Université Dr. YAHIA FARES de Médéa

Faculté des Sciences et de la Technologie

Département du Génie électrique et de l'Informatique

Mémoire de fin d'études pour obtention le diplôme

Master en Génie électrique

Option : Systèmes des Télécommunications

Thème

Reconnaissance Des Empreintes Digitales

Présenté Par :

M. DEBIEB Youcef

M. METIDJI Hamza

Encadré par :

Dr. SOLTANE Mohamed

2011 /2012

Remerciement

Au terme de ce mémoire nous tenons à remercier tout naturellement en premier lieu Dieu le tout puissant qui nous a donné la force, le courage et la patience de bien mener ce travail.

A travers ce modeste travail, nous tenons à remercier vivement notre promoteur Dr. SOLTANE Mohamed pour ses conseils précieux et pour toutes les commodités et aisances qu'il nous a apportées durant notre étude et réalisation de ce projet.

Nos remerciements les plus vifs s'adressent aussi aux messieurs le président et les membres de jury d'avoir accepté d'examiner et d'évaluer notre travail.

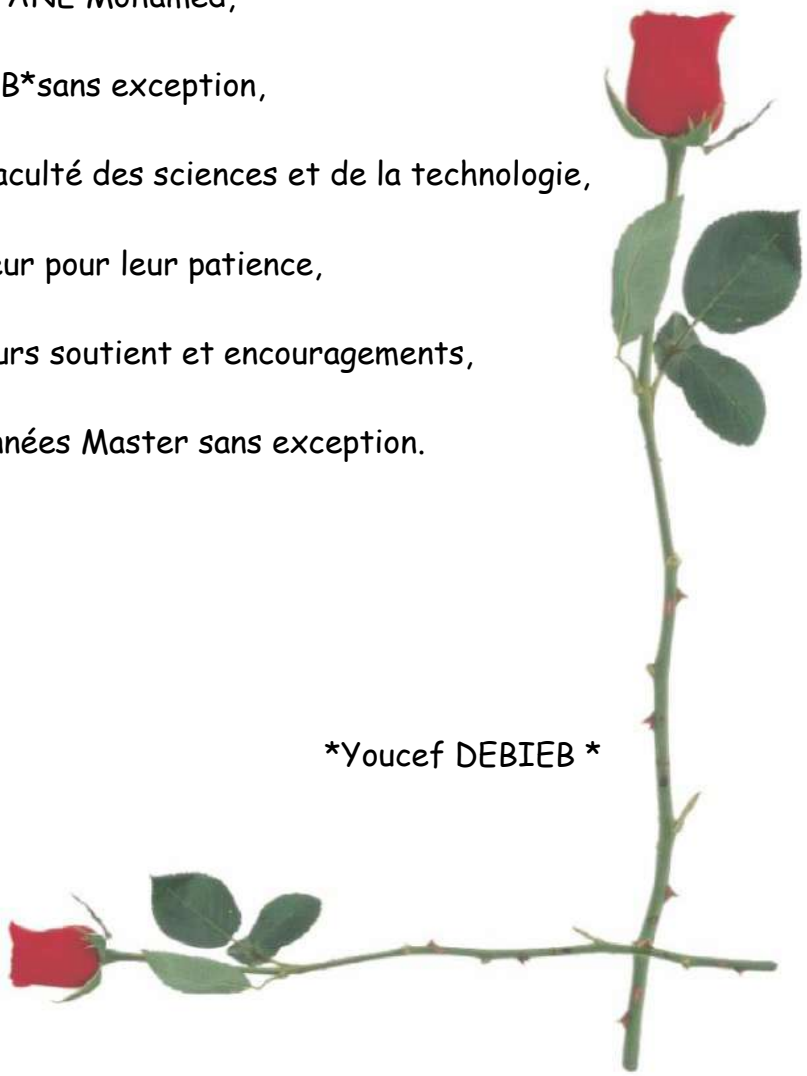
Nous exprimons également notre gratitude à tous enseignants qui ont collaboré à notre formation depuis notre premier et deuxième cycle d'étude universitaire.

Sans omettre bien sur de remercier profondément tous ceux qui ont contribué de prés ou de loin à la réalisation du présent travail.

Dédicaces

Je dédie cet humble travail,

- À mes très chers parents, pour leurs amour et sacrifices,
- A mon promoteur Dr. SOLTANE Mohamed,
- A toutes la famille *DEBIEB*sans exception,
- A tous les enseignants de faculté des sciences et de la technologie,
- À mes adorables frères, sœur pour leur patience,
- À mes proches amis pour leurs soutient et encouragements,
- A toute la promotion 2ème années Master sans exception.

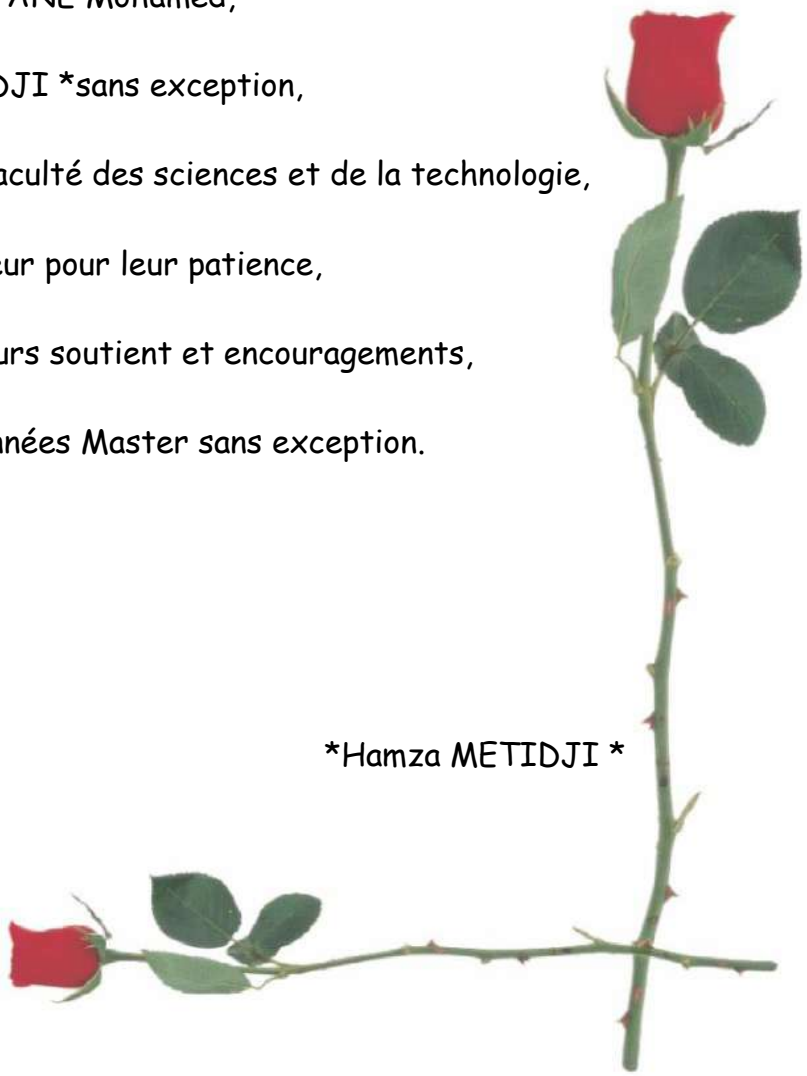


*Youcef DEBIEB *

Dédicaces

Je dédie cet humble travail,

- À mes très chers parents, pour leurs amour et sacrifices,
- A mon promoteur Dr. SOLTANE Mohamed,
- A toutes la famille *METIDJI *sans exception,
- A tous les enseignants de faculté des sciences et de la technologie,
- À mes adorables frères, sœur pour leur patience,
- À mes proches amis pour leurs soutient et encouragements,
- A toute la promotion 2ème années Master sans exception.



*Hamza METIDJI *

Liste des Figures

Figure (I.1) : Modalités biométriques……...…5
Figure (I.2) : Application biométriques…….8
Figure (I.3) : Schéma de fonctionnement d'un système biométrique (Enroulement)..……9
Figure (I.4) : Schéma de fonctionnement d'un système biométrique
(Identification/Vérification)……...….10
Figure (I.5) : graphes pour calculer les taux FAR et FRR ……..…….…….…....11

Figure (II.1) : Caractéristiques d une empreinte digitale……..14
Figure (II.2) : Les différents types de minutie……..14
Figure (II.3) : Les trois principales classes d'empreinte, boucle (a), spire (b), arche (c)…….15
Figure (II.4) : BMF BLP100-Sensor…….16
Figure (II.5) : DESLEY CMOS-Sensor……17
Figure (II.6) : Atmel FingerCHIP……17
Figure (II.7) : Veridicom 5th sense……...19
Figure (II.8) : Authentec ASE4000……..19
Figure (II.9) : Authentec AES2500…….……..20
Figure (II.10) : Transformations subies par l'image de l'empreinte digitale afin
D'extraire la signature……..22

Figure (III.1) : Vérification vs Identification……....24
Figure (III.2) : Système d'identification simplifié d'empreinte digitale……25
Figure (III.3) : Extracteur de minutie……26
Figure (III.4) : perfectionnement d'histogramme…..……28
Figure (III.5) : Perfectionnement d'empreinte digitale par FFT……29
Figure (III.6) : l'image d'empreinte digitale après binarisation…….30
Figure (III.7) : Carte de direction…….…….31
Figure (III.8) : Région originale d'image……..31

Figure (III.9) : Après opération OPEN..……..…….31
Figure (III.10) : Après opération CLOSE ….……...……32
Figure (III.11) : ROI + Bound……...…32

Figure (IV.1) : Interface graphique du système ….....38
Figure (IV.2) : fonctionnement du bouton charger ……..……39
Figure (IV.3) : fonctionnement du bouton égalisation ……...……40
Figure (IV.4) : fonctionnement du bouton TF ……..……41
Figure (IV.5) : fonctionnement du bouton direction ……...……..……42
Figure (IV.6) : fonctionnement du bouton ROI ……..…43
Figure (IV.7) : fonctionnement du bouton sup. transitoires ……44
Figure (IV.8) : fonctionnement du bouton vrai minutie ……..……45
Figure (IV.9) : fonctionnement du bouton sauvegarde …..…….……46
Figure (IV.10) : fonctionnement du bouton 1 à 1…….……...……..…47
Figure (IV.11) : fonctionnement du bouton 1 à N …….……...……...…48
Figure (IV.12) : Distribution des points corrects et des points incorrects……49
Figure (IV.13) : Courbe FAR et FRR en fct du seuil ……..50

Table des matières

Table des matières

Liste des figures

Introduction générale……1

Chapitre I : La biométrie

I.1 : Introduction.....3

I.1.1 : Identification d'empreinte digitale.....3

I.1.2 : Identification de visage.....3

I.1.3 : Identification d'iris.....4

I.1.4 : Identification de voix.....4

I.1.5 : Identification de Signature.....4

I.1.6 : Identification de main 5

I.2 : Historique 6

I.3 : Applications de la biométrie 8

I.4 : Système biométrique 9

I.4.1 : Vérification.....9

I.4.2 : Identification.....9

I.4.3 : Processus d'enregistrement.....9

I.4.4 : Processus d'identification /vérification.....10

I.4.5 : performances des systèmes biométriques 11

I.5 : Conclusion.....12

Chapitre II : L'empreinte digitale

II.1 : Introduction.....13
II.2 : Historique 13
II.3 : Caractéristiques d'une empreinte digitale.....15
II 4 : Les capteurs d'empreintes digitales.....16
II.4.1 : Le capteur de pression.....16
II.4.2 : Les capteurs optiques d'empreinte.....17
II.4.3 : Les capteurs électriques-thermique 17
II.4.4 : Capteurs capacitifs.....18
II.4.5 : Capteurs de champ-électrique.....19
II.5 : Méthode d'extraction de reconnaissance de l'empreinte digitale…….21
II.5.1 : Extraction de la signature……21
II.5.2 : Reconnaissance de l'empreinte digitale.....22
II.6 : Conclusion.....23

Chapitre III : Bases théoriques

III.1 : Introduction.....24
III.1.1 : Ce qui est identification d'empreinte digitale ?.....24
III.1.2 : Deux approches pour l'identification d'empreinte digitale ……25
III.2 : Conception de système…….....25
III.2.1 : conception au niveau système…….25
III.2.2 : Conception de niveau d'algorithme…….26
III.3 : Prétraitement d'image d'empreinte digitales……...27
III.3.1 : Perfectionnement d'image d'empreinte digitale……...27
III.3.1.1 : Égalisation d'histogramme ……..…….27
III.3.1.2 : Transformée de Fourier Rapide……..……..28
III.3.2 : Binarisation d'empreinte digitale…….29
III.3.3 : Segmentation d'image d'empreinte digitale…….30
III.4 : Extraction De Minutie…….32
III.4.1 : Éclaircissement d'empreinte digitale……..32
III.4.2 : Inscription de minutie……..32
III.5 : Traitement de minutie…….33
III.5.1 : Déplacement faux de minutie……..33
III.5.2 : Unifier les arrêts et les bifurcations ……34
III.6 : Comparaison De Minutie…….35
III.7 : Conclusion…….35

Chapitre IV : Implémentation et Résultats

IV.1 : Introduction……..…….……36

IV.2 : Base de données d'empreinte digitale utilisée…….……37

IV.3 : Implémentation et Résultats…….……..38

IV.3.1 : Introduire la commande **start_gui_single_mode** dans MATLAB R2011a.....38

IV.3.2 : le bouton **charger**.....39

IV.3.3 : le bouton **égalisation…….. .....**40

IV.3.4 : le bouton **TF.....**41

IV.3.5 : le bouton **binarization** …….……..…..42

IV.3.6 : le bouton **direction** ……..…….....42

IV.3.7 : le bouton **ROI**.....43

IV.3.8 : le bouton **squelettisation…**…….….44

IV.3.9 : le bouton **sup. coupures**.....44

IV.3.10 : le bouton **sup. transitoires**.....44

IV.3.11 : le bouton **extraction** ……..….……45

IV.3.12 : le bouton **vrai minutie** ……..…….....45

IV.3.13 : le bouton **sauvegarde**.....46

IV.3.14 : le bouton **1 à 1** ……...……47

IV.3.15 : le bouton **1 à N** …….....48

IV.3.16 : **Performance de logiciel** ……....……49

IV.4 : Conclusion.....51

Conclusion générale……..……52

Bibliographie

Annexe

Résumé

La reconnaissance d'empreintes digitales est une technique biométrique mature pour toute application d'identification ou de vérification d'individus. Dans cette thèse, nous décrivons la conception et le développement d'un système automatique d'authentification d'identité par empreintes digitales. Ce système automatique de reconnaissance d'empreintes digitales est basé sur une série d'algorithmes complexes apparentés aux domaines du traitement.

Mots clés : Biométrie, empreinte digitale

Abstract

The fingerprint recognition is a mature biometric identification for any application or verification of individuals. In this thesis, we describe the design and development of an automatic identity authentication by fingerprints. This automatic fingerprint recognition is based on a series of complex algorithms related to the areas of treatment.

Keywords: Biometrics, Fingerprint

الملخص

التعرف على بصمات الأصابع تعتبر من أهم التطبيقات لتحديد الهوية أو التحقق من الأفراد. في هذه المذكرة نقوم بتصميم وتطوير النظام الأوتوماتيكي لهذا الغرض. هذا النظام الأوتوماتيكي المتمثل في التعرف علي بصمات الأصابع مبني علي سلسلة الخوارزميات المعقدة في ميدان المعالجة الرقمية.

كلمات البحث : القياسات الحيوية، بصمات الأصابع

Introduction générale

L'identification biométrique se rapporte à l'utilisation de physiologique distinctif (par exemple empreinte digitale, iris, visage) et (par exemple démarche, signature) les caractéristiques comportementales, ont appelé les marques biométriques pour identifier des individus.

L'identification d'empreinte digitale est une des biométrique les plus ancienne et les plus fiable utilisée pour l'identification personnelle. L'identification d'empreinte digitale a été employée pendant plus de 100 années maintenant et est venue loin de l'assortiment manuel pénible d'empreinte digitale. Le procédé antique d'assortir des empreintes digitales était manuellement personnel habile extrêmement encombrant et long.

La peau de doigt se compose des arêtes de frottement et la sueur étudie à fond tous le long de ces arêtes. Des arêtes de frottement sont créées pendant la vie foetale et seulement la forme générale est génétiquement définie. La nature de distinction des caractéristiques physiques d'une personne est due à tous les deux la diversité génétique individuelle inhérente dans la population humaine aussi bien que les processus aléatoires affectant le développement de l'embryon. Les arêtes de frottement restent les mêmes durant toute sa vie adulte. Ils peuvent se reconstruire même en cas de dommages tant que les dommages ne sont pas trop sérieux.

Les empreintes digitales sont l'une des technologies biométriques les plus mûres et sont considérées les preuves légitimes de l'évidence aux Tribunaux partout dans le monde. Ces derniers temps, de plus en plus les applications commerciales civiles et emploient ou considèrent activement en utilisant l'identification empreinte basée en raison de la disponibilité des modules de balayage à semi-conducteur peu coûteux et compacts aussi bien que son supérieur et exécution assortie prouvée au-dessus d'autres technologies biométriques.

Quelques limites importantes liées aux systèmes d'identification d'empreinte digitale sont expliquées ci-dessous :

- Acquisition d'empreinte digitale : Comment acquérir des images d'empreinte digitale et comment les représenter dans un format compréhensible par une machine approprié.
- Vérification d'empreinte digitale : Pour déterminer si deux empreintes digitales sont du même doigt.
- Identification d'empreinte digitale : Pour rechercher une empreinte digitale de question dans une base de données.
- Classification d'empreinte digitale : Pour assigner une empreinte digitale donnée à une des catégories pré spécifiées selon ses caractéristiques géométriques.

I.1 : Introduction

La biométrie est un ensemble des technologies (appelées les technologies biométriques) qui exploitent des caractéristiques humaines physiques ou comportementales telles que l'empreinte digitale, la signature, l'iris, la voix, le visage, la démarche, et un geste de main pour différencier des personnes. Ces caractéristiques sont traitées par certain ordre des processus automatisés à l'aide des dispositifs comme des modules de balayage ou des appareils photo. À la différence des mots de passe ou des PINs (numéros d'identification personnelle) qui sont facilement oubliés ou exposés à l'utilisation frauduleuse, ou des clefs ou des cartes magnétiques qui doivent être portées par l'individu qui sont faciles à être volées, copiées ou perdues, ces caractéristiques biométriques sont uniques à l'individu et il y a peu de possibilité que d'autres individus peuvent remplacer ces caractéristiques, Donc les technologies biométriques sont considérées les plus puissantes en termes de sécurité. En plus les mesures biométriques sont confortables parce qu'elles n'ont pas besoin d'être portées séparément. De telles caractéristiques peuvent être bien employées pour obtenir l'identification/authentification pour accéder à des systèmes tels que les ATMs (guichet automatique). La biométrie se prouve également comme outil puissant d'identification/vérification aux scènes de crime dans le secteur juridique [3].

Les modalités biométriques généralement mises en application ou étudiées incluent la géométrie d'empreinte digitale, de visage, d'iris, de voix, de signature et de main [7]:

I.1.1 : Identification d'empreinte digitale

Empreinte digitale est la caractéristique d'un doigt. On le croit que chaque empreinte digitale est unique. Chaque personne a ses propres empreintes digitales avec l'unicité permanente. Ainsi les empreintes digitales sont utilisées depuis longtemps pour l'identification et l'investigation juridique [26].

I.1.2 : Identification de visage

La reconnaissance de la forme du visage est la technique la plus commune et Populaire. Elle est la plus acceptable parce qu'on peut l'utiliser à distance sans la Collaboration avec objet.
Utiliser une caméra permet d'acquiers la forme du visage d'un individu et puis retirer certaines caractéristiques. Les caractéristiques essentielles pour la reconnaissance du visage sont: les yeux, la bouche, le tour du visage, le bout du nez, etc. ... Selon le système utilisé, l'individu

doit être positionné devant la caméra ou peut être en mouvement à une certaine distance. Les données biométriques qui sont obtenues sont comparées au fichier référence. Le logiciel doit être capable d'identifier un individu malgré différents artifices physiques (moustache, barbe, lunettes, etc...) Le visage est une biométrie relativement peu sûre. En effet, le signal acquis est sujet à des variations beaucoup plus élevées que d'autres caractéristiques. Celles-ci peuvent être causées, entre autres, par le maquillage, la présence ou l'absence de lunettes, le vieillissement et l'expression d'une émotion. La méthode de la reconnaissance du visage est sensible à la variation de l'éclairage et le changement de la position du visage lors de l'acquisition de l'image [3].

I.1.3 : Identification d'iris

La reconnaissance de l'iris est considérée comme la technique biométrique la plus exacte. L'iris est la partie colorée de l'oeil qui entoure la pupille noire. Son inspection attentive révèle de nombreuses structures détaillées. Ces structures se développent dès le plus jeune âge et sont considérées comme uniques, même chez les vrais jumeaux. Les structures de l'iris resteront constantes jusqu'à la mort.

Pour reconnaître un individu, on extrait des paramètres de l'image de l'oeil. Puis, on compare ces paramètres avec tous les paramètres précédemment extraits et sauvegardés. La comparaison qui produira le meilleur score permettra d'identifier le nom de l'individu [3].

I.1.4 : Identification de voix

L'identification de la voix est considérée par les utilisateurs comme une des formes les plus normales de la technologie biométrique, car elle n'exige aucun contact physique avec le lecteur du système.

Les systèmes d'identification de la voix se concentrent sur les seules caractéristiques de voix qui sont uniques à la configuration de la parole d'un individu. Ces configurations de la parole sont constituées par une combinaison des facteurs comportementaux et physiologiques [3].

I.1.5 : Identification de Signature

Signer un document pour s'identifier est un geste naturel pour tout le monde. Dans la vie de tous les jours, nous signons régulièrement des documents. La reconnaissance de la signature est une des techniques biométriques comportementales. Dans le système d'identification par la signature, l'utilisateur doit signer avec un stylo lecteur sur une tablette graphique, le système analyse ensuit les variations de vitesse du stylo, la différence de pression sur la tablette

graphique au cours de la signature. Le point faible de cette technique est qu'un individu qui ne signe pas toujours de la même façon se verra souvent refuser l'accès au système. L'acceptation de cette technique est très bonne car la signature est un geste commun pour tout le monde [3].

I.1.6 : Identification de main :

Les dispositifs emploient un concept simple de mesurer et d'enregistrer la longueur, la largeur, l'épaisseur, et la superficie de la main d'un individu tandis que guidés d'un plat. Les systèmes de la géométrie de main emploient un appareil photo pour saisir une image de silhouette de la main.

La main du sujet est placée sur la plate, et guidée par cinq chevilles qui sentent quand la main est en place.

L'image saisit la surface supérieure de la main et une image latérale qui est saisie un miroir à angles. Sur la capture de l'image de silhouette, 31.000 points sont analysés et 90 mesures sont prises ; les mesures s'étendent de la longueur des doigts, à la distance entre les articulations, à la taille ou à l'épaisseur de la main et des doigts. Cette information est stockée en neuf bites de données, extrêmement - un nombre peu élevé comparé aux besoins de stockage d'autre système biométrique [11].

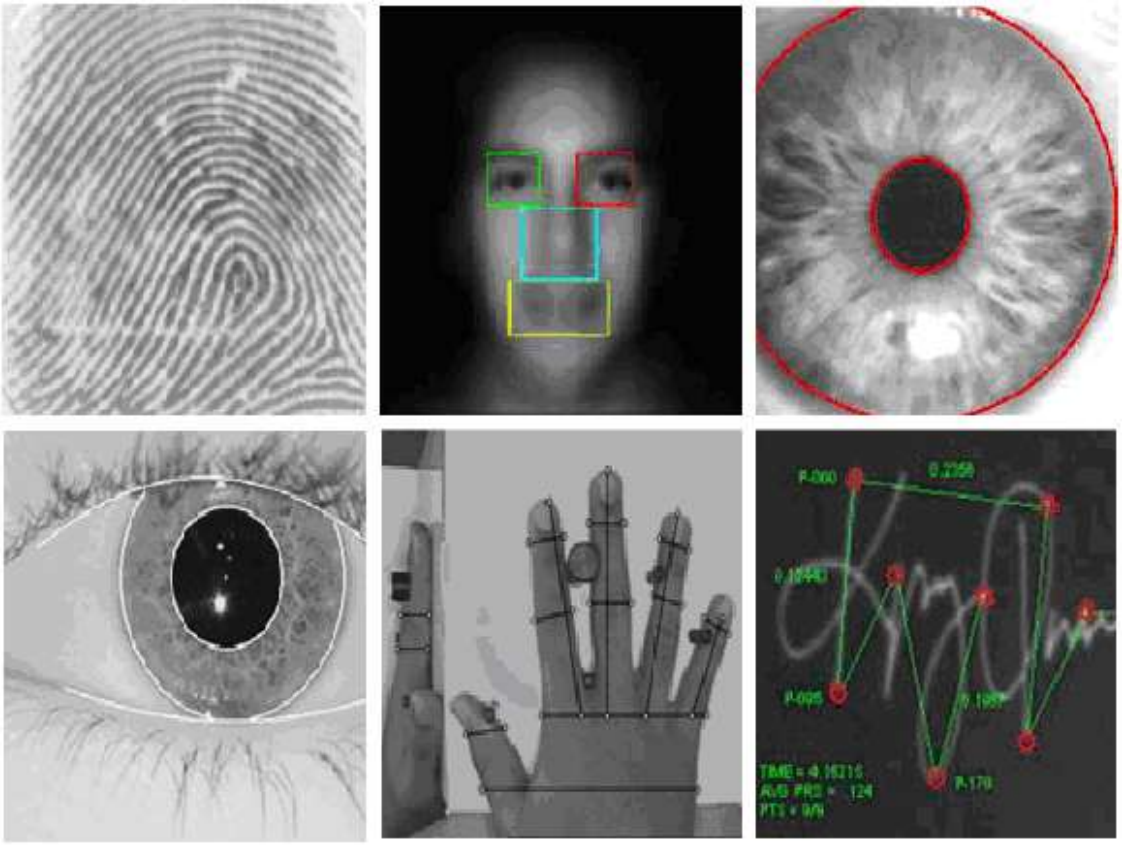


Figure (I.1) : Modalités biométriques

I.2 : Historique :

Le terme « biométrie » est dérivé des mots grecs « bio » (la vie) et « métrique » (à la mesure). Systèmes biométriques automatisés sont seulement devenus disponibles pendant les dernières décennies, dues à avances significatives dans le domaine du traitement par ordinateur. Beaucoup de ces nouvelles techniques automatisées, cependant, sont basées sur des idées c'étaient à l'origine des centaines conçues, même milliers d'années [2].

Un des exemples les plus anciens et les plus fondamentaux d'une caractéristique cela est employé pour l'identification par des humains est le visage. Depuis le commencement de la civilisation, les humains ont employé des visages pour identifier connu (familier) et individus (peu familiers) inconnus. Cette tâche simple est devenue de plus en plus provocant à mesure que les populations augmentaient et comme des méthodes plus commodes de voyage ont présenté beaucoup de nouveaux individus dans les communautés une fois petites.

D'autres caractéristiques ont été également employées dans toute l'histoire de la civilisation en tant que des moyens plus formels d'identification. Certains les exemples sont :

- Dans une caverne prévue pour être au moins 31.000 années, des murs sont ornées avec des peintures censées pour être créé par les hommes préhistoriques. Entourage de ces derniers les peintures sont de nombreux handprints aux lesquels sont sentis « … ont agi en tant que signature ONU forgeable » de son créateur.
- Il y a également d'évidence que des empreintes digitales ont été employées comme a la marque de la personne dès AVANT JÉSUS CHRIST « affaires 500 babyloniennes des transactions sont enregistrées dans des comprimés d'argile qui incluent empreintes digitales. »
- Joao de Barros, un explorateur espagnol et auteur, a écrit que les premiers négociants chinois avaient l'habitude des empreintes digitales pour arranger les transactions. Les parents chinois ont également employé empreintes digitales et empreintes de pas pour différencier des enfants les uns des autres.
- Dans l'histoire égyptienne tôt, des commerçants ont été identifiés près leurs descripteurs physiques à différencier entre les commerçants de confiance de la réputation connue et les transactions réussies précédentes, et ceux nouveaux au marché.

Par le mid-1800s, avec la croissance rapide des villes dues au Révolution Industrielle et une agriculture plus productive, il y avait besoin formellement d'identifier des personnes. Les négociants et des autorités ont été confrontés de plus en plus à plus grand et plus mobile les populations et pourraient plus ne compter seulement toutes seules expériences et connaissance locale. Influencé par les écritures de Jeremy Betham et d'autres penseurs utilitaires, les cours de ceci la période a commencé à codifier les concepts de la justice aux lesquels supporter avec nous ce jour. Spécialement, les systèmes de justice ont cherché à traiter la première fois contrevenantes plus clémente et contrevenantes de répétition plus durement. Ceci a créé un besoin de système formel qui a enregistré des offenses le long avec des traits mesurés d'identité du contrevenant. Le premier des deux des approches étaient le système de Bertillon de mesurer les divers corps dimensions, qui ont provenu en France. Ces mesures ont été écrites sur les cartes qui pourraient être assorties par taille, longueur de bras ou tout autre paramètre. Ce champ s'est appelé l'anthropométrie. L'autre approche était l'utilisation formelle des empreintes digitales par la police départements. Ce processus a émergé en Amérique du Sud, Asie, et L'Europe. La méthode 1800 a été développée pour indexer les empreintes digitales qui ont fourni la capacité de rechercher des disques. La méthode de Bertillon a été basée sur un plus métrique individualisé - modèles et arêtes d'empreinte digitale. Le premier a un tel système robuste pour des empreintes digitales d'indexation a été développé dedans L'Inde par Azizul Haque pour Edouard Henry, Inspecteur Général de Police, Bengale, Inde. Ce système, appelé le système de Henry, et les variations là-dessus sont encore en service pour classifier des empreintes digitales [21].

Les véritables systèmes biométriques ont commencé à émerger dans la dernière moitié du 20ème siècle, coïncidant avec l'apparition de l'ordinateur système. Le champ naissant a éprouvé une explosion d'activité dedans les années 90 et ont commencé à apprêter dans des applications journalières dans 2000s tôt [22].

I.3 : Applications de la biométrie :

Les techniques biométriques sont appliquées dans plusieurs domaines et ses applications sont divisées en trois groupes principaux :

- Applications commerciales: telles que l'accès au réseau informatique, la sécurité de données électroniques, le commerce électronique, l'accès d'Internet, l'ATM, la carte de crédit, le contrôle d'accès physique, le téléphone portable, le PDA, la gestion des registres médicale, l'étude de distance, etc...

- Applications de gouvernement: telles que la carte nationale d'identification, le permis du conducteur, la sécurité sociale, la contrôle de passeport, etc...

- Applications juridique: telles que l'identification de cadavre, la recherche criminelle, l'identification de terroriste, les enfants disparus, etc... [3]



Figure (I.2) : Application biométriques

I.4 : Système biométrique

Un système biométrique est essentiellement un système de reconnaissance de formes qui fonctionne en acquérant des données biométriques à partir d'un individuel, extrayant un ensemble de caractéristiques à partir des données acquises, et comparant ces caractéristiques contre la signature dans la base de données. Selon le contexte d'application, un système biométrique peut fonctionner en mode de vérification ou mode d'identification:

I.4.1 : Vérification

Le système valide l'identité d'une personne en comparant les données biométriques capturées à sa propre base de données. Dans un tel système, un individu qui désire être identifié réclame une identité, habituellement par l'intermédiaire d'un PIN (numéro d'identification personnelle), d'un nom d'utilisateur, d'une carte futée, etc., et le système conduit une comparaison d'un-à-un pour déterminer si la réclamation est vraie ou .

I.4.2 : Identification

Le système identifie un individu en recherchant les signatures (templates) de tous les utilisateurs dans la base de données. Par conséquent, le système conduit plusieurs des comparaisons pour établir l'identité d'un individu (ou échoue si le sujet n'est pas inscrit dans la base de données de système) sans devoir soumis réclamer une identité [3].

En général, tous les systèmes biométriques partagent le même schéma de fonctionnement. Ils se composent deux processus suivant :

I.4.3 : Processus d'enregistrement

Ce processus a pour but d'enregistrer les caractéristiques des utilisateurs dans la base de données.

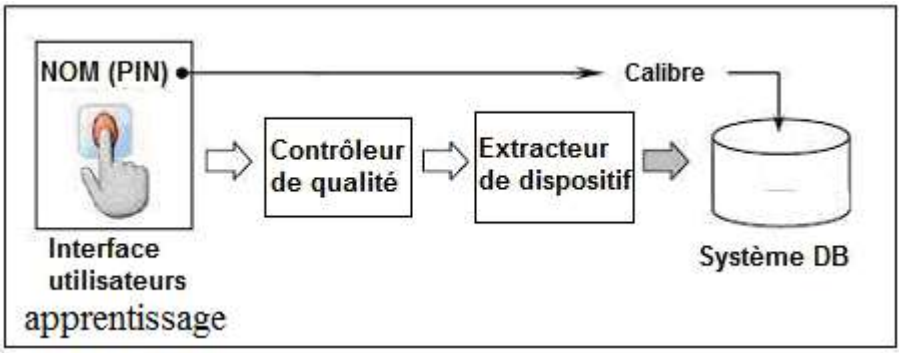


Figure (I.3) : Schéma de fonctionnement d'un système biométrique (Enroulement)

I.4.4 : Processus d'identification /vérification

Le processus d'identification/vérification est effectué lorsqu'une personne enregistrée dans a base de données biométriques doit s'identifier [3].

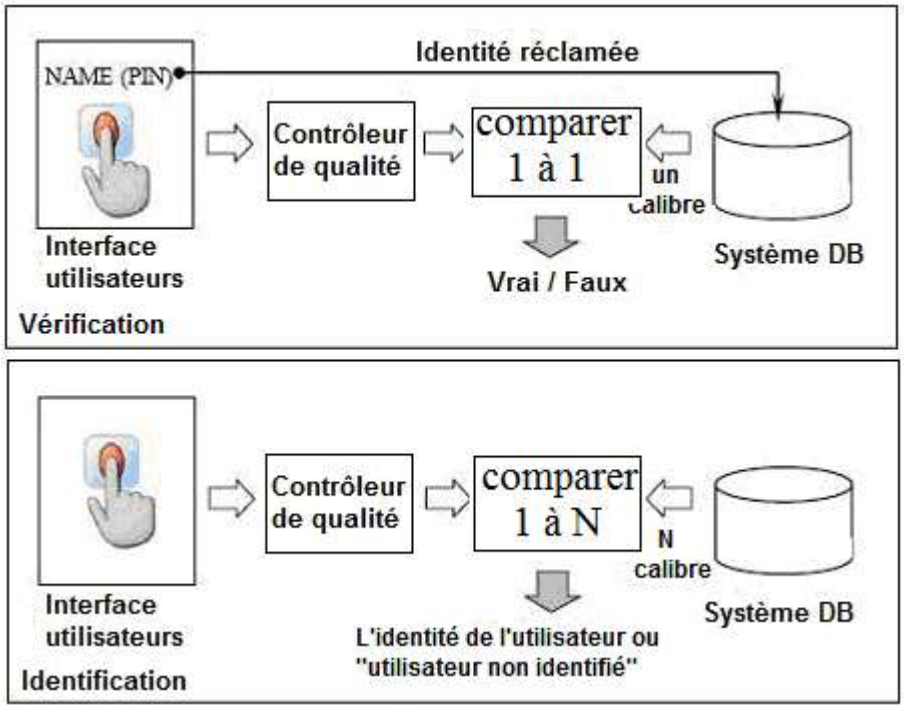


Figure (I.4) : Schéma de fonctionnement d'un système biométrique (Identification/Vérification)

I.4.5 : performances des systèmes biométriques

Dans les systèmes biométriques la phase finale d'appariement estime le degré de similitude (taux d'appariement) entre deux fichiers signatures et le compare à un seuil fixé à l'avance, ainsi le résultat n'est jamais fiable à 100% mais s'en approche selon le réglage du seuil. L'évaluation des performances de ces systèmes fait apparaître deux types d'erreur :

- le Taux de Faux Rejets (TFR) correspondant au pourcentage de personnes rejetées par erreur.
- le Taux de Fausses Acceptations (TFA) correspondant au pourcentage de personnes qui ont été acceptées et qui n'auraient pas du l'être.

La relation liant TFA et TFR est illustrée sur la (Figure 1.5). On peut voir que plus le TFR est faible et plus le TFA est élevé et inversement. Ces deux éléments dépendent du réglage du seuil qui est le résultat d'un compromis selon le choix de l'application. Pour des applications de haute sécurité (accès au coffre fort de la banque centrale par exemple), on cherchera à limiter au maximum la possibilité d'intrusion, ce qui se traduit par un TFA faible. Au contraire, dans le cadre d'applications médicales, on ne pourra pas se permettre de rejeter une personne par erreur ce qui implique un TFR le plus faible possible[30].

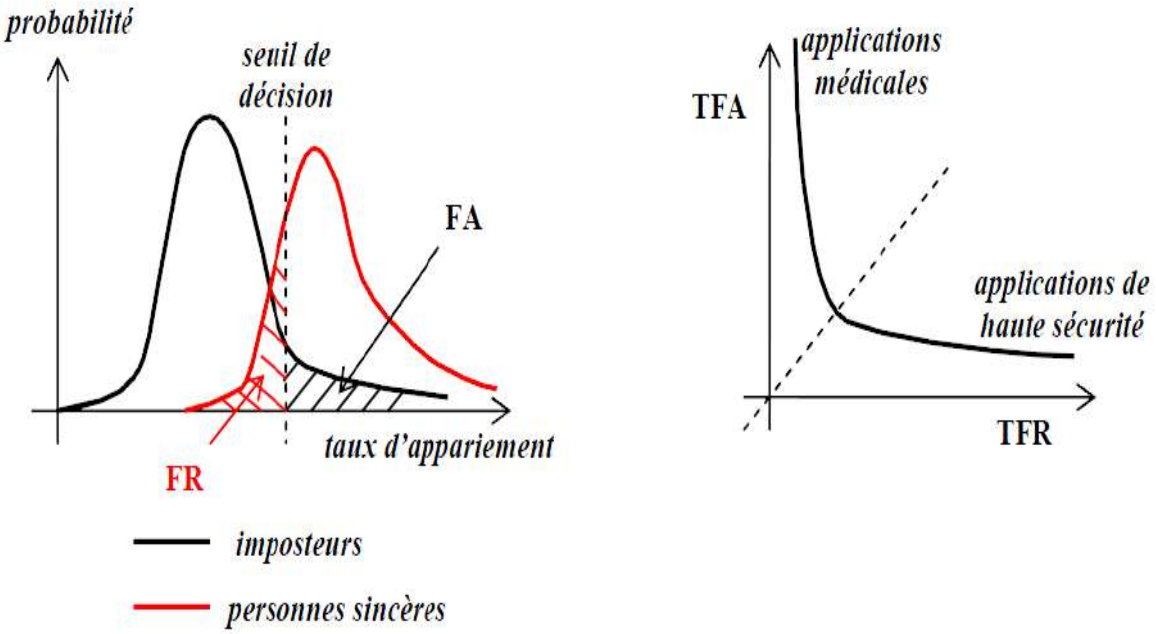


Figure (I.5) : graphes pour calculer les taux FAR et FRR

Les systèmes biométriques posent aussi des problèmes de sécurité car il n'est jamais vérifié que les données biométriques en entrée proviennent de leur réel possesseur. En effet les moyens de flouer un tel système existent, et de plus les caractères biométriques ne sont pas secrets. Il est relativement facile de se procurer une photo du visage, une empreinte digitale ou un enregistrement audio d'une personne. Une équipe japonaise a d'ailleurs montré que les systèmes actuels d'acquisition d'empreintes acceptent très bien une fausse empreinte créée à partir d'un moule en gélatine. Le problème vient de l'absence de vérification que la donnée entrée provient bien d un être vivant.

L'utilisation de la biométrie dans la vie de tous les jours pose également des problèmes de vie privée et de libertés. En France l'absence de législation spécifique sur les techniques biométriques peut poser problème et a fait l'objet d'un rapport parlementaire très détaillé. La commission Nationale de l'Informatique et des Libertés a d'ailleurs rendu un avis défavorable sur le stockage en masse de caractéristiques biométriques des personnes face aux risques de réutilisations abusives de ces données [30].

I.5 : Conclusion

De nos jours la biométrie est considérée comme moyen le plus sûr pour la sécurité. Elle est de plus en plus appliquée dans la réalité grâce à ses avantages. Ses applications sont diverses: applications de contrôle d'accès, applications dans les téléphone portables, application dans le commerce etc. ... Cependant la biométrie elle a aussi des limitations comme la précision des techniques biométriques est faible, on n'a pas encore d'habitude d'utiliser les systèmes biométriques

Dans cette étude nous avons déjà présenté une vue générale de la biométrie, un survol sur quelques techniques biométriques et nous avons présenté les détails techniques de techniques biométriques basé sur des empreintes digitales. Une étude de cas a été donnée pour montrer le fonctionnement des algorithmes présentés [3].

Chapitre I :

La biométrie

I.1 : Introduction.....3
I.1.1 : Identification d'empreinte digitale.....3
I.1.2 : Identification de visage.....3
I.1.3 : Identification d'iris.....4
I.1.4 : Identification de voix.....4
I.1.5 : Identification de Signature.....4
I.1.6 : Identification de main 5
I.2 : Historique 6
I.3 : Applications de la biométrie 8
I.4 : Système biométrique 9
I.4.1 : Vérification.....9
I.4.2 : Identification.....9
I.4.3 : Processus d'enregistrement.....9
I.4.4 : Processus d'identification /vérification.....10
I.4.5 : performances des systèmes biométriques 11
I.5 : Conclusion.....13

II.1 : Introduction

L'identification d'empreinte digitale est une de la biométrie la plus bien connue et la plus annoncée. En raison de leur unicité et uniformité avec le temps, des empreintes digitales ont été employées pour l'identification pendant plus d'un siècle, (c.-à-d. un biométrique) en raison automatisé devenant plus récemment des avancements dans des possibilités de calcul. L'identification d'empreinte digitale est populaire en raison de la facilité inhérente dans l'acquisition, les nombreuses sources (dix doigts) disponibles pour la collection, et leurs collections établies d'utiliser par police et immigration [32].

II.2 : Historique

Les premières traces d'utilisation d'empreintes digitales ont été découvertes en Egypte et datent de l'époque des pyramides il y a plus de 4000 ans. Les Chinois ont aussi utilisé très tôt ce moyen pour signer les documents officiels (le plus vieux document signé date du troisième siècle avant Jésus Christ) mais ils ne savaient sûrement pas que les empreintes étaient uniques pour chaque personne et permettaient ainsi une identification fiable. C'est en 1856 que l anglais William Herschel, après avoir utilisé les empreintes en guise de signature sur la population indienne qu il dirigeait, commença à comprendre que les empreintes étaient uniques et constantes dans le temps. En 1888 le britannique Francis Galton publia une étude sur les empreintes digitales où il établit leurs caractéristiques (unicité, invariance, minuties, classification) et en 1901 la technique d'identification au moyen des empreintes fut adoptée officiellement en Angleterre dans le système judiciaire. Cette technique fut ensuite largement développée dans les enquêtes criminelles et permit de résoudre un bon nombre d'affaires. De nos jours les empreintes sont toujours largement utilisées et reconnues comme méthode d'identification fiable [3].

II.3 : Caractéristiques d'une empreinte digitale

Une empreinte digitale est constituée d'un ensemble de lignes localement parallèles formant un motif unique pour chaque individu (Figure II.1), on distingue les stries (ou crêtes, ce sont les lignes en contact avec une surface au toucher) et les sillons (ce sont les creux entre deux stries). Les stries contiennent en leur centre un ensemble de pores régulièrement espacés.

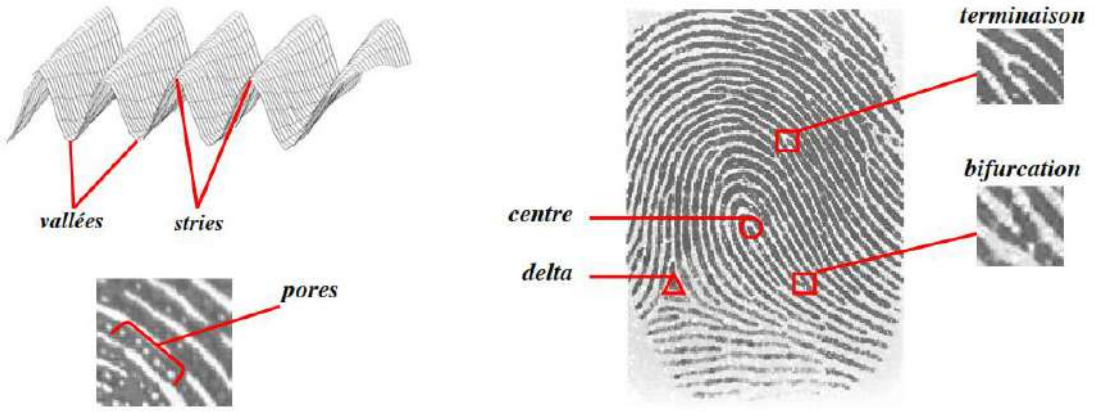
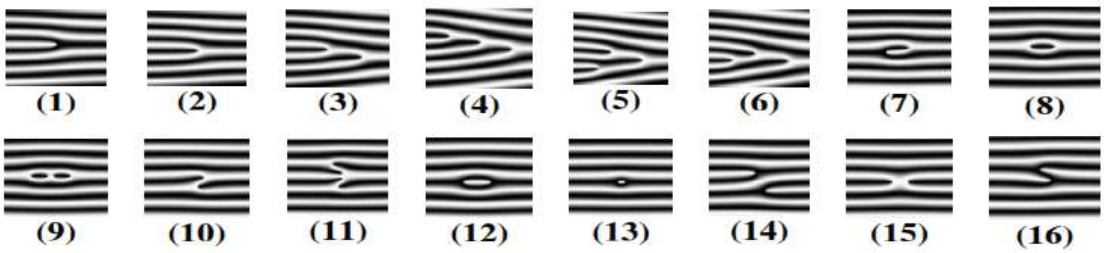


Figure (II .1) : Caractéristiques d'une empreinte digitale

Chaque empreinte possède un ensemble de points singuliers globaux (les centres et les deltas) et locaux (les minuties). Les centres correspondent à des lieux de convergences des stries tandis que les deltas correspondent à des lieux de divergence. Une étude (Figure II.2) a montré l'existence de seize types de minuties différentes mais en général les algorithmes ne s intéressent qu aux bifurcations et terminaisons qui permettent d obtenir les autres types par combinaison.



1.	terminaison	**9.**	boucle double
2.	bifurcation simple	**10.**	pont simple
3.	bifurcation double	**11.**	pont jumeau
4.	bifurcation triple I	**12.**	intervalle
5.	bifurcation triple II	**13.**	point isolé
6.	bifurcation triple III	**14.**	traversée
7.	crochet	**15.**	croisement
8.	boucle simple	**16.**	tête bêche

Figure (II.2) : Les différents types de minutie

La position et le nombre de centres et de deltas permettent de classifier les empreintes en catégorie selon leur motif général, on distingue principalement trois grandes familles (voir Figure II.3) :

- Les boucles (loop) représentent 65% des empreintes rencontrées.
- Les spires (whorl) représentent 30% des empreintes rencontrées.
- Les arches (arch) représentent 5% des empreintes rencontrées.

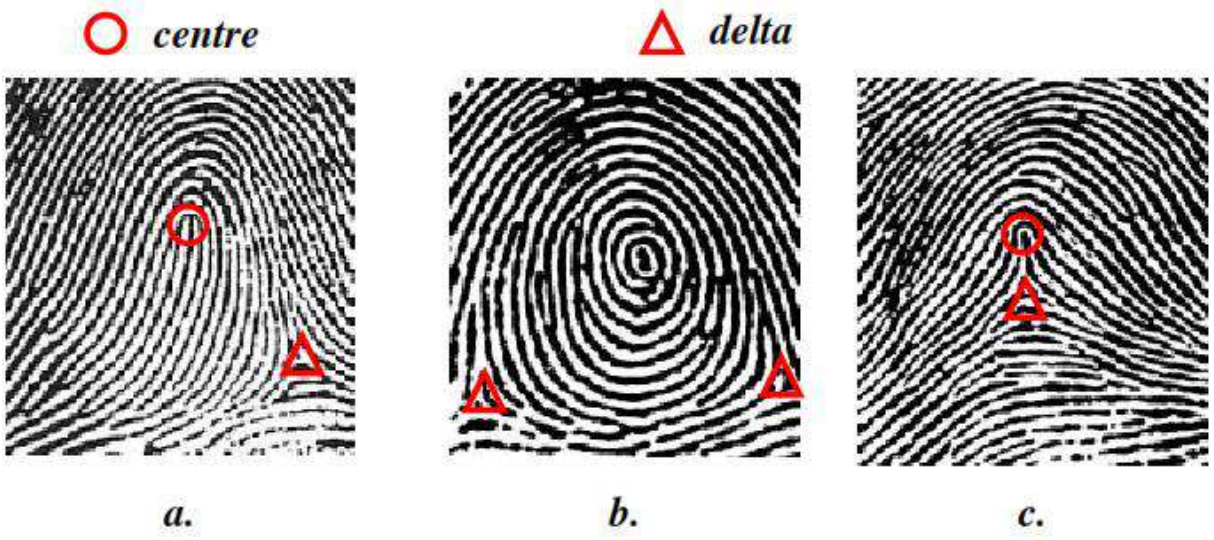


Figure (II.3) : Les trois principales classes d'empreintes, boucle (a), spire (b), arche (c)

L'ensemble formé par la disposition des points singuliers constitue un motif unique pour chaque individu, en effet il a été montré [28] que l'empreinte digitale se forme au cours du troisième mois de la vie fatale, le motif général est influencé par les gènes héréditaires mais l'apparition des détails (minuties) est créée de manière accidentelle par des pressions variables aléatoires sur les surfaces tactiles. Ainsi l'empreinte est unique pour tout individu, y compris pour des vrais jumeaux et il a été montré que les méthodes de reconnaissance actuelles permettent d'identifier efficacement les jumeaux [29] De plus les empreintes une fois formées ne changent plus au cours de la vie d'une personne, ces deux caractéristiques en font un moyen de reconnaissance très efficace [30].

II 4 : Les capteurs d'empreintes digitales

II.4.1 : Le capteur de pression

Le principe du capteur de pression réside dans le fait que lorsqu'un doigt est placé au-dessus de la zone du capteur, seuls les bosses de l'empreinte digitale rentrent en contact avec les rayons piezo du capteur. Les creux en contraste n'ont aucun contact avec les cellules du capteur. Une des différences fondamentales pour la reconnaissance et la comparaison d'empreinte digitale, par rapport aux capteurs sur le marché, demeure le capteur de pression qui génère une image binaire de 1 -bit. Une image de 1-bit contient moins d'information qu'une image de niveau de gris de 8-bit.

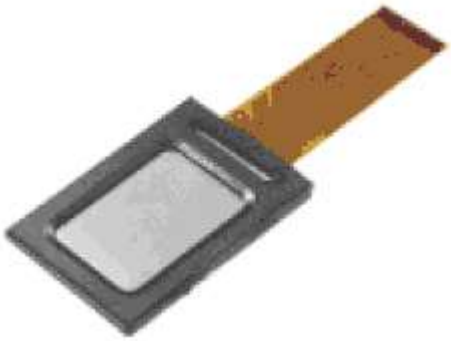


Figure (II.4) : BMF BLP100-Sensor

Un capteur de pression est capable d'enregistrer des doigts aussi bien humides que secs. De plus, sa large zone d'enregistrement permet de scanner complètement l'empreinte digitale ce qui amène à un faible taux d'erreur (EER = Equal-Error-Rate).

II.4.2 : Les capteurs optiques d'empreinte

La méthode optique est une des méthodes les plus communes. Un appareil-photo CCD (dispositif couplé chargé) est utilisé au coeur du capteur optique. Un appareil-photo CCD se compose simplement d'une rangée de diodes sensibles légères appelées photosites. En général, le doigt est placé sur une surface en verre et l'appareil-photo CCD prend la photo. Le système CCD contient une rangée de LED (diodes électroluminescentes) qui illumine les creux et les bosses du doigt. Un prix avantageux constitue l'avantage principal des systèmes optiques ; leur inconvénient est qu'ils sont faciles à détourner. L'autre problème est celui des empreintes latentes : l'empreinte digitale du doigt précédent, qui a été placé sur le capteur, peut rester. Les principaux fabricants de capteurs optiques sont Delsy, Dermalog, Smiths Heimann Biometrics.



Figure (II.5) : DESLEY CMOS-Sensor

II.4.3 : Les capteurs électriques-thermique

La méthode électrique-thermique est moins habituelle. Actuellement, le seul capteur thermique est le FingerChipâ fabriqué par Atmel.

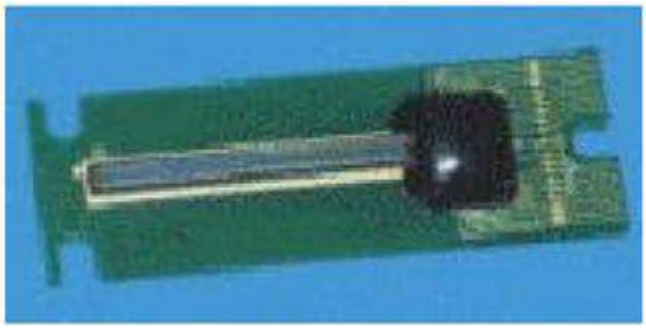


Figure (II.6) : Atmel FingerChipâ

La méthode unique du FingerChipâ, pour reconnaître l'empreinte, consiste à faire glisser le doigt le long du capteur. Les images successives ainsi capturées sont analysées par un logiciel spécial qui reconstruit l'image de l'empreinte digitale. Cette méthode permet au FingerChipâ de renvoyer une haute qualité, 500 dpi et 256 niveaux de gris.

Le capteur mesure le différentiel de température entre les creux de la peau et l'air capturé dans les bosses de l'empreinte digitale. Cette méthode donne une image d'excellente qualité même sur des empreintes de qualité médiocre telles que celles provenant de doigts secs avec peu de profondeur entre les creux et les bosses. La technologie thermique fonctionne également dans des conditions environnementales difficiles, comme lors de températures extrêmes, de taux d'humidité ou de poussière élevé, ou de contamination d'eau.

Cette méthode a également l'avantage de nettoyer le capteur, évitant ainsi que les empreintes digitales restent après le passage de chaque personne. En effet, les empreintes latentes peuvent poser des problèmes de lecture à chaque passage mais peuvent aussi être copiées et utilisées pour parvenir aux accès contrôlés. En fait, cette méthode, s'appuyant sur la technologie thermique, permet au FingerChipâ d'être un des plus résistants par rapport aux autres technologies. Le FingerChipâ fonctionne aussi dans des environnements où la température peut être basse et le taux d'humidité élevé.

L'avantage de cette technologie est donc la possibilité d'avoir une image bonne qualité et un capteur toujours propre. L'inconvénient est que la qualité de l'image dépend des compétences de l'utilisateur à savoir manipuler le capteur. Le deuxième inconvénient est le chauffage du capteur qui augmente la consommation électrique. La chaleur du capteur est nécessaire afin d'éviter un équilibre thermique entre le capteur et la surface du doigt.

II.4.4 : Capteurs capacitifs

La méthode capacitive est une des méthodes les plus populaires. Comme les autres capteurs, le capteur capacitif d'empreinte digitale reproduit l'image des creux et des bosses qui composent une empreinte digitale. Le capteur capacitif emploie des condensateurs de courant électrique pour mesurer l'empreinte digitale. Un capteur capacitif se compose d'une rangée de cellules minuscules. Chaque cellule inclut deux plaques conductrices recouvertes par un revêtement protecteur.

L'avantage principal des capteurs capacitifs est qu'ils demandent une réelle empreinte digitale. Mais ils rencontrent des difficultés avec les doigts secs et humides. Des doigts humides rendent l'image noire, tandis que des doigts secs la rendent pâle.

Les principaux fabricants de capteurs capacitifs sont Infligeons, Veridicom, Sony et ST Microelectronics.



Figure (II.7) : Veridicom 5th sense

II.4.5 : Capteurs de champ-électrique

Le capteur de champ-électrique fonctionne avec un champ-électrique et le mesure au delà de la couche extérieure de la peau où l'empreinte digitale commence. La technologie de champ-électrique peut être utilisée dans des conditions extrêmes, c'est-à-dire même si le doigt est sale ou sec.



Figure (II.8) : Authentec ASE4000

La technologie de champ-électrique crée un champ entre le doigt et le semi-conducteur adjacent qui imite la forme des creux et des bosses de la couche épidermique du doigt. Un amplificateur de sous-Pixel est utilisé pour mesurer les signaux. Les capteurs fonctionnent ensemble afin de rendre une image plus claire correspondant exactement au modèle de l'empreinte digitale. On parvient ainsi à une image plus claire que ce que peuvent donner les technologies optiques ou capacitives. Cela permet à la technologie de champ électrique d'obtenir des images d'empreinte digitale que d'autres technologies ne parviendraient pas à avoir.

Dans la technologie de champ-électrique, les rangées d'antenne mesurent la surface de la peau en générant et en détectant les formes linéaires géométriques. La couche vivante des cellules de la peau commence sous la surface de la peau.

Cela est contraire aux géométries sphériques ou tubulaires de champ produit par le capteur capacitif simple, qui lit seulement la surface supérieure de la peau. En conséquence, des doigts, qui seraient difficiles ou impossibles à scanner par des capteurs capacitifs, le seraient avec succès grâce à la technologie de champ-électrique.



Figure (II.9) : Authentec AES2500

Dans les prochains mois, une version de la technologie de champ électrique mettra sur le marché un nouveau capteur dont la capture de l'image se fera par balayage du doigt sur le capteur [19].

II.5 : Méthode d'extraction de reconnaissance de l'empreinte digitale

Il n'est pas question ici de rentrer en détail dans l'explication des algorithmes utilisés pour l'extraction et l'appariement des empreintes digitales mais plutôt de présenter brièvement leur fonctionnement à titre purement informatif.

II.5.1 : Extraction de la signature

Lors de l'extraction de la signature propre à l'empreinte digitale, le principal problème rencontré est relatif à la qualité de l'image issue du capteur. En effet l'extraction de la signature s'appuie sur une approche basée sur le repérage des minuties, qui s'avère être extrêmement sensible au bruit et aux éventuelles déformations. Les perturbations peuvent aisément laisser apparaître de fausses minuties ou au contraire en masquer certaines. C'est pourquoi un filtrage de l'image de l'empreinte digitale sera toujours effectué avant toute autre opération algorithmique.

Le filtrage de l'image pourra se dérouler suivant différentes méthodes plus ou moins coûteuses en temps de calcul. Un filtre gaussien peut être appliqué afin de réduire le niveau général de bruit mais, la plupart du temps, un filtrage directionnel s'appuyant sur des paramètres locaux ou des transformées de Fourier rapides (FFT) est préférable. Notons que dans le but d'accentuer les contours des stries, les filtres de type Laplacien donnent de très bons résultats.

Une fois améliorée, l'image est généralement binarisée (suivant un seuillage adaptif) avant d'être squelettisée de sorte que les stries ne soient représentées que par des lignes ayant un pixel de largeur. Une fois cette transformation effectuée, le repérage des bifurcations ou des points d'arrêt révélant une minutie est relativement aisée.

La signature proprement dite de l'empreinte digitale peut alors être extraite en relevant les coordonnées des points de minutie, leur type (bifurcation ou terminaison) ainsi que la direction locale des stries associées. Cette signature peut être rendue plus précise en effectuant un échantillonnage de la strie associée aux minuties détectées. La Figure suivante illustre la suite de transformations effectuées sur l'image de l'empreinte digitale afin d'extraire la signature.

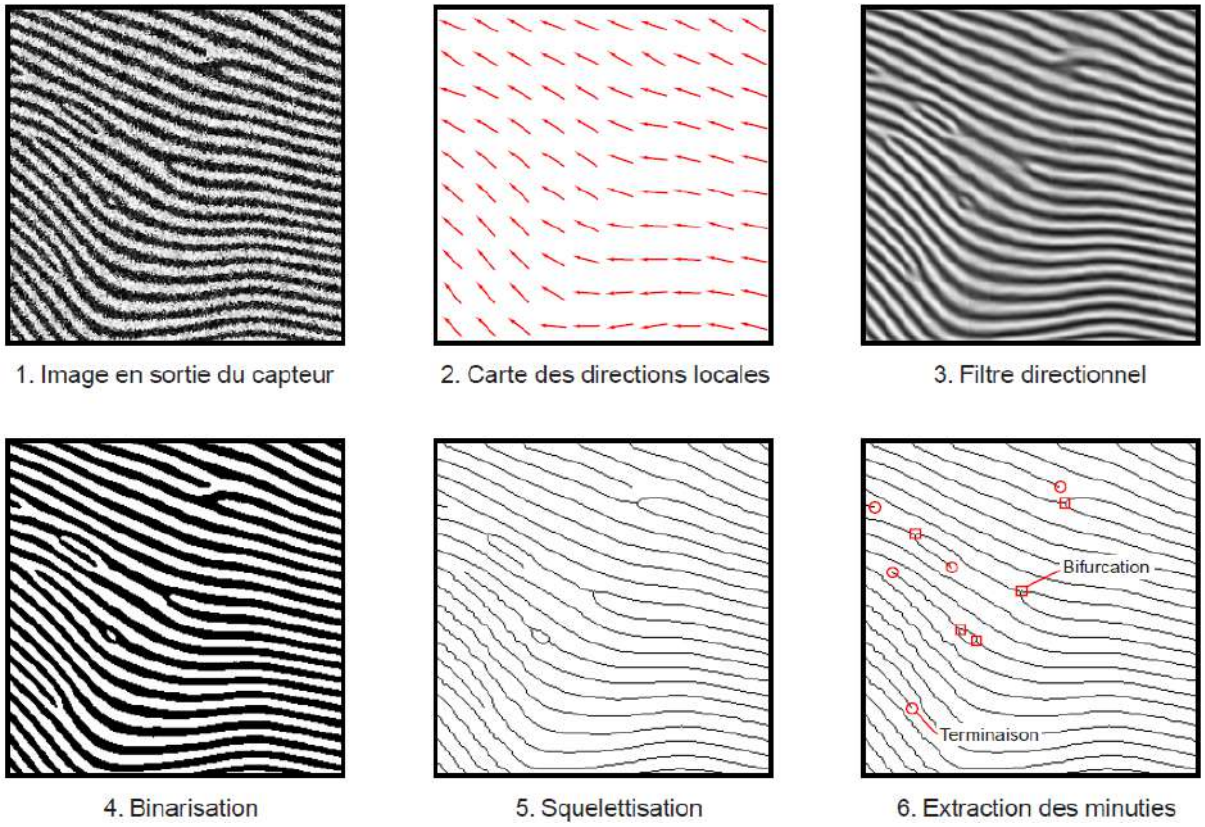


Figure (II.10) :

Transformations subies par l'image de l'empreinte digitale afin d'extraire la signature

II.5.2 : Reconnaissance de l'empreinte digitale

L'appariement consiste à comparer la signature de l'empreinte digitale de l'utilisateur à une ou plusieurs autres présentes dans une banque de données dans le but de l'identifier (utilisation mono ou pluri utilisateurs).

Notons que le résultat d'une phase d'appariement ne sera jamais une réponse formelle, la même empreinte n'aboutissant jamais exactement à la même signature. En fait le résultat de l'appariement sera toujours un indice de confiance compris entre zéro pour deux empreintes totalement différentes et un pour deux images absolument identiques.

Avant tout, l'image d'entrée (codée sous forme de signature) subit une suite d'opérations géométriques (homothéties et rotations) afin que les coordonnées de certaines minuties prises comme points de référence coïncidente avec celles codées au sein de la signature candidatent. Cette démarche permet de s'affranchir des éventuelles déformations qu'aurait pu subir l'empreinte lors de son acquisition par le capteur (rotation du doigt, vitesse de passage différente …). Une fois ces opérations effectuées, toutes les minuties sont comparées d'une

part sur leur position relative mais également sur leur type et leurs stries associées. Cette comparaison permet alors de déterminer un indice de confiance permettant de conclure sur l'identité de l'usager.

Les performances globales d'un système de reconnaissance d'empreintes digitales sont caractérisées par deux données qui sont le taux de fausses acceptations et le taux de faux rejets. La première est proportionnelle à la probabilité pour qu'une personne étrangère au système soit acceptée et la seconde, à la probabilité pour qu'une personne normalement admise soit rejetée.

Notons, à titre informatif, que selon avec la législation française, deux empreintes digitales sont considérées comme identiques lorsqu' un nombre minimum de douze points de minutie correspondent [30].

II.6 : Conclusion

Dans ce chapitre nous avons vu l'émergence des méthodes biométriques de reconnaissance et des problèmes qui en découlent. Les caractéristiques des empreintes digitales ainsi que la structure globale d'un système de reconnaissance d'empreintes ont également été décrit; il s'agit à l'heure actuelle de la technique biométrique la plus aboutie. Dans la suite de ce mémoire nous nous intéresserons à un système complet de *vérification* d'empreintes digitales basé sur l'extraction des minuties [30].

Chapitre I I :

L’empreinte digitale

II.1 : Introduction.....14
II.2 : Historique 14
II.3 : Caractéristiques d’une empreinte digitale.....15
II 4 : Les capteurs d’empreintes digitales.....17
II.4.1 : Le capteur de pression.....17
II.4.2 : Les capteurs optiques d'empreinte.....18
II.4.3 : Les capteurs électriques-thermique 18
II.4.4 : Capteurs capacitifs.....19
II.4.5 : Capteurs de champ-électrique.....20
II.5 : Méthode d’extraction de reconnaissance de l’empreinte digitale.....22
II.5.1 : Extraction de la signature.....22
II.5.2 : Reconnaissance de l’empreinte digitale.....23
II.6 : Conclusion.....24

Chapitre I I I :

Bases théoriques

III.1 : Introduction.....25
III.1.1 : Ce qui est identification d'empreinte digitale ?.....25
III.1.2 : Deux approches pour l'identification d'empreinte digitale ……26
III.2 : Conception de système…….....26
III.2.1 : conception au niveau système…….26
III.2.2 : Conception de niveau d'algorithme…….……...….27
III.3 : Prétraitement d'image d'empreinte digitales……...….……...28
III.3.1 : Perfectionnement d'image d'empreinte digitale……..28
III.3.1.1 : Égalisation d'histogramme ……..……...28
III.3.1.2 : Transformée de Fourier Rapide…….…….…..29
III.3.2 : Binarisation d'empreinte digitale…….30
III.3.3 : Segmentation d'image d'empreinte digitale…….31
III.4 : Extraction De Minutie…….33
III.4.1 : Éclaircissement d'empreinte digitale……..33
III.4.2 : Inscription de minutie……..33
III.5 : Traitement de minutie…….34
III.5.1 : Déplacement faux de minutie……..34
III.5.2 : Unifier les arrêts et les bifurcations ……35
III.6 : Vérification De Minutie……..……36
III.7 : Conclusion…….37

III.1 : Introduction

III.1.1 : Ce qui est identification d'empreinte digitale ?

Le problème d'identification d'empreinte digitale peut être groupé dans deux domaines secondaire : la vérification d'empreinte digitale et l'autre est identification d'empreinte digitale (le schéma suivant). En outre, différent de l'approche manuelle pour l'identification d'empreinte digitale par des experts, l'identification d'empreinte digitale ici est référé comme AFRS (système d'identification automatique d'empreinte digitale).

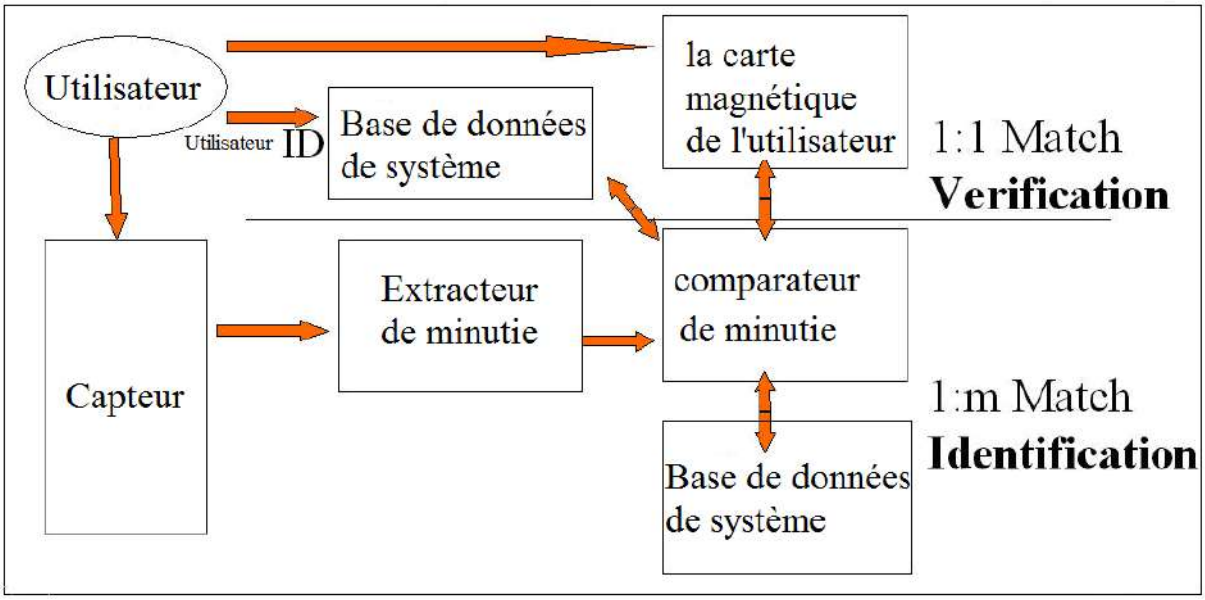


Figure (III.1) : Vérification vs Identification

La vérification d'empreinte digitale est de vérifier l'authenticité d'une personne par son empreinte digitale. L'utilisateur fournit son empreinte digitale ainsi que son information d'identité comme son numéro d'identité. Le système de vérification d'empreinte digitale recherche le calibre d'empreinte digitale selon le numéro d'identité. Et assortit le calibre avec l'empreinte digitale acquise en temps réel de l'utilisateur.

L'identification d'empreinte digitale est de spécifier une identité de la personne par ses empreintes digitales. Sans connaissance de l'identité de la personne, le système d'identification d'empreinte digitale essaye pour assortir ses empreintes digitales avec ceux dans la base de données entière d'empreinte digitale. Il est particulièrement utile pour des cas d'enquête criminelle.

Cependant, tous les problèmes d'identification d'empreinte digitale, vérification ou identification, sont finalement basés sur une représentation bien définie d'une empreinte digitale. Tant que la représentation des empreintes digitales demeure l'unicité et garde simple, l'empreinte digitale s'assortissant, pour le 1er cas de la vérification à-1 et le 2em cas d'identification à-m.

III.1.2 : Deux approches pour l'identification d'empreinte digitale

Deux formes de représentation pour des empreintes digitales séparent les deux approches pour l'identification d'empreinte digitale.

1- La première approche, basée sur minutie, représente l'empreinte digitale par ses dispositifs locaux, comme des arrêts et des bifurcations. Cette approche a été intensivement étudiée, est également l'épine dorsale des produits disponibles courants d'identification d'empreinte digitale.

2- La deuxième approche, qui emploie les méthodes basées sur l'image, essaye de faire l'assortiment basé sur les dispositifs globaux d'une image entière d'empreinte digitale. C'est une méthode avancée et nouvellement naissante pour l'identification d'empreinte digitale. Et il est utile de résoudre quelques problèmes insurmontables de la première approche.

III.2 : Conception de système

III.2.1 : conception au niveau système

Un système d'identification d'empreinte digitale constitue de l'empreinte digitale acquérant le dispositif, l'extracteur de minutie et le comparateur de minutie.

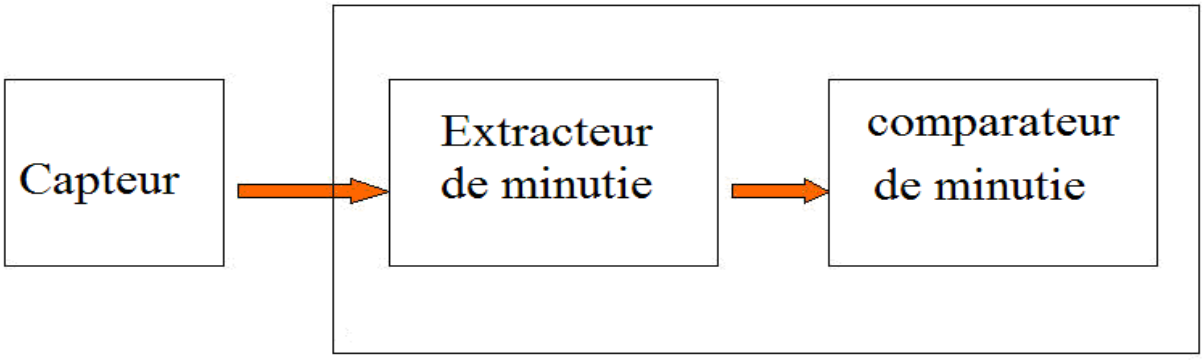


Figure (III.2) : Système d'identification simplifié d'empreinte digitale

Pour l'acquisition d'empreinte digitale, les capteurs optique ou semi-conducteur sont employés couramment. Elles ont le rendement élevé et l'exactitude acceptable excepté quelques cas que

le doigt de l'utilisateur est trop sale ou sec. Cependant, la base de données d'essai pour notre projet est des empreintes digitales disponibles fournies par FVC2002 (concurrence 2002 de vérification d'empreinte digitale) [33]. Tellement aucune étape d'acquisition n'est mise en application.

L'extracteur de minutie et les modules de comparateur de minutie sont expliqués en détail dans la prochaine pièce pour la conception d'algorithme et d'autres sections suivantes.

III.2.2 : Conception de niveau d'algorithme

Pour mettre en application un extracteur de minutie, une approche à trois étages est employée couramment par des chercheurs. Ils pré traitent, les extractions de minutie et l'étape de post-traitement.

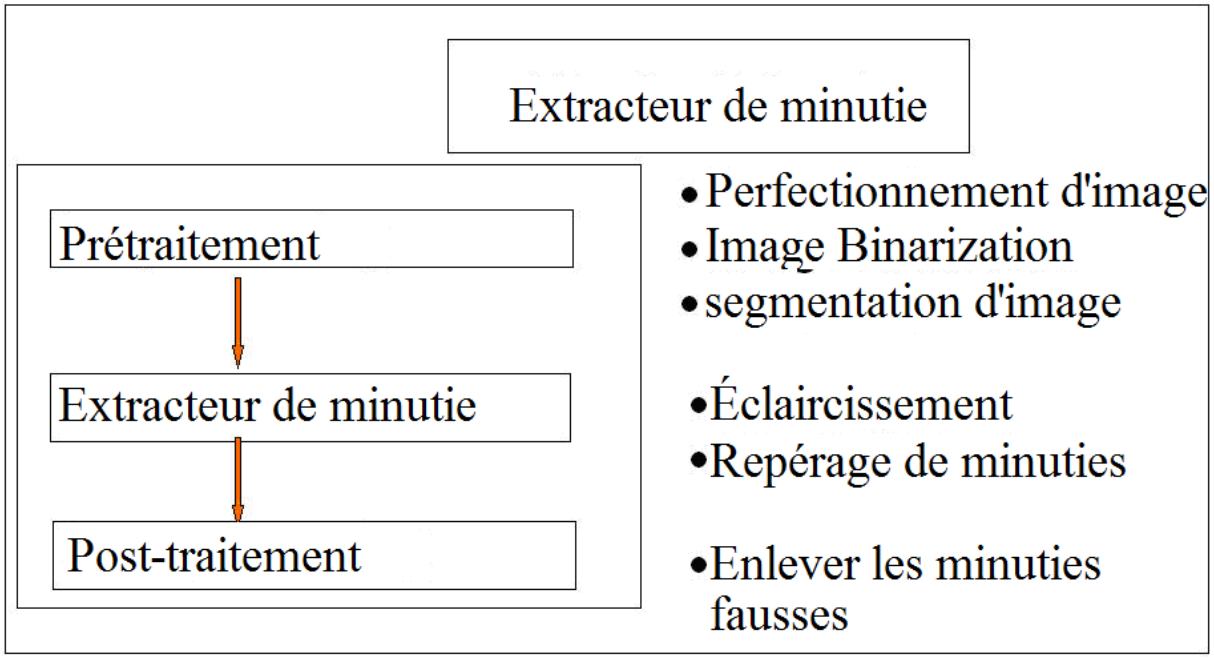


Figure (III.3) : Extracteur de minutie

Pour l'étape de prétraitement d'image d'empreinte digitale, nous employons l'égalisation et la transformée de Fourier d'histogramme pour faire le perfectionnement d'image. Et alors l'image d'empreinte digitale binarisée suivre la méthode localement adaptative de seuil. La tâche de segmentation d'image est accomplie par une approche en trois étapes : bloquer l'évaluation de direction, la segmentation par l'intensité de direction et la région de l'extraction d'intérêt par des opérations morphologiques. La plupart des méthodes employées dans l'étape de prétraitement sont développées par d'autres chercheurs mais elles forment une combinaison toute neuve dans notre projet par d'essai et l'erreur. Également les opérations morphologiques

pour le ROI d'extraction sont présentées pour relever les empreintes digitales de la segmentation d'image.

Pour l'étape d'extraction de minutie, trois algorithmes d'éclaircissement sont examinés et l'opération d'éclaircissement morphologique est finalement offerts dehors avec le rendement élevé. L'inscription de minutie est une tâche simple comme la plupart des littératures ont rapporté mais un cas spécial est trouvé pendant notre exécution et un mécanisme additionnel de contrôle est imposé pour éviter un tel genre d'inadvertance.

Pour l'étape de post-traitement, un algorithme plus rigoureux est développé pour enlever la minutie fausse basée dessus. Également on propose une représentation originale pour des bifurcations pour unifier des arrêts et des bifurcations.

Le comparateur de minutie choisit n'importe quelle minutie deux comme une paire de minutie de référence et puis assortit leurs arêtes associées d'abord. Si les arêtes s'assortissent bien, deux images d'empreinte digitale sont alignées et l'assortiment est conduit pour toute la minutie restante.

III.3 : Prétraitement d'image d'empreinte digitales

III.3.1 : Perfectionnement d'image d'empreinte digitale

Le perfectionnement d'image d'empreinte digitale est de faire le clairifiant d'image pour d'autres opérations faciles. Depuis les images d'empreinte digitale acquises des capteurs ou d'autres médias ne sont pas assurés avec la qualité parfaite, ces méthodes de perfectionnement, pour augmenter le contraste entre les arêtes et les sillons et pour relier les points d'arrêt faux des arêtes dues à la quantité insuffisante d'encre, sont très utiles pour la subsistance par exactitude plus élevée pour relever les empreintes digitales de l'identification.

Deux méthodes sont adoptées dans notre système d'identification d'empreinte digitale : le premier est égalisation d'histogramme ; le prochain est transformé de Fourier.

III.3.1.1 : Égalisation d'histogramme

L'égalisation d'histogramme est d'augmenter la distribution de valeur de Pixel d'une image afin d'augmenter l'information de perception.

Le côté droit de la figure suivante (Figure III.4) est le rendement après l'égalisation d'histogramme.



Figure (III.4) : perfectionnement d'histogramme.
Image originale (gauche). Image augmentée (droite)

III.3.1.2 : Transformée de Fourier Rapide

Nous divisons l'image en petits blocs de traitement (32 par 32 Pixel) et exécutons la transformée de Fourier selon :

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \times \exp\left\{-j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \quad \text{……(1)}$$

Pour u = 0, 1, 2,…, 31 et v = 0, 1, 2,…, 31.

Afin d'augmenter un bloc spécifique par ses fréquences dominantes, nous multiplions le FFT du bloc par sa grandeur un ensemble de périodes. Là où l'importance de l'original

FFT = abs (F (u, v)) = |F (u, v)|.

Obtenir le bloc augmenté selon

$$g(x,y) = F^{-1}\left\{F(u,v) \times \left|F(u,v)\right|^{K}\right\} \quad \text{……...(2)}$$

Là où F-1 (F (u, v)) est fait par :

$$f(x,y) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} F(u,v) \times \exp\left\{j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \quad \text{……(3)}$$

Pour x = 0, 1, 2, ..., 31 et y = 0, 1, 2, ..., 31.

Le k dans la formule (2) est une constante expérimentalement déterminée, que nous choisissons k=0.45 pour calculer. Tandis qu'avoir un « k » plus élevé améliore l'aspect des arêtes, remplir vers le haut de petits trous dans les arêtes, ayant un « k » trop élevé peut avoir

comme conséquence la jointure fausse des arêtes. Ainsi un arrêt pourrait devenir une bifurcation. (La Figure III.5) présente l'image après perfectionnement de FFT.



Figure (III.5) : Perfectionnement d'empreinte digitale par FFT
Image augmentée (gauche), image originale (droite)

L'image augmentée après que FFT ait les améliorations pour relier quelques faussement points d'arrêt sur des arêtes et pour enlever quelques faux raccordements entre les arêtes. L'image montrée à gauche de la (Figure III.5) est également traitée avec l'égalisation d'histogramme après que les FFT transforment. L'effet secondaire de chaque bloc est évident mais il n'a aucun mal aux opérations supplémentaires parce que nous trouvons l'image après que l'opération consécutive de binarisation soit assez bonne tant que l'effet secondaire n'est pas trop grave.

III.3.2 : Binarisation d'empreinte digitale

La Binarisation d'empreinte digitale est de transformer l'image grise à 8 bits d'empreinte digitale à une 1 image de bit avec 0 valeurs pour des arêtes et 1 valeur pour des sillons. Après l'opération, des arêtes dans l'empreinte digitale sont accentuées avec la couleur noire tandis que les sillons sont blancs.

Une méthode localement adaptative de binarisation est exécutée pour binariser l'image d'empreinte digitale. Une méthode si appelée vient du mécanisme de transformer une valeur

de Pixel à 1 si la valeur est plus grande que la valeur moyenne d'intensité du bloc courant (16x16) auquel le Pixel appartient (Figure III.6)



Figure (III.6) : l'image d'empreinte digitale après binarisation (gauche), Image grise augmentée (droite)

III.3.3 : Segmentation d'image d'empreinte digitale

Généralement seulement une région d'intérêt (ROI) est utile pour être reconnue pour chaque image d'empreinte digitale. Le secteur d'image sans arêtes et sillons efficaces est d'abord jeté puisqu'il tient seulement l'information de fond. Alors la limite du secteur efficace restant est esquissée dehors puisque la minutie dans la région attachée sont embrouillant avec ces fausse minutie qui sont produits quand les arêtes sont hors du capteur.

Pour extraire le ROI, une méthode en deux étapes est employée. La première étape est contrôle de variété d'évaluation de direction de bloc et de direction, alors que la seconde est intriguée de quelques méthodes morphologiques.

1 : Block direction estimation

La carte de direction est montrée dans le diagramme suivant. Nous supposons qu'il y a seulement une empreinte digitale dans chaque image.

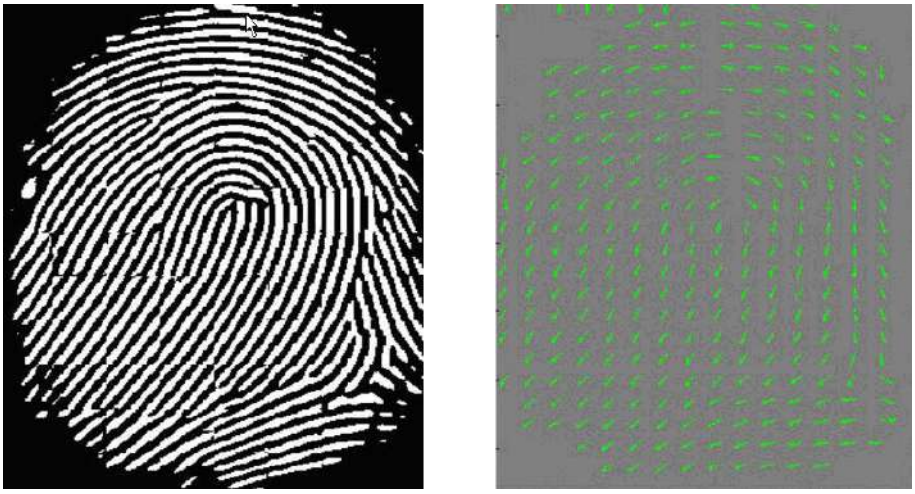


Figure (III.7) : Carte de direction.

Empreinte digitale binarisée (gauche), carte de direction (droite)

2 : Extraction de ROI par des opérations morphologiques

Deux opérations morphologiques appelées `OPEN' et le `CLOSE' sont adoptées :

L'opération `OPEN' peut augmenter des images et enlever des crêtes présentées par bruit de fond (Figure **III.9**).

L'opération `CLOSE' peut rétrécir des images et éliminer de petites cavités (figure **III.10**).

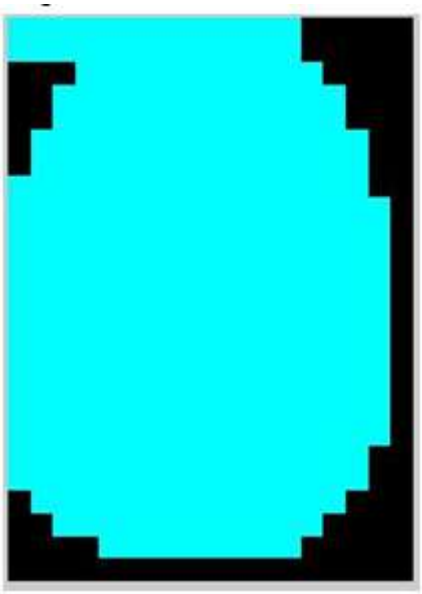


Figure (III.8) : Région originale d'image

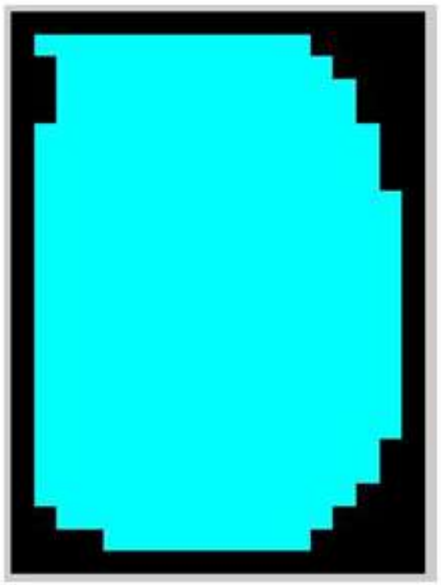


Figure (III.9) : Après opération OPEN

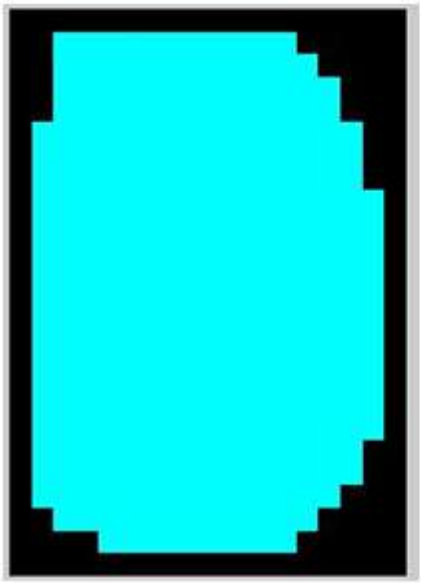


Figure (III.10) : Après opération CLOSE

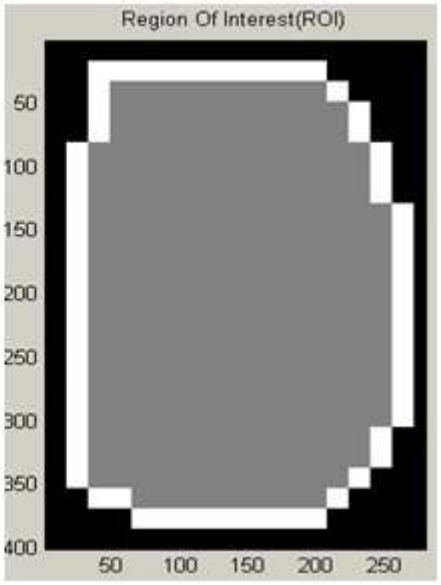


Figure (III.11) : ROI + Bound

Ces quatre figures montrent le secteur d'image d'empreinte digitale d'intérêt et sa limite. La limite est la soustraction du secteur fermé du secteur ouvert. Alors l'algorithme gâche ces extrêmes gauches, extrême droite, en-dessus hors de l'attaché afin d'obtenir la région étroitement liée contenant juste le secteur attaché et intérieur.

III.4 : Extraction de minutie

III.4.1 : Éclaircissement d'empreinte digitale

L'éclaircissement est d'éliminer les Pixel superflus des arêtes jusqu'à ce que les arêtes soient juste un Pixel au loin. Emploie un algorithme d'éclaircissement itératif et parallèle. Dans chaque balayage de la pleine image d'empreinte digitale, l'algorithme marque en bas des Pixel superflus dans chaque petite fenêtre d'image (3x3). Et enlève finalement tous ces Pixel marqués après plusieurs balayages.

III.4.2 : Inscription de minutie

Après l'arête d'empreinte digitale amincissant, marquant la minutie des points est relativement facile. Mais ce n'est toujours pas une tâche insignifiante car la plupart des littératures avoués parce qu'au moins un cas spécial évoque une attention pendant l'étape d'inscription de minutie.

III.5 : Traitement de minutie

III.5.1 : Déplacement faux de minutie

L'étape de prétraitement ne guérit pas totalement l'image d'empreinte digitale. Par exemple, on n'élimine pas totalement des coupures fausses d'arête dues à la quantité insuffisante de croix raccordements d'encre et d'arête dus à l'encrage fini. En fait toutes les parties elles-mêmes présentent de temps en temps quelques objets façonnés qui mènent plus tard à la fausse minutie. Ces minuties fausses affecteront de manière significative l'exactitude de l'assortiment s'ils sont simplement considérés comme la minutie véritable. Tellement quelques mécanismes d'enlever la minutie fausse sont essentiels pour maintenir le système de vérification d'empreinte digitale efficace.

Sept types de minutie fausse sont spécifiés dans les diagrammes suivants :

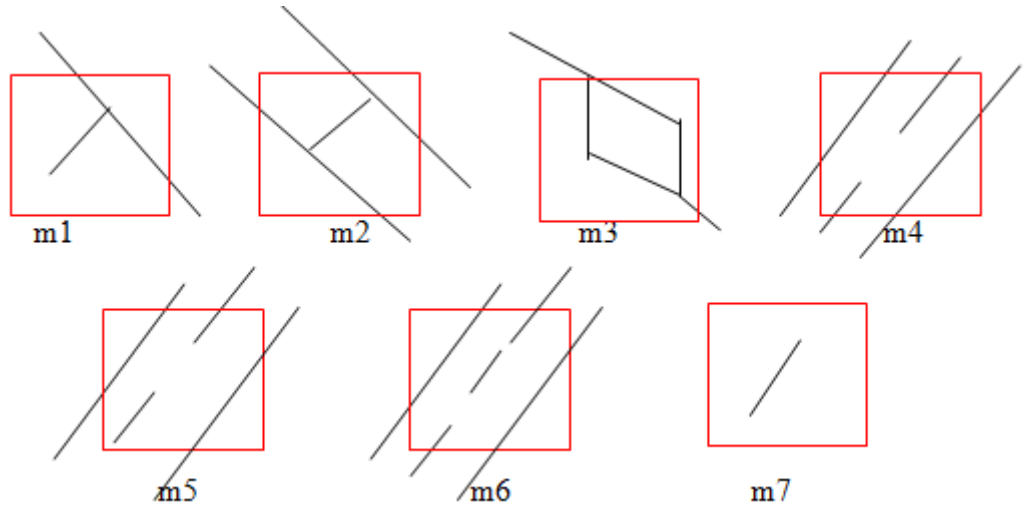


Figure (III.12) : Structures fausses de minutie. m1 est une perforation de transitoire dans une vallée. Dans le cas de m2 une transitoire relie faussement deux arêtes. Le m3 a deux bifurcations proches situées dans la même arête. Les deux points d'arrêt d'arête dans le cas m4 ont presque la même orientation et une distance courte. m5 est semblable le cas m4 excepté qu'une part de l'arête cassée est si courte qu'un autre arrêt soit produit. m6 prolonge le cas m4 mais avec la propriété supplémentaire qu'une troisième arête est trouvée au milieu des deux parties de l'arête cassée. m7 a seulement une arête courte trouvée dans la fenêtre de seuil.

Les procédures en enlevant la minutie fausse sont :

1. Si la distance entre une bifurcation et un arrêt est moins que D et la minutie deux sont dans la même arête (cas m1). Enlever les deux. Là où D est la largeur moyenne d'inter-arête représentant le moyen distancer entre deux arêtes voisines parallèles.
2. Si la distance entre deux bifurcations est moins que D et elles sont dans la même arête, enlever les deux bifurcations. (Cas m2, m3).
3. Si deux arrêts sont sur une distance D et leurs directions sont coïncidentes avec une variation sous petit angle. Et elles suffisent la condition qu'aucun n'importe quel autre arrêt n'est situé entre les deux arrêts. Alors les deux arrêts sont considérés comme la minutie fausse dérivée d'une arête cassée et sont enlevés. (Cas m4, m5, m6).
4. Si deux arrêts sont situés dans une arête courte avec la longueur moins que D, enlever les deux arrêts (m7).

Les procédures en enlevant la minutie fausse ont deux avantages. On est que l'identification d'arête est employée pour distinguer la minutie et les sept types de minutie fausse sont rivalisé strictement défini avec ceux lâchement définie par d'autres méthodes. Le deuxième avantage est que l'ordre des méthodes de dépose est longuement mûri pour réduire la complexité de calcul. Il surpasse la manière dont adoptée par n'utilisent pas les relations parmi les types faux de minutie. Par exemple, le procedure3 résout les cas m4, m5 et m6 dans une routine simple de contrôle. Et après le procédé 3, le nombre de minutie fausse satisfaisant le cas m7 est sensiblement réduit.

III.5.2 : Unifier les arrêts et les bifurcations

Puisque les diverses conditions par acquisition de données telles que la pression d'impression peuvent facilement changer un type de minutie en autre, la plupart des chercheurs adoptent la représentation d'unification pour l'arrêt et la bifurcation

III.6 : Comparaison De Minutie

Un algorithme de comparaison basé par alignement partiellement dérivé du [34] est employé dans notre projet. Il inclut deux étapes consécutives : on est étape d'alignement et la seconde est étape d'allumette.

1. Étape d'alignement. Donné deux images d'empreinte digitale à assortir, choisir n'importe quelle une minutie de chaque image, calculent la similitude des deux arêtes liées aux deux points référencés de minutie. Si la similitude est plus grande qu'un seuil, transformer chaque ensemble de minutie à un nouveau système de coordination dont l'origine est au point référencé et dont l'axe des abscisses est coïncident avec la direction du point référencé.
2. Étape de comparaison : Après que nous obtenions l'ensemble deux de points transformés de minutie, nous employons un algorithme pour compter les paires assorties de minutie en assumant la minutie deux ayant presque la même position et la direction sont identique.

III.7 : Conclusion

- Technologie totalement mature
- En authentification privée, mise en oeuvre facile et peu coûteuse
- En reconnaissance ou authentification publique : encore mal acceptée (double usage criminel et civil)

Chapitre I V :

Implémentation et Résultats

IV.1 : Introduction……..…….……38
IV.2 : Base de données d'empreinte digitale utilisée…….……39
IV.3 : Implémentation et Résultats…….……..40
IV.3.1 : Introduire la commande **start_gui_single_mode** dans MATLAB R2011a.....40
IV.3.2 : le bouton **Load** 41
IV.3.3 : le bouton **his-Equalization** 42
IV.3.4 : le bouton **fft** 43
IV.3.5 : le bouton **Binarization** ……..…..44
IV.3.6 : le bouton **Direction** …….....44
IV.3.7 : le bouton **ROI Area** 45
IV.3.8 : le bouton **Thinning**…….….46
IV.3.9 : le bouton **Remove H breaks** 46
IV.3.10 : le bouton **Remove spikes** 46
IV.3.11 : le bouton **Extract** ……..…….47
IV.3.12 : le bouton **Real Minutia** …….....47
IV.3.13 : le bouton **Save** 48
IV.3.14 : le bouton **One To One** (Vérification) ……...……49
IV.3.15 : le bouton **One To m** (Identification).....50
IV.3.16 : **Performance de logiciel** ……...……51
IV.4 : Conclusion.....53

IV.1 : Introduction

Notre projet est d'étudier les techniques courantes pour l'identification d'empreinte digitale. Cette cible peut être principalement décomposée en prétraitement d'image, extraction de dispositif et vérification de dispositif. Chaque tâche secondaire, quelques méthodes classiques et à jour dans les littératures sont analysées. Basé sur l'analyse, une solution intégrée pour l'identification d'empreinte digitale est développée pour la démonstration.

Notre programme de démonstration est codé par MATLAB. Pour le programme, on propose de l'optimisation au niveau de codage et le niveau d'algorithme pour améliorer l'exécution de notre système d'identification d'empreinte digitale. Ces perfectionnements d'exécution sont montrés par des expériences entreprises sur une série d'images d'empreinte digitale. En outre, les expériences illustrent les questions clés de l'identification d'empreinte digitale qui sont compatibles à ce que les littératures disponibles indiquent.

IV.2 : Base de données d'empreinte digitale utilisée

Afin d'examiner la validité de notre exécution, nous avons employé la base de données d'image de l'empreinte digitale FVC2002. FVC2002 était la deuxième compétition internationale pour des algorithmes de vérification d'empreinte digitale et nous avons acquis la base de données qui a été fournie aux participants de cette concurrence. Les images utilisées étaient des images en ligne d'une qualité raisonnablement bonne. Les majeures parties de la plupart des images d'empreinte digitale étaient récupérables et n'ont pas produit trop de fausses minuties après perfectionnement et l'éclaircissement.

Les détails de la base de données d'empreinte digitale employée (db2_b.zip) par nous sont comme suit :

Type de capteur	Taille d'image	Taille d'ensemble	Résolution
Capteur optique	388x374 (142 k pixels)	10 utilisateurs X 8 empreintes digitales par utilisateur	500 dpi

Cette base de données d'empreinte digitale nous a été fournie par prof. Ajay Kumar Pathak. Cependant, elle peut également être téléchargée de [33].

IV.3 : Implémentation et Résultats

IV.3.1 : Introduire la commande **start_gui_single_mode** dans MATLAB R2011a :

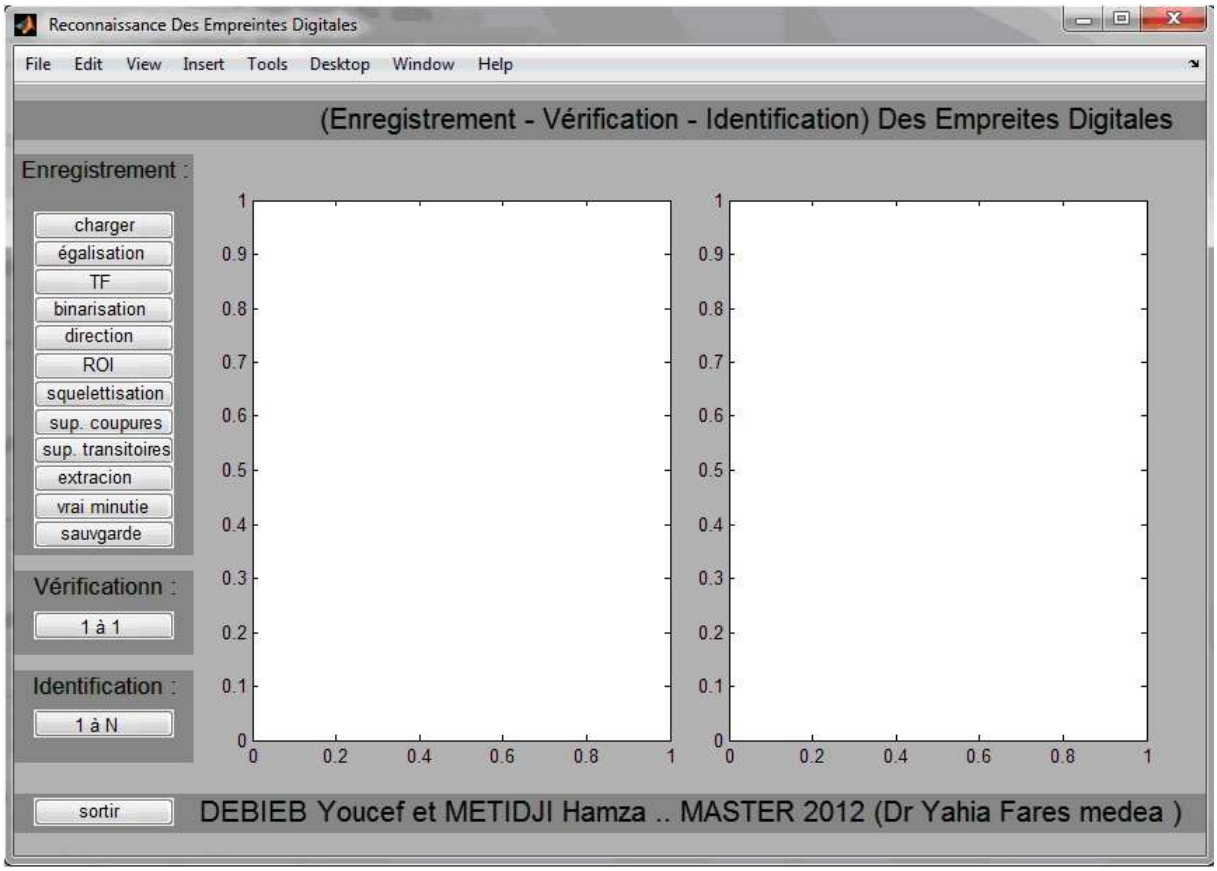


Figure (IV.1) : Interface graphique du système

L'interface utilisateurs du système d'identification d'empreinte digitale. La série de boutons du secteur gauche sera appelée séquentiellement dans la démonstration conséquente. Les deux secteurs en blanc sont employés pour montrer l'image d'empreinte digitale avant et après une transaction respectivement.

IV.3.2 : le bouton **charger :**

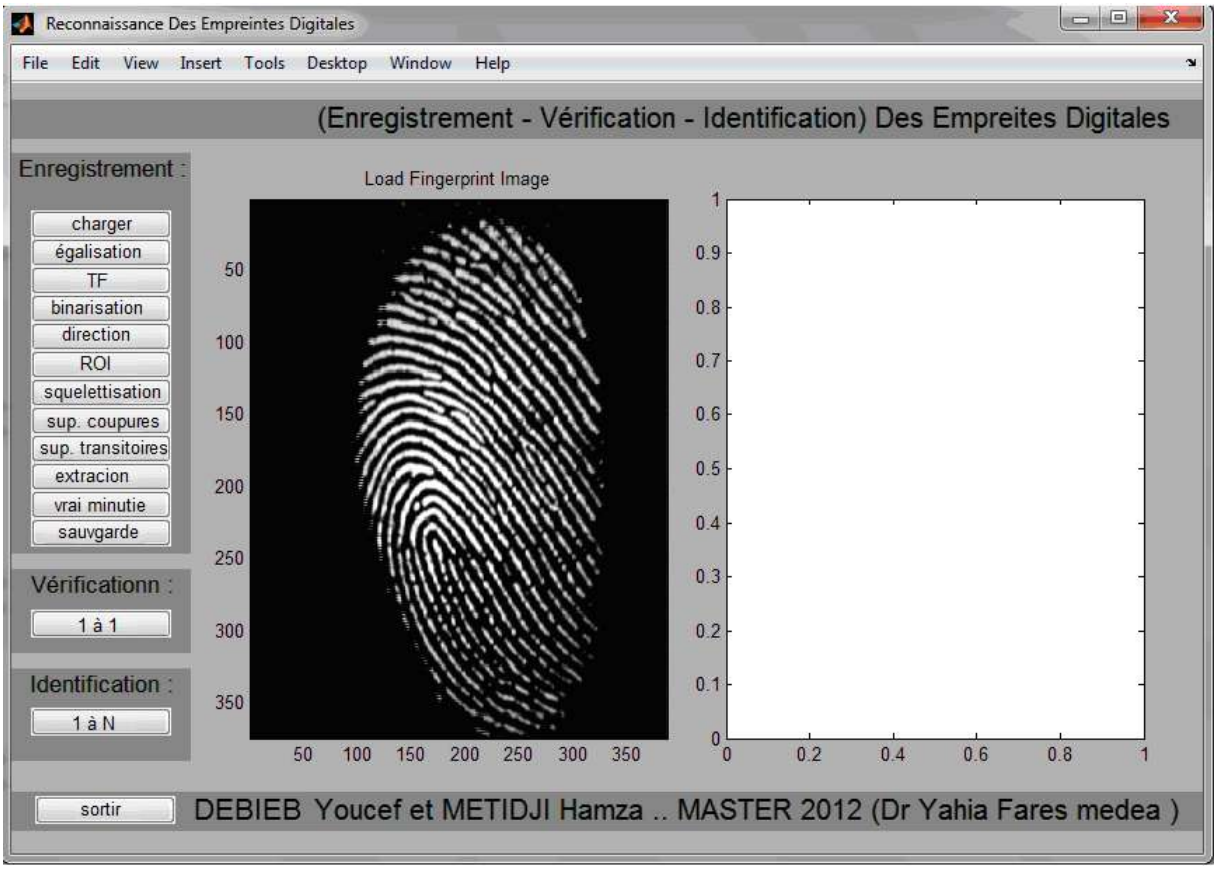


Figure (IV.2) : fonctionnement du bouton charger

Charger une image d'empreinte digitale de niveau gris d'une commande spécifique par utilisateurs. Des formats multiples sont soutenus et la taille d'image n'est pas limitée. Mais les arêtes d'empreinte digitale devraient avoir la grande intensité grise rivalisée avec le fond et les vallées.

IV.3.3 : le bouton **égalisation** :

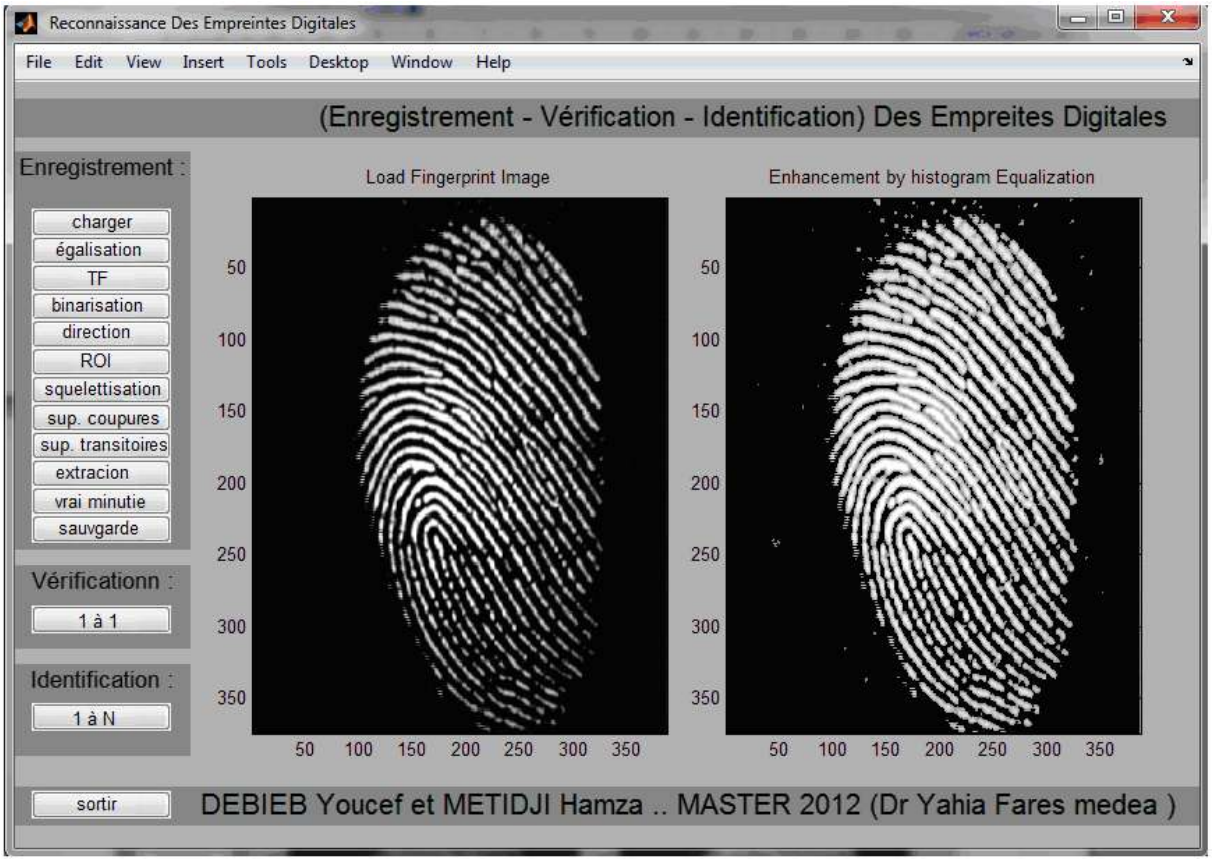


Figure (IV.3) : fonctionnement du bouton égalisation

Après l'égalisation d'histogramme. L'image du secteur gauche est l'empreinte digitale originale. L'image augmentée après l'égalisation d'histogramme est montrée du côté droit.

IV.3.4 : le bouton **TF** :

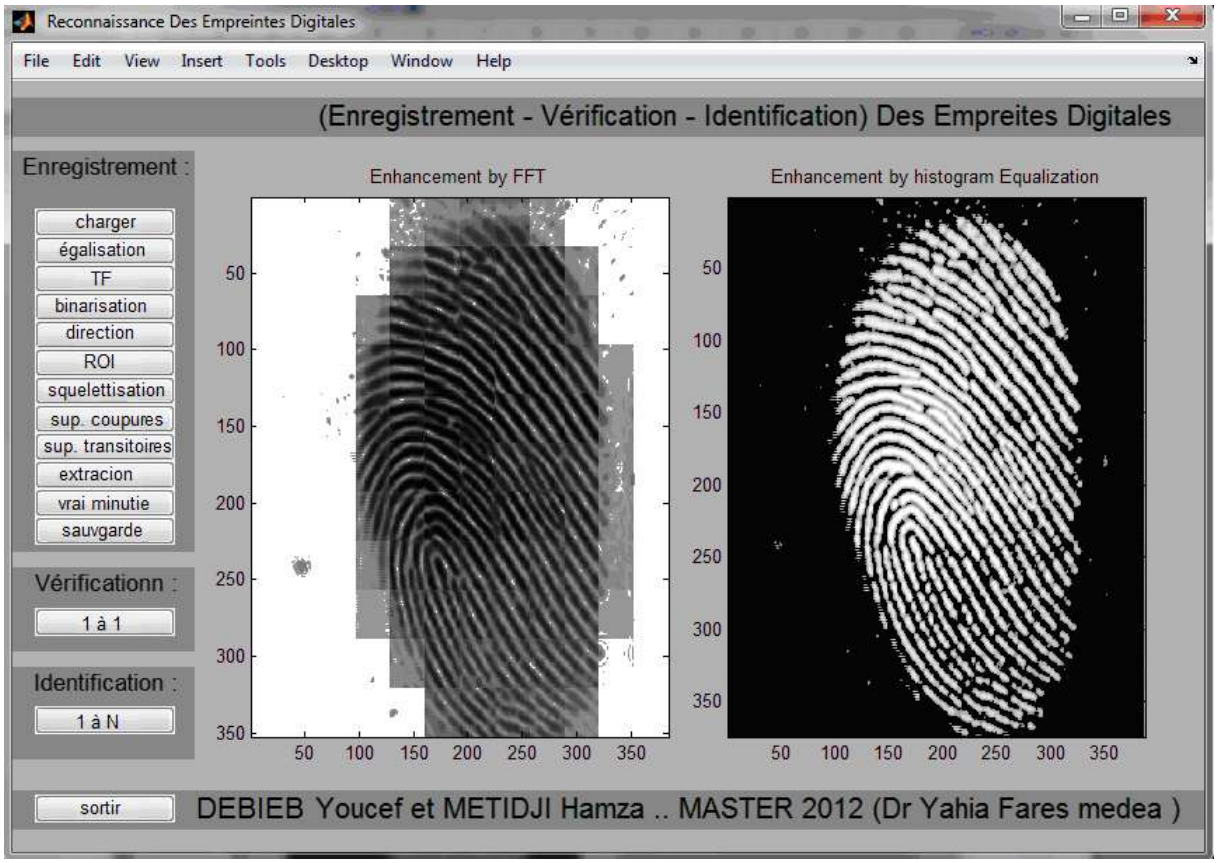


Figure (IV.4) : fonctionnement du bouton TF

Fenêtre capturée après clic sur le bouton de `TF'. Le dialogue automatique accepte le paramètre k. La teneur optimale expérimentale en k est 0.45. Les utilisateurs peuvent remplir tout autre constant dans le dialogue pour obtenir une meilleure exécution. L'image augmentée sera montrée dans la boîte gauche d'écran, qui cependant n'est pas montrée ici.

IV.3.5 : le bouton **binarisation** :

IV.3.6 : le bouton **direction** :

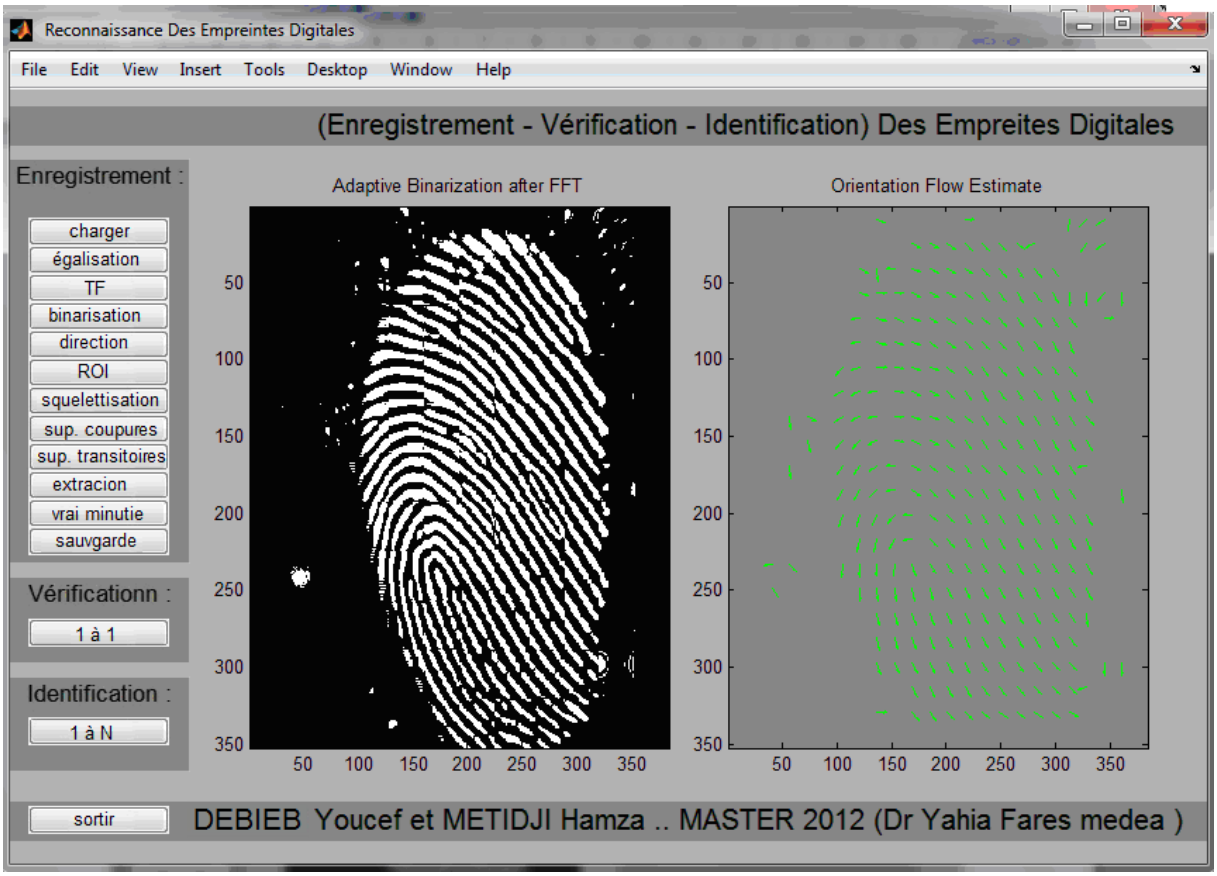


Figure (IV.5) : fonctionnement du bouton direction

La récupération d'écran après la binarisation (gauche) et l'évaluation de direction de bloc (droite).

IV.3.7 : le bouton **ROI** :

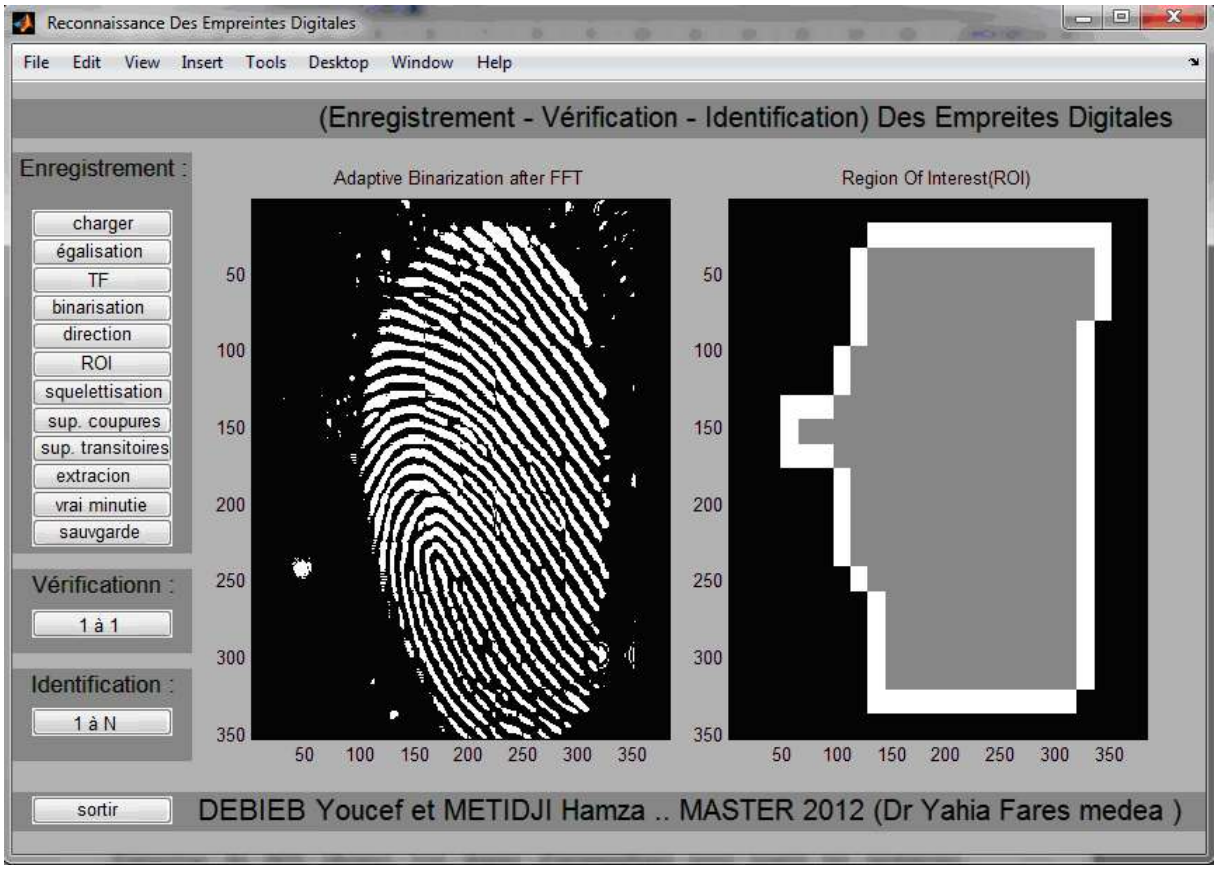


Figure (IV.6) : fonctionnement du bouton ROI

Extraction de ROI (droite). Les étapes d'intermédiaire pour toutes les opérations morphologiques telles fines et ouvertes ne sont pas montrées. La boîte droite d'écran montre la région finale d'intérêt de l'image d'empreinte digitale. Les opérations suivantes opéreront seulement la région d'intérêt.

IV.3.8 : le bouton **squelettisation** :

IV.3.9 : le bouton **sup. coupures** :

IV.3.10 : le bouton **sup. transitoires** :

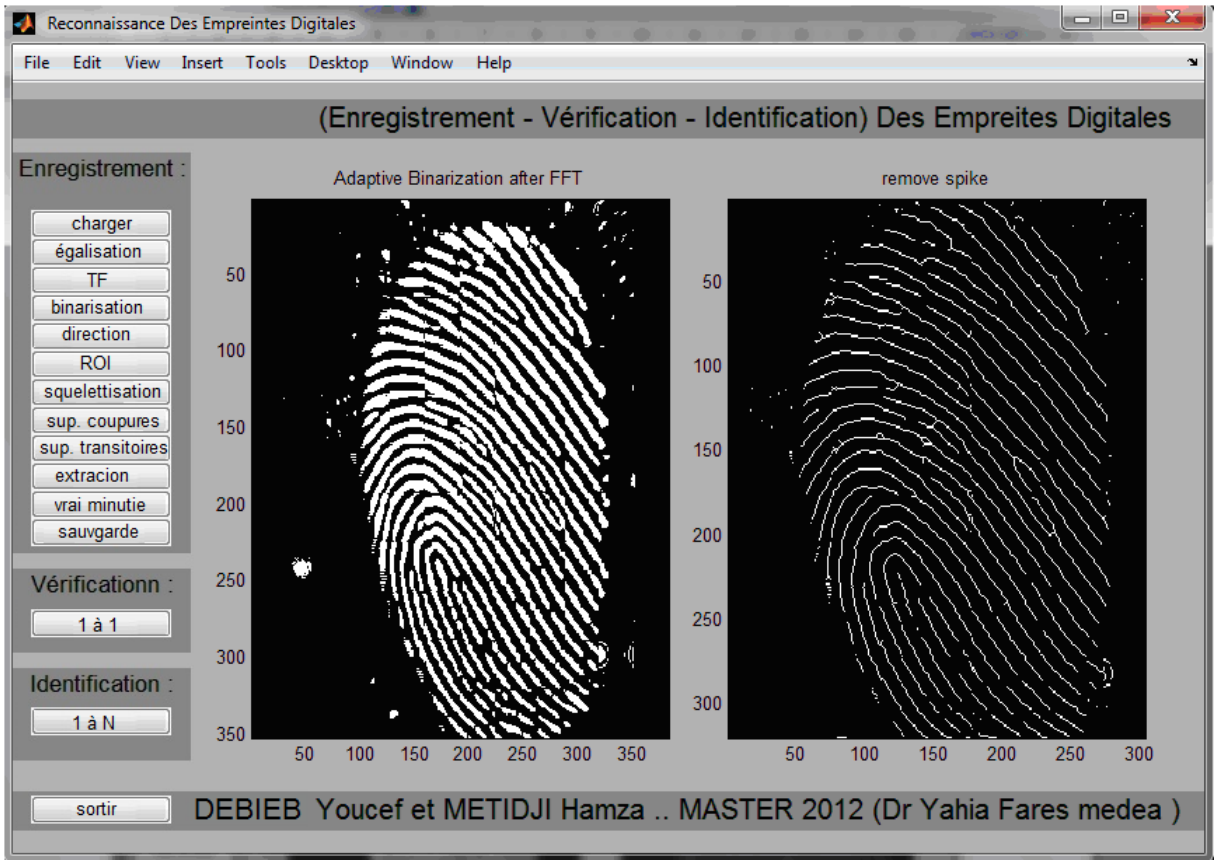


Figure (IV.7) : fonctionnement du bouton sup. transitoires

L'image d'empreinte digitale après (squelettisation), H casse le déplacement, le déplacement d'isolement de crêtes et le déplacement de transitoire. (Droit).

IV.3.11 : le bouton **extraction**

IV.3.12 : le bouton **vrai minutie**

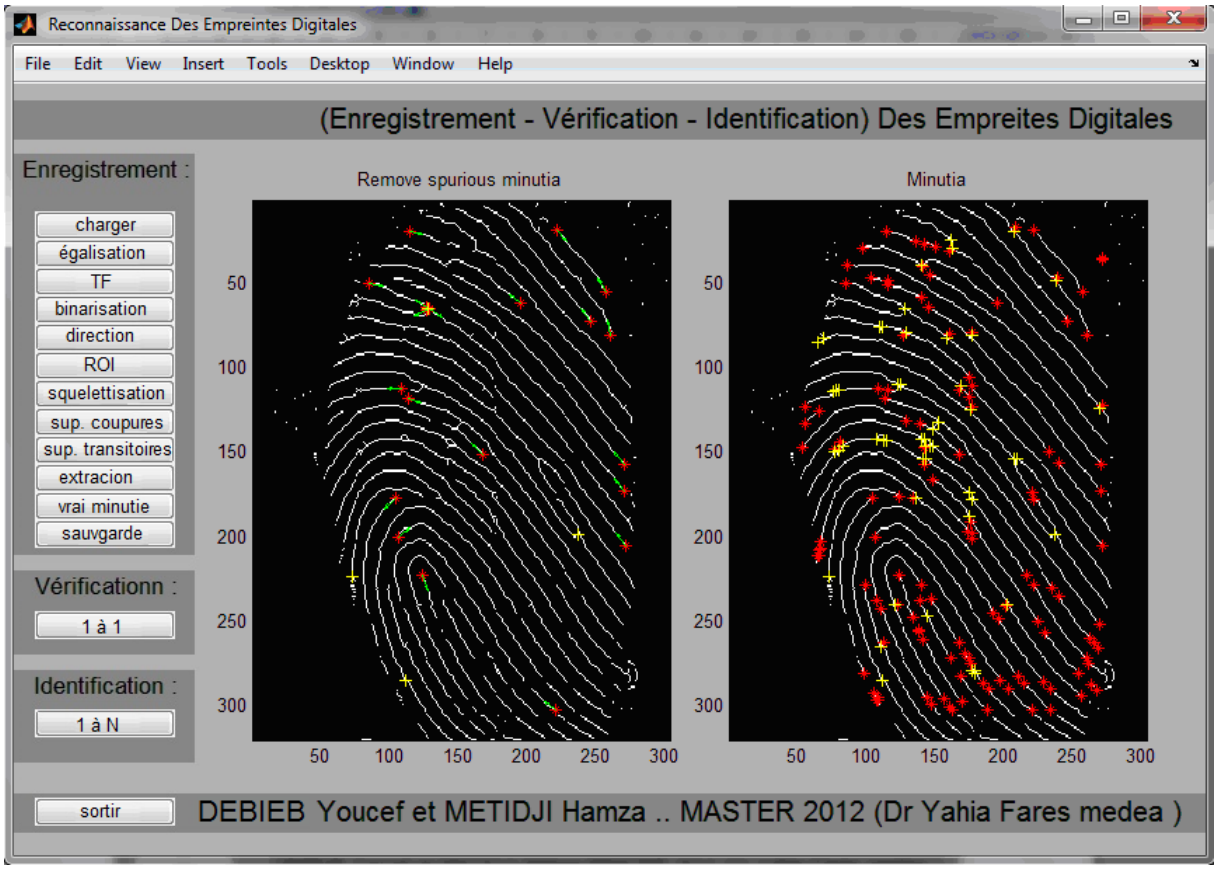


Figure (IV.8) : fonctionnement du bouton vrai minutie

Inscription de minutie (droite) et déplacement faux de minutie (gauche). Des bifurcations sont situées avec les croix jaunes et les arrêts sont dénote avec les étoiles rouges. Et les minuties véritables (gauche) sont marquées avec des orientations avec les flèches vertes.

IV.3.13 : le bouton **sauvegarde** :

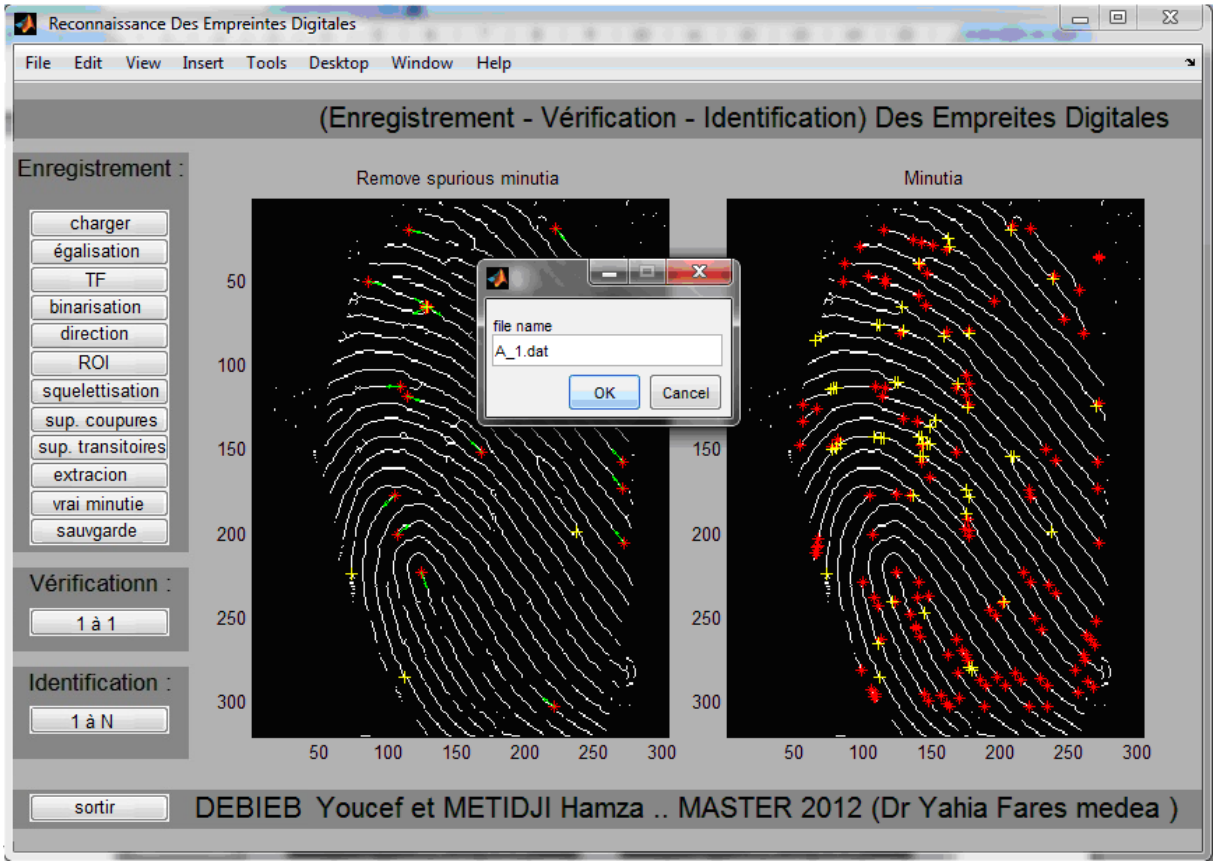


Figure (IV.9) : fonctionnement du bouton sauvegarde

Sauvegarder la minutie à un dossier des textes. Le dossier sauvegarde des textes stocke l'information sur toute la minutie véritable. Le format exact des dossiers est expliqué dans le code source.

IV.3.14 : le bouton **1 à 1 :**

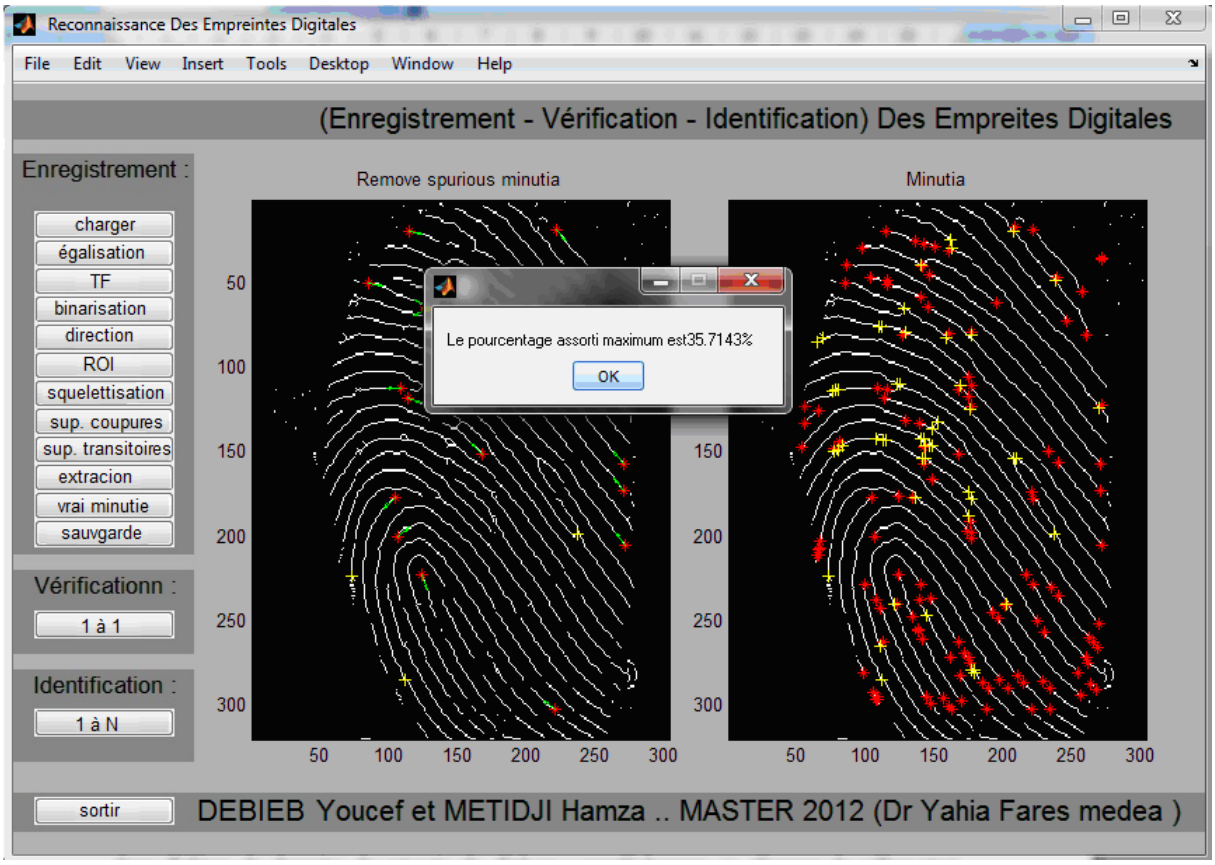


Figure (IV.10) : fonctionnement du bouton 1 à 1

Les dossiers de minutie de la charge deux et font le vérification. Les utilisateurs peuvent ouvrir deux fichiers de données de minutie du dialogue appelé bouton en cliquant sur `1 à 1'. L'algorithme de vérification renverra un message de sollicitation des points de vérification. Mais être noté que vérifiant en mode de GUI n'est pas encouragé puisque l'algorithme de vérification se fonde sur le calcul lourd. Les états se produiront après un long temps de fonctionnement flegmatique. L'essai en lots est préparé pour de vérification d'essai. Veuillez se référer les fichiers source pour l'essai en lots.

IV.3.15 : le bouton **1 à N :**

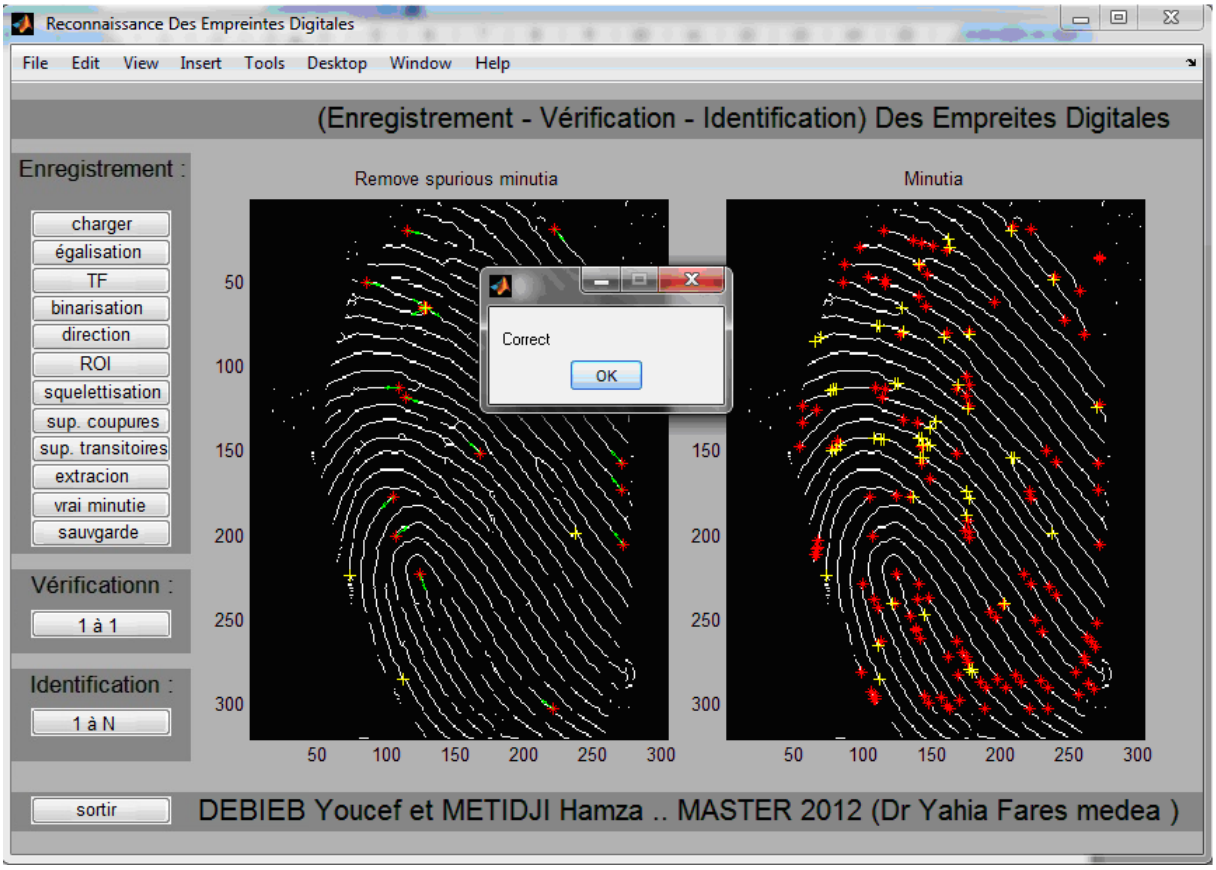


Figure (IV.11) : fonctionnement du bouton 1 à N

Les utilisateurs peuvent ouvrir un fichier de donnes de minutie en cliquant sur `1 à N '. Le programme fait une vérification entre l'empreinte du suspect et celles de base de données.
Si le message affiche « correct » ça veut dire plus de seuil=75% des empreintes vérifiées sont véritable. Sinon le message affiche « incorrect ».

IV.3.16 : **Performance de logiciel** :

Une base de données d'empreinte digitale du FVC2000 (concurrence 2000 de vérification d'empreinte digitale) est employée pour examiner l'exécution d'expérience. Nos essais de programme toutes les images sans amende - accordant pour la base de données. L'exposition d'expériences notre programme peut différencier des paires imposteurs de minutie des paires véritables de minutie à un certain niveau de confiance. En outre, les bonnes conceptions d'expérience peuvent sûrement améliorer l'exactitude comme avoué près [33]. On s'attend à ce que d'autres études sur de bonnes conceptions de la formation et essai améliorent le résultat.

Voici le diagramme pour les points corrects et la distribution incorrecte de points :

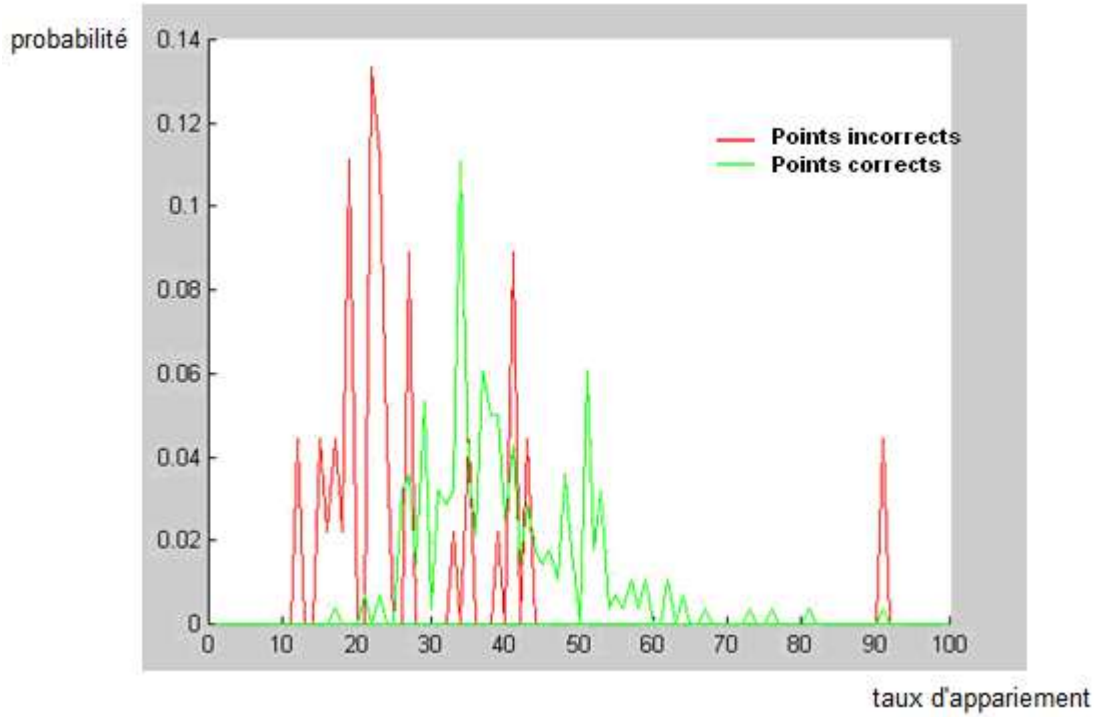


Figure (IV.12) : Distribution des points corrects et des points incorrects

Il peut voir de la figure ci-dessus que là existent deux distributions partiellement recouvertes. La courbe rouge dont les crêtes sont principalement situées à la partie gauche signifie que les points incorrects moyens d'allumette sont 25. La courbe verte dont les crêtes sont principalement situées du côté droit de la courbe rouge signifie que les points corrects moyens d'allumette sont 35. Ceci indique que l'algorithme est capable de différencient des empreintes digitales à un bon taux correct en plaçant une valeur- seuil appropriée.

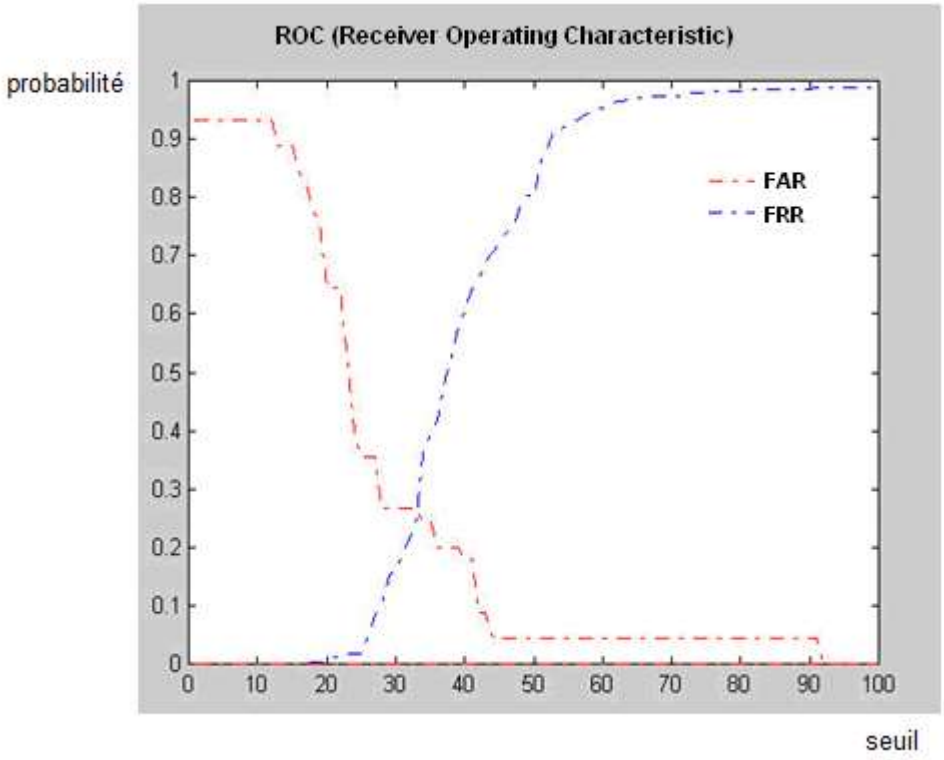


Figure (IV.13) : Courbe FAR et FRR en fct du seuil

Le diagramme ci-dessus montre le FRR et les courbes LOINTAINES. Au taux d'erreur égal 25%, les points de séparation 33 rejetteront faussement des paires véritables de minutie de 25% et accepteront faussement des paires imposteurs de minutie de 25% et ont le taux de vérification de 75%.

L'acceptation incorrecte élevée et le rejet faux sont dus à quelques images d'empreinte digitale avec la mauvaise qualité et l'algorithme vulnérable d'allumette de minutie.

IV.4: Conclusion

Notre projet a combiné beaucoup de méthodes pour construire un extracteur de minutie et une bouveteuse de minutie. La combinaison des méthodes multiples vient d'une recherche large sur des travaux de recherche. Également un certain roman change comme la segmentation des opérations morphologiques, l'inscription de minutie avec le spécial considérant le compte triple de la branche, l'unification de minutie en décomposant une branche en trois arrêts, et la vérification dans le système du même rang de x/y unifié après qu'une transformation en deux étapes soient employées dans notre projet, qui ne sont pas rapportés dans d'autres littératures.

Également un codage de programme avec MATLAB passant par toutes les étapes de l'identification d'empreinte digitale est établi. Il est utile de comprendre les procédures de l'identification d'empreinte digitale. Et démontrer les questions clés de l'identification d'empreinte digitale. [31]

Conclusion générale

La sécurité n'est pas appliquée en se concentrant sur un seul paramètre. Au lieu de résoudre un problème à une dimension, un environnement sécurisé requiert de multiples dimensions de points de contrôle critiques. L'authentification sécurisée est assurée par plusieurs paramètres. Un paramètre est un jeton de sécurité d'un individu possède de façon unique, tel qu'une clé physique ou une carte à puce. Un autre paramètre est un élément unique d'une personne sait, tel qu'un code PIN. Un paramètre supplémentaire est les caractéristiques biologiques uniques d'un individu, par exemple l'ADN ou bien un code d'iris.

La technologie biométrique pourrait avoir un impact positif considérable dans la société, si elle est correctement utilisée pour augmenter la robustesse des systèmes de sécurité à travers le monde. Cela aiderait à réduire les niveaux croissants de fraude, la criminalité et le terrorisme. Toutefois, la biométrie a le potentiel de nuire à la société en permettant aux gouvernements une quantité massive d'informations personnelles concernant les particularités. Pour intégrer un système d'identification biométriques complet sera un long processus, mais la technologie a le potentiel de changer la façon dont le monde fonctionne, aucun mot de passe et plus des cartes à puce à utiliser, simplement en utilisant votre corps comme votre clé. Toutefois, la biométrie a été utilement appliquée pour les questions de moindre importance, par exemple « time monitoring systems and industry authentication systems ». Comme les progrès de la technologie augmentent, il est assuré que la biométrie peut être effectivement appliquée à des systèmes importants.

Il ne fait aucun doute que la biométrie est la prochaine étape de la technologie de sécurité omni présents dans notre plus en plus paranoïaque, la société autoritaire. Cependant, il reste encore beaucoup à faire: les clients sont effrayés par l'échec à s'inscrire élevé et les taux de non match ainsi que les incompatibilités. En outre, la sécurité du système dans son ensemble a besoin de plus de soins à être enlevé. Les améliorations futures de la technologie d'acquisition et d'algorithmes, ainsi que la disponibilité de normes industrielle va certainement assurer un avenir prometteur pour la biométrie. **Sera-ce la fin de mot de passe classique ou d'un jeton à base de systèmes?** Certainement pas la biométrie n'est pas la solution idéale soit, c'est juste un bon compromis entre la sécurité et la facilité d'utilisation.

Bibliographie

[01] : http://www.neuroinformatik.ruhrunibochum.de/ini/VDM/research/computerVision/graphMatching/identification/faceRecognition/contents.html ; 2002 .

[02] : www.biometrics.gov

[03] : Institut de la Francophonie pour l'Informatique ; Biométrie pour l'Identification ;DANG Hoang Vu ; Hanoï Vietnam ; 2003 .

[04] : Exposé sur la technologie d´empreinte digitale ; Gerik , Alexander von Graevenitz , Bergdata Biometrics GmbH ; Bonn , Germany ; 1999 .

[05] : Lin Hong et al ; An identification system using fingerprints ; 1997

[06] : Fingerprint Handbook ; Davide Maltoni , Dario Maio , Anil K. Salil Prabhakar ; 2003

[07] : http://www.biometricscatalog.org/NSTCSubcommittee

[08] : Ecole Normale Supérieure de Lyon ; Identification de visages ; Olivier Schwander ; 7 juillet 2007

[09] : Institut des systèmes intelligents et de robotique France ; Biométrie visage

[10] : Department of Informatics University of Oslo ;Biometric Systems: A Face Recognition approach ; Erik Hjelmås ; 2001 .

[11] : http://recogsys.com/index.shtml

[12] : Eigenface Recognition ; http://et.wcu.edu/aidc/BioWebPages/eigenfaces.htm

[13] : Face Recognition by Elastic Bunch Graph Matching ; Laurenz Wiskott ; 24 April 1996

[14] : Regularized Discriminant Analysis For the Small Sample Size Problem in Face Recognition ; Pattern Recognition Letters ; J. Lu , K.N. Plataniotis , A.N. Venetsanopoulos ; December 2003

[15] : The CSU Face Identification Evaluation System: Its Purpose ; Features and Structure ; International Conference on Vision Systems ; D. Bolme , R. Beveridge , M. Teixeira , B. Draper ; Graz , Austria ; April 2003

[16] : University of Cambridge: Computer Laboratory : Webpage for John Daugman ; John Daugman ; http://www.cl.cam.ac.uk/users/jgd1000/

[17] : http://www.cybersign.com/techoverview_what.htm

[18] : http://www.gaits.com/biometrics_signature.asp

[19] : Exposé sur la technologie d´empreinte digitale ; Bergdata Biometrics ; Gerik Alexander von Graevenitz , GmbH ; Bonn , Germany

[20] : McGraw Hill Osborne ; Biometrics ; John D. Woodward, Jr. , Nicholas M. Orlans , Peter T. Higgins ; New York ; 2003

[21] : Indiana University Computer Science Department ; Z. McMahon ; 24 January 2005 http://www.cs.indiana.edu/~zmcmahon/biometricshistory. html

[22] : Biometrics – Now and Then: The development of biometrics over the last 40 years ; J.L. Wayman ; H. Daum (ed.) Biometrics in the Reflection of Requirements: Second BSI Symposium on Biometrics 2004 ; Bonn ; 2004

[23] : http://solutions.journaldunet.com/0208/020826_biometrie_1.shtml

[24] : Secugen Biometrics Solutions ; http://www.secugen.com/images/faq02.gif

[25] : International Biometric Group ; http://www.biometricgroup.com

[26] : Bioidentification: Frequently Asked Questions ; Manfred Bromba http://www.bromba.com/faq/fpfaqe.htm#Fingerprint-Sensoren

[27] : Handbook of Fingerprint Recognition ; Maltoni, Davide, Maio, Jain, and Prabhakar ; New York ; 2005

[28] : Embryologic Development of Epidermal Ridges and Their Configurations, Dermatoglyphics:Science in transition ; W.J. Babler ; New York ; 1991

[29] : Twin Test: On Discriminability of Fingerprints", Proc. 3rd International Conference on Audio- and Video-Based Person Authentication ; A.K. Jain, S. Prabhakar, S. Pankanti ; Sweden ;June 6-8, 2001

[30] : INSTITUT NATIONAL POLYTECHNIQUE DE GRENOBLE ; Fabien PARRAIN ; 02 décembre 2002

[31] : Hong Kong Baptist University ; Fingerprint Recognition ; WUZHILI ; 19 April 2002

[32] : Biometrics ; John D. Woodward , Nicholas M. Orlans, and Peter T. Higgins ; New York: McGraw Hill Osborne; 2003

[33] : FVC2002 ; http://bias.csr.unibo.it/fvc2002/

[34] : Lin Hong. "Automatic Personal Identification Using Fingerprints", Ph.D. Thesis, 1998

Annexe

Les codes_source :

Le code loadimage.m :

```
function image1=loadimage
% dialog for opening fingerprint files
[imagefile1 , pathname]= uigetfile('*.bmp;*.BMP;*.tif;*.TIF;*.jpg','Open An
Fingerprint image');
if imagefile1 ~= 0
cd(pathname);
image1=readimage(char(imagefile1));
image1=255-double(image1);
end;
```

Le code readimage.m :

```
function b = readimage(w);
% read the image w
% use the full image for further processes
a=imread(w);
b = double(a);
```

Le code drawROI_end.m :

```
function [roiImg,roiBound,roiArea] = drawROI(in,inBound,inArea,noShow)
%drawROI(grayLevelFingerprintImage,ROIboundMap,ROIareaMap,flagToDisableGUI)
%construct a ROI rectangle for the input fingerprint image and return the
%segmented fingerprint
%With the assumption that only one ROI region for each fingerprint image

[iw,ih]=size(in);
tmplate = zeros(iw,ih);
[w,h] = size(inArea);
tmp=zeros(iw,ih);
%ceil(iw/16) should = w
%ceil(ih/16) should = h

left = 1;
right = h;
upper = 1;
bottom = w;

le2ri = sum(inBound);
roiColumn = find(le2ri>0);
left = min(roiColumn);
right = max(roiColumn);
tr_bound = inBound';
up2dw=sum(tr_bound);
```

```
roiRow = find(up2dw>0);
upper = min(roiRow);
bottom = max(roiRow);
%cut out the ROI region image
%show background,bound,innerArea with different gray intensity:0,100,200

for i = upper:1:bottom
   for j = left:1:right
      if inBound(i,j) == 1
         tmplate(16*i-15:16*i,16*j-15:16*j) = 200;
         tmp(16*i-15:16*i,16*j-15:16*j) = 1;

      elseif inArea(i,j) == 1 & inBound(i,j) ~=1
         tmplate(16*i-15:16*i,16*j-15:16*j) = 100;
         tmp(16*i-15:16*i,16*j-15:16*j) = 1;

      end;
   end;
end;

in=in.*tmp;

roiImg = in(16*upper-15:16*bottom,16*left-15:16*right);
roiBound = inBound(upper:bottom,left:right);
roiArea = inArea(upper:bottom,left:right);

%inner area
roiArea = im2double(roiArea) - im2double(roiBound);

if nargin == 3
    colormap(gray);
   imagesc(tmplate);
end;
```

Le code fftenhance_end.m :

```
function [final]=fftenhance(image,f)

I = 255-double(image);
[w,h] = size(I);
%out = I;

w1=floor(w/32)*32;
h1=floor(h/32)*32;
inner = zeros(w1,h1);

for i=1:32:w1
   for j=1:32:h1
      a=i+31;
      b=j+31;
      F=fft2( I(i:a,j:b) );
      factor=abs(F).^f;
      block = abs(ifft2(F.*factor));

      larv=max(block(:));
      if larv==0
         larv=1;
      end;
```

```
      block= block./larv;
      inner(i:a,j:b) = block;
   end;
end;

%out(1:w1,1:h1)=inner*255;
final=inner*255;

%d=max(out(:)); %Find max pixel value in C.
%c=min(out(:));
%figure
%imshow(out,[c d]);

final=histeq(uint8(final));
%final=adaptiveThres2(final,32,0);
%imagesc(final);
%colormap(gray);
```

Le code direction.m :

```
function [p,z] = direction(image,blocksize,noShow)
%   DIRECTION cacluates the local flow orientation in each local window
%  with size (blocksize x blocksize)
%  direction(grayScaleFingerprintImage,blocksize,graphicalShowDisableFlag)
%  return p ROI bound
%  return z ROI area
%image=adaptiveThres(image,16,0);

[w,h] = size(image);
direct = zeros(w,h);
gradient_times_value = zeros(w,h);
gradient_sq_minus_value = zeros(w,h);
gradient_for_bg_under = zeros(w,h);

W = blocksize;
theta = 0;
sum_value = 1;
bg_certainty = 0;
blockIndex = zeros(ceil(w/W),ceil(h/W));
%directionIndex = zeros(ceil(w/W),ceil(h/W));

times_value = 0;
minus_value = 0;

center = [];
%Note that the image coordinate system is
%x axis towards bottom and y axis towards right
filter_gradient = fspecial('sobel');
%to get x gradient
I_horizontal = filter2(filter_gradient,image);

%to get y gradient
filter_gradient = transpose(filter_gradient);
I_vertical = filter2(filter_gradient,image);
gradient_times_value=I_horizontal.*I_vertical;
gradient_sq_minus_value=(I_vertical-
I_horizontal).*(I_vertical+I_horizontal);
gradient_for_bg_under = (I_horizontal.*I_horizontal) +
(I_vertical.*I_vertical);
```

```
for i=1:W:w
    for j=1:W:h
      if j+W-1 < h & i+W-1 < w
        times_value = sum(sum(gradient_times_value(i:i+W-1, j:j+W-1)));
        minus_value = sum(sum(gradient_sq_minus_value(i:i+W-1, j:j+W-1)));
          sum_value = sum(sum(gradient_for_bg_under(i:i+W-1, j:j+W-1)));

          bg_certainty = 0;
          theta = 0;

          if sum_value ~= 0 & times_value ~=0
             %if sum_value ~= 0 & minus_value ~= 0 & times_value ~= 0
             bg_certainty = (times_value*times_value +
minus_value*minus_value)/(W*W*sum_value);

            if bg_certainty > 0.05
             blockIndex(ceil(i/W),ceil(j/W)) = 1;

             %tan_value = atan2(minus_value,2*times_value);
             tan_value = atan2(2*times_value,minus_value);


                theta = (tan_value)/2 ;
                theta = theta+pi/2;

            %now the theta is within [0,pi]
            %directionIndex(ceil(i/W),ceil(j/W)) = theta;
            %center = [center;[round(i + (W-1)/2),round(j + (W-
             1)/2),theta,bg_certainty]];
center = [center;[round(i + (W-1)/2),round(j + (W-1)/2),theta]];
                end;
        end;
    end;
             times_value = 0;
          minus_value = 0;
          sum_value = 0;

   end;
end;

if nargin == 2
    imagesc(direct);

    hold on;
    [u,v] = pol2cart(center(:,3),8);
   quiver(center(:,2),center(:,1),u,v,0,'g');
   hold off;
end;

x = bwlabel(blockIndex,4);
%map = [0 0 0;jet(3)];
%figure
%imshow(x+1,map,'notruesize')

y = bwmorph(x,'close');
%figure
%imshow(y,map,'notruesize');
```

```
%z is the region of interest (ROI)
%with the index format

z = bwmorph(y,'open');
%figure
%imshow(z,map,'notruesize');
%p is the bound of ROI

p = bwperim(z);
%figure,
%imshow(p,map,'notruesize');
%directMap = directionIndex;
```

Le code mark_minutia.m :

```
function [end_list,branch_list,ridgeOrderMap,edgeWidth] = mark_minutia(in,
inBound,inArea,block);

[w,h] = size(in);
[ridgeOrderMap,totalRidgeNum] = bwlabel(in);

imageBound = inBound;
imageArea = inArea;
blkSize = block;

%innerArea = im2double(inArea)-im2double(inBound);

edgeWidth = interRidgeWidth(in,inArea,blkSize);
end_list    = [];
branch_list = [];


for n=1:totalRidgeNum
   [m,n] = find(ridgeOrderMap==n);
   b = [m,n];
   ridgeW = size(b,1);

   for x = 1:ridgeW
      i = b(x,1);
      j = b(x,2);
%if imageArea(ceil(i/blkSize),ceil(j/blkSize)) == 1 &
imageBound(ceil(i/blkSize),ceil(j/blkSize)) ~= 1
if inArea(ceil(i/blkSize),ceil(j/blkSize)) == 1
      neiborNum = 0;
      neiborNum = sum(sum(in(i-1:i+1,j-1:j+1)));
      neiborNum = neiborNum -1;


   if neiborNum == 1
        end_list =[end_list; [i,j]];

   elseif neiborNum == 3
      %if two neighbors among the three are connected directly
      %there may be three braches are counted in the nearing three cells
      tmp=in(i-1:i+1,j-1:j+1);
```

```
       tmp(2,2)=0;
       [abr,bbr]=find(tmp==1);
       t=[abr,bbr];

       if isempty(branch_list)
          branch_list = [branch_list;[i,j]];
       else

       for p=1:3
          cbr=find(branch_list(:,1)==(abr(p)-2+i) &
branch_list(:,2)==(bbr(p)-2+j) );
          if ~isempty(cbr)
             p=4;
             break;
          end;
       end;

       if p==3
          branch_list = [branch_list;[i,j]];
       end;

    end;

    end;

    end;

end;
end;
```

Le code show_minutia.m :

```
function show_minutia(image,end_list,branch_list);

%[x,y] = size(end_list);
%imag = zeros(200,200);
%imag = image;
%x
%for i=1:x
%   xx = end_list(i,1);
%   yy = end_list(i,2);
%
%   imag(xx-2:xx+2,yy-2:yy+2) = 1;
%   imag(xx,yy) = 0;
%end;

%[x,y] = size(branch_list);
%for i = 1:x
%   xx = branch_list(i,1);
%   yy = branch_list(i,2);

%   imag(xx-2:xx+2,yy-2:yy+2) = 1;
%   imag(xx-1:xx+1,yy-1:yy+1) = 0;
    %imag(xx,yy) = 0;
%end;

%figure;
colormap(gray);imagesc(image);
```

```
hold on;

if ~isempty(end_list)

plot(end_list(:,2),end_list(:,1),'*r');
if size(end_list,2) == 3
   hold on
    [u,v] = pol2cart(end_list(:,3),10);
    quiver(end_list(:,2),end_list(:,1),u,v,0,'g');
end;
end;

if ~isempty(branch_list)
hold on
plot(branch_list(:,2),branch_list(:,1),'+y');
end;
```

Le code remove_spurious_Minutia.m :

```
function [pathMap, final_end,final_branch]
=remove_spurious_Minutia(in,end_list,branch_list,inArea,ridgeOrderMap,edgeW
idth)

[w,h] = size(in);
final_end = [];
final_branch =[];
direct = [];
pathMap = [];

end_list(:,3) = 0;
branch_list(:,3) = 1;

minutiaeList = [end_list;branch_list];
finalList = minutiaeList;
[numberOfMinutia,dummy] = size(minutiaeList);
suspectMinList = [];

for i= 1:numberOfMinutia-1
   for j = i+1:numberOfMinutia
      d =( (minutiaeList(i,1) - minutiaeList(j,1))^2 + (minutiaeList(i,2)-
minutiaeList(j,2))^2)^0.5;

      if d < edgeWidth
         suspectMinList =[suspectMinList;[i,j]];
      end;
   end;
end;

[totalSuspectMin,dummy] = size(suspectMinList);
%totalSuspectMin

for k = 1:totalSuspectMin
   typesum = minutiaeList(suspectMinList(k,1),3) +
minutiaeList(suspectMinList(k,2),3);

   if typesum == 1
```

```
      % branch - end pair
      if
ridgeOrderMap(minutiaeList(suspectMinList(k,1),1),minutiaeList(suspectMinLi
st(k,1),2) ) ==
ridgeOrderMap(minutiaeList(suspectMinList(k,2),1),minutiaeList(suspectMinLi
st(k,2),2) )
         finalList(suspectMinList(k,1),1:2) = [-1,-1];
          finalList(suspectMinList(k,2),1:2) = [-1,-1];
      end;

   elseif typesum == 2
      % branch - branch pair
      if
ridgeOrderMap(minutiaeList(suspectMinList(k,1),1),minutiaeList(suspectMinLi
st(k,1),2) ) ==
ridgeOrderMap(minutiaeList(suspectMinList(k,2),1),minutiaeList(suspectMinLi
st(k,2),2) )
         finalList(suspectMinList(k,1),1:2) = [-1,-1];
          finalList(suspectMinList(k,2),1:2) = [-1,-1];
      end;

   elseif typesum == 0
      % end - end pair
      a = minutiaeList(suspectMinList(k,1),1:3);
      b = minutiaeList(suspectMinList(k,2),1:3);

      if ridgeOrderMap(a(1),a(2)) ~=  ridgeOrderMap(b(1),b(2))

      [thetaA,pathA,dd,mm] = getLocalTheta(in,a,edgeWidth);
      [thetaB,pathB,dd,mm] = getLocalTheta(in,b,edgeWidth);

      %the connected line between the two points

      thetaC = atan2( (pathA(1,1)-pathB(1,1)), (pathA(1,2) - pathB(1,2)) );


      angleAB = abs(thetaA-thetaB);
      angleAC = abs(thetaA-thetaC);


         if ( (or(angleAB < pi/3, abs(angleAB -pi)<pi/3 )) & (or(angleAC <
pi/3, abs(angleAC - pi) < pi/3)) )
            finalList(suspectMinList(k,1),1:2) = [-1,-1];
            finalList(suspectMinList(k,2),1:2) = [-1,-1];
         end;

         %remove short ridge later
      elseif  ridgeOrderMap(a(1),a(2)) ==  ridgeOrderMap(b(1),b(2))
         finalList(suspectMinList(k,1),1:2) = [-1,-1];
         finalList(suspectMinList(k,2),1:2) = [-1,-1];

      end;
   end;
end;

   for k =1:numberOfMinutia
      if finalList(k,1:2) ~= [-1,-1]
         if finalList(k,3) == 0
```

```
            [thetak,pathk,dd,mm] =
getLocalTheta(in,finalList(k,:),edgeWidth);
            if size(pathk,1) >= edgeWidth
                final_end=[final_end;[finalList(k,1:2),thetak]];
                [id,dummy] = size(final_end);
                pathk(:,3) = id;
                pathMap = [pathMap;pathk];
            end;
         else

            final_branch=[final_branch;finalList(k,1:2)];
[thetak,path1,path2,path3] = getLocalTheta(in,finalList(k,:),edgeWidth);

            if size(path1,1)>=edgeWidth & size(path2,1)>=edgeWidth &
size(path3,1)>=edgeWidth

            final_end=[final_end;[path1(1,1:2),thetak(1)]];
            [id,dummy] = size(final_end);
            path1(:,3) = id;
            pathMap = [pathMap;path1];

            final_end=[final_end;[path2(1,1:2),thetak(2)]];
            path2(:,3) = id+1;
            pathMap = [pathMap;path2];


            final_end=[final_end;[path3(1,1:2),thetak(3)]];
                path3(:,3) = id+2;
            pathMap = [pathMap;path3];

            end;

         end;
      end;
   end;

   %final_end
   %pathMap
   %edgeWidth
```

Le code match_end.m :

```
function [percent_match]=match_end(template1,template2,edgeWidth,noShow)
% MATCH_END Fingerprint Minutia Matcher Based on Ridge Alignment
%    match_end(template1,template2) accepts the two template files
%    and return the maximum similiar certainty of the two fingerprints
%       template file stores an Nx3 matrix with the following specified
format:
%     ------------------------------------------------------------------
%       minutia_1_position_x  minutia_2_position_y  minutia_1_orientation
%       ...                   ...                   ...
%     minutia_n_position_x  minutia_n_position_y  minutia_n_orientation
%     ridge_1_point_1_posx    ridge_1_point_1_posy    ridge_ID(1)
%     ...                     ...                     ...
%     ridge_1_point_m_posx    ridge_1_point_m_posy    ridge_ID(1)
%     ridge_2_point_1_posx    ridge_2_point_1_posy    ridge_ID(2)
%     ...                     ...                     ...
```

```
%     ridge_n_point_1_posx    ridge_n_point_1_posy    ridge_ID(n)
%     ...                     ...                     ...
%     ridge_n_point_m_posx    ridge_n_point_m_posy    ridge_ID(n)
%
%       n refers to the total miniutia number
%       m is set to the value of average inter-ridge width
%     ---------------------------------------------------------------
%    match_end(template1,template2,noShow) also accepts the flag 'noShow'
to disable the
%    popup dialog showing final matching percentage. The value can be
simply set to 0.
%    This function is used for batch process.

%   Decompose the template file into minutia and ridge matrixes seperately
if or(edgeWidth == 0,isempty(edgeWidth))
   edgeWidth=10;
end;

if or(isempty(template1), isempty(template2))
   percent_match = -1;
else
length1 = size(template1,1);
minu1 = template1(length1,3);
real_end1 = template1(1:minu1,:);
ridgeMap1= template1(minu1+1:length1,:);

length2 = size(template2,1);
minu2 = template2(length2,3);
real_end2 = template2(1:minu2,:);
ridgeMap2= template2(minu2+1:length2,:);

ridgeNum1 = minu1;
minuNum1 = minu1;
ridgeNum2 = minu2;
minuNum2 = minu2;
max_percent=zeros(1,3);

for k1 = 1:minuNum1
      %minuNum2

      %calculate the similarities between ridgeMap1(k1) and ridgeMap(k2)
      %choose the current two minutia as origins and adjust other minutia
      %based on the origin minutia.

      newXY1 = MinuOriginTransRidge(real_end1,k1,ridgeMap1);
   for k2 = 1:minuNum2

      newXY2 = MinuOriginTransRidge(real_end2,k2,ridgeMap2);

      %choose the minimum ridge length
      compareL = min(size(newXY1,2),size(newXY2,2));
      %compare the similarity certainty of two ridge
      eachPairP = newXY1(1,1:compareL).*newXY2(1,1:compareL);
      pairPSquare = eachPairP.*eachPairP;
      temp = sum(pairPSquare);

      ridgeSimCoef = 0;

      if temp > 0
```

```
      ridgeSimCoef = sum(eachPairP)/( temp^.5 );
      end;

if ridgeSimCoef > 0.8
        %transfer all the minutia in two fingerprint based on
        %the reference pair of minutia
         fullXY1=MinuOrigin_TransAll(real_end1,k1);
         fullXY2=MinuOrigin_TransAll(real_end2,k2);

         minuN1 = size(fullXY1,2);
         minuN2 = size(fullXY2,2);
         xyrange=edgeWidth;
         num_match = 0;

         %if two minutia are within a box with width 20 and height 20,
         %they have small direction variation pi/3
         %then regard them as matched pair

for i=1:minuN1
   for j=1:minuN2
      if (abs(fullXY1(1,i)-fullXY2(1,j))<xyrange & abs(fullXY1(2,i)-
fullXY2(2,j))<xyrange)
         angle = abs(fullXY1(3,i) - fullXY2(3,j) );
         if or (angle < pi/3, abs(angle-pi)<pi/6)
         num_match=num_match+1;
         break;
         end;
      end;
   end;
end;


% get the largest matching score
current_match_percent=num_match;
if current_match_percent > max_percent(1,1);
   max_percent(1,1) = current_match_percent;
   max_percent(1,2) = k1;
   max_percent(1,3) = k2;
end;
num_match = 0;

end;
end;
end;

percent_match = max_percent(1,1)*100/minuNum1;
end;

%if function is called in GUI mode, popup out the message box
%for final result
if nargin == 3
   text=strcat('Le pourcentage assorti maximum est
',num2str(percent_match),'%');
msgbox(text);
end;
```