l'ambiguïté d'orientation et d'éviter les irrégularités dues au bruit. Nous adoptons alors l'approche du gradient carré comme montré par l'équation (**??**), qui consiste à doubler l'angle des gradients et mettre la longueur des vecteurs gradient au carré. Ceci a pour effet que les orientations de fortes intensités auront une moyenne plus élevée par rapports à celle de faibles intensités.

$$\begin{pmatrix} G_{s,x}I(x,y) \\ G_{s,y}I(x,y) \end{pmatrix} = \begin{bmatrix} \sum wG_x{}^2 - \sum wG_y{}^2) \\ 2\sum wG_xG_y \end{bmatrix} = \begin{bmatrix} G_{xx} - G_{yy} \\ 2G_{xy} \end{bmatrix} \tag{4.5}$$

Nous calculons donc la valeur θ comme montré dans les équations (4.6) et (4.7), qui est la valeur d'orientation de l'image. Les blocs avec des valeurs de pente allant de 0 à 90° sont marqués. Ensuite, un chemin est tracé jusqu'à ce que nous rencontrions une pente qui n'est pas entre 0 et 90° et que ce bloc est marqué. Le bloc qui a le plus grand nombre de marques calculera la pente dans la direction de Y négative et sortira sur la position X et Y qui fera l'objet du point Core ayant pour coordonnées (x_center, y_center). La Figure4.2 présente un aperçu sur les étapes d'extraction du point singulier.

$$\theta = \frac{1}{2}\nabla(G_{xx} - G_{yy}, 2G_{xy}) \tag{4.6}$$

Avec $\nabla(x,y)$ est définie par (4.7) :

$$\nabla(x,y) = \begin{cases} \tan^{-1}(\frac{x}{y}) & x > 0 \\ \tan^{-1}(\frac{x}{y}) + \pi & x < 0 \quad y \geq 0 \\ \tan^{-1}(\frac{x}{y}) - \pi & x < 0 \quad y \geq 0 \end{cases} \tag{4.7}$$

4.2.3 Région du point singulier

En tant que région importante, les pixels autour du point singulier présentent des points de haut niveau sur une empreinte digitale, ainsi nous allons nous focaliser sur

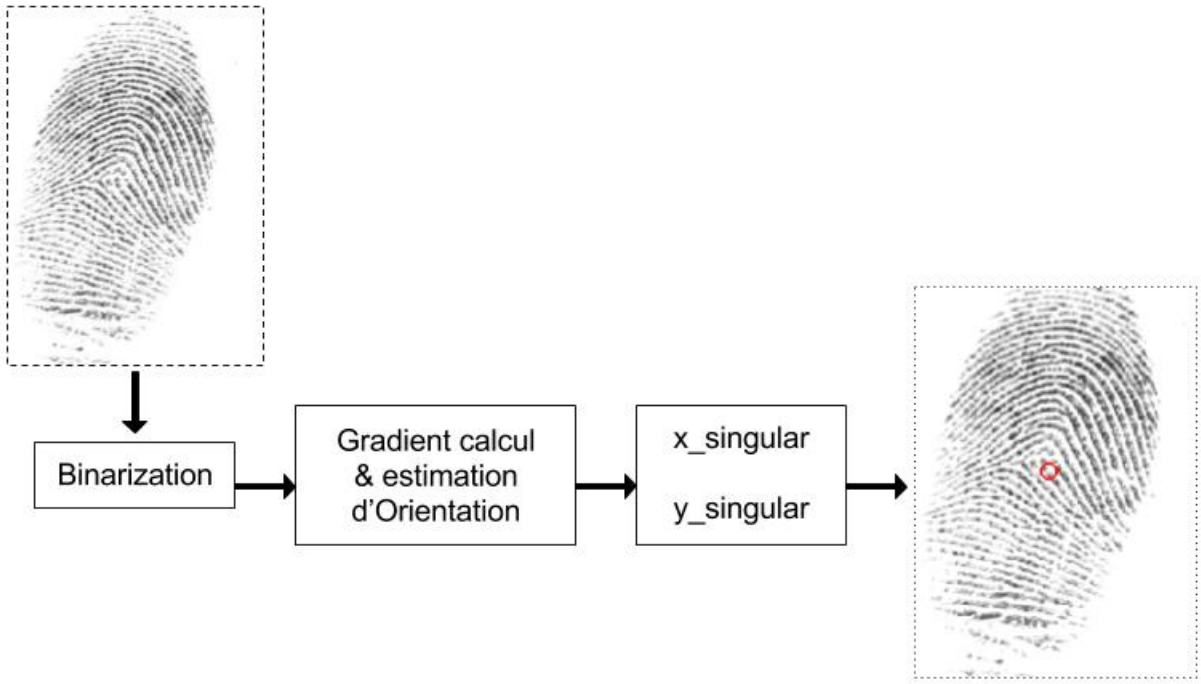


FIGURE 4.2 – Processus d'extraction du point singulier.

l'extraction des minuties autour du point singulier extrait. Beaucoup d'approches ont approuvé que le nombre élevé de minuties extraites peut diminuer le résultat correspondant ; en particulier lorsque l'on utilise en indexation par caractéristiques de minuties.

Le nombre de caractéristiques utilisés, multiplié par le nombre des minuties extraites aboutit à un grand nombre de données à considérer pour l'indexation. Le seul inconvénient ici est qu'un mauvais point extrait engendre une fausse fonctionnalité du système.
Nous proposons dans notre approche de considérer un bloc de (100×100) pixels autour du point singulier extrait comme montre la Figure 4.3, ceci réduit le nombre de minuties extraites et aide à minimiser le temps, l'erreur, et la complexité de l'appariement.

4.3 L'indexation par HDT

Nous définissons la comparaison de deux blocs d'empreintes digitales par la comparaison basée sur les triplets de Delaunay. Nous allons adopter la méthode **HDT** comme méthode.

Après avoir extrait le point singulier par le gradient comme déjà mentionné, nous redimentionnons l'image vers un bloc de 100×100 pixels, ce qui fera une nouvelle présentation de l'empreinte digitale de base. On applique par la suite les étapes du prétraitement à chaque bloc d'empreinte afin d'extraire des minuties qui seront classées dans un vecteur de terminaisons et de bifurcations.

La binarization par Otsu est appliquée pour obtenir l'image binaire. L'approche de skeletisation de Zhang a été utilisée pour résumer l'empreinte binaire en squelette. En-

FIGURE 4.3 – Limiter l'image à un bloc de 100*100 autour du pint singulier.

suite, nous appliquons le processus d'extraction de minuties composé par bifurcation et terminaisons. La méthode basée sur le cross number a été appliquée sur un voisinage de 8 pixels, comme mentionné précédemment au chapitre 1.

La Figure4.4 montre les différentes étapes appliquées sur le bloc du point singulier extrait. Ensuite, sur la base du vecteur minuties obtenu (terminaisons et bifurcation), les différents triangles possibles seront formés en appliquant une triangulation Delaunay ***(DT)*** en vue d'obtenir tous les triplets possibles des points extraits (voir Figure4.5).

Considérons deux blocs d'empreintes à comparer (**DT** Pour une image d'entrée au système, et **DT2** pour l'image enrôlée dans la base de données). Par application du théorème l'Akashi nous calculons les trois angles α, β et γ de chaque triangle **ABC** dans la triangulation de Delaunay obtenue dans **DT**.

La comparaison des deux blocs est alors basée sur la comparaison $N : N$ des deux ensembles d'angles de triangles Delaunay obtenus dans chaque blocs. L'équations (3.11) utilisées dans le chapitre précédent, fera l'objet du score de similarité dans cette étape, à côté du *Similar_DT*, et l'ensemble des triangles trouvés similaires.

En exploitant les avantages de l'indexation par la méthode **HDT** ; nous appliquons la hiérarchie de la Delaunay triangulation sur le bloc de point singulier afin de générer le modèle d'index. Ceci dit que nous calculons les points barycentre sur chaque triangle similaire obtenu dans la première comparaison des deux blocs, sous *Similar_DT*. Une deuxième triangulation Delaunay est appliquée sur les points barycentres suivie d'une comparaison de triangles obtenus et nous conservons les résultats de triangles similaires obtenus sur **DT_Similar_DT**.

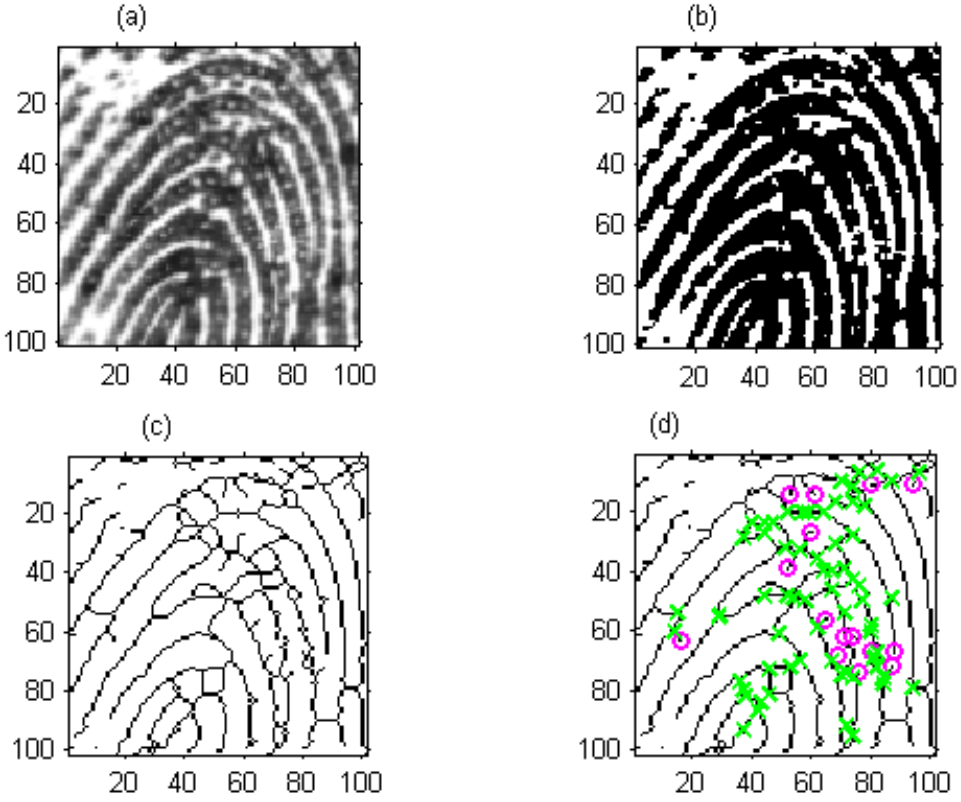


FIGURE 4.4 – Application du prétraitement autour du point singulier : (a) Bloc original, (b) Binarization du bloc, (c) Squelettisation, (d) Extraction des points minuties.

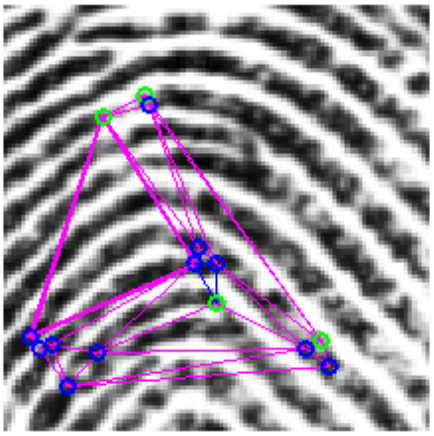


FIGURE 4.5 – Triangulation Delaunay du bloc point singulier.

Cette deuxième comparaison permet de s'assurer que les premiers triangles similaires, qui correspondent aux points minuties similaires ; sont également de vrai similaires, sinon ils seront éliminés dans la deuxième comparaison. Ceci revient au fait que trois points minuties peuvent former le même triangles que trois autres totalement différents. Or le chemin que lie 3 groupes de 3 minuties, ne peut se répéter que si et seulement s'il s'agit de la vrai similarité.

Enfin, le taux de la similarité final est basé sur les probabilités déjà définies précédemment (équations (3.11), (4.10) et (3.13)).

4.4 Résultats et discussion

Pour évaluer la performance de la méthode proposée, nous utilisons les empreintes digitales dans DB1_a de la base de données FVC2002 disponible sur **?**. DB1 et DB2 de FVC2002 contiennent 880 empreintes digitales, de qualité variable, à partir de 110 doigts distincts (c'est-à-dire que chaque personne est représentée par 8 impressions). Trois scanners différents et le générateur synthétique SFinGE ont été utilisés pour collecter les empreintes digitales.

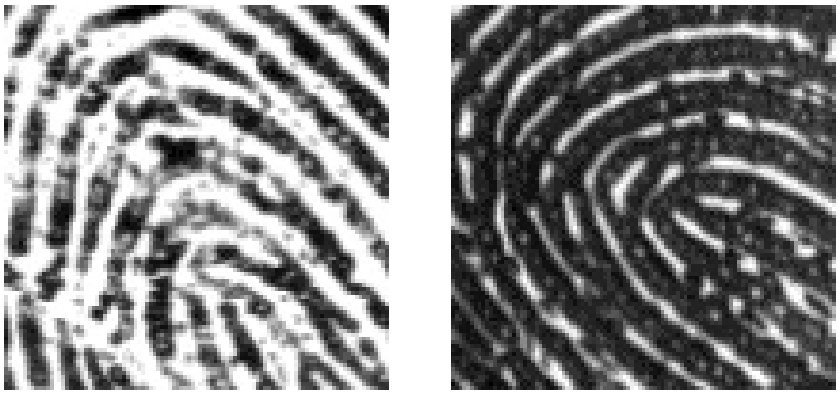
la Figure4.7 illustre un exemple de bloc autour du point singulier après son extraction dans la Figure4.6.

Étant donné deux empreintes digitales I1 et I2 différentes, la Figure4.8 présente les triangles de Delaunay (c'est-à-dire DT et DT2) extraits dans les deux blocs d'images. La Figure 4.9 illustre à son tour l'extraction des triangles Delaunay similaires dans la première comparaison(c'est-à-dire similar_DT). Sur la Figure4.10, nous présentons le barycentre généré (DT_similaire_DT pour image d'utilisateur et DT2_similaire_DT2 pour l'image de test), puis les triangles similaires extraits à cette étape (bary_similar), comme indiqué sur la Figure4.11.

(a)

(b)

FIGURE 4.6 – Extraction du point singulier : (a) Empreinte utilisateur ; et , (b) Empreinte test.



(a) (b)

FIGURE 4.7 – Bloc au voisinage du point extrait : (a) Empreinte utilisateur ; et , (b) Empreinte test.

Enfin, nous calculons la probabilité **P** calculée par les équations (4.8),(4.9) et (4.10). Le score de similarité pour le bloc d'image d'utilisateur et le bloc d'image enrôlé. Les valeurs obtenues pour P_1 et P_2 comprises entre 0 et 1 sont considérés comme valeurs probabilistes, d'où le choix du produit des deux scores est plus convenable que leurs moyenne afin de

réduire les scores presque nulles à 0.

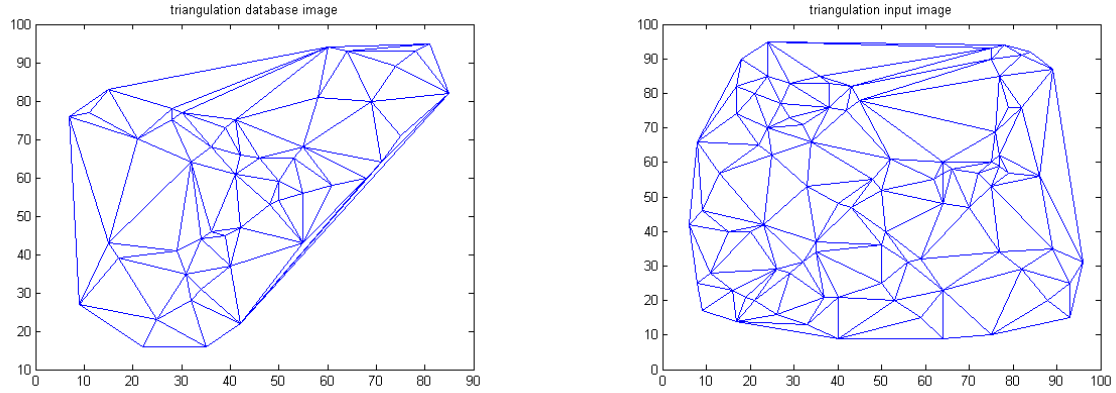
$$P_1 = \frac{|Similar\_DT|}{|DT|} \tag{4.8}$$

$$P_2 = \frac{|bary\_similar|}{|DT_Ssimilar\_DT|} \tag{4.9}$$

$$P = P_1 * P_2 \tag{4.10}$$

Nous notons que :

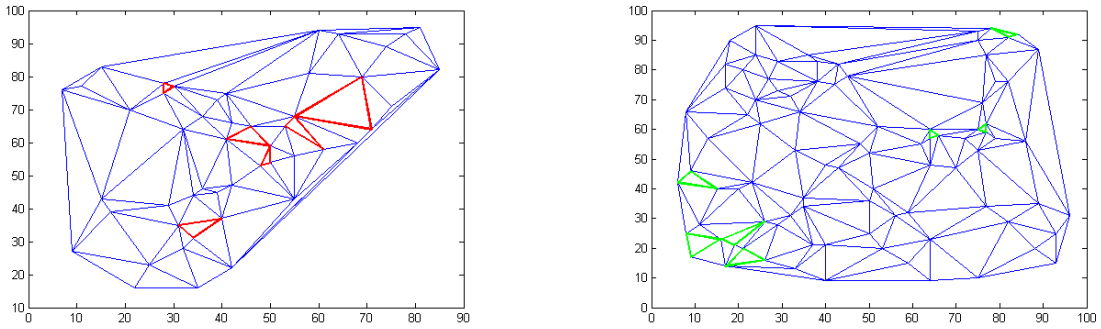
|DT| : Cardinal de triangles obtenus dans la première étape par Delaunay triangulation.
|Similar_DT| : Cardinal de triangles similaires dans la première comparaison.
|DT_Similar_DT| : Cardinal de triangles Delaunay générés à partir des points barycentres.
|bary_similar| : Cardinal de triangles similaires dans la deuxième comparaison.



(a) (b)

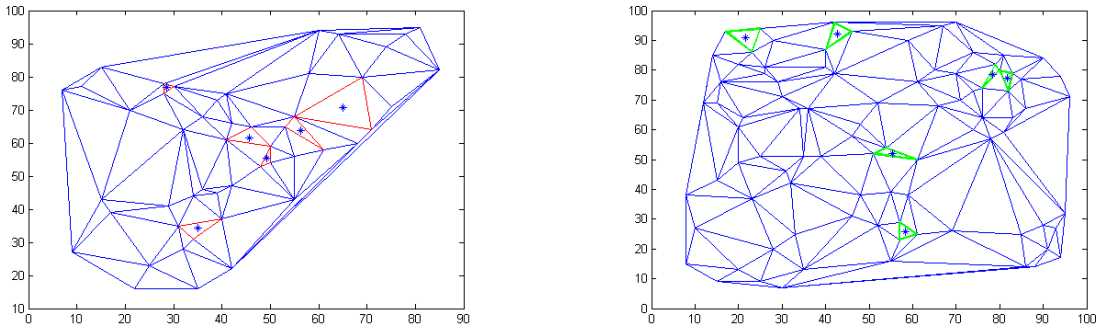
FIGURE 4.8 – Triangulation des deux blocs comparés : (a) DT d'empreinte utilisateur ; et, (b)DT2 de l'empreinte test.

En comparant une image de requête (I10) et d'autres empreintes digitales sélectionnées de la base de données, les résultats dans le tableau 4.4 prouvent que la nouvelle approche est plus précise en comparaison avec les autres méthodes : (i) appariement par simple Delaunay triangulation appliquée sur les minuties d'entrée **(SDT)**,(ii) appariement basé sur l'indexation par simple Delaunay triangulation autour du point singulier extrait **(SPSDT)** et l'approche proposée (iii) appariement basé sur l'indexation par Delanay triangulation hiérarchique autour du point singulier **(SPHTD)**.



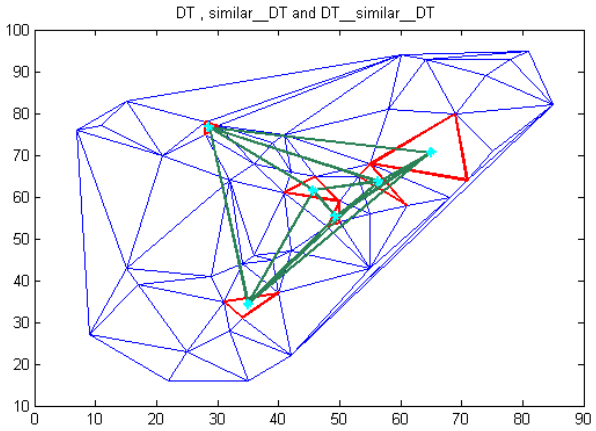
(a) (b)

FIGURE 4.9 – Extraction des triangles similaires : (a) DT d'empreinte utilisateur ; et , (b) DT2 de l'empreinte test.

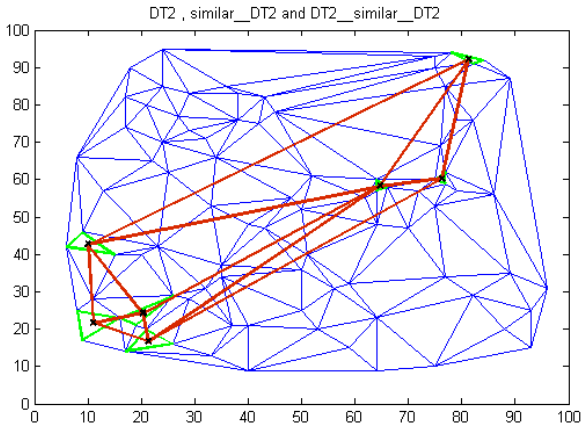


(a) (b)

FIGURE 4.10 – Définition du barycentre pour les triangles similaires : (a) L'empreinte utilisateur ; et , (b) L'empreinte test.



(a)



(b)

FIGURE 4.11 – Application de HDT pour les triangles similaires : (a) L'empreinte utilisateur ; et, (b) L'empreinte test.

Nous obtenons une similarité de 100% seulement pour l'image de la requête (I10) en utilisant notre approche proposée, et pour toutes les autres empreintes digitales non similaires nous avons 0% ou des valeurs faible de 5%, 12% et 14% comme taux de similarité. Contrairement aux autres méthodes, il existe de nombreuses fausses détections (taux différent de 0%), ainsi qu'il détecte une forte similarité de 100% pour des images quasiment différentes, ce qui diminue largement l'efficacité du système.
On note le temps de traitement moyen dans notre méthode **SPHTD** pour chaque empreinte d'environ 0,098 s.

Images comparés	SPHTD	SDT	SPSDT
I1	14%	100%	30%
I2	0%	15%	0%
I3	5%	36%	9%
I4	0%	56%	0%
I5	0%	42%	3%
I6	12%	62%	0%
I7	0%	54%	12%
I8	0%	27%	0%
I9	0%	35%	0%
I10	100%	100%	100%

TABLE 4.1 – Résultats de matching

4.5 Conclusion

Nous avons présenté dans ce chapitre, une nouvelle approche d'appariement d'empreintes digitales basée sur l'extraction du point singulier comme clé primaire de la méthode d'indexation basée sur la triangulation Delaunay hiérarchique. En tant que point important, un point singulier est considéré comme un motif d'empreinte digitale de haute qualité avec une faible probabilité de perte dans le cas de parties manquantes sur une impression d'empreinte digitale. Ceci renforce davantage la méthode d'indexation **HDT** proposée dans le chapitre précédent. L'extraction de points singuliers a approuvé une performance d'appariement élevée en considérant les minuties sur son voisin.

Tout en gardant son point fort de pertinence en garantissant la distribution topologique des minuties alignées, la **HDT** appliquée dans un bloc autour du point singulier permet de gagner de plus le défit de la contrainte du temps, vu que nous traitons une petite partie de l'empreinte digitale ce qui diminue le temps d'indexation, d'enrôlement et de comparaison.

Après avoir étudier l'importance de la pertinence du système de reconnaissance d'empreinte digitale par la méthode **HDT** d'indexation proposée, ainsi que la rapidité, nous

arrivons dans un prochain chapitre à l'étude de la sécurité du système de reconnaissance et l'impact de la méthode d'indexation sur la sécurité du système biométrique.

Chapitre

5 Evaluation de la méthode d'indexation HDT par un système d'attaque biométrique

Sommaire

L'augmentation exponentielle de l'utilisation de l'information biométrique dans la vie quotidienne donne naissance à une préoccupation croissante liée aux problèmes de confidentialité et de sécurité ; par conséquent, les menaces qui ont trait à la sécurité des systèmes biométriques ont besoin d'être soigneusement analysées. Les différents systèmes de reconnaissance d'empreintes digitales stockent les informations personnelles des individus sans aucune mesure préalable de sécurité. Ainsi, un attaquant peut facilement avoir accès à l'identité de l'utilisateur légitime. Alors le grand défi est non seulement la réalisation d'un système de reconnaissance d'empreinte digitale performant, mais aussi éligible face à tout type d'attaques. Alors, à quel point l'enjeu sécuritaire peut influencer sur la performance d'un système de reconnaissance d'empreintes digitales ?

5.1 Introduction

La reconnaissance d'empreinte digitales est l'un des systèmes biométriques les plus répondu, il se réfère à la méthode automatisée d'identification ou de vérification de l'identité individuelle basée sur la comparaison de deux empreintes digitales. C'est l'un des systèmes

de biométrie les plus utilisés, et de loin la solution la plus utilisée pour l'authentification sur les systèmes informatisés qui prennent la préoccupation majeur des chercheurs comme noté dans le livre de Maltoni *et al.* (2009).

La comparaison d'empreintes digitales et la mise en correspondance implique l'utilisation des méthodes d'indexation pour extraire les caractéristiques importantes. La performance et la sécurité des systèmes biométriques dépendent de plusieurs facteurs dont les plus importants sont les méthodes d'indexation et la robustesse face aux différentes attaques.

Quant aux méthodes d'indexation utilisées dans les systèmes biométriques, elles ont un impact très important sur la performance du système biométrique ce qui crée une forte dépendance entre la pertinence du système et les caractéristiques utilisées comme index. C'est donc le but majeurs de plusieurs approches d'indexation comme explicité dans Maltoni *et al.* (2009), Cappelli *et al.* (2006) et Feng et Zhou (2011). Nous avons montré dans le premier chapitre que les meilleurs systèmes d'indexation ont prouvé que les approches basées sur les minuties donnent de bons résultats par rapport aux autres techniques.

Malgré leur pertinence, les technologies basées sur la biométrie sont considérées comme une des composantes d'un système d'identification, où il faut souvent utiliser des systèmes complémentaires afin de créer des systèmes de secours appropriés. Cela permet de limiter la dépendance totale à la biométrie et par suite faire face aux menaces du système. D'autre part, les échantillons biométriques enregistrés dans la base de données comme modèles peuvent être utilisés afin d'usurper l'identité et la vie privé de l'utilisateur. L'attaquant s'authentifie de la même façon qu'un utilisateur requête, il suffit d'avoir une copie de l'image d'un vrai utilisateur pour qu'il puisse avoir l'acceptation, voir Figure5.1.

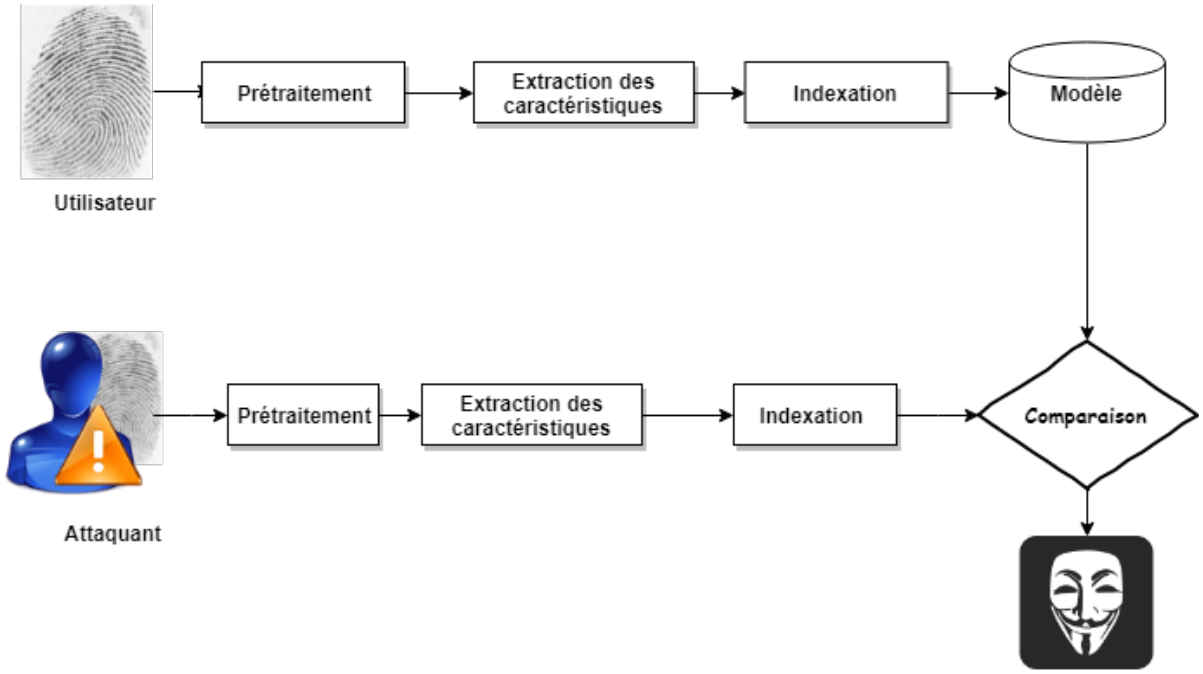


FIGURE 5.1 – Scénario de l'attaque par imitation d'empreinte digitale

Un attaquant peut exploiter plusieurs menaces et attaques. Selon la littérature il existe plusieurs types d'attaques biométrique afin d'obtenir un accès illégitime au système biométrique :

- **Attaque par imitation :** Dans ce cas l'attaquant imite le modèle de la donnée biométrique déjà enrôlée dans la base de donnée.

- **Attaque par falsification :** L'attaquant ici reproduit l'image de la donnée biométrique ; dans le cas des empreintes digitales par exemple, l'attaquant peut recopier l'image de l'empreinte à partir d'une trace laissée sur une surface ou un objet touché par l'utilisateur. Généralement, c'est la méthode utilisé par la police criminelle pour extraire l'empreinte d'un délinquant. La falsification génère une image à qualité médiocre, or que les systèmes de reconnaissance les plus pertinents n'y prennent pas en considération.

- **Attaque par répudiation :** Dans le cas où l'attaquant est un vrai utilisateur du système ; qui a pu modifier les informations secrètes et affirme qu'une autre personne a pu accéder au système.

- **Attaque par contamination :** L'attaquant peut obtenir les informations biométriques (i.e. empreinte digitale) des vrais utilisateurs afin d'avoir accès au système.

- **Attaque par collision :** Où un utilisateur légitime avec de hauts privilèges (ex.administrateur) peut modifier le système.

D'autres attaques comme l'oblitération, la distorsion et l'imitation [Yoon *et al.* (2012)], Van der

Putte et Keuning (2000)] pour contourner le système biométrique.

En outre, les données ne sont pas toujours secrètes, ce qui augmente la vulnérabilité des modèles biométriques. Par exemple, dans le cas de caractéristiques d'empreintes digitales, un attaquant utilisant un objet touché peut reproduire les données biométriques. Ce type d'altération a une relation directe avec les méthodes d'indexation utilisées, où un attaquant peut facilement accéder au système s'il utilise une méthode d'indexation à faible performance Galbally *et al.* (2011). Pour résoudre ces problèmes, des techniques de protection de modèles biométriques sont développées dans la littérature.

Malgré la recherche active menée ces dernières années pour protéger le modèle biométrique, la relation entre la méthode d'indexation et la sécurité des systèmes biométriques d'empreintes digitales n'a pas encore été étudiée. Par conséquent, le procédé de l'approche d'indexation par **HDT** que nous avons proposé dans cette thèse, offre la performance du système biométrique des empreintes digitales et une garantie de sécurité contre les attaques par modification, où l'on pourra utiliser comme méthode de protection de reconnaissance par empreinte digitale.

5.2 Transformation de caractéristiques

Les modèles biométriques sont vulnérables à plusieurs types d'attaques que nous avons citées, où un attaquant peut récupérer l'image originale de l'utilisateur par falsification ou en utilisant le modèle stocké dans la base de données. D'autre part, l'accès au modèle est considéré comme l'une des menaces importantes en terme de sécurité et de la vie privée de l'utilisateur. Pour ces raisons, il est nécessaire de développer des mécanismes robustes pour la protection des modèles biométriques. C'est dans ce besoin que les chercheurs ont pensé à développer des techniques de protection des modèles biométriques. Deux grandes catégories de solutions sont proposées dans la littérature pour protéger les modèles biométriques :(i) la transformation des caractéristiques biométriques, et (ii) les crypto-systèmes biométriques (Figure 5.2). Dans notre cas nous allons nous intéresser aux méthodes de transformation de caractéristiques de l'empreinte digitale.

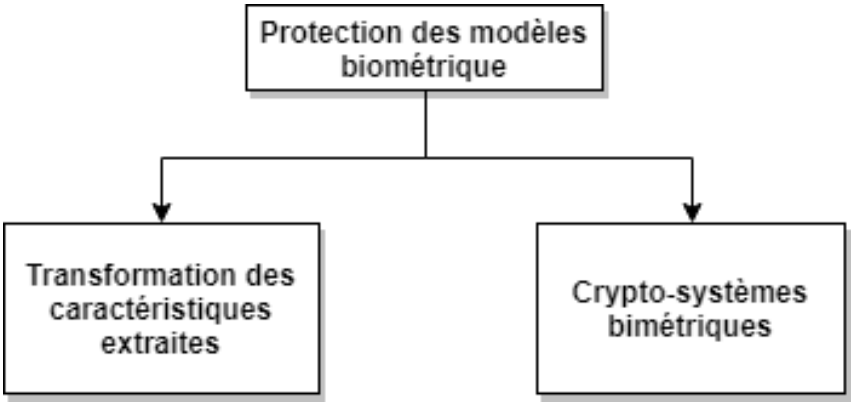


FIGURE 5.2 – Techniques de protection des modèles biométriques

Comme nous l'avons mentionné, la sécurité est devenue de plus en plus une préoccupation dans les systèmes biométriques ; elle assure la confidentialité en fournissant un processus d'authentification robuste contre tout type de tromperie et aussi contre la possibilité d'augmenter les caractéristiques biométriques originales ;Jain *et al.* (2008). Pour ce faire, des transformations de caractéristiques sont proposées comme technique de protection de gabarit biométrique. Ces méthodes sont basées sur l'application d'une fonction de transformation sur les caractéristiques biométriques.

Plus précisément, pour la reconnaissance de l'empreinte digitale, les caractéristiques transformées sont stockées dans la base de données en tant que modèle de référence. La même transformation est appliquée à la requête lors de l'authentification, puis mise en correspondance avec le modèle stocké Bringer et Chabanne (2008).

5.2.1 Méthodes de transformation de caractéristiques

Plusieurs méthodes de transformation de modèles ont été proposées et classées en deux catégories : (i) Transformation basée sur le vecteur et (ii) Transformation basée sur le point d'intérêt Teoh *et al.* (2006). Dans les premières méthodes, le modèle biométrique est représenté comme un vecteur, pour calculer la dissimilitude, on fait recours à la distance euclidienne. Le Biohashing (Jin *et al.* (2004))est un exemple de cette classe ; en l'appliquant à la méthode **HDT**, le vecteur de caractéristiques extrait est alors multiplié par une matrice de transformation orthogonale. Cependant, le Biohashing est facile à inverser lorsque la clé est connue de l'attaquant, ce qui dégrade les performances de cette méthode.

La BioPhasor est considérée comme une amélioration du biohashing, dans cette méthode un ensemble de vecteurs complexes est obtenu en utilisant le vecteur biométrique et la transformation orthogonale (utilisée comme partie imaginaire). Bien que, ce schéma est considéré comme plus fiable que le Biohashing , la complexité d'inverser cette transformation reste inconnue.

De nombreuses fonctionnalités d'empreintes digitales sont représentées par un ensemble de points minuties transformées selon un modèle quelconque. Ratha *et al.* (2001)

ont utilisé la transformation cartésienne, polaire et fonctionnelle. Dans le cas cartésien, l'empreinte est transformée en un ensemble de rectangles placés en suivant la clé associée. Dans la transformation polaire, les empreintes digitales sont divisées en coquilles et chacune d'entres elles est divisée en secteurs. Dans le cas de la transformation fonctionnelle, des gaussiennes 2D et un champ de potentiel électrique en distribution de charge 2D sont appliqués pour obtenir la minutie correspondante. Cependant, les performances sont réduites en raison d'une augmentation des variations intra-classes des utilisateurs. En outre, ces transformations nécessitent l'alignement des empreintes digitales avant la transformation.

5.2.2 Méthodes de transformation de caractéristiques par HDT

Afin d'éviter les faiblesses des méthodes de transformation existantes, nous avons proposé dans Elmouhtadi et Lafkih (2017), l'evaluation de la méthode **HDT** basée sur la transformation triangulaire des minuties extraites. Au lieu d'utiliser une clé secrète externe, notre approche est basée sur l'extraction de la clé secrète à partir des caractéristiques biométriques afin d'augmenter la sécurité du système proposé.

Nous utilisons les angles des triangles **DT**, générés dans la première phase de l'approche, comme une clé secrète pour effectuer la deuxième transformation. Ainsi le système se compose de deux transformations successives, la première représente la clé principale qui génère les caractéristiques, et la deuxième fera l'objet de la méthode de transformation de caractéristiques extraites.

5.2.3 Processus d'indexation

Dans le cas d'une empreinte digitale pivotée, le calcul de la corrélation croisée pour différents angles est inefficace sur le plan informatique Maltoni *et al.* (2009)et Nandakumar et Jain (2004).
Donc, il est nécessaire d'appliquer un ensemble de traitements sur les images d'empreintes digitales afin de les rendre prêtes à l'emploi et de conserver l'information utile.

Nous appliquons les méthodes de prétraitement définies au deuxième chapitre, pour binariser, squelettiser et extraire les minuties pour les images de test. Dans ce sens la procédure d'indexation par la méthode **HDT**, présentée dans le chapitre 3, est appliquée pour obtenir le modèle des empreintes digitale, les triangles généré étant des caractéristiques clé définissant la méthode de protection de notre système de reconnaissance développé '**HDT**'.

5.3 Application d'attaque par flou avec protection par HDT

Comme mentionné ci-dessus, la méthode d'indexation proposée est également considérée comme une approche de protection du système biométrique basée sur des techniques de transformation de caractéristiques. Les angles des triangles similaires extraits à la première étape de la méthode **HDT**, sont considérés comme une clé secrète faisant l'objet de l'information confidentielle (détaillé dans Elmouhtadi et Lafkih (2017)). Le barycentre est utilisé comme méthode de transformation. La Figure5.3 présente le scénario de la protection par **HDT**.

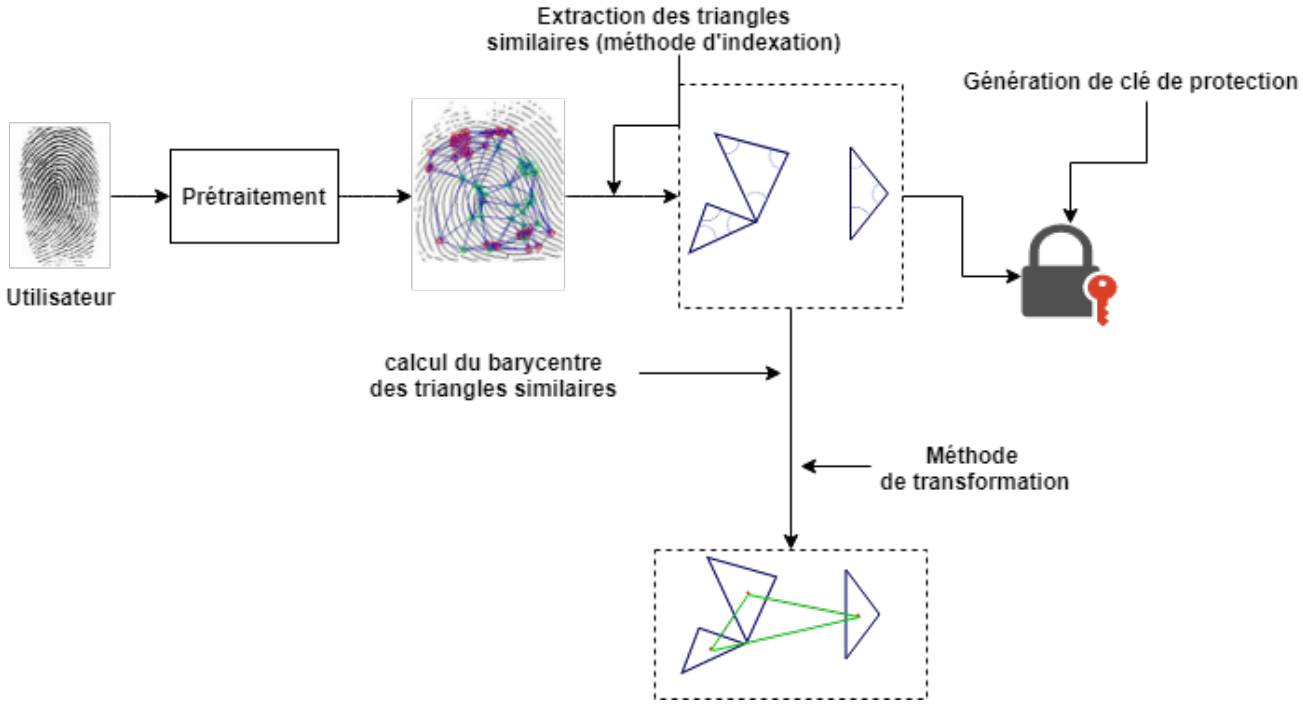


FIGURE 5.3 – Scénario de la protection par l'indexation HDT.

Les images floues sont utilisées comme type d'altération ; par conséquent, nous évaluons le système proposé sous la dégradation du flou. Des images floues sont générées sur la base du filtre 2D de Wiener, en utilisant plusieurs variantes du flou. Le tableau 5.3 présente un exemple d'image originale et floues. En outre, pour montrer la performance de l'approche proposée par rapport à la variation intraclasses et interclasses, le système est testé en utilisant à la fois les scénarios de vérification et d'identification. Dans le premier cas, on compare l'image de requête de l'utilisateur avec toutes les images stockées du même utilisateur où dans le second cas ; chaque image utilisateur est comparée à la base de données.

Les images d'altération permettent d'évaluer l'approche sur deux points.

(1). La performance de la méthode proposée sous la dégradation du signal.

(2). La sécurité de l'approche proposée contre l'attaque en utilisant des images mo-

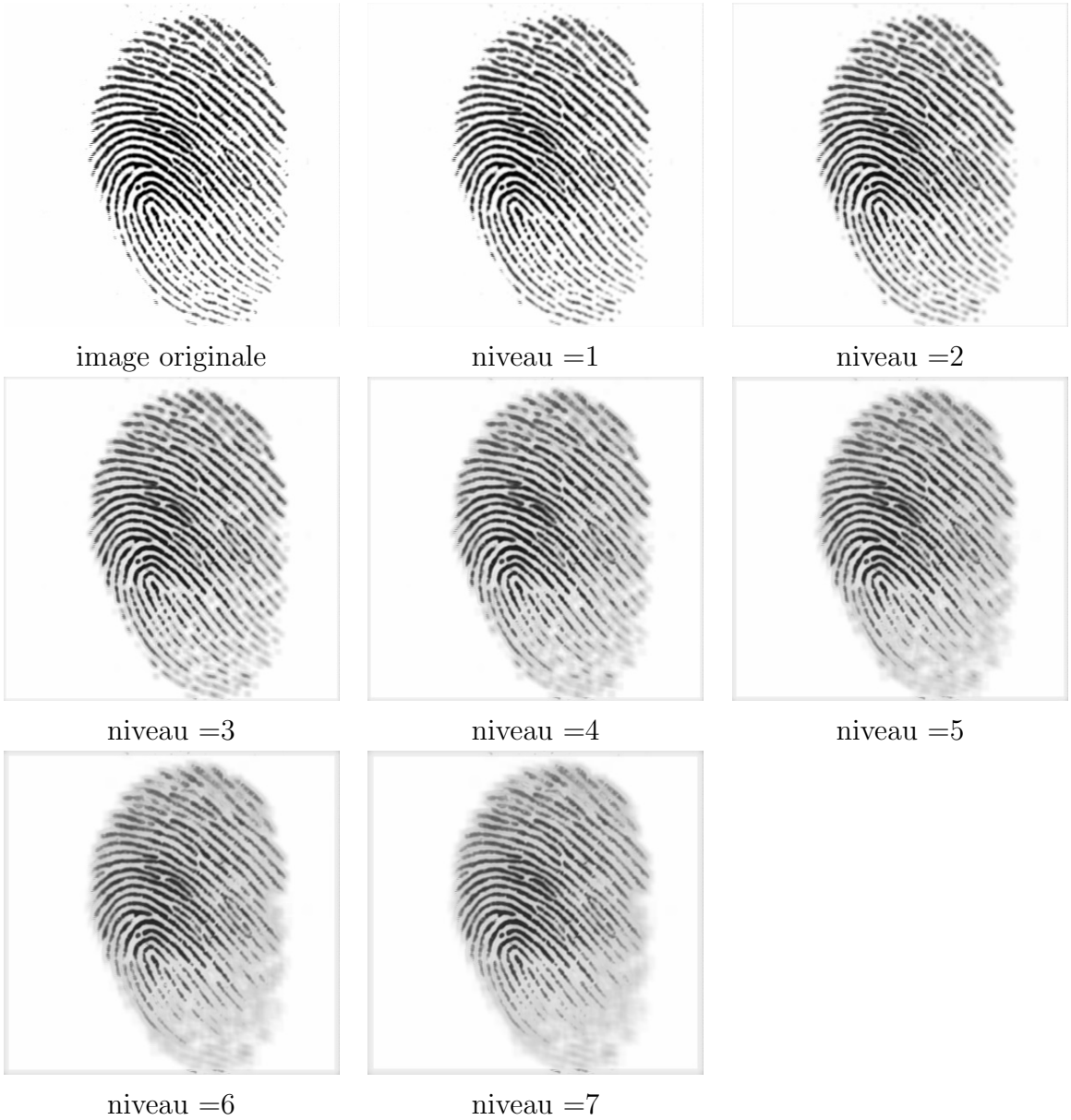


image originale | niveau =1 | niveau =2

niveau =3 | niveau =4 | niveau =5

niveau =6 | niveau =7

TABLE 5.1 – Les sept niveaux d'altération de flou

difiées où l'attaquant présent au système a modifié les images d'un utilisateur réel, comme cité dans Lafkih *et al.* (2015).

5.3.1 Environnement d'expérimentation

Les expériences ont été réalisées sur un ordinateur personnel de bureau (PC) avec les caractéristiques suivantes :

Processor : Intel®Core™i5-3230M

Clock speed : 2.60 GHz

Cache : 8 MB

RAM : 4 GB

Operating system : Microsoft Windows 10 x64

Programming languages : MATLAB.

Softwares : MATLAB R2014b.

5.3.2 Base de données utilisée

Pour évaluer la performance de la méthode proposée, nous utilisons l'ensemble des données DB1_B de la base de données FVC2002 disponible dans **?**. FVC2002 DB1 et DB2 contiennent 880 empreintes digitales, de qualité variable, à partir de 110 doigts distincts (chaque personne est représentée par 8 impressions).

5.3.3 Tests et résultats

Premièrement, nous évaluons l'approche proposée en terme de performance. Les images de chaque utilisateur testées en référence contre les images floues avec différents niveaux de flou ([0, 7]). Le premier niveau est une dégradation légère de l'image par flou, par la suite on augmente le degré de flou tout en ajoutant un autre niveau jusqu'au septième dégradation qui représente une image peu claire. Les images floues sont considérées comme des demandes présentées par l'utilisateur réel. Certaines variantes sont présentées par l'attaquant qui a accès à l'image modifiée de l'utilisateur réel (levée à l'aide d'une trace mobile ou d'un objet touché).

La Figure5.4 montre la distribution du score d'adaptation en fonction du niveau d'altération. Nous remarquons que le score d'appariement varie avec l'altération du niveau, où les scores d'appariement diminuent lorsque les niveaux augmentent. De plus, on remarque que même si le niveau est minimal (égal à 1), le score d'appariement reste limité, ceci est dû aux deux approches de transformation, basées sur le barycentre, utilisées sur notre proposition qui augmentent la performance du système et entravent l'acceptation de demande de modification qui peut être utilisée par un attaquant pour obtenir un accès illégitime.

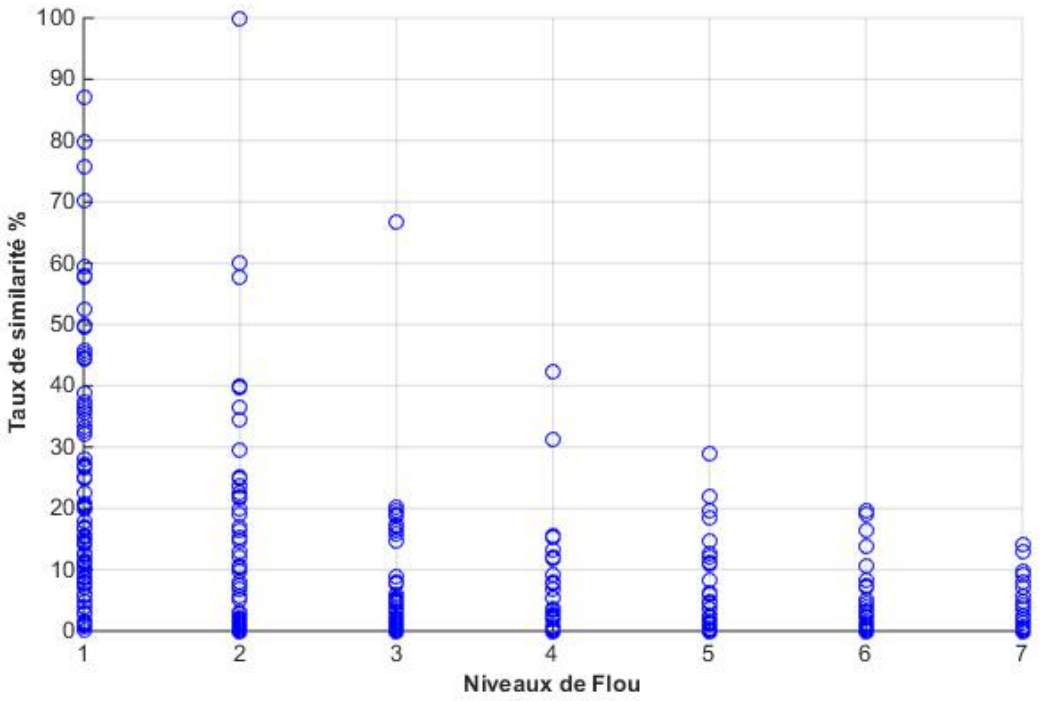


FIGURE 5.4 – Variation du score de la similarité des empreintes digitales correspondant aux différents niveaux de flou.

Plus de détails sont présentés dans la table 5.2, où le score d'appariement diffère d'un utilisateur à l'autre ; si le niveau d'altération est égal à 1, nous remarquons que le score variera entre 45 et 87. Ce score présente un faible pourcentage d'appariement pour la majorité des images de l'utilisateur ; ceci explique la robustesse obtenue par la méthode proposée contre les attaques d'altération même si l'altération est faible.

Sur la Figure5.5, nous présentons la courbe **ROC** relative à l'approche. Cela présente la variation entre les fausses images acceptées, qui identifient normalement un faux utilisateur par rapport à une image non-correspondante. Le taux de faux positifs a été généré en comparant pour chaque utilisateur les sept niveaux d'altérations selon leurs différentes variations d'image. Nous pouvons remarquer que l'approche proposée préserve,

Niveau/image de test	1	2	3	4	5	6	7
1	49,79	36,46	16,49	0	4,61	0	0
2	75,77	60	66,66	42,42	28,78	5,17	0
3	70,21	57,65	20,33	12,12	12	0	0
4	87,17	100	0	0	0	0	0
5	52,55	23,76	4,54	2,50	0,89	2,98	3,57
6	59,56	40,07	14,56	8,06	7,04	6,31	5,10
7	45,16	22,58	0	0	0	0	0

TABLE 5.2 – Scores de matching pour des empreintes de test selon les sept niveaux de flou

en général, la performance du système d'indexation proposé, ce qui signifie que l'indexation hiérarchique résiste aux attaques avec une image reconstruite sous différents niveaux d'altération.

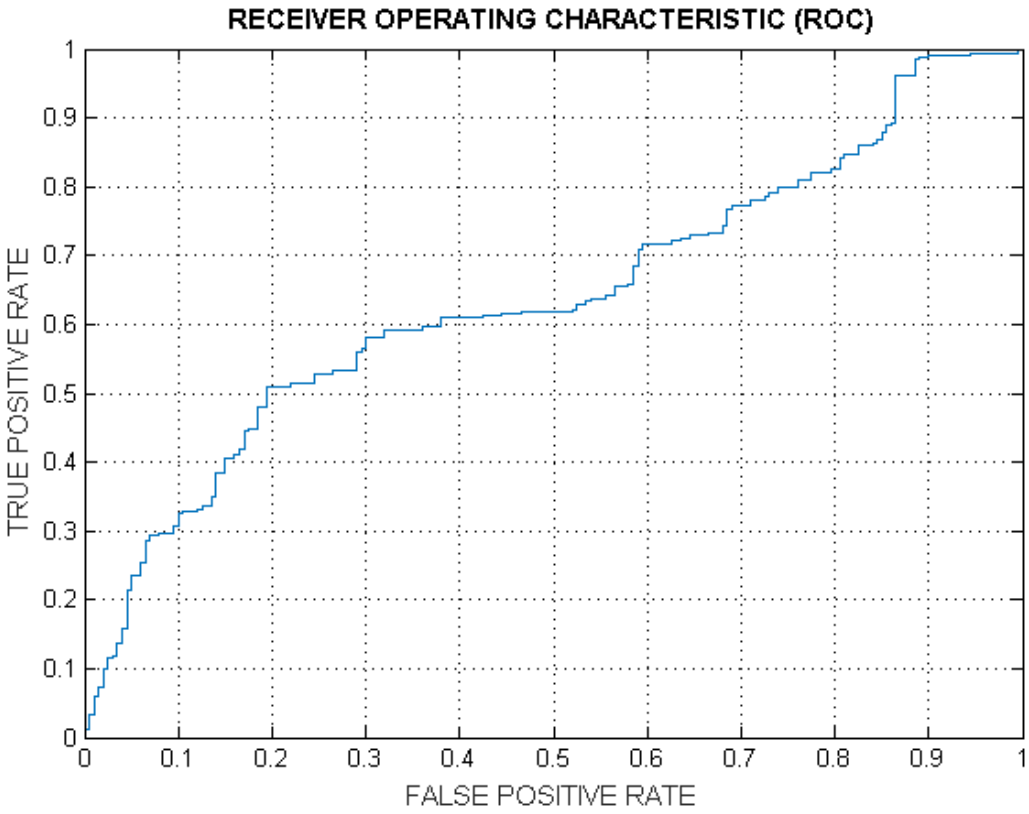


FIGURE 5.5 – La courbe Roc.

Enfin, comme l'un des principaux objectifs des algorithmes d'indexation et d'identification est d'accélérer le processus d'identification, nous énumérons dans la table 5.3.3 le temps total passé sur toutes les étapes de notre algorithme.

Étape du processus d'indexation et identification	Temps(s)
Prétraitement, extraction des minuties et le post-traitement.	12,98 s
Extraction de triangles similaires et correspondance.	2,55 s
Création d'index en générant les triangles du barycentre.	0,06 s
Moyenne de vérification d'un utilisateur existant dans la BD.	11.796 s
Moyenne vérification d'un utilisateur flou.	19,32 s

TABLE 5.3 – Résultats de matching

5.4 Conclusion

Dans ce chapitre, nous avons présenté une nouvelle approche pour la protection des modèles d'empreintes digitales basée sur la transformation des caractéristiques d'em-

preintes digitales. Dans ce contexte, nous avons proposé une méthode d'indexation basée sur le minuties triplet et leur transformation. Cette méthode est considérée comme une protection du système biométrique qui considère les angles des triangles obtenus comme clé secrète qui présente les informations confidentielles de l'empreinte digitale. Nous avons généré les images d'empreintes digitales floues comme un moyen d'altération de l'attaque. Les résultats obtenus présentent une bonne tolérance de l'attaque présentée par le système de protection proposé.

Chapitre

6 Conclusion générale et perspectives

Rappel de la problématique

La problématique principale de la thèse consiste à développer une méthode d'indexation des empreintes digitales et d'apporter des améliorations dans ce domaine. Ce qui revient à la conception d'un algorithme de type recherche d'image basées sur le contenu appliqué à des images d'empreintes digitales. Essentiellement faire face aux contraintes suivantes imposées par le sujet.

✾ Faire face à l'inefficacité des systèmes d'identification face aux transformations affines. En termes techniques, cela se traduisait par un taux de faux rejets très faible et faux acceptation faible.

✾ Établir un algorithme qui prend en considération le coût moyen en temps de calcul d'une image requête contre une image de référence.

✾ Garantir la sécurité de l'empreinte digitale en étant une information personnelle contre les menaces par attaques biométriques.

✾ Coût moyen faible en temps de calcul d'une image requête contre une image de référence.

6.1 Conclusion et perspectives.

Au cours de cette thèse, nous nous sommes intéressé par l'indexation des empreintes digitales, en s'appuyant sur les méthodes de traitement de l'image par son contenu dans les grandes bases de données. Nous avons chercher à analyser l'influence des différentes contraintes sur les systèmes de reconnaissance de bases de données.

Dans un premier lieu nous avons présenté un état de l'art sur l'importance des empreinte digitales autant que système de reconnaissance biométrique. Ensuite, une étude des caractéristiques de l'empreintes digitales a été présentée, pour but de déduire les meilleures descripteurs d'une image d'empreinte digitale en termes de robustesse de performance acquises lors de leurs utilisation.

En se basant sur des avancées scientifique, et comme première contribution, les descripteurs locaux de l'empreinte ont été choisis comme clé primaire pour établir l'indexation. Nous avons par la suite opté pour l'utilisation de la triangulation Delaunay des points minuties extraites comme méthode de transformation décrivant le vecteur principale du modèle d'indexation. Nous avons présenté par la suite notre méthode **HDT** qui consiste à la transformation hiérarchique des triangles Delaunay. Une méthode qui a été introduite pour la première fois dans le contexte d'indexation par minuties et triplet, sa performance consiste dans le fait de garantir la ressemblance de la disposition topologique des minuties appariés, en plus que sa tolérance aux transformations affines que peuvent changer l'orientation, le zoom et la qualité de l'image requête. Nous avons donc présenté un système d'indexation qui garantie la pertinence de reconnaissance, l'une des majeurs contraintes.

En adoptant les performances de la première contribution, la deuxième contribution est à la fois une méthode d'accélération de la première et hybridation avec les descrpiteurs globaux de l'empreinte digitale. Nous avons joigné l'utile à l'agréable, l'utile en étant la performance de la méthode d'indexation par **HDT**, et l'agréable consiste à minimiser le coût de temps de calcul pour chaque comparaison de deux empreintes. Nous avons commencé par l'extraction du point singulier autant que point central de l'image qui permet la localisation des minuties, considérées de haut niveau. nous avons appliqué par la suite l'indexation par **HDT** au voisinage du point singulier, une région ayant une faible possibilité de pertes de minuties. Les résultats sont prometteuses en terme de pertinence et temps de calcul. Nous avons donc établit la contrainte de rapidité de l'algorithme.

La dernière contrainte, qui consiste à sécuriser l'information biométrique, a été étudié dans le dernier chapitre. Nous avons présenté durant cette étude les différents types d'attaques biométriques, plus précisément les attaques de l'empreinte digitale. Et pour la première fois, une étude a été établit sur l'apport de la méthode de l'indexation face à la falsification de l'image de l'empreinte digitale. Ainsi que nous avons montré la sécurité de l'indexation par **HDT** avec l'application d'une attaque par flou, qui représente à son tour l'attaque par falsification ou par reconstitution d'une empreinte digitale. Les résultats de reconnaissance ont été strictement décroissantes en ajoutant du flou à l'image originale.

Ce travail peut être considéré comme une base pour les travaux futurs dans cette direction de recherche. Les perspectives de cette thèse sont nombreuses.

✾ Chercher à utiliser d'autres caractéristiques des triangles de Delaunay, dans le but d'améliorer la pertinence de la méthode proposées.

✾ La proposition d'une accélération de la méthode de triangulation en se basant sur

d'autres descripteurs de l'empreinte digitale.

✾ Tester la sécurité de la méthode HDT selon d'autres scénarios d'attaques et d'autres types d'altérations. Des travaux sont en cour d'exécution dans ce sens.

BIBLIOGRAPHIE

(2006). *The science of fingerprints : classification and uses*. Federal Bureau of Investigation.

ASSOGBA, M. K. et ALI, A. N. (2011). Fingerprint characteristic extraction by ridge orientation : An approach for a supervised contactless biometric system. *International Journal of Computer Applications*, 16(6).

ATTALI, D., di BAJA, G. S. et THIEL, E. (1995). Pruning discrete and semicontinuous skeletons. *In International Conference on Image Analysis and Processing*, pages 488–493. Springer.

ATTALI, D. et THIEL, E. (1993). Du squelette discret ou continu. *3e DGCI, Discrete Geometry for Computer Image*, pages 236–244.

AWAD, A. I. et BABA, K. (2012). Singular point detection for efficient fingerprint classification. *International Journal of New Computer Architectures and their Applications (IJNCAA)*, 2(1):1–7.

BAZEN, A. M. et GEREZ, S. H. (2002). Systematic methods for the computation of the directional fields and singular points of fingerprints. *IEEE transactions on pattern analysis and machine intelligence*, 24(7):905–919.

BEBIS, G., DEACONU, T. et GEORGIOPOULOS, M. (1999). Fingerprint identification using delaunay triangulation. *In Information Intelligence and Systems, 1999. Proceedings. 1999 International Conference on*, pages 452–459. IEEE.

BERRY, J. et STONEY, D. A. (2001). The history and development of fingerprinting. *Advances in fingerprint Technology*, 2:13–52.

BHATNAGAR, J. et KUMAR, A. (2009). On estimating performance indices for biometric identification. *Pattern Recognition*, 42(9):1803–1815.

BLUM, H. (1967). A transformation for extracting new descriptors of shape. *Models for Perception of Speech and Visual Forms, 1967*, pages 362–380.

BRINGER, J. et CHABANNE, H. (2008). An authentication protocol with encrypted biometric data. *In International Conference on Cryptology in Africa*, pages 109–124. Springer.

Cappelli, R., Maio, D., Maltoni, D., Wayman, J. L. et Jain, A. K. (2006). Performance evaluation of fingerprint verification systems. *IEEE transactions on pattern analysis and machine intelligence*, 28(1):3–18.

de Boer, J., Bazen, A. M. et Gerez, S. H. (2001). Indexing fingerprint databases based on multiple features.

Elmouhtadi, M., Aboutajdine, D. *et al.* (2018a). Fingerprint identification using hierarchical matching and topological structures. *In Advances in Soft Computing and Machine Learning in Image Processing*, pages 393–408. Springer.

Elmouhtadi, M., Aboutajdine, D. et El Fkihi, S. (2015). Fingerprint indexing based barycenter triangulation. *In Complex Systems (WCCS), 2015 Third World Conference on*, pages 1–6. IEEE.

Elmouhtadi, M., El fkihi, S. et Aboutajdine, D. (2018b). Fingerprint identification based on hierarchical triangulation. *Journal of Information Processing Systems*, 14(2): 435–447.

Elmouhtadi, M., ELfkihi, S. et Aboutajdine, D. (2016). Improving fingerprint matching using delaunay triangulation features. *In Proceedings of the International Conference on Big Data and Advanced Wireless Technologies*, page 55. ACM.

Elmouhtadi, M. et Lafkih, M. (2017). Biometric protection approach based on fingerprint hierarchical identification. *International Journal of Applied Engineering Research*, 12(21):11007–11014.

Feng, J. et Zhou, J. (2011). A performance evaluation of fingerprint minutia descriptors. *In Hand-Based Biometrics (ICHB), 2011 International Conference on*, pages 1–6. IEEE.

Galar, M., Derrac, J., Peralta, D., Triguero, I., Paternain, D., Lopez-Molina, C., García, S., Benítez, J. M., Pagola, M., Barrenechea, E. *et al.* (2015). A survey of fingerprint classification part i : Taxonomies on feature extraction methods and learning models. *Knowledge-based systems*, 81:76–97.

Galbally, J., Fierrez, J., Alonso-Fernandez, F. et Martinez-Diaz, M. (2011). Evaluation of direct attacks to fingerprint verification systems. *Telecommunication Systems*, 47(3-4):243–254.

Galton, F., Darwin, S. G. H. et Okamoto, S. (1909). *Identification by fingerprints.*

Hong, L. et Jain, A. (1999). Classification of fingerprint images. *In Proceedings of the Scandinavian Conference on image Analysis*, volume 2, pages 665–672. Citeseer.

Jain, A. et Pankanti, S. (2000). Fingerprint classification and matching. *Handbook for Image and Video Processing.*

Jain, A. et Ross, A. (2002). Fingerprint mosaicking. *In Acoustics, Speech, and Signal Processing (ICASSP), 2002 IEEE International Conference on*, volume 4, pages IV–4064. IEEE.

Jain, A. K., Nandakumar, K. et Nagar, A. (2008). Biometric template security. *EURASIP Journal on advances in signal processing*, 2008:113.

Jin, A. T. B., Ling, D. N. C. et Goh, A. (2004). Biohashing : two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognition*, 37(11): 2245–2255.

Khodadoust, J. et Khodadoust, A. M. (2017). Fingerprint indexing based on expanded delaunay triangulation. *Expert Systems with Applications*, 81:251–267.

Kong, T. Y. et Rosenfeld, A. (1989). Digital topology : Introduction and survey. *Computer Vision, Graphics, and Image Processing*, 48(3):357–393.

Kumar, D. A. et Begum, T. U. S. (2013). A comparative study on fingerprint matching algorithms for evm. *Journal of Computer Sciences and Applications*, 1(4):55–60.

Kumar, R., Chandra, P. et Hanmandlu, M. (2016). A robust fingerprint matching system using orientation features. *Journal of Information Processing Systems*, 12(1):83–99.

Lafkih, M., Lacharme, P., Rosenberger, C., Mikram, M., Ghouzali, S., El Haziti, M., Abdul, W. et Aboutajdine, D. (2015). Application of new alteration attack on biometric authentication systems. *In Anti-Cybercrime (ICACC), 2015 First International Conference on*, pages 1–5. IEEE.

Lambourne, G. (1984). *The fingerprint story*. Harrap.

Lee, H. C., Ramotowski, R. et Gaensslen, R. E. (2001). *Advances in fingerprint technology*. CRC press.

Liang, X., Asano, T. et Bishnu, A. (2006). Distorted fingerprint indexing using minutia detail and delaunay triangle. *In Voronoi Diagrams in Science and Engineering, 2006. ISVD'06. 3rd International Symposium on*, pages 217–223. IEEE.

Liu, M. (2010). Fingerprint classification based on adaboost learning from singularity features. *Pattern Recognition*, 43(3):1062–1070.

Liu, M., Jiang, X. et Kot, A. C. (2007a). Efficient fingerprint search based on database clustering. *Pattern Recognition*, 40(6):1793–1803.

Liu, M., Jiang, X. et Kot, A. C. (2007b). Efficient fingerprint search based on database clustering. *Pattern Recognition*, 40(6):1793–1803.

Liu, N., Yin, Y. et Zhang, H. (2005). A fingerprint matching algorithm based on delaunay triangulation net. *In Computer and Information Technology, 2005. CIT 2005. The Fifth International Conference on*, pages 591–595. IEEE.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J. et Jain, A. (2004). Fvc2004 : Third fingerprint verification competition. *Biometric Authentication*, pages 31–35.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L. et Jain, A. K. (2002a). Fvc2000 : Fingerprint verification competition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(3):402–412.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L. et Jain, A. K. (2002b). Fvc2000 : Fingerprint verification competition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(3):402–412.

Maltoni, D., Maio, D., Jain, A. K. et Prabhakar, S. (2009). *Handbook of fingerprint recognition*. Springer Science & Business Media.

Medina-Pérez, M. A., García-Borroto, M., Gutierrez-Rodríguez, A. E. et Altamirano-Robles, L. (2012). Improving fingerprint verification using minutiae triplets. *Sensors*, 12(3):3418–3437.

Moujahdi, C., Bebis, G., Ghouzali, S. et Rziza, M. (2014). Fingerprint shell : Secure representation of fingerprint template. *Pattern Recognition Letters*, 45:189–196.

MuñOz-BriseñO, A., Gago-Alonso, A. et HernáNdez-Palancar, J. (2013). Fingerprint indexing with bad quality areas. *Expert Systems with Applications*, 40(5):1839–1846.

Nandakumar, K. et Jain, A. K. (2004). Local correlation-based fingerprint matching. *In ICVGIP*, pages 503–508.

Otsu, N. (1979). A threshold selection method from gray-level histograms. *IEEE transactions on systems, man, and cybernetics*, 9(1):62–66.

Parker, J. R. (2010). *Algorithms for image processing and computer vision*. John Wiley & Sons.

Ratha, N. K., Connell, J. H. et Bolle, R. M. (1998). Image mosaicing for rolled fingerprint construction. *In Pattern Recognition, 1998. Proceedings. Fourteenth International Conference on*, volume 2, pages 1651–1653. IEEE.

Ratha, N. K., Connell, J. H. et Bolle, R. M. (2001). An analysis of minutiae matching strength. *In International Conference on Audio-and Video-Based Biometric Person Authentication*, pages 223–228. Springer.

Ratha, N. K., Karu, K., Chen, S. et Jain, A. K. (1996). A real-time matching system for large fingerprint databases. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 18(8):799–813.

Saleh, A., Bahaa, A. et Wahdan, A. (2011). Fingerprint recognition, advanced biometric technologies.

Sezgin, M. *et al.* (2004a). Survey over image thresholding techniques and quantitative performance evaluation. *Journal of Electronic imaging*, 13(1):146–168.

Sezgin, M. *et al.* (2004b). Survey over image thresholding techniques and quantitative performance evaluation. *Journal of Electronic imaging*, 13(1):146–168.

Teoh, A. B., Goh, A. et Ngo, D. C. (2006). Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28(12):1892–1901.

TISSE, C.-L., MARTIN, L., TORRES, L. et ROBERT, M. (2001). Système automatique de reconnaissance d'empreintes digitales. sécurisation de l'authentification sur carte à puce. *In 18Â° Colloque sur le traitement du signal et des images, FRA, 2001.* GRETSI, Groupe d'Etudes du Traitement du Signal et des Images.

Van der Putte, T. et Keuning, J. (2000). Biometrical fingerprint recognition : don't get your fingers burned. *In Smart Card Research and Advanced Applications*, pages 289–303. Springer.

Wang, S., Zhang, W. W. et Wang, Y. S. (2002). Fingerprint classification by directional fields. *In Multimodal Interfaces, 2002. Proceedings. Fourth IEEE International Conference on*, pages 395–399. IEEE.

Xia, Y. (1989). Skeletonization via the realization of the fire front's propagation and extinction in digital binary shapes. *IEEE transactions on pattern analysis and machine intelligence*, 11(10):1076–1086.

Yoon, S., Feng, J. et Jain, A. K. (2012). Altered fingerprints : Analysis and detection. *IEEE transactions on pattern analysis and machine intelligence*, 34(3):451–464.

Zaeri, N. (2011). Minutiae-based fingerprint extraction and recognition. *In Biometrics.* InTech.

Zhang, T. et Suen, C. Y. (1984). A fast parallel algorithm for thinning digital patterns. *Communications of the ACM*, 27(3):236–239.

Zhou, J., Chen, F. et Gu, J. (2009). A novel algorithm for detecting singular points from fingerprint images. *IEEE transactions on pattern analysis and machine intelligence*, 31(7):1239–1250.

Zhou, J., He, D., Rong, G. et Bian, Z.-q. (2001). Effective algorithm for rolled fingerprint construction. *Electronics Letters*, 37(8):492–494.

Résumé

Dans un monde technologiquement croissant, l'augmentation des appareils, de téléphones intelligents, et des instances de stockage, est allée de pair avec l'accroissement de l'information biométrique de l'individu.

Faciliter l'accès, l'utilisation fluide et assurer la sécurité des modèles biométriques stockés sont des problèmes qui demeurent critiques. Ainsi que se suscite le regain d'intérêt pour des recherches progressives et, à terme, pour la réalisation de solutions technologiques. Ces dernières doivent assurer la confidentialité des images biométriques, l'efficacité de la recherche, et la rapidité. Nous croyons que ces contraintes constituent les sommets du triangle de pertinence du système de reconnaissance, ainsi que le défi est de trouver le moyen d'équilibrer ces contraintes. C'est la perspective suivie dans cette thèse. Dans ce contexte, nous avons contribué dans la recherche et l'indexation des empreintes digitale par la proposition de deux approches. La première, appelée HDT, pour la mise en place d'un pertinent algorithme d'indexation fondé sur la transformation hiérarchique des caractéristiques locales par triangulation. Une deuxième approche, vise l'accélération de la méthode proposée pour la rapidité du système de reconnaissance en se basant sur la région points singuliers. Nous avons également évalué la sécurité de l'approche proposée selon un scénario d'attaque biométrique par altération d'image.

Abstract

In a technologically growing world, the increase in devices, smartphones, and storage instances has gone hand in hand with the growth of the individual's biometric information.Facilitating access, easy use and ensuring the security of stored biometric models are issues that remain critical. As well as the renewed interest for progressive research and, in term, for the realization of technological solutions. These researches must ensure the confidentiality of biometric images, the effectiveness of research, and speed. We believe that these constraints are the vertices of the recognition system relevance triangle's, and the challenge is to find a way to balance these constraints. This is the perspective followed in this thesis. In this context, we contributed to the fingerprints research and indexing by proposing two approaches. The first one, called HDT, for the implementation of a relevant indexation algorithm based on the hierarchical transformation of the local characteristics by triangulation. A second approach aims at accelerating the proposed method for the recognition system rapidity based on the singular points region. We also evaluated the security of the proposed approach according to a biometric attack scenario by image alteration.