République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur Et de La Recherche Scientifique

Faculté des Sciences et Technologie
Département des Sciences et Technologie

N°d'ordre :

N°de série :

Projet de fin d'étude présenté en vue de l'obtention du diplôme de

MASTER

Domaine : Science et Technologie
Filière : Automatique
Spécialité : Automatique

Par : GOMRI SAID Mama
FELLAN Taher

THEME:

Soutenu publiquement le :

Devant le jury :

Mr : ……	MAA.	Univ. Ghardaïa	**Président**
Mr : ……	MAA.	Univ. Ghardaïa	**Examinateur**
Mr : ……	MAA.	Univ. Ghardaïa	**Examinateur**
Mr : ……	MAA.	Univ. Ghardaïa	**Encadreur**

ANNEE UNIVERSITAIR 2016/2017

ملخص

ويندرج هذا العمل ضمن الإطار العام للالقياسات الحيوية .وبشكل أكثر تحديدا تتكون في تطوير نظام التعرف على بصمات الأصابع باستخدام تقنيات متقدمة لمعالجة الصور والتمييز والطبقية متعددة.

عموما، في نظام التعرف على بصمات الأصابع هناك ثلاث وحدات :تجهيزها، وخصائص الجيل النواقل والتصنيف.

وفيما يتعلق مرحلة التصنيف، قد وضعنا نوع من المصنفات لتعلم المصنف .(HMM) والتقطت الصور اختبار من قاعدة البيانات تستخدم على نطاق واسع وهذا هو أساس FVC2000 و.FVC2002

كلمات المفتاحية : [القياسات الحيوية، بصمات الأصابع، والاعتراف، والتصنيف، HMM]

RESUME

Ce travail entre dans le cadre général de la biométrie ; plus précisément il consiste à mettre au point un système de reconnaissance de l'empreinte digitale en utilisant des techniques évoluées du traitement de l'image et de la discrimination multi classes.

D'une manière générale, dans un système de Reconnaissance de l'empreinte digitale on trouve trois modules : prétraitement, génération de vecteur caractéristiques et classification.

Concernant l'étape de classification, nous avons mis au point un seul types de classifieurs à savoir un classifieur (HMM). Les images de test sont prises à partir d'une base largement utilisée qui est la base de données FVC2000 et FVC2002.

Mots clés : [Biométrie, Empreintes digitales, Reconnaissance, Classification, HMM]

ABSTRACT

This work falls within the general framework of biometrics; More precisely, it consists in developing a fingerprint recognition system using advanced techniques of image processing and multi-class discrimination.

Generally speaking, in a Fingerprint Recognition System there are three modules: pre-processing, character vector generation and classification.

Concerning the classification step, we have developed two types of classifiers namely a classifier (HMM). The test images are taken from a widely-used database which is the FVC2000 and FVC2002 database.

Key words: [Biometrics, Fingerprints, Recognition, Classification, HMM]

Remerciements

Avant tout, je remercie le bon dieu, tous puissant de m'avoir donnée la santé, la volonté, la patience et les moyens afin que je accomplir ce modeste travail

« Merci Dieu »

Mes vifs remerciements aussi à mes parents pour tous les sacrificiel qu'ils ont constitué à mon égard.

Je tiens à remercier sincèrement mes promoteur Mr : ARIF MOHAMMED de m'avoir dirigé, Il s'est toujours très disponible tous au Lang de la réalisation de ce mémoire

« Merci monsieur »

Je respect s'adressent à l'ensemble des enseignants qui nous ont suivis durant mon cycle d'étude et mon chef de département

M : ARIF MOHAMMED.

Enfin je tiens à exprimer ma gratitude à toute les personnes ayant contribué de près on loin à la réalisation de ce mémoire

« Merci à tous »

Dédicace

Je dédie ce travail à :

*En premier lieu à mes **parents** ; mes **grands-pères** ; mes **grand**s-mères et ma seule sœur ; **Amina** ; et mes frères **Djilali** et **Mohammed El Hadi.***

Aussi je voudrais remercier mes oncles, et mes tantes,

*A toutes les familles **GOMRI SAID &SABEUR sans** exception.*

*A toutes mes amies, particulièrement : **Yamina, Halima, Wahiba, Madjda et Assma***

Sons oublier mes voisines qu'on m'aide de continuer mes études que dieu aide tous les personnes qu'ont m'aider de préparer ma mémoire.

J'espère que je devenir une étudient symbole pour mon entourage et un bijou lumière dans la vie scientifique.

Merci

« MAMA »

Dédicace

A la mémoire de mon défunt père.

À la plus belle créature que Dieu a créée sur terre,

À cet source de tendresse, de patience et de générosité,

À mes Parent !

A mes chères sœurs : Bouchra et Khaira

À tous mes amis et collègues ***B. ABDOU ;***

B. MOUHAMED ; C. MOULOUD ; MOUSSA ;

YOUCEF ; AHMED ; A. ABDOU ; LEILA ; et cher amie G S. MAMA

À tous les étudiants de la promotion 2015/2017

Option : Automatique

A tous ceux qui, par un mot, m'ont donné la force de continuer ....

Merci

FELLANTAHER

TABLE DES MATIERES

Chapitre III

L'orientation de champ de l'empreinte digitale

Chapitre IV

Analyse, résultat et discussion

Liste de figure

Chapitre I

Chapitre II

Chapitre III

Liste de tableau

Introduction générale

La biométrie est la technologie d'authentification et d'identification des individus la plus utilisée de nos jours. Elle remplace de plus en plus les anciennes techniques d'identification qui sont basées sur la possession ou la connaissance d'identifiant externe (badge, code, clé…) susceptible d'être perdu, oublié ou encore volé. Elle s'appuie sur la prise en compte des caractéristiques physiologiques, et comportementales propres et uniques à chaque individu.

La biométrie, qui désigne la mesure d'attributs caractéristiques du corps humain, est très utile pour authentifier un individu, notamment pour le contrôle d'accès. Le marché de l'authentification par biométrie est favorisé par les récents progrès des technologies informatiques, et l'essor du commerce électronique et des objets de communication nomades (téléphones et ordinateurs portables, PDA ((Personale Digital Assistant) … etc.), qui nécessitent d'identifier d'une manière plus sûre une personne physique plutôt que d'utiliser un mot de passe ou une carte d'accès.

Le système biométrique utilise le matériel pour capturer les informations biométriques et le logiciel pour les gérer et les maintenir. Parmi toutes ces techniques, l'utilisation de l'empreinte digitale comme un moyen d'identification et d'authentification, est celle qui est la plus courante. La force de ce procédé tient du fait que l'utilisation de l'empreinte digitale est généralement plus facile d'acception par la communauté, et qu'elle est une des plus efficaces et des moins coûteuses. La raison principale de l'utilisation d'empreinte dans le système identification ou vérification est que l'empreinte est unique et reste invariable avec l'âge.

Les travaux effectués dans le cadre de ce mémoire portent donc sur la Reconnaissance de l'Empreinte Digitale (RED), qui est le moyen le plus utilisé. Cependant, la plupart des systèmes d'identification des empreintes digitales consiste à extraire en premier lieu de l'empreinte à étudier tous les points de minuties, et ensuite comparer ces points avec ceux des modèles enregistrés dans une base de données pour trouver le modèle qui présente le plus de corrélation avec l'empreinte étudiée. Mais Cette approche présente quelques difficultés comme par exemple :

- Il est très difficile d'extraire les minuties d'une image d'empreinte digitale bruitée. Ce problème est très fréquent dans la pratique.

- Le changement d'échelle, de translation et de rotation des empreintes digitales pose des difficultés pour l'étape de mise en correspondance.

Aussi, pour passer ces limitations, nous proposons dans ce travail une méthode d'identification des empreintes digitales se basant sur l'utilisation de l'orientation du champ après l'utilisation de calcul de la distance euclidienne.

Le plan du mémoire est organisé comme suit :

***Chapitre I* :** Généralités sur les systèmes de reconnaissance biométrique :

Dans le chapitre 1, nous présentons un survol des techniques pour l'identification et l'authentification automatiques de personnes ainsi que des notions sur la biométrie.

***Chapitre II* :** L'Etat de l'art de l'empreinte digital :

Ce chapitre sera consacré à l'état de l'art de l'empreinte digitale et les différentes approches de vérification de l'empreinte digitale. Cette étape comprend aussi des processus de traitement d'image en général (atténuation du bruit, binarisation, squelettisation,) et d'autres plus spécifiques au traitement de l'empreinte digitale (détection du point central, détection et élimination des fausses minuties…). En plus Les deux méthodes utilisées pour l'identification (SVM, HMM)

***Chapitre III* :** l'orientation de champ de l'empreinte digitale :

***Chapitre IV* :** Résultats, Analyses et Discussions :

Ce chapitre présente les résultats expérimentaux réalisés sur une base de données standard ainsi que les différents tests de validation effectués et la comparaison des résultats obtenus avec d'autres résultats de la même base de données.

Ce mémoire est terminé par une conclusion générale mettant en relief les résultats obtenus sur l'ensemble de cette étude ainsi que des perspectives à réaliser à long terme.

Chapitre I

Généralités sur les systèmes de reconnaissance biométrique

Dans ce premier chapitre,
nous présenterons la biométrie de manière générale, et Les systèmes de reconnaissance biométrique

I.1. Introduction

I.1.1. Introduction à la biométrie :

La biométrie est un ensemble des technologies (appelée les technologies biométriques) qui exploitent des caractéristiques humaines physiques ou comportementales telles que l'empreinte digitale, la signature, l'iris, la voix, le visage, la démarche, et un geste de main pour différencier des personnes. Ces caractéristiques sont traitées par certain ordre des processus automatisés à l'aide des dispositifs comme des modules de balayage ou des appareils - photos. A la différence des mots de passe ou des PINs (numéros d'identification personnelle) qui sont facilement oubliés ou exposés à l'utilisation frauduleuse, ou des clefs ou des cartes magnétiques qui doivent être portées par l'individu et sont faciles à être volées, copiées ou perdues, ces caractéristiques biométriques sont uniques à l'individu et il y a peu de possibilité que d'autres individus peuvent remplacer ces caractéristiques, donc les technologies biométriques sont considérées les plus puissantes en termes de sécurité.

En plus les mesures biométriques sont confortables parce qu'elles n'ont pas besoin d'être portées séparément. De telles caractéristiques peuvent être bien employées pour obtenir l'identification/authentification pour accéder à des systèmes tels ATMs (guichet automatique). La biométrie se prouve également comme outil puissant d'identification/vérification aux scènes de crime dans le secteur juridique.

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

I.1.2. Vérification :

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

I.1.3. Identification :

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

Problématique :

L'ingénieur étant une personne capable d'apporter toujours des solutions aux problèmes de sa nation, nous nous sommes proposés de concevoir et de mettre en place un système de reconnaissance biométrique des empreintes digitales qui va rendre l'authenticité des documents de trafic tels le passeport ou autres documents aux citoyens détenteurs.

Comme il y a tant des fraudes des documents de trafic, la reconnaissance biométrique des empreintes digitales est idéale pour résoudre le problème de la sécurité lorsqu'on effectue des trafics via différentes frontières. Nous allons donc concevoir et mettre en place un système de reconnaissance biométrique qui va minimiser les fraudes.

Nous nous permettons ici d'évoquer les besoins aux quels notre système de reconnaissance d'empreinte doit répondre :

1- Doit donné des résultats corrects de la reconnaissance d'une manière claire et nette ;
2- Doit gérer si le document de trafic est actif ou non - actif ;
3- Doit générer les rapports de trafic pendant une période.

Qu'est-ce que la biométrie ؟

Une ancienne définition du mot biométrie est : « Étude statistique des dimensions et de la croissance des êtres vivants » ou « Mesure des dimensions du corps humain, d'un organe ». Une définition plus récente décrit la biométrie connue étant une « Technique permettant de contrôler l'identité de quelqu'un par la reconnaissance automatique de certaines de ses caractéristiques physiques ou comportementales préalablement enregistrées (empreintes digitales, visage, voix, etc.) » [Larousse 2015]. Ainsi, la biométrie repose sur « Technique qui permet d'associer à une identité une personne voulant procéder à une action, grâce à la reconnaissance automatique d'une ou de plusieurs caractéristiques physiques et comportementales de cette personne préalablement enregistrées (empreintes digitales, visage, voix, etc.) ».

I.2. Définition :

La biométrie peut être définie comme étant « la reconnaissance automatique d'une personne en utilisant des traits distinctifs ». Une autre définition de la biométrie est « toutes caractéristiques physiques ou traits personnels automatiquement mesurables, robustes et distinctives qui peuvent être utilisées pour identifier ou pour vérifier l'identité prétendue d'un individu » [1].

La biométrie consiste en l'analyse mathématique des caractéristiques biologiques d'une personne et a pour objectif de déterminer son identité de manière incontestable. Contrairement à ce que l'on sait ou ce que l'on possède, la biométrie est basée sur ce que l'on est et permet ainsi d'éviter la duplication, le vol, l'oubli ou la perte.

Un système biométrique peut avoir deux modes opératoires [2] :

I.2.1. L'identification :

Elle permet d'établir l'identité d'une personne à partir d'une base de données, le système biométrique pose et essaye de répondre à la question, « qui est la personne X ? », il s'agit d'une comparaison du type un contre plusieurs (1 : N).

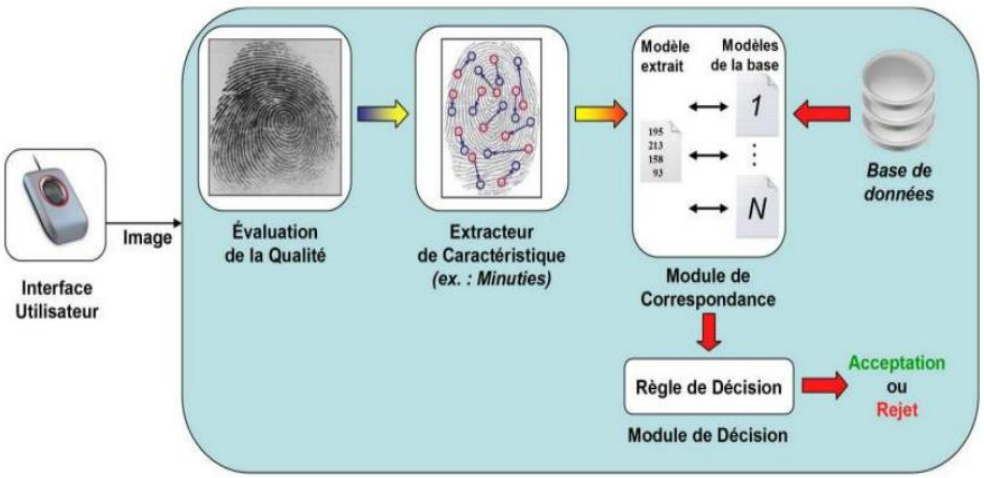


Figure I-1 : Identification d'une personne dans un système biométrique [3].

I.2.2. La vérification ou l'authentification :

Le système biométrique demande à l'utilisateur son identité et essaye de répondre à la question, « est - ce la personne X ? ». Dans une application de vérification, l'utilisateur annonce son identité

par l'intermédiaire d'un mot de passe, d'un numéro d'identification, d'un nom d'utilisateur, ou toute combinaison des trois. Le système sollicite également une information biométrique provenant de l'utilisateur, et compare la donnée caractéristique obtenue à partir de l'information entrée, avec la donnée enregistrée correspondante à l'identité prétendue, c'est une comparaison un à un (1 :1). Le système trouvera ou ne trouvera pas d'appariement entre les deux. La vérification est communément employée dans des applications de contrôle d'accès et de paiement par authentification.

La biométrie offre beaucoup plus d'avantages que les méthodes existantes d'authentification (ID), les mots de passe et les cartes magnétiques. En effet, elle fournit encore plus de sûreté et de convenance ce qui engendre d'énormes avantages économiques et elle comble les grandes failles de sécurité des mots de passe.

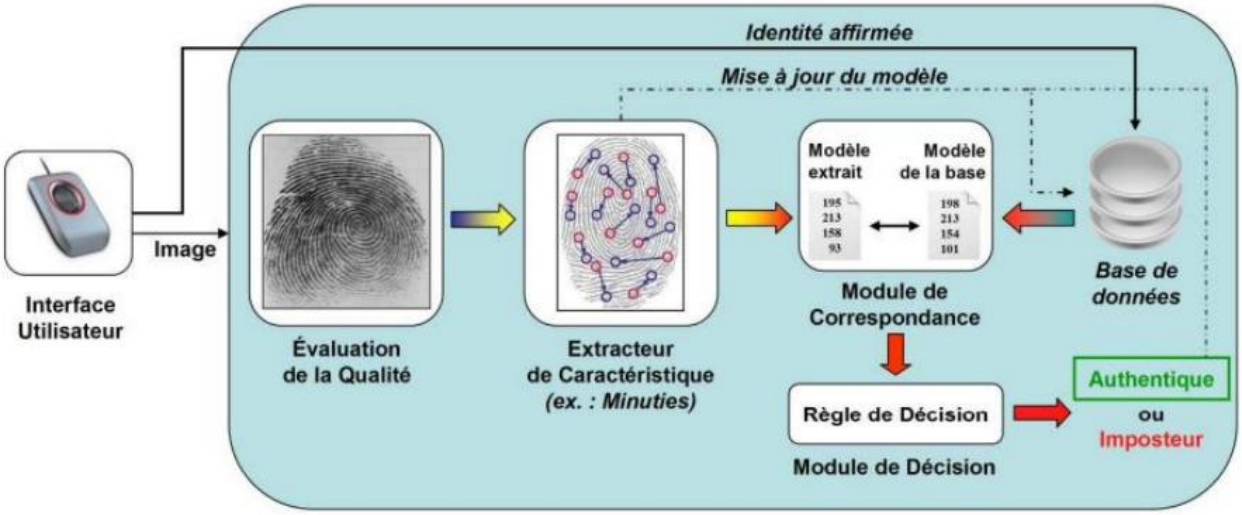


Figure I-2 : Authentification d'une personne dans un système biométrique [3].

I.3. Généralité sur la biométrie

Les systèmes biométriques sont de plus en plus utilisés depuis quelques années. L'apparition de l'ordinateur et sa capacité à traiter et à stocker des données ont permis la création des systèmes biométriques informatisés. Il existe plusieurs caractéristiques physiques uniques pour un individu, ce qui explique la diversité des systèmes appliquant la biométrie, selon ce que l'on prend en compte :

1- L'empreinte digitale

2 -La géométrie de la main

3 -L'iris

4 -La rétine

5 -La voix ... etc.

Nous allons voir dans ce chapitre, les principales technologies biométriques, puis nous allons nous focaliser sur les systèmes de reconnaissance des empreintes digitales, leurs avantages et les problèmes liés à leurs applications.

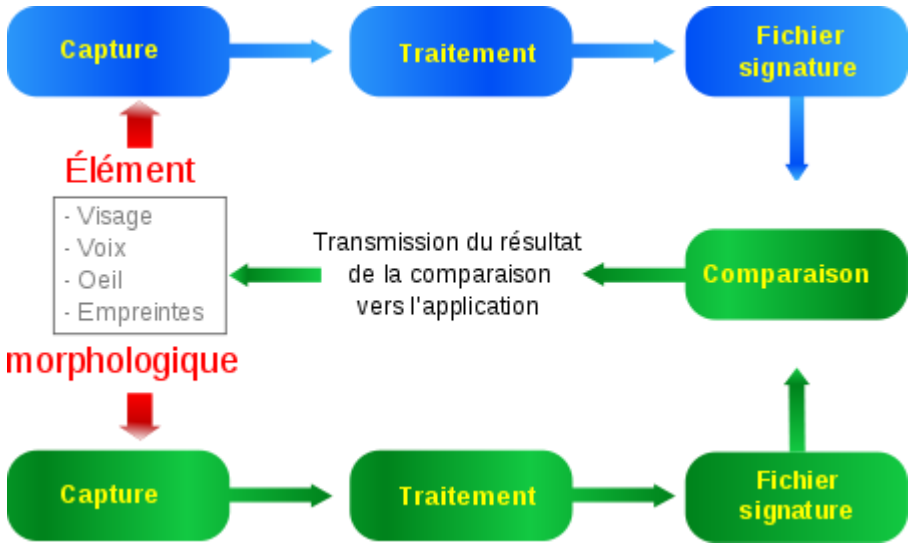


Figure I-3 : Schéma de fonctionnement d'un système biométrique

I.3.1. Présentation de quelque technologie biométrique

Aucune biométrie unique ne pouvait répondre efficacement aux besoins de toutes les applications d'identification. Un certain nombre de techniques biométriques ont été proposées, analysées et évaluées. Chaque biométrie à ses forces et ses limites, et en conséquence, chaque biométrie est utilisée dans une application particulière. Pour les caractéristiques physiques, nous décrirons la reconnaissance de visage, les empreintes digitales, la géométrie de la main et l'iris. Pour les caractéristiques comportementales, nous décrirons les biométries basées sur la voix et la signature.

Il existe d'autres systèmes biométriques basés sur les veines de la main, l'A.D.N, l'odeur corporelle, la forme de l'oreille, la forme des lèvres, le rythme de frappe sur un clavier, la démarche, qui ne seront pas développées dans ce chapitre.

I.3.1.1. Les empreint digitales

A l'heure actuelle, la reconnaissance des empreintes digitales est la méthode biométrique la plus utilisée. Les empreintes digitales sont composées de ligne localement parallèle présentant des points singuliers (minuties) et constituent un motif unique, universel et permanent. Pour obtenir une image de l'empreinte d'un doigt, les avancées technologiques ont permis d'automatiser la tâche au moyen de capteurs intégrés, remplaçant ainsi l'utilisation classique de l'encre et du papier. Ces capteurs fonctionnant selon différents mécanismes de mesure (pression, champ électrique, température) permettent de mesurer l'empreinte d'un doigt fixe positionné sur ce dernier (capteur matriciel) ou en mouvement (capteurs à balayage).

L'image d'empreinte d'un individu est capturée à l'aide d'un lecteur d'empreinte digitale puis les caractéristiques sont extraites de l'image puis un modèle est créé. Si des précautions appropriées sont suivies, le résultat est un moyen très précis d'authentification.

Les techniques d'appariement des empreintes digitales peuvent être classées en deux catégories : les techniques basées sur la détection locale des minuties et les techniques basées sur la corrélation. L'approche basée sur les minuties consiste à trouver d'abord les points de minuties puis trace leurs emplacements sur l'image du doigt.

Cependant, il y a quelques difficultés avec cette approche lorsque l'image d'empreinte digitale est d'une qualité médiocre, car l'extraction précise des points de minutie est difficile. Cette méthode ne tient pas en compte la structure globale de crêtes et de sillons. Les méthodes basées sur la corrélation sont capables de surmonter les problèmes de l'approche fondée sur les minuties.

Ces méthodes utilisent la structure globale de l'empreinte, mais les résultats sont moins précis qu'avec les minuties. De plus, les techniques de corrélations sont affectées par la translation et rotation de l'image de l'empreinte. C'est pour cela que les deux approches sont en général combinées pour augmenter les performances du système. [5]

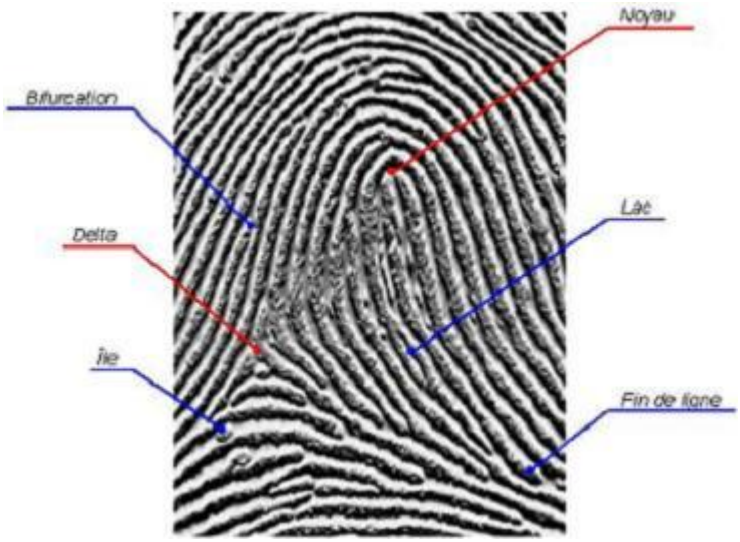


Figure I-4 : Empreinte digitale [5]

I.3.1.2. La voix

De tous les traits humains utilisés dans la biométrie, la voix est celle que les humains apprennent à reconnaitre dès le plus jeune âge. Les systèmes de reconnaissance de locuteur peuvent être divisés en deux catégories : les systèmes dépendant du texte prononcé et les systèmes indépendants du texte. Dans le premier cas, l'utilisateur est tenu d'utiliser un texte (un mot ou une phrase) fixe prédéterminé au cours des séances d'apprentissage et de reconnaissance. Alors que, pour un système indépendant du texte le locuteur parle librement sans texte prédéfini. Cette dernière catégorie est plus difficile, mais elle est utile dans le cas où l'on a besoin de reconnaitre un locuteur sans sa coopération. La recherche sur la reconnaissance de locuteur est en pleine croissance, car elle ne nécessite pas de matériel cher, puisque la plupart des ordinateurs personnels de nos jours sont équipés d'un microphone. Toutefois, la mauvaise qualité et le bruit ambiant peuvent influencer la vérification et par suite réduire son utilisation dans les systèmes biométriques.

Dans un système de reconnaissance vocal, le signal est premièrement mesuré puis décomposé en plusieurs canaux de fréquences passe - bande. Ensuite, les caractéristiques importantes du signal vocal sont extraites de chaque bande. Parmi les caractéristiques les plus communément utilisées sont les coefficients Cepstraux. Ils sont obtenus par le logarithme de la transformée de Fourier du signal vocal dans chaque bande. Finalement, la mise en correspondance des coefficients Cepstraux permet de reconnaitre la voix. Dans cette étape, généralement on fait

appel à des approches fondées sur les modèles de Markov cachés, la quantification vectorielle, ou la déformation temps dynamique. [5]

Figure I-5 : la reconnaissance vocale [5]

I.3.1.3. Liris :

L'utilisation de l'iris comme caractéristique biométrique unique de l'homme a donné lieu à une technologie d'identification fiable et extrêmement précise. L'iris est la région, sous forme d'anneau, située entre la pupille et le blanc de l'oeil, il est unique. L'iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu. Les algorithmes utilisés dans la reconnaissance de l'iris sont si précis que la planète toute entière pourrait être inscrite dans une base de données de l'iris avec peu d'erreurs d'identification. L'image de l'iris est généralement capturée à l'aide d'une caméra standard. Cependant, cette étape de capture implique une coopération de l'individu. De plus, il existe plusieurs contraintes liées à l'utilisation de cette technologie. Par exemple, il faut s'assurer que l'iris de l'individu est à une distance fixe et proche du dispositif de capture, ce qui limite l'utilisation de cette technologie. [6]

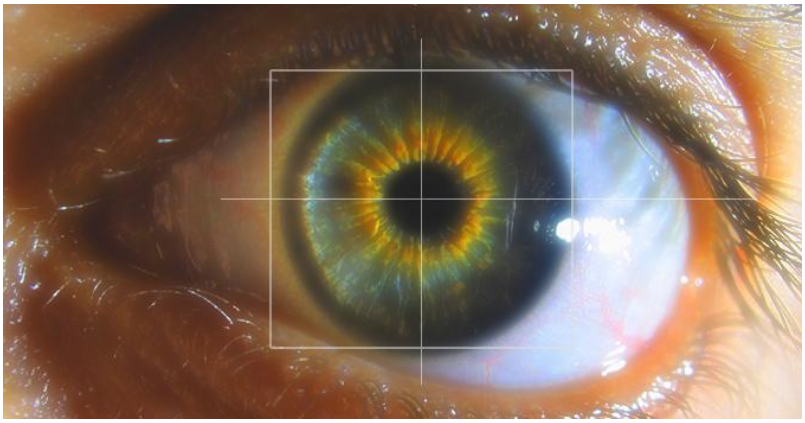


Figure I-6 : L'utilisation de l'iris [6]

I.3.1.4. La géométrie de la main

La géométrie de la main est une technologie biométrique récente. Comme son nom l'indique, elle consiste à analyser et à mesurer la forme de la main, c'est - à - dire mesurer la longueur, la largeur et la hauteur de la main d'un utilisateur et de créer une image 3-D. Des LEDs infrarouges et un appareil - photo numérique sont utilisés pour acquérir les données de la main.

Cette technologie offre un niveau raisonnable de précision et est relativement facile à utiliser. Cependant, elle peut être facilement trompée par des jumeaux ou par des personnes ayant des formes de la main proches. Les utilisations les plus populaires de la géométrie de la main comprennent l'enregistrement de présence et le contrôle d'accès. Par contre, les systèmes de capture de la main sont relativement grands et lourds, ce qui limite leur utilisation dans d'autres applications comme l'authentification dans les systèmes embarqués : téléphones portables, voitures, ordinateurs portables,etc.[6]

Figure I-7 : La géométrie de la main

I.3.1.5. Le visage :

Nos visages sont des objets complexes avec des traits qui peuvent varier dans le temps. Cependant, les humains ont une capacité naturelle à reconnaitre les visages et d'identifier les personnes dans un coup d'œil. Bien sûr, notre capacité de reconnaissance naturelle s'étend au - delà de la reconnaissance du visage, où nous sommes également en mesure de repérer rapidement des objets, des sons ou des odeurs. Malheureusement, cette aptitude naturelle n'existe pas dans les ordinateurs. C'est ainsi qu'est né le besoin de simuler artificiellement la reconnaissance afin de créer des systèmes intelligents autonomes. Simuler notre capacité naturelle de la reconnaissance faciale dans les machines est une tâche difficile mais pas impossible. Tout au long de notre vie, de nombreux visages sont vus et conservés naturellement dans nos mémoires formant une sorte de base de données.

La reconnaissance faciale par ordinateur nécessite également une base de données qui est habituellement construire en utilisant des images du visage ou parfois des images différentes d'une même personne pour tenir compte des variations dans les traits du visage. Les systèmes actuels de reconnaissance faciale sont composés d'un module d'acquisition d'imagesavec une caméra. Il procède d'abord à une détection du visage dans l'image acquise. Ensuite, l'image du visage détectée est normalisée pour êtretransmise au module de reconnaissancequi va la traiter en utilisant des algorithmes afin d'extraire une signature faciale.

Finalement, cette signature est comparée, à l'aide d'un classificateur, avec les signatures déjà existantes dans une base de données locale, afin d'identifier l'individu en question..Durant la dernière décennie de recherche, la performance des systèmes de reconnaissance faciale s'est grandement améliorée, mais les résultats sont encore loin d'être parfaits. Ces systèmes sont très sensibles aux variations d'illumination et de pose. [6]

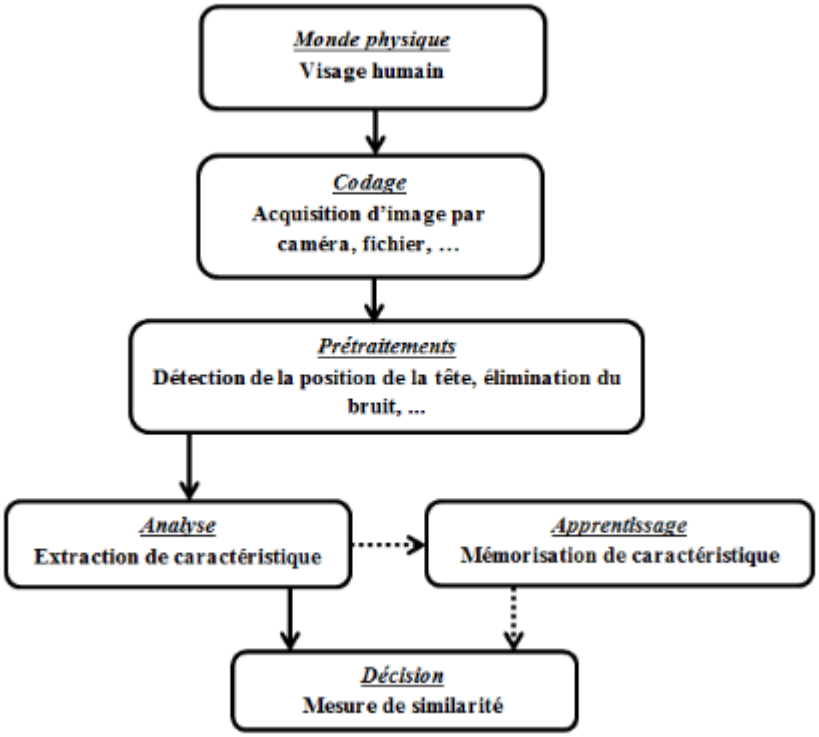


Figure I-8 : Schéma synoptique d'un système de reconnaissance faciale [6]

I.4. Architecture d'un système biométrique

Il existe toujours au moins deux modules dans un système biométrique : Le module d'apprentissage et celui de reconnaissance [6].

Le troisième module (facultatif) est le module d'adaptation. Pendant l'apprentissage, le système va acquérir une ou plusieurs mesures biométriques qui serviront à construire un modèle de l'individu.

I.4.1. Module d'apprentissage

Au cours de l'apprentissage, la caractéristique biométrique est tout d'abord mesurée grâce à un capteur ; on parle d'acquisition ou de capture. En général, cette capture n'est pas directement stockée et des transformations lui sont appliquées. En effet, le signal contient de l'information inutile à la reconnaissance et seuls les paramètres pertinents sont extraits. [6]

I.4.2. Module de reconnaissance

Au cours de la reconnaissance, la caractéristique biométrique est mesurée et un ensemble de paramètres est extrait comme lors de l'apprentissage. Le capteur utilisé doit avoir des propriétés aussi proches que possibles du capteur utilisé durant la phase d'apprentissage. Si les deux capteurs ont des propriétés trop différentes, il faudra en général appliquer une série de prétraitements supplémentaires pour limiter la dégradation des performances. La suite de la reconnaissance sera différente suivant Le mode opératoire du système identification ou vérification. En mode identification, le système doit deviner l'identité de la personne. Il répond donc à une question de type : « Qui suis-je ? ». Dans ce mode, le système compare le signal mesuré avec les différents modèles contenus dans la base de données (problème de type 1 : n). En général, lorsque l'on parle d'identification, on suppose que le problème est fermé, c'est-à-dire que toute personne qui utilise le système possède un modèle dans la base de données. [6]

I.4.3. Module d'adaptation :

Pendant la phase d'apprentissage, le système biométrique ne capture souvent que quelques instances d'un même attribut afin de limiter la gêne pour l'utilisateur. Il est donc difficile de construire un modèle assez général capable de décrire toutes les variations possibles de cet attribut. De plus, les caractéristiques de cette biométrie ainsi que ses conditions d'acquisition peuvent varier. L'adaptation est donc nécessaire pour maintenir voire amélioré la performance d'un système utilisation après utilisation. [6]

I.4.4. Applications de la biométrie

On distinguera quatre groupes importants d'utilisateurs de ces différentes techniques biométriques. On parlera alors de service public, application de la loi, transaction commerciale et bancaire, accès physique et logique. [6]

A) Service publique : utilisée surtout pour le contrôle automatique des entrées et sorties d'un territoire, le contrôle des flux d'immigrations, dans les aéroports, on notera sur tout l'utilisation de techniques telles que : l'iris, l'empreinte digitale, les traits du visage.

B) Application de la loi : dans ce cas précis, la biométrie permet de faciliter certaines opérations comme l'authentification d'identité de criminels par reconnaissance automatique de leurs empreintes digitales. Cette pratique qui a montré son efficacité se mondialise, du coup, la réalisation d'une base de données mondiale est en cours de réflexion. On trouve aussi d'autres utilisations, comme le suivi des prisonniers à domicile assuré par des systèmes de vérification de la voix dans certains états des Etats Unis. On trouvera même que certaines de ces techniques ont aidé à identifier des victimes lors de kidnapping ou à retrouver une identité masquée.

C) Transaction commerciale et bancaire : Utilisé aussi dans des opérations de commerce électronique visant à renforcer l'achat d'un bien ou d'un service.

Pour renforcer ces échanges, on a vu l'apparition de machine de retraits automatiques disposant d'un système de vérification par l'iris.

D) Accès physique et logique : on parle de contrôle d'accès physique lorsqu'on cherche à sécurises l'accès à un lieu (entrée d'un bâtiment), alors que le contrôle d'accès logique concerne l'accès informatique à un terminal, serveur ou réseau informatique ou de télécommunication (ex :ordinateur, téléphone portable, base de données privée).

Pourquoi la biométrie ?

Les arguments pour la biométrie se résument en 2 catégories : Praticité : Les mots de passe comme les cartes de crédit, les cartes de débit, les cartes d'identité ou encore les clés peuvent être oubliés, perdus, volés et copiés. En plus, aujourd'hui tous et chacun doivent se rappeler une multitude de mots de passe et avoir en leur possession un grand nombre de cartes.

De son côté la biométrie serait immunisée contre ce genre de maux en plus qu'elle serait simple et pratique, car il n'y a plus ni cartes ni mots de passe à retenir. La biométrie serait capable de réduire, sans l'éliminer, le crime et le terrorisme car, à tout de moins, elle complique la vie des criminels et des terroristes. [5].

La biométrie est basée sur l'analyse de données liées à l'individu et peut être classée en trois grandes,catégories

- L'analyse morphologique : les empreintes digitales, l'iris, la forme de la main, les traits du visage, le réseau veineux de la rétine.

- L'analyse biologique : l'ADN, le sang, la salive, l'urine, l'odeur, la thermographie.
- L'analyse comportementale : la reconnaissance vocale, la dynamique de frappe au clavier, la dynamique de signature, la manière de marcher. [6]

I.5. Fonctionnement des systèmes biométriques [6]

D'abord, ces systèmes fonctionnent sur une base de probabilité et non d'une simple comparaison. Plus précisément, même si deux vecteurs sont

Identiques il en résultera quand même que deux lectures biométriques du même doigt (pour les scanographes d'empreintes digitales par exemple) ne donneront jamais exactement le même résultat. Cela à cause des conditions environnementales, des changements de température, des légers.

Changements sur les vecteurs biométriques (doigt enflé suite à un coup par exemple), des changements dans la façon dont la personne présente son doigt au lecteur et beaucoup d'autres imprévus. Ainsi la machine quantifie la probabilité que deux vecteurs proviennent de la même personne. Les personnes en autorité déterminent le seuil de tolérance, c'est-à-dire le niveau d'erreurs que la machine acceptera (car deux lectures d'un même vecteur, même provenant du même doigt et de la même personne, ne donneront jamais le même résultat), donc le seuil qui détermine le niveau de similitude minimum entre le vecteur emmagasiné et celui qui est présenté au lecteur afin de déterminer si une personne sera ou non reconnue comme légitime.

Ce faisant, il y a deux types d'erreur que les lecteurs peuvent engendrer :les fausses acceptations, le système accepte ceux qui ne le devraient pas; les faux rejets, le système rejette des gens dont la signature biométrique devrait être acceptée.

Il Y a deux utilisations des systèmes biométriques, soit l'identification et l'authentification. La première constitue la recherche d'une personne parmi tant d'autres, il y a donc une banque de données et il y a utilisation d'un vecteur pour trouver si et à quel fichier la personne correspond, il faut ainsi trouver qui elle est. L'authentification est la comparaison entre un fichier précis et le vecteur que la personne présente, il ne s'agit plus de trouver qui est la personne comme avec l'identification, mais bien de savoir si elle est qui elle prétend être.

Une nouvelle tendance en biométrie est l'approche multimodes (Multimodal) où plusieurs capteurs différents sont intégrés. C'est ce que tente Accenture Technologie Labos qui déploie un cadre bayésien (Bayesianframework) pour intégrer de nombreux capteurs pour la surveillance complexe et plus globale. Cette approche intègre 30 caméras, des capteurs IR (infra-rouge) et un lecteur d'empreintes digitales. Le tout pour surveiller 18 000 pieds carrés (1 672 m2) de superficie

d'un édifice à bureaux. Tout le monde est surveillé en permanence, mais en plus l'ordinateur calcule la probabilité qu'une personne se trouve à un endroit précis en utilisant des « a priori» (quelqu'un se trouve plus souvent à un endroit que ses autres collègues) et des probabilités transitionnelles (personne ne peut être à deux endroits au même moment par exemple).Situation de l'industrie des systèmes biométriques Au printemps 2002, les solutions biométriques n'avaient pas encore atteint le grand public. Les utilisateurs actuels ont tendance à être des organismes gouvernementaux, des militaires et de très grandes entreprises. Bien que la recherche dans ce domaine soit bien établie, l'application des solutions de la biométrie n'a pas encore véritablement trouvé sa voie sur le marché. Le groupe des fournisseurs est plutôt fragmenté et il est principalement formé de petites entreprises spécialisées dans des solutions biométriques destinées à régler des problèmes particuliers. Récemment, des fusions, des acquisitions et des ententes importantes ont été conclues entre ces fournisseurs, ce qui prouve que l'industrie se dirige vers des entreprises plus grandes et plus stables offrant une plus vaste gamme de produits. Voici deux exemples de fusions majeures annoncées récemment :

● Identix (Nasdaq : IDNX) et Visionics (Nasdaq : VSNX) ont annoncé leur fusion le 22 février 2002. On pourrait dire qu'Identix est le principal fournisseur de systèmes biométriques de reconnaissance des empreintes digitales, tandis que Visionics est un chef de file des systèmes biométriques de reconnaissance de la forme du visage et des empreintes digitales.

● L'acquisition d'Ankari, entreprise canadienne d'avant-garde spécialisée dans la biométrie des empreintes digitales, par Active Card (Nasdaq: ACTI), fournisseur principal de cartes à mémoire et de produits d'identification numérique, a été annoncée le 14 novembre 2001.

I.6. Le marché mondial de la biométrie

Régulièrement, un rapport sur le marché de la biométrie est édité par IBG (International Biométrique Group). Cette étude est une analyse complète des chiffres d'affaires, des tendances de croissance, et des développements industriels pour le marché de la biométrie actuel et futur.

La lecture de ce rapport est essentielle pour des établissements déployant la technologie biométrique, les investisseurs dans les entreprises biométriques, ou les développeurs de solutions biométriques.

Le chiffre d'affaires de l'industrie biométrique
incluant les applications judiciaires et celles du secteur public, se développe rapidement. Une grande partie de la croissance sera attribuable au contrôle d'accès aux systèmes d'information (Ordinateur / réseau) et au commerce électronique, bien que les applications du secteur public continuent à être une partie essentielle de l'industrie.
On prévoit que le chiffre d'affaires des marchés émergents (accès aux systèmes d'information, commerce électronique et téléphonie, accès physique et surveillance) dépasse le chiffre d'affaires des secteurs plus matures (identification criminelle et identification des citoyens).[5]

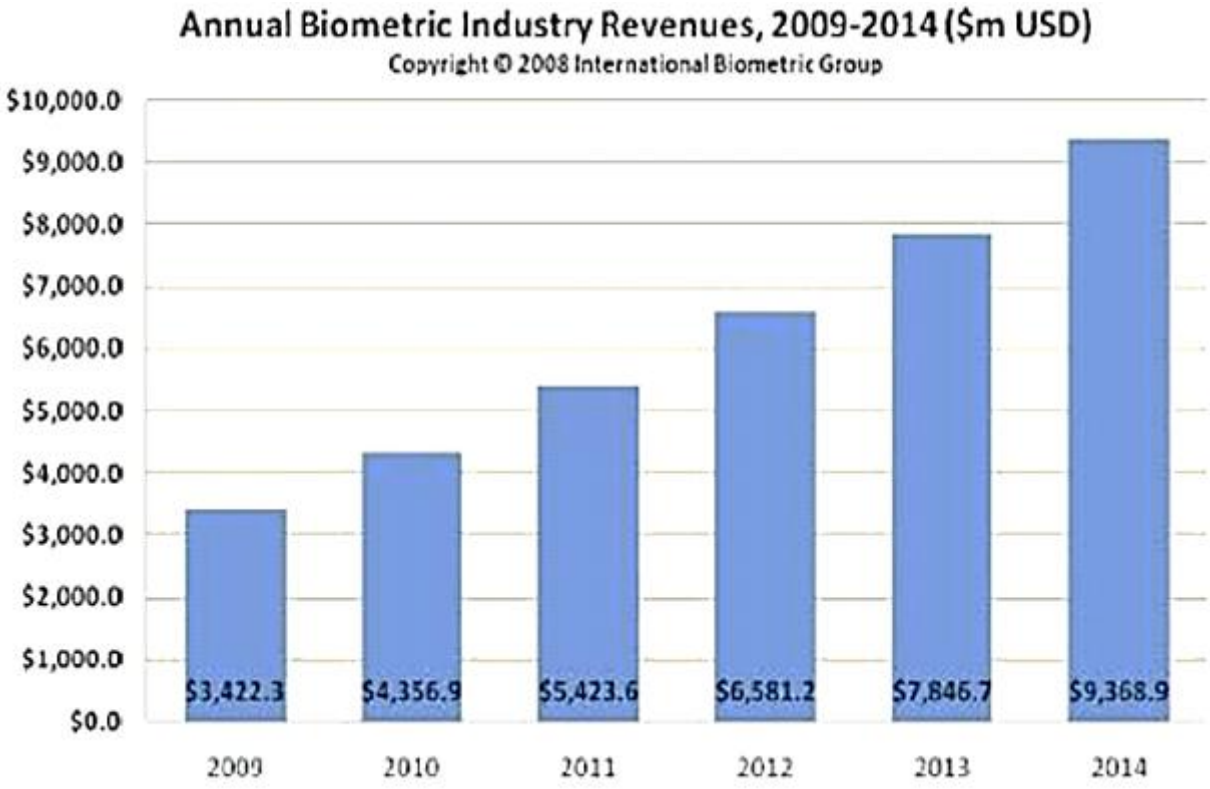


Figure I-9 : Evolution du marché international de la biométrie [7].

I.7.Conclusion

Au cours de ce premier chapitre de généralité sur les systèmes de reconnaissance biométrique, nous avons tout d'abord expliqué qu'est-ce que veut dire la biométrie et exposé comment authentifier et identifier automatiquement un individu ainsi que donné un aperçu des différentes technologies existantes. Alors que certaines d'entre elles sont employées depuis plus d'un siècle pour identifier des individus, d'autres technologies plus innovantes ne sont encore qu'à un stade purement expérimental.

Ces technologies émergentes ne seront peut-être jamais réellement développées, car jugées incompatibles avec les spécifications imposées par un marché de masse (prix, acceptabilité, et Pour conclure ce chapitre, nous soulignons l'impact potentiel de la biométrie sur la protection des renseignements personnels et la vie privée. La biométrie a été présentée comme un remède universel aux problèmes de sécurité (terrorisme, fraude, plus de mots de passe ou cartes qu'on égare, etc.) - Mais « bien que la plupart des techniques biométriques soient des outils de sécurité fort efficaces, elles ne brillent pas par leur innocuité en ce qui concerne la protection de la vie privée et des renseignements personnels ».

Chapitre II

Etat de l’art de l’empreinte digital

Dans ce chapitre, nous présentons le prétraitement de l’empreinte digitale et la détection du point centrale.

II.1. Les empreintes digitales :

Définition de l'empreinte digitale : L'empreinte digitale scientifiquement est composée des crêtes qui contiennent des pores et des sillons, et les pores permettent de sortir 80% eaux et 20% matières organiques, ces matières laissent des marques sous formes des lignes. [1]

II.2. Historique

Les premières traces d'utilisation d'empreintes digitales ont été découvertes en Egypte et datent de l'époque des pyramides il y a plus de 4000 ans. Les Chinois ont aussi utilisé très tôt ce moyen pour signer les documents officiels (le plus vieux document signé date du troisième siècle avant Jésus Christ) mais ils ne savaient sûrement pas que les empreintes étaient uniques pour chaque personne et permettaient ainsi une identification fiable. C'est en 1856 que l'anglais William Herschel [1], après avoir utilisé les empreintes en guise de signature sur la population indienne qu'il dirigeait, commença à comprendre que les empreintes étaient uniques et constantes dans le temps. En 1888 le britannique Francis Galton publia une étude sur les empreintes digitales où il établit leurs caractéristiques (unicité, empreintes fut adoptée officiellement en Angleterre dans le système judiciaire).Cette technique fut ensuite largement développée dans les enquêtes criminelles et permit de résoudre un bon nombre d'affaires. De nos jours les empreintes sont toujours largement utilisées et reconnues comme méthode d'identification fiable.[1]

II.2.1. Quelques repères chronologiques :

Dès la préhistoire, les traces d'empreintes humaines apparaissent sur des murs ou d'anciennes poteries. L'empreinte digitale est alors utilisée comme signature lors de transactions. On a retrouvé une empreinte de pouce sur une tablette à Babylone deux siècles av. J-C, en Chine, des scellés sont identifiés grâce à une empreinte digitale.

A partir de la fin du 17Eme siècle, les sciences connaissent un développement remarquable.

- 1684: le scientifique anglais Grewrédige un premier traité détaillé sur l'empreinte.

Entre 1820 et 1880, commence une période où l'on souhaite classifier les individus suivant leurs caractéristiques physiques : c'est le début de l'anthropométrie. En effet, les malfaiteurs changeant fréquemment d'état civil, cette classification est un moyen de les identifier.

On établit des mesures de crânes et de membres que l'on reporte sur des fiches signalétiques, de nombreux résultats liés à la nature des empreintes sont obtenus.

II.2.2. Quelques dates importantes :

- 1823 : Le physiologiste tchèque Purkinje classe les empreintes en neuf catégories.
- 1832 : Abolition de la marque sur les détenus, le problème de l'identification des récidivistes se pose.

-1860 : Le diplomate anglais Herschel note que « les empreintes digitales sont formées avant la naissance et restent inchangées tout au long de la vie ».

- 1870 : Le Français Alphonse Bertillon simple employé à l'origine est chargé de classer les dossiers que la préfecture établit sur des criminels notoires. Nommé ensuite chef du service photographique de la préfecture de police de Paris, il affirme qu'en prenant quatorze mensurations (taille, pied, main, nez, oreilles, etc.) sur n'importe quel individu, il n'y a qu'une seule chance sur deux cent quatre-vingt-six millions pour qu'on retrouve les mêmes chez une autre personne. Un matériel spécialisé est dès lors utilisé dans tous les établissements pénitentiaires : table, tabouret, toise, compas de proportion, tablette et encreur pour prise d'empreintes digitales. Il a donné son nom à la technique appelée « bertillonnage »

-1880 : Le médecin écossais Fauldsaffirme que les empreintes sont spécifiques à chaque individu et propose une méthode pour enregistrer les empreintes avec de l'encre d'imprimerie.

Les recherches scientifiques trouvent leur application dans le domaine de la criminalistique l'étude des empreintes digitales appelée la dactyloscopie permet de donner un caractère scientifique à la notion de preuve qui était jusqu'alors essentiellement basée sur l'aveu.

C'est un élément qui s'ajoute à l'enquête policière. La dactyloscopie s'imposera ensuite comme moyen d'identification des récidivistes.

- 1891 : le premier fichier d'empreintes est mis en place en Argentine.

-1892 : le policier argentin Vucetichest le premier à identifier une criminelle par ses empreintes digitales.

- 1892 : L'anthropologue anglais Francis Galtonétudie les empreintes digitales pendan dix ans et publie un ouvrage Finger-Prints. Il établit une classification expérimentale de plus de 2500 séries d'empreintes. Il calcule qu'il y a seulement une chance sur 64 milliards que deux individus aient la même empreinte.
- 1893 : Création du service d'identité judiciaire en France. Pour ce service, l'identité judiciaire permet de pallier les problèmes des différents alias pris par un même individu.
- 1898 : Sir Edward Richard Henrychef de la police londonienne a mis en place un système de classification des empreintes, ce système a été largement adopté et a remplacé le Bertillonnage.
- 1902: en France, Bertillonidentifie par ses empreintes digitales l'auteur d'un crime,

Sheffer. Il avait ajouté récemment ce caractère à ses fiches anthropométriques dans lesquelles apparaît le double portrait face-profil avec un étalon métrique inclus dans l'image.

-1910 : Edmond Locard, élève de Bertillon, crée le laboratoire scientifique de Lyon. à cette époque, le relevé d'empreintes des dix doigts(fiches déca dactyloscopiques) s'effectue contre quatre du temps de Bertillon.

Il élabore la Théorie de l'échange : tout malfaiteur laisse des traces sur le lieu du délit et emporte avec lui des traces de ce même lieu .

Il a rédigé Le Traité de Police Scientifique en 7 volumes. Cet ouvrage propose une méthodologie de cette nouvelle science et sert même à l'heure actuelle de base à tous les laboratoires de police scientifique du monde.

- 1937 :Etats-Unis :

A partir des années 1970: L'ensemble des fiches déca dactyloscopiques obtenues manuellement vont être informatisées, et des logiciels vont permettre le traitement informatique des empreintes et de leur reconnaissance.

- 1994 : Le Fichier Automatisé des Empreintes Digitales (F.A.E.D) est opérationnel. Il comprend les empreintes de 1 million 600 mille individus mis en cause dans des affaires pénales. Il permet d'identifier 130 individus par mois environ. Il rend le traitement et l'identification des empreintes découvertes plus rapides. Une trace relevée et lancée au FAED a une chance sur cinq d'être identifiée par le service de l'Identité Judiciaire

D'autres moyens d'identifications apparaissent : la biométrie se développe ainsi que la recherche d'ADN, l'exploitation des images issues de la vidéosurveillance, le prélèvement des odeurs sur les scènes de crimes. L'utilisation des empreintes digitales est encore à ce jour un moyen fiable et économique.

II.3. Caractéristiques des empreintes :

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

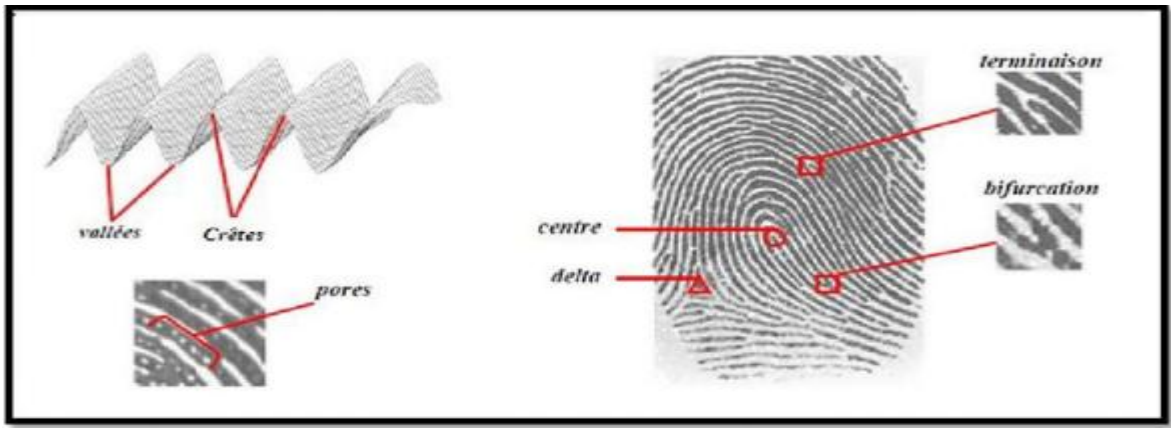
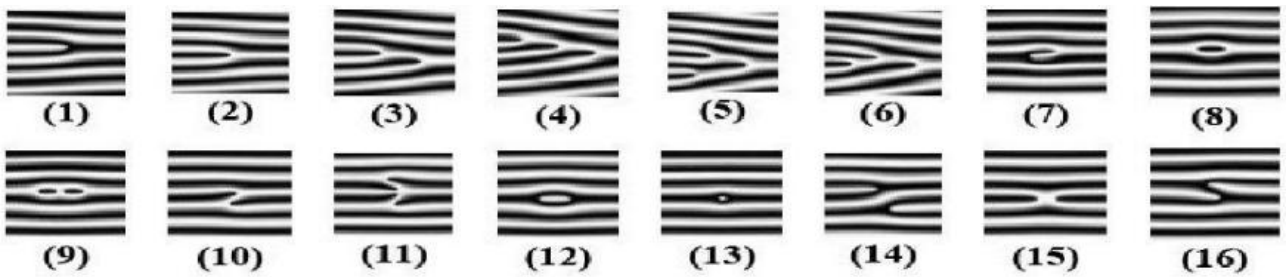


Figure II-1 : Caractéristiques d'une empreinte digitale [1]

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



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

Figure II-2 : Les différents types de minuties [2].

La position et le nombre de centres et de deltas permettent de classifier les empreintes en catégorie selon leur motif général, on distingue principalement trois grandes familles (voir Figure II-3) :
Les boucles (loop) représentent 65% des empreintes rencontrées.
Les spires (whorl) représentent 30% des empreintes rencontrées.
Les arches (arch) représentent 5% des empreintes rencontrées.

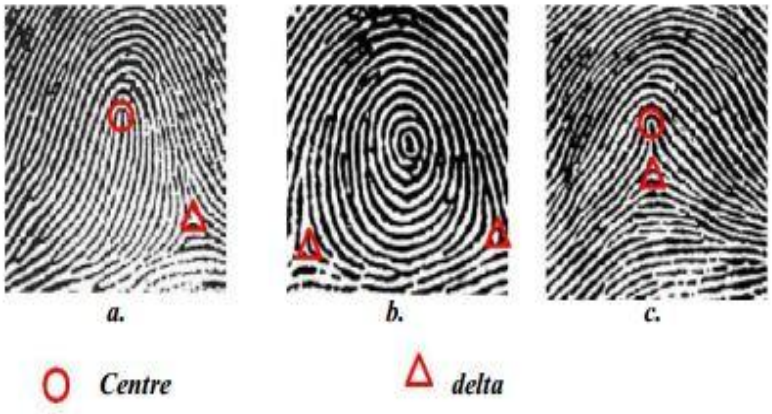


Figure II-3 : Les trois principales classes d'empreintes, boucle (a), spire (b), arche (c) [2].

L'ensemble formé par la disposition des points singuliers constitue un motif unique pour chaque individu, en effet il a été montré [2] que l'empreinte digitale se forme au cours du troisième mois de la vie vitale, le motif général est influencé par les gènes héréditaires mais l'apparition des détails (minuties) est créée de manière accidentelle par des pressions

variables aléatoires sur les surfaces tactiles. Ainsi l'empreinte est unique pour tout individu, y compris pour des vrais jumeaux et il a été montré que les méthodes de reconnaissance actuelles permettent d'identifier efficacement les jumeaux [3]. De plus les empreintes une fois formées ne changent plus au cours de la vie d'une personne, ces deux caractéristiques en font un moyen de reconnaissance très efficace.

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

II.4.1. Principe général :

Un système automatique complet de reconnaissance d'empreintes 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 et des méthodes très différentes de traitement ont été proposées [4]. Cependant ces systèmes répondent toujours à la même structure (Figure II-4).

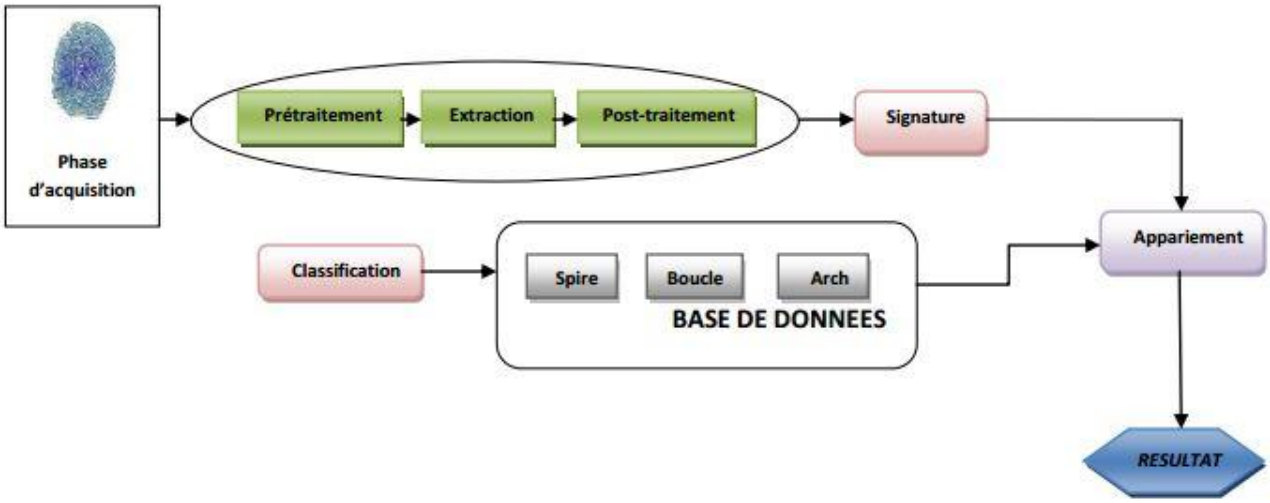


Figure II-4 : Architecture générale d'un système complet de reconnaissance d'empreintes [4]

La première phase permet d'obtenir une image de l'empreinte de l'utilisateur (acquisition), laquelle va subir un prétraitement pour extraire l'information utile de l'image (signature) suivi éventuellement d'un traitement supplémentaire permettant d'éliminer de possibles fausses informations qui se seraient glissées entre temps dans la chaîne de traitement. Ensuite si l'utilisation du système consiste juste à créer une base de données (stockage) la signature est éventuellement compressée puis stockée dans la base de données au moyen d'une technique d'archivage (classification).Pour un système d'identification, l'ensemble des empreintes présentes dans la base de données pouvant correspondre à celle de l'utilisateur (modèle identique) sont désarchivées et comparées (appariement) une à une avec celle de l'utilisateur, si une éventuelle correspondance est trouvée des informations personnelles concernant l'utilisateur sont renvoyées par le système. Dans le cas d'un système de vérification il n'y a qu'une seule

comparaison et un résultat binaire est renvoyé, permettant l'acceptation ou le rejet de l'utilisateur. [4]

II.4.2. L'acquisition de l'empreinte :

L'acquisition d'empreinte s'agit de capturer les images numériques d'empreintes qui consistent à trouver les lignes tracées par les crêtes (en contact avec le capteur) et les vallées. La qualité d'image de l'empreinte digitale peut varier selon que la peau du doigt est sale, trop humide ou trop sèche, huileuse ou affligée d'une coupure. La pression que l'on exerce sur le lecteur optique de l'appareil est aussi déterminante quant aux détails qui sont recueillis. Un bon système biométrique tiendra compte de ces facteurs. Le point commun à toutes les technologies utilisées pour la prise d'image d'une empreinte, est que l'image est constituée à partir des points de contact du doigt sur le capteur les techniques d'acquisition sont diverses on citera [5]

II.4.2.1. Les capteurs

a. Les capteurs optiques d'empreinte

La méthode optique est une des méthodes les plus communes. Un appareil-photo CCD (Dispositif Charge Couplé) est utilisé au cœur du capteur optique. Un appareil-photo CCD se compose simplement d'une rangée de diodes sensibles légères appelées photo sites. En général, le doigt est placé sur une surface en verre et l'appareil-photo CCD prend la photo. Le système CCD contient une rangée de LED qui illumine les creux et les bosses du doigt. Un prix avantageux constitue l'avantage principal des systèmes optiques ; leur inconvénient est qu'ils sont faciles à détourner.

L'autre problème est celui des empreintes latentes : l'empreinte digitale du doigt précédente, qui a été placé sur le capteur, peut rester. [5]

Figure II-5 : Les capteurs optiques d'empreinte [5]

b. Les capteurs électriques-thermique

La méthode pour reconnaître l'empreinte, consiste à faire glisser le doigt le long du capteur. Le capteur mesure la différence de température entre les creux de la peau et l'air capturé dans les bosses de l'empreinte digitale. Cette méthode donne une image d'excellente qualité même sur des empreintes de qualité médiocre telles que celles provenant de doigt sec avec peu de profondeur entre les creux et les bosses. La technologie thermique fonctionne également dans des conditions environnementales difficiles, comme lors de températures extrêmes, de taux d'humidité ou de poussière élevé, ou de contamination d'eau. Cette méthode a également l'avantage de nettoyer le capteur, évitant ainsi que les empreintes digitales restent après le passage de chaque personne. En fait, cette méthode, s'appuyant sur la technologie thermique permet au capteur d'être un des plus résistant par rapport aux autres technologies. L'inconvénient est le chauffage du capteur qui augmente la consommation électrique. [5]

Figure II-6 : Les capteurs électriques-thermique [5]

c. Capteurs capacitifs

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

L'avantage principal de ces capteurs est qu'ils demandent une réelle empreinte digitale.
Mais ils rencontrent des difficultés avec les doigts secs et humides. [5]

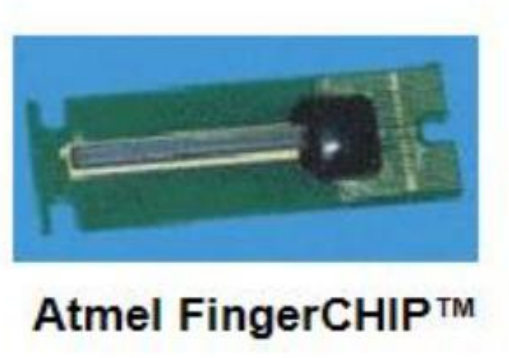


Figure II-7 : Capteurs capacitifs [5]

d. Capteurs de champ-électrique

Ce capteur fonctionne avec un champ-électrique et le mesure au-delà de la couche extérieure de la peau où l'empreinte digitale commence. Cette technologie peut être utilisée dans des conditions extrêmes, c'est-à-dire même si le doigt est sale ou sec. La technologie de champ-électrique crée un champ entre le doigt et le semi-conducteur adjacent qui imite la forme des creux et des bosses de la couche épidermique du doigt. Un amplificateur de sous Pixel est utilisé pour mesurer les signaux. Les capteurs fonctionnent ensemble afin de rendre une image plus claire correspondant exactement au modèle de l'empreinte digitale.
On parvient ainsi à une image plus claire que ce que peuvent donner les technologies optiques ou capacitives. L'inconvénient est la basse résolution d'images et une trop petite zone d'image, ce qui a pour conséquence de générer un haut taux d'erreur. [5]

DELSY CMOS-Sensor

Figure II-8 : Capteurs de champ-électrique [5]

II.4.2.2. Le prétraitement de l'empreinte digitale

a. Principe :

La méthode la plus répandue consiste à extraire les minuties à partir d'un squelette de l'image. Comme le montre la Figure II-9, l'empreinte est d'abord préparée à l'étape d'extraction au moyen d'une binarisation et d'une squelettisation, ensuite un fichier signature est extrait de l'empreinte après la détection du point central.

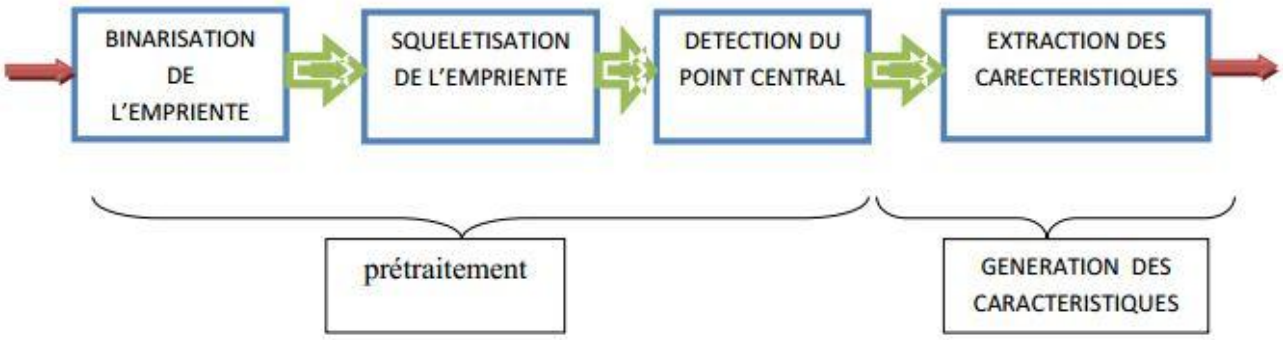


Figure II-9 : La phase d'extraction de la signature. [6]

b. La binarisation de l'image :

Pour permettre la squelettisation, l'image doit d'abord être binarisée, c'est-à-dire que l'image en 256 niveaux de gris dont nous disposons à ce stade est transformée en image binaire où les pixels noirs correspondent aux stries et les pixels blancs aux vallées. Il existe de nombreuses techniques de binarisation d'images [6], cette étape n'occupant pas une place très importante dans notre système, nous avons choisi d'utiliser une méthode de seuillage simple. Pour effectuer ce traitement la valeur de chaque pixel P (x, y) est comparée à un seuil M et si cette

valeur est supérieure au seuil le pixel prend la valeur un (blanc), sinon il prend la valeur zéro (noir).

P_1	P_2	P_3
$P_8=P_0$	p	P_4
P_7	P_6	P_5

Le seuil peut être fixé dès le départ (seuillage global). Dans ce cas l'image est divisée en N blocs et pour chaque bloc la moyenne des pixels du bloc est calculée, le bloc est ensuite binarisé en fonction de cette moyenne qui va correspondre au seuil.

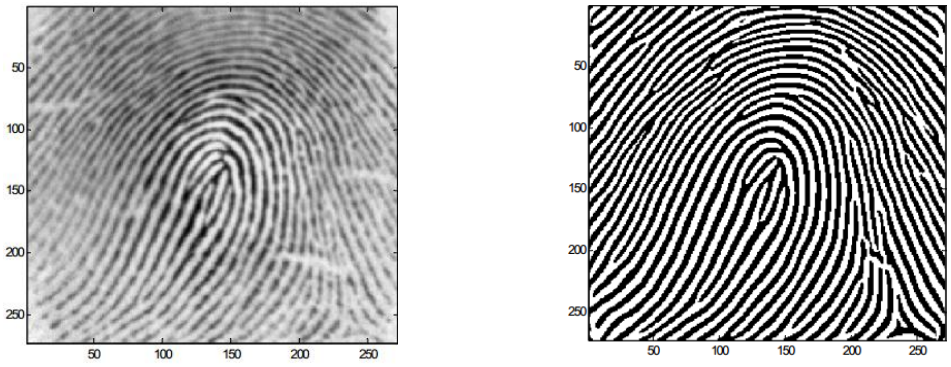


Figure II-10 : Résultats de l'étape de binarisation, base des données FVC 2002

c. Squelettisation de l'image :

Pour faciliter l'extraction des minuties l'image doit être squelettisée : une suite d'opérations morphologiques d'érosion va réduire l'épaisseur des stries jusqu'à ce que cette dernière soit égale à un pixel tout en conservant la connexité des stries (c'est-à-dire que la continuité des stries doit être respectée, il ne faut pas introduire de trous). Nous avons utilisél'algorithme de Rosenfeld [7] pour sa simplicité, mais il existe de nombreuses autres méthodes possibles [8]. Dans le cadre d'une implémentation matérielle il sera utile de revenir au choix de la méthode car les temps de calcul peuvent être diminués de façon significative en fonction de la technique utilisée [9]. Pour chaque pixel P_0on considère son voisinage immédiat $\{p_i \quad i \ \epsilon \ 1..8\}$ de 8 pixels

Pour l'algorithme de squelettisation on considère les définitions suivantes [9]

1. P_0est un point frontière Nord si P_2=0.
2. P_0est un point frontière Est si P_4=0.
3. P_0est un point frontière Sud si P_6=0.
4. P_0est un point frontière Ouest si P_8=0.

5. P_0 est un point 8-terminal si un seul de ses voisins est noir, il s'agit en fait d'une minutie de type terminaison.

6. P_0 est un point 8-isolé si aucun de ses voisins n'est noir.

7. P_0 est un point 8-simple si la connexité de ses 8 voisins n'est pas altérée quand on le transforme en pixel blanc. La squelettisation consiste à répéter les opérations d'érosion suivantes jusqu' à ce que plus aucun pixel ne soit changé:

Etape 1 : tous les pixels noirs vérifiant (1) et (7) et ne vérifiant pas (5) et (6) sont changés en pixels blancs (érosion des points frontières Nord).

Etape 2: tous les pixels noirs vérifiant (2) et (7) et ne vérifiant pas (5) et (6) sont changés en pixels blancs (érosion des points frontières Est).

Etape 3: tous les pixels noirs vérifiant (3) et (7) et ne vérifiant pas (5) et (6) sont changés en pixels blancs (érosion des points frontières Sud).

Etape 4: tous les pixels noirs vérifiant (4) et (7) et ne vérifiant pas (5) et (6) sont changés en pixels blancs (érosion des points frontières Ouest).La propriété (7) peut être ignorée dans les étapes d'érosions car bien qu'un point unique corresponde à une minutie, sa présence à ce stade du traitement est très probablement due à un résidu de bruit, il vaut donc mieux l'effacer. Il est à noter que plus l'épaisseur des stries sera importante et plus le processus sera long. La (Figure II-6) montre le résultat obtenu à partir d'une image binaire.

Image original Image squelette

Figure II-11 : Résultats de l'étape de squelettisation.

II.5. Conclusion

Une brève définition et une étude historique sur le développement de l'utilisation et le traitement de l'empreinte digitale est présenté dans le début de ce chapitre, puis nous donnons la structure d'un système de reconnaissance d'empreinte digitale et expliquons en détail la phase de prétraitement.

Dans le chapitre suivant, on donne un algorithme nous aidons à extraire les paramètres ou les points caractérisent une empreinte digitale.

Chapitre III

L’orientation de champ d’une empreinte digitale

Dans ce chapitre nous présentons l’orientation de champ d’une empreinte digitale et que cet orientation de champ est très importante pour la reconnaissance automatique de l'empreinte digitale

III.1. Introduction

Une grande variété de techniques biométriques, la reconnaissance de l'empreinte digitale est considérée comme la plus populaire et la plus fiable pour les automates. Identification personnel. Au cours des dernières années, il a reçu de plus en plus d'attention [1] -[2]. Bien que la performance de Les systèmes de reconnaissance d'empreintes digitales sont très bons pour les applications Une petite base de données, elle n'est pas satisfaisante pour les applications à grande échelle [3].

Une empreinte digitale est le motif des crêtes et des vallées à la surface du bout du doigt dans la Fig. III-1 (a), une empreinte digitale est représentée dans Cette figure, les crêtes sont noires et les vallées sont blanches. Ses Champ d'orientation, défini comme l'orientation locale des structures de ridgevalley, est représenté sur la Figure III-1 (b). Les minuties, les extrémités des arêtes et les bifurcations, et les points singuliers, sont également montrés dans la Figure III-1 (a). Les points singuliers peuvent être considérés comme des points où les le champ d'orientation est discontinu. Les empreintes digitales sont habituellement divisées en six classes principales en fonction de leurs macro-singularités, à savoir, l'arc, l'arc en tentes, la boucle gauche, la boucle droite, la boucle jumelée et Whorl (voir figure III-2).

La plupart des algorithmes classiques de reconnaissance d'empreintes digitales [1], [2], [4], [5] prennent les minuties et les points singuliers, y compris Leurs coordonnées et leur direction, en tant que caractéristiques distinctives Représentent l'empreinte digitale dans le processus d'appariement menus détails l'extraction comprend principalement les étapes ci-dessous: champ d'orientation Estimation, extraction ou amélioration de la crête, amincissement de la crête Et l'extraction des minuties. Ensuite, la fonction minutie est comparée Avec le modèle minutie ; si le score correspondant dépasse un Seuil prédéfini, ces deux empreintes digitales peuvent être considérées Comme appartenant à un même doigt. Voir la (Fig.III-3) pour l'organigramme. Des algorithmes conventionnels de reconnaissance d'empreintes digitales comme montré Ci-dessus, l'estimation du champ d'orientation est généralement une base Étape pour un système de reconnaissance complète. Donc, un algorithme pour Il est souhaitable d'estimer le champ d'orientation précis et robuste. En outre, il est également important pour la classification des empreintes digitales et correspondant [6] - [7].

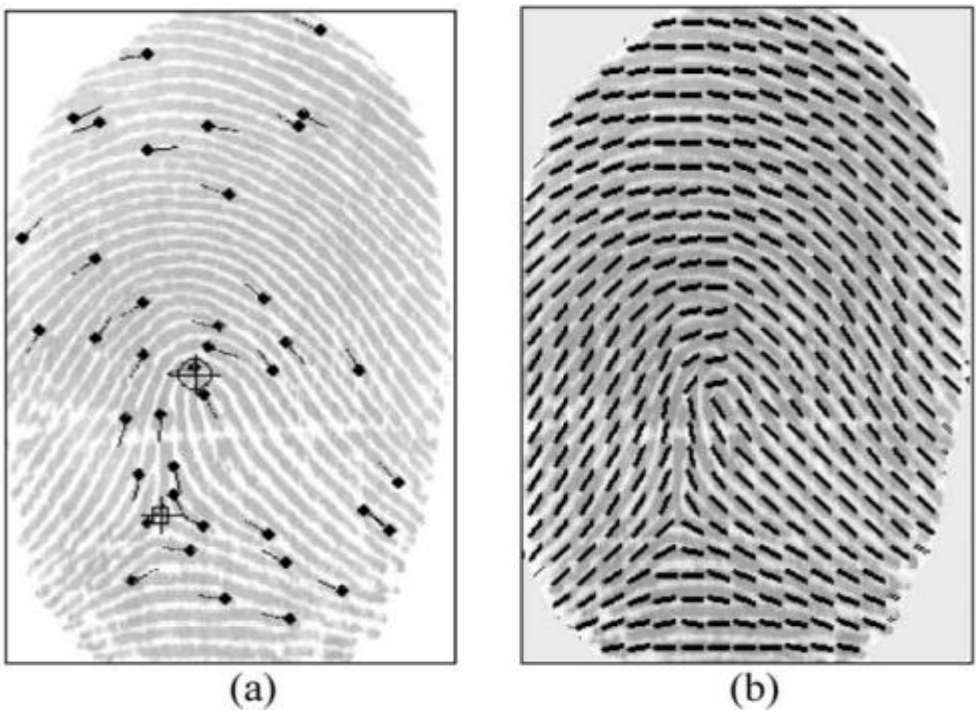


Figure III-1 : Exemple d'empreinte digitale: (a) points singuliers et minuties avec son Direction et (b) champ d'orientation montré avec vecteur unitaire. [1]

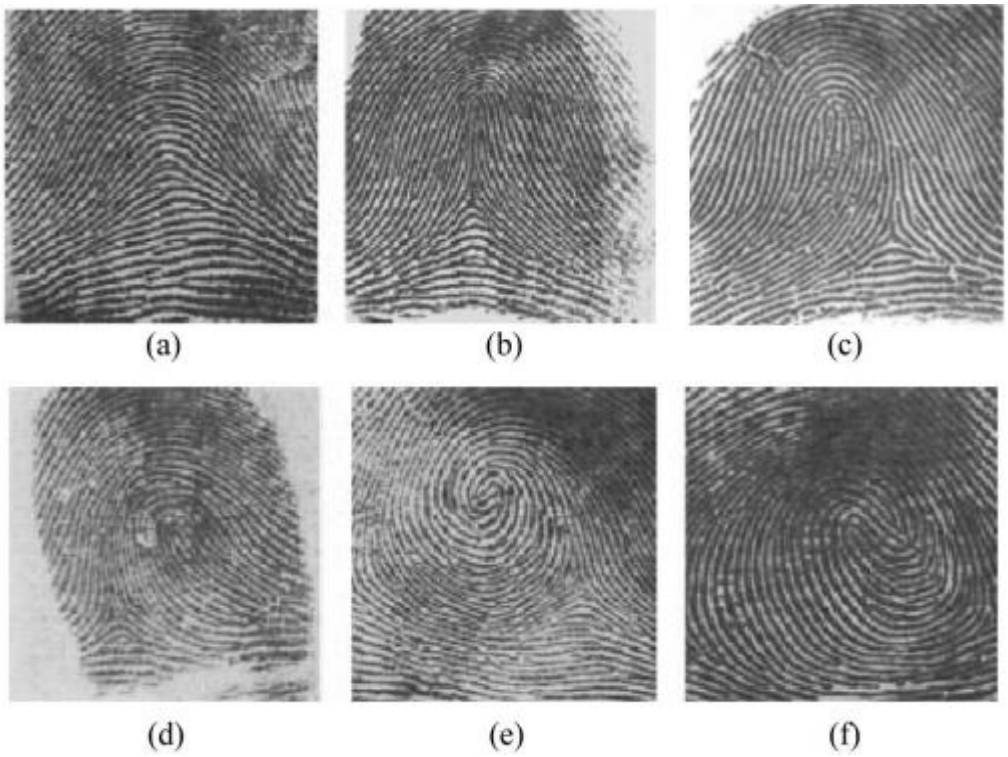


Figure III-2 : Une empreinte digitale pour chacune des six classes principales [1] (a) arc, (b) arc de tentes (boucle creuse, (d) boucle droite, (e) whorl, et (f) boucle jumelée.

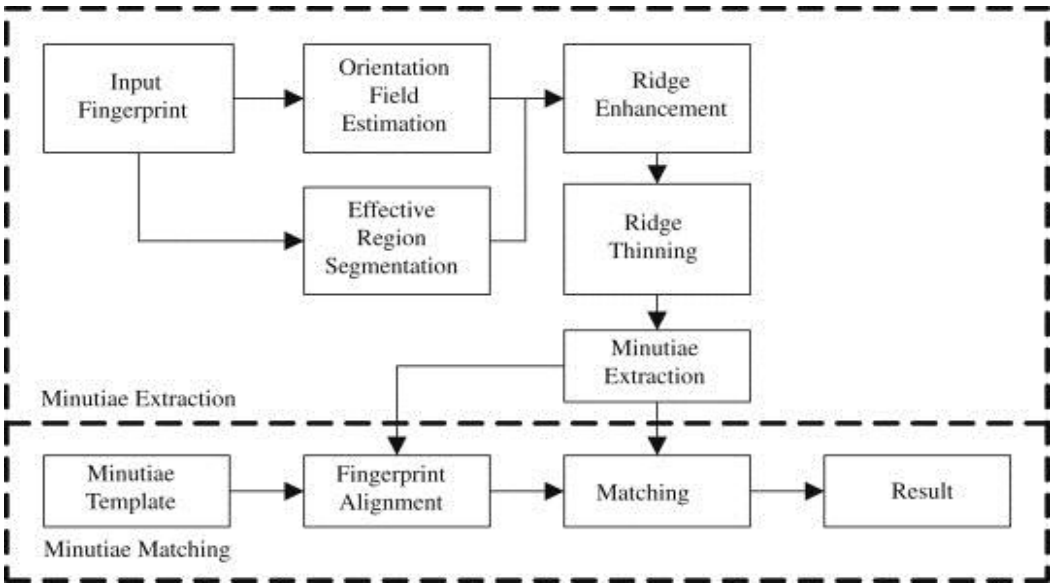


Figure III-3 : Organigramme des systèmes conventionnels de reconnaissance d'empreintes digitales.[2]

III.2. Modèle de combinaison du champ d'orientation

Sherlock et Monro [8] ont proposé un soi-disant zéro-pole Modèle de champ d'orientation basé sur des points singuliers, qui prend Le noyau comme zéro et le delta comme pôle dans le plan complexe. Le L'influence d'un noyauZc, est ½ arg (Z-Zc) pour le point Z, et que D'un delta Zd est. -1/2 arg (Z-Zd) L'orientation à est la somme De l'influence de tous les noyaux et deltas. C'est simple mais inexacte Parce que de nombreuses empreintes digitales ont les mêmes points singuliers Peut encore différer en détail. Vizcaya et GerHardt [17] avaient fait Une amélioration en utilisant un modèle d'approximation linéaire par morceaux Autour de points singuliers pour ajuster le zéro et le comportement du

Tout d'abord, le voisinage de chaque point singulier est uniformément Divisé en huit régions et l'influence du point singulier Est supposé changer linéairement dans chaque région. Une optimisation Mis en œuvre par gradient-descend est alors effectué pour obtenir Une fonction linéaire par morceaux, ces deux modèles ne peuvent pas faire face avec une empreinte digitale sans point singulier tel que l'arc simple classé par Henry [9]. En outre, comme ils ne considèrent pas La distance entre les points singuliers et l'influence d'un singulier point est le même que n'importe quel point sur la même ligne centrale, que ce soit Près ou loin du point singulier, une grave erreur

sera causée par La modélisation des régions loin des points singuliers. Par conséquent,ces deux modèles ne peuvent pas être utilisés pour une approximation précise de champ d'orientation de l'empreinte réelle.

Nous proposons ici un modèle combiné pour la matrice d'orientation. Étant donné que l'orientation des empreintes digitales est assez lisse et continue sauf dans des points singuliers, nous appliquons un polynôme modèle pour approximer le champ d'orientation global. À chaque point singulier, un modèle de charge ponctuelle similaire au modèle à pôle zéro est utilisé pour décrire la région locale. Ensuite, ces deux modèles sont combinés en douceur à travers une fonction de poids. De la Fig. III-2 (b), nous pouvons voir que le motif d'orientation d'une empreinte digitale est assez lisse et continu, sauf près du singulier points. Cela signifie que nous pouvons appliquer une fonction simple et lisse pour l'approximer globalement. Puisque la valeur de l'orientation d'une empreinte digitale est définie à [0,π] l'intérieur, il semble donc que cette représentation ait une discontinuité intrinsèque (en fait, l'orientation, 0, est identique à l'orientation π, dans le motif de la crête). Alors Nous ne pouvons pas modéliser le champ d'orientation directement. Une solution à cela Problème est de cartographier le champ d'orientation vers un complexe continu. Fonction [10], [11]. En indiquant $\theta(x,y)$ et U(x,y) en tant que champ d'orientation et la fonction transformée, respectivement, le mappage peut être défini comme

$$U=RE+i\ IM= \cos 2\theta+i\sin 2\theta \qquad \text{.....(1)}$$

Où RE et IM indiquent respectivement la partie réelle et partie imaginaire de la fonction complexe, U (x, y). Évidemment, RE (x, y) et IM (x, y) sont continus. Le mappage ci-dessus est une transformation one-to-one et θ (x, y) Peut être facilement reconstruit à partir des valeurs de et pour représenter globalement RE (x, y) et IM (x, y), deux bi variés des modèles polynomiaux sont établis, qui sont désignés par PR, respectivement RI. Ces deux polynômes peuvent être formulés comme

$$PR(x,y)= (1\ x\ \ldots\ x^n).P_1.\begin{pmatrix} 1 \\ y \\ . \\ . \\ . \\ y^n \end{pmatrix} \qquad \text{.....(2)}$$

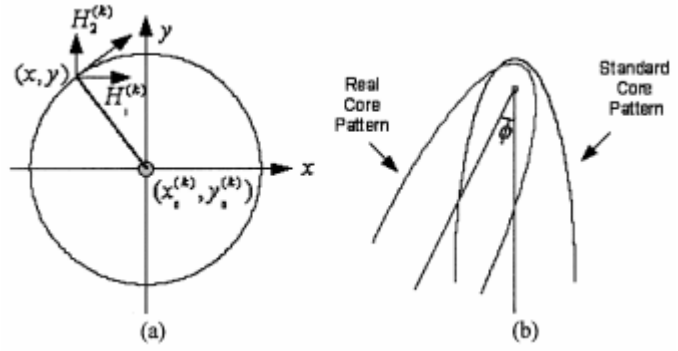


Figure III-4 : Une illumination pour le modèle de charge ponctuelle : (a) influence le vecteur autour Un noyau standard et (b) un motif de crête réelle près d'un noyau avec un angle de rotation, θ

Et :

$$PR(x,y)= (1\ x\ ...\ x^n).P_2.\begin{pmatrix} 1 \\ y \\ . \\ . \\ . \\ y^n \end{pmatrix} \quad .....(3)$$

Dans une image d'empreinte digitale réelle, le motif de crête au singulier les points peuvent avoir un angle de rotation par rapport à la norme un. Si l'angle de rotation dans le sens des aiguilles d'une montre par rapport à la position standard est ΦΦ ϵ (-π, π] Voir la figure 4 (b)), une transformation peut être faite comme

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x_0 \\ y_o \end{pmatrix} + \begin{pmatrix} cos\Phi & sin\Phi \\ -\sin\Phi & cos\Phi \end{pmatrix}.\begin{pmatrix} x - x_0 \\ y - y_0 \end{pmatrix}. \quad .....(4)$$

Ensuite, le modèle de charge de points peut être modifié en prenant x' et Y'au lieu de x et y, pour les noyaux dans (4) et les deltas dans (5), respectivement. Pour combiner le modèle polynomial, (PR, PI), avec le modèle de tartre en douceur, une fonction de poids peut être utilisée.

III.3. Estimation de champ d'orientation à base de modèle

Sur la base du modèle combiné de la section II, une nouvelle méthode De l'estimation du champ d'orientation peut être proposée. Ses étapes sont décrites ci-dessus

A. Calcul du champ d'orientation grossière :

Afin d'obtenir une représentation précise du domaine d'orientation, Nous adoptons une approche basée sur le dégradé pour le calcul de Champ d'orientation grossier dans notre travail. Il a été démontré que pour un motif d'intensité fortement orienté selon une direction, le spectre de puissance d'un tel Forme des grappes le long d'une ligne à travers l'origine dans le domaine de transformation de Fourier et la direction de la ligne est perpendiculaire À l'orientation spatiale dominante. Au lieu du calcul réel dans le domaine de transformation de Fourier, l'orientation grossière O(x, y),et W(x,y) de résistance anisotrope, peut être Calculé directement par

$$O(x,y) = \frac{1}{2}\tan^{-1}\frac{\sum_{\Gamma} 2G_X G_y}{\Sigma_{\Gamma}(G_x^2 - G_Y^2)} + \frac{\pi}{2} \qquad \text{.....(5)}$$

$$W(x, y) = \frac{\left(\Sigma_{\Gamma}(G_x^2 - G_y^2)\right) + 4\left(\Sigma_{\Gamma} G_x G_y\right)^2}{\left(\Sigma_{\Gamma}(G_x^2 + G_y^2)\right)} \qquad \text{.....(6)}$$

B. Extraction du point singulier :

Pour mettre en œuvre notre algorithme, nous devons également identifier les position et type de points singuliers. De nombreuses approches ont a été proposé pour l'extraction de points singuliers [12], [13], [10], [9], [8] - [11]. Parmi eux, les algorithmes basés sur le Poincaré l'index est utilisé populairement. En suivant un contour fermé dans le sens inverse des aiguilles d'une montre autour d'un noyau dans le champ d'orientation et en ajoutant les différences entre les angles suivants entraînent un changement cumulatif dans l'orientation π et la mise en œuvre de cette procédure autour des résultats delta dans -π. Toutefois, le changement d'orientation cumulatif sera nul lorsque la procédure est appliquée à des points non spécifiques. Basé sur les règles ci-dessus, un petit filtre bidimensionnel est développé pour extraire tous les points singuliers, y compris certains faux points singuliers causée par un champ d'orientation irrégulier [8]. Ensuite, certaines étapes sont pour vérifier le point détecté et indiquer s'il s'agit d'un noyau, un delta ou un faux point singulier.

C. Approximation par modèle :

Les deux polynômes variés peuvent être calculés en utilisant l'algorithme pondéré (WLS) pondéré [14]. Les coefficients du polynôme sont obtenus en minimisant la pondération erreur carrée entre le polynôme et les valeurs de RE (x, y) et IM (x, y) calculé à partir du champ d'orientation grossier. Comme ci-dessus, la fiabilité W (x, y), peut indiquer à quel point l'orientation correspond à la crête réelle. Plus la fiabilité est élevée, la plus grande influence que le point devrait avoir. Puis peut être W (x,y).

Utilisé dans le facteur de pondération au point, (x,y). En conséquence, il peut réduire efficacement l'influence d'une orientation inexacte estimation. Comme nous le savons, le polynôme d'ordre 4 (n=4) supérieur peut fournir un meilleur mais, en même temps, cela entraînera moins de généralisation et un coût de calcul beaucoup plus élevé. Dans notre étude, nous choisissez les polynômes à 4 ordres pour l'approximation globale. Les résultats expérimentaux ont montré qu'ils se sont bien comportés assez pour la plupart des empreintes digitales réelles, tout en préservant un petit coût pour le stockage et le calcul les coefficients du modèle de charge ponctuelle aux points singuliers peut être obtenu en deux étapes. Premièrement, deux paramètres sont estimés pour chaque point singulier : l'angle de rotationΦ, et l'efficacité Rayon, Deuxièmement, les charges de points singuliers sont estimées par optimisation. Puisque l'orientation moyenne près du point singulier peut être Déduite du résultat de l'approximation polynomiale, l'angle de rotation, qui peut être considéré comme l'angle de croisement entre la ligne verticale et l'orientation moyenne du motif de crête autour du point singulier, peut être facilement calculé. Pour les noyaux, nous peut également indiquer si c'est vers le haut ou vers le bas en faisant correspondre le noyau avec un noyau supérieur et un modèle de noyau descendant, qui sont générés à partir du modèle standard de charge ponctuelle. Pour la commodité du calcul, la valeur de R peut être définie en avance. Dans nos expériences, R est choisi comme 80 pixels pour chaque noyau indépendamment de la différence entre les images d'empreintes digitales. Quand vous faites affaire avec deltas, il est défini comme 40 pixels pour toutes les images d'empreintes digitales. Ensuite, nous devons estimer les frais pour les points singuliers. Étant donné que notre but est de minimiser l'erreur d'approximation, la fonction objective pour les points singuliers peut être représentée comme

$$\text{Min J} = \sum_{\Omega}([RE(x \cdot y) - \cos 2O]^2 + [IM(x,y) - sin2O]^2 \quad \text{.....(7)}$$

Où O est le domaine d'orientation original et Ω est efficace région pour le modèle de charge ponctuelle. Pour chaque point singulier, c'est la région efficace est un petit cercle à rayon R.Ω Est

l'union définie de tous ces petits cercles. Les variables dans l'optimisation ci-dessus problème sont les accusations de points singuliers $\{Q_1, Q_2, \ldots Q_K\}$ ils peuvent être calculés en résolvant les équations suivantes comme.

$$\frac{\partial \mathrm{j}}{\partial \mathrm{Q}} = 0, \qquad \mathrm{K} = 1,2, \ldots, \mathrm{K}. \qquad \ldots\ldots\ldots\ldots (8)$$

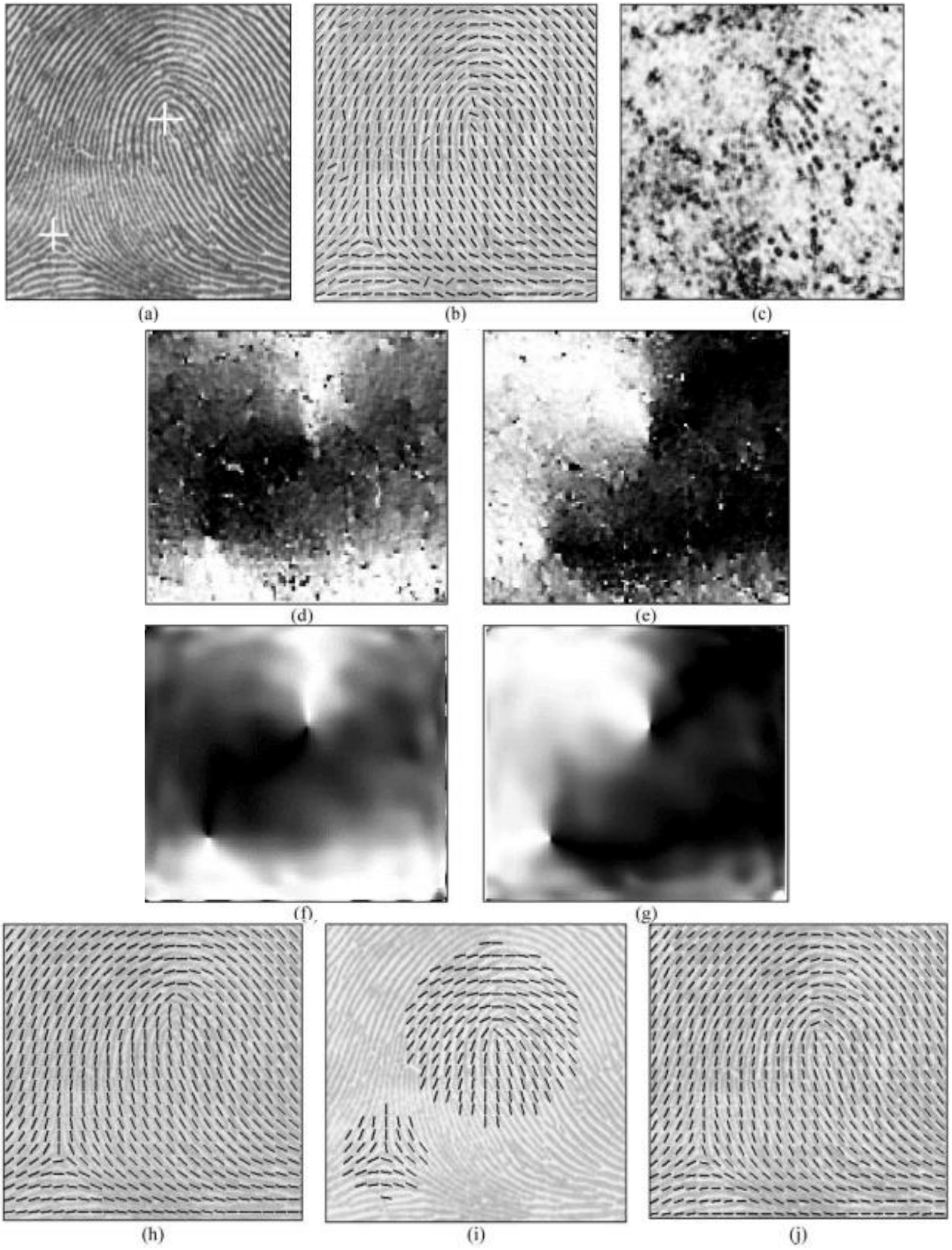


Figure III-5 : Les résultats de chaque étape de notre schéma de mise en œuvre

Fig. III-5: (a) une empreinte digitale originale avec des points singuliers marqués; (B) le champ d'orientation grossier, O; (C) la fiabilité carte W; (D) et (e) sont cos (2O) et sin (2O), c'est-à-dire les images transformées du champ d'orientation grossier, O; (F) et (g) sont les résultats d'approximation de (d) et (E), respectivement, c'est-à-dire les images transformées du champ d'orientation reconstruit; (H), (i) et (j) sont le champ d'orientation reconstruit en utilisant le polynôme modèle, modèle de charge ponctuelle et le modèle combiné, respectivement.

	1	x	X^2	X^3	X^4
1	-7.8438e-001	1.9917e-003	2.0761e-006	-3.0891e-008	6.9663e-011
Y	4.40940e-003	-6.7147e-007	-4.0080e-007	-1.0381e-010	4.9800e-012
Y^2	8.2981e-005	4.7903e-008	-1.4876e-009	-3.6954e-010	1.2433e-014
Y^3	-1.3853e-007	1.0910e-010	7.71227e-012	3.3846e-016	-8.4374e-017
Y^4	-1.1518e-009	-2.8448e-012	3.6522e-014	2.5511e-017	-4.3809e-019

Tableau III-1 : valeurs estimées de la matrice des coefficients, p1, pour la modèle polynomial (correspondant à la Figure III-5)

	1	x	X^2	X^3	X^4
1	-2.6544e-001	-6.0876e-003	4.6536e-006	5.0258e-008	-2.3940e-011
Y	49.0604e-003	-3.8196e-005	-4.8907e-007	9.4291e-010	5.7193e-012
Y^2	-4.1217e-005	-4.6452e-008	5.2624e-010	-2.6768e-013	-4.1850e-014
Y^3	-2.1019e-007	4.9850e-010	9.2636e-012	-1.8273e-016	-8.7261e-017
Y^4	3.1875e-010	2.0254e-012	-1.6866e-014	1.6578e-017	1.6555e-019

Tableau III-2 : valeurs estimées de la matrice des coefficients, p2, pour la modèle polynomial (correspondant à la Figure III-5)

(D) et (e), respectivement, c'est-à-dire les images transformées du champ d'orientation reconstruit ;(H), (i) et (j) sont les reconstitués champs d'orientation en utilisant le modèle polynomial, la charge ponctuelle le modèle et le modèle de combinaison, respectivement. Dans le tableau I et Tableau II, les valeurs estimées des matrices de coefficients, P1 et (en (2), (3)), pour le modèle polynomial sont fournis, Où l'origine des coordonnées est choisie comme image centre, l'axe est de gauche à droite

horizontalement et l'axe est de vers le bas verticalement. Les charges du point central et du delta Point sont 4.8138e-001 et 9.3928e-001, respectivement. Les angles de rotation du point central et du point delta sont -15,4 degrés et -2,4 degrés, respectivement. En comparant (h) et (j), nous pouvons Trouve que le champ d'orientation estimé en utilisant uniquement le modèle polynomial est plutôt précis, sauf pour un petit quartier du point central. Il montre que le champ d'orientation d'une empreinte digitale peut être approché globalement en utilisant uniquement le modèle polynomial, en garantissant la performance de notre modèle méthode dans les cas de points singuliers déplacés, faux ou manquants tout en traitant des images d'empreintes digitales de mauvaise qualité.

III.4 Résultats expérimentaux

Deux expériences sont menées pour tester la performance de notre algorithme. Tout d'abord, nous appliquons notre algorithme à certaines images d'empreintes digitales (base de données FCV 2002) et évaluons la précision et la robustesse de l'estimation d'orientation. La deuxième expérience est une évaluation de l'application d'Estimation l'orientation du champ en termes de reconnaissance d'empreinte digitale application.

A. Evaluation de l'estimation de l'orientation :

Cette expérience est réalisée sur 480 images d'empreintes digitales de 3 ensembles. L'ensemble 1 contient un ensemble d'échantillons de 40 empreintes roulées et incrustées de NIST Spécial Data base 14 [12] ; L'ensemble 2 comprend 320 images d'empreintes digitales à partir de la base de données d'échantillons de FVC2002 [15], Qui contient 4 sous-ensembles collectés avec différents capteurs / technologies ; L'ensemble 3 comprend 120 images d'empreintes digitales sélectionnées parmi base de données FVC 2002, qui sont capturés avec live scanners. Ces images d'empreintes digitales ont des tailles différentes et varient En différentes qualités. En eux, plus de 40% de ces images Souffrent de l'affection des grands plis, des cicatrices et des taches

Dans les crêtes ou la sécheresse et les flous des doigts. Dans la Fig. III-5, certains Les images d'empreintes digitales testées sont répertoriées. Ces empreintes digitales proviennent Différentes parties de la base de données. Parmi eux, il existe différents Types d'empreintes digitales : arc simple, arc en tentes, boucle droite, boucle gauche, Whorl, double boucle et type accidentel.

Trois algorithmes pour l'estimation du champ d'orientation sont évalués sur la base de données: l'algorithme hiérarchique à gradient [6], [7] (dans lequel le seuil de niveau de cohérence

est choisi comme (π/6), L'algorithme basé sur les banques de filtres [10] et le modèle basé sur le modèle algorithme. Dans l'approximation globale de notre algorithme, on utilise des polynômes variés à 4 ordres. Dans l'algorithme basé sur banque de filtrage Gabor, totalement 64 filtres sont utilisés pour obtenir un sortie précise.

Algorithme basé sur les banques de filtres et l'algorithme basé sur le modèle (y compris l'extraction de points singuliers). C'est-à-dire que le rapport entre le coût de calcul est d'environ 1,2 : 12,5 : 1 pour ces trois algorithmes. Par rapport aux deux autres algorithmes, en particulier pour l'algorithme basé sur la banque de filtres, l'algorithme basé sur le modèle présente un avantage évident de faible coût de calcul.

Figure III-6 : Certaines images d'empreintes digitales utilisées dans nos expériences : (a) arc simple, (b) boucle gauche, (c) boucle droite, (d) arc de tentes, (e) whorl, (f) whorl, (g) boucle jumelée et (H) classe accidentelle

III.5. Conclusion

. Dans ce chapitre on a basé sur la méthode de calcul orientation du champ et un modèle mathématique de calcule l'orientation du champ et en considérant sa douceur à l'exception de plusieurs points singuliers. Les résultats expérimentaux montrent par la modèle polynomial P1 et P2 et dans les tableaux

Chapitre IV

Résultats, Analyses et Discussions

Dans ce chapitre, nous présentons les résultats expérimentaux recueillis au cours de notre travail développé dans le cadre de la reconnaissance des empreintes digitales avec le test.

IV.1. Introduction

Ce chapitre est dédié à la présentation des résultats obtenus pour la validation de notre système. La description de la base de données utilisée est tout d'abord présentée. Puis plusieurs expériences sont menées pour l'étude de l'influence des paramètres initiaux sur les performances du système. Les résultats obtenus sont présentés dans les tableaux avec la combinaison des différentes catégories de caractéristiques.

IV.2. Amélioration des images de test

La robustesse d'un système de reconnaissance est étroitement liée à la qualité des images utilisées. Dans la plupart des cas, ces images sont sujettes au bruit, elles sont floues et peu contrastées. Ceci est dû à plusieurs facteurs comme la qualité de capteurs utilisés. C'est ainsi qu'une étape de prétraitement, qui vise à minimiser voire supprimer les imperfections et les artéfacts des images afin de les rendre exploitables par la suite est nécessaire.

IV.1.1. La base des donnée FVC

Pour la base des empreintes digitales nous avons utilisé la base FVC2002 (Fingerprint Vérification Compétition), base qui a été collectée par l'université de Bologne. Elle comporte 80 images, représentant les empreintes de 10 personnes, en faisant 8 occurrences du même doigt. Nous avons choisi la base BD_1 recueillie par un capteur capacitif à bas prix. Les images sont de taille 388 × 374 pixels et de résolution 500 DPI (Dots Per Inch ou Points Par Pouce).

IV.1.2. La normalisation Min-Max

La normalisation Min-Max est la technique de normalisation la plus simple, et la plus adaptée lorsque les bornes (valeurs minimales et valeurs maximales) des scores sont connues. Dans ce cas on translate les scores minimum et maximum respectivement vers 0 et 1. Si les scores minimum et maximum ne sont pas connus nous pouvons les estimer à partir d'un jeu D'entraînement de score donné, cependant la technique reste valable mais pas robuste (Sensible aux valeurs aberrantes dans les données utilisées pour l'estimation).

IV.3. Tests et résultats

IV.3.1. Extraction des points singuliers et apprentissage

Dans ce travaille nous avons choisi d'extraire les points où l'orientation de champ est nul (les racines (zéros) des polynômes déterminer précédemment au chapitre III, (Annexe A2)), puis prendre les coordonnées (x, y) de ces points pour calculer la distance euclidienne pour les 8 images de chaque personne à partir de l'origine de l'image (0, 0) qui est le point haut et gauche.

La distance euclidienne (Annexe C), c'est la distance classique que :

$AB=\sqrt{(X_B - X_A)^2 + (Y_B - Y_A)^2}$

Pour l'apprentissage nous utilisons une méthode classique et simple basé sur le calcul de la déférence en distance entre les points singuliers de 6 premières images de chaque personne pour déterminer un intervalle [min, max] appelé intervalle d'apprentissage où intervalle de confiance (Annexe B1) qui représente notre modèle pour les prochaines mesures ou tests.

IV.3.2. Les tests

Pour les tests nous choisissons les images 7 et 8 qui nous avons déjà calculé leur distance euclidienne et faisons la différence en distance entre les images 7 et 8 et les 6 autres images de différentes classes (8 personnes) et comparons ces différences avec notre intervalles de confiance (Annexe B2) à la fin nous calculons les paramètres suivantes :

a- Taux de reconnaissance (TR)

$$TR\ (\%) = \frac{\text{nombre d'empreint reconnus par classe}}{nombre\ totale\ des\ classes}$$

b- Taux de Fausses Acceptations (TFA, FAR : False Acceptance Rate)

$$TFA\ (\%) = \frac{nombre\ de\ fausses\ d'empreintes\ acceptées}{nombre\ totale\ des\ empreintes\ de\ test}$$

c- Taux de faux rejets (TFR, FRR : False Rejection Rate)

$$TFR\ (\%) = \frac{\text{nombre d'empreintes rejtées par classe}}{nombre\ totale\ des\ classes}$$

d- Taux d'égale erreur (TEE, EER: Equal Error Rate)

$$EER\ (\%) = \frac{FAR+FRR}{2}$$

Pers / Image	01	02	03	04	05	06	07	08
Im7-p1	**100**	100	0	0	100	100	0	0
Im7-p2	0	**100**	0	0	0.	0	0	100
Im7-p3	100	100	**100**	0	0	0	0	100
Im7-p4	100	100	0	**100**	100	100	0	100
Im7-p5	0	100	0	0	**100**	0	0	0
Im7-p6	0	0	0	0	100	**100**	0	0
Im7-p7	100	100	0	0	0	0	**100**	0
Im7-p8	0	100	0	100	100	0	0	0

Tableau IV-1 : Matrice de confusion calculée Image 7

Ce tableau représente la matrice de confusion entre ces 8 personnes comme suite :

- Les valeurs indexées en gras (diagonale) désignent le nombre (**100%**) des empreintes digitales avec une bonne acceptation (même image de même classe, personne).

- Les autres nombres qui restent désignent le pourcentage des empreintes digitales avec une fausse acceptation. Par exemple : 100% d'empreintes de l'image 7 de première (Im7-p1) personne reconnues comme deuxième personne.

TR=700% /8 = 87.5%

TFA = 1900% /64=29.6875%

TFR=100%/8=12.5%

EER= (29.6875 + 12.5) / 2 = 21.09375%

Nous remarquons que le taux de reconnaissance de notre modèle proposé basée sur la différence de distance euclidienne est très acceptable (87.5%) et même pour le taux d'erreur (21.09375) donc ce système est efficace pour le premier test.

Pers / Image	01	02	03	04	05	06	07	08
Im8-p1	**100**	100	0	100	0	0	0	0
Im8-p2	100	**100**	100	0	100	0	100	100
Im8-p3	0	100	0	0	100	100	0	100
Im8-p4	0	0	0	**100**	100	0	0	0
Im8-p5	100	100	100	0	**100**	0	0	0
Im8-p6	100	100	0	100	0	**100**	100	0
Im8-p7	0	100	0	0	0	0	0	0
Im8-p8	100	0	0	100	0	0	0	**100**

Tableau IV-2 : Matrice de confusion calculée Image 8

Ce tableau représente la matrice de confusion entre ces 8 personnes comme suite :

- Les valeurs indexées en gras (diagonale) désignent le nombre (**100%**) des empreintes digitales avec une bonne acceptation (même image de même classe, personne).

- Les autres nombres qui restent désignent le pourcentage des empreintes digitales avec une fausse acceptation. Par exemple : 100% d'empreintes de l'image 7 de première (Im7-p1) personne reconnues comme deuxième personne.

TR= 600% / 8 = 75%

TFA =2100% / 64 = 32.8125 %

TFR = 200% / 8 = 25%

EER = (32.8125 + 25) / 2 = 28.90625%

Nous remarquons que les résultats pour le deuxième test sont moins efficacité que le premier mais reste acceptable, le taux de reconnaissance est (75%) et pour le taux d'erreur (28.90625%) donc ce système reste efficace pour le deuxième test.

IV.3.2. Efficacité et rentabilité du modèle

Selon les deux tests font, on dire que le modèle de différence de la distance euclidienne est efficace pour la base de données FVC 2002, et la rentabilité de ce système est claire en ce tableau de comparaison de nos résultats avec d'autres de même base de données FVC 2002 [1] :

Méthodes	TR	TFA	TFR
Distance euclidienne	87.5	29.6875	12.5
	75	32.8125	25
HMM	99	0	23.85
	99.5	4.18	9.93
	99.9	8.91	5.15

Tableau IV-3 : comparaison des résultats

Nous remarquons que les résultats d'utilisation de HMM sont mieux que nos résultats de l'utilisation de la distance euclidienne car le HMM prend une grande capacité de calcul et plus de nombre de points d'itérations pour l'apprentissage et ça pour TR et TFA mais pour TFR sont proches pour nos tests et le premier et deuxième test de HMM.

Donc à la fin nous disons que notre système et efficace et rentable pour cette base de donnée et dans les capacités de calcule donné.

IV.4. Conclusion

Ce chapitre était consacré à l'évaluation des performances de notre système en testant plusieurs configurations des différentes caractéristiques pour assurer le meilleur taux de reconnaissance des empreintes digitales. Les résultats obtenus montrent que les taux de

reconnaissance sont très encourageants et comparables à ceux référencés dans des articles récents. Ces bonnes performances sont liées à la combinaison de test (Data Base FVC2002).

Conclusion Générale

Le travail de recherche développé dans ce mémoire contribue à l-étude d'un système pour la reconnaissance d'empreinte digitale en utilisant l'orientation de champ.

Afin d'atteindre notre objectif, il était nécessaire d'étudier dans un premier temps le fonctionnement général d'un système biométrique. L'étude des différentes technologies a mis en évidence qu'il n'existe pas, à l'heure actuelle tout au moins, une unique technique biométrique qui aborde idéalement toutes les problématiques de l'authentification d'individus.

Le second point de ce mémoire visait à discuter l'historique et les divers travaux de recherche trouvés dans la littérature concernant les systèmes de reconnaissance d'empreinte digitale.

Notre étude s'est basée sur l'extraction des points singuliers en appliquant l'algorithme de l'orientation de champ qui nous donne des bons résultats d'extraction des points de gradient nul.

Les coordonnées des points singuliers nous nous permettons de calculer les distances euclidiennes des empreintes. Le choix de la différence en distance euclidienne comme algorithme de vérification nous a donné les résultats encourageant de la base FVC 2002 discutés dans le chapitre 4.

Néanmoins, comme toute approche biométrique, la technique de vérification que nous avons proposée n'est pas parfaite car elle donne quand même des erreurs. Pour ces raisons, nos perspectives sont très ouvertes et motivantes en même temps.

Choisir autres algorithmes pour l'extraction des singuliers.

· Essayer d'utiliser autres paramètres pour la vérification,

Utilisant autre méthode pour la vérification par exemple HMM, SVM, …….

Bibliographies

Chapitre I

[1]. John D. Woodward, Jr; Christopher Horn, Julius Gatune and Aryn Thomas, «Biometrics A look at Facial Recognition», documented briefing by RAND Public Safety and Justice for the Virginia State Crime Commission, 2003.

[2]. Florent Perronnin, Jean - Luc Dugelay, « Introduction à la biométrie : Authentification des individus par traitement Audio - vidéo », Institut Eurocom, Multimedia Communications Department, Revue Traitement du signal, vol.19, N°4, 2002.

[3]. http://www.biometricgroup.com

[4]. S.Liu, M. Silveman, «A pratical guide to biometric security technology», IEEE Computer society, IT Pro - security, January - February, 2001.

[5] biometrie-online.net/technologies/empreintes-digitales

[6] http://www.memoireonline.com/03/15/8967/Conception-et-mise-en-place-dune-plateforme-de-securisation-par-synthese-et-reconnaissance-biom.html

Chapitre II

[1] 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.

[2] A.K. Jain, S. Prabhakar and S. 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.

[3] H. Ailisto and M. Linholm, "A reviex of fingerprint image enhancement methods", International Journal of Image and Graphics, Vol. 3, No. 3, pp. 401-424, 2003.

[4] N. Yager and A. Amin, "Fingerprint verification based on minutiae features: a review", Pattern Analysis and Applications, Vol. 7, No. 1, pp. 94-113, April 2004.

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

[6] M. Sezgin and B. Sankur, "Survey over image thresholding techniques and quantitative performance evaluation", Journal of Electronic Imaging, Vol. 13, pp. 146-165, January 2004.

[7] R. Stefanelli, A. Rosenfeld, "Some parallel thinning algorithms for digital pictures", Journal of the ACM, Vol.18, No2, pp.255-264, April 1971.

[8] L.Lam, S.W. Lee and C.Y. Suen, "Thinning Methodologies-A Comprehensive Survey", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 14, Issue 9, pp. 869-885, September 1992.

[9] Y.Y. Zhang and P.S.P. Wang, "Design of Parallel Thinning Algorithms", Proceedings of the 3rdInternational Workshop on Parallel Image Analysis, pp. 183-194, College Park, 1994.

[10] https://www.police-scientifique.com/empreintes-digitales/caracteristiques

[11] https://www.police-scientifique.com/empreintes-digitales/type-de-dessin-et-classification

[12] Mansukhani, P., S. Tulyakov and V. Govindaraju, 2007. Using support vector machines to eliminate false minutiae matches during fingerprint verification. Proc. SPIE Int. Soc. Optical Eng., 6539: 65390B.1-65390B.

[Nad 04] Nedjem Eddine Ayat, «Sélection de modèle automatique des machines à vecteurs de support: application à la reconnaissance d'images de chiffres manuscrits.», École de Technologie Supérieure université Du Québec, 2004, p : 45

[**Xié 04]** «Xièmes rencontres de la Société francophone de classification», Bordeaux, France, 2004.

[Oua 09] Ouamane Abdelmalik et Mehdaoui Abdelghaffar, «identification et authentification des visages en biométrie», Mémoire de Fin d'Etudes, en vue de la préparation du diplôme: INGENIEUR, Département de Génie Electrique, Université Mohamed Keider Biskra, 2009.

Chapitre III

[1] A. K. Jain, R. Bolle, and S. Pankanti, Eds., *BIOMETRICS: Personal Identification in Networked Society*. New York: Kluwer, 1999.

[2] D. Zhang, *Automated Biometrics: Technologies and Systems*. New York: Kluwer, 2000.

[3] K. Hrechak and J. A. McHugh, "Automated fingerprint recognition using structural matching," *Pattern Recognit.*, vol. 23, pp. 893–904, 1990.

[4] R. S. Germain, A. Califano, and S. Colville, "Fingerprint matching using transformation

parameter clustering," *IEEE Comput. Science Eng.*, vol. 4, no. 4, pp. 42–49, 1997.

[5] S. Pankanti, S. Prabhakar, and A. K. Jain, "On the individuality of fingerprints," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 24, no. 8, pp.
1010–1025, 2002.

[6] A. Jain and L. Hong, "On-line fingerprint verification," *IEEE Trans.Pattern Anal. Machine Intell.*, vol. 19, no. 4, pp. 302–314, 1997.

[7] A. Jain, L. Hong, S. Pankanti, and R. Bolle, "Identity authentication using fingerprints," *Proc. IEEE,* vol. 85, no. 9, pp. 1365–1388, 1997.

[8] A. M. Bazen and S. H. Gerez, "Systematic methods for the computation of the directional fields and singular points of fingerprints," *IEEE Trans Pattern Anal. Machine Intell.*, vol. 24, no. 7, pp.
905–919, 2002.

[9] A. K. Jain, S. Prabhakar, and L. Hong et al., "Filterbank-based fingerprint matching," *IEEE Trans. Image Processing*, vol. 9, no. 5, pp. 846–859, 2000.

[10] A. Jain, S. Prabhakar, and L. Hong, "A multichannel approach to fingerprint classification," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 21, no. 4, pp. 348–359, 1999.

[11] K. Karu and A. K. Jain, "Fingerprint classification," *Pattern Recognit.*, vol. 17, no. 3, pp. 389–404, 1996.

[12] L. O'gorman and J. V. Nickerson, "An approach to fingerprint filter design," *Pattern Recognit.*, vol. 22, no. 1, pp. 29–38, 1989.

[13] P. Whittle, *Prediction and Regulation by Linear Least-Square Methods*. London, U.K.: The English Universities Press Ltd, 1963

[14] **NIST Special Database** 14: NIST Mated Fingerprint Card Pairs (MFCP2)http://www.nist.gov/srd/nistsd14.htm [Online]

[15] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2000: Fingerprint verification competition," IEEE Trans. Pattern Anal. Machine Intell., vol. 24, no. 3, pp. 402–412, 2002.

Chapitre IV

Bibliographies

[1] . HAO GUO, "A HIDDEN MARKOV MODEL FINGERPRINT MATCHING APPROACH", Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, 18-21 August 2005

.

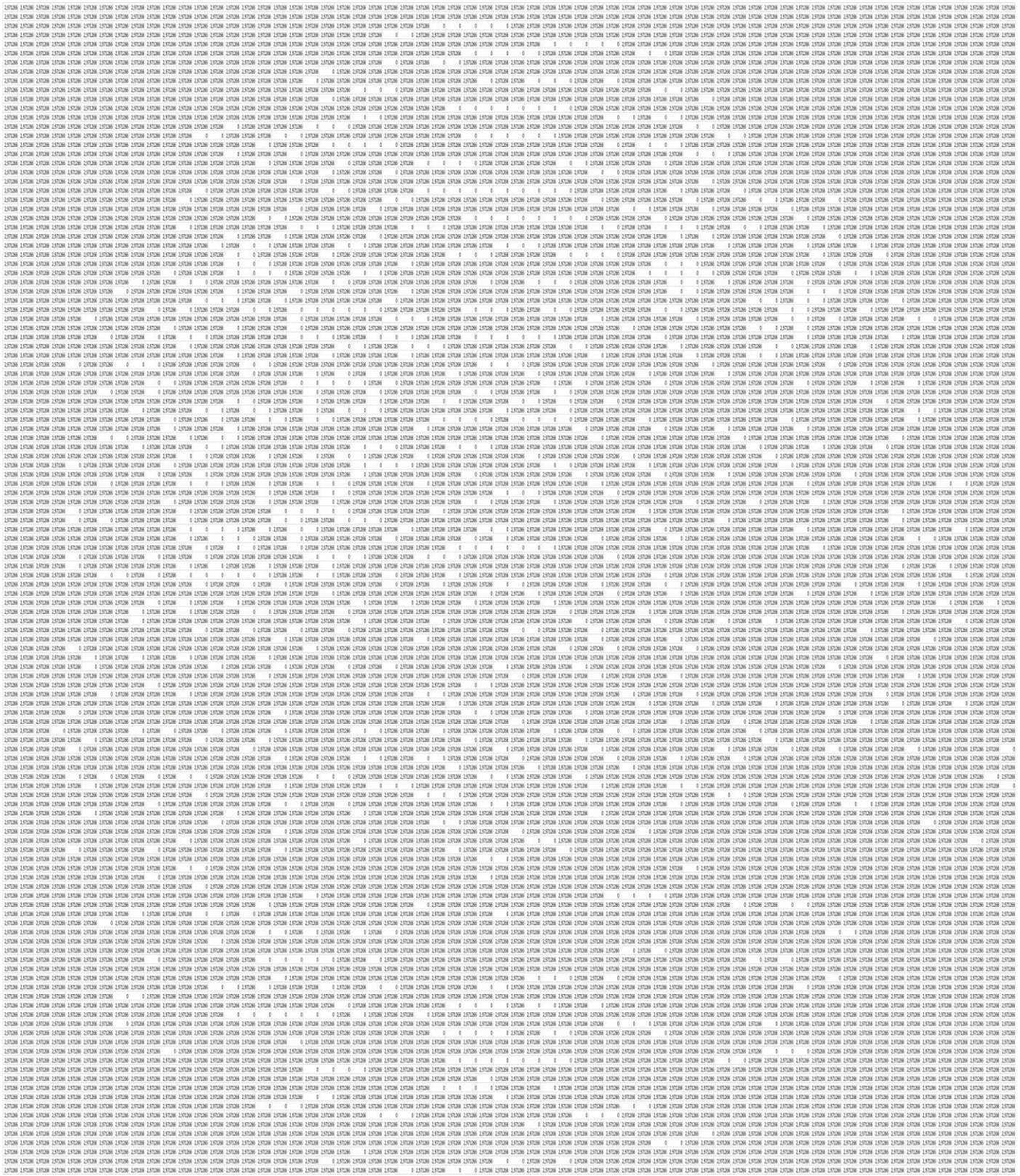
ANNEXE

ANNEXE A1

Image 101_7 après Squelettisation

ANNEXE

ANNEX A2



L’extraction des points singulier à partir de l’image 101_7

ANNEXE

ANNEXE B1

0,537689471	24,9749934
2,050827956	27,54564652
4,420491379	40,46274722
1,427816873	31,43562168
2,496751231	34,99973067
0,116095285	41,64997516
2,298194319	39,72791854
1,062769717	28,68476853
2,928250358	20,22214307
2,981870786	20,15339359
0,877473738	20,08112899
0,327063806	20,00579978
1,332635272	19,59656905
1,385904919	24,94810495
0,747839293	28,36084322
0,298256097	40,12366509
0,629170796	36,65390413
0,302380272	36,05830446
0,051609517	16,560371
0,194100374	16,59083786
0,434680385	14,21067369
0,276100668	11,31597945
0,038468655	23,47162505
0,784928889	23,68360457
1,562318575	27,9565359
0,821776093	17,01223211
1,413760507	16,54462139
3,512103673	41,73251934
3,780433201	41,47794474
3,559068856	30,12083352
2,147235644	24,29991878
0,960640609	23,89821729
0,884577417	34,56935661
1,403556211	32,12382294
0,182006692	20,33937928

Matrice Min et Max pour la 1ère personne

ANNEXE B2

14,56347739	7,774603438	5,470331292	11,76626338	52,11574643	17,08476299
12,68104777	9,639282928	3,680064399	10,03322038	53,83270655	15,34731139
11,95950304	10,33788164	3,05363315	9,46282937	51,91448952	11,20374226
8,723457867	10,47419705	2,987164063	9,451142477	50,10672722	9,955761823
8,476058416	10,74281162	2,701887104	9,219316586	49,72041413	8,795520059
4,368048188	29,67914833	2,284588589	9,603687534	49,76936186	9,075801105
1,464111147	26,81057978	1,770430444	9,053564494	49,7062717	8,93956558
18,30352372	9,084426007	14,84912401	0,455074046	35,99977661	17,35083613
13,92393682	13,40293438	10,14516967	0,430239003	39,6007302	14,57544263
9,986517346	15,01552001	5,881562919	3,266724834	43,72547757	10,07840555
9,697833595	14,45475997	18,2712659	6,290256047	43,2985323	10,71367387
9,417632729	13,98768805	12,92350087	6,087361748	43,80028938	8,253589307
4,671390149	6,006173075	22,15402865	28,12725588	27,48143954	12,95947056
10,73845986	3,637581846	19,73111249	26,42061687	25,7361073	10,52802763
7,960037417	3,162251942	11,56980201	19,83522656	33,051407	3,345698514
6,376190704	5,073702553	10,23886521	17,87187833	35,14675917	1,379572518
6,266675481	7,334619138	12,10303106	10,14980818	40,85977036	0,297708619
6,107992838	8,561868152	10,33135819	5,734552466	46,77499657	3,638371778
5,505388394	9,524921084	10,82659541	0,384564768	43,98356437	4,284151918
4,698085747	10,22327613	11,522462	1,102778987	44,50448179	5,469737862
6,35605837	34,05832052	3,405804339	2,763030355	45,81716471	6,639027396
31,74313988	1,938877044	1,39117603	27,09680435	21,7224017	10,5708702
29,2834608	2,3936661	0,692404597	26,49306703	23,45506275	11,58621384
26,90622262	0,114703714	0,120745155	24,18530814	30,06745967	11,07413822
12,1266923	14,3174221	14,04373271	11,10840752	44,57610068	3,356867784
12,91465241	15,45592115	9,733715495	10,43845548	40,31111404	3,972579261
7,375519542	15,31756071	10,14432129	10,87053514	45,5400886	27,97455762
8,101038853	12,77008508	11,65175614	8,896430299	46,71537411	27,43721753
13,40521799	8,218508639	9,768141095	5,604000544	25,59549498	5,966339841
14,51100553	3,708630895	5,693663392	3,847275775	26,06361263	1,216689003
16,97316915	1,342763481	3,767159538	8,122532836	35,53238894	4,584120999
19,35246838	1,265172496	1,390296649	5,811243722	35,35584909	2,997433827
10,44008931	31,69417574	7,265054162	1,877725382	43,39450167	5,98481292
10,9377222	32,01045923	7,670631271	3,948893097	44,07705635	5,463632158
9,041138634	30,38662983	9,206885776	3,213896546	45,8890583	30,20749872

Matrice image (7) personne 1

ANNEXE

ANNEX C

33,13608305	43,26661531
34,13209633	54,56189146
37,12142239	52,32590181
30,2654919	58,05170109
35,22782991	52,49761899
29,73213749	48,54894438
31,6227766	67,62396025
28,23118843	53,60037313
31,01612484	56,72741841
39,56008089	57,38466694
35,11409973	47,5394573
21,40093456	51,623638
40,16217126	52,15361924
41,10960958	60,8276253
42,05948169	56,40035461
29,15475947	57,00877125
33,54101966	57,62811814
27,01851217	63,63961031
37,12142239	54,3783045
39,81205847	60,46486583
41,34005322	61,03277808
55,4616985	61,6116872
57,69748695	56,36488268
42,44997055	62,68173578
43,18564576	68,60029154
48,27007354	69,20260111
49,04079934	59,48108943
40	67,41661516
44,55333882	60,20797289
62,76941931	61,40032573
66,24198065	61,98386887
43,93176527	62,64183905
51,85556865	63,2455532
52,63078947	77,82673063
53,41348144	120,5072612
51,73973328	

La distance euclidienne de l'image 101_7, personne 1

ANNEXE