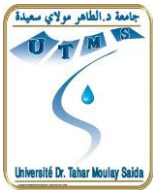
الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي و البحث العلمي
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université Dr. Tahar Moulay SAIDA — جامعة د الطاهر مولاي سعيدة

Faculté : Technologie — كلية التكنولوجيا

Département : Informatique — قسم : الإعلام الآلي



MEMOIRE DE MASTER

Option : Sécurité Informatique et Cryptographie

THEME

Conception d'un Système d'Identification Biométrique

<<< Empreintes digitales >>>

Présenté par :

AKKAL BRAHIM
DAHOUNI MOUSSA

Encadré par :

Mme : Meddah

A U : 2015 /2016

Remerciement

Merci Allah de nous avoir donné la capacité d'écrire et de réfléchir, et l'espoir nécessaire Pour accomplir ce travail et surmonter l'ensemble des difficultés.

Nous tenons à remercier vivement notre encadreur Mme Meddah pour ses conseils, sa disponibilité et son encouragement qui nous ont permis de réaliser ce travail dans les meilleures conditions.

Nous remercions également les membres de jury de nous faire l'honneur de juger notre travail.

Nous remercions profondément toutes les personnes qui ont contribuées à l'élaboration de ce travail.

Finalement, nous remercions nos grandes familles, nos amies, nos collègues de l'université Dr Moulay Tahar SAIDA

Et toute la promotion 2016 de l'informatique

Dédicace

A

Nos parents

Pour les sacrifices déployés à notre égards ; pour leur patience

Leur amour et leur confiance en nous.

Ils ont tout fait pour notre bonheur et notre réussite.

Qu'ils trouvent dans ce modeste travail, le témoignage de notre profonde affection et de notre attachement indéfectible.

Nulle dédicace ne puisse exprimer ce que nous leur devons

Que dieu leur réserve la bonne santé et une longue vie.

A

Nos amis

En témoignage de nos sincères reconnaissances pour les efforts qu'ils ont consentis pour nous soutenir au cours de nos études.

Que dieu nous garde toujours unis

A

Toute personne qui nous a aidé à réaliser notre projet.

Table des matières

Chapitre III : L'empreinte Digitale

Chapitre IV : Implémentation

Introduction générale

De nos jours, Le besoin d'accès sécurisés à des environnements physiques ou virtuels, notamment pour des services personnalisés est en pleine croissance. Ces besoins requièrent des moyens fiables pour vérifier l'identité d'une personne qui se présente au système d'accès. Or les moyens classiques reposants sur des mots de passe ou des cartes magnétiques associées à un code personnel présentent un certain nombre d'inconvénients. Un mot de passe peut être oublié ou volé par un autre individu, ou même cédé à quelqu'un d'autre ; les cartes d'accès peuvent également être perdues ou volées.

Par conséquent, il devient de plus en plus évident que ces mécanismes ne sont pas suffisants pour déterminer d'une manière fiable l'identité d'une personne et qu'un mécanisme plus solide basé sur quelque chose que vous êtes, à savoir la biométrie, est plus que nécessaire.

La biométrie est donc une alternative aux anciens modes d'identification. Elle consiste à identifier une personne à partir de ses caractéristiques physiques ou comportementales.

Le visage, les empreintes digitales, l'iris, etc… sont des exemples de caractéristiques physiques et comportementales.

C'est dans ce contexte que notre projet de mémoire est défini afin de réaliser un système d'identification par empreintes digitales

Dans le cadre de ce travail, notre mémoire est structuré de la manière suivante:

- Une introduction générale définie ci-dessus.
- Un premier chapitre dans lequel on définit le concept de sécurité et ces protocoles. .
- Le deuxième chapitre présente une élude générale sur la biométrie.
- Le troisième chapitre présente une élude théorique au niveau de la reconnaissance des empreintes digitales.
- Le quatrième chapitre explique notre conception et la façon dont elle est implémentée.
- On termine par une conclusion générale.

Chapitre I : Les protocoles de sécurité

1. introduction :

Les exigences de la sécurité de l'information au sein des organisations ont conduit à deux changements majeurs au cours des dernières décennies. Avant l'usage généralisé d'équipements informatiques, la sécurité de l'information était assurée par des moyens physiques (classeurs fermés par un cadenas) ou administratifs (examen systématique des candidats au cours de leur recrutement). Avec l'introduction de l'ordinateur, le besoin d'outils automatisés pour protéger fichiers et autres informations stockées est devenu évident. Ce besoin est accentué pour un système accessible via un téléphone public ou un réseau de données. On donne à cette collection d'outils conçus pour protéger des données et contrecarrer les pirates le nom de sécurité informatique

Le second changement majeur qui affecte la sécurité est l'introduction de systèmes distribués et l'utilisation de réseaux et dispositifs de communication pour transporter des données entre un terminal utilisateur et un ordinateur, et entre ordinateurs. Les mesures de sécurité des réseaux sont nécessaires pour protéger les données durant leur transmission. On parle alors de sécurité des réseaux.

Les menaces engendrent des risques et coûts humains et financiers : perte de confidentialité de données sensibles, indisponibilité des infrastructures et des données, dommages pour le patrimoine intellectuel. Les risques peuvent se réaliser si les systèmes menacés présentent des vulnérabilités.

La sécurité des systèmes d'information a été radicalement bouleversée par l'évolution rapide de l'Internet, elle ne saurait s'y réduire ; il s'agit d'un vaste problème dont les aspects techniques ne sont qu'une partie. Les aspects juridiques, sociaux, ergonomiques, psychologiques et organisationnels sont aussi importants, sans oublier les aspects immobiliers.

Aspects techniques de la sécurité :

Les problèmes techniques actuels de sécurité informatique peuvent provisoirement être classés en deux grandes catégories :

- ✓ Ceux qui concernent la sécurité de l'ordinateur proprement dit, serveur ou poste de travail, de son système d'exploitation et des données qu'il abrite.

- ✓ Ceux qui découlent directement ou indirectement de l'essor des réseaux, qui multiplie la quantité et la gravité des menaces.

Si les problèmes de la première catégorie citée existent depuis la naissance de l'informatique, il est clair que l'essor des réseaux, puis de l'Internet, multiplié l'impact potentiel en permettant leur combinaison avec ceux de la seconde catégorie.[1]

2. Définition des risques et des objets à protéger :

2.1. Périmètre de sécurité:

Il est inutile de se préoccuper de sécurité si on ne défini pas ce qui est à protéger : en d'autres termes toute organisation désireuse de protéger ses systèmes et ses réseaux doit déterminer son *périmètre de sécurité*.

Le périmètre de sécurité, au sein de l'univers physique, délimite l'intérieur et l'extérieur, mais sa définition doit aussi englober (ou pas) les entités immatérielles qui peuplent les ordinateurs et les réseaux, essentiellement les logiciels et en particulier les systèmes d'exploitation.

Il faut aussi élaborer une politique de sécurité, c'est à- dire décider de ce qui est autorisé et de ce qui est interdit. À cette politique viennent bien sûr s'ajouter les lois et les règlements en vigueur, qui s'imposent à tous. il sera possible de mettre en place les solutions techniques appropriées à la défense du périmètre selon la politique choisie. Mais les dispositifs techniques ne pourront pas résoudre tous les problèmes de sécurité. [1]

2.2. Périmètre et frontière:

Le périmètre de sécurité devient de plus en plus fragile au fur et à mesure que les frontières entre l'extérieur et l'intérieur de l'entreprise ainsi qu'entre les pays deviennent plus floues et plus poreuses. les ordinateurs portables entrent et sortent des locaux et des réseaux internes pour aller se faire contaminer à l'extérieur aussi les lois et les règles peuvent s'appliquer à un serveur hébergé aux États- Unis, qui appartient à une entreprise française et qui sert des clients brésiliens et canadiens. [1]

Exemple:

Un certain nombre d'organisations ont déposé devant les tribunaux français des plaintes destinées à faire cesser la propagation de pages Web à contenus négationnistes, effectivement attaquables en droit français. Mais les sites négationnistes étaient installés aux États-Unis, pays dépourvu d'une législation anti négationniste, ce qui interdisait tout recours contre les auteurs et les éditeurs des pages en question. Les plaignants se sont donc retournés contre les FAI français, par l'intermédiaire desquels les internautes pouvaient accéder aux pages délictueuses.

Ressources publiques, ressources privées

Les systèmes et les réseaux comportent des données et des programmes que nous considérerons comme des *ressources*. Certaines ressources sont d'accès public, comme certains serveurs Web, d'autres sont privées pour une personne, comme une boîte à lettres électronique, d'autres sont privées pour un groupe de personnes, comme l'annuaire téléphonique interne d'une entreprise.

Ce caractère plus ou moins public d'une ressource doit être traduit dans le système sous forme de *droits d'accès*.[1]

3. Identification et authentification :

Les personnes qui accèdent à une ressource non publique doivent être *identifiées* ; leur identité doit être *authentifiée* ; leurs droits d'accès doivent être *vérifiés* au regard des *habilitations* qui leur ont été attribuées.
à ces trois actions correspond l'un domaine des techniques de sécurité.

3.1 L'authentification :

Est la vérification d'informations relatives à une personne ou à un processus informatique. L'authentification complète le processus d'identification dans le sens où l'authentification permet de prouver une identité déclarée.

Dans un serveur, un processus de contrôle valide l'identité et après authentification, donne l'accès aux données, applications, bases de données, fichiers ou sites Internet, dans le cas contraire, l'accès est refusé.

L'authentification peut se faire de multiples manières, et notamment par la vérification de:

- ✓ « Ce que je sais », un mot de passe par exemple,
- ✓ « Ce que je sais faire », une signature manuscrite sur écran tactile/digital (de type PDA),
- ✓ « Ce que je suis », une caractéristique physique comme une empreinte digitale,
- ✓ « Ce que je possède », une carte à puce par exemple.

Le choix de telle ou telle technique dépend en grande partie de l'usage que l'on souhaite en faire : authentification de l'expéditeur d'un email, authentification d'un utilisateur qui se connecte à distance, authentification d'un administrateur au système, authentification des parties lors d'une transaction de B2B (Business to Business), etc.

La combinaison de plusieurs de ces méthodes (aussi appelées facteurs d'authentification) permet de renforcer le processus d'authentification, on parle alors d'authentification forte.

Les techniques d'authentification les plus utilisées sont les mots de passe, les Certificats de clés publiques. [2]

4. Protocoles d'authentification couramment utilisés :

4.1 Protocole RADIUS :

Le protocole RADIUS (Remote Authentication Dial-In User Service) développé par Livingston Enterprise et standardisé par l'IETF (cf. RFC 2865 et 2866) s'appuie sur une architecture client/serveur et permet de fournir des services d'authentification, d'autorisation et de gestion des comptes lors d'accès à distance. [2]

4.2 Protocole SSL :

Le protocole SSL (Secure Socket Layer) développé par Netscape Communications Corp. avec RSA Data Security Inc. permet théoriquement de sécuriser

tout protocole applicatif s'appuyant sur TCP/IP i.e. HTTP, FTP, LDAP, SNMP, Telnet, etc. mais en pratique ses implémentations les plus répandues sont LDAPS et HTTPS.

Le protocole SSL permet non seulement de fournir les services d'authentification du serveur, d'authentification du client (par certificat à partir de SSL version 3) mais également les services de confidentialité et d'intégrité.[2]

4.3 Le protocole TLS:

Version 1.0 (Transport Security Layer) est la version normalisée de SSL version 3.0 (cf. RFC 2246 de l'IETF). Les versions de TLS sont amenées à évoluer, au moins au fur et à mesure que de nouvelles attaques apparaissent. En Février dernier, une faiblesse majeure a été identifiée dans le protocole SSL : des chercheurs de l'Ecole Polytechnique de Lausanne ont montré qu'il est possible en moins d'une heure de trouver le mot de passe d'un internaute connecté à un service d'eCommerce. Que l'URL (Uniform Resource Locator) soit « sûre » ou pas, c'est-à-dire qu'une société dont la réputation n'est plus à faire héberge ce site Internet ou bien qu'il s'agisse d'une compagnie dont la sécurité des transactions n'est pas une priorité, la faille de sécurité basée sur une usurpation d'identité était bien présente pour les plates-formes Linux, Unix, Solaris et dérivés. L'information a été rapidement transmise à l'organisation OpenSSL afin de mettre à jour le protocole et développer une nouvelle Version de SSL qui résiste à cette attaque (cf. le site www.openssl.org pour les différentes mises à jour). [2]

4.4 Protocole WTLS :

Le protocole WTLS (Wireless Transport Layer Security) est la transposition du protocole TLS dans le monde des réseaux sans fil. Cependant, les négociations entre le client et le serveur ont été adaptées afin derépondre aux contraintes du réseau «wireless ».

Dans les entreprises, les certificats de clés publiques sont stockés dans des annuaires LDAP (*Lightweight Directory Access Protocol)*. Pour un usage personnel de MAC ou autres applications utilisant la cryptographie asymétrique, les certificats des utilisateurs ainsi que leur AC sont souvent stockés dans les Navigateurs (Microsoft Internet Explorer et Netscape Communicator). Ceux-ci comportent déjà par défaut un certain nombre de certificats d'AC racines (cf. Outils/Options internet/Contenu/Certificats).[2]

5. Méthodes courantes d'authentification :

5.1 Mots de passe :

Les mots de passe pris dans leur ensemble sont le moyen d'authentification le plus répandu à ce jour. On distingue deux catégories : les mots de passe statiques et les mots de passe Dynamiques.

Les mots de passe statiques sont des mots de passe qui restent identiques pour plusieurs connexions sur un même compte. Ce type de mot de passe est couramment rencontré sous Windows NT ou Unix. Cette technique d'authentification est la plus utilisée dans les entreprises mais aussi la moins robuste. En fait, les Entreprises devraient restreindre l'usage des mots de passe statiques à une authentification locale d'un utilisateur car les attaques qui permettent de capturer un mot de passe qui circule sur un réseau sont nombreuses et faciles à mettre en pratique.

Pour palier les faiblesses de l'usage des mots de passe statiques, sont apparues des solutions d'authentification combinant deux facteurs « ce que je possède » et « ce que je sais » afin d'obtenir une authentification Forte.

Les mots de passe sont obtenus par des Générateurs de mots de passe activés à l'aide d'un code d'identification personnel ou PIN (*Personal Identification Number*).

La mise en place d'un tel mécanisme d'authentification forte rend la capture du mot de passe en cours d'aucune utilité puisque, dès que le mot de passe dynamique a été utilisé, celui-ci devient caduc.

Parmi ces mots de passe à usage unique – One Time Password (OTP)– on trouve notamment le programme SKEY dont la sécurité repose sur une fonction à sens unique et qui permet de générer un mot de passe différent pour chaque nouvelle connexion. En version logicielle, ces générateurs de mots de passe dynamiques utilisent certains composants du PC, comme le microprocesseur, le CPU ou l'Horloge interne (on parle alors de méthode d'authentification en mode synchrone dépendant du temps). Que le mot de passe à usage unique soit obtenu à partir d'un générateur matériel ou logiciel,

l'utilisateur est authentifié de manière forte grâce à la vérification du mot de passe dynamique par un serveur appelé serveur d'authentification.

Afin d'éviter aux utilisateurs de retenir de nombreux mots de passe, il est possible de mettre en place un outil qui rende l'authentification de l'utilisateur unique pour chaque session : le Single Sign On (SSO).

La mise en place d'un SSO ne renforce en aucun cas la robustesse du processus de contrôle d'accès au SI, il sert juste de point d'entrée unique au SI : c'est une mesure pratique pour les utilisateurs. Par conséquent, si ce point d'entrée venait à céder à la suite d'une malveillance, d'un disfonctionnement ou d'une attaque venant d'Internet, cela pourrait avoir des conséquences désastreuses pour la sécurité du SI de l'entreprise. Il est donc souhaitable de coupler le contrôle d'accès des utilisateurs au système d'information via un serveur SSO à une méthode d'authentification forte comme un mot de passe Jetable (i.e. mot de passe à usage unique), des certificats X.509 ou des systèmes biométriques, suivant le niveau de risque des informations auxquelles l'utilisateur nécessite un accès.

L'authentification peut aussi reposer sur un protocole d'authentification réseau, le protocole Kerberos, qui permet de sécuriser les mots de passe statiques lorsqu'ils sont transmis sur le réseau. Ce protocole, créé par le Massachusetts Institute of Technology (MIT), utilise la cryptographie à clés publiques.[3]

5.2Certificats de clés publiques :

La cryptographie à clé publique peut être utilisée pour chiffrer des mots de passe. En outre, elle peut également être employée pour signer des données, qu'il s'agisse d'un contrat afin que les parties qui l'ont signé ne puissent pas en répudier le contenu a posteriori, ou qu'il s'agisse d'une valeur aléatoire pour assurer l'authentification.

En effet, les certificats de clés publiques sont l'une des techniques d'authentification les plus usitées à ce jour, certes loin derrière les mots de passe mais ce moyen d'authentification devient de plus en plus populaire. [3]

La cryptographie asymétrique fait intervenir deux éléments qui sont mathématiquement liés entre eux : la clé privée et la clé publique.

La clé publique est :

- ✓ Disponible pour tout le monde.
- ✓ Utilisée par une personne qui souhaite authentifier l'émetteur d'un document électronique signé avec la clé privée. Le contrôle de la signature permet aussi de s'assurer de l'intégrité du fichier.
- ✓ Utilisée par une personne souhaitant chiffrer un message afin que ce dernier soit uniquement lisible par le possesseur de la clé privée associée.

La clé privée est :

- ✓ Conservée secrète par son possesseur.
- ✓ Utilisée par son possesseur pour signer un document électronique (message, contrat ou autre).
- ✓ Utilisée par son possesseur pour déchiffrer un message chiffré à son attention.

5.3 Biométrie

Une autre méthode de l'authentification est de satisfaire la contrainte " ce que je suis", par les méthodes biométrique dont on peut citer les empreints digitales, l'iris, la rétine, l'ADN, ...etc

Le prochain chapitre détaillera tout ce qui concerne la biométrie.

Chapitre II : La biométrie

1. Introduction

La biométrie est originaire d'une contraction des deux anciens termes grecs « Bios » qui signifie : la vie et du mot «métrique» qui veut dire mesure. La biométrie consiste à extraire ou à calculer les paramètres physiques ou comportementaux propres à chaque individu dans le but de pouvoir l'identifier de manière fiable.

La biométrie comportementale est généralement utilisée pour la vérification alors que la biométrie physique peut être utilisée soit pour l'identification ou la vérification. [1]

2. L'histoire de la biométrie :

La biométrie a une longue histoire Depuis des temps immémoriaux, l'homme reconnaît ses semblables en scrutant leurs visages, leurs voix et leur morphologie.

Mais même cette biométrie n'est pas nouvelle: l'utilisation de la biométrie remonte à bien plus longtemps que ce que la plupart des personnes croient. En effet, dès -3000 avant J-C, les historiens ont des traces d'échanges commerciaux babyloniens utilisant les empreintes digitales pour la transaction de biens [2], et en XI^{ème} siècle les Chinois et les japonais utilisaient l'empreinte digitale pour authentifier couramment certains documents.

Depuis, il fût une période « d'inactivité », durant laquelle on ne parlait plus de la biométrie jusqu'au 17ème siècle, où des connaissances sur les empreintes digitales se développent. En effet, c'est en 1684 qu'un scientifique anglais, *Nehemiah Grew*, écrit le premier traité détaillé sur les empreintes digitales.[3]

Deux ans plus tard, l'anatomiste italien *Marcello Malpighi* fût le premier à étudier les empreintes digitales sous un microscope, il en déduit que " les rides des doigts permettent la saisie et celles des pieds, la traction ".[4]

En 1823 le physiologiste tchèque, *Johannes Purkinje*, proposa de classer les empreintes digitales en neuf catégories de motifs.

Puis, en 1860, l'administrateur britannique aux Indes, *William James Herschel*, note que " les empreintes digitales sont formées avant la naissance et restent inchangées

tout au long de la vie sauf en cas de blessures profondes ". Il imagina alors de les utiliser pour signer des chèques.

En résumé, c'est dans ce chapitre que seront abordés les grands moments de la biométrie, ces moments qui ont marqué son histoire et qui doivent être compris afin d'entrevoir son évolution.

2.1 le Bertillonnage :

En 1870, le premier laboratoire de police scientifique fût créé par *Alphonse Bertillon*, criminologue français. Le but était de procéder à l'identification des criminels. Il créa également un système de mesures anthropométriques, que l'on appela également « **le bertillonnage** », ce qui permettait de décrire les individus, en partant du principe qu'à vingt ans l'ossature humaine se stabilise. [5]

Alphonse Bertillon a beaucoup contribué à la progression des techniques d'identification et a rédigé plusieurs ouvrages à ce sujet. Son système a été adopté par la plupart des services de police européens et américains. [6]

La méthode de bertillonnage repose sur 9 mesures :

Il y a d'abord la mensuration de l'envergure c'est à dire la longueur d'un bout de bras à l'autre, puis la taille, la hauteur du buste, la longueur et la largeur de la tête, la longueur de l'oreille droite, la longueur du pied gauche, la longueur de la coudée gauche enfin la longueur du médius gauche (le majeur). [7]

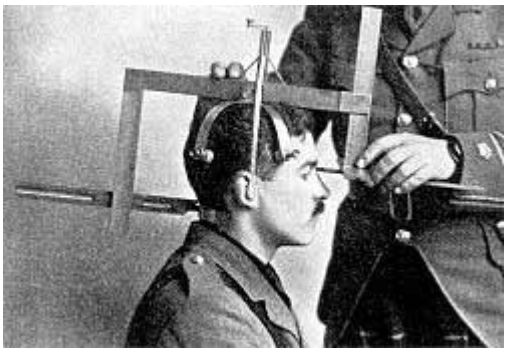


Figure 1 : le Bertillonnage

Les valeurs sont par la suite rapportées sur une fiche d'identité, qui sera bien entendue classée. Ce qui permet de la retrouver facilement dès que l'individu déjà signalisé se représentera.

Le Bertillonnage fut ainsi victime de l'expansion de l'informatique. Le système informatisé garantissait une meilleure sécurité, et ses données se révélaient quasi-infalsifiables. De plus, le traitement des données est largement plus rapide. Il est concurrencé par le profil ADN, qui est cependant plus internes et qui nécessite des technologies plus performantes.

2.2 les empreintes digitales:

Les premières traces d'utilisation d'empreintes digitales ont été découvertes en Egypte et datent de l'époque des pharaons « pyramides » il y a plus de 4000 ans.

Les empreintes digitales, la seule forme de biométrie reconnue jusqu'au XXe siècle, ont des origines très lointaines comme en témoigne une fresque murale où des tribus de Nouvelle-Écosse ont dessiné une main avec les empreintes de la paume et des doigts. Ou encore, dans la Babylone antique où les empreintes étaient utilisées pour régler des transactions.

En 1892, l'anthropologue anglais, *Francis Galton* a réalisé des recherches sur les mensurations des hommes (taille, poids et d'autres caractères) et a établit des statistiques a ce propos. Il a déduit de ces travaux que les figures cutanées (formant les empreintes digitales) sont le moyen d'identification le plus performant et a expliqué que les empreintes digitales sont propres a chaque humain, qu'elles sont uniques et permanentes, il estima la probabilité que deux humains aient les mêmes empreintes digitales est de une (1) chance sur 64 milliards.

Galton s'appuie sur toutes les recherches pour décréter que les empreintes sont uniques pour chaque individu et permettent l'identification d'une personne de manière fiable.

Suite aux travaux de *Galton*, le policier et statisticien argentin, *Juan Vucetich*, décida d'ajouter les empreintes digitales aux mesures anthropométriques de tout criminel, et dans la même année *Juan Vucetich* fût le premier à identifier une criminelle par ses empreintes digitales, la veuve *Rojas* qui a tué ses deux enfants.

L'Argentine fût le premier pays à abandonner l'anthropométrie mise au point par *Bertillon* au profit des empreintes digitales seulement.

En 1880, *Alphonse Bertillon* invita la police scientifique française à ajouter les empreintes digitales sur les fiches des criminels. En 1902, il identifie l'auteur d'un crime grâce à ses empreintes digitales après avoir échoué avec l'anthropométrie. [8]

Au début des années 1980. L'utilisation des empreintes digitales par les moyens 'informatique est omniprésente dans les systèmes de sécurité actuels.

Figure 2 : empreinte digitale

2.3 Géométrie de la main

La géométrie de la main est une technologie biométrique récente qui utilise la mesure de la main c'est-à-dire mesurer la longueur, la largeur et la hauteur de la main, la paume et la forme de la main. [9]

La reconnaissance par géométrie de la main est un des systèmes biométriques commerciaux les plus anciens.

Des appareils de mesure viables de la géométrie de la main sont fabriqués depuis le début des années 1980, faisant de la géométrie de la main la première donnée biométrique dont l'utilisation électronique a été généralisée. Cette technique est encore

largement employée, notamment pour contrôler l'accès des personnes et dans les systèmes de pointage des heures et des présences.

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. [10]

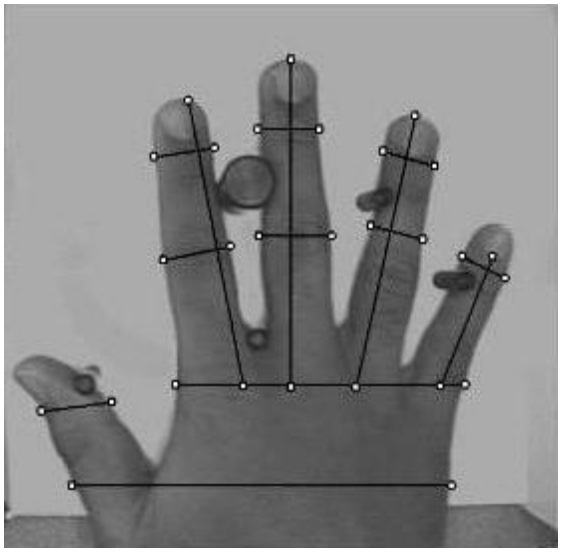


Figure 3 : La reconnaissance de la main

2.4 Reconnaissance faciale

Au début des années 1970, la reconnaissance par le visage (faciale) était principalement basée sur des attributs faciaux mesurables comme l'écartement des yeux, des sourcils, des lèvres, la position du menton, la forme, etc. Depuis les années 1990, les différentes technologies utilisées exploitent toutes les découvertes effectuées dans le domaine du traitement d'image.

L'arrivée de la reconnaissance faciale comme outil biométrique est aussi assez récente, C'est la technique la plus simple et la moins contraignante. Mais elle a encore de gros progrès à faire.[11]

La technologie de reconnaissance faciale vise à identifier des individus ou à authentifier leur identité en comparant leur visage avec des visages connus stockés dans une base de données pour trouver une correspondance.

Ce système se caractérise par sa facilité de reconnaissance. Quelques secondes devant la caméra suffisent pour une bonne reconnaissance. [12]

2-4 .1 Reconnaissance faciale automatisée :

La reconnaissance faciale automatisée consiste à identifier un individu à partir de la géométrie de son visage. Pour que cette technologie soit efficace, il faut disposer d'une image numérique de qualité du visage de l'individu dans une base de données d'images numériques d'individus identifiés et d'un logiciel de reconnaissance faciale capable d'établir une correspondance exacte entre l'image d'un individu et une image d'un individu identifié qui est enregistrée dans la base de données.

En 2001 la reconnaissance faciale a fait son entrée dans l'esprit du citoyen américain dans le match final de <<Superbowl>>. Chaque personne qui entrait au stade avait, à son insu et sans son consentement, son visage comparé à ceux compris dans une banque de données de criminels et de terroristes. [13]

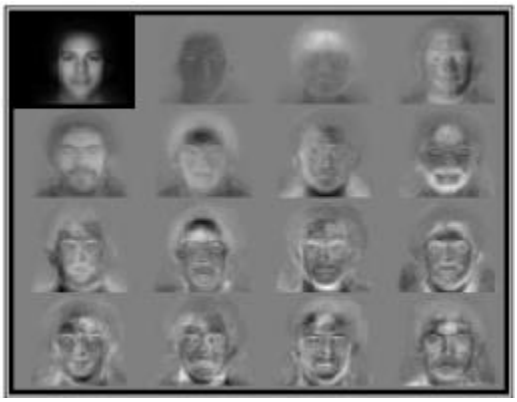


Figure 4 : la reconnaissance de visage

2.5 L'Iris

La reconnaissance de l'iris pour l'identification d'une personne était proposée à l'origine en 1936 par l'ophtalmologiste *Frank Burch*.

Cependant, ce concept est resté sans suite jusqu'en 1987, où les ophtalmologistes *Léonard Flom* et *Aran Safir* ont affirmé que chaque iris était unique et pouvait ainsi servir à l'identification des individus

Deux années plus tard, ils reçoivent un brevet pour ce concept. Le docteur *John Daugman* est contacté par le Dr *Flom* afin de trouver un algorithme de reconnaissance de l'iris. En 1995, les trois scientifiques de la Defense Nuclear Agency complètent et testent avec succès l'algorithme de reconnaissance automatique de l'iris et c'est dans la même année que le produit de ces recherches est commercialisé. [14]

La technique d'identification par l'iris est principalement exploitée dans le domaine frontalier. Depuis 2003, le Canada s'est doté d'un tel procédé afin de faciliter le contrôle douanier des utilisateurs qui font fréquemment le voyage en provenance des États-Unis. Sur une base volontaire, ce type de voyageur doit préalablement enregistrer l'image de son iris, lequel se retrouve alors sur une carte sous forme de code. Lors du passage à la douane, l'usager doit alors authentifier son iris avec son code. L'Australie travaille également à l'implantation d'un tel système d'identification pour ses frontières. [15]

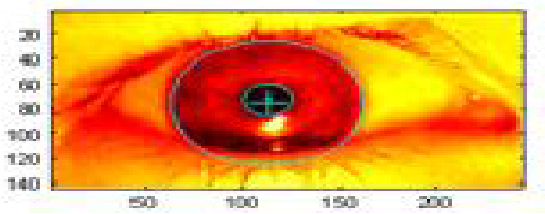


Figure 5: la reconnaissance de l'iris

2.6 La voix

Les travaux sur la reconnaissance de la parole ont commencé en début du 20eme siècle par le professeur suédois *Gunnar Fant*. C'est en 1952 que le premier système pouvant faire de la reconnaissance de la parole est mis au ponit.

L'entreprise Texas Instruments a inventé un prototype pour l'armée de l'air des États-Unis, en1976. Dans les années 1980, le NIST a sérieusement entrepris de développer un système de reconnaissance vocale avec son « Speech grouP» et depuis 1996 ce groupe tient des évaluations annuelles et reçoit un financement de la NSA (National Security Agency). [16]

La voix d'une personne se caractérise par beaucoup de paramètres. Chaque personne possède une voix propre que l'on peut analyser par enregistrement avec un micro. Les sons se caractérisent par une fréquence, une intensité et une tonalité.

Malgré toutes les difficultés apparentes, la voix reste un moyen biométrique intéressant à exploiter car elle est pratique et disponible via le réseau téléphonique, contrairement à ses concurrents.

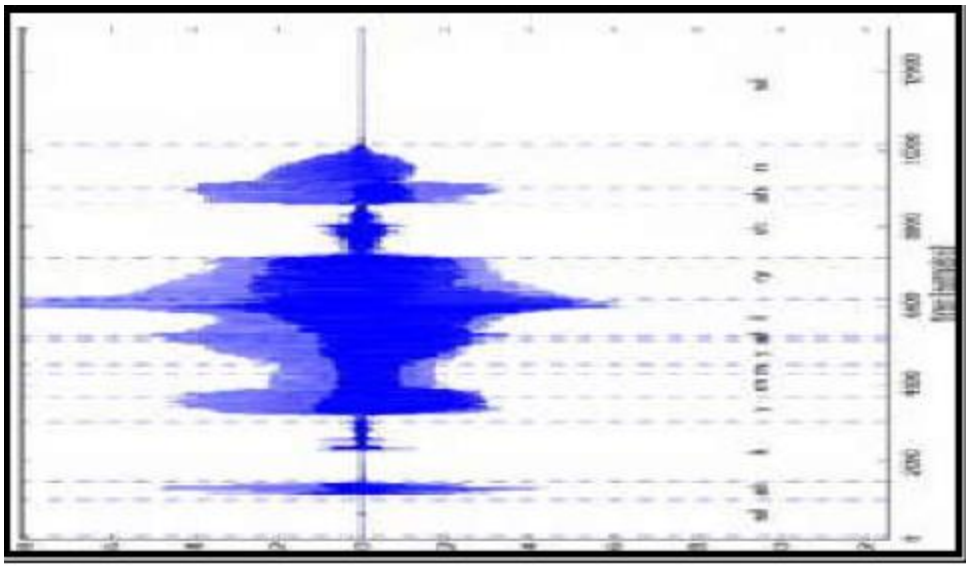


Figure 6: la reconnaissance de la parole

2.7 Rétine

La rétine est la couche sensorielle de l'œil qui permet la vision. Cette zone est parcourue par des vaisseaux sanguins qui émergent au niveau de la papille optique, où l'on distingue l'artère et la veine centrale de la rétine qui se divisent elles-mêmes en artères et veines de diamètre plus faible pour vascularisé les cellules qui permettent la vision. La grande variété de configurations des vaisseaux sanguins présentent la même diversité que les empreintes digitales. L'aspect des vaisseaux peut être modifié par l'âge ou la maladie, mais la position respective des vaisseaux reste inchangée durant toute la vie de l'individu.

La biométrie par la rétine procure un haut niveau en matière de reconnaissance. Il est bien adapté pour des applications de haute sécurité (sites militaires, salles de coffres forts, etc).

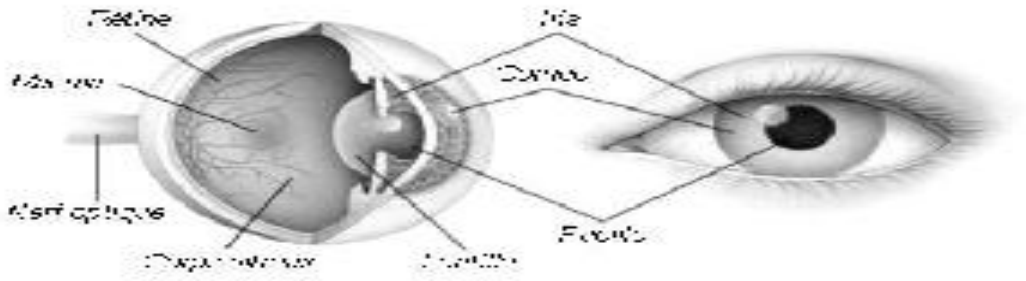


Figure 7 : la reconnaissance de la rétine

2.8 L'ADN

Présent dans les cellules du corps, il est spécifique d'un individu et permet de l'identifier de manière certaine à partir d'un simple fragment de peau, d'une trace de sang ou d'une goutte de salive.

L'analyse de l'ADN et sa reconnaissance mobilisent des techniques lourdes à mettre en œuvre, dont le résultat n'est pas immédiat et coûtent cher.

L'information génétique d'un individu est unique car aucun membre de l'espèce ne possède la même combinaison (ADN). La notion d'empreintes génétiques fut introduite par un biologiste anglais *Alec Jeffreys* en 1985. La technique a bénéficié de l'invention de la PCR par *Kary Mullis*, biochimiste américain, « réaction de polymérisation en chaîne de l'ADN » qui permet d'obtenir des quantités substantielles

d'ADN à partir d'une seule molécule. *Kary Banks Mullis*, biochimiste américain, partagea le prix Nobel de chimie de 1993 avec le Canadien *Michael Smith* pour avoir découvert une méthode permettant de manipuler les molécules d'acide désoxyribonucléique (ADN). [18]

L'invention de la PCR en 1985, et son perfectionnement en 1988, ont révolutionné la biologie moléculaire. Avant la PCR, les chercheurs devaient passer des semaines ou même des mois à générer une quantité suffisante d'ADN pour entreprendre leurs recherches. La PCR, qui permet de copier un segment d'ADN à une vitesse exponentielle, a réduit cette tâche à quelques heures. Méthode ultrasensible de détection, la PCR est notamment utilisée dans les tests de détection du VIH (virus du sida).

Trace individuelle unique, l'ADN est "l'outil" d'identification par excellence. 76 Etats à travers le monde et 35 pays européens possèdent ou programment la mise sur pied d'une base des données génétiques. L'utilisation de l'ADN facilite largement la désignation du coupable, en 2003-2004, 43% des crimes étaient éclaircis. [17]

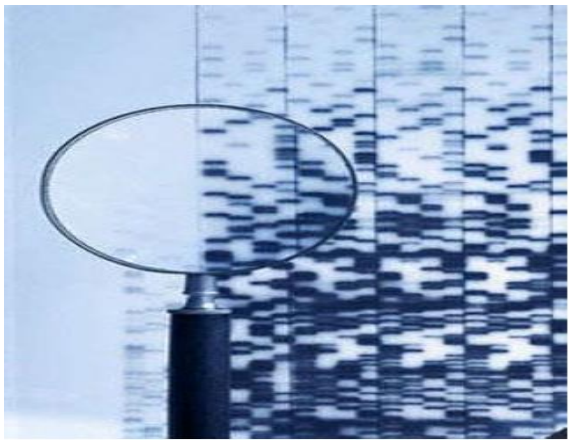


Figure 8 : L'ADN

3. Pourquoi la biométrie ?

Plusieurs raisons peuvent motiver l'usage de la biométrie:

a. **Gain en sécurité** : La biométrie permet de garantir l'identité d'un individu ou d'authentifier qu'il est le porteur légitime d'un badge, quand les autres

technologies ne peuvent garantir l'identité de l'usager d'un code ou du porteur d'une clef ou d'un badge. Avec la biométrie, l'usager « devient » sa propre clef infalsifiable. La biométrie palie au risque d'usurpation d'identité, de copie, emprunt ou vol de clef ou de badge, d'indiscrétion ou piratage de mot de passe. Avec la biométrie, nul autre que vous ne peut accéder à votre place à vos locaux ni à vos informations : « vous devez être qui vous prétendez être».

b. **Confort** : en remplaçant juste le mot de passe, exemple pour l'ouverture d'un système d'exploitation, la biométrie permet de respecter les règles de base de la sécurité (ne pas inscrire son mot de passe à côté du PC, ne pas désactiver l'écran de veille pour éviter des saisies de mots de passe fréquentes). Et quand ces règles sont respectées, la biométrie évite aux administrateurs de réseaux d'avoir à répondre aux nombreux appels pour perte de mot de passe (que l'on donne parfois au téléphone, donc sans sécurité).

Les systèmes d'authentification biométriques mettent fin aux problèmes liés à l'utilisation des systèmes d'authentification classiques tels que :

- ✓ La duplication.
- ✓ Le vol.
- ✓ L'oubli.
- ✓ La perte.

4 .Caractéristiques de la biométrie

Un certain nombre de caractéristiques sont utilisées dans diverses applications. Chaque trait biométrique a ses avantages et ses inconvénients, c'est pourquoi, le choix de la technique pour une application particulière dépend d'une variété de questions en plus de sa performance. *Jain et al* [20] ont identifié sept facteurs déterminant la convenance des traits physiques ou comportementaux pour être utilisés dans une application biométrique : [21]

- ✓ **Universalité** : toute personne ayant accès à l'application doit posséder le trait.
- ✓ **Unicité** : le trait doit être suffisamment différent d'une personne à une autre.
- ✓ **Permanence** : le trait biométrique d'une personne doit être suffisamment invariant au cours d'une période de temps.

- ✓ **Mesurabilité** : il devrait être possible d'acquérir et de numériser les données biométriques à l'aide d'un dispositif approprié.
- ✓ **Performance** : la précision de la reconnaissance et les ressources nécessaires pour atteindre la précision que doit satisfaire les contraintes imposées par l'application.
- ✓ **Acceptabilité** : les individus qui vont utiliser cette application doivent être disposés à présenter leurs traits biométriques au système.
- ✓ **Contournement** : il s'agit de la facilité avec laquelle le caractère d'un individu peut être imité en utilisant des objets (par exemple : faux doigts dans le cas de traits physiques et le mimétisme, dans le cas de traits de comportement).

5 .Le marché mondial de la biométrie

Le marché de la biométrie est en plein boom, selon l'agence Markets & Markets, le marché mondial de la biométrie représente 8,5 milliards d'euros en 2015. Cette expansion se fait particulièrement sentir dans les pays émergents où les états civils, quand ils existent, sont souvent parcellaires. [19]

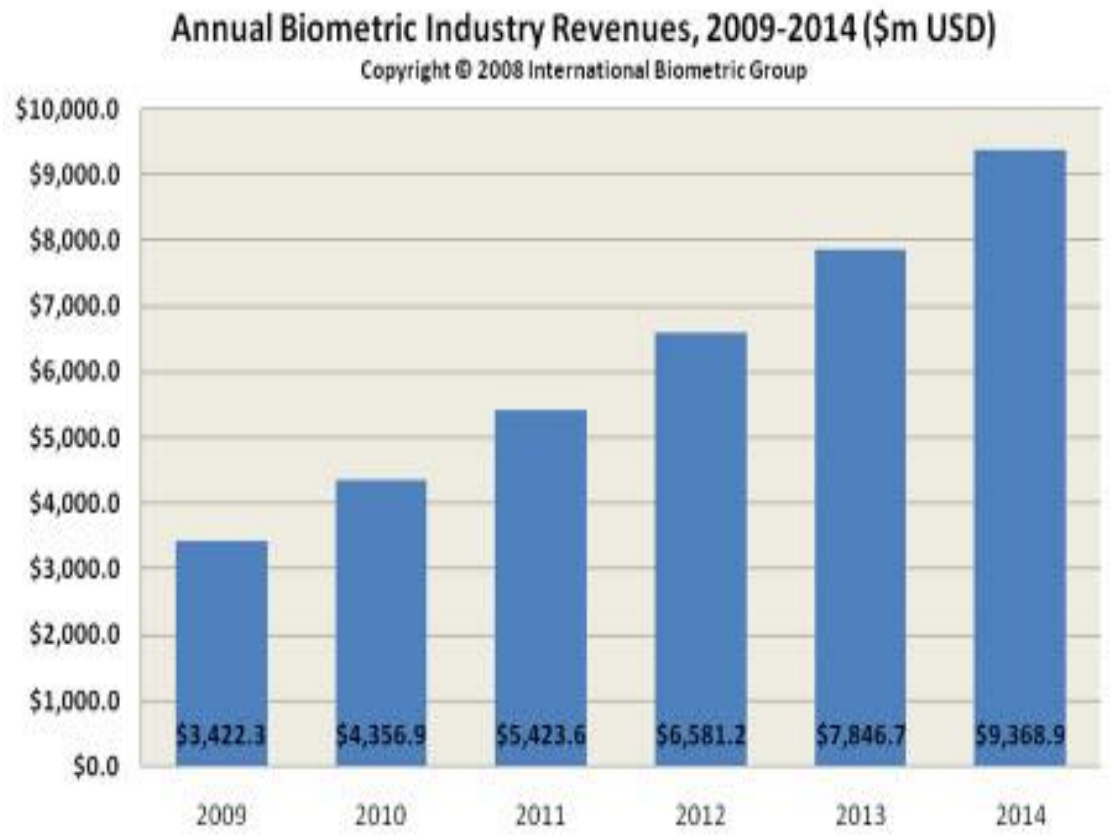


Figure 9 : le marché mondial de la biométrie

Conclusion :

On retiendra plusieurs faits marquants concernant la biométrie :

Il ne suffit pas de remplacer un login/mot de passe par une mesure de biométrie; il faut également repenser tout le système et sécuriser l'architecture complète.

Il ne faut pas utiliser une mesure biométrique seule pour procéder à une authentification; on préférera la coupler avec une carte à puce, un token sécurisé (petit élément de stockage présentant une grande résistance aux attaques, même physiques), un mot de passe.

On utilisera la biométrie de préférence pour les opérations d'identification plutôt que d'authentification.

Enfin, on peut conclure que la biométrie regroupe l'ensemble des techniques informatiques qui permettent de reconnaître un individu sur ses caractères biologiques, physiques ou comportementaux.

Chapitre III : L’empreinte Digitale

1– Introduction

Les Empreintes digitales humaines sont détaillées, présumée être presque unique, difficile à modifier, et durable sur la vie d'un individu, ce qui les rend appropriés comme marqueurs à long terme de l'identité humaine. Ils peuvent être employés par la police ou d'autres autorités pour identifier les personnes qui souhaitent cacher leur identité, ou d'identifier les personnes qui sont frappées d'incapacité ou décédés et donc incapables de se repérer, comme à la suite d'une catastrophe naturelle. Analyse d'empreintes digitales, en usage depuis le début du 20e siècle, a conduit à de nombreux crimes résolus. [1]

2 -Définition :

Les empreintes digitales sont les marques laissées par les lignes de la peau des doigts. Le Dessin qu'elles forment est propre à chaque personne et garde la même forme tout au long de la vie, ce qui explique pourquoi les empreintes digitales servent à l'identification des personnes.

Il existe deux types de trace (forme) : l'empreinte directe (qui laisse une marque visible) et l'empreinte latente (invisible à l'œil nu).Elles sont uniques et immuables.

La probabilité de trouver deux empreintes digitales similaires est de 10^{24}. Les jumeaux, par exemple, venant de la même cellule, auront des empreintes très proches mais pas semblables. [2]

3 – Caractéristiques d'une empreinte digitales

Chaque empreinte digitale possède un grand nombre de caractéristiques qui dépendent du patrimoine génétique**.**

Les pointes caractéristiques ou les crêtes sont utilisées pour différencier deux empreintes digitales et aussi faires une classification selon les points singuliers globaux et les points singuliers locaux.

3.1 - Les points singuliers globaux :

On distingue les points caractéristiques globaux par le Core et le Delta.

- **Le Core :** le centre ou le noyau qui contient les courbures maximales des lignes de l'empreinte les plus internes. Il est aussi appelé le point core.
- **Le Delta :** est proche du lieu où se deux lignes, aussi est le lieu de divergence des lignes les plus internes. (voir Figure 1) [3]

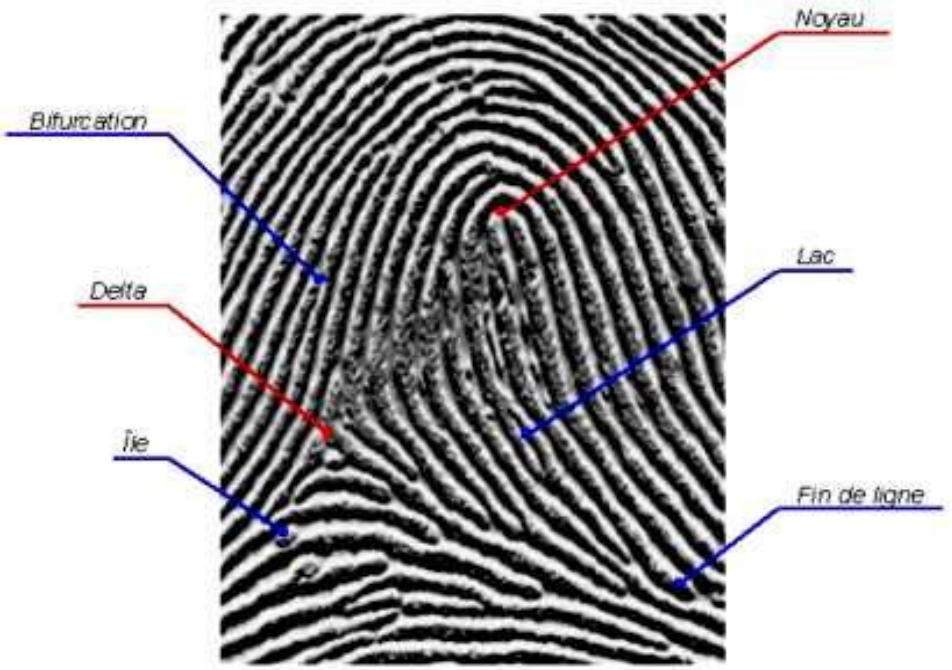


Figure 1 : **les noyaux et les deltas**

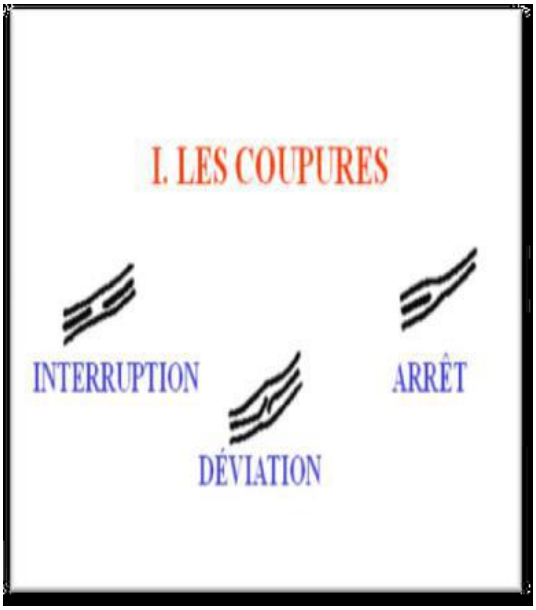
3.2 -Les points singuliers locaux (minutiers)

Dans chaque empreinte il y a des minuties spécifiques qui permettent de différencier et de classer les empreintes.

Il ya plusieurs formes de minutiers, généralement on a quatre formes :

1-Les coupures : terminaison à droite ou à gauche, minuties située en fin de stries. (voir Figure 2-1)

2-Les divisions : Bifurcation à droite ou à gauche, intersection de deux stries. (voir Figure 2-2) [4]



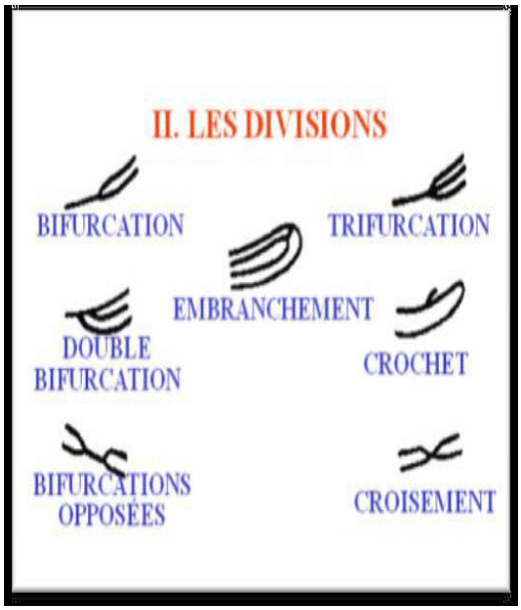
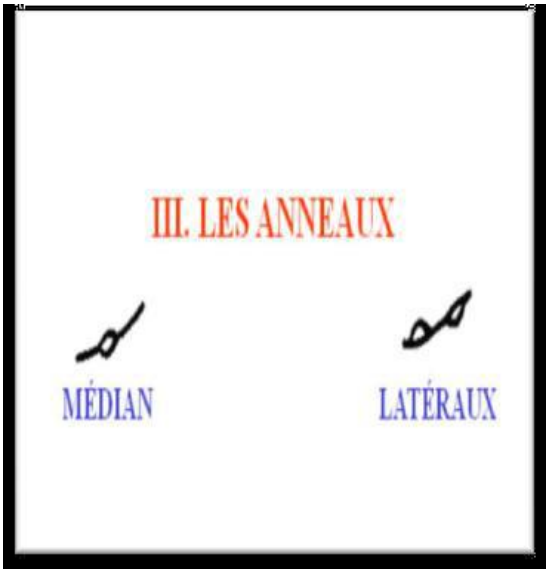


Figure 2-1: Les Coupures. **Figure 2-2:** Les Divisions**.**

3-Les anneaux : Lac, assimilée à deux bifurcations. (voir Figure 2-3)

4-Les ilots: assimilés à deux terminaisons. (voirII.Figure2-4)



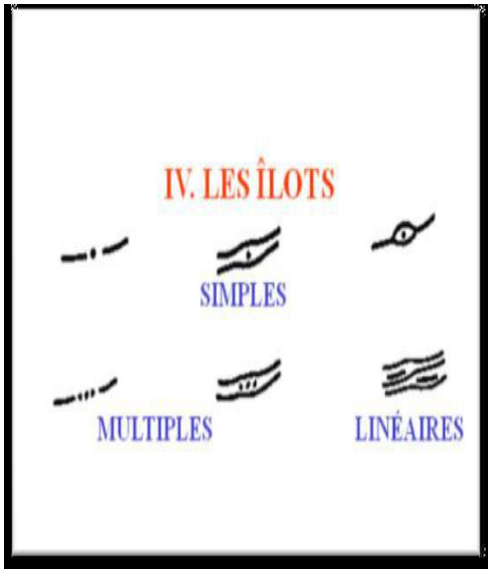


Figure 2.3: Les Anneaux **Figure 2.4**: Les îlots**.**

3.3 Les types des minuties :

Une empreinte complète contient en moyenne une centaine de ces points caractéristiques (les "minuties"). Si l'on considère la zone réellement scannée, on peut extraire environ 40 de ces points. Pour l'histoire, le nombre 12 provient de la règle des

12 points selon laquelle il est statistiquement impossible de trouver deux (2) individus présentant les mêmes 12 points caractéristiques, même en considérant une population de plusieurs dizaines de millions de personnes.

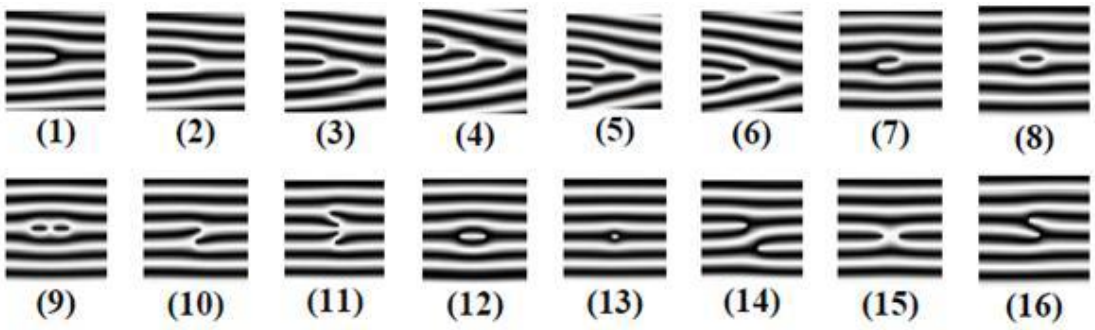


Figure 3 : les types des minuties

1	Terminaison	6	Bifurcation triple III	11	Pont jumeau
2	Bifurcation simple	7	Crochet	12	Intervalle
3	Bifurcation double	8	Boucle simple	13	Point isolé
4	Bifurcation triple I	9	Boucle double	14	Traversée
5	Bifurcation triple II	10	Pont simple	15	Croisement

4 - Classification des empreintes digitales

Les empreintes digitales possèdent des motifs différents. En tenant compte de ces derniers, il est possible d'établir un classement. En effet, il existe 3 grandes familles d'empreintes qui regroupent à elles seules 95% des doigts humains. [4]

- **Empreinte en boucle** : les lignes se replient sur elles-mêmes, soit vers la droite, soit vers la gauche (motif courant).

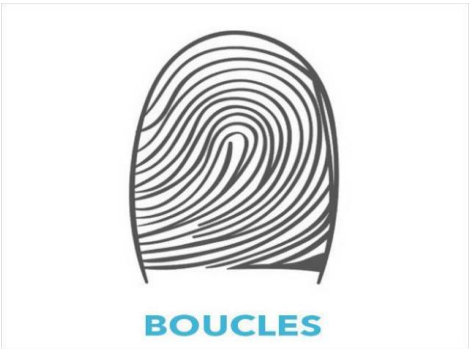


Figure 4: Empreinte en boucle

- **Empreinte en verticille** : présence de lignes qui s'enroulent autour d'un point en formant une sorte de tourbillon.

Figure 5: Empreinte en verticille

- **Empreinte en arc** : les lignes sont disposées les unes au-dessus des autres, en formant une sorte de A (motif rare).

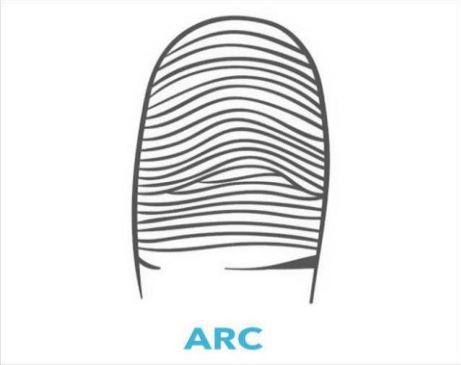


Figure 6: Empreinte en Arc

5 - Techniques de révélation d'une empreinte digitale :

Au par avant, pour prélever les empreintes digitales d'un individu, il suffisait d'appliquer une fine couche d'encre sur le bout du doigt, et d'apposer le doigt sur une feuille de papier afin de pouvoir les comparer à d'autres empreintes répertoriées dans une base de données, ou les utiliser, Avant de pouvoir analyser et traiter. [5]

Aujourd'hui, il est nécessaire d'acquérir l'image des empreintes digitales. Pour ceci, on utilise divers capteurs basés sur différentes technologies.

6 -Les capteurs d'empreinte digitale :

Il existe quatre principaux types de matériel de lecteur d'empreintes digitales:

6.1-Lecteurs optiques :

sont le type le plus commun des lecteurs d'empreintes digitales. Le type de capteur dans un lecteur optique est un appareil photo numérique qui acquiert une image visuelle de l'empreinte digitale. En général, le doigt est placé sur une surface en verre et l'appareil-photo CCD (dispositif couplé chargé) prend la photo. Le système CCD contient une rangée de LED (diodes électroluminescentes) qui illumine les creux et les bosses du doigt Leur avantage réside dans leur prix, ils ne sont pas très chers ; leur inconvénient est qu'ils sont faciles à détourner.

Ce procédé de capture d'image est le plus ancien après l'encre. Il est fréquemment utilisé particulièrement dans les applications judiciaires pour la qualité des images.[6]

Figure 7 : Capteur optique d'empreinte digitale

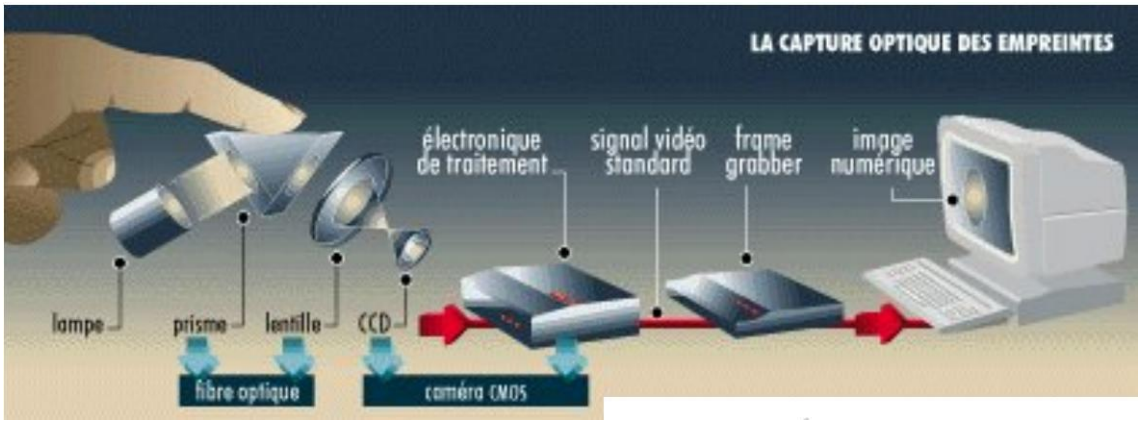


Figure 8: La capture optique des empreintes

6.2-Lecteurs capacitifs (silicium):

Également appelés lecteurs CMOS, le capteur capacitif d'empreinte digitale reproduit l'image des creux et des bosses qui composent une empreinte digitale

Un lecteur CMOS utilise des condensateurs et ainsi de courant électrique afin de former une image de l'empreinte digitale. Les lecteurs CMOS sont plus chers que les lecteurs optiques. [7]

Un avantage important de lecteurs capacitifs sur les lecteurs optiques est qu'un lecteur capacitif nécessite une forme réelle d'empreintes digitales plutôt que seulement une image visuelle. Ceci rend les lecteurs CMOS plus difficile à tromper.

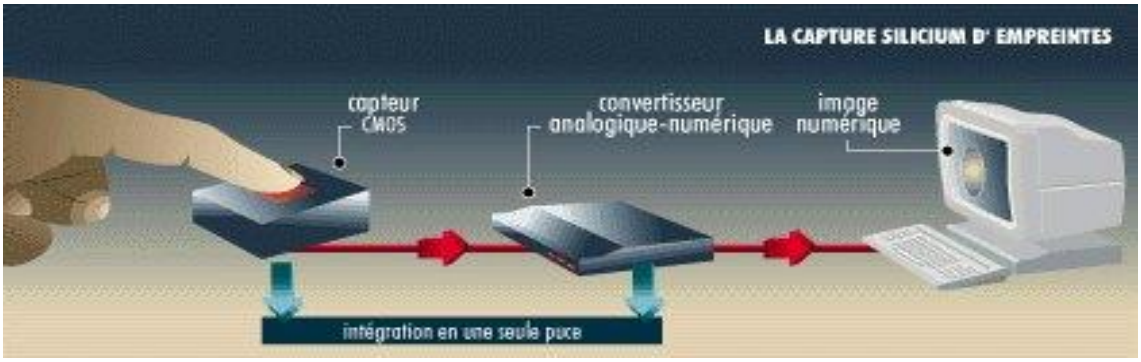


Figure 9: Capteur silicium d'empreinte digitale (capacitif)

6.3- Lecteurs ultrasons :

sont le type le plus récent de lecteurs d'empreintes digitales, ils utilisent des ondes sonores à haute fréquence pour pénétrer l'épiderme couche (externe) de la peau. Ils lisent l'empreinte digitale sur la couche de la peau dermique, ce qui élimine la nécessité d'une surface propre,.

Tous les autres types de lecteurs d'empreintes digitales doivent acquérir une image de la surface extérieure, ce qui nécessite des mains propres ou nettoyées et exempt de cicatrices avant la lecture. Ce type de lecteur d'empreintes digitales est beaucoup plus cher que les deux premiers, mais en raison de leur précision et le fait qu'ils sont difficiles à tromper les lecteurs d'ultrasons sont déjà très populaires. [7]

7- Principe de contrôle d'accès par les empreintes digitales

Un système automatique complet de reconnaissance d'empreinte digitales est une chaine 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 première phase permet d'obtenir une image d'empreintes digitales 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 les possibles fausses informations qui se seraient glissées dans la chaine de traitement. Ensuite, si l'utilisation du système consiste 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.

Pour un système d'identification, l'ensemble d'empreintes digitales présentes dans la base de données pouvant correspondre à celles de l'utilisateur (modèle identique) sont désarchivées et comparées (appareillement) une à une avec celles 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'acquisition ou le rejet de l'utilisateur.

Le schéma ci-dessous illustre ces différentes séquences.

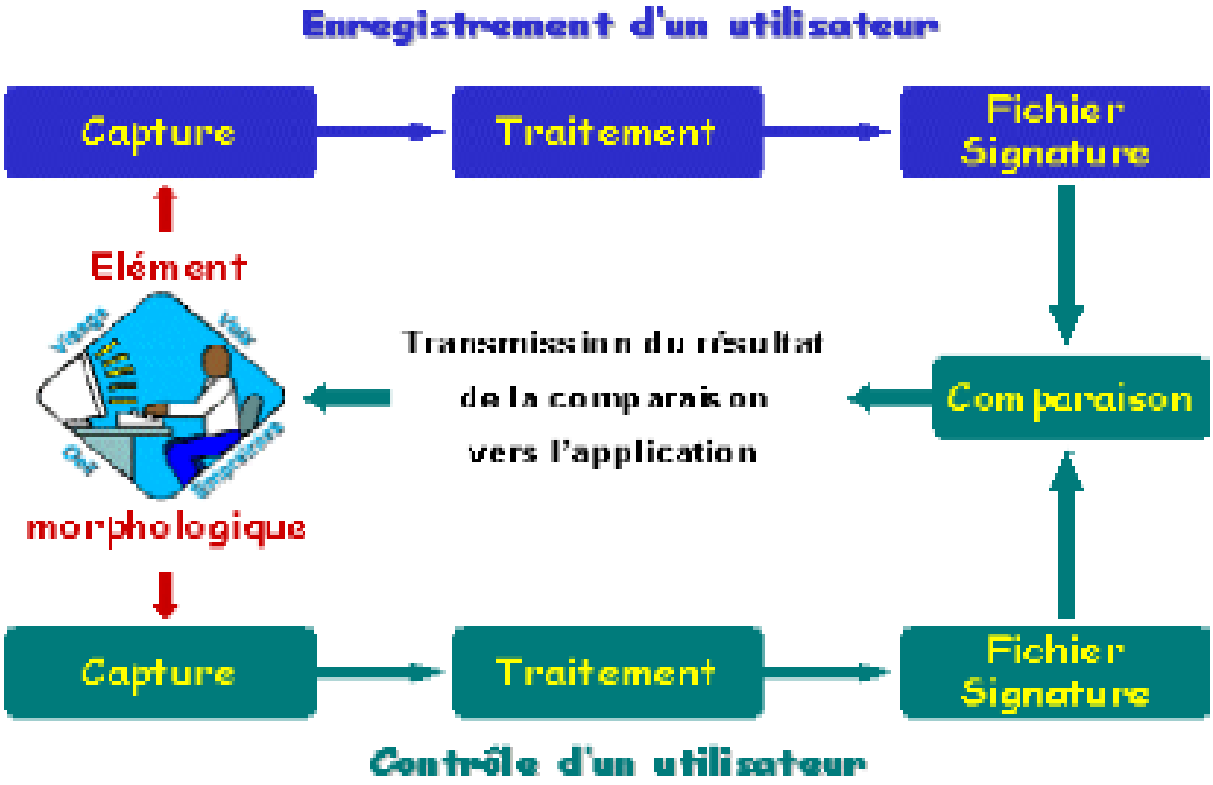


Figure10: Schéma de traitement des données biométriques

7.1- Image numérique et voisinage

Une image numérique peut être considérée comme un tableau (matrice 2D) de points échantillonnés à partir de l'image continu (photo), dont chacun a une luminosité particulière quantifiée;

- Ces points sont les pixels qui constituent l'image numérique.

–Les pixels qui entourent un pixel donné constituent son voisinage

- Un voisinage peut être caractérisé par sa forme qui est une matrice: par exemple, on peut parler d'un voisinage de 3x3, ou d'un d'un voisinage de 5x7.

Par exemple :

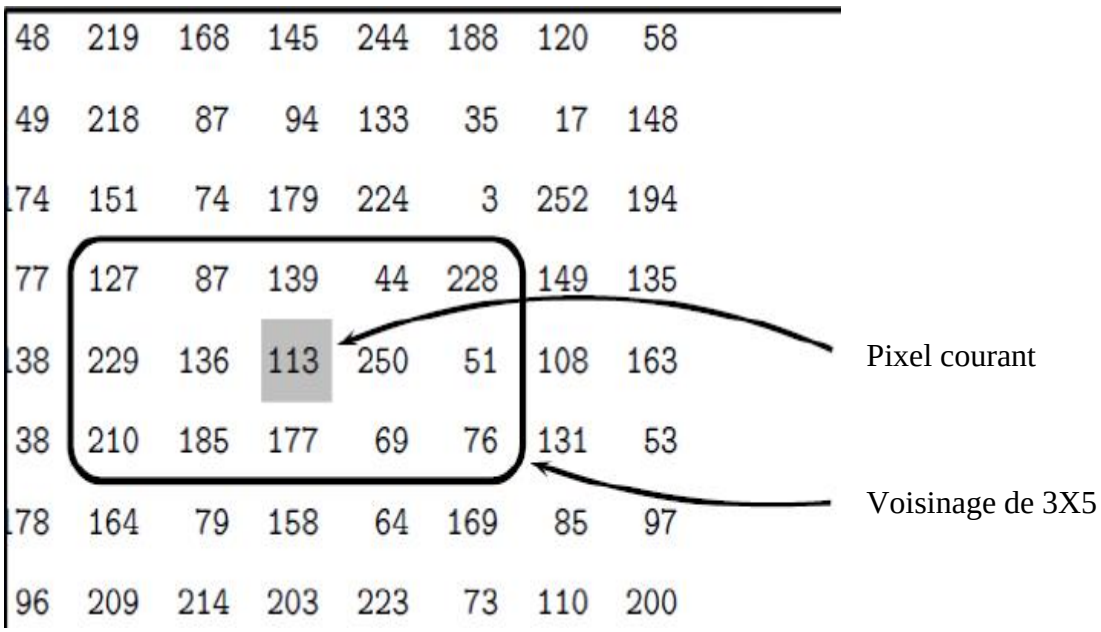


Figure 11 : matrice d'une image numérique

- les voisinages ont un nombre impair de lignes et de colonnes, ce qui garantit que le pixel courant est dans le centre de la zone ;voisinage 3x3, 9x9.
- Sinon, il peut être nécessaire de spécifier quel pixel dans ce voisinage est le

« Pixel courant »

7.2- Les étapes du traitement d'images :

- **L'acquisition de l'image**: Caméra CCD ou scanner,
- **Prétraitement** : Améliorer le contraste, la suppression du bruit et identifier les régions susceptibles de contenir le code postal.
- **Segmentation** : Extraction de la partie qui ne contient que le code postal,
- **Représentation et description** : Chercher des courbes, les trous et les coins qui nous permettrons de distinguer les différents chiffres qui constituent le code postal.
- **Reconnaissance et interprétation** : Attribuer des étiquettes à des objets en fonction de leurs descripteurs (de l'étape précédente), et assigner des significations à ces labels.

8 - Traitement d'une empreinte digitale :

Après la capture (acquisition) d'une image d'empreinte digitale par le lecteur d'empreintes digitales, cette empreinte doit être interprétée. Elle doit être traitée de manière efficace pour pouvoir la stocker d'une manière efficace et la comparer avec d'autres au moment voulu.

L'étape de traitement des images capturées est primordiale, elle permet de les normalisés. Son but est de supprimer toute ambiguïté en détectant des zones de bruit et en faisant ressortir la plus grande partie possible d'information utile au système.

L'image d'origine est binarisée (noir et blanc) puis squelettisée (les stries ont toutes la même épaisseur de 1 pixel). [7]

On peut ensuite, grâce à différents algorithmes, extraire les minuties et éjecter les « fausses ». On récupère ainsi en moyenne une centaine de minuties par empreinte.

L'image suivante montre le résultat d'un traitement d'une empreinte digitale.

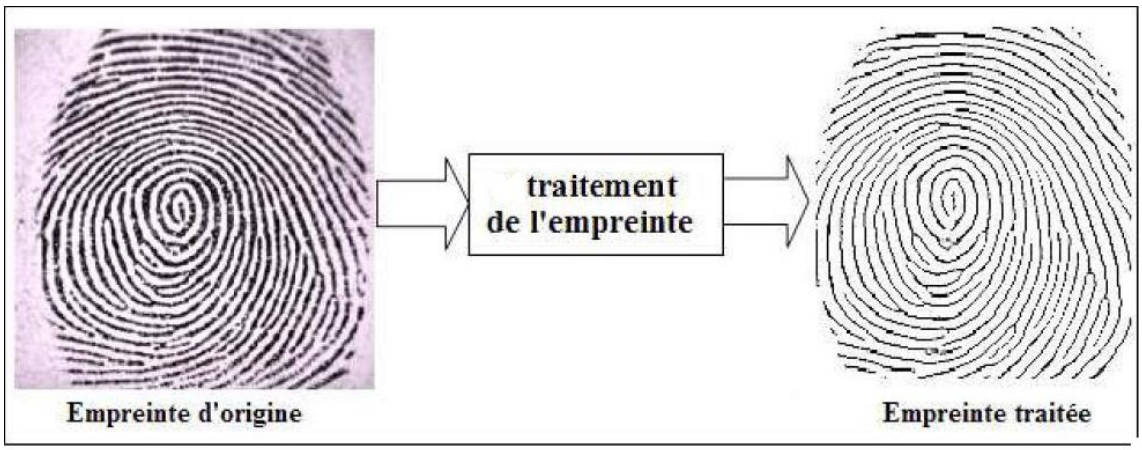
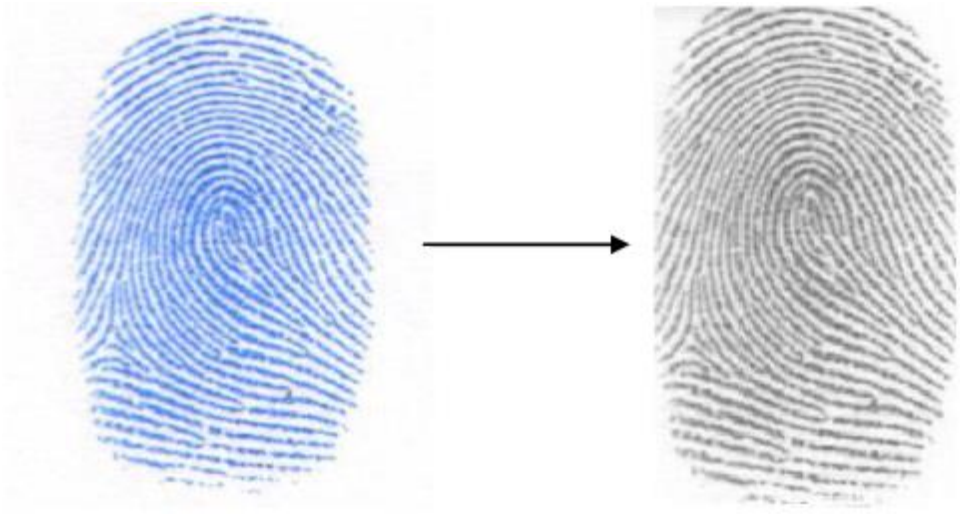


Figure 12 : Exemple du traitement des empreintes

8.1-Niveau de gris :

Le niveau de gris est une image de profondeur k=8 bits, chaque pixel prendre l'une des valeurs entre de l'intervalle [0 …..255], tel que le zéro représente le noir et 255 représente le blanc. Les valeurs intermédiaires correspondent à des niveaux de gris allant du noir au blanc.

Dans les applications professionnelles 8 bits n'est pas suffisants, donc il y a d'autre type d'image de niveaux de gris de profondeur k=14 bits ou k=16 bits.



L'empreinte originale. L'empreinte digitale en gris.

Figure 13 : L'empreinte digitale en gris.

Figure 14 : 255 niveaux de gris .

•255 niveaux de gris différents sont suffisants pour la reconnaissance (présentation) de la plupart des objets naturels.

8.2-La binarisation de l'image :

Pour permettre la squelettisation, une image doit d'abord être binarisée,

La binarisation consiste à transformer une image à plusieurs niveaux en une image en noir et blanc (deux niveaux seulement). C'est le moyen privilégié pour isoler des objets.

Par suite, une image binaire peut être représentée par une matrice booléenne dont chaque élément signifie Vrai (1 = blanc) ou Faux (0 = noir).

Il existe de nombreuses algorithmes de binarisation d'images :[8]

8.2.1- la méthode de Seuillage globale :

C'est la technique de binarisation la plus simple, Le principe du seuillage global est d'utiliser une valeur seuil à partir de laquelle on peut choisir à quelle classe le pixel appartient. La transformée peut s'écrire ainsi :

$\forall i, j \in N \times M \quad I(i, j) = << 1$ si $f(i, j) > S$

0 sinon >>

Avec

- $N \times M$: nombre de colonnes et de lignes de l'image ;
- I : image binarisée ;
- f : valeur fonction de l'image d'origine ;
- S : seuil de binarisation.

8.2.2- Binarisation d'images par la méthode d'Otsu:

Le but de cet algorithme est la binarisation d'images à niveaux de gris. Ceci revient à séparer les pixels de l'image en deux classes, la première ayant un niveau maximal (typiquement 255) et la seconde un niveau minimal (0).

La méthode d'OTSU est utilisée pour effectuer un seuillage automatique à partir de la forme de l'histogramme de l'image.Cette méthode nécessite donc le calcul préalable de l'histogramme de l'image. L'algorithme suppose alors que l'image à binariser ne contient

que deux classes, (Les objets et l'arrière-plan). L' algorithme itératif calcule alors le seuil optimal T qui sépare ces deux classes afin que la variance intra-classe soit minimale et que la variance inter-classe soit maximale.

1.Variance intra-classe :

$$\sigma_w^2 = \omega_1(T) \times \sigma_1^2(T) + \omega_2(T) \times \sigma_2^2(T)$$

Oméga 1 représente la probabilité d'être dans la classe 1

Oméga 2 représente la probabilité d'être dans la classe 2

Sigma 1 représente la variance de la classe 1

Sigma 2 représente la variance de la classe 2

2.Variance inter-classe :

$$\sigma_y^2 = \sigma^2 - \sigma_w^2$$

Sigma représente la variance de l'image

Sigma w représente la variance intra-classe

3.Calcul de la probabilité de la classe 1 et 2 :

Pour calculer la probabilisé d'être dans la classe 1 ou 2 en fonction du seuil T, il suffit de sommer les probabilités de chaque niveau de gris.

$$\omega_1(T) = \sum_{k=1}^{T} P(k)$$

$$\omega_2(T) = \sum_{k=T+1}^{256} P(k)$$

4. Calcul de l'histogramme :

L'histogramme est un graphique représentant la répartition des valeurs de niveau de gris dans une image. Pour calculer l'histogramme, il faut donc parcourir l'image dans sa totalité et compter le nombre de pixels qu'il y a pour chaque niveau de gris.

$$Hist(k) = \sum_{i=1}^{N}\sum_{j=1}^{M}(Image(i,j) == k)$$

5.Calcul de la probabilité de chaque niveau de gris :

La probabilité de chaque niveau de gris est calculée en divisant le nombre de pixels présent pour chaque niveau de gris par le nombre total de pixels dans l'image.

$$P(k) = \frac{Hist(k)}{Nombre\ total\ de\ pixels\ dans\ l'image}$$

6.Calcul de la variance de chaque classe :

$$\sigma_1^2(T) = \frac{\sum_{i=1}^{T}(N1(i) - Moy_1(T))^2 \times P(i)}{\omega_1}$$

$$\sigma_2^2(T) = \frac{\sum_{i=T+1}^{256}(N2(i) - Moy_2(T))^2 \times P(i)}{\omega_2}$$

N1 est un vecteur de 0 à T-1

N2 est un vecteur de T à 255

Moy1 représente la moyenne de la classe 1

Moy2 représente la moyenne de la classe 2

8.2-3 Binarisation d'images par la méthode de SAUVOLA :

La méthode de SAUVOLA est une technique de seuillage local. Avec cette méthode, le seuil T pour chaque pixel de l'image est donnée par :

$$T(x,y) = mean(x,y) \times \left[1 + k \times \left(\frac{s(x,y)}{R} - 1\right)\right]$$

R représente la valeur maximale de l'écart-type dans un document en niveau de gris (R = 128).

k est un paramètre qui prend une valeur positive dans l'intervalle [0.2, 0.5].

mean (x,y) représente la matrice des moyennes locales pour chaque pixel de l'image.

s(x,y) représente la matrice des écarts-types locaux pour chaque pixel de l'image.

Pour déterminer le seuil T correspondant à chaque pixel de l'image, il est donc nécessaire de calculer la matrice des moyennes locales de l'image et la matrice des écarts-types locaux de l'image.

1.Calcul de la moyenne locale de chaque pixel de l'image :

La méthode consiste à faire la somme de tous les pixels sur une fenêtre carrée de taille donnée W centrée sur le pixel et ensuite de diviser par W² (Convolution 2D).

La figure ci-dessous représente un masque moyen de taille 3*3 (W) qu'il faut appliquer sur chaque pixel de l'image pour obtenir leur moyenne locale.

1/9	1/9	1/9
1/9	1/9	1/9
1/9	1/9	1/9

$$mean(x,y) = \frac{1}{W^2} \sum_{i=x-W/2}^{x+W/2} \sum_{j=y-W/2}^{y+W/2} (Image(i,j))$$

Figure 15 : un masque moyen de taille 3*3.

La fenêtre 2D utilisée pour calculer la moyenne locale étant séparable, il est donc possible de calculer cette moyenne en utilisant deux fenêtres 1D. L'avantage de cette seconde méthode est qu'elle réduit considérablement la complexité et par conséquent le temps de calcul.

2. Calcul de l'écart-type local d'une image :

L'écart-type local de chaque pixel étant égal à la racine carré de la variance locale de chaque pixel.

Le principe consiste à sommer tous les pixels de la fenêtre qui ont été retranchés par la moyenne et élevés à la puissance de deux. Ensuite, il faut diviser le résultat de cette somme par le nombre de pixel dans la fenêtre.

$$s^2(x,y) = \frac{\sum_{i=x-w/2}^{x+w/2} \sum_{j=y-w/2}^{y+w/2} (Image(i,j) - mean(x,y))^2}{W^2}$$

W représente la taille de la fenêtre

mean(x,y) représente la matrice des moyennes locales de chaque pixel

image(i,j) représente l'image de départ

8.2.4 Méthode de Wolf :

Pour remédier aux problèmes de l'algorithme de Sauvola (faible contraste, écart de niveaux de gris etc.), Wolf et al. [12] proposent de normaliser le contraste et la moyenne de niveaux de gris de l'image, et calculer le seuil par :

$$T = (1-k)*m+k*M* \alpha / R(m-M)$$

Tel que k est fixé à 0.5, M est le niveau de gris minimum de l'image et R vaut l'écart-type maximum de niveaux de gris obtenu sur toutes les fenêtres. [9]

Image originale *Image filtrée* *Image binarisée*

Figure 16: Binarisation de l'empreinte digitale.

Les principales étapes de traitement sont illustrées sur ces images:

Au début nous avons l'image brute, c'est-à-dire que nous retrouvons ce qu'on appelle le bruit qui va brouiller l'empreinte. Le but de cette étape est de supprimer toute ambiguïté en détectant les zones de bruit et en faisant ressortir la plus grande partie possible d'information utile au système.

Cette fonction se charge également de détecter l'absence d'empreinte, un niveau élevé de bruit dans l'image (image sale ou lecteur défectueux), un positionnement incorrect du doigt.

Puis après avoir obtenu une image nette de l'empreinte, il faut identifier les minuties selon les algorithmes appliqués c'est-à-dire les points remarquables d'une empreinte. C'est pourquoi il va squelletiser l'empreinte en réduisant chaque trait à une épaisseur de 1 pixel.

Après avoir squelletiser l'empreinte, on peut enfin lire les minuties ceci nous permet de comparer les empreintes. [9]

8.3-La squelettisation de l'image

Dans l'image binarisée (noir et blanc) les lignes se voient clairement mais elles ont des tailles différentes. Pour pouvoir détecter rapidement les minuties (terminaisons, bifurcations), il est nécessaire d'obtenir une image plus schématique de l'empreinte.
c'est-à-dire on réalise une suite d'opérations morphologiques d'érosion va réduire l'épaisseur des stries jusqu' à ce que cette dernière soit égale à un pixel. [8]

L'empreinte originale L'empreinte en gris L'empreinte Binaraisé

Figure 17: Squelettisation de l'empreinte digitale.

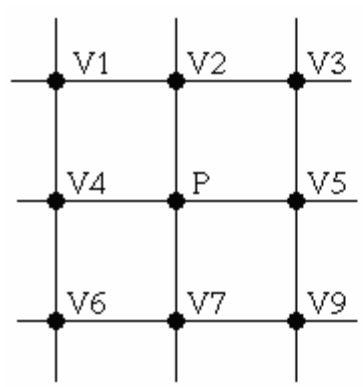
Il existe actuellement une grande variété de méthodes permettant de construire des squelettes, parmi ces méthodes on a :

8.3.1- Algorithme de Marthon

C'est un algorithme de suppression de points. Soit le point M considéré de coordonnées (x, y). Soit l'ensemble Mi (xi, yi) de ses points voisins en n-connexité, la conservation ou non du point M lors de la squelettisation dépend des deux valeurs X et Y définies comme suit :

$$X = (x1-x) + (x2-x) +...+ (xn-x)$$

$$Y = (y1-y) + (y2-y) +...+ (yn-y)$$



$$\begin{bmatrix} X \\ Y \end{bmatrix} = \sum \overrightarrow{PVi\ (P)}$$

- Si un point est intérieur à l'objet alors |X|+|Y| est petit.
- Si le point est au bord de l'objet alors |X|+|Y| est grand.

  En conséquence :

  - ✓ Si |X|+|Y| = 4, alors le point M est supprimé.
  - ✓ Si |X|+|Y|<=2, alors le point M est conservé.
  - ✓ Si |X|+|Y| = 3, alors le point M est conservé ou supprimé suivant le nombre de ses voisins. [13]

8.3.2 -Algorithme de Zhang et Suen

L'algorithme de Zhang et Suen introduit deux critères pour décider si un pixel P doit être éliminé. En premier lieu, il s'assure que le pixel considéré est un pixel noir et au moins l'un de ses voisins est blanc.

La 1ère itération pour transformer le pixel en pixel blanc si les conditions suivantes dans (t) sont réalisées. (voir **Table 2**)

A la 2ème itération les conditions (1) et (2) ne changent pas plus les conditions suivantes dans (t) sont réalisées.(voir **Table 2**)

Les pixels réalisant ces conditions doivent être supprimés.

A la fin s'il n'y a aucun pixel à supprimer,

alors l'algorithme s'arrête. [13]

P1	P2	P3
P8	P	P4
P7	P6	P5

Critère 1(première itération)	Critère 2(deuxième itération)
1. La connectivité est égale à 1 2. Il y a au moins 2 et au plus 6 voisins de valeur noir. 3. Au moins l'un des pixels P2, P4, P6 est blanc. 4. Au moins l'un des pixels P4, P6, P8 est blanc.	3'. Au moins l'un des pixels P4, P2, P8 est blanc. 4'. Au moins l'un des pixels P2, P6, P8 est blanc

Table 2 : Table des conditions à chaque itération

8.3.3 -Algorithme de Tohmé

Cet algorithme extrait de la figure originale un squelette composé de points inessentiels.

Définition : Un point p inessentiel a au moins un 0 dans son voisinage en 4-connexité. Mais ceci n'est pas suffisant. Il faut en plus que l'ensemble des 1 du voisinage en 8-connexité soit 8-connexe et l'ensemble des 0 du voisinage en 8-connexité soit 4-connexe.

Les 16 configurations suivantes sont un résumé de l'ensemble de toutes les configurations où p est inessentiel.

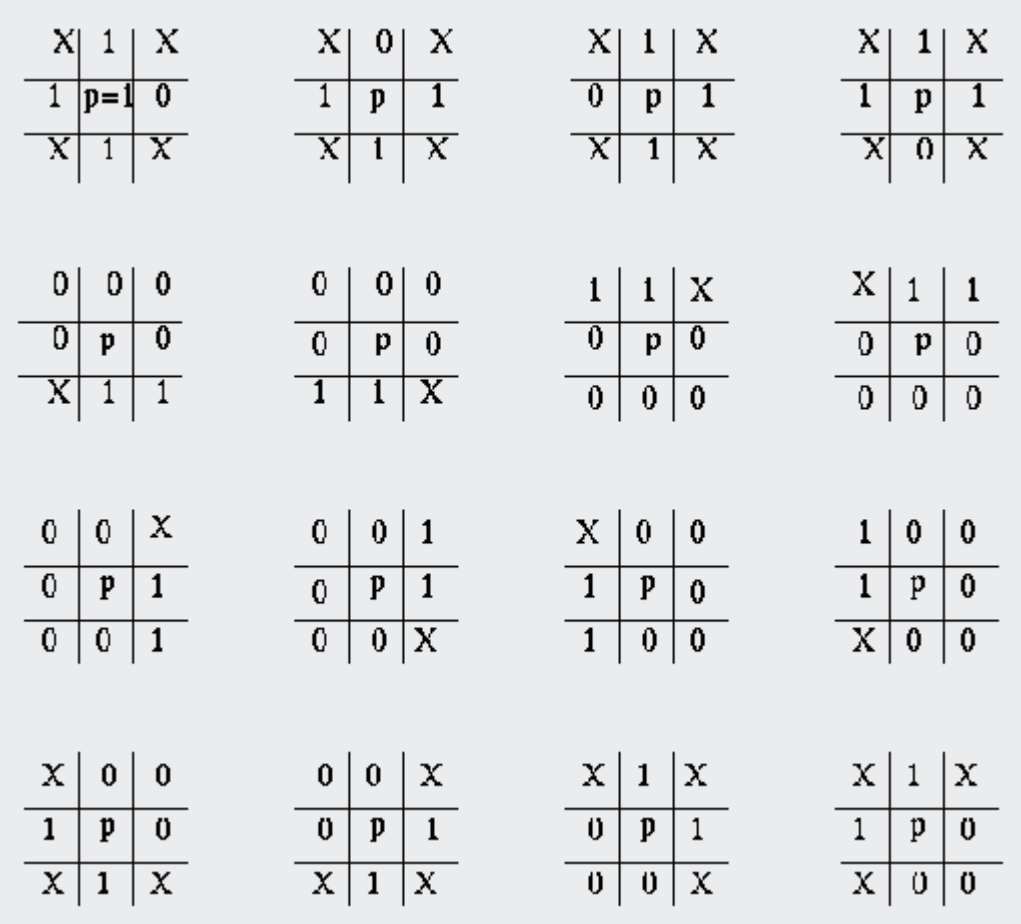


figure 18 : Ensemble des configurations de points inessentiels

La figure et son squelette sont c-équivalents. Rappelons que deux sous-ensembles sont c-équivalents si et seulement si ils ont le même nombre de composantes et le même nombre de trous.L'algorithme est de type parallèle, il supprime plusieurs points inessentiels à la fois.

8.4-Extraction des minuties :

C'est le processus final qui complète l'obtention de la "signature" de l'empreinte.

Les deux étapes de préparation à l'extraction (binarisation et squelettisation) ont grandement facilité cette phase.

A partir d'une image de l'empreinte préalablement traitée, on extrait grâce à différents algorithmes une structure de données (ou signature).

La caractérisation de l'empreinte est basée sur un ensemble suffisant et fiable de minuties, On entend par suffisant, le nombre minimum de minuties nécessaires pour pouvoir établir des comparaisons fiables entre empreintes. Par expérience, ce minimum se situe à 14 minuties.

On entend par fiable, les minuties qui ne sont pas influencées par des défauts lors de l'acquisition de l'image ou par l'altération temporaire de l'empreinte digitale (blessure, érosion, etc.).

Avec un petit nombre de minuties (15 ou 20) correctement localisées, il est possible d'identifier une empreinte parmi plusieurs millions d'exemplaires.[10]

Algorithme :

Pour chaque pixel I(i,j), on traite un fenêtre de 3 x 3 autour de (i,j), cinq cas différents sont reconnus :

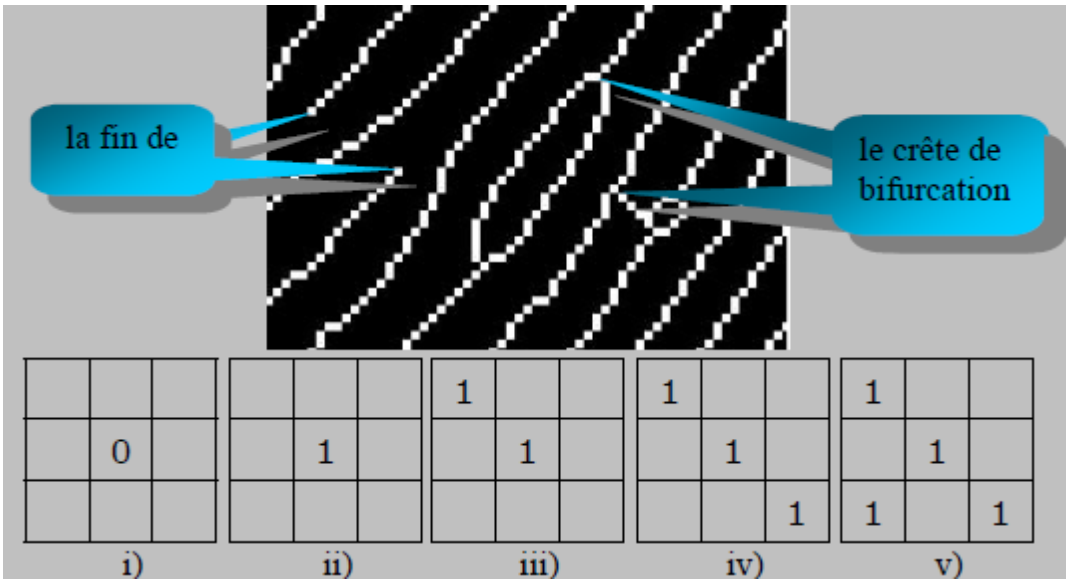


Figure 19: Type de minuties

i. I(i,j) = 0, c'est le fond d'empreinte digitale.

ii. I(i,j) =1 et aucune crête voisine. C'est une île (marquer pour minutie).

iii. I(i,j) = 1 et une seule crête voisine. C'est un pixel à la fin de ligne (marquer pour une minutie).

iv. I(i,j) =1 et deux crêtes voisines. C'est une ligne continue et pas de minutie. Donc, on supprime cette crête.

v. I(i,j)=1 et trois crêtes voisines. C'est une crête de bifurcation (marquer pour une minutie).

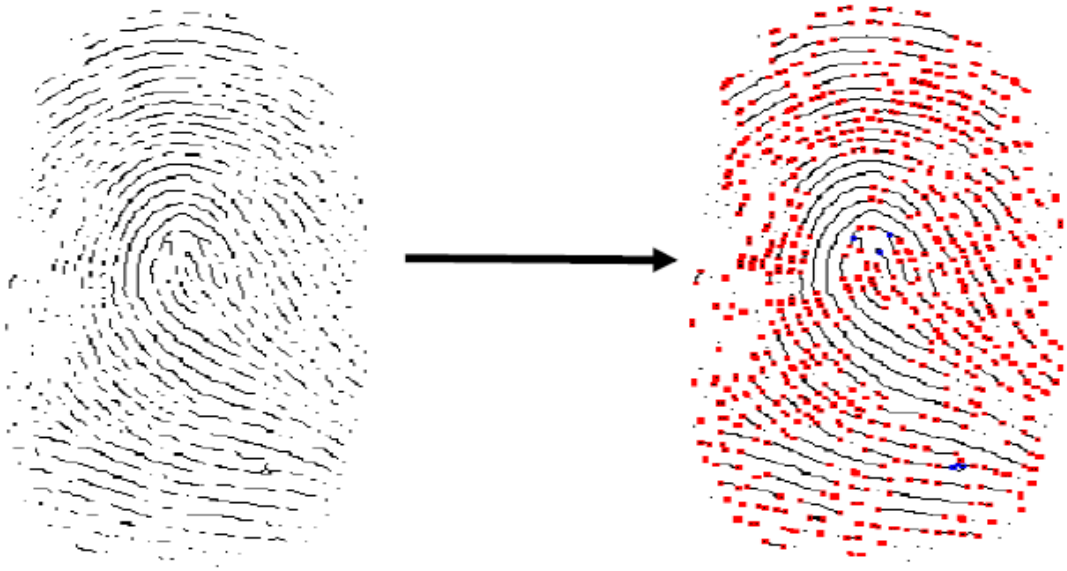


Figure 20 : Extraction des minuties

8.5 - Comparaison et prise de décision :

Le système de vérification d'identité est basé sur la comparaison de deux ensembles de minuties, correspondants respectivement à deux doigts à comparer. Pour déterminer si deux ensembles de minuties extraits de deux images correspondent à des empreintes du même doigt, il est nécessaire d'adopter un système de comparaison qui soit insensible à d'éventuelles translations, rotations et déformations qui affectent systématiquement les empreintes digitales. A partir de deux ensembles de minuties extraites, le système est capable de donner un indice de similitude ou de correspondance qui vaut :

- 0 % si les empreintes sont totalement différentes.
- 100 % si les empreintes viennent de la même image. [10]

9-Conclusion :

La biométrie par l'empreinte digitale est la technologie la plus employée à travers le monde. On voit fleurir des solutions de plus en plus abordables et performantes. D'ici quelques années, les lecteurs d'empreintes digitales n'étonneront plus personne et seront rentrés dans les mœurs au même titre que le téléphone portable.

Chapitre IV : Implémentation

1.Introduction :

L'Implémentation est la dernière étape dans ce travail, elle est l'étape la plus importante pour atteindre l'objectif voulu qui est la réalisation des fonctionnalités présentés dans notre application. Pour obtenir le succès il faudra regrouper plusieurs facteurs majeurs comme les logiciels utilisés dans travail est le langage de programmations ….

Dans ce dernier chapitre, nous présentons les différentes étapes réalisées durant le développement de notre application.

2.Description du projet :

Ce projet consiste à concevoir, développer et tester un système d'identification biométrique « une empreinte digitale ». Cette plateforme doit permettre plusieurs choses à un utilisateur :

- ✓ prendre l'empreinte d'un individu.
- ✓ la traiter et la sauvegarder dans une Base De Données sous format numérique.
- ✓ pouvoir comparer une empreinte avec celles qui sont dans la BDD.
- ✓ identifier l'individu à partir de son empreinte.

3 .La mise en œuvre du système :

Après la présentation de l'architecture de notre système nous allons, dans ce qui suit, décrire les différents aspects techniques liés à l'implémentation et le déploiement de notre Project.

Pour mener à bien notre travail, nous avons fait appel à une panoplie d'outils et langages de développement permettant la réalisation et la mise en œuvre de notre application. Nous tenons à les présenter tout en argumentant nos choix avant d'entamer la description de notre système.

3.1. Développement et environnement :

3.1.1. Langage JAVA : Notre choix du langage de programmation s'est porté sur le langage JAVA et cela pour diverses raisons :

- ✓ JAVA est un langage orienté objet simple ce qui réduit les risques d'incohérence.

- ✓ JAVA est portable. Il peut être utilisé sous Windows, sur Macintosh et sur d'autres plates-formes sans aucune modification. JAVA est donc un langage multiplateforme, ce qui permet aux développeurs d'écrire un code qu'ils peuvent exécuter dans tous les environnements.
- ✓ JAVA possède une riche bibliothèque de classes comprenant des fonctions diverses telles que les fonctions standards, le système de gestion de fichiers, les fonctions multimédia et beaucoup d'autres fonctionnalités.

3.1.2 NetBeans:

NetBeans est un environnement de développement intégré (EDI), placé en open source par Sun en juin 2000 sous licence CDDL (Common Development and Distribution License) et GPLv2. En plus de Java, NetBeans permet également de supporter différents autres langages, comme C, C++, JavaScript, XML, Groovy, PHP et HTML .Il comprend toutes les caractéristiques d'un IDE moderne (éditeur en couleur, projets multi-langage, refactoring, éditeur graphique d'interfaces et de pages Web).

Conçu en Java, NetBeans est disponible sous Windows, Linux, Solaris (sur x86 et SPARC), Mac OS X ou sous une version indépendante des systèmes d'exploitation (requérant une machine virtuelle Java). Un environnement Java Development Kit JDK est requis pour les développements en Java.

NetBeans constitue par ailleurs une plate forme qui permet le développement d'applications spécifiques (bibliothèque Swing (Java)). L'IDE NetBeans s'appuie sur cette plate forme.

3.1.3.L'environnement matériel :

Pour développer cette application nous avons utilisé une machine configurée comme suit :

- Pc portable lenovo
- Mémoire Vive : 4 Go.
- Disque Dur : 500 Go.
- Processeur : Intel (R) dual-Core (TM) I 3 GHz.
- Type de système : Windows 7

3.2. L'implémentation du système :

Nous commençons par l'implémentation des différentes parties de notre système, ensuite les tests et les résultats.

3.2.1 Présentation de l'interface :

Notre prototype est constitué de la représentation de traitement d'image en utilisant : les opérateurs de filtrage (graissage, seuillage, squelettisation) pour simplifier au maximum l'empreinte digitale puis une vérification dans les fichiers de l'existence de l'empreinte traitée.

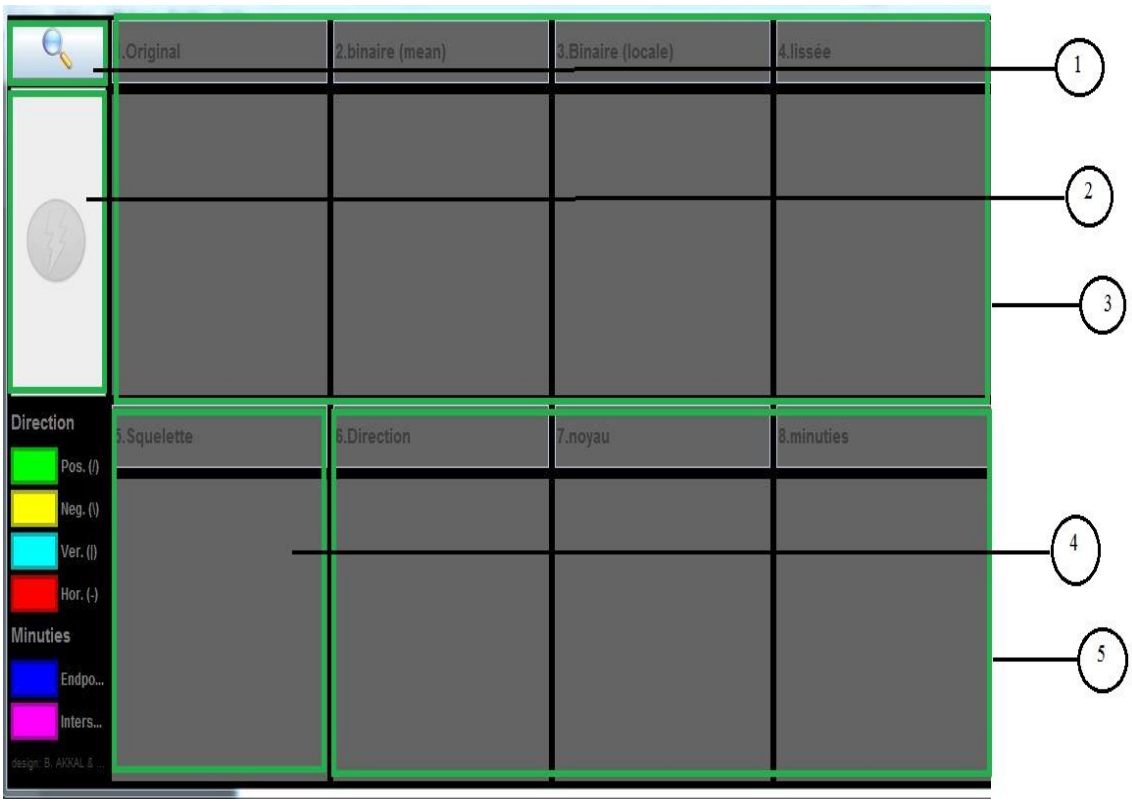


Figure 1 : Fenêtre d'accueil de l'application

3.2.1.1 Sélection de l'empreinte digitale :

La 1ère étape de fonctionnement de l'application consiste à sélectionner une empreinte digitale à partir de la base de données qui contient des images des empreintes. Pour cela, on clique sur le bouton qui se trouve dans la zone (1)

La fenêtre suivante nous permet de choisir l'image à sélectionner :

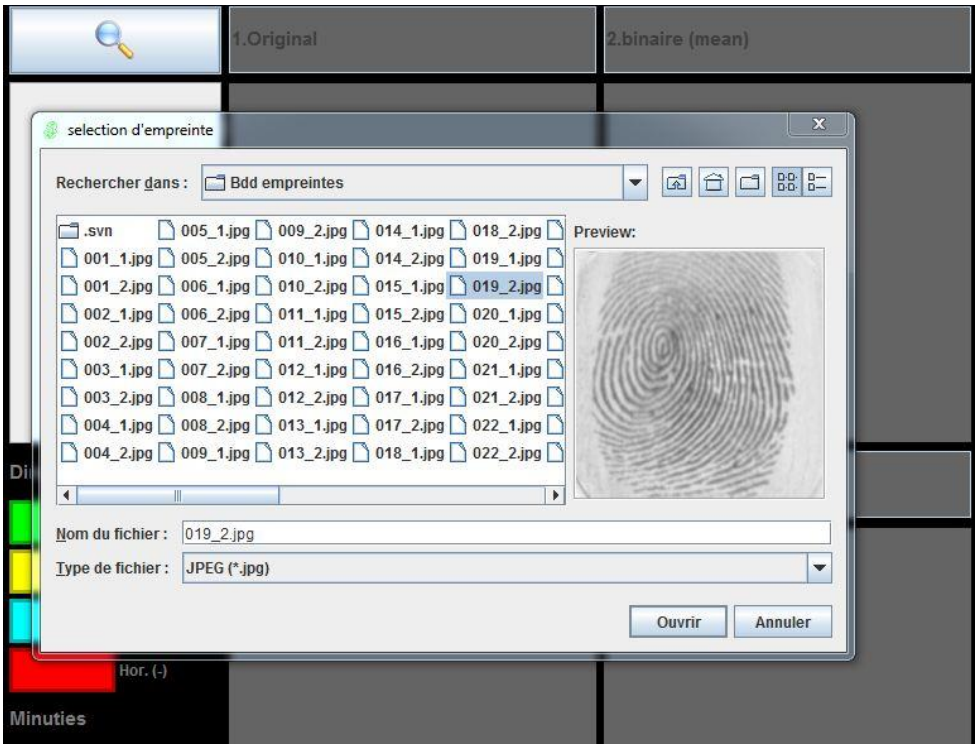


Figure 2: sélection d'une empreinte digitale

3.2.1.2 Les opérations de filtrage:

Le filtrage de l'image de l'empreinte est effectué par un ensemble d'algorithmes développés en NetBeans. Pour cela, on clique sur le bouton qui se trouve dans la zone (2)

Dans l'étape de binarisation qui affiche ses résultats dans la zone (3) plusieurs méthodes sont appliquées :

A. Transformation en niveaux de gris: Pour obtenir un niveau de gris, il faut que les trois valeurs (RVB) soient identiques.

La méthode la plus simple utilisée : $$Gris = \frac{Rouge + Vert + Bleu}{3}$$

B. Binairisation de l'image: Le filtre moyen est un filtre spatial à fenêtre glissante simple qui remplace la valeur centrale de la fenêtre avec la valeur moyenne (moyenne) de toutes les valeurs de pixels dans la fenêtre. La fenêtre, ou le noyau, est généralement carrée.

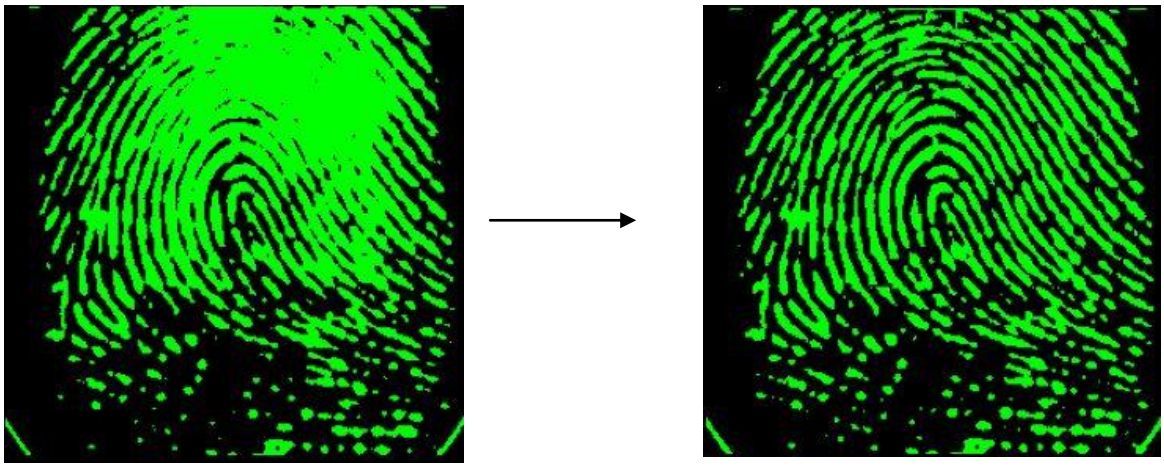


Figure 3 : Binarisation de l'empreinte

3.2.1.3 Segmentation (squelettisation) :

Dans l'étape précédente, les lignes de l'image binarisée se voient clairement mais elles ont des tailles différentes. Pour pouvoir détecter rapidement les minuties (terminaisons, bifurcations), il est nécessaire d'obtenir une image plus schématique de l'empreinte, dans laquelle toutes les lignes ont la même épaisseur (1 pixel).

Donc pour finir le prétraitement de l'image d'empreinte digitale, on réalise une squelettisation qui s'affiche dans la zone (4) pour cela on a utilisé l'algorithme Zhang-Suen. Cet algorithme de squelettisation est une méthode parallèle qui signifie que la nouvelle valeur obtenue dépend uniquement de la valeur de l'itération précédente. Il est rapide et simple à mettre en œuvre.

L'algorithme Zhang-Suen :

Soit *Pi, i=1..8* les voisins di pixel *p*;

Soit la fonction de voisinage V définit comme suite:

$$V(p) = \sum_{i=1}^{8} p_i$$

Soit **T** une fonction de transition de **0** à **1** dans le sens de l'horloge, elle est définit comme suite:

$$T(p) = \sum_{i=1}^{8} \begin{cases} 1, & si\,(p_i = 0\ et\ p_{i+1} = 0) \\ 0, & sinon \end{cases}$$

Sachant que *: P9=P1*

Algo.Zhang-Suen
Etape1: **passe 1:** **pour** chaque pixel *P* dans l'image faire 1-calculer **V** et **T** 2-**si** une condition de ces 4 suivantes n'est pas satisfaite pour *P*: marque *P* cond1: 2 <=V(p)<= 6 cond2: T(P)=1 cond3: P2*P4*P6=0 cond4: P4*P6*P8=0 **fin pour** Elimine tous les point marqué (P<-0) **passe 2:** **pour** chaque pixel *P* dans l'image faire 1-calculer **V** et **T** 2-**si** une condition de ces 4 suivantes n'est pas satisfaites pour *P*: marque *P* cond1: 2 <=V(p)<= 6 cond2: T(P)=1 cond3: P2*P4*P8=0 cond4: P2*P6*P8=0 **fin pour** Elimine tous les point marqué (P<-0) **étape 2** répéter **l'étape 1** jusqu'a ce qu'on a plus de pixel à éliminer

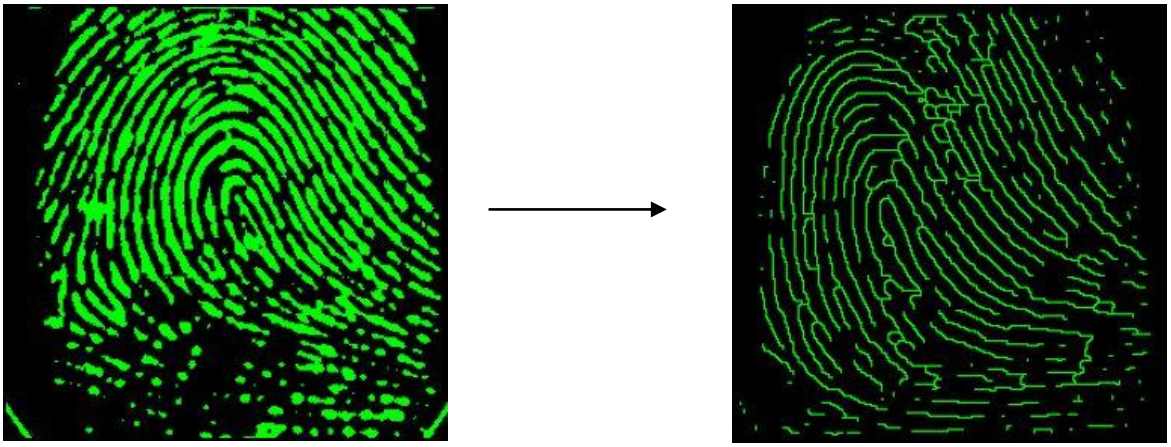


Figure 4 : squelettisation de l'empreinte

3.2.1.4 Extraction des points et recherche dans la BDD:

Extraction des minuties : Dans ce projet, nous distinguons une minutie comme l'un des deux types, une terminaison de crête ou d'une bifurcation.

Nous utilisons une fenêtre de 3 x 3 à balayer l'image amincie pour calculer un nombre de passage. En fonction de la valeur du numéro de passage, il identifie un point comme étant soit une terminaison d'arête, une bifurcation, ou rien. Le calcul du nombre de passage et d'identification est indiqué ci - dessous:

1- En calculant la «connectivité » CN en chaque point de l'image de la manière suivante

$$CN = 0.5\sum_{i=1}^{8}|P_i - P_{i+1}|, \qquad P_9 = P_1$$

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

P9 = P1, Pi est la valeur des pixels dans le voisinage 3*3 de P

En effet le coefficient CN présente des caractéristiques qui permettent d'identifier la nature d'une minutie en fonction du résultat obtenu lors du calcul de CN.

CN	Property
0	Isolated point
1	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

Figure 5 : formule Nombre Traversant et l'identification des minuties

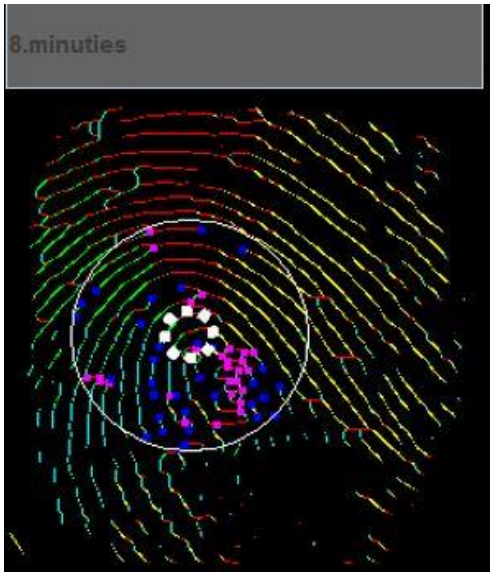


Figure 6 : Extraction des minuties

Après l'extraction des points minuties, si l'empreinte digitale est déjà enregistrée dans la base de données, on affiche les caractéristique de la personne correspondante (ID, Nom, Prénom).

Figure 7 : Mini-Fiche d'authentification de la personne

Sinon on demande un enregistrement dans la BDD, un ID sera attribué automatiquement.

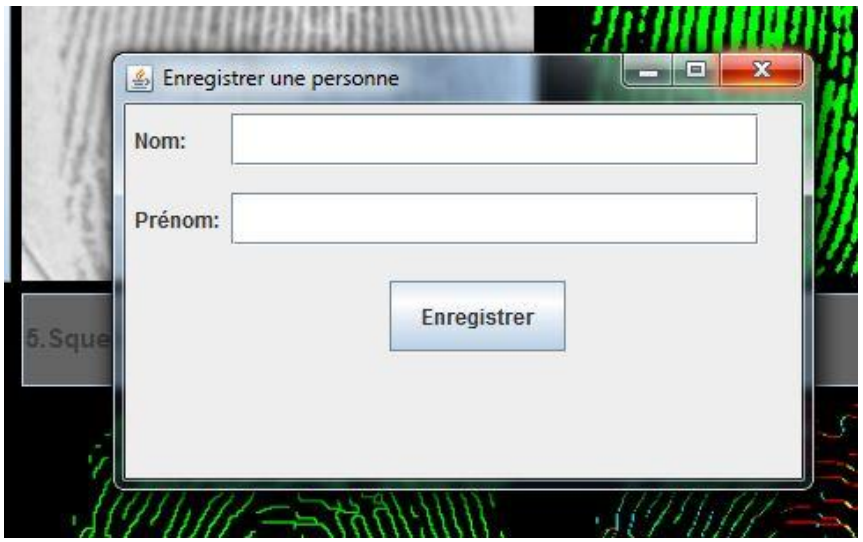


Figure 8 : Formulaire d'enregistrement de la personne

Algo .proposé pour la comparaison des empreints
Input : Emp: tableau de pixel Inter, termi :tableau de pixel Début Traiter (emp); Inter= extraire-inter( ) ; Termi= extraire-termi( ); Comparer (termi,inter,bdd); Si termi existe et inter existe alors Afficher nom-personne( ); Sinon Enregistrer-nouvelle (inter,termi); Fin si; Fin.

4.Conclusion :

Pour conclure, il nous semble opportun de dire que mener ce projet de bout en bout fut extrêmement enrichissant. Cela nous a permis de nous rendre compte de la réalité des entreprises qui produisent des logiciels de ce type, à petite échelle, certes.

C'est également la première fois que nous travaillons sur un projet aussi «Important » en termes d'investissement et de contenu, et il est difficile de comparer une telle expérience aux projets que nous avions menés jusqu'ici.

Conclusion Générale

Conclusion Générale

Actuellement, la reconnaissance des empreintes digitales est la branche la plus exploitée de la biométrie.

Les systèmes de reconnaissance des empreintes digitales sont utilisés dans plusieurs applications dont nous nous servons quotidiennement (sécuriser l'accès à un ordinateur, à une clé USB, l'entrée d'un établissement. . .), et dans le domaine anticriminel

Dans ce mémoire, nous nous sommes intéressés au problème de l'identification par une reconnaissance biométrique « des empreintes digitales ». Nous avons souligné durant ce travail les principales difficultés rencontrées lors de la reconnaissance des empreintes digitales, et dont nous avons proposé quelques solutions qui ont été évaluées durant la phase de test.

Aussi, au cours de ce mémoire, nous avons présenté les différentes étapes de la conception et la réalisation de notre application, et approcher les différentes méthodes de traitement d'images.

Ainsi, avec ce modeste travail, on estime avoir réalisé un système d'identification qui répond à l'objectif que nous nous sommes fixés au départ.

En guise de perspectives, ce travail peut être réalisé avec d'autres algorithmes et d'autres approches ce qui permettra à l'avenir de faire des comparaisons et de faire un choix du système le mieux adapté en termes de coûts et de performances.

Chapitre 2 : La biométrie

Chapitre 3 : L'empreinte Digitale

Liste de Figures

Chapitre 4 : Implémentation

Bibliographie :

Chapitre I

[1] « Authentication » par Richard Smith (Edition Addison Wesley)
[2] "Sécuriser ses échanges électroniques avec une PKI - Solutions techniques et aspects juridiques" par Thierry Autret, Marie-Laure Oble Laffaire et Laurent Bellefin (Edition Eyrolles).
[3]Article « Smart card vs. Password » disponible sur http://www.scmagazine.com/scmagazine/2003_09/feature_1 (2eme article de la page)

Chapitre II

[1] https://www.securiteinfo.com/conseils/biometrie.shtml

[2] http://biometrie-tpe68.e-monsite.com/pages/introduction/historique.html

[3]http://policescientifique-role21.e-monsite.com/pages/content/empreintes digitales

[4]http://www.citesciences.fr/archives/francais/ala_cite/expositions/biometrie/nonvoyants/ programme_details_3_1.htm

[5]https://investigationderrierelescrimes.wordpress.com/2013/12/18/lebertillonnage-technique-scientifique/

[6] http://www.biometrie-online.net/biometrie/histoire

[7] https://investigationderrierelescrimes.wordpress.com/2013/12/18/lebertillonnage-technique-scientifique/

[8] http://biometrie-tpe68.e-monsite.com/pages/introduction/historique.html

[9] http://biometrics.over-blog.com/pages/La_geometrie_de_la_main-2019729.html

[10] https://hal.archives-ouvertes.fr/hal-00091740/document

[11]http://www.linternaute.com/science/biologie/dossiers/06/0607biometrie/visage.shtml

[12] http://www.nedap.fr/contenu/biomtrie/autres-technologies/253/434/

[13] https://www.priv.gc.ca/information/research-recherche/2013/fr_201303_f.pdf

[14] http://www.biometrie-online.net/technologies/iris

[15]http://www.linternaute.com/science/biologie/dossiers/06/0607biometrie/iris.shtml

[16] http://www.biometrie-online.net/technologies/voix

[17] http://www.ldh-france.org/IMG/pdf/5.pdf

[18] Marshal Mandelkern, John G. Elias, Don Eden et Donald M. Crothers, « The dimensions of DNA in solution », Journal of Molecular Biology, vol. 152, no 1, 15 octobre 1981, p. 153-161

[19] http://www.biometrie-online.net/biometrie/le-marche / biometricgroup.com

Chapitre III

[1] Hueske, Edward. Firearms and Fingerprints. Facts on File/Infobase Publishing, New York. 2009.

[2]http://www.police-scientifique.com/specialites/empreintes-digitales-et-traces-papillaires/

[3] http://www.crimescene-forensics.com/Fingerprints.html

[4] IDENTIFICATION OF CORE AND DELTA POINTS IN FINGERPRINT IMAGES.

http://www.mva-org.jp/Proceedings/CommemorativeDVD/1990/papers/1990263.pdf

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

[6] http://la-police-scientifique.e-monsite.com/pages/iii-identifier-le-suspect-grace-aux-empreintes/3-techniques-de-revelation-d-une-empreinte-digitale-et-experience.html

[7] http://www.biometrie-online.net/technologies/empreintes-digitales

[8] Handbook of fingerprint recongnition (second edition) crée par davide maltoni

[9] Afsar, F. A., M. Arif, and M. Hussain. “Fingerprint identification and verification system using minutiae matching.” National Conference on Emerging Technologies. 2004.

[10] http://documents.irevues.inist.fr/bitstream/handle/2042/13225/PAPER023.pdf

[11] N. GALY, " Etude de système complet de reconnaissance d’empreintes digitales pour un capteur microsystème à balayage", Thèse de Doctorat, InstitutNational Polytechnique de GRENOBLE, 2005.

[12] N. Otsu, A threshold selection method from grey scale histogram, IEEE Trans. on Syst. Man and Cyber., vol 1, pp 62-66, 1979

[13]F.Jaam, M.Rebaiaia et A.Hasnah. "A Fingerprint Minutiae Recognition System Based on Genetic Algorithms ". The Internationnal Arab Journal of Information Technology, Vol.3, No.3, pp.243-245, July 2006

[14] M. R. Gupta, N. P. Jacobson, E. K. Garcia, « OCR binarization and image preprocessing for searching historical documents », Pattern Recognition, 40, p. 389-397, 2007.