**REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE**

**MINISTERE DE L'ENSEIGNEMENT SUPERIEUR & DE LA RECHERCHE SCIENTIFIQUE**

**UNIVERSITE DR. YAHIA FARES DE MEDEA**



**Faculté de la Technologie**
**Département de Génie Electrique**

# Projet de fin d'études

Pour l'obtention du diplôme de Master en Génie électrique

***Spécialité* : systèmes intelligents et communiquents**

THEME

# SYSTEME AUTOMATIQUE DE RECONNAISSANCE D'EMPREINTES DIGITALES

**Réalisé par :**

***ZILMI Hakim***

***SOUALHI Mohamed***

**Proposé et Dirigé par :**

***M. BOUCHERIT ISMAIL***

**Juin 2017**

# *REMERCIEMENTS*

Je tiens avant tout à remercier Allah pour la force et la volonté qu'il m'a données pour pouvoir achever ce travail.
J'exprime toute ma reconnaissance à mon directeur de mémoire BOUCHERIT ISMAIL pour son aide, son soutien, ses conseils ainsi que la confiance qu'il m'a fait en acceptant de m'encadrer.

Je remercie tous les membres de jury qui ont pris de leurs temps pour lire et juger ce travail ainsi que pour leur déplacement le jour de la soutenance.
Merci à Monsieur OUD ZMIRLI MOHAMED, responsable de Master SIC qui a su me guider vers les bonnes références.

Je tiens ensuite à remercier l'ensemble de mes collègues du SIC pour leur sympathie et bonne humeur.

Enfin, Je ne saurais oublier l'apport de mes parents pour l'accomplissement de ce travail, je tiens à leur rendre hommage à travers cette mémoire.

# *Dédicaces*

Je dédie ce travail

à mes très chers parents, dont

le sacrifice, la tendresse, l'amour, la patience,

le soutien, l'aide et les encouragements sont le secret de ma réussite.

Sans eux, je ne serais pas ce que je suis aujourd'hui. Je dédie ce travail également

À mon frère et mes Sœurs pour leurs soutiens, leurs aides, leurs encouragements.

À mon grand-mère et grands-pères et toute ma famille.

À tous mes enseignants, du primaire au niveau supérieur.

À tous mes amis.

ZILMI HAKIM

# *Dédicaces*

Je dédie ce travail
à mes très chers parents, dont
le sacrifice, la tendresse, l'amour, la patience,
le soutien, l'aide et les encouragements sont le secret de ma réussite.
Sans eux, je ne serais pas ce que je suis aujourd'hui. Je dédie ce travail également
À mon frère et mes Sœurs pour leurs soutiens, leurs aides, leurs encouragements.
À toute ma famille.
À tous mes enseignants, du primaire au niveau supérieur.
À tous mes amis.

***SOUALHI Mohamed***

# Table des matières

*Résumé* ..... *vii*

*Liste des abréviations* ..... *viii*

*Introduction General* ..... *1*

*I. Chapitre I : LA BIOMETRIE* ..... *3*

**I.1 Introduction** ..... **4**

**I.2 La biométrie** ..... **4**

**I.3 Les caractéristiques biométriques** ..... **5**

**I.4 Architecture d'un système biométrique** ..... **9**

**I.5 Les modèles biométriques** ..... **10**

**I.6 Modes de fonctionnement d'un système biométrique** ..... **11**

I.6.1 Le mode enrôlement ..... 11

I.6.2 Le mode authentification ..... 12

I.6.3 Le mode identification ..... 13

**I.7 Utilisation de la biométrie** ..... **14**

**I.8 Evaluation des systèmes biométriques** ..... **15**

**I.9 Les techniques biométriques** ..... **16**

**I.10 Description des principales techniques biométriques** ..... **17**

**I.11 Mesure de la performance d'un système biométrique** ..... **19**

**I.12 Comparaison des différentes techniques biométriques actuelles** ..... **22**

**I.13 Les modalité** ..... **25**

**I.14 Conclusion** ..... **27**

*II. Chapitre II : La Reconnaissance des Empreintes Digitales* ..... *28*

**II.1 Introduction** ..... **29**

**II.2 Reconnaissance biométrique par empreinte digitale** ..... **29**

II.2.1 Caractéristique d'empreinte digitale ..... 29

II.2.2 Représentation de l'image d'empreinte et prise de décision ..... 32

II.2.2.1 Image ..... 33

II.2.2.2 Représentation en minuties ..... 33

II.2.2.3 Les descripteurs de texture ..... 34

II.2.3 Propriétés des images d'empreintes digitales ..... 35

II.2.4 Extraction des caractéristiques ..... 37

II.2.5 Travaux antérieurs ..... 37

II.2.5.1 Les approches de binarisation ..... 37

II.2.5.2 Les approches d'extraction à partir de l'image en niveau de gris ..... 39

II.2.6 Les problèmes rencontrés lors de l'extraction des minuties ..... 40

**II.3 Travaux existants sur la reconnaissance par empreinte digitale ..... 41**
II.3.1 Analyse de l'existant ..... 42
**II.4 Conclusion ..... 45**
***III. Chapitre : Reconnaissance d'empreintes digitales basé sur l'extraction des minuties 46***
**III.1 Introduction ..... 47**
**III.2 Le système de vérification d'empreinte digitale proposé ..... 47**
III.2.1 Etape de prétraitement ..... 49
III.2.2 Extraction de la Région d'intérêt ..... 49
III.2.3 Extraction de caractéristiques d'empreinte digitale ..... 50
III.2.3.1 Extraction de minuties basée sur l'image binaire ..... 50
III.2.3.2 Estimation spatiale de la carte directionnelle de l'image ..... 52
III.2.3.3 Le calcul de la direction locale d'un pixel ..... 53
III.2.3.4 Le lissage de la carte directionnelle ..... 53
**III.3 Représentation des minuties ..... 55**
**III.4 Enregistrement ..... 56**
**III.5 Etape de comparaison d'empreinte digitale ..... 59**
**III.6 Résultats expérimentaux ..... 60**
III.6.1 Base de données ..... 60
III.6.2 Critères d'évaluation ..... 61
III.6.3 Évaluation du système ..... 62
**III.7 Conclusion ..... 63**
***Conclusion générale ..... 64***
***Références ..... 65***

# Liste des figures

Figure I-1 : Evolution du marché international de la biométrie [2]. 4
Figure I-2: Exemples de différentes caractéristiques biométriques : 7
Figure I-3: Architecture générique d'un système biométrique (extrait de l'Organisation Internationale de Normalisation ISO/IEC 19795-1 10
Figure I-4: Enrôlement d'une personne dans un système biométrique [6]. 11
Figure I-5: Authentification d'un individu dans un système biométrique [6]. 12
Figure I-6: Identification d'un individu dans un système biométrique [6]. 13
Figure I-7: Parts de marché des techniques biométriques en 2009 [7]. 14
Figure I-8: Aspects d'évaluation des systèmes biométriques [10]. 16
Figure I-9: Exemples de différents capteurs biométriques concernant : 19
Figure I-10: Courbe ROC. 20
Figure I-11: Courbes CMS. 22
Figure I-12: Comparaison des différentes méthodes biométriques. 23
Figure II-1 : Exemple d'empreinte digitale. 30
Figure II-2: Les différents types d'empreintes 30
Figure II-3: Exemple de quatre familles de crêtes. 31
Figure II-4: Les points singuliers. 32
Figure II-5 : Les caractéristiques principales des minuties. (a)terminant, (b) bifurcation. 34
Figure II-6: Exemple d'une représentation d'une empreinte par sa carte de minuties. 34
Figure II-7: Projection des crêtes sur une image orientée. 36
Figure II-8: Quelques minuties sur une image d'empreinte. **Erreur ! Signet non défini.**
Figure II-9: Extraction des minuties par binaraisation. 39
Figure II-10: Des images de différentes qualités. 41
Figure II-11 : Différents types de minuties 42
Figure III-1: Démarche générale du système de vérification par empreinte digitale proposé 48
Figure III-2: Exemple d'une empreinte digitale prétraitée (a) l'image originale, (b) l'image rehaussée 49
Figure III-3: localisons zone autour de l'image réorientée. 50
Figure III-4: 3×3 région. 51
Figure III-5: a) image niveau de gris originale. b), point de bifurcations et de fin de crête. 52
Figure III-6: Exemples de carte directionnelle sur des images. 54
Figure III-7: Processus généraux pour correspondance d'empreinte digitale à base de détails. 55
Figure III-8: Les points Minutai de 2 empreintes différentes sont mappés après l'enregistrement, les cercles gris représentant des paires avec des contraintes confirmées (équations 7 à 9). 59
Figure III-9: comparaison les minutai de deux empreints 60
Figure III-10: Représentation graphique des performances d'un système FAR et FRR, 62
Figure III-11: Courbe ROC. 63

# Liste des tableaux

Tableau I-1: Comparaison des modalités biométriques selon les propriétés 8
Tableau I-2: Avantages et inconvénients des différentes technologies biométriques. 24
Tableau I-3: Comparaison des 4 grandes modalités biométriques. 25
Tableau 4 II-1 : Tableau comparatif de quelques systèmes de reconnaissance par empreinte digitale. 43

# ملخص

**التعرف على بصمات الأصابع هو تقنية بيومترية ناضجة لأي تطبيق لتحديد الأفراد أو التحقق منهم. في هذا العمل، نحن نصف تطور نظام التعرف على بصمات الأصابع. في الوقت الحاضر، التعرف على بصمات الأصابع هو الأسلوب البيومتري الأكثر استخداما ونجاحا. وتتكون بصمات الأصابع من خطوط موازية ذات نقاط مفردة (مينوتياي) وتشكل نمطا فريدا وعالميا ودائما. نحن هنا نقوم بتطوير طريقة تقوم على استخراج مينوتياي من بصمات الأصابع.**



**الكلمات المفتاحية: الأصابع بصمات ,بيومترية , استخراج مينوتياي**



# Résumé

La reconnaissance des empreintes digitales est une technique biométrique mature pour toute application d'identification ou de vérification des individus. Dans ce travail, nous décrivons le développement d'un système de reconnaissance d'empreintes digitales. À l'heure actuelle, la reconnaissance de l'empreinte digitale est la méthode biométrique la plus utilisée et réussie. Les empreintes digitales sont composées de lignes parallèles avec des points singuliers (minuties) et constituent un motif unique, universel et permanent. Nous développons une méthode basée sur l'extraction minutieuse des empreintes digitales.



**Mots clés :** empreinte digitale, biométrique, extraction minutieuse.

# Abstract

Fingerprint recognition is a mature biometric technique for any application of identification or verification of individuals. In this work, we describe development of a fingerprint recognition system. At present, fingerprint recognition is the most widely used and successful biometric method. The fingerprints are composed of parallel lines with singular points (minutiae) and constitute a unique, universal and permanent pattern. We develop a method based on minutiae extraction of fingerprints



**Keywords:** Fingerprint, biometric, minutiae extraction.


# Liste des abréviations

**RED** : Reconnaissance des empreintes digitales
**FPRC** : Fingerprint Recognition system (système de Reconnaissance des empreintes digitale).
**SVM** : Support Vector Machine (Machine à Vecteurs de Support).
**MLP** : Multi layer perception.
**NER** : Nombre des empreintes reconnus.
**FAR** : False Accepted Rate.
**FRR** : False Rejected Rate .
**ERR :** Error Rejected Rat.
**SS** :Un Score de Similitude.
**FTA** : Taux d'échec à l'acquisition.
**courbe ROC** :**R**eceiver **O**perating **C**haracteristic

# *Introduction General*

La biométrie est un terme dont on entend de plus en plus parler dans la vie de tous les jours. La biométrie n'est pas vraiment récente, son apparition remonte au 19ème siècle, avec les premières études alors appelées anthropométrie.

Les empreintes digitales sont utilisées pour l'identification des personnes par la police. Cette utilisation policière n'a d'ailleurs jamais été abandonnée, et les empreintes digitales sont toujours utilisées (aujourd'hui de manière automatique avec les traitements informatiques) pour l'identification criminelle.

La biométrie souffre d'ailleurs un peu de cette image policière et a du mal à se faire accepter par le grand public pour d'autres types d'applications. Cela dit, aujourd'hui la biométrie n'est plus limitée aux empreintes digitales et à l'identification criminelle. De nombreuses modalités sont aujourd'hui utilisées pour des applications de contrôle d'accès à des locaux ou à des objets personnels. On peut citer le visage, la voix, la signature, l'iris ou la forme de la main, et d'autres encore sont à l'étude comme la démarche, la forme de l'oreille ou la dynamique de frappe au clavier et articulations des doigts.

L'objet de ce mémoire est le développement d'un système de reconnaissance d'empreintes digitales. Le travail effectué fait appel principalement à des techniques de traitement d'images (filtrage, extraction des caractéristiques d'une image, comparaison). Ce mémoire est structuré en trois chapitres.

Dans le premier chapitre, nous introduirons la notion de biométrie et les applications qui en découlent. Nous insisterons plus particulièrement sur l'utilisation des empreintes digitales dans les systèmes d'identification de personnes.

Nous proposons dans le deuxième chapitre un panorama sur les systèmes de Reconnaissances des Empreintes Digitales. Nous montrons que ces systèmes atteignent actuellement des performances satisfaisantes, notamment grâce aux progrès réalisés ces dernières années.

Le troisième chapitre sera consacré tout d'abord au traitement de l'image filtrée permettant l'extraction de l'information utile à l'identification d'une personne. Puis la vérification de deux empreintes sera détaillée. La méthode utilisée pour les tests ainsi que les résultats similarité obtenus seront décrits.

# I. Chapitre I : LA BIOMETRIE

# I.1 Introduction

Dans ce chapitre nous commencerons par présenter la biométrie de manière générale ainsi que les diverses applications qui en découlent, en insistant plus particulièrement sur l'utilisation des empreintes digitales. Puis nous détaillerons les différentes étapes composant un système complet de reconnaissance d'empreintes.

# I.2 La biométrie

Depuis quelques décennies l'explosion de l'informatique et des réseaux de communication a fait augmenter de manière significative le besoin d'identification des personnes. Jusqu'à présent les méthodes usuelles d'identification sont basées sur ce que l'on possède (carte d'identité, carte à puce, badge magnétique) ou sur ce que l'on sait (mot de passe, code PIN) mais ces méthodes posent de gros problèmes de fiabilité (falsification de document, oubli de son code, décryptage du mot de passe via des logiciels spécifiques). Depuis les récents actes terroristes et les menaces qui pèsent sur de nombreux pays, une identification fiable des personnes est devenue un problème majeur pour des raisons de sécurité (contrôle aux frontières, accès aux lieux publics, transport). Tous ces problèmes ont ainsi provoqué un développement accru des techniques biométriques d'identification **[1]** comme en témoigne l'étude des perspectives du marché de la biométrie (Figure I-1).

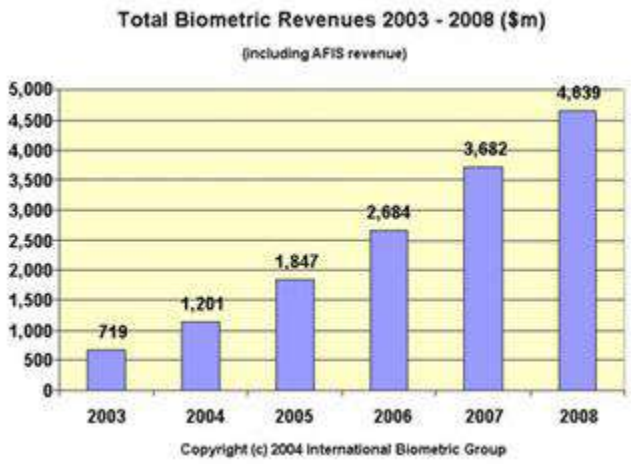



*Figure I-1 : Evolution du marché international de la biométrie [2].*

La biométrie consiste en l'analyse mathématique des caractéristiques biologiques d'une personne et a pour objectif de déterminer son identité de manière irréfutable. Contrairement à *ce que l'on sait* ou *ce que l'on possède* la biométrie est basée sur *ce que l'on est* et permet ainsi d'éviter la duplication, le vol, l'oubli ou la perte. Les caractéristiques utilisées doivent être *universelles* (c'est-à-dire communes à tous les individus), *uniques* (pour pouvoir différencier deux individus) et *permanentes* (c'est-à-dire invariantes dans le temps pour chaque individu).

Il existe deux types de systèmes de reconnaissance biométrique : ceux basés sur la *vérification* et ceux basés sur l'*identification*. La vérification, également appelée authentification, consiste à confirmer ou infirmer l'identité d'une personne (suis-je celui que je prétends être ?).

Il s'agit d'une comparaison du type *''un contre un'' ;* les caractéristiques de l'individu sont comparées à celles présentes dans un enregistrement de référence. Quant à l'identification elle permet d'établir l'identité d'une personne (qui suis-je ?) à partir d'une base de données, il s'agit d'une comparaison du type *"un contre plusieurs"*.

L'application qui vient immédiatement à l'esprit est l'utilisation des empreintes digitales par les forces de l'ordre pour ficher les criminels. A titre d'exemple le FBI possèderait une base de données de 250 millions d'empreintes.

Outre l'utilisation policière la biométrie apporte des solutions dans de nombreuses applications telles que le contrôle d'accès à un lieu physique (aéroport, gare), la surveillance (systèmes de vidéosurveillance des rues, contrôle des détenus dans les prisons), le contrôle d'accès à un espace virtuel (e.g. accès à un réseau local pour éviter la fraude par mot de passe), le paiement en ligne (pour sécuriser la transaction) [1].

## I.3 Les caractéristiques biométriques

Les caractéristiques biométriques par lesquelles il est possible de vérifier l'identité d'un individu sont appelées modalités biométriques. La figure I.2 illustre un exemple de quelques modalités biométriques. Ces modalités sont basées sur l'analyse des données liées à l'individu et sont généralement classées en trois catégories biométrie biologique, comportementale et morphologique. La biométrie biologique se base sur l'analyse des

données biologiques liées à l'individu (salive, ADN, etc.). La biométrie comportementale se base sur l'analyse de comportements d'un individu (manière de marcher, dynamique de frappe au clavier, etc.) La biométrie morphologique se base sur les traits physiques particuliers qui, pour toutes personnes, sont permanents et uniques (empreinte digitale, visage, etc.). Pratiquement, n'importe quelle Caractéristique morphologique ou comportementale peut être considérée comme une caractéristique biométrique, dans la mesure où elle satisfait les propriétés suivantes [3] :

– Universalité : toutes les personnes à identifier doivent la posséder ;

– Unicité : l'information doit être aussi dissimilaire que possible entre les différentes personnes ;

– Permanence : l'information collectée doit être présente pendant toute la vie d'un individu ;

– Collectabilité : l'information doit être collectable et mesurable afin d'être utilisée pour les comparaisons ;

– Acceptabilité : le système doit respecter certains critères (facilite d'acquisition, rapidité, etc.) Afin d'être employé.

Les caractéristiques biométriques ne possèdent pas toutes ces propriétés, ou les possèdent mais à des degrés différents. Le tableau 1.1, extrait de [4], compare les principales modalités biométriques selon les propriétés suivantes : universalité, unicité, permanence, collectabilité, acceptabilité et performance. Ce tableau montre qu'aucune caractéristique n'est donc idéale et qu'elles peuvent être plus ou moins adaptées à des applications particulières. Par exemple, l'analyse basée sur l'ADN est une des techniques les plus efficaces pour vérifier l'identité d'un individu ou l'identifier [5]. Néanmoins, elle ne peut pas être utilisée pour le contrôle d'accès logique ou physique pour des raisons de temps de calcul, mais aussi, parce que personne ne serait prêt à donner un peu de sang pour faire la vérification. Le choix de la modalité ainsi effectué selon un compromis entre la présence ou l'absence de certaines de ces propriétés selon les besoins de chaque application. À noter que le choix de la modalité biométrique peut aussi d´éprendre de la culture locale des usagers. En Asie, les méthodes nécessitant un contact physique comme les empreintes digitales sont rejetées pour des raisons d'hygiène alors que les méthodes sans contact sont plus répandues et acceptées



(a)



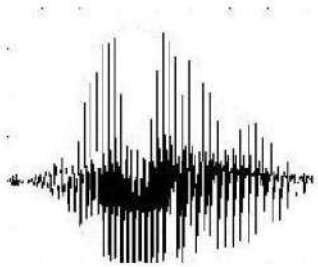
(b)



(d)



(e)



(e)



(f)

Figure I-2: Exemples de différentes caractéristiques biométriques :

Empreinte digitale (a), visage (b), main (c), iris (d), empreinte vocale (e), signature (f)

Suivantes : (U) Universalité, (N) Unicité, (P) Permanence, (C) Collectait´, (A) Acceptabilité et (E) Performance. Pour la performance, le nombre d'étoiles est relié à la valeur du taux d'égale erreur (EER) obtenue dans l'état de l'art [4].

| Information | U | N | P | C | A | E |
|---|---|---|---|---|---|---|
| ADN | Oui | Oui | Oui | Faible | Faible | ***** |
| Sang | Oui | Non | Oui | Faible | Non | * |
| démarche | Oui | Non | Faible | Oui | Oui | *** |
| Dynamique de frappe | Oui | Oui | Faible | Oui | Oui | **** |
| Voix | Oui | Oui | Faible | Oui | Oui | **** |
| Iris | Oui | Oui | Oui | Oui | Faible | ***** |
| Rétine | Oui | Oui | Oui | Oui | Faible | ***** |
| Visage | Oui | Non | Faible | Oui | Oui | **** |
| Géométrie de la main | Oui | Non | Oui | Oui | Oui | **** |
| Oreille | Oui | Oui | Oui | Oui | Oui | ***** |
| Empreinte digitale | Oui | Oui | Oui | Oui | Moyenne | **** |

Tableau I-1: Comparaison des modalités biométriques selon les propriétés

## I.4 Architecture d'un système biométrique

L'architecture d'un système biométrique contient cinq modules comme le montre la Figure I-3 :

– Le module de capture qui consiste à acquérir les données biométriques afin d'extraire une représentation numérique. Cette représentation est ensuite utilisée pour l'enrôlement, la vérification ou l'identification. Il s'agit d'un capteur biométrique qui peut être de type sans ou avec contact ;

– Le module de traitement du signal qui permet de réduire la représentation numérique extraite afin d'optimiser la quantité de données à stocker lors de la phase d'enrôlement, ou pour faciliter le temps de traitement pendant la phase de vérification et l'identification. Ce module peut avoir un test de qualité pour contrôler les données biométriques acquises ;

– Le module du stockage qui contient les modèles biométriques des utilisateurs enrôles du système ;

– Le module de similarité qui compare les données biométriques extraites par le module d'extraction de caractéristiques `à un ou plusieurs modèles préalablement enregistrés. Ce module d´détermine ainsi le degré de similarité (ou de divergence) entre deux vecteurs biométriques ;

– Le module de décision qui détermine si l'indice de similarité retourné est suffisant pour déterminer l'identité d'un individu.

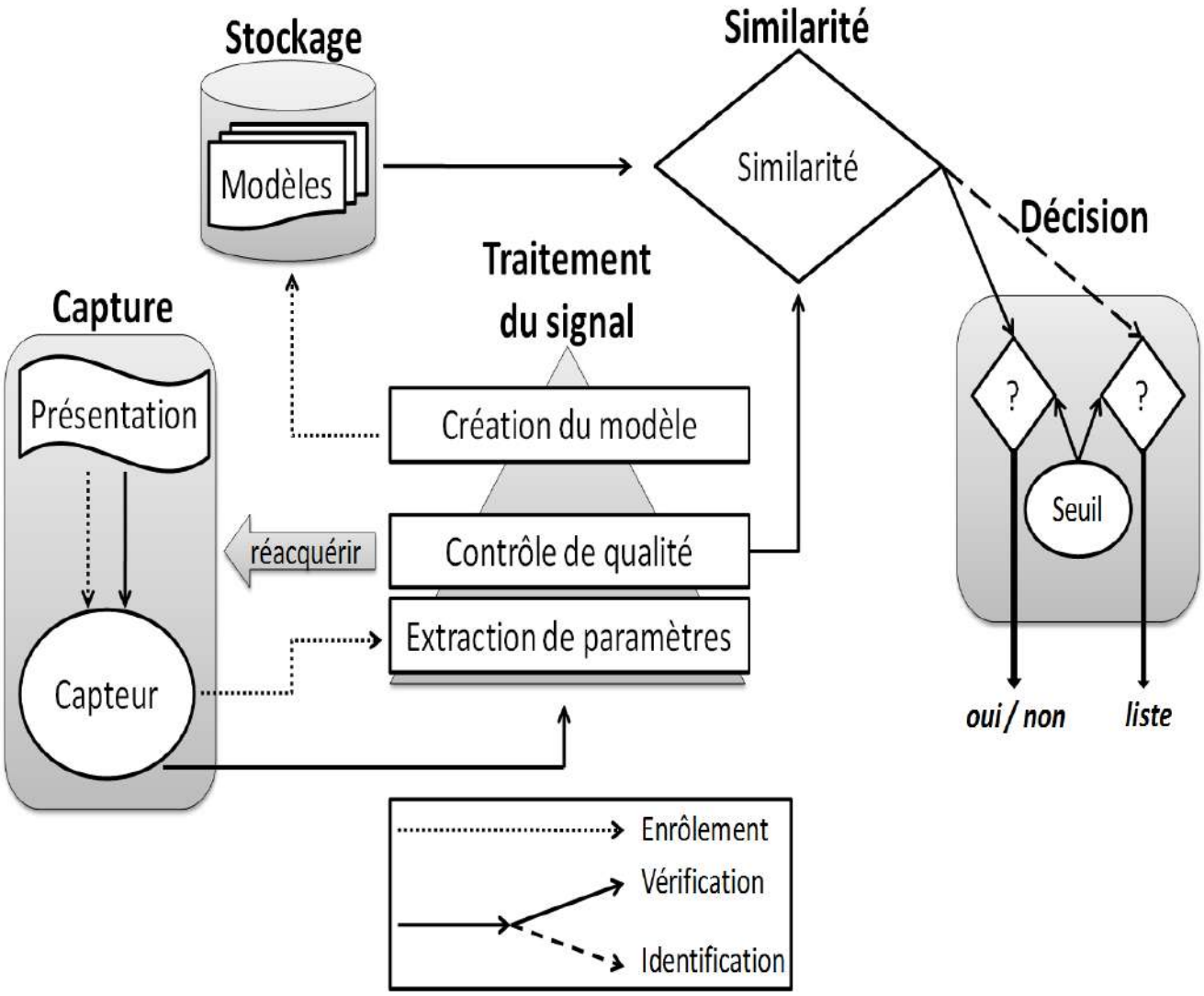



Figure I-3: Architecture générique d'un système biométrique *(extrait de l'Organisation Internationale de Normalisation ISO/IEC 19795-1*

## I.5 Les modèles biométriques

Un modèle biométrique (appelé aussi gabarit ou Template) est l'ensemble des données utilisées pour représenter un utilisateur. Les caractéristiques biométriques acquises ne sont pas enregistrées et utilisées telles quelles. Une phase de traitement est effectuée pour réduire les données biométriques brutes et produire ainsi le modèle biométrique. La Figure I-3 illustre quelques exemples de modèles biométriques. Pour le stockage de ces modèles, il existe quatre emplacements principaux que sont la clé USB, la base centralisée, la machine individuelle de travail et le capteur biométrique.

Chacun de ces emplacements présente des avantages et faiblesses en termes de temps de traitement, confidentialité et respect de la vie privée.

## I.6 Modes de fonctionnement d'un système biométrique

Les systèmes biométriques peuvent fournir trois modes de fonctionnement, à savoir, l'enrôlement, l'authentification (ou vérification) et l'identification. Dans ce qui suit, les figures illustreront l'exemple d'un système biométrique utilisant l'empreinte digitale comme modalité.

### I.6.1 Le mode enrôlement

C'est la première phase de tout système biométrique, pendant laquelle les caractéristiques biométriques d'un individu sont enregistrées dans la base de données pour la première fois. Cet enregistrement est parfois accompagné de référence biographique correspond à cette personne comme le nom, le prénom, etc. qui sera utilisée plus tard dans la phase d'authentification. Pendant l'enrôlement on extrait des caractéristiques biométriques en utilisant des algorithmes adéquats, ces caractéristiques seront réduites par la suite pour minimiser la quantité de données à stockée en facilitant ainsi la vérification et l'identification [6].

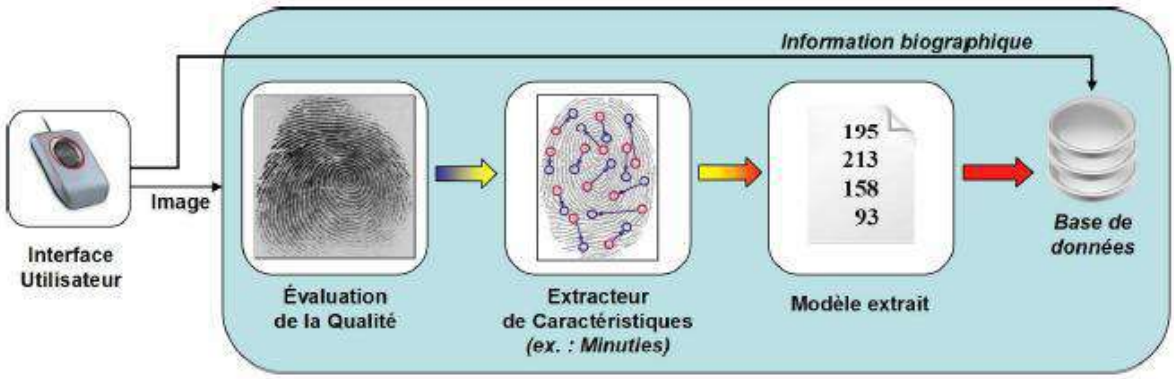



Figure I-4: Enrôlement d'une personne dans un système biométrique [6].

## I.6.2 Le mode authentification

L'utilisateur affirme son identité et le système vérifie si cette affirmation est valide ou non (Figure I-5).

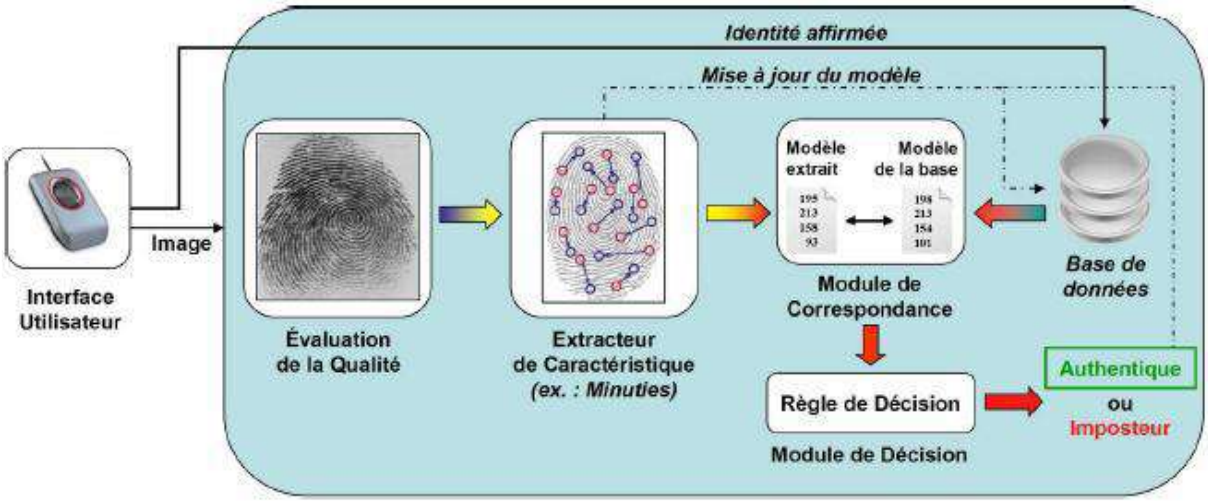



Figure I-5: Authentification d'un individu dans un système biométrique [6].

Pour illustrer ce principe, prenons la situation où un utilisateur (*M. X*) souhaite retirer de l'argent à un distributeur de billets en entrant son code personnel d'identification (code PIN) et en présentant une modalité biométrique. Le système acquiert alors les données biométriques et va les comparer uniquement avec le modèle enregistré correspondant à *M. X*. On parle alors de correspondance 1:1. Ainsi, si l'entrée biométrique de l'utilisateur et le modèle enregistré dans la base de données correspondant à l'identité affirmée possèdent un degré de similitude élevé, l'affirmation est validée et l'utilisateur est considéré comme étant un authentique. Dans le cas contraire, l'affirmation est rejetée et l'utilisateur est considéré comme étant un imposteur. En résumé, un système biométrique opérant en mode vérification répond à la question "*Suis-je bien M. X ?*".

## I.6.3 Le mode identification

L'utilisateur ne dévoile pas explicitement son identité (Figure I-6) Cependant, l'affirmation implicite faite par l'utilisateur est qu'elle est une des personnes déjà enrôlées par le système. Ainsi, l'échantillon biométrique de l'individu est comparé avec les modèles de toutes les personnes de la base de données. On parle alors de correspondance 1 : N. La sortie du système biométrique est constituée par l'identité de la personne dont le modèle possède le degré de similitude le plus élevé avec l'échantillon biométrique présenté en entrée. Typiquement, si la plus grande similarité entre l'échantillon et tous les modèles est inférieure à un seuil de sécurité minimum fixé, la personne est rejetée, ce qui implique que l'utilisateur n'était pas une des personnes enrôlées par le système. Dans le cas contraire, la personne est acceptée.

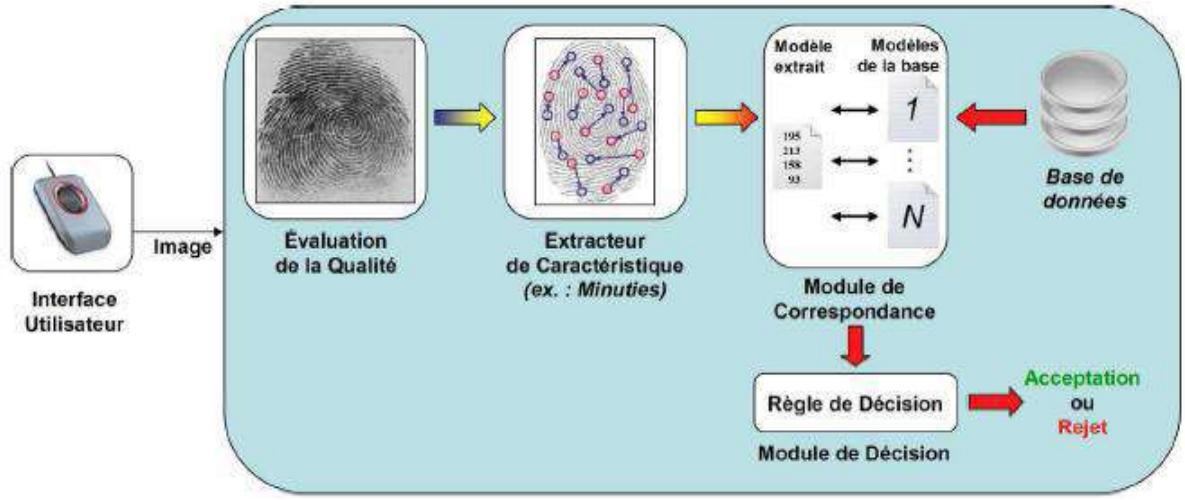



Figure I-6: Identification d'un individu dans un système biométrique [6].

Un exemple de système opérant en mode identification serait l'accès à un bâtiment sécurisé : tous les utilisateurs qui sont autorisés à entrer dans le bâtiment sont enrôlés par le système ; lorsqu'un individu essaye de pénétrer dans le bâtiment, il doit d'abord présenter ses données biométriques au système et, selon la détermination de l'identité de l'utilisateur, le système lui accorde le droit d'entrée ou non. En résumé, un système biométrique opérant en mode identification répond à la question *"Suis-je bien connu du système ?"*.

# I.7 Utilisation de la biométrie

Le champ d'application de la biométrie est très vaste. En effet, tous les domaines qui nécessitent de vérifier ou déterminer l'identité de personnes sont concernés. On retrouve ainsi des applications de la biométrie pour gérer l'accès à des ressources physiques (comme l'accès à des lieux sécurisés) et logiques (comme le commerce électronique).
La biométrie intéresse aussi plusieurs pays (l'Europe, les Etats-Unis, etc.) afin de produire des titres d'identité plus sûrs, telle que la carte nationale d'identité ou le passeport biométrique. A noter qu'en France, le passeport biométrique est désormais d´éployé. Il intègre une puce RFID qui contient au moins deux informations biométriques : une empreinte digitale et une image du visage numérisée. Enfin, la biométrie n'a pas que des applications à vocation sécuritaire, mais également des applications qui facilitent le quotidien des usagers. Ainsi, la biométrie est utilisée dans certains aéroports permettant aux clients réguliers de ne pas perdre de temps lors de l'embarquement. La Figure I-7, réalisée d'après les chiffres d'International Biometric Group, montre les parts de marché des principales méthodes biométriques en 2009 [7]. Les empreintes digitales sont toujours les plus utilisées, suivies par la reconnaissance faciale. Ces deux modalités représentent les trois quarts du marché de la biométrie.

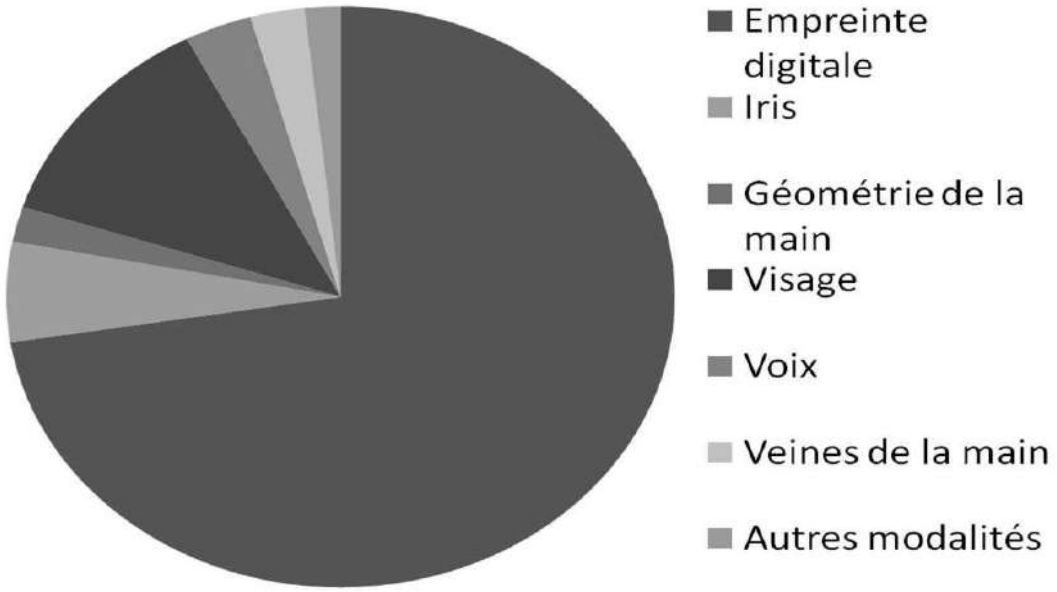



Figure I-7: Parts de marché des techniques biométriques en 2009 [7].

## I.8 Evaluation des systèmes biométriques

L'évaluation des systèmes biométriques a pour objectif d'en diminuer les limitations vues dans la section I.5. L'évaluation de ces systèmes est généralement réalisée selon trois aspects d'évaluation comme le montre la Figure I-8 :

1. La performance qui mesure l'efficacité d'un système biométrique en termes d'erreur tel que le taux d'échec à l'acquisition (FTA : Taux d'échec à l'acquisition) [8] ;
2. L'usage qui mesure l'acceptabilité et la satisfaction des utilisateurs lors de l'utilisation de systèmes biométriques ;
3. La sécurité qui mesure la robustesse d'un système biométrique (capteur et algorithmes) contre la fraude.

L'évaluation des systèmes biométriques est un enjeu majeur en biométrie pour plusieurs raisons. Premièrement, elle permet d'offrir aux chercheurs et aux développeurs un outil pour mieux tester et évaluer leurs systèmes avec ceux qui existent dans l'état de l'art. Deuxièmement, elle permet de prendre en considération le comportement des utilisateurs durant le processus d'évaluation, ce qui permet de mieux comprendre leur besoin et mieux déployer cette technologie dans notre vie quotidienne. Enfin, elle permet d'identifier, pour chaque système, les applications industrielles en se basant sur divers critères que sont la performance, l'usage, la sécurité et le coût de déploiement de la technologie.

En biométrie, les travaux liés à la qualité, l'usage et la sécurité sont beaucoup moins nombreux que ceux liés à la performance. L'Organisation Internationale de Normalisation ISO/IEC 19795-1 [8] à proposer plusieurs métriques pour évaluer et comparer la performance des systèmes biométriques. Ainsi, nous avons choisi d'axer cet aspect d'évaluation sur l'évaluation de la qualité de données biométriques.

Une telle évaluation est utile pour améliorer la performance globale des systèmes biométriques. Ce type d'information pourra également être exploité dans les approches multimodales ou pour évaluer les capteurs biométriques [9] [10].

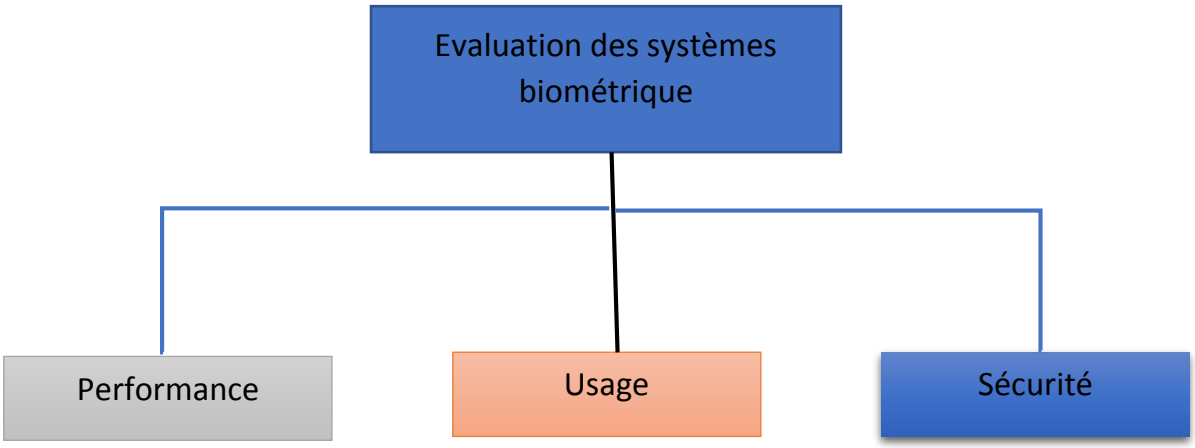



Figure I-8: Aspects d'évaluation des systèmes biométriques [10].

## I.9 Les techniques biométriques

Les techniques biométriques sont actuellement utilisées pour les applications de sécurité. Chacune a des avantages et des inconvénients, le choix d'une technique se fait en fonction de l'application. La figure I.1 montre quelques techniques biométriques. Les modalités biométriques peuvent être classées en trois catégories :

- Les modalités qui reposent sur l'analyse de traces biologiques (odeur, sang, ADN,…) ;
- Les modalités morphologiques qui utilisent une partie du corps humain tels que l'empreinte digitale, l'iris, etc.
- Les modalités comportementales utilisent un trait personnel du comportement, tels que la signature, la démarche, etc.

Les modalités morphologiques sont les plus utilisées par rapport aux modalités comportementales. Cela est dû à leur stabilité dans le temps et la difficulté de falsification de ces modalités. De plus, les modalités comportementales sont, généralement, affectées par l'état moral des individus.

Les techniques biométriques se divisent en deux groupes selon la coopération ou non de l'individu :

**1. Techniques intrusives :** Ces techniques requièrent un contact physique avec l'individu pour l'identifier, tel que les empreintes digitales, la rétine, iris ou la forme de la main. Leur usage est généralement mal accepté.

**2. Techniques non intrusives :** Ces techniques ne requièrent pas la coopération de l'individu en question leur application peut se faire à distance en utilisant des capteurs qui ne nécessitent pas de contact directe avec l'utilisateur (visage, démarche,…).

## I.10 Description des principales techniques biométriques

***L'empreinte digitale* :** l'empreinte digitale est le modèle de relief cutané des doigts. L'identification par cette caractéristique est la technique la plus anciennement utilisée. En fait, c'était toujours le choix biométrique évident pour les services de police depuis plus de 100 ans, c'est pour cela qu'elle est généralement mal acceptée par les utilisateurs en raison de l'alignement fort avec la criminologie. Il existe plusieurs types de système de capture d'empreinte digitale : optique, thermique, électromagnétique et ultrasons [11].

***Le visage* :** le visage est le moyen le plus naturel pour identifier les personnes, ce qui explique pourquoi cette caractéristique est bien acceptée par les utilisateurs. L'image de visage peut être captée par une caméra numérique, ou un appareil photo. Plusieurs recherches sont effectuées, pendant 25 ans [12], [13] pour améliorer la performance de ce genre de système cependant de nombreux problèmes se posent.

***La géométrie de la main*** : cette modalité consiste à analyser la forme de la main sa longueur, sa largeur, son hauteur, la courbure des doigts etc. Cette technique est récente, simple, et bien acceptée par les utilisateurs qui suivent des guides des capteurs (LEDs infrarouge, des appareils photos numériques) pour qu'ils bien positionner leurs doigts, ce qui rende ainsi la détection / la segmentation plus aisée, cependant ce genre de système peut être trompé par de vrais jumeau ou même par des personnes ayant des formes de la main proches.

***L'iris*** : l'iris est la région annulaire située entre la pupille et le blanc de l'œil. La biométrie par ce trait est la plus récente, et la plus fiable, selon les estimations de Daugmann1 La probabilité de trouver 2 iris suffisamment identiques est 1 sur 10^**72**

environ. L'image de l'iris est capturée par une caméra standard contraignantes (exemple la distance entre la camera et l'iris ne dépasse pas un mètre), ce qui limite l'utilisation de cette modalité.

***La rétine*** : la rétine est la couche sensorielle de l'œil qui permet la vision, cette zone est parcouru par des vaisseaux sanguins dont leurs positions est inchangeable durant toute la vie de la personne. L'identification de la rétine n'est pas récente, elle remonte aux années 30. Cette technologie est la plus fiable toutefois elle est mal acceptée par les utilisateurs à cause des contraintes de l'acquisition.

***La voix*** **:** la reconnaissance de la voix est une biométrie comportementale n'exige aucun contact physique avec le lecteur de système. En 1962 Lawrence Kersta [14] a prouvé que la voix de chaque personne est unique et qu'il est possible de la présenter graphiquement. Il existe deux principales méthodes de traitements de ce trait biométrique, la première dépend de texte prononcé, et la deuxième (la plus difficile) est indépendante de texte. Bien que cette modalité ne nécessite pas de matériel cher (microphone par exemple), cependant le bruit ambiant et les propriétés acoustiques telles que la réflexivité et l'absorption influencent la vérification de la voix en réduisant ainsi son utilisation.

***La démarche*** **:** la démarche est l'une des biométries comportementale. Elle consiste à identifier les individus par leurs manières de marché, qui est supposée (presque) unique pour chaque individu. Deux types de techniques d'identification de ce trait peuvent être distingués, l'approche "*Model-based"* qui dépend de quelques paramètres comme la longueur des parties du corps, la longueur de pas, la jointure d'angle etc. et l'approche "*appearance-based"* qui analyse directement l'image en extrayant les caractéristiques. L'avantage de cette biométrie consiste dans le fait qu'on peut identifier la personne à distance, cependant l'exécution d'un tel système est particulièrement difficile.

***La signature*** : la vérification par la signature est l'une des premières méthodes utilisées dans le domaine de la biométrie. Les systèmes de reconnaissance de l'écriture analysent soit la géométrie de la signature (mode statique), soit ses caractéristiques spécifiques comme la vitesse, la pression sur le crayon, ce mode qui s'appelle le mode dynamique est le plus discriminant. La capture se fait à l'aide d'une tablette graphique. Bien que la

signature soit bien acceptée par les utilisateurs, sa variabilité (à cause de l'état de santé ou l'état émotionnel de l'individu) pose un grand problème.

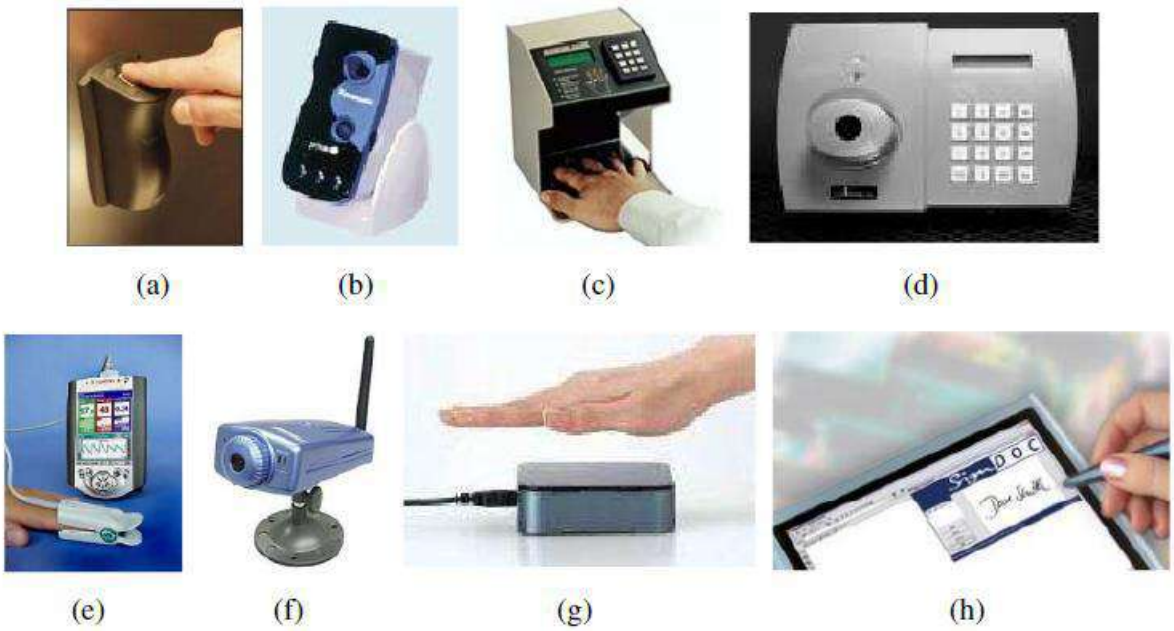



Figure I-9: Exemples de différents capteurs biométriques concernant :

(a) l'empreinte digitale, (b) l'iris, (c) la géométrie de la main, (d) la rétine, (e) la pulsation cardiaque, (f) le visage, (g) la thermographie de la main, et (h) la signature.

## I.11 Mesure de la performance d'un système biométrique

Tout d'abord, afin de comprendre comment déterminer la performance d'un système biométrique, il nous faut définir clairement trois critères principaux :

1. Le premier critère s'appelle le **taux de faux rejet** ("**F**alse **R**eject **R**ate" ou **FRR**). Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système ;

2. Le deuxième critère est le **taux de fausse acceptation** ("**F**alse **A**ccept **R**ate" ou **FAR**). Ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système ;

3. Le troisième critère est connu sous le nom de **taux d'égale erreur** ("**E**qual **E**rror **R**ate" ou **EER**). Ce taux est calculé à partir des deux premiers critères et constitue un point de mesure de performance courant. Ce point correspond à l'endroit où FRR = FAR, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations.

Selon la *nature* (*authentification* ou *identification*) du système biométrique, il existe deux façons d'en mesurer la performance :

– Lorsque le système opère en *mode authentification*, on utilise ce que l'on appelle une **courbe ROC** ("**R**eceiver **O**perating **C**haracteristic"). La courbe ROC (voir Figure I-10) trace le taux de faux rejet en fonction du taux de fausse acceptation. Plus cette courbe tend à épouser la forme du repère, plus le système est performant, c'est-à-dire possédant un taux de reconnaissance global élevé.

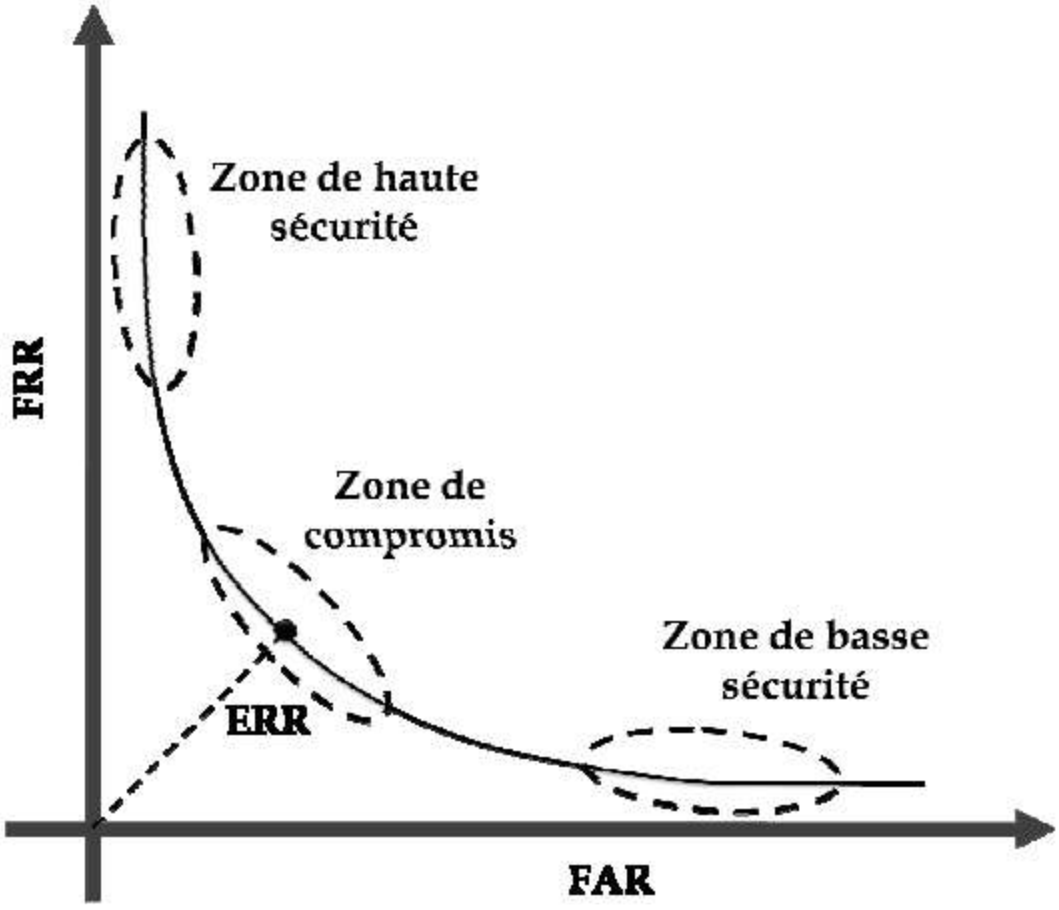



Figure I-10: Courbe ROC.

Dans le cas d'un système utilisé en *mode identification*, les applications peuvent être déployées en monde fermé (F) ou en monde ouvert (O).

**a)** ***En monde fermé :*** le taux d'identification est la mesure la plus utilisée mais il n'est pas toujours suffisant. En effet, en cas d'erreur, il peut être utile de savoir si le bon choix se trouve dans les *N* premières réponse. On trace alors ce que l'on appelle une courbe de scores cumulés CMS (pour **C**umulative **M**atch **S**core). La courbe (CMS) (voir Figure I-11) donne le pourcentage de personnes reconnues en fonction d'une variable que l'on appelle le rang. On dit qu'un système reconnaît au rang 1 lorsqu'il choisit la plus proche image comme résultat de la reconnaissance. On dit qu'un système reconnaît au rang 2, lorsqu'il choisit, parmi deux images, celle qui correspond le mieux à l'image d'entrée, etc…[15] [16].

**b)** ***En monde ouvert :*** les performances pour un système d'identification en monde ouvert sont caractérisées par deux mesures : le taux d'identification et le taux de fausse alarme. Dans le cas où l'identité recherchée se trouve dans la galerie, le taux d'identification est la fraction des images de test qui est correctement détectée et identifiée. Dans l'autre cas où l'échantillon de test n'appartient pas à une identité de la galerie, (FAR) correspond à la fraction des images de test qui est faussement détectée [15].

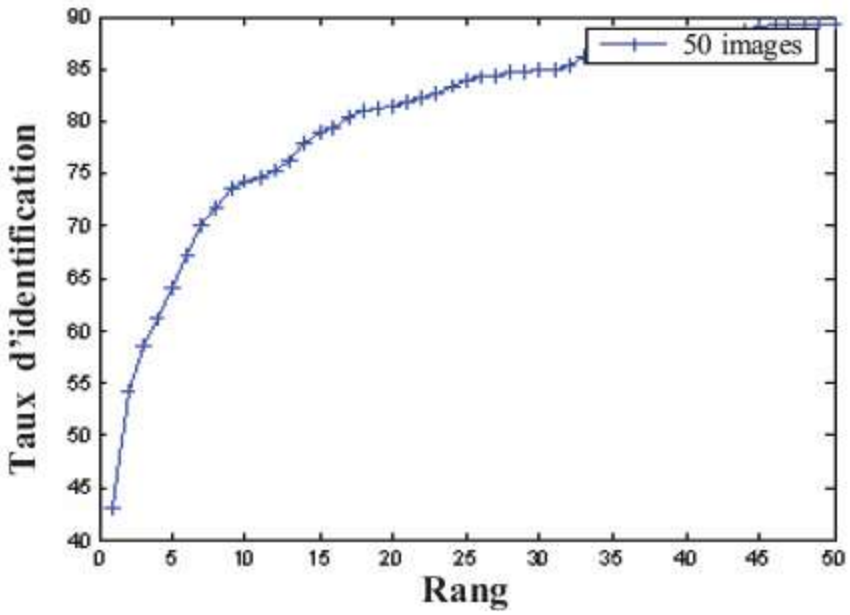



Figure I-11: Courbes CMS.

## I.12 Comparaison des différentes techniques biométriques actuelles

Malgré l'existence de plusieurs modalités biométriques, il n'y a pas de système biométrique parfait. D'une part, le Groupe International de la Biométrie IBG (*I*nternational *B*iometric *G*roup) 2 a procédé à une comparaison des différentes technologies biométriques appelée Analyse Zéphyr. Les résultats de cette comparaison sont illustrés sur la figure I.12. Cette comparaison est basée sur quatre (04) critères principaux [17] :

- ***Effort*** : effort fourni par l'utilisateur lors de l'authentification.
- ***Intrusion*** : information sur l'acceptation du système par les usagers.
- ***Coût*** : coût de la technologie (lecteurs, capteurs, etc.).
- ***Précision*** : efficacité de la méthode (liée au taux d'erreur).

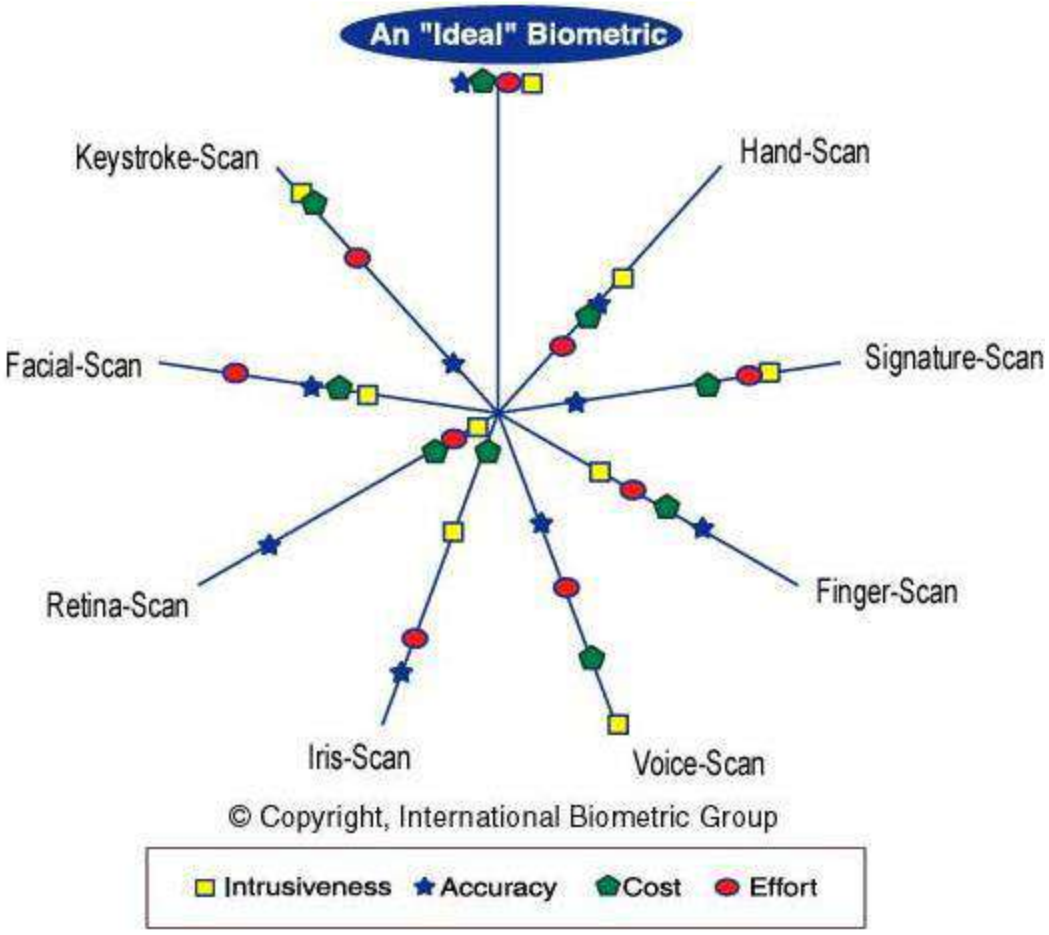



Figure I-12: Comparaison des différentes méthodes biométriques.

D'autre part, le CLUSIF (*CLU*b de la *S*écurité des *S*ystèmes d'*i*nformation *F*rançais) 3 a également proposé une autre comparaison des différentes modalités biométriques basée sur les avantages et les inconvénients de chacune. Le tableau I.2 montre le résultat global de cette comparaison.

| Technique | Avantages | Inconvénients |
|---|---|---|
| **Empreinte digitale** | Peu coûteuse ;<br>Ergonomie moyenne ;<br>Facilité d'utilisation ;<br>Petite taille du lecteur ;<br>La plus éprouvée ;<br>Traitement rapide. | Qualité optimale des appareils de mesure (fiabilité) ;<br>Acceptabilité moyenne ;<br>Possibilité d'attaques. |
| **Géométrie de la main** | Très ergonomique ;<br>Bonne acceptabilité. | Système encombrant ;<br>Coûteuse ;<br>Perturbation possible par des blessures. |
| **Visage** | Peu Coûteuse ;<br>Peu encombrant ;<br>Bonne acceptabilité. | Jumeaux identiques ;<br>Psychologie ;<br>Vulnérabilité aux attaques. |
| **Rétine** | Fiabilité ;<br>Durabilité. | Coûteuse ;<br>Acceptabilité faible. |
| **Iris** | Fiabilité.<br>Durabilité. | Coûteuse ;<br>Acceptabilité faible ;<br>Contraintes d'acquisition. |
| **Voix** | Facilité. | Vulnérabilité aux attaques. |
| **Signature** | Ergonomie. | Psychologie ;<br>Dépend de la fiabilité de la signature. |
| **Frappe au clavier** | Ergonomie. | Etat physique et psychique. |

Tableau I-2: Avantages et inconvénients des différentes technologies biométriques.

Ces deux comparaisons permettent de choisir une technologie appropriée en fonction des contraintes liées à l'application demandée. Par exemple, on remarque que l'iris et l'empreinte digitale sont les modalités les plus discriminantes. Cela est utile pour les systèmes d'identification à grande-échelle nécessitant un haut niveau de sécurité.
Parmi les indices de performance utilisés pour juger l'efficacité d'une modalité, les taux de FAR et FRR (décrits précédemment) sont utilisés (Tableau I.3) [18].

| Modalité biométrique | FAR (%) | FRR (%) |
|---|---|---|
| **Iris** | 0.00129 | 0.583 |
| **Empreinte digitale** | 0.01 | 2.54 |
| **Géométrie de la main** | 0.05 | 7.29 |
| **Visage** | 1 | 10 |

Tableau I-3: Comparaison des 4 grandes modalités biométriques.

Les caractéristiques physiques et comportementales utilisées par les modalités biométriques actuelles ne sont pas toujours fiables à 100%. Par exemple, la reconnaissance par les empreintes digitales est loin d'être si parfaite et si précise. Elle peut être attaquée par une fine couche de silicone reproduisant la géométrie et les empreintes des doigts. De même, il arrive que des utilisateurs qui n'ont pas des empreintes d'assez bonne qualité ne soient pas correctement identifiés. De plus, la qualité des empreintes peut être dégradée au cours du temps, notamment chez les personnes ayant des activités manuelles. La reconnaissance de la géométrie de la main souffre aussi de mêmes types d'inconvénients que dans le cas de la reconnaissance des empreintes digitales, notamment chez les personnes de la même famille et plus particulièrement chez les jumeaux. Pour les systèmes biométriques à reconnaissance faciale, de la voix, ou de l'iris, de nombreux problèmes liés aux attaques sont connus (e.g. conditions d'acquisition, attaque par voix enregistrée, attaque par photographie statique ou dynamique, etc.) [18].

## I.13 Les modalité

Bien qu'il existe un grand nombre des techniques de reconnaissance biométrique uni modales (utilisant une seule modalité) améliorées, cependant celles-ci souffrent de plusieurs facteurs qui dégradent leurs performances [19] tels que :

- ✓ *Le bruit* : introduit par le capteur défaillant ou mal entretenu (exemple l'accumulation de poussière sur le capteur d'empreinte digitale), il peut sérieusement compromettre la précision du système [20].
- ✓ *Non-universalité* : en fait certaines modalités ne sont pas vraiment universelles par exemple certaines personnes peuvent avoir des empreintes non enregistrables à cause d'un accident ou d'un travail manuel prolongé. Selon l'estimation de NIST (*National Institute of Standards and Technologies)* il est impossible d'obtenir une bonne qualité d'empreinte digitale pour environ 2% de la population. C'est le cas d'une personne muette avec la modalité voix, ou une personne handicapée avec la modalité signature, ou les personnes qui ont une maladie oculaire ou ayant des long cils pour la modalité iris ou rétine. Ces problèmes entraînent des erreurs d'enrôlement "*Failure to Enroll*" et/ou des erreurs de capture "*Failure to Capture*".
- ✓ *Manque d'individualité* : nous pouvons avoir une similarité des caractéristiques extraites de deux personnes différentes cela dû à des facteurs génétiques (exemple les jumeaux, les membres de la même famille, ou même les membres de la même population), ce qui affecte significativement la performance de système biométrique en augmentant le taux de fausse acceptation.
- ✓ *Manque de représentation invariante* : les caractéristiques biométriques ne sont pas invariantes ni dans leur enrôlement ni dans leur nature, c'est ainsi nous pouvons avoir deux signatures différentes correspond à la même personne. Par exemple on ne peut jamais trouver deux images du même visage strictement identiques et cela est dû au changement de pose, des expressions faciales, des conditions d'éclairage, et même de l'utilisation des capteurs différents. Ces variations à l'intérieur d'une même modalité biométrique est appelées "variation intra-classe", elles augmentent le taux de faux rejet de système biométrique.
- ✓ *Sensibilité aux attaques* : le problème du fraude et du vol semble s'éliminer par les méthodes biométriques, cependant on ne fait que les réduire. Des études [21], [22] ont montré qu'il est possible de voler une empreinte digitale

et de la produire (en utilisant par exemple la silicone), c'est le cas des modalités signature et voix qui sont faciles à falsifier.

## I.14 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 reconnaissance d'empreintes digitales basé sur l'extraction des minuties. Le chapitre Suivant est dédié aux systèmes d'acquisitions des empreintes.

# II. Chapitre II : La Reconnaissance des Empreintes Digitales

# II.1Introduction

Le traitement d'image est devenu une discipline nécessaire pour en extraire l'information et automatiser son traitement dans le but d'améliorer l'aspect visuel de l'image et d'en extraire des informations jugées pertinentes.

La Reconnaissance des Empreintes Digitales est une branche de la Biométrie la plus rependue, aussi bien dans le domaine de la sécurité publique (contrôle, enquête), que privée (accès à un bâtiment, protection de biens …..).

Les systèmes de Reconnaissances des Empreintes Digitales sont utilisés dans plusieurs applications par exemples : sécuriser l'accès à un ordinateur, et dans le domaine Anticriminels, les corps policiers utilisent l'empreinte digitale comme moyen d'identification d'une personne depuis plus de 100 ans.

Le principe de la Reconnaissance des Empreintes Digitales consiste à comparer des empreintes fournies au système à plusieurs autres empreintes aussi appelé « Template» ou signatures, le système biométrique renvoie un résultat positif au cas où l'empreinte fournie à l'entrée correspond à l'un des Template, et un résultat négatif dans le cas contraire.

# II.2Reconnaissance biométrique par empreinte digitale

Dans cette partie, nous présentons les caractéristiques d'empreinte digitale puis, nous citons les différentes représentations de l'image d'empreinte, en suite nous identifions les propriétés des images d'empreintes digitales, puis nous citons les différentes approches et les travaux qui portent sur l'extraction des caractéristiques de cette modalité. En terminera cette partie par les différents problèmes rencontrés lors de l'extraction des minuties.

## II.2.1 Caractéristique d'empreinte digitale

L'empreinte digitale (figure II.1) se compose des crêtes et des vallées alternatives, flottant à la direction constante locale. Le modèle de crête et de vallée est unique pour chaque individu et ne change pas pendant la vie individuelle sauf l'accident comme meurtrissure ou coupe de bout du doigt. Cette propriété fait l'empreinte devenir une

biométrie d'identité attractive. On peut classer les empreintes digitales en trois classes principales (figure II.2) :



Figure II-1 : Exemple d'empreinte digitale.

- ✓ ***Les arcs*** : les lignes vont d'un bord à l'autre du doigt.
- ✓ ***Les boucles*** : les lignes ont un trajet récurrent et reviennent aux bords dont elles sont parties.
- ✓ ***Les verticilles*** : les lignes présentent un trajet plus au moins spirale et limite vers les bords du doigt.

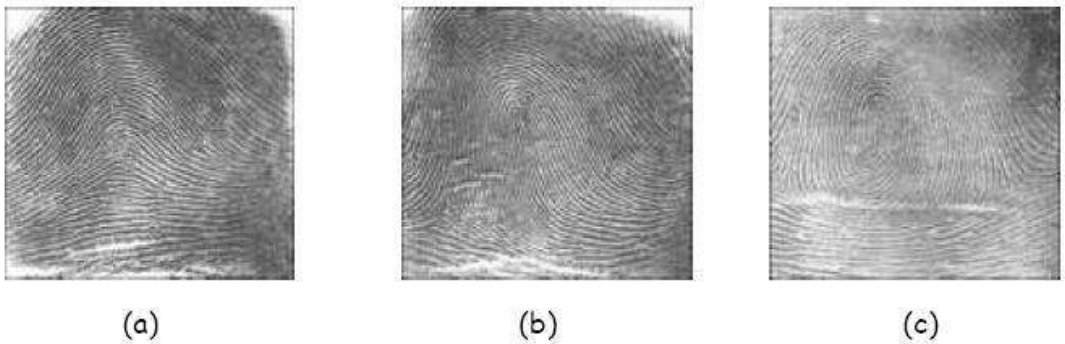



Figure II-2: Les différents types d'empreintes

*(a) Image de type arc, (b) Image de type boucle, (c) Image de type spiral*

Les empreintes digitales sont entièrement formées à environ sept mois du développement du fœtus et les configurations des crêtes du doigt ne changent pas à moins d'accidents telles que des contusions et des coupes sur les bouts du doigt. Cette propriété fait des empreintes digitales une marque biométrique très attrayante. En pratique, on préférera extraire les caractéristiques principales suivantes [27] :

- ✓ ***Les minuties*** : Les empreintes digitales présentent plusieurs types de points dont la détermination repose sur des règles précises et complexes. Les bifurcations et les fins de crêtes permettent la reconstitution de toutes les minuties, toute autre minutie peut se composer de combinaisons de bifurcations et de fins de crêtes. Par exemple, les anneaux peuvent être visualisés en tant que deux bifurcations qui se superposant et un ilot peut être représenté par deux fins de crêtes à courte distance (figure II.3).

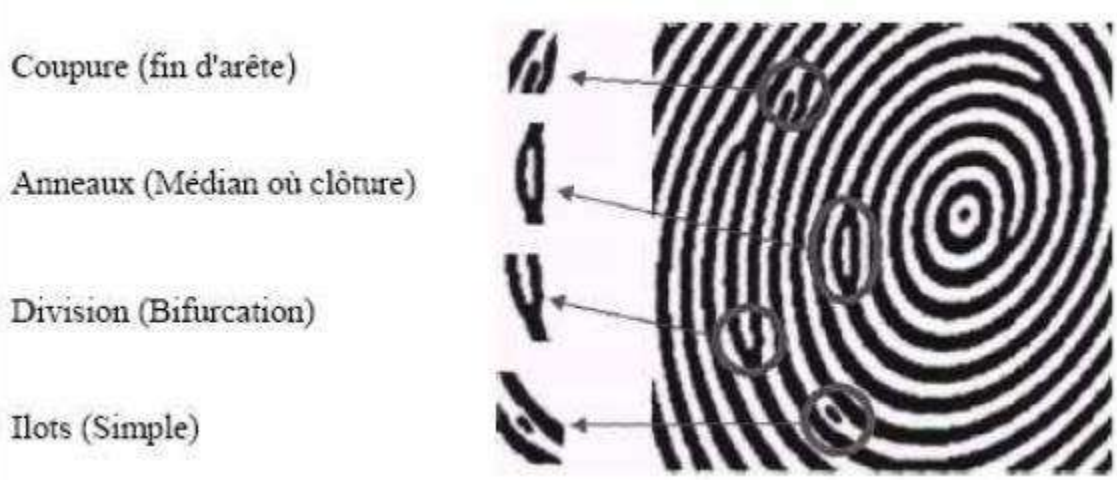



Figure II-3: Exemple de quatre familles de crêtes.

- ✓ Les points singuliers :

– ***Le centre*** : le centre est le lieu de courbure maximale des lignes d'empreinte les plus internes. Il est aussi appelé le point coré.

– ***Les deltas*** : un delta est proche du lieu où se séparent deux lignes d'empreintes vérifiant les propriétés suivantes : ces lignes se séparent suivant deux directions orthogonales et sont les lignes les plus internes vérifiant la propriété précédente (figure II.4).




Figure II-4: Les points singuliers.

## II.2.2 Représentation de l'image d'empreinte et prise de décision

Une empreinte apparait comme une surface alternée de crêtes et de vallées parallèles sur la plupart des régions. Différentes caractéristiques permanentes ou semi-permanentes tels que les blessures, les coupures et les bleus sont aussi présentes sur l'empreinte. Qu'il s'agisse d'un problème de vérification ou de classification, il est nécessaire de définir sur l'empreinte une **représentation invariante** : des caractéristiques qui ne s'altèrent pas avec le temps. Cette représentation peut être **globale** prenant en compte toute l'image ou, **locale** c'est-à-dire constituée d'un ensemble de composantes dérivée chacune d'une région restreinte sur l'empreinte.

Lorsqu'il est question d'un problème d'appariement (vérification de la similarité entre deux empreintes), les algorithmes d'appariement peuvent être classifiés en fonction de la représentation de l'empreinte ; qui elle peut appartenir à l'une des catégories suivantes :

### *II.2.2.1 Image*

Dans cette représentation, c'est toute l'image qui est considérée comme une représentation possible. L'appariement est réalisé par corrélation. La corrélation entre les deux images *I1(x, y), I2 (x, y)* est donnée dans le domaine spatial par :

$$I_c = \sum_x \sum_y I_1 (x + k, y + l) I_2(x, y) \qquad (II_1)$$

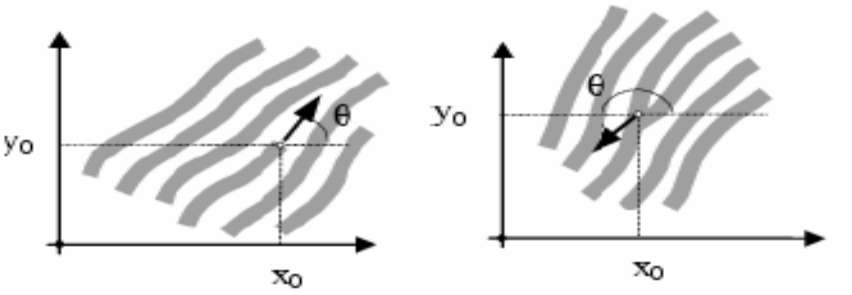
Le corrélateur établit la correspondance par la recherche de la magnitude du pic dans l'image de corrélation *IC*. La position du pic indique la translation entre les images et la valeur du pic informe sur le degré de similarité. L'exactitude de cette corrélation se dégrade avec les transformations de l'image comme les phénomènes de translation et de rotation.

### *II.2.2.2 Représentation en minuties*

Le but d'un algorithme d'appariement est de comparer deux images ou deux gabarits et de retourner le score de similarité qui correspond à la probabilité que deux empreintes se correspondent. A l'exception des algorithmes basés sur la corrélation, la plupart des algorithmes extraient des caractéristiques dans le but de faire l'appariement. Les détails de minutie constituent la représentation la plus populaire de toutes les représentations existantes, elles répondent efficacement au problème de taille posé précédemment.

Les minuties représentent des discontinuités locales et marquent les positions ou la crête se termine ou bifurque. Cela constitue les types de minutie les plus fréquentes, bien qu'un total de 18 types de minuties ait été identifié.

Chaque minutie peut être décrite par un nombre d'attributs tels que la position (x, y), l'orientation θ et d'autres informations susceptibles d'aider à l'appariement. Cependant, la plupart des algorithmes considèrent seulement sa position et son orientation (figure II.5) :




**(a)** **(b)**

Figure II-5 : Les caractéristiques principales des minuties. *(a)terminant, (b) bifurcation*

Les minuties peuvent être appariées en considérant le problème comme un problème d'appariement de primitives point (point pattern matching). La figure suivante est une représentation en minuties d'une empreinte (figure II.6) :



Figure II-6: Exemple d'une représentation d'une empreinte par sa carte de minuties.

### *II.2.2.3 Les descripteurs de texture*

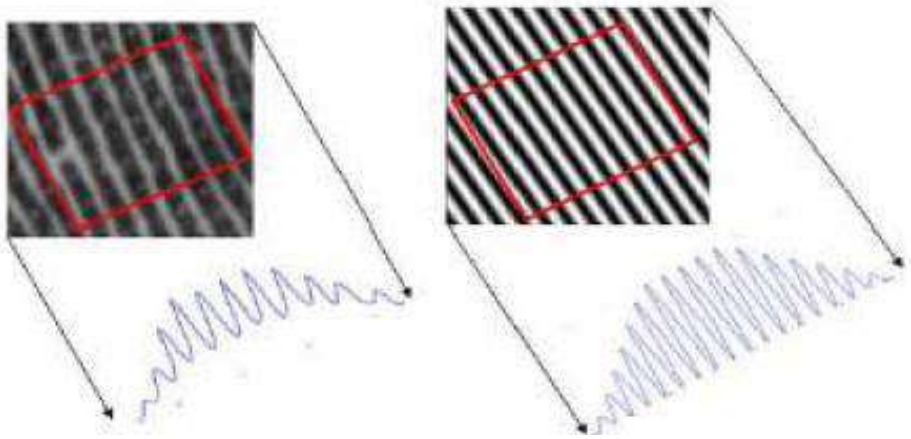
Les algorithmes d'appariement basés sur les minuties ne s'exécutent pas bien quand la surface de l'empreinte est petite étant donné que le nombre de minuties n'est pas suffisant pour l'appariement. De plus, le processus d'extraction des minuties est plus

enclin à l'erreur dans ce genre de cas. Prabhakar et al [28] proposent une méthode basée sur un banc de filtres pour effectuer l'appariement de cette sorte d'images. Ils décrivent un nouveau descripteur de texture appelé "code d'empreinte". Les informations de texture (moyennes et variances) sont extraites en effectuant une sectorisation [29] de l'image autour d'un point de référence (le point core) ; et l'appariement est basé sur le calcul de la distance euclidienne entre deux codes. L'inconvénient de cette approche est que le point core doit être localisé de façon exacte. Cela n'est pas possible pour des images de mauvaise qualité. De plus, la performance est inférieure comparée aux appariements basés sur les minuties. Cependant, une décision qui combine les paramètres de texture et les minuties aurait un meilleur rendement.

### II.2.3 Propriétés des images d'empreintes digitales

Les travaux qui ont été faits dans le domaine de l'analyse d'empreintes s'appuient sur les propriétés intrinsèques qui caractérisent ce type d'image :

- ✓ L'empreinte est par essence une image de lignes.
- ✓ Une empreinte est une alternance de crêtes et de vallées qui évoluent dans une direction précise.
- ✓ Un bloc de l'image bien défini possède une direction locale constante.
- ✓ Sur un bloc, les niveaux de gris des crêtes et des vallées constituent une forme sinusoïdale le long de la direction normale à l'orientation locale des crêtes (figure II.7). L'amplitude, la fréquence de cette forme sont des indicateurs sur le type de la région constituant le bloc considéré. Seuls les points singuliers constituent une discontinuité de cette forme présumée.



*(a)* *(b)*

Figure II-7: Projection des crêtes sur une image orientée.

*(a) un échantillon d'empreinte (b) une empreinte synthétique.*

- L'empreinte est une image texturée.
- Les valeurs des niveaux de gris atteignent leur maximum local le long de la direction normale aux crêtes.
- Lors de la saisie d'une empreinte digitale, il arrive assez souvent que certaines parties de l'empreinte soient sous ou sur encrées, ce qui peut être gênant pour les traitements ultérieurs. La définition précédente nous indique que cette image est non stationnaire. En effet, la moyenne des niveaux de gris dans une fenêtre de la partie sous-encrée est différente de la moyenne dans une fenêtre d'une partie "normale" de l'empreinte. Pour remédier à cette contrainte, beaucoup d'algorithmes utilisent une étape de **normalisation.**

Ces propriétés peuvent être matérialisées par des représentations spécifiques sous forme d'image appelée ***images intrinsèques***. Cela inclut :

- *L'image d'orientation* : l'image d'orientation *O* représente l'orientation locale des crêtes sur chaque point de l'image [30] [31].
- *L'image de fréquence* : la fréquence locale des crêtes indique la distance moyenne entre les crêtes sur un bloc [32] [33].

• *Le masque des régions* : le masque indique l'ensemble des régions ou apparaissent des crêtes. Il est aussi appelé masque région fond. D'autres masques [32] sont capables de distinguer les régions exploitables parmi celles qui sont irrécupérables.

Le calcul de ces images intrinsèques forme une étape critique dans un processus d'extraction de caractéristiques. Une erreur survenue lors de leur calcul va se propager le long de tout le procédé. L'image d'orientation est utilisée pour l'amélioration de l'image, la détection des points singuliers, la segmentation et la classification des images. Le masque est utilisé pour éliminer les fausses minuties.

## II.2.4 Extraction des caractéristiques

La représentation des attributs de l'empreinte constitue la phase la plus cruciale lors de la conception d'un système de vérification. La représentation détermine nettement la précision du système. Les systèmes existants se basent sur les détails des minuties, les descripteurs de texture ou sur la représentation de l'image entière [34]. Il reste néanmoins que les minuties sont de loin les attributs les plus largement utilisés.

Les minuties marquent des points de discontinuité locale (Figure II-8). FBI utilise un modèle d'identification qui repose sur deux types de minuties : les terminaisons qui marquent les fins de crêtes et les bifurcations qui correspondent aux points ou la crête se diverge.

## II.2.5 Travaux antérieurs

Les algorithmes d'extraction de minuties présents dans la littérature peuvent être généralement catégorisés en ceux qui se basent sur l'extraction à partir de l'image en niveau de gris et ceux basés sur l'extraction à partir de l'image binarisée.

### *II.2.5.1 Les approches de binarisation*

Dans cette approche, l'image en niveau de gris est convertie en une image binaire. Malgré le fait que les algorithmes existants différent dans les divers aspects d'implémentation, ils suivent tous les étapes communes suivantes (figure II.9) :

**1. Segmentation/binarisation** : dans cette étape, l'image est convertie en une image binaire à travers un processus de seuillage ou une méthode de binarisation adaptative. Le but est le repérage des crêtes. Cette étape est aussi appelée dans la littérature segmentation. Toutefois, cela ne doit pas se confondre avec la segmentation de l'image entre région d'intérêt et région de fond lors de la génération du masque des régions.

**2. Amincissement** : l'image binaire est ensuite amincie à travers un schéma itératif morphologique résultant en une carte de crêtes d'une largeur d'un pixel.

**3. Détection de minuties** : dans le cas où l'amincissement serait utilisé, cette étape devient triviale. Elle se base sur une scrutation de voisinage. Les fins de crêtes ont un seul voisin et les bifurcations possèdent plus de deux voisins

**4. Post-traitement** : l'extraction de minuties peut produire deux sortes d'erreurs : les fausses détections c'est à dire des minuties qui n'existent pas sur l'image originale et les minuties oubliées qui sont de vraies minuties qui n'apparaissent pas sur le gabarit résultat. Alors que rien ne peut être fait pour éviter les oublis de vraies minuties, les fausses minuties peuvent être éliminées en considérant leurs relations spatiales. Différentes heuristiques peuvent être appliquées pour filtrer les fausses minuties.

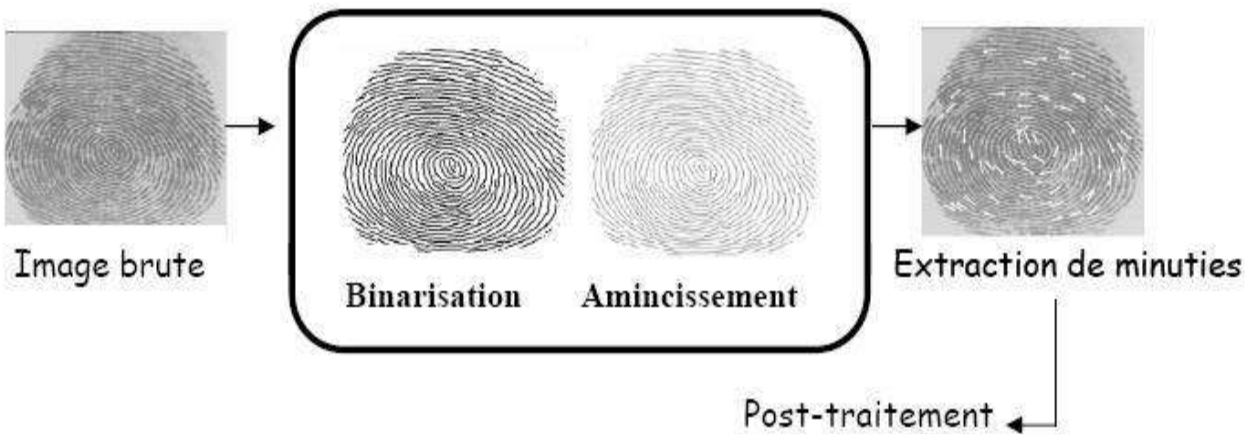



Figure II-9: Extraction des minuties par binaraisation.

### *II.2.5.2 Les approches d'extraction à partir de l'image en niveau de gris*

Peu d'approches d'extraction de minuties ne suivant pas le schéma conforme de binarisation - squelettisation ont été proposées :

M.T.Leung et al introduisent dans un réseau de neurones pour la détection des minuties. Une autre approche plus directe a été proposée par Maio et Maltoni dans [34]. Cette approche traque les crêtes en localisant les maxima locaux par un suivi de lignes le long du flot directionnel des crêtes. Seulement, avec cette approche les maxima locaux peuvent ne pas être bien définis dans le cas d'une image de mauvaise qualité. Néanmoins les approches de niveau de gris possèdent de nombreux avantages :

- ✓ Le schéma de binarisation implique quelques formes de seuillage. Un simple seuillage n'est pas adéquat lorsque l'image n'a pas une illumination uniforme, ce qui est commun pour les capteurs optiques. Un seuillage adaptatif n'est pas très fiable dans une image de faible qualité.
- ✓ L'étape de squelettisation est gourmande en temps machine dans le sens où elle est impartialement récursive. Le suivi de ligne est beaucoup plus rapide.
- ✓ Le suivi de crêtes est intrinsèquement immunise contre les coupures de crêtes souvent présentes dans l'empreinte contrairement aux autres procédés de

binarisation qui restent très sensibles à ce genre de bruit et nécessitent systématiquement un post-traitement.

### II.2.6 Les problèmes rencontrés lors de l'extraction des minuties

Un fiable algorithme d'extraction de caractéristiques est une étape critique pour la performance d'un système automatique d'authentification d'identité en utilisant l'empreinte digitale. La performance d'un algorithme d'extraction et de mise en correspondance des images d'empreintes digitales dépend fortement de la qualité de l'image en entrée. Les algorithmes présentés ultérieurement opèrent bien à condition que l'image en entrée soit de bonne qualité (quand la qualité de l'empreinte ne peut pas être mesurée de façon objective, elle peut être grossièrement déduite de la clarté de la structure des crêtes : Une image de bonne qualité possède un fort contraste et un ensemble de crêtes et de vallées bien définies). Cependant, dans la pratique un pourcentage signifiant d'images est en mauvaise qualité. Cela est dû :

- Aux conditions d'acquisition.
- A l'état de l'épiderme.
- Au dispositif de prise de vue.
- A une mauvaise coopération du sujet.
- Qualité de l'empreinte rencontrée durant la vérification.

La qualité de l'empreinte rencontrée durant la vérification est très incertaine, elle varie sur une grande portée. La plus grande partie est endommagée par l'état de l'épiderme (voir figure II.10) :

- Les crêtes se cassent par la présence de blessures, de coupures.
- Des empreintes très sèches donnent des crêtes fragmentées.
- Les empreintes qui transpirent font une sorte de pontage entre les lignes de crêtes (raccordement).




Figure II-10: Des images de différentes qualités.

*La qualité décroit de la gauche vers la droite. (a) image de bonne qualité avec un bon contraste (b) distinction insuffisante sur le centre de l'image (c)une empreinte sèche.*

Cela peut engendrer les problèmes suivants :

- ✓ Création de fausses minuties.
- ✓ Ignorance de vraies minuties.
- ✓ Introduction d'erreurs de localisation (position et direction).

Par la suite une carte de fausses minuties va engendrer l'échec de l'algorithme d'appariement. Une étape de prétraitement pour améliorer la clarté s'avère donc nécessaire. Ce qui explique le fait que la plupart des recherches soient principalement vouées à **l'amélioration de l'image en entrée**.

## II.3Travaux existants sur la reconnaissance par empreinte digitale

On peut classer les systèmes de reconnaissance de l'empreinte digitale en trois catégories :

· Les systèmes basés sur les minuties

· Les systèmes basés sur la corrélation

· Les systèmes basés sur l'image

Nous allons présenter dans ce que soit quelques méthodes :



(a) (b) (c) (d) (e)

Différents types de minuties : (a)terminaison (b) bifurcation, (c) pont, (d) lac et (e) ile

Figure II-11 : Différents types de minuties

## II.3.1 Analyse de l'existant

Une empreinte complète contient en moyenne une centaine de ces points caractéristiques (les « minuties »). Ainsi, la majorité des travaux de la littérature propose à représenter l'image d'empreinte digitale par les points caractéristiques appelés « minuties ». Ces points caractérisent l'empreinte digitale d'une manière fiable et les systèmes proposés ont prouvé la fiabilité de l'utilisation de ces points. Mais le problème majeur rencontré lors de l'extraction de ces points se manifeste dans les images de mauvaises qualités. Donc pour une image de mauvaise qualité on peut générer de faux points ce qui diminue la performance de cette méthode.

Tableau 4 II-1 : Tableau comparatif de quelques systèmes de reconnaissance par empreinte digitale

| | Prétraitement | Extraction de caractéristique | | Comparaison | Résultats expérimentaux |
|---|---|---|---|---|---|
| **Anil Jain (Jain et *al.*, 2007)** | Image de forte résolution 1000p/i<br>Vérification à la base de 3 niveaux de caractéristiques<br><br>Normalisation à la base des Filtres de Gabor<br>+ Transformation de Wavelet Pour extraction de pores | Combiner l'image normalisée par les filtres de Gabor et celle filtré par la transformation de Wavelet pour détecter le contour de ride par convolution de l'image binarisé par le filtre H | filtre H | Classifieur hiérarchique utilisant 3 scores calculés à la base des 3 niveaux de caractéristique (orientation, minuties, pores et rides) | Base de 410*2*2<br>A 1000 Ppi |
| **Arun Ross (Ross et *al.*, 2003)** | Filtres de Gabor 2D<br>Représentation de Fourrier | Normalisation +<br>Quadriller l'image<br>Segmentation (niveaux de gris) | Pour chaque cellule extraction de l'orientation de rides+ les caractéristiques de minuties | Deux scores calculés (Rides, minuties), les combinés pour en déduire un | Base de 160*2*4<br>84%, ERR=4% |
| **Aparecido Nilceu Marana (Marana et *al.*, 2005)** | Squelettisation pour extraction de rides (niveau de gris) | Transformation de Hough pour extraction de lignes droite (des rides) | Alignement des 2 empreintes Digitales à la base des paramètres de translation et de rotation détectés | Un score : maximum de rides des 2 images en question | MSU-VERIDICOM :160*4<br>66.87% |

| | | | | | |
|---|---|---|---|---|---|
| **K. Umamaheswaril ( Umamaheswaril et *al.*, 2007)** | Compressé l'image par un algorithme basé sur Wavelet | Normalisation, amincissement, extraction des minuties | réseaux neuronaux pour la classification (arche,..) | Feedback (RN)+ kppv (crisp)score de vraisemblance | Base de test :200<br>Base d'apprentissage 700<br>97.4% |
| **Unsang Park (Park et *al.*, 2008) SIFT+ minuties** | Ajuster le niveau de gris<br>Suppression de bruit des caractéristiques SIFT | Opérateur Gaussienne pour la squelettisation<br>Extraction des extrema | Fenêtre (16X16) pour l'extraction du gradient des points extrema locaux | Chercher les points égaux et non égaux des deux images + Distance Euclidienne | **ERR**<br>**DB1 :**<br>SIFT :8.44%<br>Minutie :1.75%<br>SIFT+Minutie :0.99%<br>**DB2 :**<br>SIFT :10.76%<br>Minutie :2.13%<br>SIFT+Minutie :1.07% |
| **Xuejun Tan (Tan et *al.*, 2005)** | Extraction de minuties | Représentation chromosomique à la base des paramètres déjà extraits (27 bits) | fonction de corrélation | Génération de la population (sélection + croisement)+ des règles heuristiques | la base de NIST-4<br>99.1% imposteurs<br>11.5% légitimes |
| **(Bengueddoudj et *al.*, 2013)** | Sans rehaussement de l'image d'empreinte digitale | Extraction des minuties | Algorithme de Jiang modifié<br>Elimination des pairs de minuties dont leur score de vraisemblance est inférieure à un seuil<br>Un score global est calculé à partir des scores locaux affectés aux pairs de minuties non éliminés | | La base FVC2004<br>Sous base DB2 :9%<br>Sous base DB3 :17.72 4 |

# II.4Conclusion

Selon cette étude bibliographique, nous pouvons conclure que les systèmes de reconnaissance d'empreinte digitale présentent des étapes communes dans leurs processus. Chaque système procède à prétraiter l'image d'empreinte digitale pour bien localiser la zone d'intérêt puis passe à l'étape d'extraction de caractéristiques pour représenter l'empreinte par un vecteur de primitives et fini par une étape de comparaison et décision.

Mais chaque système intègre des techniques différentes que les autres systèmes.

# III. Chapitre : Reconnaissance d'empreintes digitales basé sur l'extraction des minuties

# III.1Introduction

La reconnaissance de l'empreinte digitale ou l'authentification par empreinte digitale se réfère à la méthode automatisée de vérification d'une correspondance entre deux empreintes humaines. Dans ce chapitre, nous présentons les résultats expérimentaux recueillis au cours de notre travail.

# III.2Le système de vérification d’empreinte digitale proposé

La figure III.1 présente la démarche générale de notre système de vérification d’empreinte digitale. Deux phases sont nécessaires pour tout système biométrique : une phase d’apprentissage dans laquelle on prépare les gabarits de la modalité biométrique de base et une phase de test permettant d’évaluer la performance du système. Pour notre système, ces deux phases ont trois étapes communes : une étape de prétraitement, une étape de localisation de la région d’intérêt (RI) et une étape d’extraction de caractéristique. Mais au niveau de l’apprentissage, nous finissons cette phase par l’étape de représentation possibiliste des caractéristiques extraites et préparer le gabarit final de l’empreinte digitale d’apprentissage. Alors qu’au niveau de la phase de test, après l’extraction de caractéristiques, nous passons à l’étape de comparaison possibiliste et la prise de décision sans avoir besoin de donner une représentation possibiliste aux caractéristiques de l’empreinte de test.

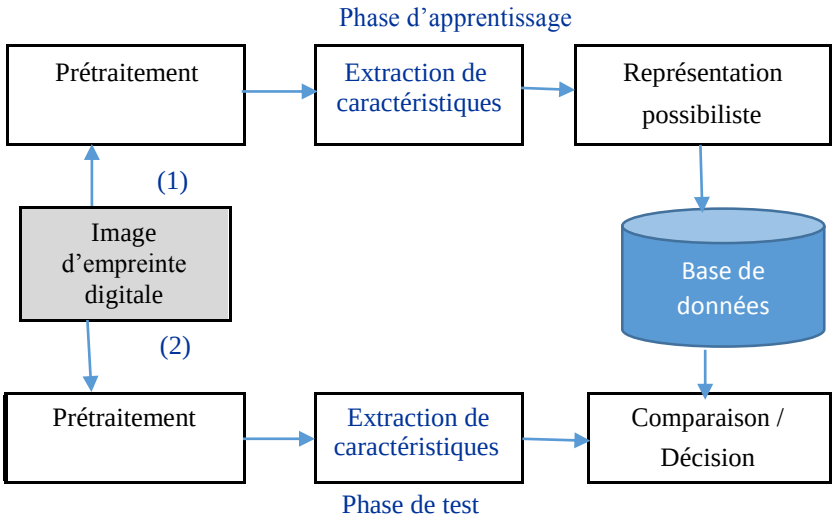



Figure III-1: Démarche générale du système de vérification par empreinte digitale proposé

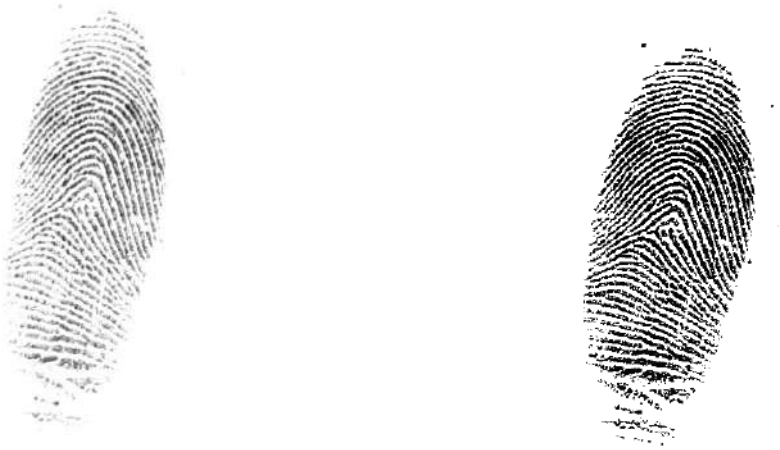
(1) : Empreinte digitale de référence ; (2) : Empreinte digitale de test

Dans la phase d'apprentissage de notre processus de vérification des empreintes digitales, nous procédons à prétraiter l'image puis localiser la zone d'intérêt. Cette zone d'intérêt sera l'entrée au module d'extraction de caractéristiques pour donner une autre représentation discriminative en se basant sur la transformée en cervelet qui nous génèrent des sous-bandes.

Pour chaque sous-bande, nous calculons des primitives statistiques. Ces primitives sont considérés imprécises et la représentation générale de l''empreinte digitale peut être incertaine. Pour ce fait, après avoir extrait les primitives, nous proposons une méthode qui donne une autre représentation pour ces primitives. Cette représentation est générée par la théorie possibiliste qui analyse l'aspect imprécis et incertain de ces primitives. Par la suite, notre méthode de comparaison mesure un degré de similarité entre la représentation possibiliste d'une empreinte digitale de référence et les primitives de l'empreinte de test extraites par l'extracteur basé sur la transformée en cervelet.

### III.2.1 Etape de prétraitement

Pour rehausser la qualité de l'image des empreintes digitales et éliminer le bruit, nous avons appliqué la technique proposée de prétraitement comme l'égalisation d'histogramme comme montrée dans la figure III-2



(a) (b)

Figure III-2: Exemple d'une empreinte digitale prétraitée (a) l'image originale, (b) l'image rehaussée

### III.2.2 Extraction de la Région d'intérêt

Après le rehaussement de l'image d'empreinte digitale, nous la localisons zone carrée ROI de démontions (388 pixels × 374 pixels) autour de l'image réorientée.



Figure III-3: localisons zone autour de l'image réorientée.

## III.2.3 Extraction de caractéristiques d'empreinte digitale

L'approche basée sur les minuties est la plus utilisée dans la plupart des systèmes modernes de reconnaissance d'empreintes digitales. Les principales étapes de l'extraction des minuties sont : lissage, l'estimation de l'orientation, l'amincissement et la détection des minuties.

### *III.2.3.1 Extraction de minuties basée sur l'image binaire*

Dans la méthode basée sur l'image binaire, la binarisation de l'image niveau de gris est la première étape à réaliser.

Ceci exige que chaque valeur d'intensité de pixel soit transformée à une intensité binaire de noir (0) ou le (1) blanc. L'approche la plus simple est d'appliquer un seuil mondial où Chaque pixel est cartographié selon

$$I(x,y) = \begin{cases} 1 & \text{si} \quad \mathrm{I(x,y)} \geq \mathrm{t} \\ 0 & \text{autrement.} \end{cases} \qquad \textbf{(III.1)}$$

**Avec I : intensité , t : seuil =0.46%**

Les points de fin de crête et les points de bifurcation de l'image squelette sont les deux types de points critiques à extraire. Une fois produit, l'image binaire subit d'habitude

une opération de d'amincissement morphologique, où les structures des crêtes sont réduites à l'épaisseur à 1 pixel, nommées comme le squelette, L'objectif de la squelettisation est de représenter un ensemble avec un minimum d'information pour aider la détection de détails. L'image binaire amincie qui en résulte est donc analysé afin de trouver la position de minutie.

Ceci est réalisé par utilisation de 8 voisinages (des pixels dans 3 × 3 fenêtre centrée à p) circulaire traversé dans en sens inverse des aiguilles d'une montre

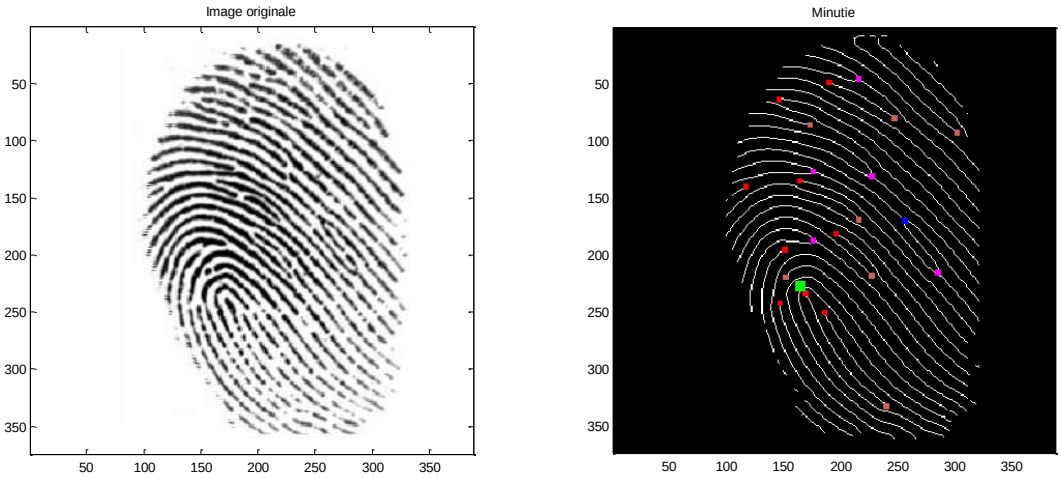
| | | |
|---|---|---|
| P1 | P2 | P3 |
| P8 | P0 | P4 |
| P7 | P6 | P5 |

Figure III-4: 3×3 région

Si P0 est 1 et le nombre de transition $N_{trans}$ entre 0 et 1 (et vice versa) de P1 a P8 est supérieur ou égal à 6, alors P0 un point de jonction (ou bifurcation), et si $N_{trans}$ est égale à 2 alors P0 un point de fin de crête. Mathématiquement, cela peut s'exprimer avec l'équation suivante :

$$N_{trans} = \sum_{i=1}^{8} |p_{i+1} - p_i| \qquad \text{(III.2)}$$

Où P9=P1




(a) (b)

Figure III-5: a) image niveau de gris originale. b), point de bifurcations et de fin de crête.

Bien que binarisation en accord avec **squelettisation** fournisse un cadre simple pour l'extraction de détails, il y a une problématique caractéristique : Les détails faux (faux minuties) en raison d'algorithmes de d'amincissement, ou fins de crêtes irrégulières.

### *III.2.3.2 Estimation spatiale de la carte directionnelle de l'image*

La direction locale des stries est régulièrement utilisée dans la reconnaissance d'empreintes (filtrage directionnel, caractérisation d'une minutie, critère de correspondance dans la phase d'appariement). Dans les trois approches qui suivent la direction est utilisée pour choisir un filtre adapté localement aux caractéristiques locales fréquentielles et directionnelles de la zone filtrée. Nous présentons ici le calcul de la carte directionnelle de l'empreinte.

Cette mesure doit être fiable, car dans le cas d'un filtrage directionnel une mauvaise évaluation de la direction provoquerait une dégradation de l'image.

### *III.2.3.3 Le calcul de la direction locale d'un pixel*

Pour calculer la direction associée à un pixel *x, y* de l'image on considère son voisinage *V* de taille *W× W pixels*. On calcule les gradients, $G_x(i, j)$ en *x* et, $G_y(i, j)$ en *y* (Equ.3) pour chaque pixel *i, j* du voisinage *V*. Pour le calcul du gradient l'utilisation des masques de Sobel s'est avéré la plus efficace dans le cas de nos images. Ainsi la direction locale au voisinage *V* est estimée par la relation suivante [36] :

$$\theta(x,y) = \frac{1}{2}\tan^{-1}\left(\frac{\sum_{i=1}^{W}\sum_{j=1}^{W} 2\cdot G_x(i,j)\cdot G_y(i,j)}{\sum_{i=1}^{W}\sum_{j=1}^{W}(G_x^2(i,j)-G_y^2(i,j))}\right) \quad \textbf{(III.3)}$$

Avec $G_x = V(x,y) \otimes \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix}$ et $G_{yx} = V(x,y) \otimes \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{bmatrix}$

Il est ainsi possible de calculer la direction locale en chaque pixel de l'image [37] mais ceci est très coûteux en temps de calculs, ainsi il est beaucoup plus efficace de diviser l'image en blocs adjacents et d'évaluer la direction moyenne locale au bloc quitte à interpoler la direction pour chaque pixel.

L'utilisation de blocs de taille comprise entre 8 pixels et 16 pixels de large s'est montrée suffisamment efficace dans le cas d'images standard (faible variation de la distance inter strie).

### *III.2.3.4 Le lissage de la carte directionnelle*

Pratiquement il est possible d'avoir localement un bloc tellement bruité que l'estimation directionnelle soit complètement faussée. Ceci provoque alors une très importante variation angulaire entre deux blocs adjacents. Or une empreinte possède une certaine continuité directionnelle, une telle variation entre deux blocs adjacents est alors représentative d'une mauvaise estimation. Pour éliminer de telles discontinuités un filtre passe-bas est appliqué à la carte directionnelle. Cette opération de lissage ne pouvant être effectuée directement sur les valeurs d'angle en raison de la discontinuité de la fonction arc tangente on calcule la table des sinus (Equ.4) et des cosinus (Equ.5) au lieu de la table des angles (Equ.3) :

$$\sin(2\theta) = \frac{\sum_{i=1}^{w}\sum_{j=1}^{w}(G_x^2(i,j) - G_y^2(i,j))}{\sum_{i=1}^{w}\sum_{j=1}^{w}(G_x^2(i,j) + G_y^2(i,j))} \quad \textbf{(III.4)}$$

$$\cos(2\theta) = \frac{\sum_{i=1}^{w}\sum_{j=1}^{w} 2 \cdot G_x(i,j) - G_y(i,j)}{\sum_{i=1}^{w}\sum_{j=1}^{w}(G_x^2(i,j) + G_y^2(i,j))} \quad \textbf{(III.5)}$$

Un filtre binomial 3 ×3 est ensuite appliqué à la carte des sinus et cosinus.

Un exemple de cartes directionnelles pour les deux catégories principales d'empreinte est présenté sur la Figure III-6

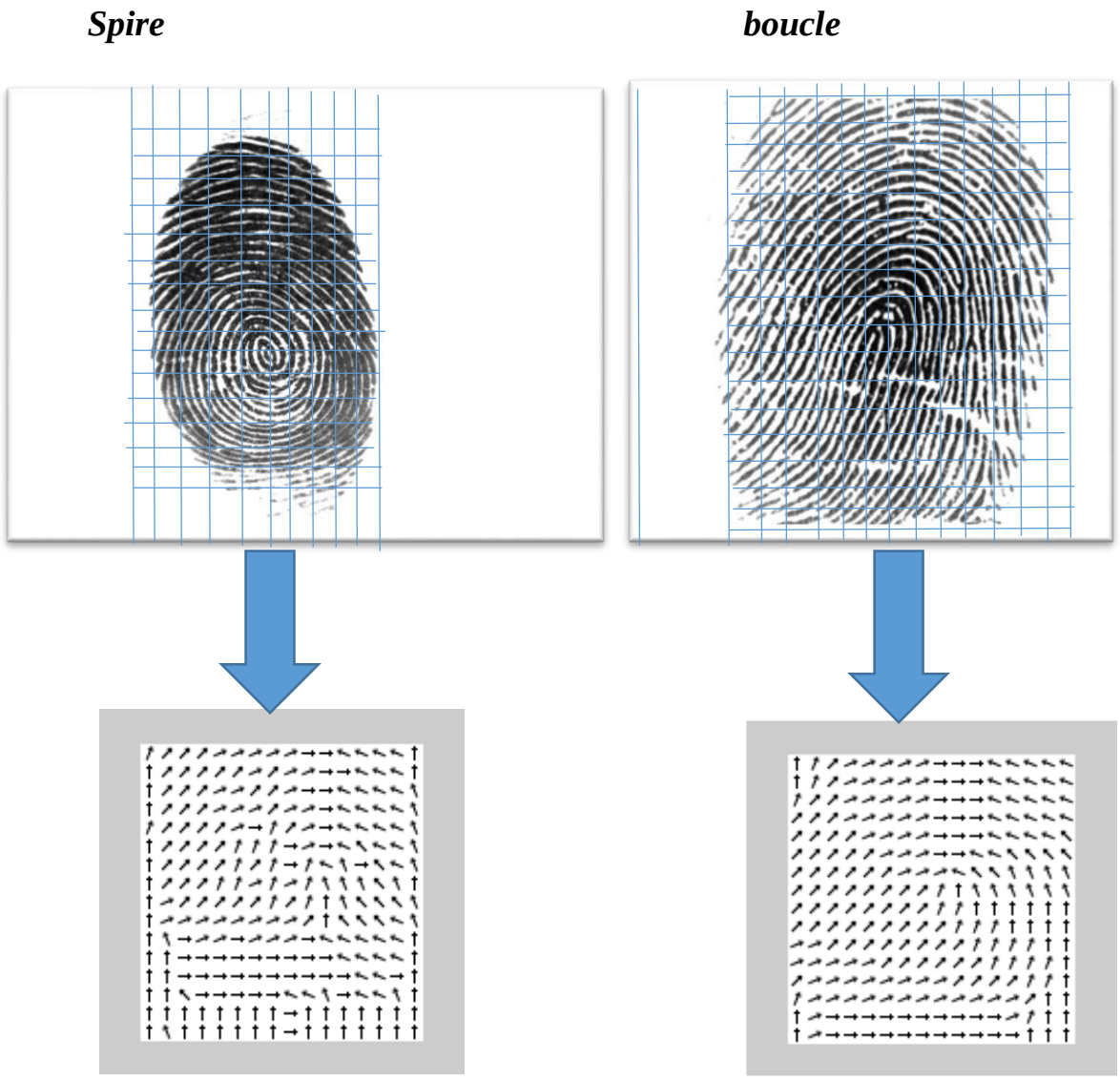



Figure III-6: Exemples de carte directionnelle sur des images.

# III.3Représentation des minuties

Les algorithmes de correspondance basés sur les minuties dépendent en grande partie des informations minuties extraites. Les algorithmes robustes de correspondance basés sur les minuties doivent traiter des occurrences de minuties manquantes et parasites, où des minuties manquantes peuvent se produire en raison d'une détection inexacte des caractéristiques, d'un traitement après traitement ou d'un obscurcissement des nuages d'image, et des minuties fausses peuvent être introduites par sec La peau, les plis, les algorithmes de détection de fonctionnalités et d'autres agents potentiellement causant le bruit. Les processus généraux d'un algorithme d'appariement d'empreintes digitales sont présentés à la figure III.7.

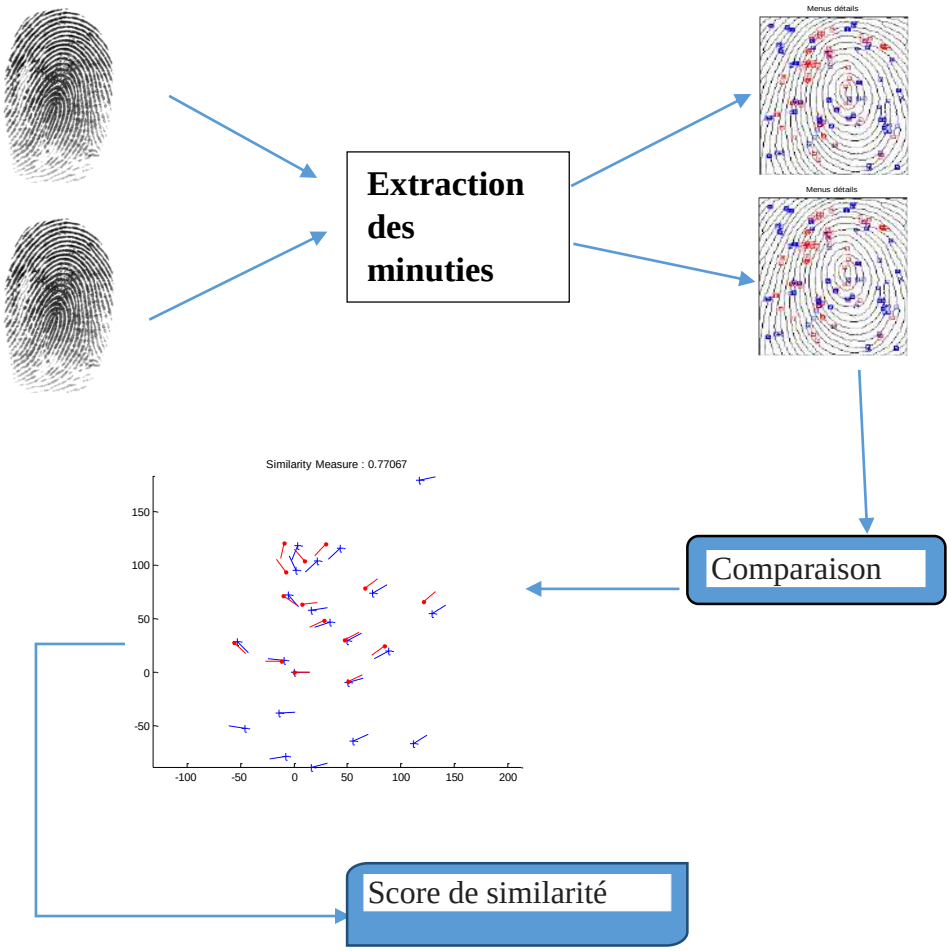



*Figure III-7: Processus généraux pour correspondance d'empreinte digitale à base de détails.*

Dans l'équation basée sur les minuties, les minuties sont généralement représentées comme des structures minuties appelées triches de minutie, où minutia,$m_i$, est décrite comme $m_i$= {x, y, θ} avec x, y représentant la coordonnée x-y de la minutie et θ l'angulaire Direction de la crête principale .

L'objectif principal de l'appariement basé sur les minuties est d'effectuer une cartographie ou un couplage individuel de points minutieux à partir d'un ensemble de minuties de l'image de test

$$A = \{m_{A1}, m_{A2}, \ldots, m_{Ap},\}, \text{ où } m_{Ai}, = \{x_{Ai}, y_{Ai}\ , \theta_{Ai}, \}\ \textbf{et}\ \ 1 \leq i \leq p \qquad \textbf{(III.6)}$$

À un modèle reflètent l'ensemble de minutie

$$B = \{m_{B1}, m_{B1}, \ldots, m_{Bq}, \}, \text{ où } m_{Bj}, = \{x_{Bj}, y_{Bj}\ , \theta_{Bj}, \}\ \textbf{et}\ 1 \leq j \leq q, \qquad \textbf{(III.7)}$$

En formant les paires de minuties ($m_{Ak}$,$m_{B\pi(k)}$) avec $\pi$ (k) comme la permutation de cartographie de paires d'ensemble A à B.

Malheureusement, nous ne pouvons pas continuer à trouver des paires de minuties de triplets sans certain prétraitement pour les raisons critiques suivantes :

- Des impressions d'empreinte digitale peuvent différer dans l'orientation, considérant le champ de direction dans le triplet
- Inutile, Des impressions d'empreinte digitale peut différer dans la compensation, considérant les champs (domaines) x-y dans le triplet inutile,
- Et l'élasticité de peau crée l'altération non-linéaire ou 'déformant' pour arriver quand différent directionnel la pression est appliquée causant le triplet x-y des variations arrivé.

En général, le manque des caractéristiques invariables de la structure de triplet l'interdit pour aider le processus de trouver des paires de détails.

## III.4Enregistrement

Afin d'aborder les problèmes liés au manque d'invariance de la structure triplet, une inscription globale est requise. L'enregistrement global concerne l'alignement et la

superposition du modèle et teste les empreintes digitales afin que les régions correspondantes des empreintes aient une distance géométrique minimale l'une de l'autre. L'enregistrement peut être réalisé géométriquement en appliquant (à l'ensemble de minutie d'empreinte de l'épreuve ou du modèle) une transformée affine guidée de manière heuristique, où les valeurs minuties des champs triplets sont mises à jour avec

$$\begin{bmatrix} xnew \\ ynew \end{bmatrix} = \begin{bmatrix} \cos(\theta\Delta) & -\sin(\theta\Delta) \\ \sin(\theta\Delta) & \cos(\theta\Delta) \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} x\Delta \\ y\Delta \end{bmatrix}, \quad \textbf{II.8)}$$

$$\text{Et} \qquad \theta_{\text{new}} = \theta - \theta_{\Delta}'. \quad \textbf{(III.9)}$$

Où θΔ est la différence d'orientation et (xΔ, yΔ) est la différence de déplacement afin de superposer une impression d'empreinte digitale l'une sur l'autre avec un chevauchement précis et une direction uniforme. Même avec l'avènement d'une distorsion élevée, les points minutieux au sein d'une image d'empreinte digitale devraient également conserver leur position globale par rapport à la majorité des autres minuties des points et d'autres points de repère clés (tels que les noyaux et les deltas) lorsque l'alignement est atteint. Plus précisément, la répartition spatiale ou les propriétés géométriques des minuties voisines devraient avoir une différence minimale même dans les images déformées. Si l'on considère qu'il existe des limites claires en terme de minuties par rapport à la variabilité de positionnement (même avec une forte distorsion), tout en reconnaissant que les différentes impressions d'empreintes digitales ont des différences d'orientation et de déplacement, alors le processus d'enregistrement global réduit considérablement l'espace de recherche. Cela réduit la complexité de l'algorithme pour trouver des paires de minuties, puisque des paires correspondantes sont formées dans des quartiers locaux plus petits (c'est-à-dire des contraintes ajoutées pour les mappages de minuties) une fois alignés. Cela permet d'éviter un processus d'appariement minutai de la force brutale naïve.

Après le processus d'enregistrement, nous pouvons maintenant produire des contraintes géométriques pour la découverte de paires de correspondances minuties, y compris la distance géométrique :

$$\text{dist}_r\,(m_{Ai}, m_{Bi}) = \sqrt{\left(x_{Ai} - x_{Bj}\right)^2 + \left(y_{Ai} - y_{Bj}\right)^2} < r\delta, \qquad \textbf{(III.10)}$$

Et différence d'angle minutieux,

$$\text{dist}_\theta\,(m_{Ai}, m_{Bi}) = \min\left(|\theta_{Ai} - \theta_{Bj}|, 360^\circ - |\theta_{Ai} - \theta_{Bj}|\right) < r\theta\,. \qquad \textbf{(III.11)}$$

La tolérance géométrique rδ est en place pour tenir compte de la distorsion qui peut se produire, tandis que rθ est la tolérance pour les différences angulaires qui peuvent survenir en raison des estimations d'orientation à partir des images d'orientation de la crête. Après l'enregistrement global, une recherche locale peut maintenant être effectuée, afin de faire correspondre les minuties dans le voisinage δ qui répondent aux contraintes des équations 7-9 (voir la figure 5 à droite).

Une fois que des paires minuties authentiques sont produites, une métrique de similarité, habituellement appelée le score de similitude, peut alors être calculée. Le score de similarité doit décrire avec précision comment ressemblent deux empreintes digitales, en tenant compte de toutes les informations pertinentes obtenues à partir des étapes précédentes, telles que le nombre de couples de minuties authentiques et la similarité de chaque paire. Un Score de Similitude (SS) donné dans [38] défini par

$$\text{SS (A, B)} = \frac{n^2 match}{n_A * n_B} \qquad \textbf{(III.12)}$$

Où $n_{match}$ est le nombre de paires de minuties correspondantes, et $n_A$,$n_B$ sont le nombre de minuties dans les régions superposées du modèle et testent les empreintes digitales après l'enregistrement.

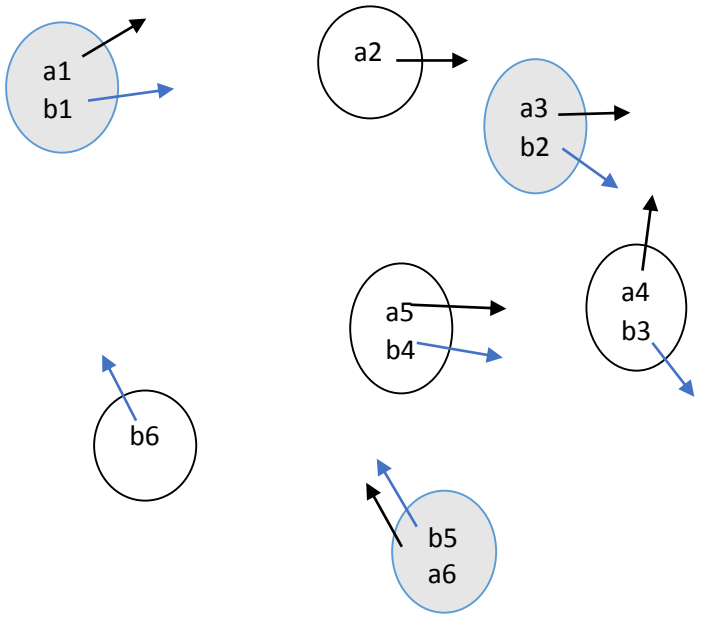



*Figure III-8: Les points Minutai de 2 empreintes différentes sont mappés après l'enregistrement, les cercles gris représentant des paires avec des contraintes confirmées (équations 7 à 9).*

## III.5Etape de comparaison d'empreinte digitale

La figure III. Représente la comparaison entre les minuties d'une image test et les minuties d'une image enregistrée, le nombre de minuties dans cet exemple est 21. Le degré se similarité est de 77% ; c'est-à-dire il y a 16 couple qui sont compatible. Le nombre de pixels maximum est 15 pixels, c'est-à-dire que la distance maximales entre deux minuties 15 pixels. Pour l'angle maximale nous avons pris la valeur $\theta_{max} = 0.24\, rad$ ;

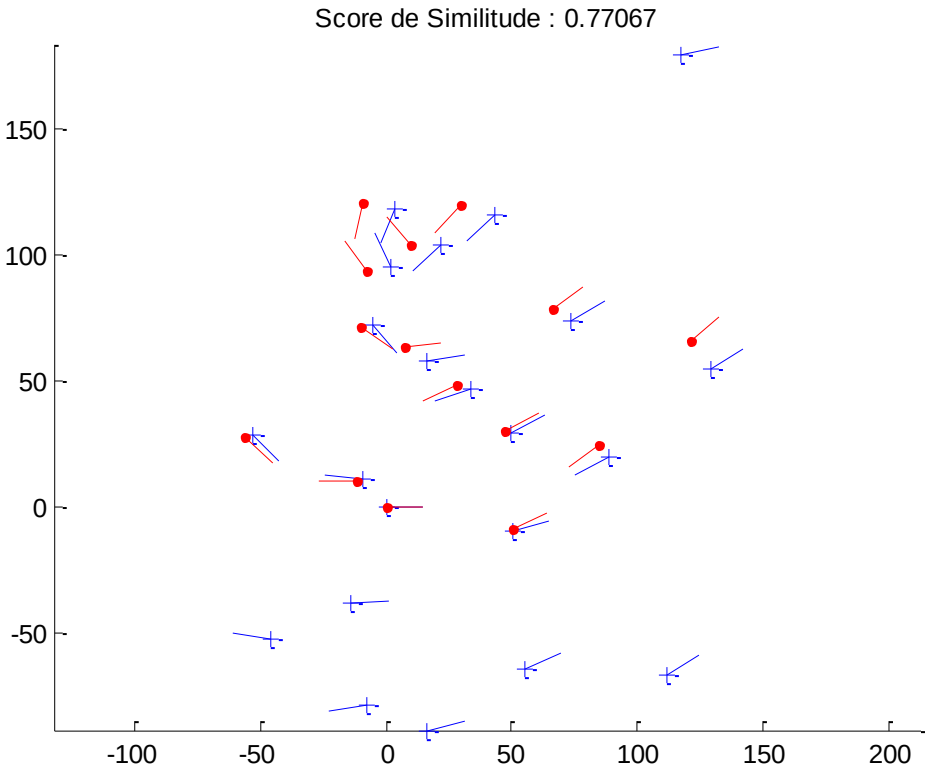



Figure III-9: comparaison les minutai de deux empreints

# III.6Résultats expérimentaux

## III.6.1 Base de données

Une grande base de données d'images des empreintes digitales est une condition préalable pour le développement et l'évaluation des systèmes de reconnaissance des empreintes digitales.

L'expérience a été réalisée sur une la base de données FVC2002 Db1set A qui contient 100 empreintes de doigts (100 doigts avec 8 impressions chacune). Le protocole FVC2002 (Maio et al. (2002)) [39] a été utilisé dans l'expérimentation,

Dans notre travail nous ne disposons que 10 empreintes (10 empreinte avec 8 impressions chacune), que nous avons utilisé.

Chaque échantillon dans le sous-ensemble A (8 empreintes) est comparé aux autres échantillons du même doigt pour calculer le FRR. Donc on a tentatives de n × 8 × 7/2 = 280 authentique. Avec n=10.

Et pour le FAR on compare la première empreinte dans chaque sous-ensemble avec la première des reste des ensembles, donc on tentatives de n × (n − 1)/2 = 45 imposteurs. Si la correspondance de g contre h est effectuée, la symétrique (c'est-à-dire h contre g) n'est pas exécutée pour éviter la corrélation. C'est pour ça on divise par 2 pour les deux cas.

L'amélioration de l'image pour la base de données FVC2002 a été réalisée via la méthode STFT (Short-time Fourier transform) [40], tandis que la méthode d'extraction de minuties basée sur la binarisation / amincissement et la création d'image d'orientation lisse ont été utilisés pour l'extraction de caractéristiques, ainsi que l'algorithme de détection de points de base basé sur la méthode décrite dans [41].

Il convient de noter que les paramètres n'ont pas été réglés pour cette base de données, mais ont toujours réussi à fonctionner très bien.

## III.6.2 Critères d'évaluation

Nous décrivons dans ce paragraphe les critères les plus souvent employés pour évaluer la performance des systèmes de reconnaissance en phase de généralisation. L'objectif est d'obtenir une estimation la plus fidèle possible du comportement du système dans des conditions réelles d'utilisation. Pour cela, des critères classiques comme par exemple le taux de reconnaissance est presque systématiquement utilisé.

En général, quand les échantillons étiquetés à disposition sont suffisamment nombreux, ils sont séparés en deux parties disjointes et en respectant les propositions par classes de la base initiale. Une partie sert pour former la base d'apprentissage et l'autre pour former la base de test.

$$FAR(TFA)(\%) = \frac{nombre\ de\ fausses\ empreintes\ accepteer}{nombre\ totale\ des\ \ empreintes\ de\ test} \qquad \textbf{(III.13)}$$

$$FRR(TFR)(\%) = \frac{nombre\ de\ vraie\ empreintes\ rejetees}{nombre\ totale\ des\ \ empreintes\ de\ test} \qquad \textbf{(III.14)}$$

## III.6.3 Évaluation du système

Les figures 9 et 10 montrent les graphiques FAR et FRR.

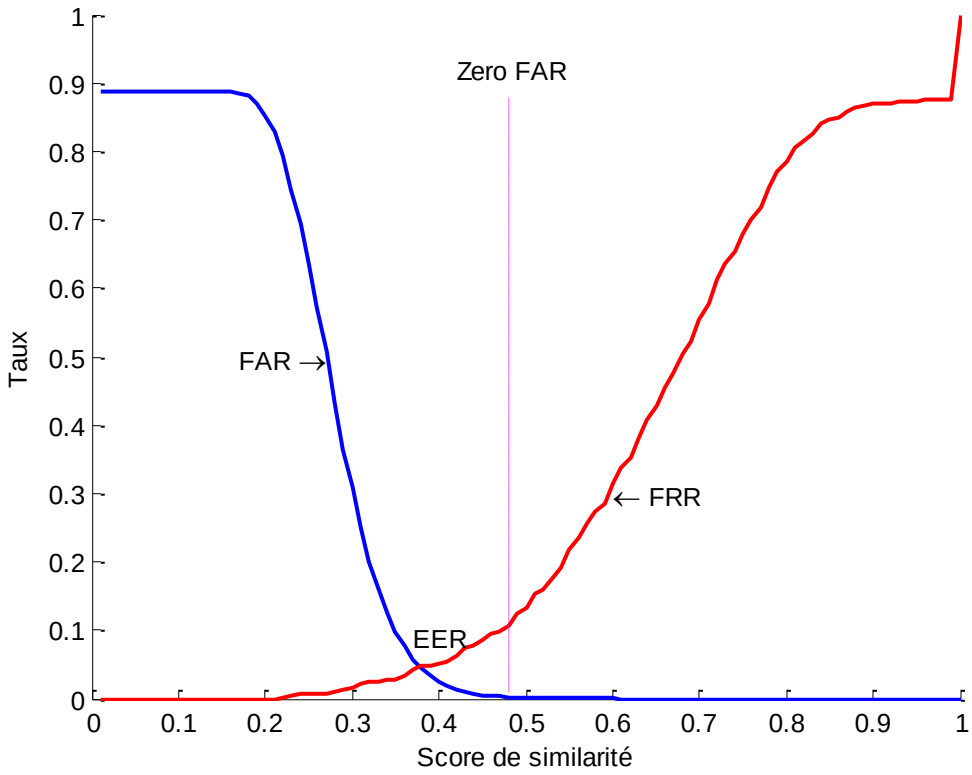



Figure III-10: Représentation graphique des performances d'un système FAR et FRR,

A partir de la figure on remarque que le FAR est constant dans l'intervalle 0 jusqu'à 0.2, ce qui signifie que le nombre des faux images acceptées est le même 90%, haut de là, le FAR commence à diminuer jusqu'à ce qu'il atteint la valeur 0 pour un SS=0.48. Le FRR est nulle pour des SS inférieure à 0.2, puis commence à augmenter. Pour un SS=1, le FRR change brusquement sa valeur de 0.9 à 1 %, ce qui signifiait que le système de reconnaissance d'empreinte a rejeté tous les empreintes. L'EER est 5 %.

– Lorsque le système opère en mode authentification, on utilise ce que l'on appelle une courbe ROC ("Receiver Operating Characteristic"). La courbe ROC (voir Figure III-13) trace le taux de faux rejet(FRR) en fonction du taux de fausse acceptation(FAR). Plus cette courbe tend à épouser la forme du repère, plus le système est performant, c'est-à-dire possédant un taux de reconnaissance global élevé.

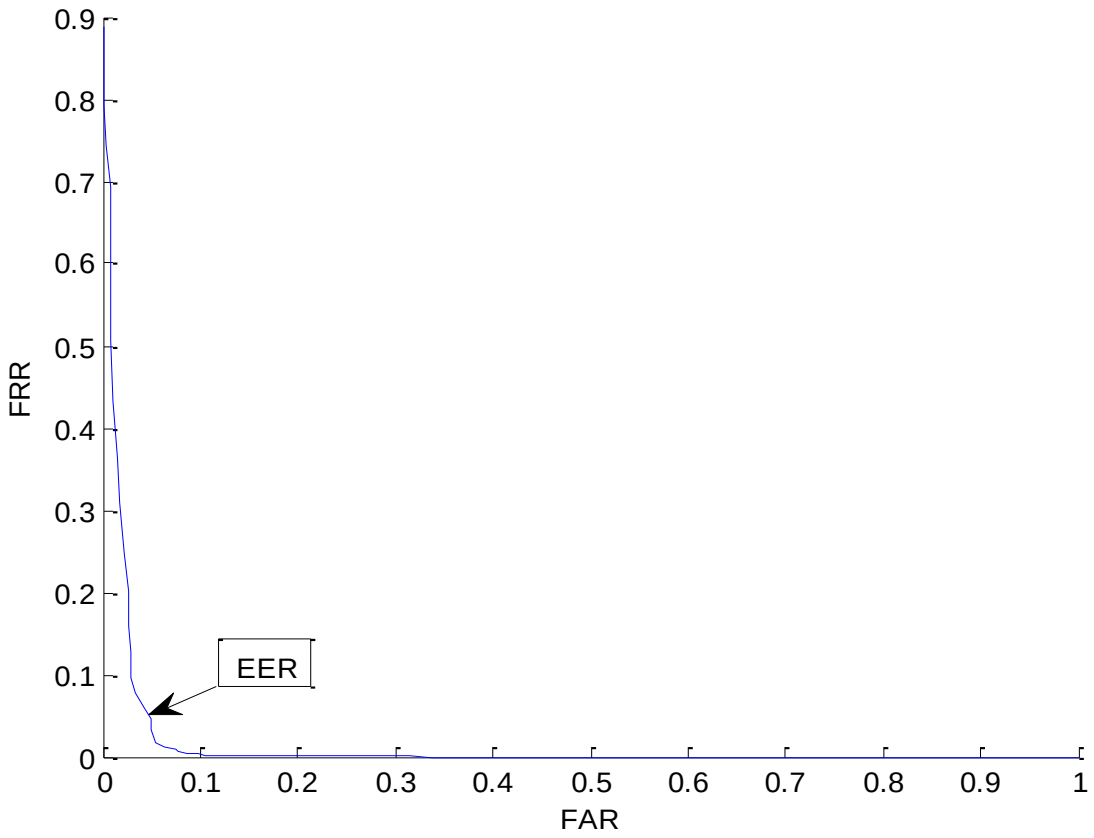



Figure III-11: Courbe ROC.

# III.7Conclusion

Dans ce chapitre nous avons présenté un système complet de vérification d'empreintes digitales. Ce système est basé sur l'extraction des minuties. Les résultats sont jugé acceptable vu que le EER est enivrent 5 %.

# *Conclusion générale*

Au cours de cette mémoire, nous nous sommes intéressés à étudier profondément la biométrie d'une manière générale et la biométrie des empreintes digitales d'une manière plus particulière afin de créer un produit biométrique.
Dans une première étape, nous avons présenté la biométrie, leurs caractéristiques et leurs limitations.

Puis, nous sommes passés à présenter durant le deuxième chapitre les nouvelles approches de reconnaissance par empreinte digitale.
Nous avons donc décrit dans le troisième chapitre les différentes étapes nécessaires à la construction d'un système de reconnaissance des empreintes digitales à savoir : les prétraitements, l'extraction des caractéristiques et l'appariement.
La méthode de comparaison d'empreinte digitale permet d'analyser les aspects d'incertitude et d'imprécision des caractéristiques extraites à partir des empreintes digitales. Cette méthode de comparaison est basée sur la théorie de possibilités. Pour évaluer la méthode d'extraction de caractéristiques proposée, nous avons prouvé sa performance par des résultats similarités faites sur la base publique FVC2002. Le taux d'erreur du système de vérification est 5%.

Nous estimons avoir réalisé un système répondant à l'objectif que nous nous sommes fixés au départ, à savoir la mise en œuvre d'un système permettant la reconnaissance d'individus et le contrôle d'accès.

# Références


[1] X. Xia and L. O'Gorman, "Innovations in fingerprint capture devices", *Pattern Recognition*, Vol. 36, pp. 361-369, 2003.

[2] Identification Services from Identix company, website : www.identix.com/iis 12/03/2017

[3] S. Prabhakar, S. Pankanti, and A. K. Jain. Biometric recognition: Security and privacy concerns. IEEE Security & Privacy, 1:33–42, 2003.

[4] J. Mahier, M. Pasquet, C. Rosenberger, and F. Cuozzo. Biometric authentication. Encyclopedia of Information Science and Technology, pages 346–354, 2008. [Cite p. 8, 9, 158]

[5] N. Rudin, K. Inman, G. Stolovitzky, and I. Rigoutsos. Biometrics : Personal Identification in Networked Society, chapter DNA Based Identification, pages 287– 309. Kluwer Academic Publishers, 2002. [Cité p. 8]

[6] N. Morizet, "Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris", Ecole Nationale Supérieure des Télécommunications, 2009.

[7] International Biometric Group. http ://www.biometricgroup.com/, 2010. [Cite p. 11,15, 154]

[8] ISO/IEC 19795-1. Information technology – biometric performance testing and reporting – part 1 : Principles and framework,

[9] M. Theofanos, B. Stanton, and C. A. Wolfson. Usability & Biometrics: Ensuring Successful Biometric Systems. National Institute of Standards and Technology (NIST), 2008.

[10] ISO/IEC FCD 19792. Information technology – security techniques – security evaluation of biometrics, 2008.

[11] P. Meenen, R. Adhami, "Fingerprinting for Security", IEEE potentials, vol. 20, n°3, p. 33-38, 2001.

[12] R. Chellappa, C. Wilson, S. Sirohey, "Human and Machine Recognition of Faces: A Survey", Proceedings of IEEE, vol. 83, p.705-740, 1995.

[13] W. Zhao, R. Chellappa, A. Rosenfeld, P.Phillips, "Face Recognition: A Literature Survey", UMD CAR-TR, 2000.

[14] Bruce E. Koenig "Spectographic voice identification: A forensic survey", FBI,

[15] Engeineering section, Technical Service Division, 1986.A. Chaari, "Nouvelle approche d"identification dans les bases de données biométriques basée sur une classification non supervisée", Thèse de doctorat, Université d"Evry Val d"Essonne, 2009.

[16] N. Morizet, "Reconnaissance Biométrique par Fusion Multimodale du Visage et de l"Iris", Ecole Nationale Supérieure des Télécommunications, 2009

[17] S. Hocquet, "Authentification biométrique adaptative Application à la dynamique de frappe et à la signature manuscrite", Thèse de doctorat, Université François Rabelais Tours, 2007.

[18] S. Hocquet, "Authentification biométrique adaptative Application à la dynamique de frappe et à la signature manuscrite", Thèse de doctorat, Université François Rabelais Tours, 2007.

[19] A. K. Jain and A. Ross, "Multibiometric systems", Communications of the ACM, special issue on multimodal interfaces, vol. 47, no. 1, p. 34-40, 2004.

[20] Y. Chen, S. Dass, A. Jain, "Fingerprint Quality Indices for Predicting Authentication Performance", Proceedings of Fifth International Conference on Audio- and Video-ased Biometric Person Authentication (AVBPA), p. 160-170, 2005.

[21] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact of Artificial “Gummy” Fingers on Fingerprint Systems", Proceedings of SPIE : Optical Security and Counterfeit Deterrence Techniques IV, p. 275-289, 2002.
[22] T. Putte, J. Keuning, "Don’t Get Your Fingers Burned", Proceedings of IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, p. 289-303, 2000.
[23] A. Ross and A. Jain, "Information fusion in biometrics", Pattern Recognition Letters, vol. 24, no. 13, p. 2115-2125, 2003.
[24] A. Ross, K. Nandakumar, A. Jain, "Handbook of Multibiometrics". Springer-Verlag New York, Inc., 2006.
[25] K. Nandakumar, "Integration of Multiple Cues in Biometric Systems". Master’s thesis, Michigan State University, 2005.
[26] K. Chang, K. Bowyer, P. Flynn, "An Evaluation of Multimodal 2D+3D Face Biometrics". IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 27, no. 4, p. 619-624, 2005.
[27] H. Touati et N. Adlene, “Identification des empreintes digitales”, Mémoire de fin d‟études, Ecole Militaire polytechnique, Alger, 2004.
[28] S. Prabhakar, A. Jain, L. Hong et S. Pankanti, “FingerCode: A Filterbank for Fingerprint Representation and Matching”, 1999.
[29] A.K. Jain et A. Ross, “Fingerprint Mosaicking”, IEEE Intentional Conference on ICASSP, Vol. 4, May 2002.
[30] Viscaya et Gerhardt, “A Nonlinear Orientation Model for Global Description of Fingeprints”, Pattern Recognition, Vol. 29, no. 7, pp. 1221–1231, 1996.
[31] B.G. Sherlok, D.M. Monro et K. Millard, “Fingerprint Enhancement By Directional Fourier Filtering”, IEEE Proc. Vis. Image Signal Process, Vol. 141, no. 2, pp. 87-94, April 1994.
[32] L. Hong, Y. Wan et A.K. Jain, “Fingerprint Image Enhancement: Algorithm and Performance Evaluation”, Pattern recognition and Image Processing Loboratory, Michigan State University, 1998.
[33] D. Maio, D. Maltoni, “Direct Grey -Scale Minutiae Detection in Fingerprints”, IEEE Trans. Pattern Anal. Machin Intell., Vol. 19, no. 1, pp. 27-40, 1997.
[34] B.C. Seow, S.K. Yeoh, S.L. Lai et N.A. Abu, “Image Based Fingerprint Verification”, Student Conference on Reseach and Development Proceedings, Malaysia, 2002.
[35] D. Maio, D. Maltoni, “Direct Grey -Scale Minutiae Detection in Fingerprints”, IEEE Trans. Pattern Anal. Machin Intell., Vol. 19, no. 1, pp. 27-40, 1997.
[36] A.M. Bazen and S.H. Gerez, "Directional Field Computation for Fingerprints Based on the Principal Component Analysis of Local Gradients", *in Proceedings of ProRISC2000, 11th Annual Workshop on Circuits, Systems and Signal Processing*, Veldhoven, Netherland, November 2000.
[37] A.K. Jain, L. Hong, S. Pankanti and R. Bolle, "An Identity-Authentication System Using Fingerprints", *Proceedings of the IEEE*, Vol. 85, No. 9, pp. 1365-1388, 1997.
[38] Liang, X. & Asano, T. (2006). Fingerprint matching using minutia polygons, ICPR06, pp. I : 1046–1049.
[39] Maio, D., Maltoni, D., Cappelli, R., Wayman, J. & Jain, A. K. (2002). "fvc2002: Second fingerprint verification competition"
[40] Chikkerur, S., Wu, C. & Govindaraju, V. (2004). A systematic approach for feature extraction in fingerprint images, Biometric Authentication LNCS 3072: 344–350.
[41] Julasayvake, A. & Choomchuay, S. (2007). An algorithm for fingerprint core point detection, Proc. of International Symposium on Signal Processing and its Applications 2007 (ISSPA-2007) 1(1): 1–4.