

Sommaire

Résumé

Abstract

Remerciement

Sommaire

Liste des figures

Liste des tableaux

Introduction générale..... 1

Chapitre I Les caractéristiques biométriques

I.1 Introduction..... 3

I.2 Les Caractéristiques biométriques..... 3

I.3 Analyse et mesure des caractéristiques biométriques..... 3

I.3.1 Analyse comportementale..... 3

i) La dynamique des frappes au clavier (*keystroke-scan*) 4

ii) La reconnaissance vocale (*voice-scan*) 5

iii) La dynamique des signatures (*signature-scan*) ... 6

I.3.2 Analyse morphologique..... 7

i) Reconnaissance par empreintes digitales (*finger-scan*) 7

ii) Reconnaissance par Iris..... 9

iii) Reconnaissance faciale..... 10

I.4 Choix d'une caractéristique biométrique..... 11

I.5 Architecture et fonctionnement des systèmes biométriques.....	13
I.6 Performance des systèmes biométriques.....	14
I.7 Conclusion.....	15

Chapitre II : Tour d’horizon sur les empreintes digitales

II.1. Introduction.....	16
II.2.Historique.....	16
II.3 Caractéristiques d’une empreinte digitale	17
II.4 Structure d’un système complet de reconnaissance d’empreinte	18
II.4.1 Acquisition de l’empreinte.....	19
II.4.1 .1 Les familles de capteurs	19
II.4.2 L’extraction de la signature.....	20
II.4.3 le stockage et l’appariement.....	20
II.5 Représentation de l’empreinte digitale	21
II.5.1 Représentation en image.....	22
II.5.2 Représentation avec les descripteurs de texture.....	22
II.5.3 Représentation en minuties.....	22
II.6 Conclusion.....	24

Chapitre III : Approche classique d’extraction de minuties

III.1 Introduction.....	25
III.2 Approche Classique d’extraction de minuties.....	26
III.2.1 La Binarisation.....	26
III.2.2 La Squelettisation (amincissement)	27
III.2.3 L’extraction des minuties.....	27
III.2.3.1 Les problèmes rencontrés lors de l’extraction des minuties.....	29

III.2.3.2 Elimination des fausses minuties	30
III.2.4.1 Traitement des terminaisons détectées.....	30
III.2.4.2 Traitement des bifurcations détectées.....	31
III.3 Approche d'extraction directe à partir de l'image en niveau de gris.....	31
III.4 Conclusion.....	32

Chapitre IV : Détection de ligne, jonctions de lignes et terminaisons dans l'empreinte digitale

IV.1 Introduction.....	33
IV.1.1 L'empreinte digitale : une image de lignes.....	33
IV.2 La détection des lignes dans une empreinte digitale.....	34
IV.2.1 Modélisation du filtre par une fonction.....	34
IV.2.2 Extension du filtre en deux dimensions.....	35
IV.2.3 Représentation de la fonction de détection	35
IV.2.4 Représentation de la fonction de projection.....	36
IV.2. 5 Algorithme de détection des lignes de crêtes	36
IV.2.5.1 Filtrage de l'empreinte digitale	36
IV.2.5.2 Suppression des non maxima par l'algorithme de Canny.....	37
IV.3 Détection des jonctions et terminaisons des lignes.....	39
IV.3.1 Estimation de la courbure locale d'une ligne	39
IV.3.2 Localisation des jonctions des lignes.....	42
IV.3.3 Localisation des terminaisons.....	43
IV.4 Conclusion.....	44

Chapitre V Résultats expérimentaux

V.1 Introduction	45
V.2 Extraction des minuties par l'approche binarisation/Squelettisation	46
V.2.1 L'image de l'empreinte digitale	46
V.2.2 La Binarisation	46
V.2.3 La Squelettisation	47
V.2.4 La détection des minuties	48
V.3 Approche de détection des lignes, jonctions des lignes et terminaisons	49
V.3.1 Algorithme de détection des lignes	51
V.3. 2 Implémentation de l'approche de détection	51
V.3.2.1 Implémentation du filtrage	51
V.3.2.2 Implémentation de la suppression des non maxima	52
V.4 Conclusion	50
VI Conclusion générale	52

Bibliographie

Liens Internet

Liste de figures

Fig I.1. Reconnaissance par la dynamique du clavier.....	4
Fig I.2. Identification vocale.....	5
Fig I.3. Identification par signature.....	6
Fig I.4. Représentation d’une empreinte digitale.....	7
Fig I.5. Techniques d’acquisition d’empreinte digitale.....	8
Fig I.6 Localisation de l’iris dans l’œil.....	9
Fig I.7. Reconnaissance faciale.....	10
Fig I.8. Critères de choix des caractéristiques biométriques.....	12
FigI.9. Architecture d’un système biométrique.....	13
Fig I.10. Performance des systèmes biométriques.....	14
FigII.1 Caractéristiques d’une empreinte digitale	17
Fig II.2 Exemples de quatre familles de crêtes.....	17
Fig II. 3 Les trois principales classes d’empreintes : Arche, Boucle, tourbillon.....	18
FigII.4 architecture generale d’un systeme complet de reconnaissance d’empreinte digitale	19
Fig II.5. Les caractéristiques principales des minuties	22
Fig II.6. Exemple d’une représentation d’une empreinte par sa carte de minuties.....	23
Fig III.1. Quelques minuties sur une image d’empreinte.....	25
Fig III.2 Extraction des minuties par Binarisation.....	26
Fig III.3 Processus de binarisation/amincissement.....	27
Fig III.4 Le nombre de connexion et le type des minuties.....	28
Fig III.5 Détection des minuties sur l’image amincie.	28
Fig III.6 Des images d’empreintes de différentes qualités.....	29

FigIII.7 Exemple de détection de fausses minuties.....	30
Fig III.8 Exemple de minuties détectées	30
Fig III.9 Validation des terminaisons détectées	31
Fig III.10 Définitions associées à une bifurcation lors de la phase de validation.....	31
Fig IV.1 Projection des crêtes sur une image orientée	33
Fig.IV.2. Filtre optimal de détection des contours de types lignes de crêtes	34
Fig.IV.3 Filtrage de l’empreinte digitale.....	37
Fig.IV.4 Résultat du détecteur de lignes.....	35
Fig.IV.5 Jonction de deux lignes.....	39
Fig.IV.6 exemples de courbures.....	39
Fig.IV.7 exemple d’estimation de courbure.....	42
Fig.IV.8 Propagation des vecteurs d'orientation à partir des frontières.....	43
Fig.IV.9 Réponse du détecteur de lignes pour les terminaisons.....	43
Fig V.1 schéma récapitulatif sur l’approche de détection de minuties par binarisation	46
Fig V.2 Exemple1 de binarisation et squelettisation	47
Fig V.3 Exemple2 de binarisation et squelettisation	47
Fig V.4 Exemple3 de binarisation et squelettisation	48
Fig V.5 Exemple4 Extraction de minuties	48
Fig V.6 Exemple 5 Extraction de minuties	49
Fig V.7 Exemple 6 Binarisation, squelettisation et extraction des minuties.....	49
Fig V.8 schéma récapitulatif sur la détection des lignes	50
Fig V. 9 la console du programme principal	51
Fig.V. 10 Exemple 7 Implémentation du filtrage	52
Fig.V. 11 Exemple 8 Implémentation du filtrage	52
Fig V.12 exemple 9 Détection des lignes	53
Fig V.13 exemple 10 Détection des lignes	53

Liste de tableaux

Tab I.1. Avantages et inconvénients de l'identification par la dynamique de Clavier.....	4
Tab I.2. Avantages et inconvénients de l'identification par la voix.....	5
Tab I.3. Avantages et inconvénients de l'identification par signature.....	6
Tab I.4. Avantages et inconvénients de l'identification par empreinte digitale.....	8
Tab I.5. Avantages et inconvénients de l'identification par Iris.....	8
Tab I.6. Avantages et inconvénients d'identification faciale.....	9

Introduction Générale

Introduction générale

L'identification des personnes par la biométrie s'est imposée comme une approche de sécurisation fiable dans le marché, différentes techniques ont été développées en exploitant les caractéristiques humaines, ces techniques appelées généralement « méthode biométriques » ont donné naissance à ce qu'on appelle le « le mot de passe biométrique ».

L'avantage d'un mot de passe biométrique est lié au fait qu'il ne pourrait pas être volé, oublié ou transmis à une autre personne. Certaines caractéristiques sont plus fiables que d'autres mais toutes doivent assurer une représentation unique et infalsifiable de l'individu. Le choix d'une méthode biométrique dépend de son efficacité, son coût et l'effort requis par l'utilisateur.

Dans notre travail, nous avons choisi « l'empreinte digitale » comme modalité d'identification de par son ancienneté, sa mise à l'épreuve et son coût abordable. Les minuties, qui représentent des discontinuités locales dans le flot des crêtes de l'empreinte digitale, sont utilisées pour l'identification. Cependant, l'image d'empreinte est rarement en parfait état, elle est souvent entachée de bruit empêchant l'extraction d'une carte de minuties correcte. Cette dégradation peut être le cumul de plusieurs facteurs : dispositif de prise de vue, état de la peau (sécheresse, humidité, plis, blessures), pression du doigt, etc. Une étape critique dans le processus d'identification par empreinte digitale consistera à une extraction fiable des minuties à partir de l'image de l'empreinte. La plupart des systèmes utilise l'approche classique de détection de minuties basée sur la binarisation/squelettisation. Cette approche est simple et fiable lorsque l'on dispose d'un squelette précis de l'image. L'inconvénient vient de la perte d'information et du bruit introduit au cours de la Binarisation, ce qui provoque l'apparition d'une multitude de fausses minuties et nécessite un traitement à posteriori relativement, en plus l'étape de squelettisation est couteuse en temps de calcul car plusieurs balayages sont nécessaires selon l'épaisseur des stries de l'empreinte digitale. Bien que des progrès significatifs aient été enregistrés pour les systèmes d'identification par empreinte digitale, la performance est encore loin d'être satisfaisante. Les travaux de recherche se basent actuellement sur l'amélioration de l'image de l'empreinte avant de passer à l'extraction et / ou l'élimination des fausses minuties après l'extraction. Ces considérations nous ont amené à étudier une autre approche qui porte sur la détection des lignes, jonctions des lignes et terminaisons directement de l'image en niveau de gris en utilisant la courbure. Etant donné

que l’empreinte digitale est une image de lignes. Nous avons testé et validé les résultats d’un détecteur de lignes sur les images d’empreintes digitales et comme perspectives, nous souhaiterons implémenter la détection des jonctions et terminaisons pour extraire de l’empreinte digitale les minuties de type bifurcations et terminaisons.

Le mémoire sera présenté suivant les chapitres suivants :

Le premier chapitre est dédié à la présentation des caractéristiques ou modalités biométriques. Nous citerons les avantages et limites de chacune, nous expliquerons ainsi l’architecture générale d’un système d’identification biométrique.

Le deuxième chapitre mettra l’accent sur la modalité la plus ancienne et la plus mature d’identification biométrique qui est l’empreinte digitale, nous étudierons les propriétés de cette modalité ainsi que la structure complète d’un système de reconnaissance par empreinte digitales.

Le troisième chapitre traitera l’approche classique d’extraction de minuties, basée sur la binarisation/squelettisation dont l’avantage réside dans la simplicité à extraire et détecter les minuties lorsque l’on dispose d’un squelette précis de l’image mais l’inconvénient vient de la perte de l’information et du bruit introduit lors du processus de squelettisation.

Le quatrième chapitre introduit une méthode optimale d’extraction de minuties visant l’amélioration préalable de l’image de l’empreinte digitale avant de passer à l’extraction. Nous y montrons les avantages de cette dernière par rapport aux approches classiques.

Le cinquième sera consacré à l’implémentation de deux méthodes d’extraction de minuties à partir de l’empreinte digitale, la première est basée sur le processus de Binarisation/squelettisation et la deuxième se base sur la détection des lignes et comme perspective nous souhaitons utiliser la détection des jonctions et terminaisons des lignes pour extraire de l’empreinte digitale, les minuties de types Bifurcations et Terminaisons.

Et en fin Une conclusion générale fera le point de notre recherche où nous dévoilons nos perspectives.

Chapitre I

Les caractéristiques biométriques

I.1 Introduction

Plusieurs techniques biométriques ont été développées par la recherche scientifique pour identifier les personnes. Ces techniques, généralement appelées *méthodes biométriques*, ont donné naissance à ce qu'on appelle **le mot de passe biométrique**. **L'avantage principal d'un mot de passe biométrique est qu'il** ne pourrait pas être volé, oublié ou transmis à une autre personne. En effet, chaque individu possède sa propre caractéristique biométrique, permettant de l'identifier. Par conséquent et dans un futur relativement proche, le mot de passe biométrique remplacera le mot de passe conventionnel dans toutes les applications nécessitant un niveau élevé de sécurité [1].

I.2 Les Caractéristiques biométriques

Une caractéristique biométrique est une donnée contenant l'essentiel d'informations permettant de différencier deux individus. Pratiquement n'importe quelle caractéristique physiologique ou comportementale peut être considérée comme une caractéristique biométrique, dans la mesure où elle est [2]:

Universelle : existe chez tous les individus.

Unique : différente pour chaque individu.

Permanente : stable dans le temps.

Enregistrable : atteignable.

Mesurable : une technologie de capteur existe.

Utilisable : acceptation par l'utilisateur.

Non imitable : difficilement copiable.

I.3 Analyse et mesure des caractéristiques biométriques

L'identification biométrique consiste à analyser l'une des caractéristiques comportementales ou morphologiques de l'individu. On distingue dans la pratique deux technologies biométriques :

I.3.1 Analyse comportementale

L'individu possède plusieurs éléments liés à son comportement qui lui sont propres :

i) La dynamique des frappes au clavier (*keystroke-scan*)

Les frappes au clavier sont influencées par le texte tapé et sa nature, certaines attaques utilisent ce moyen pour essayer d'inférer son contenu ou sa nature de façon à remonter jusqu'à un mot de passe.

Généralement les facteurs comportementaux pris en compte sont :

- Les durées entre les frappes.
- La fréquence des erreurs.
- La durée de la frappe elle-même.

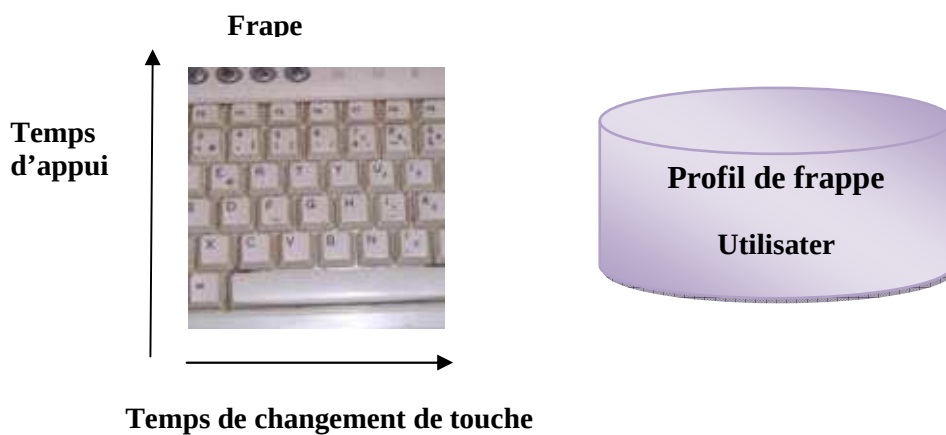


Fig I.1. Reconnaissance par la dynamique du clavier

Cette technique consiste à demander à l'utilisateur de saisir son mot de passe une dizaine de fois de suite. A l'aide d'un algorithme qui exploite le temps d'appui sur chaque touche et le temps entre les touches, la dizaine de saisie est « moyennée » pour construire un Profil de frappes qui servira de référence.

Aux accès suivants, en suivant la même approche, la saisie du mot de passe donnée sera couplée à un profil de frappe qui sera comparé au profil de référence.

Avantages	Inconvénients
Moyen non intrusif qui exploite un geste naturel.	Dépendance de l'état physique de la personne (âge, maladie...).

Tab I.1. Avantages et inconvénients de l'identification par la dynamique de Clavier [Clu, 03]

ii) La reconnaissance vocale (*voice-scan*)

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

Les données utilisées par la reconnaissance vocale proviennent à la fois des facteurs physiologiques (le sexe, l'âge, la tonalité, la fréquence, l'accent, l'harmonie, ...etc.) et comportementaux (la vitesse, le rythme, ...).



Fig I.2. Identification vocale [3]

Avantages	Inconvénients
Disponible via les réseaux téléphoniques. - les imitateurs utilisent les caractéristiques vocales sensibles au système auditif humain, mais ne sont pas capable de récréer les harmoniques de la voix, servant de base à l'identification. Il est quasi impossible d'imiter la voix stockée dans la base de données. - Non intrusif.	- L'utilisation d'un micro nécessite un dispositif adapté présent sur l'environnement. - Sensibilité à l'état physique et émotionnel de l'individu. - Sensibilité aux conditions d'enregistrement de la parole (bruit ambiant, parasite, qualité du microphone, qualité de l'équipement, lignes de transmission).

TabI.2. Avantages et inconvénients de l'identification par la voix [Clu, 03]

iii) La dynamique des signatures (*signature-scan*)

Le procédé est habituellement combiné à une palette graphique (ou un équivalent) munie d'un stylo.



Fig I.3. Identification par signature

lors de la signature, Ce dispositif va mesurer (la vitesse, l'ordre des frappes, la pression et les accélérations, le temps total...)

Les difficultés liées à la capture d'une signature viennent du fait qu'une personne ne signe jamais deux fois de la même façon, même à quelques secondes d'intervalle. En effet suivant les émotions ou la fatigue, une signature peut fortement évoluer. D'où la mise au point d'algorithmes très complexes capables de prendre en compte ces évolutions possibles.

Avantages	Inconvénients
Geste naturel qui responsabilise le signataire.	- Détermination d'un seuil. - Dépendance de l'état émotionnel de la personne.

Tab I.3. Avantages et inconvénients de l'identification par signature [Clu, 03]

I.3.2 Analyse morphologique

Il existe plusieurs caractéristiques physiques qui se révèlent être uniques pour un individu, et il existe également pour chacune d'entre elles plusieurs façons de les mesurer :

i) Reconnaissance par empreintes digitales (finger-scan)

L'empreinte digitale est caractérisée par le dessin représenté par les crêtes et sillons de l'épiderme, son unicité est valable pour chaque individu.

Il est pratiquement difficile de mémoriser toutes les informations fournies par ce dessin, il est préférable alors d'en extraire les caractéristiques principales telles que les bifurcations des crêtes, les terminaisons etc une empreinte complète contient en moyenne une centaine de ce genre de points appelée « les minuties » mais les contrôles ne sont effectués qu'à partir d'une quinzaine de points ((12 au minimum vis-à-vis de la loi), Statistiquement, il est impossible de trouver 2 individus présentant 12 points caractéristiques identiques, même en considérant une population de plusieurs dizaines de millions de personnes [10].

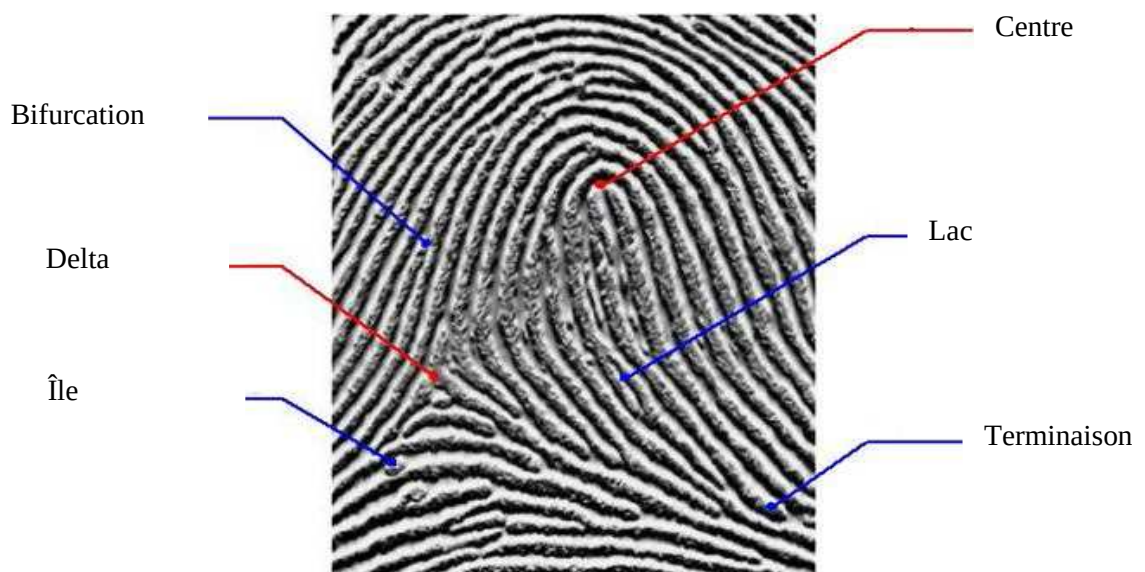


Fig I.4. Représentation d'une empreinte digitale [7]

il existe plusieurs techniques d'acquisition de l'empreinte digitale (capteur optique, thermique, ultrason...), le procédé consiste former une image à partir des points de contact du doigt sur le capteur comme le montre la Figure Fig I.5 :

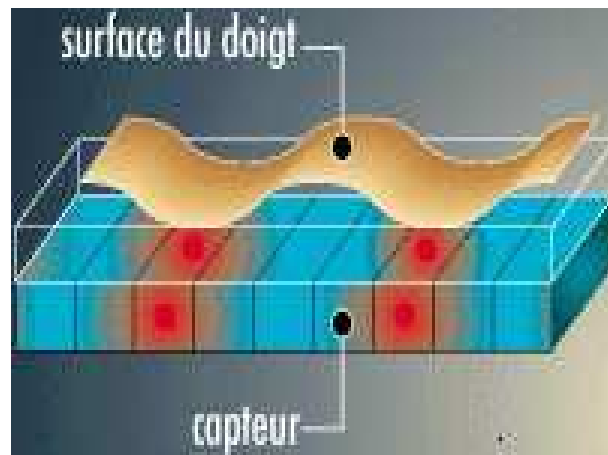


Fig I.5. Techniques d'acquisition d'empreinte digitale

Avantages	Inconvénients
• Son ancienneté et sa mise à l'épreuve. • Sa résistance aux changements de température, jusqu'à un certain point. • Son cout abordable. • Sa capacité à fournir des résolutions de plus de 500 dpi. • Bon compromis entre le taux de faux rejet (le risque de rejeter quelqu'un à tort) et le taux de fausse acceptation (le risque d'accepter une personne par erreur).	• Besoin de la coopération de l'utilisateur (pose correcte du doigt sur le lecteur). • Il est possible que l'empreinte d'utilisateurs précédents reste latente, d'où une possibilité de dégradation de l'image par sur-impression. • Apparition possible de rayure sur la fenêtre. • D'autre part, le dispositif CCD peut s'user avec le temps et devenir moins fiable. • Problème de contraste (doigt propre et sec devient trop clair tandis qu'un doigt humide devient très foncé).

Tab I.4. Avantages et inconvénients de l'identification par empreinte digitale [Clu, 03]

ii) Reconnaissance par Iris

L'iris est la zone colorée visible à l'intérieur de l'œil, l'iris est responsable de régler la taille de la pupille et déterminer la quantité de lumière qui y pénètre. La forme et l'apparence générale de l'iris est déterminée génétiquement, sa texture détaillée est propre à chaque individu. De plus, cette texture est stable et ne peut être modifiée sans perte importante des capacités visuelles. La première étape de la reconnaissance par l'iris est d'isoler la zone de l'iris de l'œil dans une image numérique.

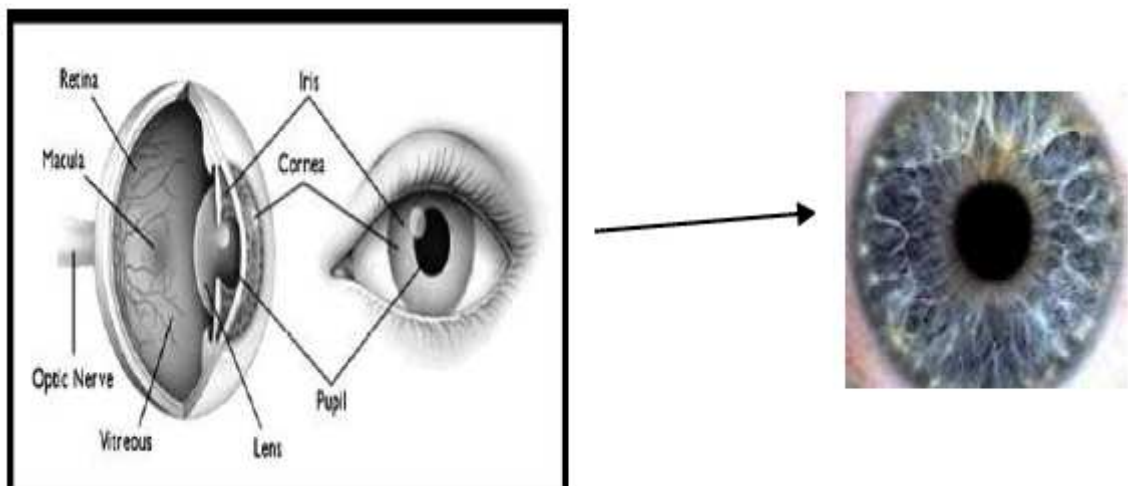


Fig.I.6. Localisation de l'iris dans l'œil [8]

L'individu se place en face du capteur (caméra CCD/CMOS) qui scanne son iris. L'iris présente une quasi-infinité de points caractéristiques qui ne varient pas pendant la vie d'une personne contrairement à *la couleur de l'iris* qui, elle, peut changer. Des problèmes peuvent se poser à cause des reflets qui nécessite d'avoir un éclairage restreint et maîtrisé, et lors de la détection des faux yeux (photos) et autres fraudes. [10]

Avantages	Inconvénients
• Fiable. • Grande informations contenues dans l'iris. • Des vrais jumeaux ne sont pas confondus.	• Système intrusif mal accepté physiologiquement (hygiène, proximité de l'objectif). • Contrainte d'éclairage.

Tab I.5. Avantages et inconvénients de l'identification par Iris [Clu, 03]

iii) Reconnaissance faciale

Les images faciales sont probablement la caractéristique biométrique la plus communément employée pour effectuer l'identification d'une personne.

L'utilisation d'une caméra permet de capter la forme du visage d'un individu et d'en dégager certaines particularités. Selon le système utilisé, l'individu doit être positionné devant l'appareil ou peut être en mouvement à une certaine distance. Les données biométriques qui sont obtenues sont par la suite comparées au fichier référence.

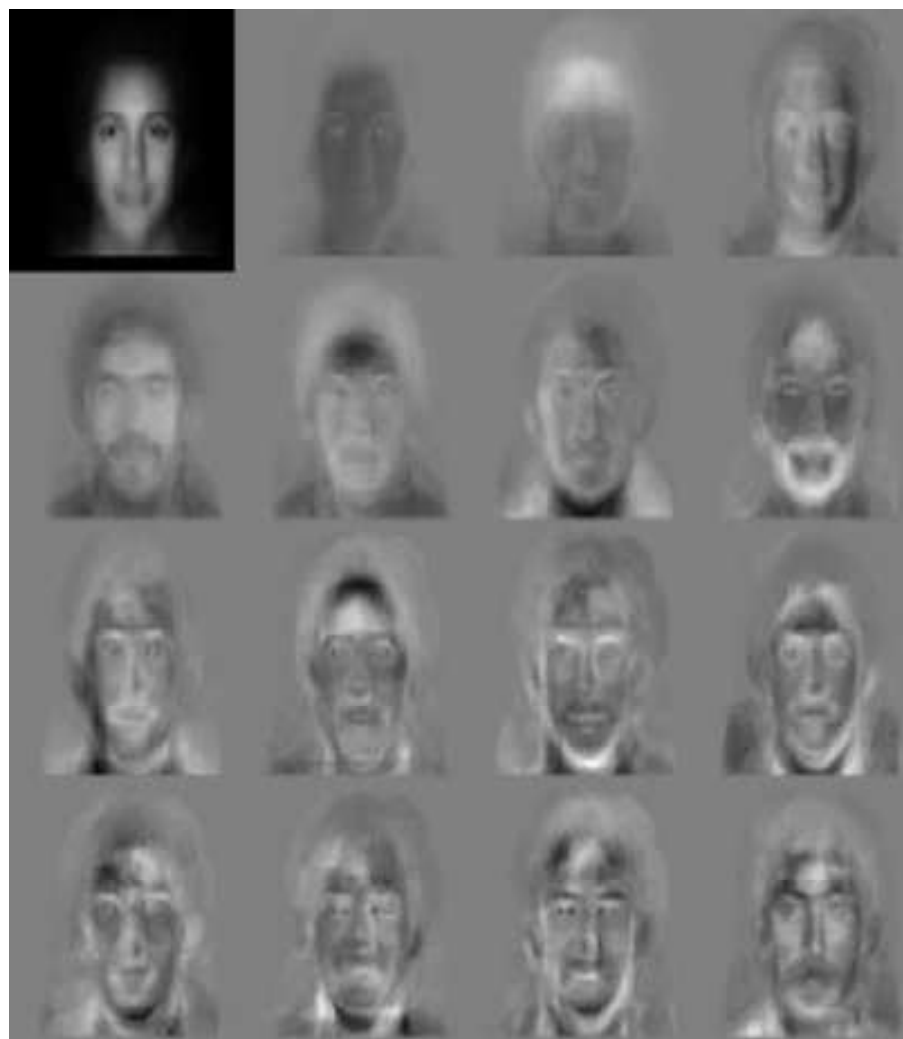


Fig I.7. Reconnaissance faciale [12]

La reconnaissance par le visage est basée sur des attributs faciaux mesurables comme l'écartement des yeux, des sourcils, des lèvres, la position du menton, la forme...etc.

Avantages	Inconvénients
• Technique peu couteuse. • Absence de contact avec le capteur. • Méthode non intrusive pour la personne. • Pas de risque sur la santé.	• Les vrais jumeaux ne sont pas différenciés. • Le visage n'est pas traditionnellement reconnu comme un mécanisme fiable d'authentification (il peut être dupé l'utilisation de maquillage ou un masque de silicone). • Technique trop sensible au changement d'éclairage. • Changement d'échelle (taille du visage ou distance de la caméra). • Changement de position lors de l'acquisition de l'image (inclination de la tête ou expression). • Tout élément tel que les lunettes de soleil, chapeau, moustache, barbe, blessure peut causer des anomalies avec les systèmes d'identification du visage.

Tab I.6. Avantages et inconvénients d'identification faciale [Clu, 03]

I.4 Choix d'une caractéristique biométrique

Le choix d'une modalité dépend de sa nature d'un coté et du niveau de sécurité qu'elle apporte aux applications (Certaines modalités présentent des contraintes d'ergonomie, de coût et d'acceptabilité) ainsi que l'environnement de leurs usages (facilité d'emploi, d'analyse, de stockage, et de vérification).

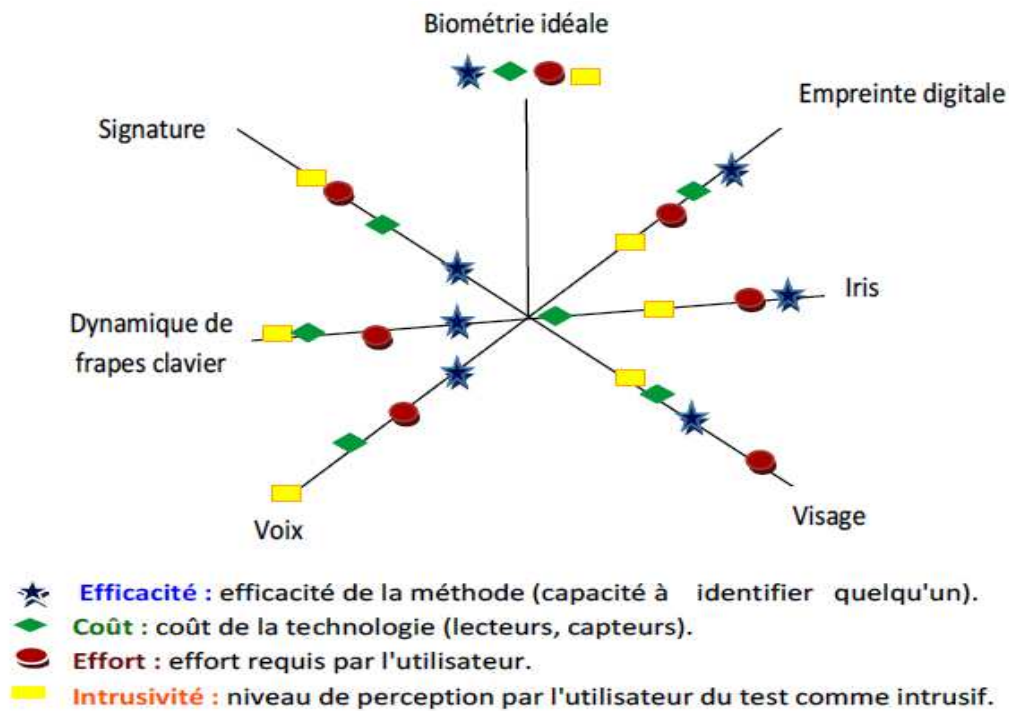
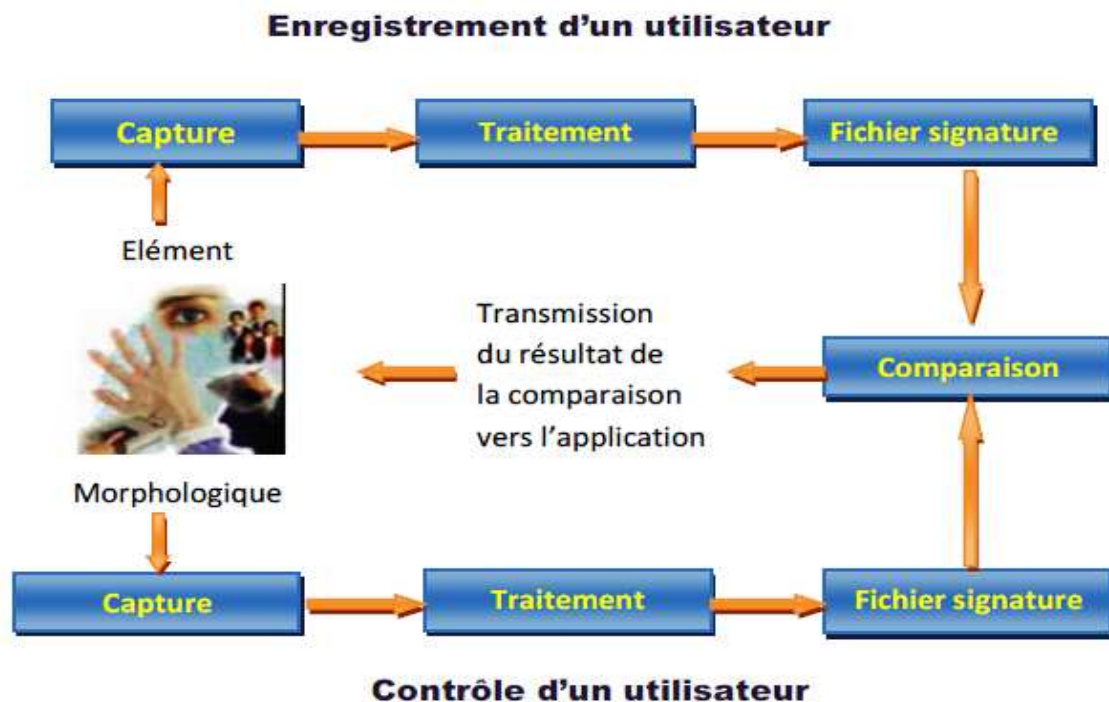


Fig I.8. Critères de choix des caractéristiques biométriques [9]

Nous remarquons dans la figure Fig 1.8 que l'empreinte digitale est proche d'être une modalité idéale par rapport aux autres caractéristiques biométriques, de par son efficacité, son coût minimal de mise en œuvre avec un moindre effort requis par l'utilisateur, ce qui rend intrusive la méthode surtout que c'est la plus ancienne et la plus mature.

I.5 Architecture et fonctionnement des systèmes biométriques

Chaque système biométrique utilise des spécificités liées à la caractéristique analysée (empreinte, iris, visage, ... etc.) et également liées à la technologie du système :



FigI.9. Architecture d'un système biométrique [9]

- Capture de l'information à analyser (image ou son).
- Traitement de l'information et création d'un fichier " signature/gabarit ", puis l'enregistrement de ce fichier de référence sur un support (disque dur, carte à puce, code barre).
- Dans la phase de vérification, le même procédé se répète pour la création du fichier " signature/gabarit " de référence,
- Comparaison des deux fichiers pour déterminer leur taux de similitude et prendre la décision qui s'impose.

I.6 Performance des systèmes biométriques

En comparant avec les systèmes d'authentification basés sur des objets ou mot de passe qui retournent des réponses absolues (Oui ou Non), les systèmes biométriques sont plus fluctuantes donnent des réponses en termes de pourcentage de similitude (entre 0% et 100% et le 100% n'étant jamais atteint) [9]. La solution était donc de définir un seuil de décision (acceptation ou refus) compris entre 0% et 100% de similitude au sein des applications. Ce seuil peut être différent pour chaque personne.

. Les performances des systèmes d'authentification biométriques s'expriment par :

- **Le F.R.R (False Rejection Rate) :** Taux de Faux Rejets : Pourcentage de personnes rejetées par erreur.
- **Le F.A.R (False Acceptance Rate) :** le Taux de Fausses Acceptations donne le pourcentage d'acceptations par erreur.
- **Le E.E.R (Equal Error Rate):** le Taux d'Egale Erreur donne un point sur lequel le F.R.R. est égal au F.A.R.

Ces taux vont dépendre de la qualité des systèmes, mais aussi du niveau de sécurité souhaité.

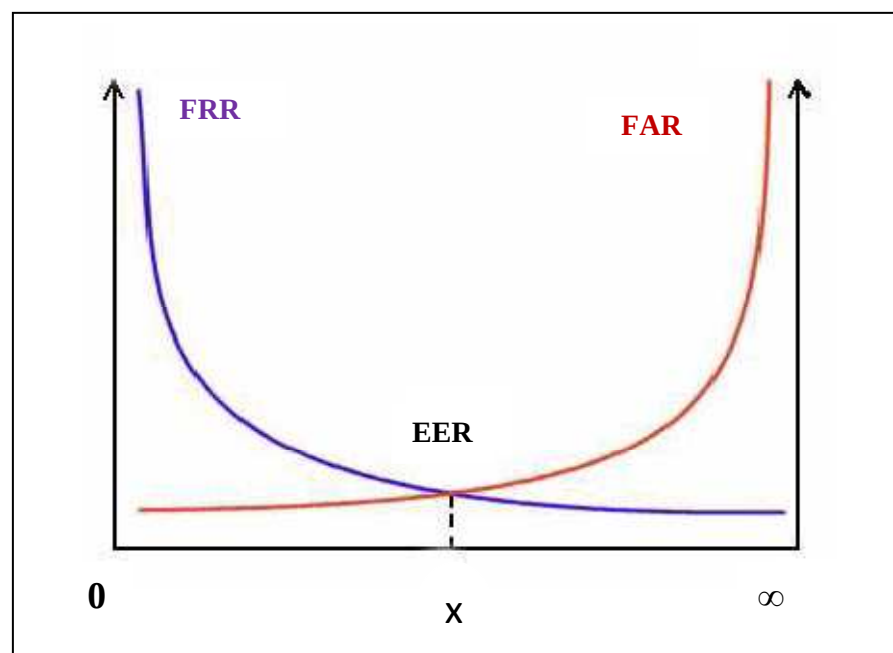


Fig I.10. Performance des systèmes biométriques [9]

Ce graphe représente la marge d'erreur autorisée par le système, variant de 0 à l'infini.

- Plus la marge d'erreur autorisée est importante, plus le taux de fausses acceptations augmente, c'est-à-dire que l'on va accepter de plus en plus de personnes qui ne sont pas autorisées et donc la sécurité du système diminue. Par contre on voit que le taux de rejet des personnes autorisées diminue également, ce qui rend le système plus fonctionnel et répond mieux aux attentes des utilisateurs.
- si l'on diminue la marge d'erreur acceptée par le procédé de mesure biométrique, les tendances des deux taux sont inversées : on va de moins en moins accepter des individus essayant de frauder mais on va aussi, par la même occasion, avoir un taux de rejet sur des personnes autorisées qui sera trop important pour être toléré dans la plupart des cas. Le compromis habituel est de prendre la jonction des courbes (x), c'est à dire le point x où le couple (FAR, FRR) est minimal (voir la figure Fig I.10) [9]

I.7 Conclusion

L'analyse morphologique et comportementale permettent d'identifier une personne non par ce qu'elle possède (passeport, CNI, badge,...), ou ce qu'elle sait (mot de passe, code pin,...), mais par ce qu'elle est, ce qui la rend unique et infalsifiable. Les caractéristiques physiques ont l'avantage d'être stables dans la vie d'un individu et ne subissent pas autant les effets du stress par exemple, que l'on retrouve dans l'identification comportementale.

L'amélioration des technologies biométriques existantes consiste à : (i) réduire le taux d'erreur, (ii) faciliter leur intégration dans les appareils mobiles et, (iii) les rendre plus accessible à l'égard de l'utilisateur. Une comparaison des technologies biométriques existantes a montré que l'utilisation de l'empreinte digitale comme moyen d'identification représente nettement la solution préférée par la communauté (facilité d'accès). Sa force tient au fait qu'elle efficace (pas de risque d'accepter ou rejeter une personne par erreur), moins intrusive et moins coûteuse.

Chapitre II

Tour d'horizon sur les empreintes digitales

II.1 Introduction

Plusieurs caractéristiques humaines ont été exploitées par la biométrie pour l'identification et la vérification automatique des individus, Les empreintes digitales sont un outil d'identification rapide, fiable et moins onéreux que certains autres. L'utilisation de l'empreinte digitale comme moyen d'identification d'une personne n'est pas nouvelle. C'est la technique biométrique la plus ancienne et la plus mature. Les empreintes ont formellement été acceptées comme identificateur de personnes valide dès le début du siècle. Elles ont d'abord étaient utilisées dans les milieux juridiques, avant de devenir une technique d'authentification effective.

II.2 Historique

L'histoire des empreintes est longue, nous donnons ici un bref aperçu [4]

Les empreintes n'ont pas été décrites sur les manuscrits jusqu'au 17eme siècle.

- En 1686, Marcello Malpighi un professeur d'anatomie à l'université de Bologne (Italie) décrit les crêtes papillaires dans son traite .
- En 1888, le Britannique F.Galton un anthropologue anglais et cousin de Charles Darwin démontre la permanence du dessin papillaire de la naissance à la mort ainsi que son inaltérabilité. Cet arrangement particulier des lignes papillaires forme des points caractéristiques nommés minuties ou points de Galton qui sont à l' origine de l'individualité des dessins d'empreintes. En se basant sur ces calculs, la probabilité pour que les empreintes de deux individus différents se correspondent est de 1 sur 64 Billions.
- En 1901, les empreintes furent introduites pour l'identification de criminels en Grande Bretagne. Les observations de Galton et leur révision par Edward Henry ont été utilisées. Cela marque le fondement du système de classification de Henry. L'avènement de l'ordinateur et les progrès récents réalisés dans le domaine de la reconnaissance des formes ont aidé à développer les systèmes d'identification automatiques. Ces systèmes ont considérablement amélioré la productivité opérationnelle des agences de loi et ont réduit le cout d'employer et de former les experts d'empreintes digitales.

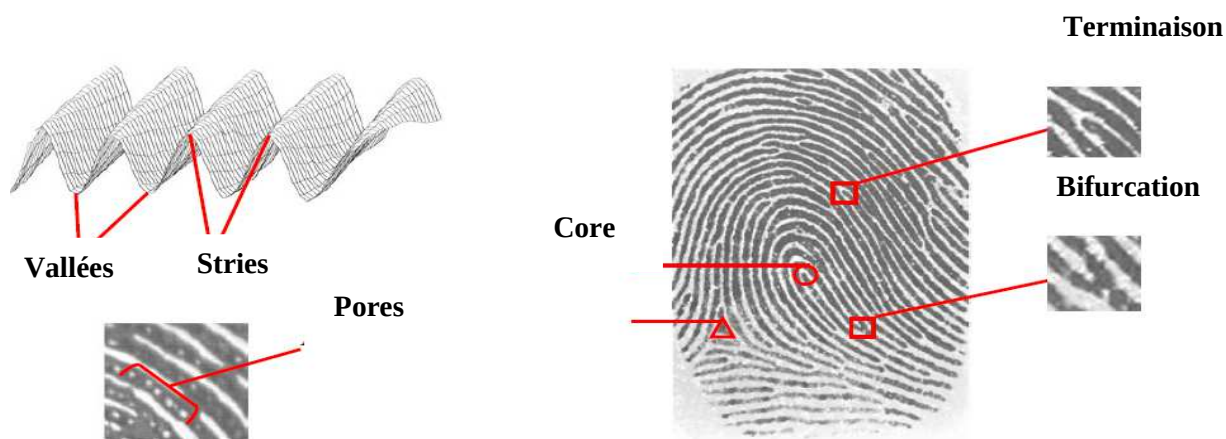
II.3 Caractéristiques d'une empreinte digitale

Une empreinte digitale est constituée d'un ensemble de lignes localement parallèle formant un motif unique pour chaque individu (FigII.1), on distingue :

Les stries (ou crêtes) : Les lignes en contact avec une surface au toucher

Les sillons : les creux qui se trouvent entre les stries.

Les pores : des trous *qui sont* régulièrement espacés dans les stries.



FigII.1 Caractéristiques d'une empreinte digitale

Le centre : un point singulier global où les stries convergent.

Le delta : un point singulier global où les stries divergent.

Les minuties : des points locaux où la strie bifurque ou termine (FigII.2). il existe plusieurs types de minuties mais dans la pratique les algorithmes ne s'intéressent qu'aux *Bifurcations* et *Terminaisons* qui permettent d'obtenir les autres types par combinaison.

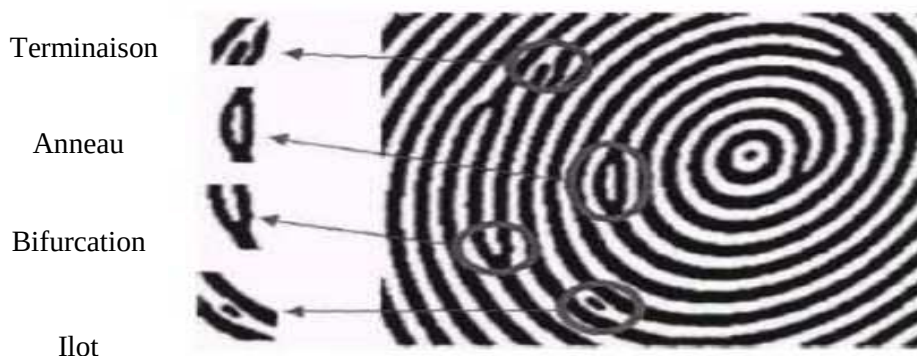


Fig II.2 Exemples de quatre familles de crêtes [Bel, 06]

La position et le nombre de centre et deltas permettent de classer les empreintes en Trois grandes catégories (FIG II.3) :



Fig.II.3 Les trois principales classes d'empreintes : Arche, Boucle, tourbillon [13]

- (a) **La Classe Arche** : les lignes vont d'un bord à l'autre du doigt.
- (b) **La Classe Boucle** : les lignes ont un trajet récurrent et reviennent aux bords dont elles sont parties.
- (c) **La Classe Tourbillon** : les lignes présentent un trajet plus au moins spirale et limité vers les bords du doigt.

La forme des crêtes du doigt ne changent pas à moins d'accidents telles que des contusions et des coupes sur les bouts du doigt. L'empreinte se forme à partir du troisième mois de la vie fœtale [Bab, 91], le motif général est influencé par les gènes héréditaires mais l'apparition des minuties est créée accidentellement par des pressions variables et aléatoire sur les surfaces tactiles. Ainsi, l'empreinte est unique pour tout individu y compris les jumeaux. Et actuellement, les méthodes de reconnaissance par empreinte digitale permettent d'identifier efficacement les jumeaux. [Jai et al, 01]

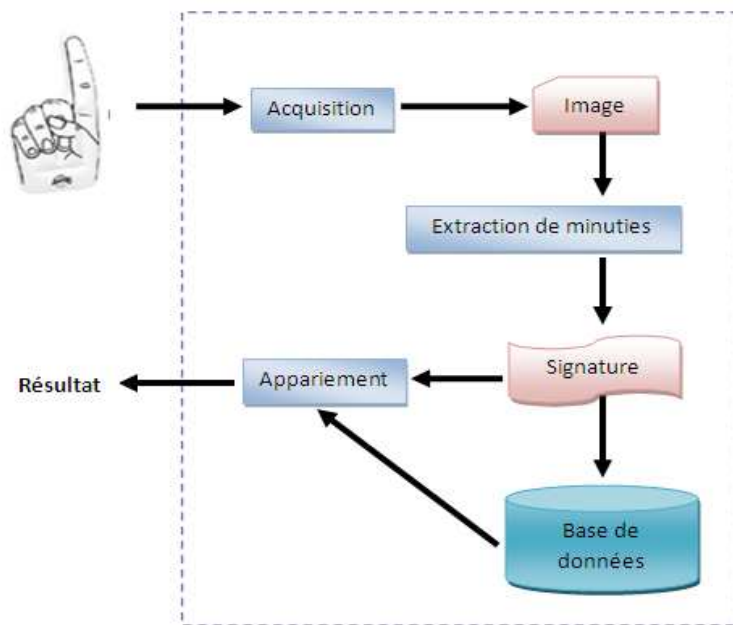
De plus l'empreinte une fois formée, ne change plus au cours de la vie de l'individu, cette propriété fait des empreintes digitales une marque biométrique très attrayante.

II.4 Structure d'un système complet de reconnaissance d'empreintes

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

protection. La réalisation d'un tel système a fait l'objet de très nombreuses recherches [Yag et al, 04]. Quoique ces systèmes répondent toujours à la même structure (Fig II.4).

La première phase consiste en l'acquisition de l'image qui subira ensuite un traitement afin d'en extraire les informations utiles (*signature*). Ensuite s'il s'agit d'une identification, la signature est éventuellement compressée puis stockée dans la base de données. Pour un système de vérification, une comparaison sera effectuée puis un résultat sera renvoyé pour accepter ou refuser l'utilisateur en question.



FigII.4 Architecture générale d'un système complet de reconnaissance d'empreinte digitale

II.4.1 Acquisition de l'empreinte

L'*acquisition* de l'image d'une empreinte digitale consiste à trouver les lignes tracées par les crêtes (en contact avec le capteur) et les vallées (creux) [13].

L'image sortante est constituée à partir des points de contact du doigt sur le capteur.

II.4.1 .1 Les familles de capteurs

- i) **Le capteur optique** : la technologie la plus ancienne après l'ancre et la plus répandue surtout dans les applications judiciaires. Il s'assimile à une mini caméra. Le doigt est apposé sur une platine en plastique dur ou en quartz, qui est en vis-à-vis de la mini caméra. Il résiste très bien aux fluctuations de température, mais est gêné par une lumière ambiante trop forte [12].

ii) Le capteur thermique : La technique de capture thermique est utilisée par le FingerChip d'Atmel. Le capteur mesure une différence de température obtenue selon que la peau touche (dans le cas d'une crête de l'empreinte) ou ne touche pas (pour une vallée) le capteur. Cette technologie présente de nombreux avantages. En particulier, elle permet d'obtenir une image de très grande qualité avec des empreintes « difficiles », par exemple quand les crêtes et les vallées sont très peu marquées [12].

iii) Le capteur à ultrasons : la lecture par ultrasons d'empreinte n'est pas courante. C'est une sorte d'échographie du doigt. La lecture par ultrasons requiert un assez gros dispositif et est assez chère. Ce n'est pas une technique commode pour de la production de volume à faible cout. Son principal intérêt réside dans la lecture du derme, sous la surface, plutôt que la surface elle-même [Bel, 06].

II.4.2 l'extraction de la signature

Une identification fiable nécessite un appariement pour améliorer la qualité de l'image avant de passer à l'extraction de la signature (informations nécessaires à l'identification ou à l'archivage dans la base de données) [Yag et al ,04].

Certains algorithmes permettent une extraction directe à partir de l'image en niveau de gris en suivant le maximum local des stries [Mai, 97] quoique, cela nécessite une bonne qualité d'image en entrée, c'est pour cette raison que les algorithmes préfèrent travailler sur un squelette binaire de l'image ce qui simplifie et facilite l'extraction. L'inconvénient de cette méthode est l'apparition d'un nombre important de fausses minuties, un poste traitement est alors nécessaire pour les éliminer [Bia et al ,02] les pores de l'empreinte ont été utilisées dans [Sto et al ,94] mais cela nécessite de très hautes définitions. La structure globale de l'empreinte peut être aussi utilisée [Soi et al ,96], mais les résultats sont généralement moins précis en comparant avec les caractéristiques locales.

Ce genre de méthodes est en général associé à l'extraction des minuties pour augmenter la performance du système, ou utilisé pour classifier les empreintes.

II.4.3 le stockage et l'appariement

Le temps de calcul de la signature pose un problème pour les systèmes disposant de grosses bases de données, un processus de classification est alors nécessaire pour limiter le temps de recherche de la signature.

Lorsqu'une image est stockée, un groupe d'attributs lui est associé en fonction de ses caractéristiques. Lors d'une identification, l'ensemble des signatures de la base correspondant au groupe de l'empreinte nécessitant l'identification, est désarchivé. Puis chacune des images désarchivées est comparées avec celle de l'utilisateur. Ceci permet de réduire sensiblement le temps de recherche en limitant le nombre d'images à comparer, à condition que les différentes catégories soient judicieusement choisies. Parmi les différentes techniques existantes [EM et al ,01] on distingue principalement, l'approche syntaxique (l'image est décrite au moyen de règles et de symboles et une analyse grammaticale permet de lui associer une classe), L'extraction des singularités de l'image (la position des centres et delta permet de déterminer la classe de l'empreinte) et l'utilisation des réseaux de neurones.

La phase d'appariement est la phase critique des systèmes de reconnaissance d'empreinte digitale, elle reçoit en entrée deux signatures issues de deux acquisitions différentes d'empreinte et renvoie en sortie un résultat binaire indiquant si les signatures proviennent de la même empreinte ou non. Bien entendu deux empreintes provenant de la même personne ne seront jamais identiques en raison de l'élasticité de la peau, la présence de poussière, de l'orientation du doigt, lors de l'acquisition...etc. Ceci est caractéristique des systèmes biométriques. La phase d'appariement va calculer le degré de similarité (taux d'appariement) entre les deux signatures et décider si elles peuvent être considérées identiques en fonction d'une valeur de seuil. [Pan et al ,02]

II.5 Représentation de l'empreinte digitale

Les systèmes de reconnaissance par empreinte digitale rencontrent des problèmes lors du processus d'acquisition de l'empreinte digitale tels que (les blessures, les coupures, les bleus ... etc). L'objectif étant de représenter l'empreinte digitale de façon invariante qui ne s'altère 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 [Bel, 06].

II.5.1 Représentation en image

Cette représentation prend en considère toute l'image et l'appariement se réalise par la corrélation. La corrélation entre les deux images $I_1(x, y)$, $I_2(x, y)$ est définie dans le domaine spatial par :

$$I_C(k, l) = \sum_x \sum_y I_1(x + k, y + l) I_2(x, y)$$

La mise en correspondance consiste à rechercher la magnitude du pic dans l'image de corrélation I_C . Sa position indique la translation entre les images et sa valeur informe sur le degré de similarité. Les phénomènes de translation et de rotation dégrade l'exactitude de cette corrélation. Les méthodes de corrélation locale peuvent surmonter le problème de distorsion mais l'inconvénient principal de cette représentation est la taille conséquente de l'image à sauvegarder durant l'inscription [Bel, 06].

II.5.2 Représentation avec les descripteurs de texture

Les algorithmes basés sur les descripteurs de texture utilisent les informations telles que (la moyenne et la variance) et l'appariement s'effectue en calculant la distance euclidienne entre deux descripteurs [Bel, 06]. Une mauvaise qualité risque de fausser la localisation des points. De plus, la performance est inférieure comparée aux appariements basés sur les minuties.

II.5.3 Représentation en minuties

Les minuties représentent des discontinuités locales et marquent les positions où la crête se termine ou bifurque. Chaque minutie peut être décrite par un nombre d'attributs tels que : [Bel, 06].

- Le type de minutie : Bifurcation ou Terminaison.
- La position de la minutie dans l'image : coordonnées (x,y)
- La direction du bloc local associé à la strie θ

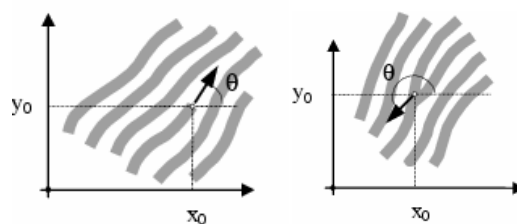


Fig II.5. Les caractéristiques principales des minuties. [Bel, 06]

La figure suivante est une représentation en minutes d'une empreinte :



Fig II.6. Exemple d'une représentation d'une empreinte par sa carte de minutes [14]

L'appariement basé sur les minutes dépasse rarement 1ko contrairement aux algorithmes basés sur la corrélation qui nécessitent des gabarits de grandes taille. De plus, Les points minutes sont invariants et ils ne sont pas influencés par les phénomènes de translation et rotation contrairement aux attributs de texture qui dépend de la qualité de l'image.

II.6 Conclusion

Dans ce chapitre nous avons fait un tour d'horizon sur les caractéristiques principales de l'empreinte digitale ainsi, nous avons décrit la structure globale d'un système de reconnaissance par empreinte digitale et décrit les différentes représentations possibles de l'empreinte digitale. Nous avons montré aussi que la représentation en minuties était avantageuse et la plus aboutie. Dans les chapitres suivants nous allons étudier la phase d'extraction des minuties dont la détermination repose sur des règles précises et complexes.

Chapitre III

**Approche classique d'extraction
des minuties**

III.1 Introduction

Les minuties constituent les attributs les plus utilisés pour l'identification par empreinte digitale. Les systèmes existants se basent sur les détails des minuties, les descripteurs de texture ou sur la représentation de l'image entière. [Seo,02] Les minuties marquent des points de discontinuité locale (FigIII.1). Dans notre travail, nous traitons deux types de minuties : les terminaisons qui marquent les fins de crêtes et les bifurcations qui correspondent aux points où la crête se diverge.



Fig III.1. Quelques minuties sur une image d'empreinte [15]

La détection de minuties est une étape importante dans le processus de reconnaissance de l'empreinte digitale qui se base principalement en l'appariement de minuties. Plusieurs méthodes ont été développées pour réaliser une extraction de minuties efficace. Les méthodes d'extraction de minuties peuvent être classées dans la littérature en deux grandes catégories: celles qui se basent sur la binarisation de l'image et celles qui travaillent directement sur l'image en niveau de gris [Mal et al, 03], [Nal et al, 04].

III.2 Approche Classique d'extraction de minuties

Dans cette approche, l'image en niveau de gris est convertie en une image binaire. Puis elle sera amincie (squelettisée) afin de diminuer l'épaisseur des stries (Fig III.2), à ce stade, les minuties seront bien visible et facile à détecter. [Rav et al,09]

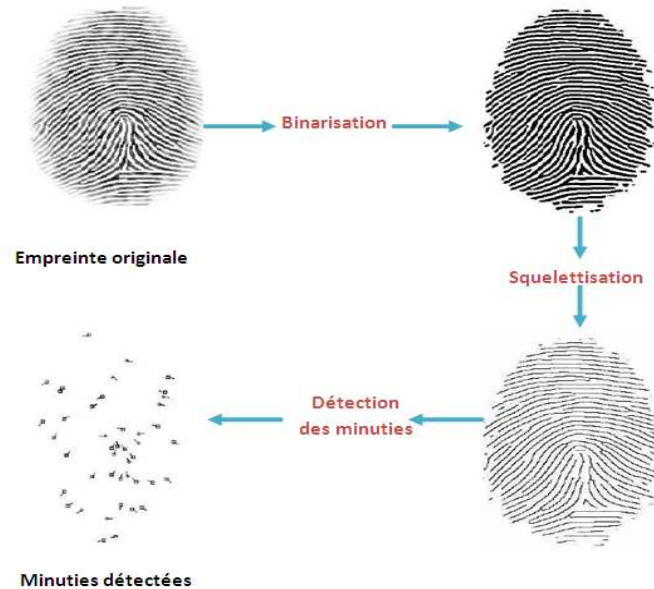


Fig III.2 Extraction des minuties par Binarisation [Rav et al,09]

III.2.1 La Binarisation

la Binarisation repose sur le choix d'un seuil global T . les pixels dont le niveau de gris est en dessous du seuil deviennent noirs, et ceux au dessus deviennent blancs.

$$I_T(x,y) = \begin{cases} 1 & \text{si } I(x,y) > T \\ 0 & \text{si } I(x,y) \leq T \end{cases}$$

Dans le cas d'une empreinte digitale, le but de la binarisation est de repérer les crêtes. Il existe des méthodes de binarisation optimales qui déterminent le seuil T en se basant sur la distribution des niveaux de gris [Ots,79]. Cependant, Le contraste dans une image d'empreinte digitale peut varier considérablement à travers les différentes régions constituant l'image. Par conséquent, un seuil unique n'est pas suffisant pour une segmentation correcte. Ainsi, une binarisation adaptative est souvent préférée pour ce type d'images où le seuil T se détermine dans un voisinage local. Néanmoins, ces techniques manquent leur efficacité si l'image de l'empreinte digitale est de mauvaise

qualité, la solution étant d'utiliser la structure des crêtes pour réaliser la segmentation/binarisation [Bel,09].

III.2.2 La Squelettisation (amincissement)

La **squelettisation** consiste à réduire une forme en un ensemble de courbes, appelées **squelettes**. C'est un outil d'analyse de forme non-scalaire, qui conserve les propriétés topologiques de la forme d'origine ainsi que ses propriétés géométriques, selon la méthode employée. La squelettisation est une méthode qui a été développée à l'origine dans les années soixante par Harry Blum, en vue de créer un nouveau descripteur de formes. Son but est de limiter la perte d'information [Bel, 06].

Nous avons implémenté sous matlab une méthode de squelettisation qui porte sur la morphologie mathématique [16], [Lam et al, 92] sur une image d'empreinte digitale binarisée avec [Ots,79] et ça a donné le résultat suivant :



Image Originale [6]

Image Binarisée

Image squelettisée

Fig III.3 Processus de binarisation/amincissement

La squelettisation réduit l'épaisseur des crêtes en un seul pixel, ce qui facilite et simplifie l'étape de détection des minuties.

III.2.3 L'extraction des minuties

L'extraction des minuties consiste à calculer le nombre de connexion **CN** de chaque pixel blanc avec ses 08 voisins [Rav et al,09].

Le couple (x, y) dénote un pixel sur une crête amincie et $P_0, P_1, \dots, P_7$ dénotent ses 8 voisins, ainsi le nombre de connexion $CN = (\sum_{i=0}^7 P_i)$.

- si un pixel est sur une crête amincie, alors il prend la valeur 0 et sinon il prend la valeur 1.
- Un pixel (x, y) est une fin de crête (Terminaison) si $CN = 1$
- Un pixel (x, y) est une Bifurcation si $CN > 2$.

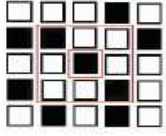
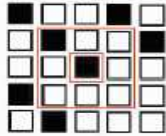
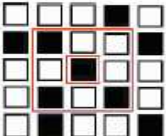
	Crossing Number = 2. Normal ridge pixel.
	Crossing Number = 1. Termination point.
	Crossing Number = 3. Bifurcation point.

Fig III.4 Le nombre de connexion et le type des minuties [Rav et al,09]

L'implémentation de l'extraction des minuties a donné ceci :

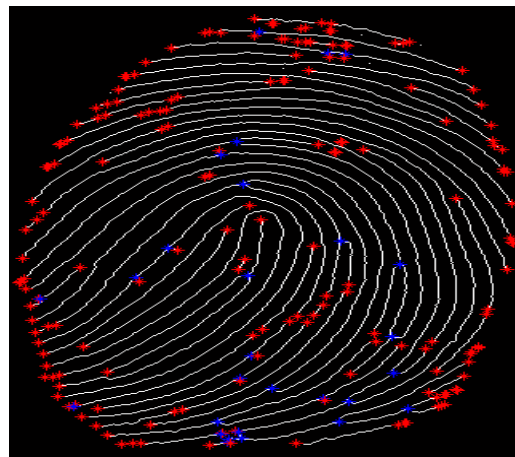


Fig III.5 Détection des minuties sur l'image amincie.

“Les terminaisons sont coloré en rouge et les Bifurcations en bleu. ”

III.2.3.1 Les problèmes rencontrés lors de l'extraction des minuties

La performance d'un système de reconnaissance d'empreinte digitale dépend de l'extraction des minuties et leurs appariements. Cependant, la mauvaise qualité de l'image en entrée engendre les problèmes suivant [Bel,09] :

- Création de fausses minuties.
- Ignorance de vraies minuties.
- Problème de localisation (position et direction).

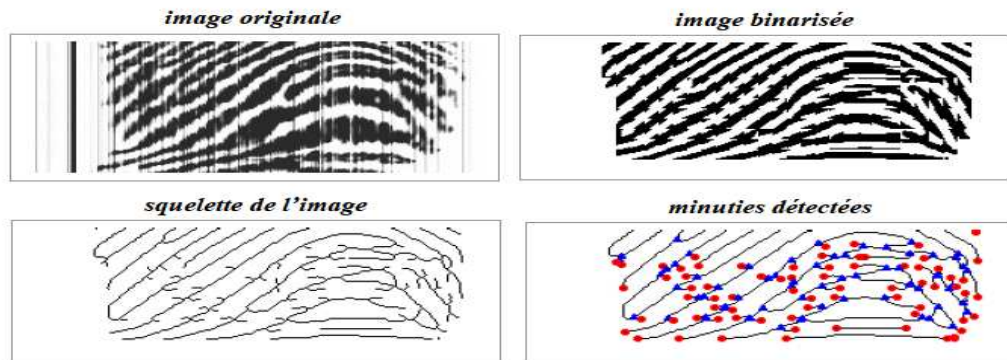
La qualité de l'empreinte rencontrée durant la vérification est très incertaine, elle varie sur une grande portée. La plus grande partie est endommagée par l'état de l'épiderme (Fig III.6) :

- Les crêtes se cassent par la présence de blessures, de coupures.
- Des empreintes très sèches donnent des crêtes fragmentées.



Fig III.6 Des images d'empreintes de différentes qualités. La qualité décroît 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) un empreinte sèche. [Bel,09]

Les fausses minuties engendrent par la suite, l'échec de l'algorithme d'appariement.



FigIII.7 Exemple de détection de fausses minuties [Gal,

2007]

III.2.3.2 Elimination des fausses minuties

Des solutions ont été proposées dans [Bia et al ,02] et [Kim et al ,01] pour éliminer les fausses minuties produites au cours du processus de binarisation et squelettisation. L'objectif étant de ne conserver que les vraies minuties. Pour cela, La distance entre les minuties a été utilisée comme moyen pour éliminer les minuties voisines qui ne répondent pas aux critères. En effet, la distance entre deux minuties voisines est toujours supérieure à un certain seuil et pratiquement, il est extrêmement rare de trouver deux vraies minuties très proches. Par contre on a approximativement une concentration locale de plusieurs fausses minuties.

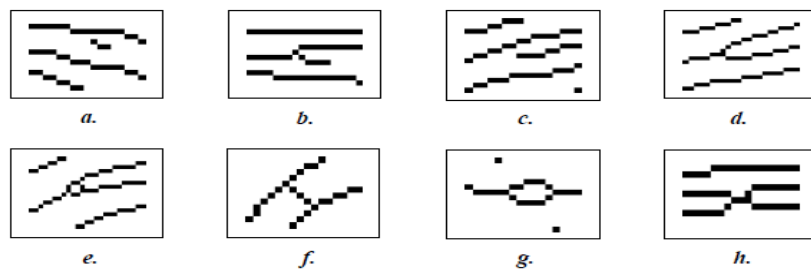


Fig III.8 Exemple de minuties détectées, segment trop court (a), branche parasite (b), vraie terminaison (c), vraie bifurcation (d), triangle (e), pont (f), ilot (g), segment trop court (h)

Le nombre de connexion CN utilisé dans le processus d'extraction de minuties est exploité pour éliminer les fausses minuties

III.2.4.1 Traitement des terminaisons détectées

un point $T(x_T, y_T)$ est considéré, ce point est une terminaison si $(CN(T)=1)$, afin d'éliminer les fausses minuties nous devons vérifier si celui-ci se situe au bord de l'image car, la majorité des fausses terminaisons se trouvent aux bord de l'image. Pour les terminaisons restantes T , on parcourt la strie qui lui est associée sur une distance maximum K jusqu'à atteindre le point A ($d=TA \leq K$, Fig III.09) [Gal, 05].

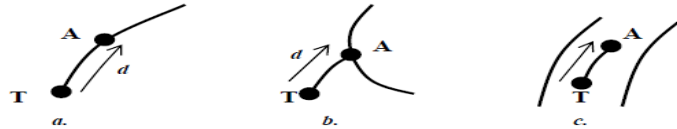
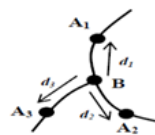


Fig III.9 Validation des terminaisons détectées : Vraie terminaison(a), Branche parasite (b)

Segment trop court (c)

III.2.4.2 Traitement des bifurcations détectées

Lorsque l'on détecte un point B candidate pour le titre de *Bifurcation* ($CN(B)=3$), on parcourt les trois stries qui lui sont associées sur une distance maximum de K jusqu'à atteindre trois points A_1 , A_2 et A_3 (Fig III.10) [Gal, 05]



$$d_1=BA_1$$

$$d_2=BA_2$$

$$d_3=BA_3$$

Fig III.10 Définitions associées à une bifurcation lors de la phase de validation

III.3 Approche d'extraction directe à partir de l'image en niveau de gris

Pratiquement, toutes les approches d'extraction de minuties existantes se basent sur le processus de binarisation-squelettisation, peu d'approches d'extraction à partir de l'image en niveau de gris ont été proposées :

Une utilisation des réseaux de neurones pour la détection des minuties a été introduite par M.T. Leung et al dans [Leu, 90].

Une autre approche basée sur la localisation des maximums locaux par un suivi des lignes le long du flot directionnel des crêtes a été proposée par Maio et Maltoni [Mai,97].

Contrairement à l'approche classique basée sur l'extraction des minuties par le processus de binarisation-squelettisation et qui nécessite un traitement à posteriori pour éliminer les fausses minuties.

III.4 Conclusion

La plupart des systèmes utilise l'approche classique de détection de minuties basée sur la binarisation-squelettisation dont l'avantage réside dans la simplicité à extraire et détecter les minuties lorsque l'on dispose d'un squelette précis de l'image. L'inconvénient vient de la perte d'information et du bruit introduit au cours de la Binarisation, ce qui provoque l'apparition d'une multitude de fausses minuties et nécessite un traitement à posteriori, en plus l'étape de squelettisation est couteuse en temps de calcul car plusieurs balayages sont nécessaires selon l'épaisseur des stries. Ces considérations nous ont amené à étudier une autre approche que nous allons détaillé dans le chapitre suivant et qui porte sur l'extraction directe à partir de l'image en niveau de gris, cette approche est basée sur la détection des lignes, jonctions des lignes en utilisant la courbure.

Chapitre IV

Détection de ligne, jonctions de lignes

Et terminaisons dans l'empreinte digitale

IV.1 Introduction

Les lignes constituent l'une des caractéristiques principales dans l'image de l'empreinte digitale. Elles correspondent à des discontinuités ou variations locales des niveaux de gris. Elles comportent certains points représentant des informations particulièrement robustes telles que les intersections et les points terminaux des lignes. Ce chapitre décrit une approche proposée par F. DESCHENES, D. ZIOU et M.-F. AUCLAIR-FORTIER [Des, 04] portant sur la détection des lignes, jonctions des lignes et terminaisons à partir de l'image en niveau de gris en utilisant la courbure, nous souhaitons nous servir de cette approche pour extraire de l'empreinte digitale, les minuties de type bifurcation et terminaison. L'approche se divise en deux étapes principales. D'abord, à partir des informations sur les lignes extraites de l'image originale (position, plausibilité et orientation), la courbure locale est calculée. A cette fin, deux mesures différentes ont été développées, testées et comparées. La première consiste en la projection du taux de changement de direction des vecteurs d'orientation le long de la ligne. La seconde mesure est la moyenne des produits scalaires des vecteurs d'orientation à l'intérieur d'un voisinage donné. Par la suite, les jonctions et terminaisons de lignes sont localisées à partir de la courbure locale. Dans ce chapitre nous allons détailler les étapes de cette approche.

IV.1.1 l'empreinte digitale : une image de lignes

La propriété principale qui caractérise l'image de l'empreinte digitale est l'alternance des lignes de crêtes et de vallées qui évoluent dans une direction précise.

Un bloc de l'image possède une direction locale constante dans lequel, les niveaux de gris des lignes (crêtes et vallées) constituent une forme sinusoïdale le long de la direction normale à l'orientation locale des crêtes (Fig IV.1). Les valeurs des niveaux de gris atteignent leur maximum local le long de la direction normale aux crêtes [Bel, 06].

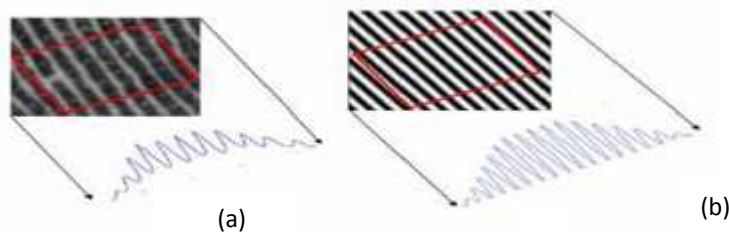


Fig IV.1 Projection des crêtes sur une image orientée.

(a) un échantillon d'empreinte (b) une empreinte synthétique [Bel, 06]

IV.2 La détection des lignes dans une empreinte digitale

La détection des lignes porte sur l’estimation de la plausibilité et l’orientation de chaque pixel de l’image. En se basant sur les performances des critères de Canny, l’approche propose une détection de lignes optimale qui opère séparément sur les directions horizontales et verticales. Sa rapidité est due à son implémentation sous forme de filtres récurrents à impulsion infinie IIR et un temps réduit d’exécution.

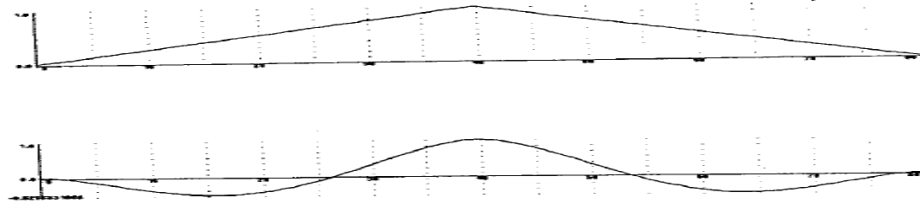


Fig.IV.2. Filtre optimal de détection des contours de types lignes de crêtes
[Can,83]

L’approche est une continuité des travaux de Canny qui assure une détection complète et exacte des lignes. Canny a montré en procédant par une optimisation numérique qu’un bon détecteur doit avoir la forme de la figure **Fig.IV.2**. [Zio et all, 89]

A partir du graphe de ce filtre monodimensionnel, les auteurs ont proposé :

- Une fonction permettant de représenter le filtre monodimensionnel.
- L’extension de ce filtre en deux dimensions.
- La réalisation de ce filtre sous forme de filtres récurrents (IIR).

IV.2.1 Modélisation du filtre par une fonction

- La fonction modélisant le filtre est paire et fourni zéro en réponse au signal constant.
- Une interprétation de la figure **Fig.IV.2** a mener les auteurs à proposer comme fonction la deuxième dérivée d’une gaussienne, mais pour des raisons de commodité, une fonction similaire a été proposée qui a la particularité d’être réalisée facilement par un filtre IIR. [Zio 91].

$$f(x) = (-c\alpha \sin(w|x|) + cw \cos(w|x|)) e^{-\alpha|x|} \quad (1)$$

α , c et w sont des constantes.

IV.2.2 Extension du filtre en deux dimensions

L'extension du filtre en deux dimensions nécessite la prise en compte de l'orientation du contour en un point donné. L'orientation d'un contour correspond à l'orientation normale à la direction qui maximise la variance des niveaux de gris, le calcul de cette orientation nécessite d'effectuer deux convolutions de masques 2D orthogonaux sur l'image. Un masque dans la direction X (respectivement Y) est le résultat du produit de la fonction de détection f (équation 1) dans la direction X (respectivement Y) par la fonction de projection g (équation 2) dans la direction Y (respectivement X).

$$g(x) = \frac{k}{a^2 + w^2} (\alpha \sin(w|x|) + w \cos(w|x|)) e^{-\alpha|x|} \quad (2)$$

- Le masque dans la direction X s'écrit alors : $X(x, y) = f(x) * g(y)$
- Le masque dans la direction Y s'obtient symétriquement : $Y(x, y) = f(y) * g(x)$

IV.2.3 Représentation de la fonction de détection

La représentation d'un filtre par un autre filtre récursif est souhaitable pour deux raisons : l'efficacité et l'optimisation de l'erreur d'approximation [Der, 87]. Cette représentation doit cependant conserver les propriétés du filtre utilisé, comme la stabilité et la réponse fréquentielle.

la fonction $f(n)$ est considérée obtenue par échantillonnage de $f(x)$. La transformation en Z de $f(n)$ fournit les équations aux différences suivantes :

$$\begin{aligned} y^+(n) &= a_0 x(n) + a_1 x(n-1) - b_1 y^+(n-1) - b_2 y^+(n-2) \\ y^-(n) &= a_2 x(n+1) + a_3 x(n+2) - b_1 y^-(n+1) - b_2 y^-(n+2) \\ y(n) &= y^-(n) + y^+(n) \end{aligned}$$

$$\text{Avec } a_0 = cw, \quad a_1 = -c(w \cos(w) + \alpha \sin(w))e^{-\alpha}, \quad a_2 = a_1 - a_0 b_1, \quad a_3 = a_0 b_2,$$

La stabilité est assurée pour $\alpha > 0$. La normalisation de la fonction de détection s'écrit :

$$c = \frac{2b_1 + 2b_2}{w - w e^{-2\alpha} - 2\alpha \sin(w) e^{-\alpha}} \quad (3)$$

IV.2.4 Représentation de la fonction de projection

En suivant le même raisonnement pour la fonction de projection, on obtient les équations aux différences suivantes :

$$\begin{aligned} y^+(n) &= a_0x(n) + a_1x(n-1) - b_1y^+(n-1) - b_2y^+(n-2) \\ y^-(n) &= a_2x(n+1) + a_3x(n+2) - b_1y^-(n+1) - b_2y^-(n+2) \\ y(n) &= y^-(n) + y^+(n) \end{aligned}$$

Avec $a_0 = c_2$, $a_1 = (-c_2 \cos(\omega) + c_2 \sin(\omega))e^{-\alpha}$, $a_2 = a_1 - c_2b_1$,
 $a_3 = -c_2b_2$, $b_1 = -2e^{-\alpha} \cos(\omega)$, $b_2 = e^{-2\alpha}$, $c_1 = \frac{k\alpha}{\alpha^2 + \omega^2}$ et $c_2 = \frac{k\omega}{\alpha^2 + \omega^2}$

La stabilité est assurée pour $\alpha > 0$. La normalisation de la fonction de projection s’écrit :

$$k = \frac{(1 - 2e^{-\alpha} \cos(\omega) + 2e^{-2\alpha})(\alpha^2 + \omega^2)}{2\alpha e^{-\alpha} \sin(\omega) + \omega - \omega e^{-2\alpha}} \quad (4)$$

IV.2. 5 Algorithme de détection des lignes de crêtes

L’algorithme d’extraction des lignes se déroule principalement en deux étapes :

IV.2.5.1 Filtrage de l’empreinte digitale

1. Filtrage de l’image de nbl lignes et nbx colonnes dans la direction horizontale.

D et P sont deux images intermédiaires de calcul, et Ix est l’image résultante.

$$\begin{aligned} D^+(i, j) &= a_0I(i, j) + a_1I(i, j-1) - b_1D^+(i, j-1) - b_2D^+(i, j-2) \\ i &= 1, 2 \dots nbl \quad j = 3, 4, \dots nbx \\ D^-(i, j) &= a_2I(i, j+1) + a_3I(i, j+2) - b_1D^-(i, j+1) - b_2D^-(i, j+2) \\ i &= 1, 2, \dots nbl \quad j = nbx - 2, \dots 1 \\ D(i, j) &= D^-(i, j) + D^+(i, j) \quad i = 1, 2, \dots nbl \quad j = 1, 2, \dots nbx \\ P^+(i, j) &= a_0D(i, j) + a_1D(i-1, j) - b_1P^+(i-1, j) - b_2P^+(i-2, j) \\ i &= 3, 4, \dots nbl \quad j = 1, 2, \dots nbx \\ P^-(i, j) &= a_2D(i+1, j) + a_3D(i+2, j) - b_1P^-(i+1, j) - b_2P^-(i+2, j) \\ i &= nbl - 2, \dots 1 \quad j = 1, 2, \dots nbx \\ Ix(i, j) &= P^-(i, j) + P^+(i, j) \quad i = 1, 2, \dots nbl \quad j = 1, 2, \dots nbx \end{aligned}$$

2. Filtrage symétrique de l'image dans la direction verticale. Soit I_y l'image résultat.

Nous avons implémenté testé le filtrage horizontal et vertical sur une image d'empreinte digitale [6] et ça a donné le résultat suivant :

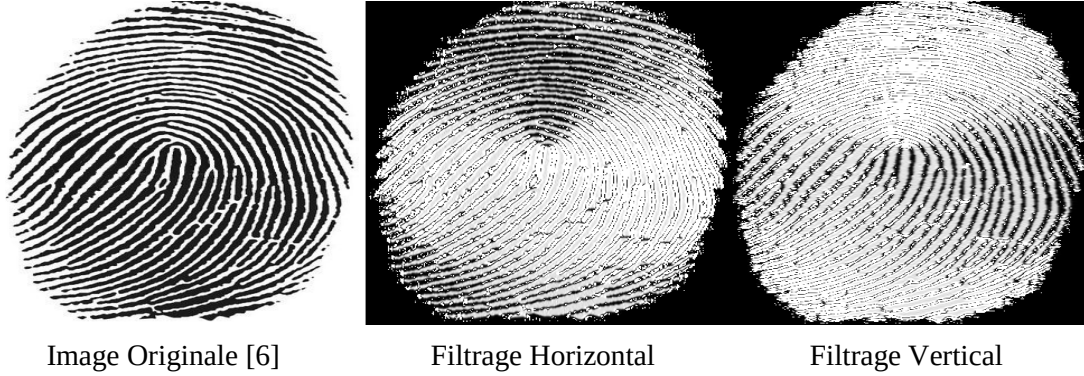


Fig.IV.3 Filtrage de l'empreinte digitale

IV.2.5.2 Suppression des non maxima par l'algorithme de Canny

Le processus consiste en la suppression des non maxima par l'algorithme de Canny dans la direction qui maximise la variance. Initialement l'orientation optimale de chaque point contour est calculée :

Le module M et l'orientation θ qui maximisent la variance sont calculés comme suit:

$$\theta = \frac{1}{2} \arctan \left(\frac{W * (IxIy) + (W * Ix)(W * Iy)}{W * I^2x + (W * Ix)^2 - W * I^2y - (W * Iy)^2} \right) \quad (5)$$

$$M = \sqrt{(W * (IxIy) + (W * Ix)(W * Iy))^2 + (W * I^2x + (W * Ix)^2 - W * I^2y - (W * Iy)^2)^2} \quad (6)$$

Où $W(x,y)$ est une gaussienne utilisée comme une fonction de pénalisation.

Dans le cas 2D, nous devons d'abord trouver la direction perpendiculaire à la ligne, c'est-à-dire présentant la courbure maximale de la fonction.

Posons $f(x, y)$, une image discrète. Cette direction peut être déterminée en calculant les valeurs propres et les vecteurs propres de la matrice du Hessian $H(x,y)$:

$$H(x, y) = \begin{bmatrix} (I * X)(x, y) & (I * Z)(x, y) \\ (I * Z)(x, y) & (I * Y)(x, y) \end{bmatrix} \quad (7)$$

où I^*X , I^*Y et I^*Z sont les dérivées partielles du second ordre de $f(x, y)$.

La direction présentant la courbure maximale est la direction perpendiculaire à la ligne. C'est la direction du vecteur propre correspondant à la valeur propre ayant la valeur absolue maximale. Si cette valeur propre est négative, c'est une ligne claire et si elle est positive, c'est une ligne foncée. Les deux valeurs propres de $H(x, y)$ peuvent être calculées comme suit :

$$\lambda = \frac{(f_{xx} + f_{yy}) \pm \sqrt{(f_{xx} - f_{yy})^2 + 4f_{xy}^2}}{2} \quad (8)$$

La direction normalisée perpendiculaire à la ligne est :

$$\vec{n} = (n_x, n_y) = \begin{cases} \frac{(\lambda_{max} - f_{yy}, f_{xy})}{\sqrt{(\lambda_{max} - f_{yy})^2 + f_{xy}^2}} \\ \frac{(f_{xy}, \lambda_{max} - f_{xx})}{\sqrt{f_{xy}^2 + (\lambda_{max} - f_{xx})^2}} \end{cases} \quad \text{ailleurs} \quad (9)$$

Où λ_{max} représente la valeur propre ayant la valeur absolue maximale au point (x, y) .

Avec cette valeur propre, nous pouvons définir une mesure de plausibilité de ligne.

- La valeur propre maximale de $H(x, y)$ correspond au point (x, y) qui a une valeur absolue maximale.
- Le maximum local dans le signal de sortie correspond au contour cherché.
- Un point (x, y) est un pixel ligne si λ_{max} est maximale dans les n direction dans ce point.

La suppression des non maxima a donné le résultat suivant :

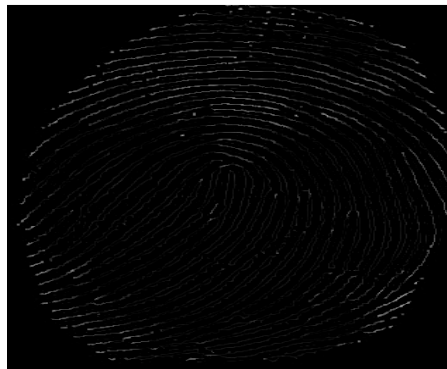


Fig.IV.4 Résultat du détecteur de lignes

IV.3 Détection des jonctions et terminaisons des lignes

Une *jonction* de lignes est une région ou un point dans le quel l’orientation change, comme l’illustre la figure (Fig.IV.5) :

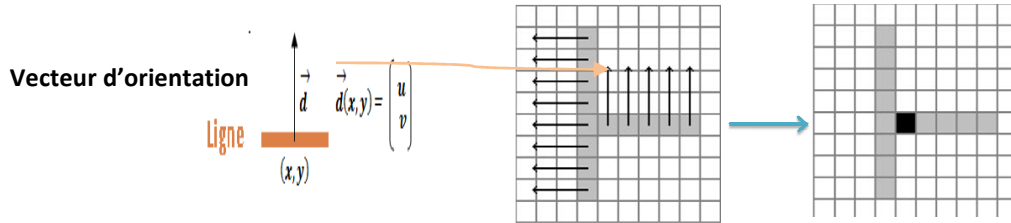


Fig.IV.5 Jonction de deux lignes [Des, 00]

Elle possède une valeur maximale pour les points appartenant à la zone entourant une jonction ce qui explique un changement significatif de la direction dans une telle région [Des,00] :

- Si la différence entre deux vecteurs d’orientation voisins n’est pas nulle alors on est sur une jonction.
- Sinon, les deux voisins appartiennent à la même ligne.

IV.3.1 Estimation de la courbure locale d’une ligne

Le taux de changement de la direction d’une ligne est communément appelée *courbure*.

Selon cette définition, une jonction idéale correspond à un maximum local de la courbure de la ligne [Des, 99], tel qu’illustré par la figure Fig.IV.6

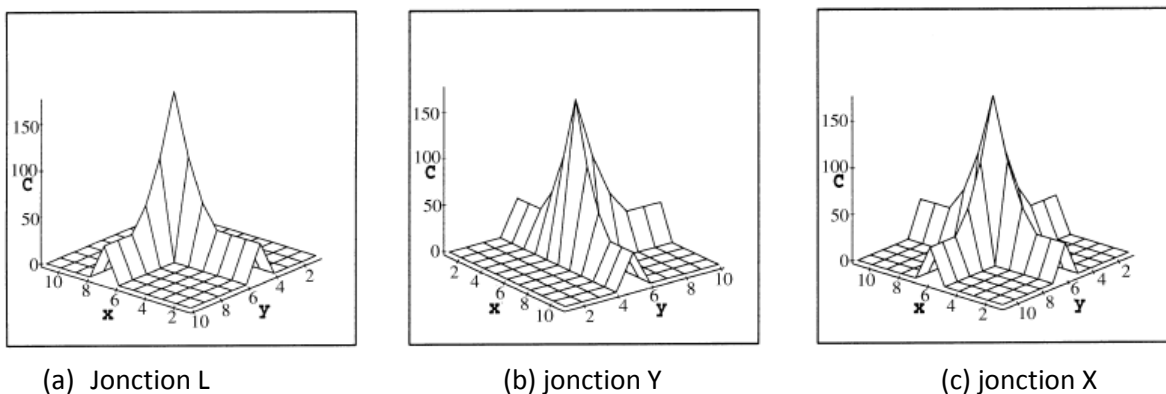


Fig.IV.6 exemples de courbures [Des, 99]

Les informations (plausibilité, orientation et position) des lignes ont été préalablement supposées extraites de l'image originale à l'aide du détecteur de lignes, la courbure locale peut alors être estimée, deux mesures différentes ont été testées et comparées par les auteurs. La première est inspirée d'une mesure proposée dans [Kit et al, 82] pour les coins de marches. La version originale est définie comme étant le taux de changement de la direction du gradient le long du contour multiplié par l'amplitude du gradient. Étant donné que l'amplitude du gradient correspond à la plausibilité des contours de type marche, la valeur de la courbure résultante est élevée pour tout point (x,y) appartenant à un contour de fort contraste qui tourne rapidement. Comme le gradient d'une ligne est faible, voire même nul [Zio, 98], cette mesure n'est pas adaptée aux lignes.

Elle doit donc être modifiée. Pour ce faire, calculons le taux de changement de direction à partir de $\vec{d}(x,y)=(u,v)$, vecteur d'orientation non normalisé perpendiculaire à un point (x,y) de la ligne. La direction θ de d est donnée :

$$\theta(x,y) = \begin{cases} \arctan\left(\frac{u}{v}\right) & \text{si } u \neq 0 \\ \frac{\pi}{2} & \text{sinon} \end{cases} \quad (10)$$

Les dérivées partielles de θ sont respectivement:

$$\theta_x = \frac{v_x u - u_x v}{u^2 + v^2} \quad \text{et} \quad \theta_y = \frac{v_y u - u_y v}{u^2 + v^2} \quad (11)$$

où, u_x et v_x représentent les dérivées partielles de u et v . Ainsi, la projection du vecteur (θ_x, θ_y) le long de la Ligne, multipliée par l'amplitude de $\vec{d}$ fournit une mesure de courbure donnée par :

$$\begin{aligned} C(x,y) &= ((\theta_x, \theta_y) \cdot \frac{(-v, u)}{\sqrt{u^2 + v^2}}) \sqrt{u^2 + v^2} \\ &= \frac{u_x v^2 + v_y u^2 - uv(u_y + v_x)}{u^2 + v^2} \end{aligned} \quad (12)$$

Où $\cdot$ représente le produit scalaire. Cette quantité est grande pour tout point appartenant à une région avoisinant une jonction (**Fig.IV.7 (d)**). Ceci est dû au changement significatif de la direction de θ à l'intérieur d'une telle région.

Cette seconde mesure repose sur la dissimilitude entre les vecteurs d'orientation des pixels de la ligne à l'intérieur d'un voisinage donné. La mesure de dissimilarité entre n'importe quelle paire d'orientations $d(x_1, y_1)$ et $d(x_2, y_2)$ est donnée par l'équation 13 :

$$s(\vec{d}(x_1, y_1), \vec{d}(x_2, y_2)) = 1 - \frac{|\vec{d}(x_1, y_1) \cdot \vec{d}(x_2, y_2)|}{\|\vec{d}(x_1, y_1)\| \|\vec{d}(x_2, y_2)\|} \quad (13)$$

Tel que $\cdot$ est le produit scalaire qui vaut 1 si les vecteurs sont perpendiculaires et 0 si les vecteurs sont parallèles.

La courbure peut donc être estimée en calculant la moyenne des $s(\vec{d}(x, y), \vec{d}(x + \Delta x, y + \Delta y))$ au sein d'un voisinage local $(2*M+1) * (2*M+1)$, elle est donnée par :

$$C(x, y) = \frac{1}{N} \sum_{\Delta x=-M}^M \sum_{\Delta y=-M}^M \beta(\Delta x, \Delta y) \cdot \left[1 - \frac{|\vec{d}(x, y) \cdot \vec{d}(x + \Delta x, y + \Delta y)|}{\|\vec{d}(x, y)\| \|\vec{d}(x + \Delta x, y + \Delta y)\|} \right] \quad (14)$$

Tel que :

$$\beta(\Delta x, \Delta y) = \begin{cases} e^{(-(\Delta x^2 + \Delta y^2))} & \text{Si un chemin formé de pixels ayant une plausibilité Non - Nulle existe entre } (x, y) \text{ et } (x + \Delta x, y + \Delta y) \\ 0 & \text{Sinon} \end{cases}$$

N représente le nombre de points $(x + \Delta x, y + \Delta y)$, tel que $\beta \neq 0$, et $(\Delta x^2 + \Delta y^2)$ est la distance entre le pixel considéré et son voisin, β assure qu'un voisin lointain contribue moins dans le calcul de la courbure C , Cette fonction assure également que seuls les points appartenant à une ligne sont considérés, ce qui signifie qu'il n'est pas nécessaire d'utiliser explicitement la plausibilité de la ligne dans l'équation (2). Ainsi, la valeur de $C(x, y)$ est grande pour tout point de la ligne appartenant au voisinage d'une jonction.

Nous avons choisi d'implémenter cette mesure pour la détection des jonctions et terminaisons des lignes, les auteurs de l'approche ont démontré que cette mesure basée sur la moyenne des produits scalaires dans un voisinage donne un bon résultat en comparant avec le rapport du changement de directions des lignes, comme le montre la figure **Fig.IV.7** :

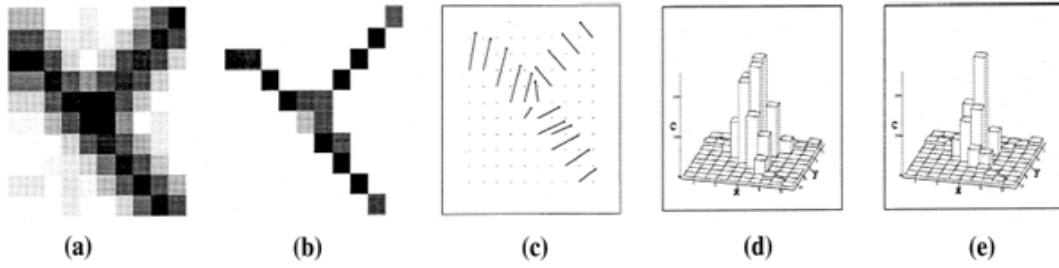


Fig.IV.7 exemple d’estimation de la courbure **(a)** image originale, **(b)** lignes extraites, **(c)** estimation des vecteurs d’orientation, **(d)** estimation de la courbure par le rapport de changement d’orientation, **(e)** estimation de la courbure par le produit scalaire [Des, 00]

IV.3.2 Localisation des jonctions des lignes

Pour localiser une jonction, il suffit de limiter le territoire et ne calculer la moyenne des produits scalaires que pour les pixels de la ligne comme le montre l’équation (15) :

$$p(x, y) = [1 - C(x, y)] \cdot L(x, y) \quad (15)$$

$C(x, y)$ représente la courbure calculée par l’équation (14) et $L(x, y)$ est la plausibilité de la ligne fournie par le détecteur de lignes. $p(x, y)$ est maximale pour les points de frontières dont la courbure est trop petite et la plausibilité est très élevée. A l’aide des frontières de faible courbure, les vecteurs d’orientation de chacune des jonctions sont ensuite déduits, puis utilisés afin de mettre à jour la courbure. À cette fin, à partir de chacune des frontières, tous les voisins de forte courbure dans la direction de la ligne sont visités à tour de rôle. Un pixel (x, y) de forte courbure est ainsi visité (zéro, une ou plusieurs fois). A chaque visite, il reçoit le vecteur d’orientation du pixel frontière courant $\vec{d}(x, y)$, tel que montré dans la figure **Fig.IV.7**. A la fin des visites, la courbure $C(x, y)$ des pixels de forte courbure est mise à jour selon la règle de l’équation 16 :

$$C(x, y) = C_0(x, y) + \sum_{i=1}^n \sum_{j=1}^n s(d_i(x, y), d_j(x, y)) + k \quad (16)$$

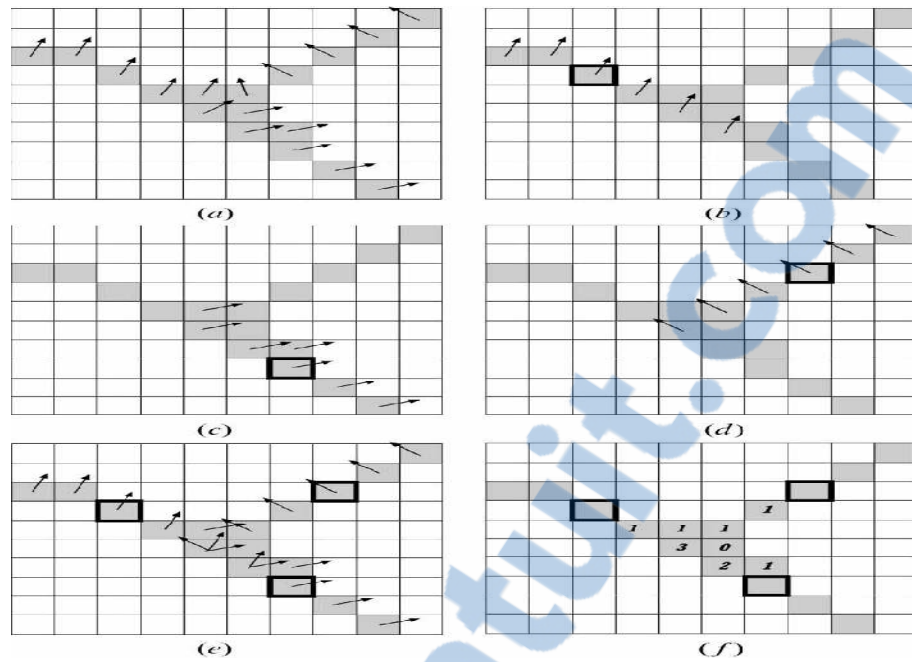


Fig.IV.8 Propagation des vecteurs d'orientation à partir des frontières [Des, 04]

IV.3.3 Localisation des terminaisons

Rappelons qu'une terminaison, correspond à une jonction T formée par l'intersection de deux contours dont l'un est très court. Comme le montre la figure **Fig.IV.9**, la réponse d'un détecteur de lignes en présence d'une terminaison confirme cette définition. Dans cette figure, la terminaison est celle de droite.

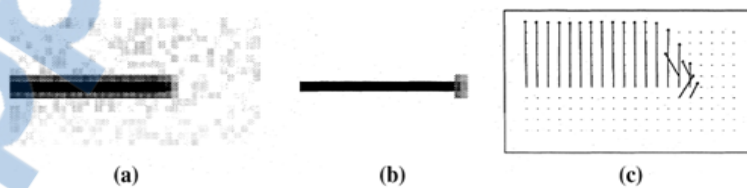


Fig.IV.9 Réponse du détecteur de lignes pour les terminaisons, **(a)** la ligne originale (la terminaison réelle est à droite), **(b)** la ligne extraite, **(c)** les vecteurs d'orientation [Des, 04]

En se basant sur ces propriétés, les terminaisons de lignes peuvent être localisées par la méthode décrite précédemment. Premièrement, le changement de direction des vecteurs d'orientation à l'intérieur du voisinage local de la terminaison garantit que la courbure est grande en ce point. Les vecteurs d'orientation sont propagés dans une direction unique qui

est celle de la ligne. Cela garantit que l'extrémité en question sera visitée et que sa courbure sera mise à jour par l'équation (16).

IV.4 Conclusion

Nous avons vu dans ce chapitre une approche qui opère directement sur l'image en niveau de gris en procédant, d'abord par la détection des lignes puis la détection des jonctions et terminaisons des lignes, en effet, à partir des lignes extraites de l'image originale, la courbure locale a été calculée. Les auteurs de l'approche ont développé, testé et comparé deux mesures d'estimation de la courbure: le taux de changement de direction des vecteurs d'orientation le long de la ligne (équation 12) et la moyenne des produits scalaires des vecteurs d'orientation à l'intérieur d'un voisinage donné (équation 14). Ensuite, un traitement additionnel, basé sur la courbure estimée et les informations du voisinage, est effectué en vue de localiser avec précision les jonctions et les extrémités. Une évaluation subjective de l' algorithme a été effectuée pour chacune des deux mesures de courbure proposées et il a été montré que la seconde mesure permet d'obtenir une réponse unique à une jonction de lignes. Nous avons testé et validé les résultats du détecteur de lignes sur les images d'empreintes digitales (Fig IV.4) et comme perspectives, nous souhaiterons implémenter la détection des jonctions et terminaisons pour extraire de l'empreinte digitale les minuties de type bifurcations et terminaisons.

Chapitre V

Tests et résultats expérimentaux

V.1 Introduction

L'empreinte digitale peut être représentée globalement par les points singuliers (les *Centres* et les *Deltas*) ou localement par les minuties dont la détermination est basée sur des règles complexes et précises. Dans notre travail, nous nous intéressons à l'extraction des minuties de type (Terminaison et bifurcation). Les minuties marquent des discontinuités locales dans l'image de l'empreinte digitale où la crête se termine ou bifurque.

Dans ce chapitre, nous avons testé et évalué deux approches :

1. La première approche est basée sur le processus de Binarisation-Squelettisation, l'image en entrée est binarisée par la méthode [Ots,79] puis squelettisée par [Lam et al, 92] et l'extraction des minuties se fait par le calcul du nombre de connexion des pixels blancs. La méthode de par sa simplicité présente des inconvénients :
 - La binarisation produit des fausses minuties.
 - La squelettisation est coûteuse en temps de calcul.
 - La mauvaise qualité des empreintes digitales provoque l'apparition de fausses minuties.
2. La deuxième approche se base sur l'extraction des minuties à partir de l'image en niveau de gris, l'intérêt de cette approche est de détecter les lignes, les intersections des lignes et les terminaisons des lignes dans les images. Nous nous sommes servi de cette approche pour détecter les minuties de type (jonction et terminaison).

V.2 Extraction des minuties par l'approche binarisation/Squelettisation

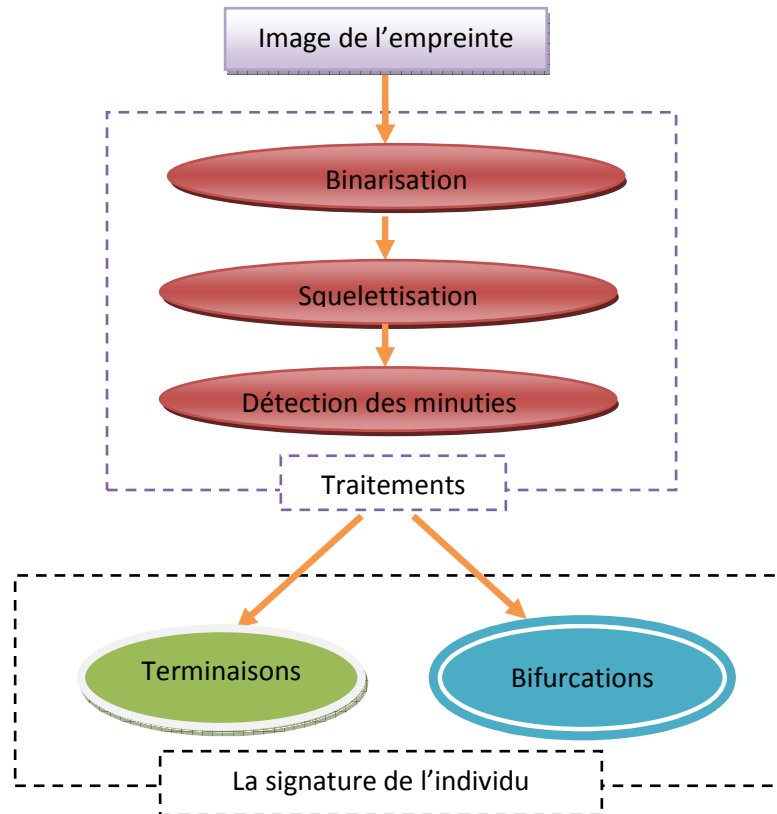


Fig V.1 schéma récapitulatif sur l'approche de détection de minuties par Binarisation/squelettisation

V.2.1 L'image de l'empreinte digitale

L'origine des images en entrée n'a pas d'importance (scanner, fichier, caméra ...).

V.2.2 La Binarisation

La binarisation d'une empreinte digitale a comme but le repérage des crêtes. Le contraste dans une image d'empreinte peut varier considérablement à travers les différentes régions constituant l'image. Nous avons utilisé l'algorithme de binarisation d'Otsu [Otsu,79].

V.2.3 La squelettisation

Dans l'image binarisée (noir et blanc) les lignes se voient clairement mais elles ont des tailles différentes. Pour pouvoir détecter rapidement les minuties (terminaisons, bifurcations), il est nécessaire d'obtenir une image plus schématique de l'empreinte, dans laquelle toutes les lignes ont la même épaisseur (1 pixel), nous réalisons une squelettisation sous MATLAB définie dans [Lam et al, 92] ; Nous présentons dans ce qui suit quelques résultats de notre programme :



Fig V.2 Exemple1 de binarisation et squelettisation



Fig V.3 Exemple2 de binarisation et squelettisation

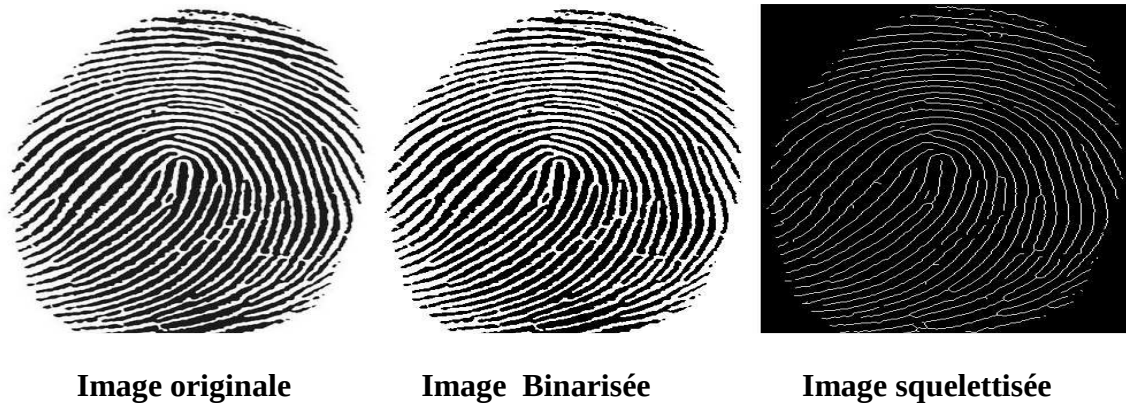


Fig V.4 Exemple3 de binarisation et squelettisation

V.2.4 La détection des minuties

La détection des minuties est une tâche insignifiante quand une idéale carte de crêtes amincie est obtenue. (voir chapitre III (Fig III.4)). [Rav et al,09]

Le processus d'extraction consiste à compter le nombre de connexions CN de chaque pixel P blanc. $CN(P)$ aura trois valeurs possibles :

- $CN(P)=1$: Il s'agit d'une minutie de type *terminaison*
- $CN(P)=2$: c'est le cas le plus courant, il s'agit d'un pixel appartenant à une strie, il n'y a pas de minuties.
- $CN(P)=3$: Il s'agit d'une minutie de type *bifurcation*

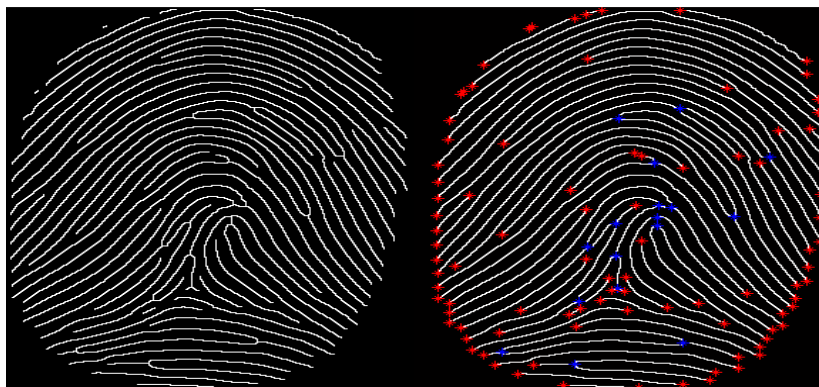


Fig V.5 Exemple4 Extraction de minuties

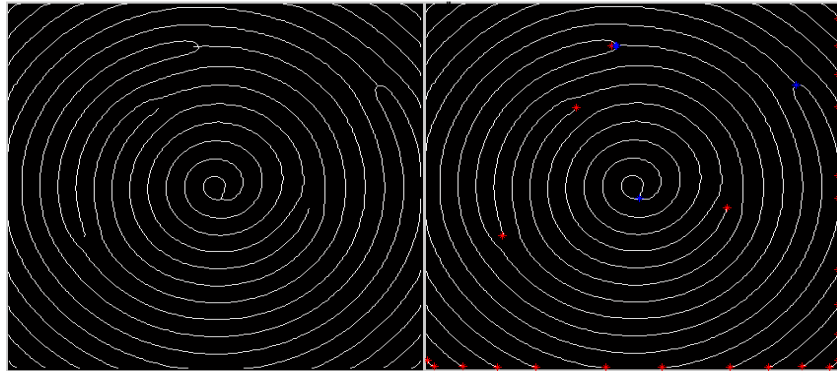


Fig V.6 Exemple5 Extraction de minuties



Fig V.7 Exemple 6 Binarisation, squelettisation et extraction des minuties

L'environnement de developpement

Nous avons utilisé pour cette partie l'environnement MATLAB, un environnement interactif qui permet d'effectuer des tâches de calcul intensif plus rapide.

V.3 Approche de détection des lignes, jonctions des lignes et terminaisons

L'extraction des lignes porte sur l'estimation de la plausibilité et l'orientation de chaque pixel de l'image. En utilisant les performances des filtres de Canny, l'approche de [Des et al, 04] propose un détecteur de lignes optimal qui opère séparément sur les directions horizontales et verticales. Ce détecteur a l'avantage d'être rapide de par son implémentation sous forme de

filtres récurrents à impulsion infinie IIR, de plus il est moins coûteux en temps d'exécution. L'algorithme d'extraction des lignes se déroule en deux étapes :

- 1- Filtrage de l'image dans les différentes directions horizontale, verticale et (horizontale&verticale) pour obtenir respectivement les images (I_x , I_y et I_z).
- 2- Suppression des non maxima par l'algorithme de Canny dans la direction qui maximise la variance. La figure Fig V.8 illustre la démarche d'extraction des lignes

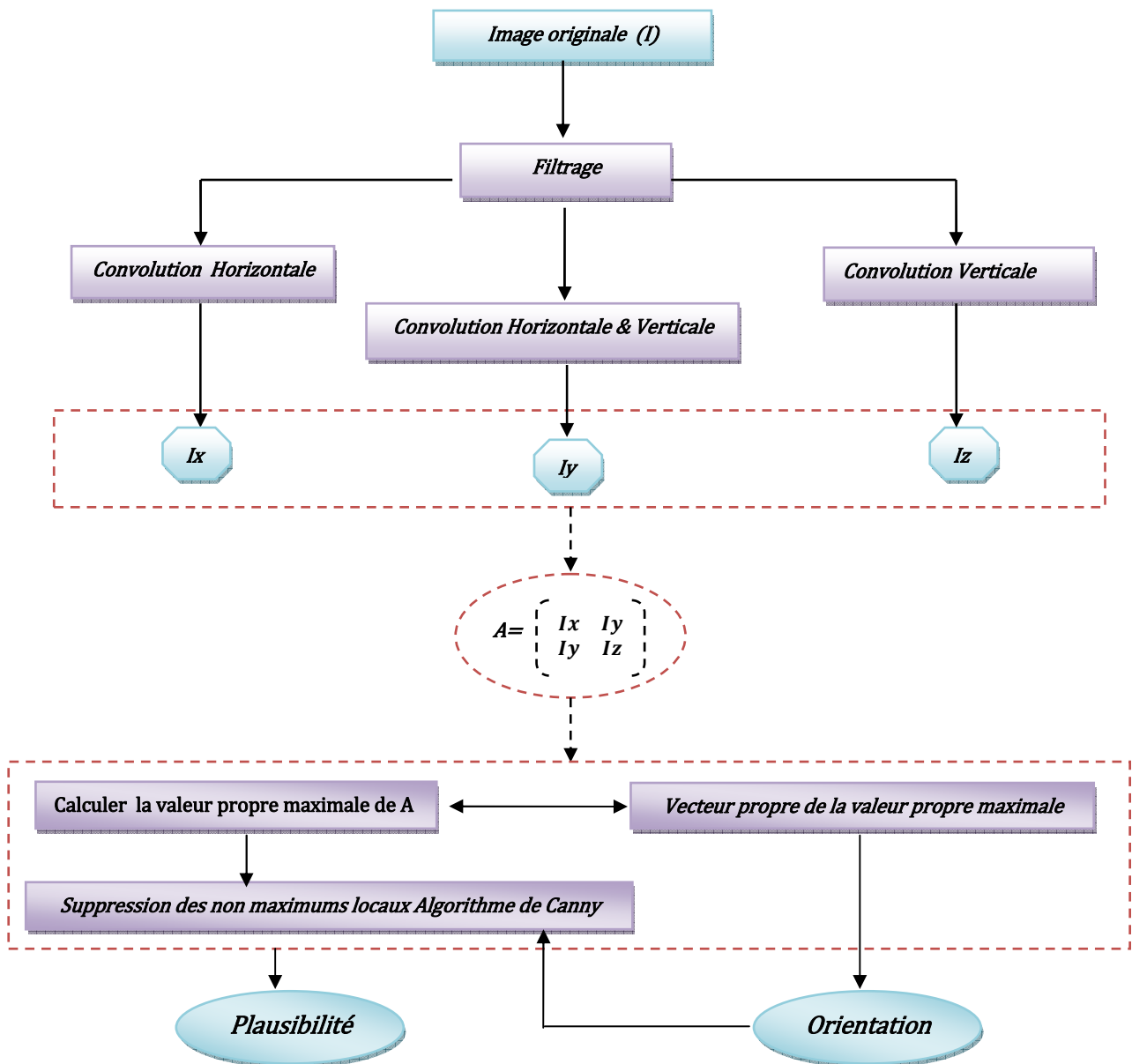


Fig V.8 schéma récapitulatif sur la détection des lignes

V.3.1 Algorithme de détection des lignes

- 1- Filtrage de l'image originale I avec les filtres: X , Y et Z : Images obtenues: I_X , I_Y et I_Z .
- 2- Etablir la matrice $A = \begin{bmatrix} I_x & I_y \\ I_y & I_z \end{bmatrix}$
- 3- Suppression des non maximums dans la direction du vecteur propre qui correspond à la valeur propre maximale $\lambda_{\max}$ de la matrice en utilisant l'algorithme de Canny.

V.3.2 Implémentation de l'approche de détection

Cette deuxième approche a été développée en C avec l'éditeur Code ::Block et la bibliothèque Opencv afin de profiter des fonctionnalités du traitement d'image qu'elle fournit.

La console du programme principal est présentée comme suit :

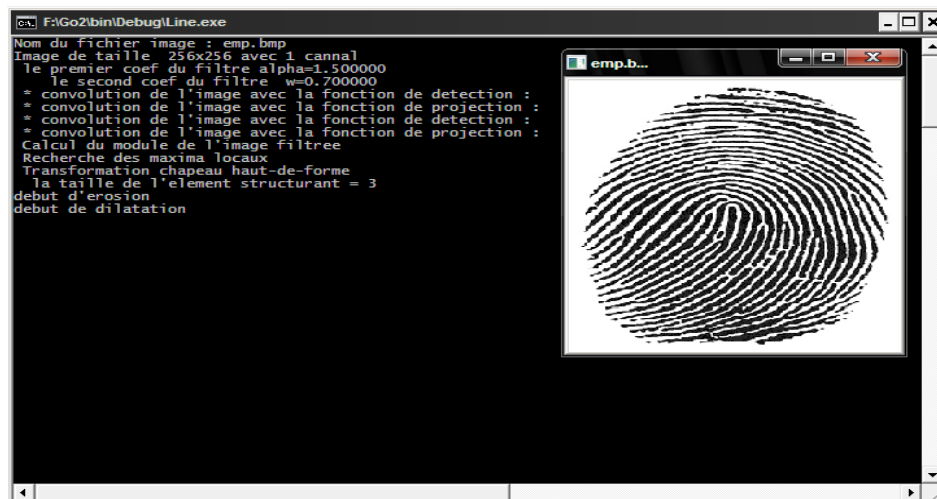


Fig V. 9 la console du programme principal

V.3.2.1 Implémentation du filtrage

Les paramètres recommandés par le filtrage horizontal et vertical avec $\alpha \in [0.75, 1.5]$ et $w \in [0.001, \alpha]$, pour $\alpha = 1,5$ et $w = 0.7$ le résultat est comme suit :



Fig.V. 10 Exemple 7 Implémentation du filtrage

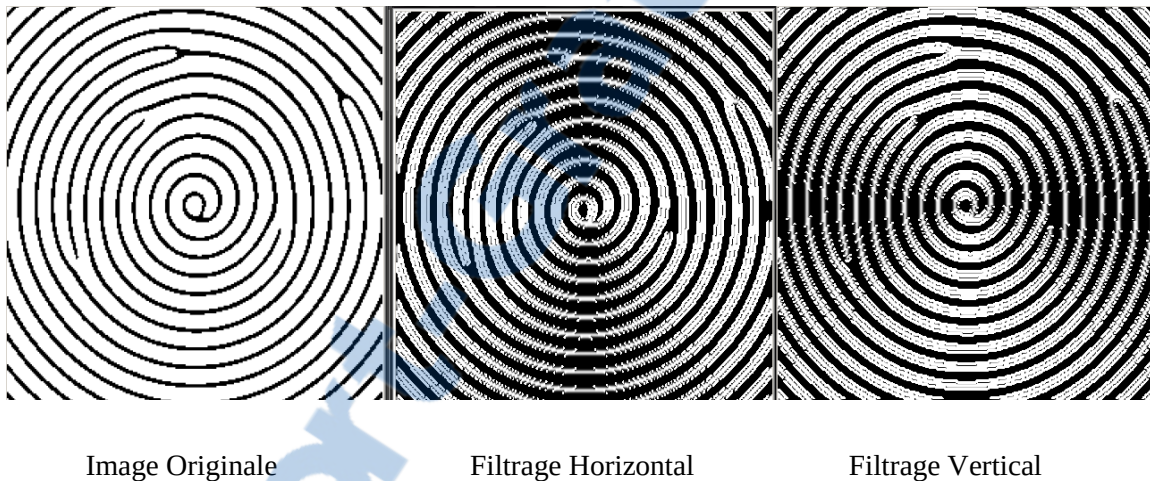


Fig V. 11 Exemple 8 implémentation du filtrage

V.3.2.2 Implémentation de la suppression des non maxima

La détection des lignes consiste en la suppression des non maxima par l'algorithme de Canny [Can 83] dans la direction qui maximise la variance (chapitre I V).



Fig V.12 exemple 9 Détection des lignes

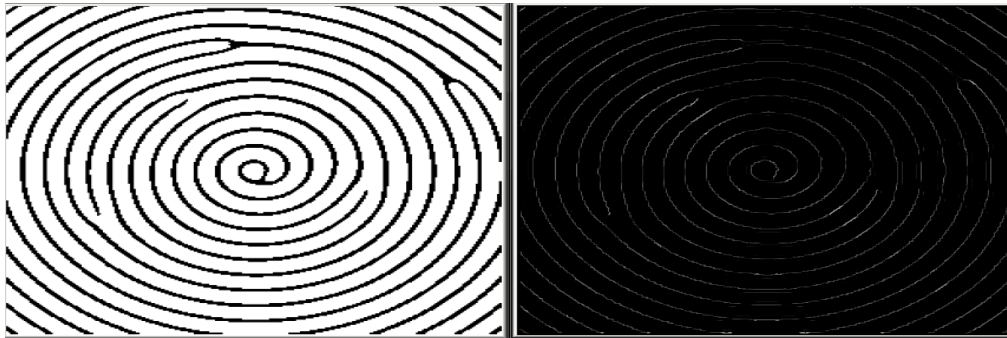


Fig V.13 exemple 10 Détection des lignes

V.4 Conclusion

L'avantage de l'utilisation de l'approche de binarisation/squelettisation réside dans la simplicité à extraire et détecter les minuties lorsque l'on dispose d'un squelette précis de l'image. L'inconvénient vient de la perte d'information et du bruit introduit au cours de la Binarisation, ce qui provoque l'apparition d'une multitude de fausses minuties et nécessite un traitement à posteriori (chapitre III (Fig III.9)), en plus l'étape de squelettisation est coûteuse en temps de calcul car plusieurs balayages sont nécessaires selon l'épaisseur des stries. Ces considérations nous ont amené à étudier une autre approche qui porte sur la détection des lignes, jonctions des lignes et terminaisons directement de l'image en niveau de gris en utilisant la courbure. La détection des lignes porte sur l'estimation de la plausibilité et l'orientation de chaque pixel de l'image. En utilisant les performances des critères de Canny,

l'approche propose un détecteur de lignes optimal qui opère séparément sur les directions horizontales et verticales. Ce détecteur a l'avantage d'être rapide de par son implémentation sous forme de filtres récurrents à impulsion infinie IIR, de plus il est moins coûteux en temps d'exécution. Nous avons testé et validé les résultats du détecteur de lignes sur les images d'empreintes digitales et comme perspectives, nous souhaitons implémenter la détection des jonctions et terminaisons pour extraire de l'empreinte digitale les minuties de type bifurcations et terminaisons.

Conclusion Générale

Et perspectives

Conclusion Générale et Perspectives

L'identification et la vérification par les systèmes biométriques utilise les caractéristiques humaines pour différencier les individus, plusieurs caractéristiques humaines ont été exploitées, certaines plus fiables que d'autres, mais toutes devaient être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu. Dans notre travail, nous avons choisi « l'empreinte digitale » comme modalité d'identification de par son ancienneté et sa mise à l'épreuve. Les minuties, qui représentent des discontinuités locales dans le flot des crêtes de l'empreinte digitale, sont utilisées pour l'identification. La plupart des systèmes utilise l'approche classique de détection de minuties basée sur la binarisation/squelettisation. Nous avons montré la simplicité d'extraire et détecter les minuties lorsque l'on dispose d'un squelette précis de l'image. L'inconvénient vient de la perte d'information et du bruit introduit au cours de la Binarisation, ce qui provoque l'apparition d'une multitude de fausses minuties et nécessite un traitement à posteriori, en plus l'étape de squelettisation est couteuse en temps de calcul car plusieurs balayages sont nécessaires selon l'épaisseur des stries de l'empreinte digitale. Ces considérations nous ont amené à étudier une autre approche qui porte sur la détection des lignes, jonctions des lignes et terminaisons directement de l'image en niveau de gris.

La détection des lignes est basée sur des filtres récurrents à impulsion infinie en retournant la plausibilité et l'orientation de chaque pixel de la ligne, donc l'image est améliorée avant de passer à l'extraction des jonctions et terminaisons, ceci favorise la méthode surtout quand il s'agit d'empreintes digitales de mauvaise qualité.

La détection et la localisation des jonctions et terminaisons des lignes sont réalisées par la suite en utilisant la courbure. L'utilisation des concepts mathématiques renforce la fiabilité des résultats et comme perspectives nous souhaiterons nous en profiter pour extraire de l'empreinte digitale, les minuties de type bifurcation et terminaisons, ensuite, passer à la sélection des minuties candidates à l'identification et l'authentification des personnes.

Bibliographie

Bibliographie

- [Bab,91] W.J.Babler, « Embryologic Development of Epidermal Ridges and Their Configurations », Dermatoglyphics: Science in transition. Birth defects, New York.Wiley-Liss, pp.95-112,1991.
- [Bel,06] R. Belguechi, «Contribution a la reconnaissance d'empreintes digitales par une approche hybride », thèse de magister, Institut National de formation en Informatique (I.N.I),Alger, 2006.
- [Bia et al, 02] Z.Bian .D.Zhang and W.Shu,"Knowledge-Based Fingerprint Post-Processing". International Journal of Pattern Recognition and Artificial Intelligence .Vol. 16,No1,pp.53-67,2002
- [Can,83] J.F.Canny.Finding Edges and Lines in Images. Technical report n°.720, Massachussts Institut of Technology,1983.
- [Clu, 03] **Club** de la **s**écurité des **S**ystèmes d'**I**nformation **F**rançais, Techniques de contrôle d'accès par biométrie, dossier technique de la commission de sécurité physique © Clusif, 2003
- [Der,87] R.Deriche Optimal Edge Detection Using Recursive Filtering.Proceedings of the first International Conference on Computer Vision (ICCV),pages 501-505,Londres,1987.
- [Des et al, 04] F. DESCHENES, D. ZIOU* and M.-F. AUCLAIR-FORTIER, Detection of lines, line junctions and line terminations, INT. J. REMOTE SENSING, ,VOL. 25, NO. 3, pp 511–535, 10 FEBRUARY, 2004
- [EM et al ,01] L.C.Em and G.Sulong,"fingerprint Classification Approches : An Overview ".Internationnal Symposium on Signal Proceeding and its Applications .Kuala Lumpur ,Malaysia ,13-16 August ,2001
- [Des, 99] F. Deschênes, Estimation des Jonctions du mouvement apparent et du relief

en vue d'une reconstruction 3D de la scène mémoire présenté au Département de mathématiques et d'informatique en vue de l'obtention du grade de maître des sciences (M.Sc.), université de Sherbrooke, Québec, Canada, Décembre 1999

- [Des, 00] F. Deschênes, D. Ziou * Detection of line junctions and line terminations using curvilinear features, Département de Mathématiques et d'Informatique, Fac des Sciences, Université de Sherbrooke, Québec, Canada J1K 2R1, Pattern Recognition Letters 21, 637-649, 2000
- [Gal, 05] Nicolas Galy, Etude d'un système complet de reconnaissance d'empreintes digitales pour un capteur microsysteme à balayage, thèse de doctorat, école doctorale électrotechnique, automatique, télécommunication, signal, institut national polytechnique de Grenoble, 2005
- [Jai et al,01] A.K Jain,S.Prabhakar and Pankanti ,”Twin Test : On Discriminability of Fingerprints ”,Proc.3rd International Conference on Audio-and Video Based Person Authentication,pp.211-216,Sweden,June 6-8,2001.
- [Kim et al ,01] S. Kim,D.Lee and J.Kim.”Algorithm for Detection and Elimination of False Minutiae inFingerprint Images” Lecture Notes in Computer Science .Springer Verlag.Vol. 2091.pp.235-240.2001.
- [Kit et al, 82] L.Kitchen and A.RosenEeld. Gray level Corner Detection. Pattern Recognition Letters I, pages 95-102, 1982.
- [Lam et al, 92] Lam, L., Seong-Whan Lee, and Ching Y. Suen, "Thinning Methodologies-A Comprehensive Survey," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol 14, No. 9 page 879, September 1992
- [Leu, 90] M.T.Leung. "Fingerprint Image Processing Using Neural Network", IEEE Proc on Computer and Communication Systems, 1990
- [Mai,97] 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

- [Mal et al, 03] D.Maltoni, D.Maio, A.K. Jain, S. Jain, S. Prabhakar. "Handbook of Fingerprint Recognition: Section 2.6 Fingerprint scanners and their features", Spring, New York, 2003
- [Nal, 04] Nalini Ratha, Ruud Bolle Automatic Fingerprint Recognition Systems, Springer, New York, 2004.
- [Ots,79] N. Otsu. " A Threshold Selection Method from Gray Level Histograms", IEEE Transactions on System, Man and Cybematics, Vol.9, pp.62-66, 1979.
- [Pan et al, 02] S.Pankanti, S.Prabhakar, A.K.Jain. "On The Individuality of Fingerprints", Transactions on PAMI, Vol. 48, No. 8, pp. 1010–1025, 2002.
- [Pra,01] Prabhakar, S,"Fingerprint Classification and Matching Using a Filterbank", Thèse PHD,Michigan State University in partial fulfillment of the requirements, 2001.
- [Rav et al,09] RAVI.J*, K.B.RAJA**, VENUGOPAL.K.R** fingerprint recognition using minutiae score matching, International Journal of Engineering Science and Technology, Vol.1(2), 35-42, 2009
- [Seo,02] B.C.Seow,S.K.Yeoh,S.L.Lai,N.A.Abu. " Image Based Fingerprint verification ", student Conference on Research and Development Proceedings,Malaysia,2002.
- [Soi et al ,96] V.Soifer ,V.Kotlyar,S.Khonima and Skidanov "Fingerprint identification using the directions field" ICPR proceedings,Vol.3,pp.586-590,1996
- [Sto et al ,94] J.D,Stosz and L.A.Alyea "Automated system for fingerprint authentication using pores and ridge structure" Proceeding of SPIE in automatic Systems for the Identification and Inspection of Humans,Vol,2277,pp.210-223,October 1994
- [Yag et al, 04] N.Yager and A. Amin "Finger print verification based on minutiae features: a review", Pattern Analysis and Applications, Vol. 7, No. 1, pp. 94-113, April 2004.

- [Zio,89] Ziou. D, WROBEL-DAUTCOURT. B «Filtres rékursifs pour la détction de contours “lignes de crêtes” et “marche” », Douzième Colloque Grets –Juan-Les-Pins, pp.637-640, JUIN1989.
- [Zio,98] Ziou, D., and S. Tabbone, "Edge Detection Techniques - An Overview", International Journal of Pattern Recognition and Image Analysis, vol. 8, no. 4, pp. 537–559, 1998.

Liens Internet

Liens Internet

- [1] <http://dit-archives.epfl.ch/FI00/fi-sp-00/sp-00-page25.html>

- [2] <http://www.parl.gc.ca/Content/LOP/ResearchPublications/06-30-f.htm>

- [3] <https://www.aiservice.fr/images/articles/2015/biometrie-vocale-depannage-informatique-paris-domicile.jpg>

- [4] <http://onin.com/fp/fphistory.html>

- [5] <http://www.biometrie-online.net/technologies/empreintes-digitales>

- [6] <http://www.sciencepresse.qc.ca/revue-presse/2010/11/03/comment-se-forment-structures-plissees>

- [7] <http://clercsvt.jimdo.com/curiosit%C3%A9s/le-saviez-vous/>

- [8] <http://www.biometrie-online.net/technologies/retine>

- [9] <http://www.biometrie-online.net/technologies/fonctionnement>

- [10] <https://www.securiteinfo.com/conseils/biometrie.shtml>

- [11] http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint_sensors_physics.html

Liens Internet

- [12] <http://www.biometrie-online.net/technologies/visage>

- [13] <http://www.lerepairedessciences.fr/sciences/forensics/empreintes/empreintes.htm>

- [14] http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint_algo.htm

- [15] <http://www.gettyimages.com/detail/photo/black-fingerprint-royalty-free-image/78718515>

- [16] http://www.mathworks.com/help/images/ref/bwmorph.html?s_tid=srchtitle

Résumé

L'identification et la vérification des identités de personnes se sont imposées comme une approche de sécurisation dans un environnement où un individu pourrait avoir plusieurs. Nous utilisons l'empreinte digitale.

L'extraction des minuties est une étape critique pour la performance d'un système d'identification et de vérification. Nous traitons deux méthodes : une méthode classique basée sur l'extraction des minuties depuis le squelette binaire de l'image d'empreinte digitale et une deuxième méthode basée sur l'extraction depuis l'image en niveau de gris.

Mots Clés :

Empreinte Digitale; Minutie; Extraction; Binarisation; Squelettisation; Bifurcation; Jonctions; Terminaison; Ligne; Courbure.