TABLE DES MATIERES

CHAPITRE III : RECONNAISSANCES DES EMPREINTES DIGITALES

CHAPITRE IV: CONCEPTION ET IMPLEMENTATION

Liste des figures

INTRODUCTION GENERALE

De nos jours, nous parlons de plus en plus de l'insécurité dans divers secteurs ainsi que des moyens informatiques à mettre en œuvre pour contrer cette tendance. La vérification et l'identification des individus est l'un des moyens permettant d'assurer cette sécurité.

L'être humain se sert quotidiennement de son système visuel pour identifier les personnes de façon automatique, bien que le processus mis en jeu soit complexe. l'homme a mis en place des moyens de vérification d'identité qui sont liés, soit à ce que possède une personne telle qu'une carte d'identité ou un passeport, soit à ce que sait cette personne, c'est le cas du mot de passe ou un code PIN. Néanmoins, ces éléments peuvent être oubliés, volés ou falsifiés ; Pour contourner ces limitations, un autre moyen de sécurité a été développé. Ce nouveau moyen permet d'utiliser, non pas l'information qu'un individu possède ou connaît, mais une information propre a cette personne qui le caractérise. Cette nouvelle façon d'identification des individus s'appelle la biométrie.

La biométrie est une solution alternative aux anciens moyens mesurables et uniques.
les caractéristiques biométriques sont uniques (deux personnes ne peuvent pas posséder exactement les mêmes caractéristiques). Ces caractéristiques sont aussi permanentes ce qui signifie qu'elles ne varient pas ou très peu au cours du temps. Pour que des caractéristiques collectées puissent être qualifiés de modalités biométriques, elles doivent être :

- universelles (exister chez tous les individus).
- uniques (permettre de différencier un individu par rapport à un autre).
- permanentes (autoriser l'évolution dans le temps).
- enregistrables (collecter les caractéristiques d'un individu avec son accord).
- mesurables (autoriser une comparaison future).

L'intérêt principal de la biométrie est de reconnaître et d'identifier automatiquement les identités des individus en utilisant leurs caractéristiques physiologiques ou comportementales.

CHAPITRE I : LA BIOMETRIE

I.1 Introduction

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 de grandes masses de données qui ont permis la création et le développement des systèmes biométriques. L'être humain possède plusieurs caractéristiques physiques qui le différencie des autres individus, ce qui explique la diversité des systèmes biométriques, ainsi nous pouvons citer :

- Empreinte digitale
- Forme de la main ou des doigts de la main
- Rétine de l'œil
- Iris de l'œil
- la voix
- Forme des veines de la main
- ADN
- cheveux et poils

En ce qui concerne les applications, l'authentification de l'utilisateur est utilisée dans tous les domaines nécessitant un accès contrôlé : les applications bancaires, les endroits hautement sécurisés comme les sièges de gouvernement, et Internet. Quant à la reconnaissance, elle est souvent utilisée par la police et les services d'immigration dans les aéroports, ainsi que dans la recherche dans la base de données criminelles . Elle figure aussi dans les applications civiles où l'authentification des cartes de crédit, de permis de conduire et des passeports est de plus en plus courante. Nous pouvons dire que notre identité est vérifiée quotidiennement par de multiples organisations : lorsque nous accédons à notre lieu de travail, lorsque nous utilisons notre carte bancaire, lorsque nous nous connectons à un réseau informatique, etc.

Il existe traditionnellement deux manières d'identifier un individu :

- La première se fait à partir d'une connaissance qui correspond à un mot de passe ou un code qui permet d'activer un appareil numérique.
- La deuxième est effectuée grâce à une possession, il peut s'agir d'une pièce d'identité, d'une clef, d'un badge.

La biométrie est une alternative à ces deux modes d'identification, elle consiste à identifier un individu à partir de ses caractéristiques physiques et comportementales.

Nous consacrons ce chapitre à la présentation de la biométrie comme moyen de sécurité dans les systèmes d'information et leur caractéristiques ainsi que le champ d'application de cette nouvelle technique.

I.2 Définition

La biométrie peut être définie comme étant « la reconnaissance automatique d'une personne en utilisant des traits distinctifs ».

La biométrie peut regrouper « toutes les caractéristiques physiques ou traits personnels automatiquement mesurables, robustes et distinctives qui peuvent être utilisées pour identifier un individu ou pour vérifier l'identité prétendue d'un individu »[1].

La biométrie consiste en l'analyse mathématique des caractéristiques biologiques d'une personne, elle a pour objectif de déterminer son identité de manière claire .

Contrairement à ce que l'on sait ou ce que l'on possède la biométrie est basée sur ce que l'on est et elle permet ainsi d'éviter la duplication, le vol, l'oubli ou la perte[3].

I.3 Les systèmes biométriques

I.3.1 Définition

Un système de reconnaissance d'individus est un système biométrique qui permet l'identification d'une personne sur la base de caractères physiologiques ou de traits comportementaux automatiquement reconnaissables et vérifiables.

La biométrie utilise les caractéristiques physiques de certaines parties du corps humain. On trouve parmi les plus courantes :

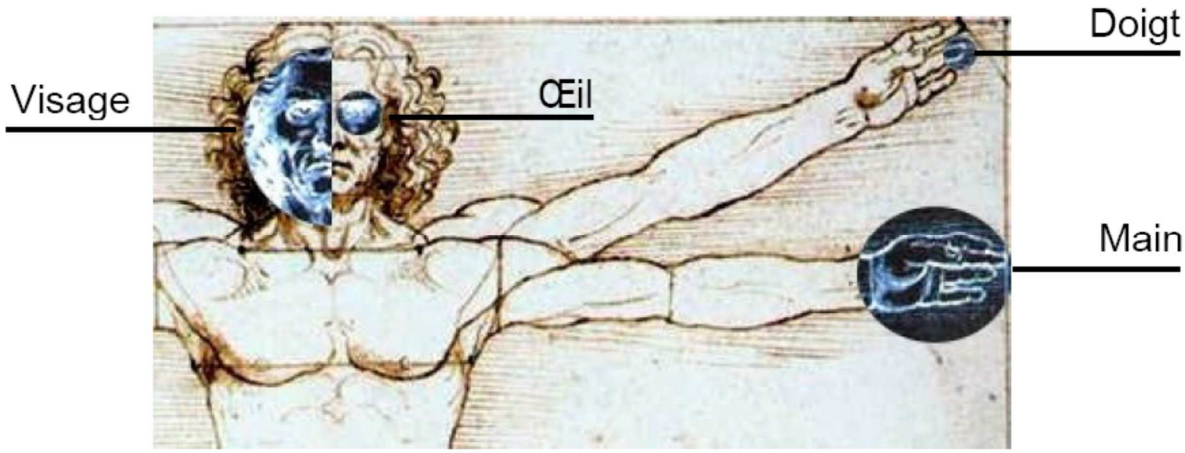

Figure I.1 Les caractéristiques physiques utilisé en biométrie.

Quel que soit le mode de reconnaissance ,la technique utilisée reste la même :

1- Un capteur prend « une image » de la caractéristique .

2- L'image est ensuite analysée par un logiciel de traitement d'image qui repère les points caractéristiques.

3- L'ensemble de ces données est traité par un algorithme puis transformé en un code unique.

4-Ce code sera délivré par le lecteur biométrique à l'unité de contrôle d'accès auquel il est raccordé.

On peut définir deux modes de fonctionnement d'un système biométrique[2] :

I.3.2Identification

L'identification consiste à déterminer l'identité de la personne qui se présente en recherchant l'échantillon biométrique fourni par cette personne avec une liste d'échantillons existants déjà. Il s'agit de la réponse à la question « Qui suis-je ? ». La figure 2 représente un schéma explicatif de l'identification.

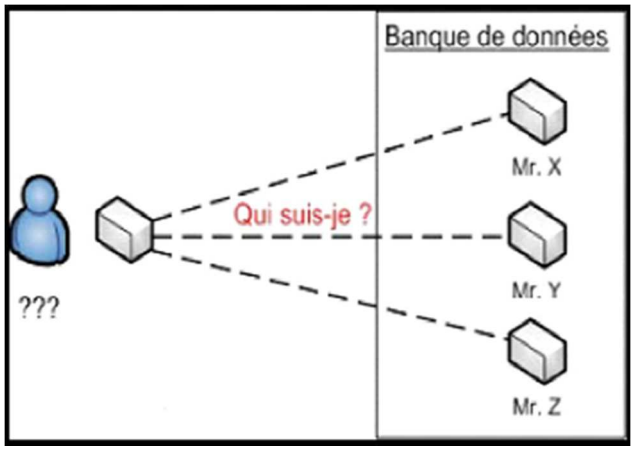

Figure I.2 Schéma explicatif de l'identification d'un individu.

L'action d'identification est la même que lorsque l'on renseigne son login dans un système login/password. Le système va rechercher les informations concernant ce login dans sa base de références.

I.3.3Authentification

L'authentification consiste à vérifier que la personne qui se présente est bien la personne qu'elle prétend être. Pour cela, la personne donne son identité et fournit un échantillon biométrique. Cet échantillon est comparé avec un échantillon biométrique propre à cette personne fourni antérieurement. Si les deux échantillons coïncident, avec une marge d'erreur prédéfinie, la personne est authentifiée. Il s'agit de la réponse à la question « Suis-je bien Mr X ? ». La figure 3 représente un schéma explicatif de l'authentification.

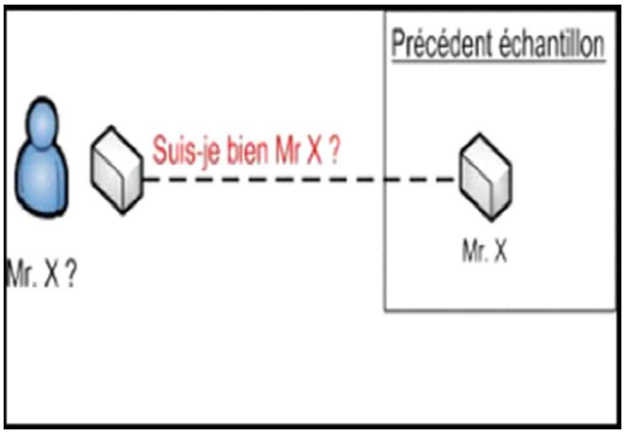

Figure I.3 Schéma explicatif de l'authentification d'un individu.

L'action d'authentification est la même que lorsque l'on procède à la vérification du mot de passe dans un système login/ password. Après s'être identifié, on s'authentifie par un mot de passe que le système compare à celui qu'il possède dans sa base de références.

I.4Architecture générale d'un système biométrique

I.4.1Définition

Un système biométrique est un système de reconnaissance de formes qui procède en premier par l'acquisition des données biométriques de l'individu à reconnaître , puis extrait un ensemble de caractéristiques à partir de celles-ci , enfin il compare ces caractéristiques avec les modèles de la base de données. Selon le contexte de l'application, un système biométrique peut fonctionner soit en mode vérification ou d'identification [1]. Tout système biométrique comporte deux processus qui se chargent de réaliser les opérations d'enregistrement et de tests:

- Processus d'enregistrement : Ce processus a pour but d'enregistrer les caractéristiques des utilisateurs dans la base de données.
- Processus de tests (identification /vérification): Ce processus réalise l'identification ou la vérification d'une personne. Dans chacun des deux processus précédents le système exécute quatre opérations fondamentales, à savoir:

  - **L'acquisition**

On utilise un système d'acquisition pourvu d'un capteur pour acquérir une caractéristique spécifique de l'individu, par exemple: un microphone dans le cas de la voix.

  - **L'extraction**

Après avoir fait l'acquisition d'une image ou d'une voix, on réalise l'extraction de la caractéristique dont le processus d'authentification a besoin. Par exemple: extraire le visage du fond d'une image dans le cas de l'identification de visage.

- **La classification**

En examinant les modèles stockés dans la base de données, le système collecte un certain nombre de modèles qui ressemblent le plus à celui de la personne à identifier, et constitue une liste limitée de candidats. Cette classification intervient uniquement dans le cas d'identification car l'authentification ne retient qu'un seul modèle (celui de la personne proclamée).

- **La décision**

En ce qui concerne l'authentification, la stratégie de décision nous permet de choisir entre les deux alternatives suivantes: l'identité de l'utilisateur correspond à l'identité proclamée ou recherchée ou elle ne correspond pas. Elle est basée sur un seuil prédéfini. L'estimation du seuil de la décision constitue la plus grande difficulté de ces techniques, et elle peut engendrer deux types d'erreurs, souvent prises comme mesures de performances pour ces techniques d'authentification: faux rejet (FR) qui correspond à rejeter un vrai utilisateur ou une identité valable, et fausse acceptation (FA) qui donne accès à un imposteur.

I.4.2 Mode de fonctionnement

Tout système biométrique fonctionne soit en mode vérification ou en mode d'identification. En mode vérification, le système vérifie l'identité d'une personne en comparant les données biométriques acquises avec celles stockées dans la base de données. Dans un tel système, la personne revendique une identité, généralement via un code PIN (Personal Identification Number), un nom d'utilisateur, une carte à puce, etc. Le système effectue alors une comparaison afin de déterminer si la déclaration est correcte ou fausse.

La vérification de l'identité est généralement utilisée pour empêcher que plusieurs personnes n'utilisent la même identité. En mode identification, le système cherche à reconnaître un individu en comparant son modèle avec tous les modèles existant dans la base de données pour une éventuelle correspondance. Par conséquent, le système effectue une comparaison, du modèle de la personne, avec plusieurs modèles pour établir son identité. Ici l'individu n'a pas à revendiquer une identité. L'identification de l'identité est généralement utilisée pour empêcher qu'une personne n'utilise plusieurs identités[2].

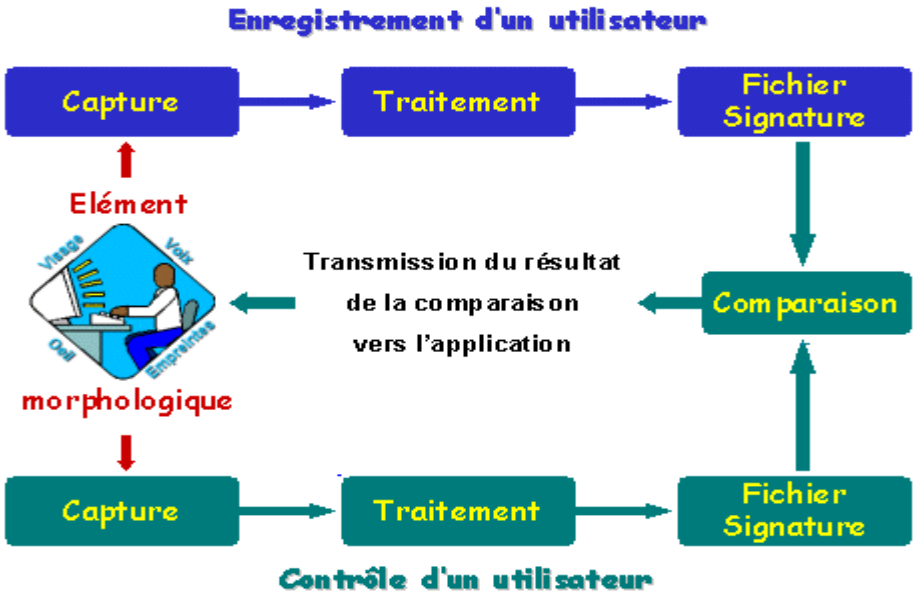

Figure I.4 Architecture d'un système biométrique.

I-5 Evaluation de performance

La performance d'un système d'identification peut se mesurer principalement à l' aide de trois critères :

- La précision.
- L'efficacité (vitesse d'exécution).
- Le volume de données qui doit être stocké pour chaque individu.

L' identification et la vérification sont des modes opératoires différents, elles nécessitent donc des mesures de précision différentes[14].

I.5.1 Evaluation de l'identification

Le taux d'identification est la mesure la plus couramment utilisée mais il n'est pas toujours suffisant. En effet, en cas d'erreur, il peut être utile de savoir si le bon choix se trouve dans les N premiers. On trace alors le score cumulé (cumulative match score) qui représente la probabilité que le bon choix se trouve parmi les N premiers [6]. Dans le cas où il existe plusieurs modèles pour chaque individu dans la base de données, les mesures classiques des systèmes de recherche dans une base de données (data base retrie val system) peuvent être utilisées. La précision est le rapport entre le nombre de modèles correctement retrouvés par le système dans la base de données et le nombre total de modèles retrouvés. Le rappel (recall) est le rapport entre le nombre de modèles correctement retrouvés dans la base de données et le nombre total de modèles qui auraient dû être retrouvées.

I.5.2 Evaluation de la vérification

Lorsqu'un système fonctionne en mode vérification, celui-ci peut faire deux types d'erreurs. Il peut rejeter un utilisateur légitime et dans ce premier cas on parle de faux rejet(false rejection). Il peut aussi accepter un imposteur et on parle dans ce second cas de fausse acceptation (false acceptance). La performance d'un système se mesure donc à son taux de faux rejet (False Rejection Rate ou FRR) et a son taux de fausse acceptation (False Acceptance Rate ou FAR).

La vérification est un problème de décision similaire à la détection d'un signal dans le bruit en théorie de l'information. Il peut être formulé de la manière suivante. Soient H_0 l'hypothèse : « la capture C provient d'un imposteur » et H_1 l'hypothèse : « la capture C provient de l'utilisateur légitime ». Il faut donc choisir l'hypothèse la plus probable. On considère que la capture C provient d'un utilisateur légitime si : $P\left(\frac{H_1}{C}\right) > P\left(\frac{H_0}{C}\right)$

En appliquant la loi de Bayes on obtient : $\frac{P\left(\frac{H_1}{C}\right)P(H_1)}{P(C)} > \frac{P\left(\frac{H_0}{C}\right)P(H_0)}{P(C)}$

Ce qui implique : $\frac{P\left(\frac{C}{H_1}\right)}{P\left(\frac{C}{H_0}\right)} > \frac{P(H_0)}{P(H_1)}$

Le taux de vraisemblance $\frac{P\left(\frac{C}{H_1}\right)}{P\left(\frac{C}{H_0}\right)}$ est comparé à un seuil 0 appelé seuil de décision. Les valeurs $P(H_0)$ et $P(H_1)$ qui représentent respectivement la probabilité pour qu'un imposteur ou un utilisateur légitime essayent d'accéder au système sont des valeurs difficile à estimer.Nous avons représenté sur la figure 4, la distribution hypothétique des taux de Vraisemblance qu'obtiendraient les utilisateurs légitimes et les imposteurs d'un système de vérification donné. Les FAR et FRR sont représentés en hachuré. Idéalement, le système devrait avoir des FAR et FRR égaux à zéro. Comme ce n'est jamais le cas en pratique, il faut choisir un compromis entre FAR et FRR. Plus le seuil de décision 0 est bas, plus le système acceptera des utilisateurs légitimes mais plus il acceptera aussi des imposteurs. Inversement, plus le seuil de décision 0

est élevé, plus le système rejettera des imposteurs mais plus il rejettera aussi des utilisateurs légitimes.

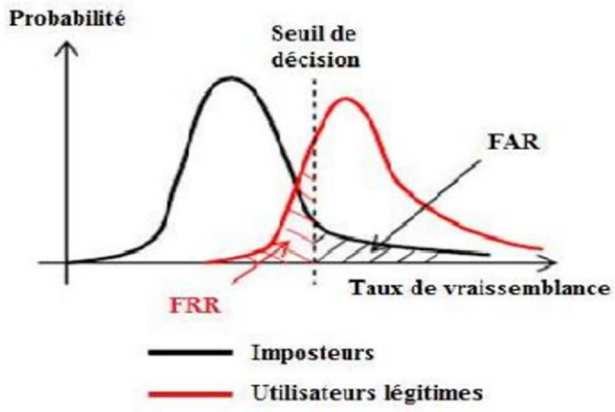

Figure I.5 Distributions du taux de vraisemblance des utilisateurs légitimes et imposteurs.

Il est donc impossible en faisant varier le seuil de décision de faire diminuer les deux types d'erreurs en même temps.

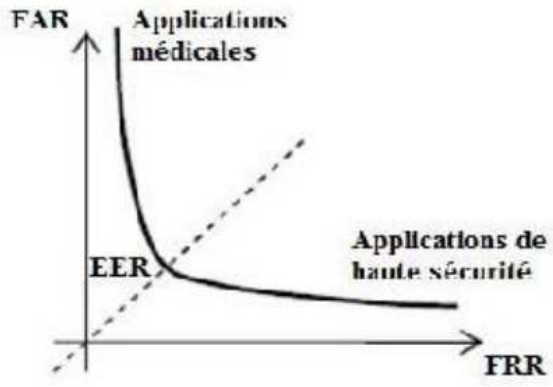

Figure I.6 Courbe ROC

La courbe dite ROC(Receiver Operating Characteristic), représentée sur la figure 5 permet de représenter graphiquement la performance d'un système de vérification pour les différentes valeurs de 0. Le taux d'erreur égal (Equal Error Rate ou EER) correspond au point FAR=FRR, c'est-à-dire graphiquement à l'intersection de la courbe ROC avec la première bissectrice. Il est fréquemment utilisé pour donner un aperçu de la performance d'un système. Cependant, il est important de souligner que l'EER ne résume en aucun cas toutes les caractéristiques d'un système biométrique.

Le seuil 0 doit donc être ajusté en fonction de l'application ciblée : haute sécurité, basse sécurité ou compromis entre les deux.

I.6 le champ d'application de la biométrie

L'authentification par la biométrie est utilisée dans tous les domaines nécessitant un accès contrôlé tels que celui des applications bancaires, les endroits hautement sécurisés comme les sièges du gouvernement, parlement, armée, service de sécurité etc. Quant à la reconnaissance, elle est souvent utilisée par la police et les services d'immigration dans les aéroports, ainsi que dans la recherche de bases de données criminelles. On la retrouve aussi dans les applications civiles où l'authentification des cartes de crédit, de permis de conduire et des passeports.

Parmi les applications pouvant utiliser la biométrie pour contrôler tout accès, nous citons :

- Contrôle d'accès physiques aux locaux : Salle informatique, site sensible (service de recherche, site nucléaire, bases militaires...).
- Contrôle d'accès logiques aux systèmes d'informations : Lancement du système d'exploitation, accès au réseau informatique, commerce électronique, transaction (financière pour les banques, données entre entreprises), tous les logiciels utilisant un mot de passe.
- Equipements de communication : Terminaux d'accès à internet, téléphones portables.
- Machines et Equipements divers : Coffre-fort avec serrure électronique, distributeur automatique de billets, contrôle des adhérents dans un club, carte de fidélité, gestion et contrôle des temps de présence, voiture (anti démarrage) etc.

Ces applications peuvent être divisées en trois classes:

- **Applications commerciales** : telles que l'ouverture de réseau informatique, la sécurité de données électroniques, l'e-commerce, l'accès Internet, la carte de crédit, le contrôle d'accès physique, le téléphone cellulaire, la gestion des registres médicaux, l'étude à distance, etc.

- **Applications gouvernementales** : telles que la carte d'identité nationale, le permis de conduire, la sécurité sociale, le contrôle des frontières, le contrôle des passeports, etc.

- **Applications légales (juridique)** : telles que l'identification de corps et l'identification de cadavre , la recherche criminelle ,l'identification de terroriste, etc.

Il existe plusieurs systèmes biométriques déployés afin d'assurer l'identification et la vérification des personnes. Parmi ces systèmes, nous citons le système biométrique« Schiphol Privium »qui est déployé au niveau de l'aéroport d'Amsterdam Schiphol, afin d'accélérer la procédure d'immigration. Ce système est basé sur la reconnaissance de l'iris en utilisant les cartes à puce. Les passagers, volontairement inscrits dans ce système, insèrent leur carte à puce à l'entrée et doivent se placer devant une caméra qui acquiert l'image de leur œil. Ensuite, un processus du système utilise cette image pour localiser l'iris et en extraire l'exemplaire correspondant. Enfin, ce dernier est comparé à celui enregistré dans la carte à puce afin de vérifier l'identité du passager [6].

Figure I.7 le champ d'application de la biométrie.

I.7 Conclusion

Dans ce chapitre nous avons présenté une vue générale de la biométrie et aussi nous avons introduit le concept de systèmes biométrique, son architecture et les différentes applications de la biométrie.

Nous avons aussi constaté que les performances des systèmes biométriques dépendent de plusieurs facteurs et qu'elles varient d'un système à un autre. Dans le chapitre qui suit, nous détaillerons les principales techniques biométriques.

CHAPITRE II: DESCRIPTION DES PRINCIPALES TECHNIQUES BIOMETRIQUES

II.1 Introduction

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 technique biométrie est utilisée dans une application particulière. Pour les caractéristiques Morphologiques (physiques), nous décrirons la reconnaissance de visage, les empreintes digitales, la géométrie de la main et l'iris et pour les caractéristiques comportementales, nous décrirons les biométries basées sur la voix et la signature et le rythme de frappe du clavier. Il existe d'autres méthodes biométriques (biologiques) basées sur les veines de la main, l'A.D.N, l'odeur corporelle, la forme de l'oreille, la forme des lèvres et la démarche.

II.2 Description des techniques

II.2.1 Techniques biométriques Morphologiques

Il existe plusieurs caractéristiques physiques qui se révèlent être uniques pour un individu :

a. Empreinte digitale :

La donnée de base dans le cas des empreintes digitales est le dessin représenté par les crêtes et sillons de l'épiderme. Ce dessin est unique et différent pour chaque individu. En pratique, il est quasiment impossible d'utiliser toutes les informations fournies par ce dessin (car trop nombreuses pour chaque individu), il est donc préférable d'extraire les caractéristiques principales telles que les bifurcations de crêtes, les lignes qui disparaissent, etc. 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. Pourtant, là encore, les produits proposés sur le marché ne se basent que sur une quinzaine de ces points (12 au minimum), voire moins pour beaucoup d'entre eux (jusqu'à 8 minimum), le nombre 12 provient de la règle des 12 points selon laquelle il est statistiquement impossible de trouver 2 individus présentant les mêmes 12 points caractéristiques, même en considérant une population de plusieurs dizaines de millions de personnes[24].

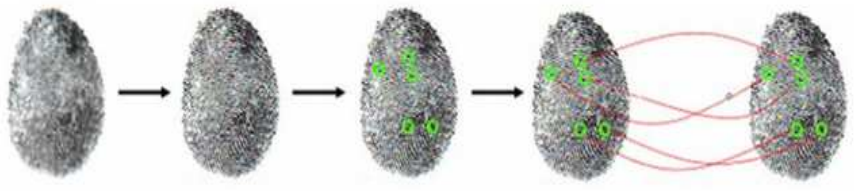

Figure II.1 le processus de reconnaissance par empreinte digitale.

b. Forme de la main ou des doigts de la main :

Ce type de mesure biométrique est l'une des plus répandus, notamment aux Etats Unis. Elle consiste à mesurer plusieurs caractéristiques de la main, tel que la forme de la main, la longueur et la largeur des doigts, la forme des articulations, longueurs inter-articulations, etc. La technologie associée à ce type de mesure est principalement de l'imagerie infrarouge. D'une façon générale, le système présente des FAR (False Acceptation Rate) assez élevés, surtout entre les personnes de la même famille ou bien encore des jumeaux [9].

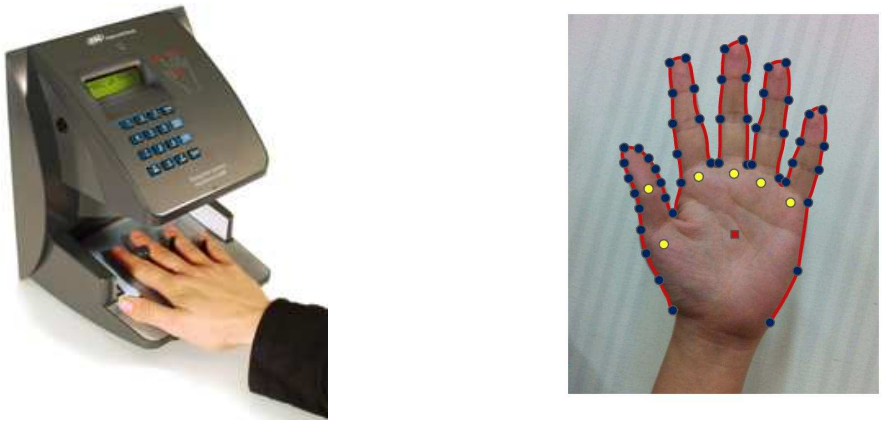

Figure II.2 Dispositif de reconnaissance de la géométrie de la main.

c. Forme du visage :

Cette technologie représente 15% des applications, elle consiste à faire une photographie plus ou moins évoluée pour en extraire un ensemble de facteurs qui se veulent propres à chaque individu. Ces facteurs sont choisis pour leur forte invariabilité et concernent des zones du visage tel que le haut des joues, les coins de la bouche, l'écartement des yeux et la taille de la bouche par exemple. On évitera d'autre part par exemple les types de coiffures, les zones occupées par des cheveux en général ou toute zone sujette à modification durant la vie de la personne. Cette technique est capable de déjouer le port de lunettes, de barbe ou d'autres artifices[12].

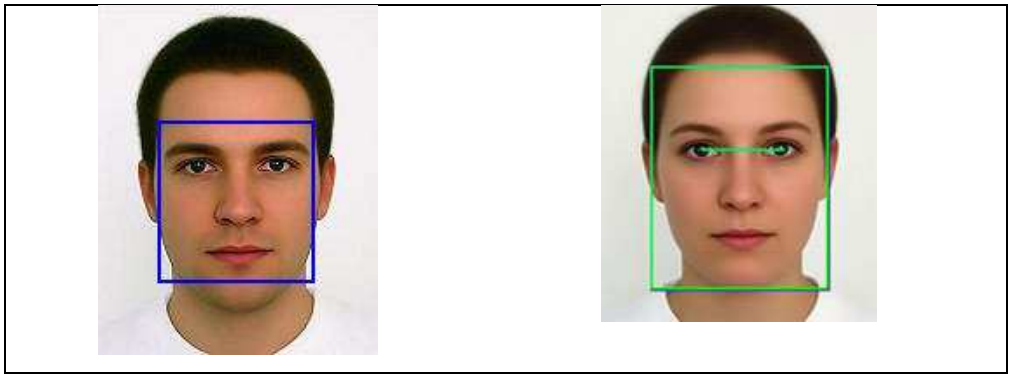

Figure II.3 Reconnaissance Faciale.

d. Rétine de l'œil :

Cette mesure biométrique est plus ancienne que celle utilisant l'iris, mais elle a été moins bien acceptée par le public et les utilisateurs, sans doute à cause de son caractère trop contraignant : la mesure doit s'effectuer à très faible distance du capteur , qui effectue ensuite un balayage de la rétine[18]. Il est physiquement impossible d'effectuer une mesure rétinienne à une distance de 30cm ou plus sur un sujet mobile. Cette méthode requiert des sujets coopératifs. ainsi elle est unique pour chaque individu, différent entre jumeaux et assez stable durant la vie de la personne. La mesure peut ainsi fournir jusqu'à 400 points caractéristique du sujet, que l'on peut comparer aux 30 à 40 points fournis par une empreinte digital. En conclusion, la mesure rétinienne est la plus difficile à utiliser mais également la plus dure à contrefaire.

e. Iris de l'œil :

Pour les deux techniques, il faut tout d'abord faire la distinction entre l'iris et la rétine :

Figure II.4 Reconnaissance de l'iris.

L'individu se place en face du capteur (caméra CCD/CMOS) qui scanne son iris. Celui-ci représente quelque chose de très intéressant pour la biométrie car il est à la fois toujours différent (même entre jumeaux, entre l'œil gauche et le droit, etc...), indépendant du code

génétique de l'individu, et très difficilement falsifiable. En effet, l'iris présente une quasi-infinité de points caractéristiques (que certains comparent en nombre à ceux de l'ADN), qui ne varient pratiquement pas pendant la vie d'une personne contrairement à la couleur de l'iris qui, elle peut changer. Mais cela n'a aucune influence car les images d'iris obtenues par les capteurs sont en noir et blanc. Le seul problème de cette technique est liée à la mesure en elle-même, qui peut être source d'erreurs ou de problèmes [10]. Ainsi, on peut quasiment dire que le nombre de problèmes rencontrés lors de cette mesure augmente proportionnellement avec la distance entre l'œil et la caméra.

f. Forme des veines de la main :

Cette technique est habituellement combinée à une autre, comme l'étude de la géométrie de la main. Il s'agit ici d'analyser le dessin formé par le réseau des veines sur une partie du corps d'un individu (la main) pour en garder quelques points caractéristiques.

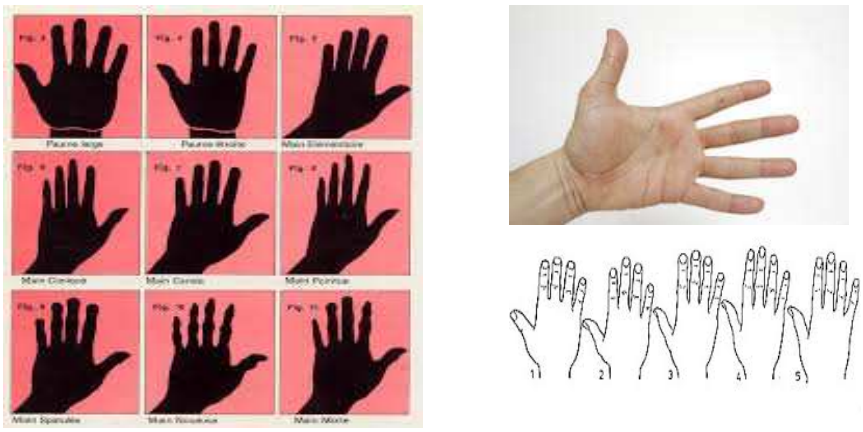

Figure II.5 Forme de la main.

II.2.2 Techniques biométriques Comportementales

Outre les caractéristiques physiques, un individu possède également plusieurs éléments liés à son comportement qui lui sont propres :

a. La voix :

La voix est une diffusion de son, elle est produite par les cordes vocales créant des vibrations dans l'air, elle est créée par le choc de la glotte sur les muscles du larynx. Elle est composée de trois principaux paramètres :

- L'intensité
- La hauteur
- La durée

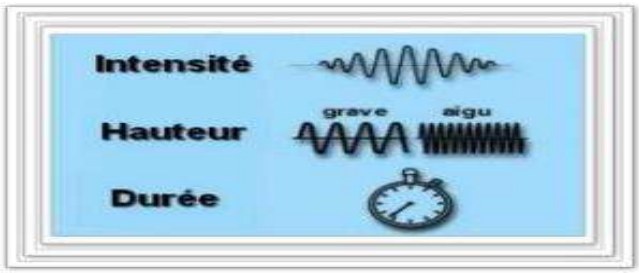

Figure II.6 Paramètres de la voix.

La technologie de reconnaissance vocale se base sur les caractéristiques de la parole, elle est également constituée d'une combinaison de facteurs comportementaux (vitesse, rythme, etc.) et physiologiques (tonalité, âge, sexe, accent, etc.). Un des avantages de la reconnaissance vocale est que la personne à identifier n'est pas en contact direct avec un lecteur biométrique, elle n'est donc pas perçue comme intrusive par l'utilisateur. Une fois capturée par un micro, la voix est convertie par un algorithme mathématique [11]. La reconnaissance vocale n'est pas considérée comme une des meilleures techniques de reconnaissance biométrique.

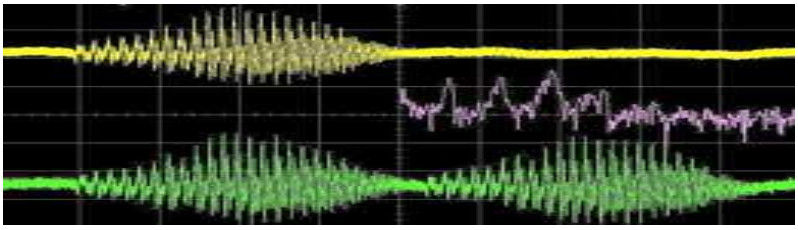

Figure II.7 Reconnaissance vocale.

b. La signature :

Chaque personne a un style d'écriture unique. On peut donc définir, à partir de la signature d'une personne, un modèle qui pourra être employé pour effectuer une identification. De plus, la signature est utilisée dans beaucoup de pays comme élément juridique ou administratif. Elle permet de justifier de la bonne foi d'une personne ou de la confondre devant des documents signés. Le grand avantage des systèmes biométriques à base de signature réside dans la reconnaissance de cette méthode comme une forme acceptable juridiquement pour l'identification des personnes

Figure II.8 La signature

II.2.3 Techniques biométriques Biologiques :

a. ADN :

L'analyse des empreintes génétiques est devenue en quelques années l'un des outils majeurs de la criminalistique. L'analyse de l'ADN est couramment utilisée en criminologie pour identifier une personne à partir d'un morceau de peau, d'un cheveu ou d'une goutte de sang. Souvent les échantillons d'ADN trouvés sur le lieu du crime sont trop infimes pour être analysés. Dans le cas des tests de paternité, on atteint une fiabilité de 99,999%. Mais il existe des appareils d'amplification en chaîne par polymérase (PCR) qui utilisent le même procédé naturel que l'ADN pour recopier et amplifier. Ils procurent ainsi aux criminalistes des brins d'ADN répliqués et exploitables**.** Mais les analyses d'ADN nécessitent des délais de plusieurs semaines, ce qui interdit toutes les applications d'identification en temps réel.

Figure II.9 ADN

b. Odeur :

L'identification humaine à partir de l'odeur corporelle n'est pas nouvelle. Les polices s'en servent depuis plus d'un siècle en faisant appel à des chiens renifleurs, dont l'odorat est suffisamment puissant pour retrouver une personne à partir d'un échantillon qu'ils ont senti. Dès lors, avec les moyens techniques dont nous disposons aujourd'hui, serions-nous en mesure de créer un système de reconnaissance biométrique basé sur l'odeur corporelle ?

c. Sang :

La détection d'une trace de sang sur une scène de crime s'effectue dans un premier temps à l'œil nu. Mais lorsque les taches sont trop petites, pas assez visibles il est nécessaire de procéder à des techniques d'identification chimiques. Le sang est principalement constitué d'hémoglobine aussi c'est sur cette caractéristique que les tests de reconnaissance se basent pour déterminer la présence de sang. En effet, l'hémoglobine catalyse l'oxydation de toutes sortes de substances oxydables par l'eau oxygénée. Dans les tests, ces substances oxydables sont choisies

pour que le produit obtenu au terme de la réaction, soit un produit coloré ou un produit luminescent.

II.3 Conclusion

La biométrie différencie les individus entre eux car elle repose sur des caractéristiques propres à chacun. La technique la plus utilisée est l'identification par empreintes digitales car c'est la plus simple. Mais, on utilise également l'identification par l'iris qui est efficace mais très coûteuse, par la voix, qui est plus une méthode d'authentification que d'identification, et par le visage, qui est la méthode considérée comme la plus naturelle.

Aujourd'hui, on utilise la biométrie surtout lorsqu'il s'agit de sécurité : on la retrouve dans les aéroports, dans certaines entreprises (qui s'en servent pour remplacer les badges. Certains états l'utilisent beaucoup plus que d'autres comme les Etats-Unis par exemple, qui sont très portés sur la sécurité. Elle est utilisée maintenant dans les passeports biométriques, afin d'être sûr que la personne présentant son passeport est bien celle qu'elle prétend être.

Dans un futur proche, il est presque certain que la biométrie sera présente partout et au quotidien. Elle remplace de plus en plus les autres moyens d'identification comme d'authentification.

Pour notre projet nous avons choisi l'identification par empreintes digitales, et nous consacrons le chapitre suivant pour détailler cette technique et son utilisation, ainsi que ces caractéristiques et l’architecture de système de reconnaissance de cette technique.

CHAPITRE III: RECONNAISSANCE DES EMPREINTES DIGITALES

III.1 Introduction

La biométrie est une technique globale visant à établir l'identité d'une personne en basent sur une de ses caractéristiques physiques. Il peut y avoir plusieurs types de caractéristiques physiques, certaines plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu. L'utilisation de l'empreinte digitale comme moyen d'identification d'une personne n'est pas nouvelle. En fait, les corps policiers utilisent cette technique depuis plus de 100 ans. Aujourd'hui, les empreintes digitales sont recueillies sur une scène de crime et sont ensuite comparées à celles contenues dans un serveur central. Le recours à l'empreinte digitale compte pour plus du tiers du marché des procédés biométriques. Elle représente nettement la solution préférée des entreprises œuvrant dans ce domaine. La force de ce procédé tient au fait que l'utilisateur de l'empreinte digitale est généralement plus facile d'acceptation par la communauté et qu'elle est une des plus efficaces et des moins coûteuses.

Dans ce chapitre nous allons présenter les caractéristiques de cette technique et les différentes moyens utiliser afin d'identifier un individu.

III.2 Caractéristiques des empreintes digitales

L'empreinte se compose les crêtes et les vallées alternatives, flottant à la direction constante locale. Le modèle de crête et de vallée est unique pour chaque individu et ne change pas pendant la vie individuelle sauf l'accident comme meurtrissure ou coupe de bout du doigt. Cette propriété fait l'empreinte devenir une biométrie d'identité attractive. Généralement, Il existe trois catégories d'empreintes digitales, à l'intérieur de chacune de ces catégories, il y a un grand nombre d'éléments qui différencient chaque empreinte de manière unique.

Figure III.1 Les catégories d'empreintes digitales.

Ces éléments qui permettent de différencier les empreintes sont appelés minuties[7]. La minutie est l'arrangement particulier des lignes papillaires formant des points caractéristiques à l'origine de l'individualité des dessins digitaux. Une empreinte complète contient en moyenne une centaine de ces points caractéristiques mais les contrôles ne sont effectués qu'à partir de 12 points[25]. Statistiquement, il est impossible de trouver 2 individus présentant 12 points caractéristiques identiques, même dans une population de plusieurs millions de personnes.

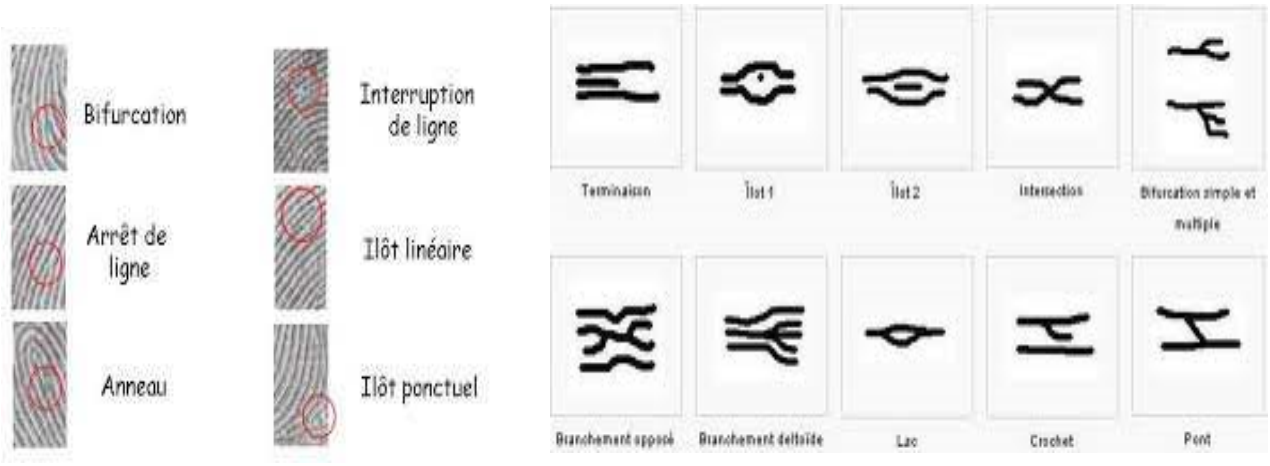

Figure III.2 Les différentes catégories de minuties

III.3 Architecture d'un système de reconnaissance des empreintes digitales

Le système de l'authentification d'empreintes est divisé par trois étapes :

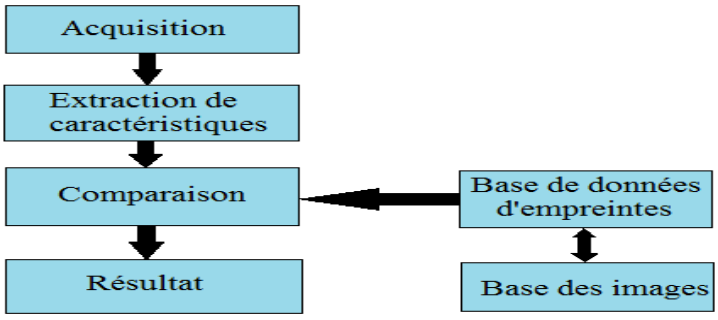

Figure III.3 Les différentes étapes pour la reconnaissance d'empreintes digitales.

III.3.1 Acquisition

Un système d'acquisition équipé d'un capteur est utilisé pour acquérir une caractéristique spécifique de l'utilisateur. L'image d'empreinte est prise selon le mode traditionnel qui est un scanner du doigt couvert d'encre, ou en utilisant un dispositif d'acquisition d'image spécifique.

III.3.2 Extraction des caractéristiques

Depuis une image capturé, une étape de segmentation permet d'extraire les caractéristiques (les terminaisons et les bifurcations) dont le processus d'authentification a besoin. C'est une étape clé pour donner un résultat précis[6].

III.3.3 Comparaison

Calculer la différence entre les caractéristiques extraites et la base de données existante et décider laquelle est la plus semblable à l'entrée..

III.3.4 La décision

En ce qui concerne l'authentification, la stratégie de décision nous permet de choisir entre les deux alternatives suivantes: l'identité de l'utilisateur correspond à l'identité proclamée ou recherchée. Elle est basée sur un seuil prédéfini. L'estimation du seuil de la décision constitue la plus grande difficulté de ces techniques, et elle peut engendrer deux types d'erreurs, souvent prises comme mesures de performances pour ces techniques d'authentification: faux rejet (FR) qui correspond à rejeter un vrai utilisateur ou une identité valable, et fausse acceptation (FA) qui donne accès à un imposteur.

III.4 Les capteurs d'empreintes digitales

La capture de l'image d'une empreinte digitale consiste à trouver les lignes tracées par les crêtes (en contact avec le capteur) et les vallées (creux).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.

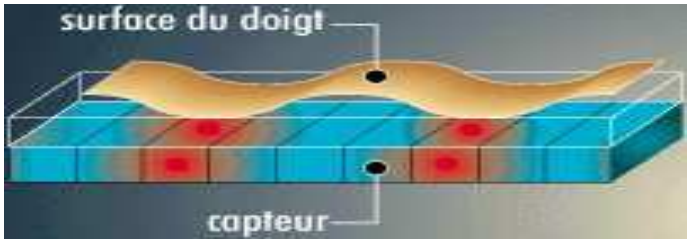

Figure III.4 : Capture de l'image d'une empreinte digitale.

III.4.1 Capteur optique

Il s'assimile à une mini caméra. Le doigt est apposé sur une platine en plastique dur ou en quartz, qui est en vis-à-vis de la mini caméra. Il résiste très bien aux fluctuations de température, mais est gêné par une lumière ambiante trop forte.De plus il est assez volumineux. Son coût est intéressant, et il est intrinsèquement protégé contre les décharges électrostatiques. Il permet d'avoir des images précises et nettes. 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. Le principe physique utilisé est "la réflexion totale frustrée".

III.4.2 Capteur en silicium

Il utilise l'un de quatre effets observables sur les semi-conducteurs : l'effet piézo-électrique, l'effet capacitif, l'effet thermoélectrique et l'effet photo-électrique. Il est en général de très petite taille, d'une durée de vie assez longue, et son coût est très intéressant. Mais, comme tout composant, il est fragile aux décharges électrostatiques et il peut être détruit si des règles de fabrication et d'installation ne sont pas observées. Ces nouvelles technologies visent surtout les applications de masses, grâce à une taille réduite et des coûts moins importants que les lecteurs optiques.

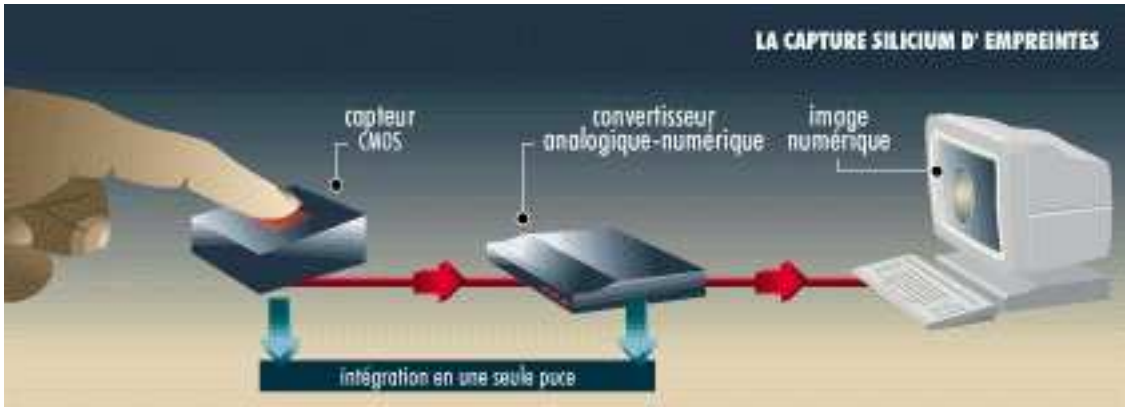

Figure III.5 Capteur en silicium.

III.4.3 Capteur thermique

La technique de capture thermique est utilisée par le Finger Chip d'Atmel. Le capteur mesure une différence de température obtenue selon que la peau touche (dans le cas d'une crête de l'empreinte) ou ne touche pas (pour une vallée) le capteur. Le Finger Chip est constitué d'une puce en silicium recouverte d'une couche de matériau pyroélectrique, c'est-à-dire sensible aux différences de température. La puce est elle-même formée d'une matrice de pixels adjacents. La différence de température, initialement apparue au contact du matériau pyroélectrique, est transformée de par les propriétés de ce matériau en charges électriques. Celles-ci sont alors amplifiées et mesurées par les pixels en silicium de manière à former une image en noir et blanc traduction fidèle de l'empreinte de l'utilisateur[22].

Cette technologie thermique présente de nombreux avantages. En particulier, elle permet d'obtenir une image de très grande qualité avec des empreintes « difficiles », par exemple quand les crêtes et les vallées sont très peu marquées.

III.4.4 Capteur ultra sonique

Il utilise une onde ultra sonore qu'il envoie vers le doigt. Puis, il calcule le temps mis par l'onde pour faire un aller-retour et point par point, il fournit l'image de l'empreinte. Il est très précis et il hérite des propriétés des ultrasons qui traversent certains matériaux (gants en latex, saletés, etc.). Il est volumineux et très coûteux, il est intéressant pour une population d'utilisateurs très hétérogène.

III.5 Etapes de traitement de l'empreinte digitale

III.5.1 Extraction des minuties

D'une manière générale on distingue deux catégories d'algorithmes de reconnaissance d'empreintes digitales la première catégorie concerne les algorithmes plutôt « conventionnels » qui s'appuient sur la position relative des minuties entre elles, alors que la seconde regroupe les algorithmes visant à extraire d'autres particularités de l'empreinte digitale telles que la direction locale des sillons, ou encore les composantes fréquentielles locales de la texture au cœur de l'image.

III.5.2 Binarisation de l'image

En traitement d'image, la binarisation est une opération qui produit deux classes de pixels, en général, ils sont représentés par des pixels noirs et des pixels blancs. Etant donné que

les minuties sont de très petits détails difficilement visibles de l'empreinte, il convient de bien les mettre en évidence avant de procéder à leur extraction. C'est la grande utilité de binariser l'image de l'empreinte. L'idée consiste à donner une même intensité aux lignes et une autre intensité très différente aux vallées, afin de bien distinguer ces deux régions de l'empreinte. La technique la plus utilisée consiste à se fixer un seuil d'intensité t, parcourir la matrice de pixels de l'image . En assignant la valeur 0 à tous les pixels dont la valeur d'intensité est inférieure à t (ce qui revient à mettre en noir les points correspondants sur l'image), et en assignant une autre valeur (typiquement 1) aux pixels de valeur supérieure ou égale à t. Ainsi, ayant une faible intensité au départ, les lignes de l'empreinte seront en noir (valeur 0) et les vallées seront en blanc (plus forte intensité car 1 > 0).

Figure III.6 Binarisation de l'empreinte digitale

La binarisation de l'image est importante pour augmenter la visibilité des minuties, mais cela ne suffit pas. Une fois l'image binarisée, on procède à une diminution de la taille de lignes, c'est donc une sorte "d'amincissement" de l'image, qualifiée de squelettisation). A ce stade, les minuties sont bien visibles et facilement détectables. Le crossing number $c_n(p)$ d'un pixel p est défini comme la moitié de la somme des différences en valeur absolue de pixels adjacents dans un voisinage de 8 pixels entourant p. En analysant le squelette binaire de l'image de l'empreinte, on remarque que les pixels correspondant aux minuties possèdent un crossing number différent de 2. Le crossing number d'un pixel p se calcule par la formule suivante :

$$Cn(p)=\frac{1}{2}\sum_{i=1}^{8}\left|val(Pi \bmod 8)-val(P_{i-1})\right|$$

p_0, p_1, .., p_7 sont les 8 pixels au voisinage de p et val(p) vaut 0 ou 1(car image binarisée). Il est alors facile de remarquer qu'un pixel p dont val(p) = 1 :

a) est un point d'une ligne de l'empreinte si $c_n(p) = 2$.

b) correspond à une terminaison si $c_n(p) = 1$;

c) correspond à une minutie plus complexe (bifurcation, îlot. . .) si $c_n(p) \geq 3$.

Cependant, les méthodes basées sur la binarisation ont quelques défauts :

1. Il est possible de perdre beaucoup d'informations lors du processus de binarisation .

2. La binarisation et la squelettisation sont une perte de temps et diminuent par conséquent la performance des algorithmes .

3. La squelettisation peut introduire un certain nombre de fausses minuties .

4. L'application de la méthode sur une empreinte de mauvaise qualité produit de mauvais résultats.

Il existe cependant certains processus d'amélioration de l'image avant de procéder à l'extraction de minuties, "enhancement step" [19]

Le système peut éventuellement rejeter l'image de l'empreinte lorsque le contrôle de qualité révèle une image de très mauvaise qualité.

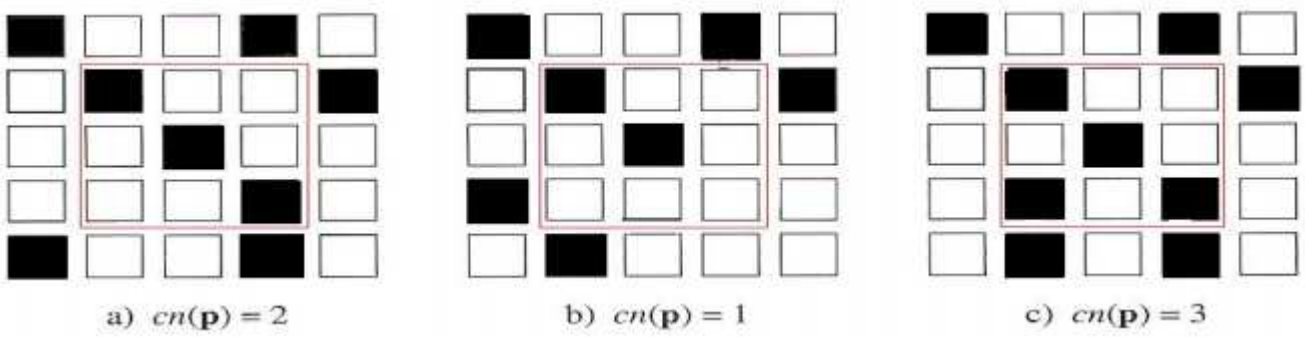

Figure III.7 Calcul du crossing number dans un voisinage de 8 pixels.

Les pixels de valeur 1 et ceux de valeur 0 sont respectivement symbolisés par les carrés noirs et les carrés blancs. a) point d'une ligne de l'empreinte, b) terminaison, c) bifurcation.

Ces méthodes restent très pratiques car elles sont faciles à mettre en place et donc moins coûteuses. Elles sont souvent combinées avec d'autres méthodes plus complexes pour assurer la fiabilité et la robustesse du système.

III.5.3 Squelettisation de l'image

La squelettisation consiste à effectuer récursivement l'opération d'amincissement jusqu'à ce que l'image ainsi créée ne change plus. Le but est de produire une image dans laquelle le diamètre de chaque crête est « un pixel », donc réduire les formes en un ensemble de courbes. La squelettisation permet d'extraire des caractéristiques importantes, comme les intersections et le nombre de tracés, leurs positions relatives. Il est possible de renormaliser l'épaisseur de l'écriture à partir du squelette. Le squelette doit remplir trois conditions:

- Il doit être aussi fin que possible (1 pixel d'épaisseur).
- Il doit respecter la connexité.
- Il doit être centré dans la forme qu'il représente.

Un autre moyen d'obtenir le squelette est de procéder par affinages successifs : la forme est "épluchée" (peeling) de manière itérative, en maintenant valide le critère de connexité. L'algorithme de Hilditch [HIL69] exploite ce principe[5]. On définit le voisinage du pixel P1 comme suit (figure III.8):

P_9	P_2	P_3
P_8	P_1	P_4
P_7	P_6	P_5

Figure III.8 Voisinage d'un pixel

On définit également:

- $A(P_1)$: Nombre de transitions 0 vers 1 dans la séquence $P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9$.
- $B(P_1)$: Nombre de pixels noirs dans le voisinage de P1 (P1 étant exclu).
- $B(P1)=\sum P_i, avec \begin{cases} P_i=1 & si\ le\ pixel\ est\ noir \\ P_i=0 & si\ le\ pixel\ est\ blanc \end{cases}$

L'image est parcourue de multiples fois, un pixel noir est marqué comme effaçable s'il respecte les conditions suivantes:

$2 \le B(P_1) \le 6$

$A(P_1)=1$

$P_2.P_4.P_8=0$ *où* $A(P_2)\neq 1$

$P_2.P_4.P_6=0$ *où* $A(P_4)\neq 1$

Tous les points marqués comme effaçables sont ensuite effacés, et on réitère l'opération sur la nouvelle image, jusqu'à ce que plus aucun point ne soit effaçable[23].

De manière générale, les méthodes d'obtention du squelette par érosions successives fonctionnent selon le principe suivant :

Figure III.9 Amincissement d'une image d'empreinte.

Une fois la squelettisation (amincissement) accompli, l'étape de détection des minuties s'avère être une opération simple.

```
DEBUT
I : image binaire en entrée ;
Changé : booléén ;
Changé = vrai ;
Tant que (changé = vrai) Faire
   DTQ
    Changé = faux ;
     Pour  i allant de 1 à longueur de l'image I
          Pour j allant de 1 à largeur de I
               DPR
                SI ( Imge[i,j] = 1 ) Alors
                  DSI
                     Parcourir le voisinage 3x3 du pixel (i,j)
                      SI une des configurations C se présente Alors
                          DSI
                           Image[i,j]= 0;
                           Changé = vrai;
                           FSI

                          /* Les configurations structurelles C sont : */
```

0	0	0	0	0			1			1		1	1	1	1		0	0		1		0	0
	1		0	1	1	0	1	1	1	1	0		0		1	1	0	0	1	1	1	1	0
1	1	1		1		0	0			0	0	0	0	0	1		0			1			

```
                           FSI
                      FPR
   FTQ
FIN.
```

Figure III.9 Algorithme qui utilise le voisinage des pixels

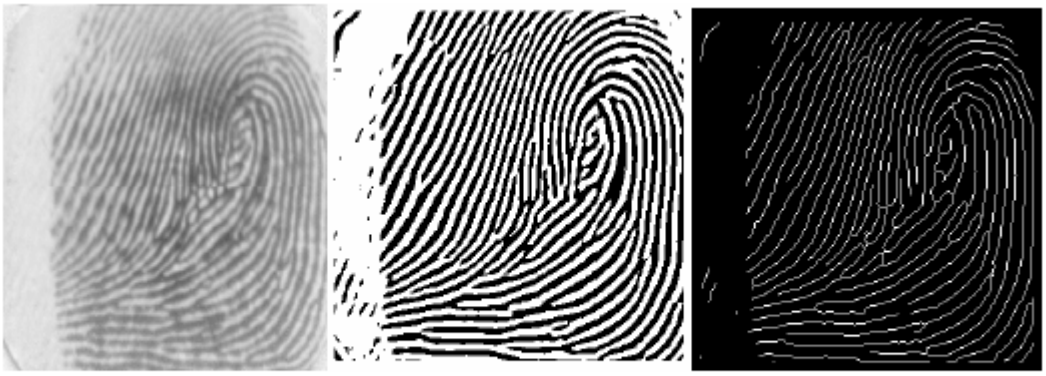

Figure III.10 binarisation et squelettisation d'une empreinte

Le premier algorithme de traitement des images d'empreintes digitales permet de s'affranchir du bruit lié à la mesure, perturbations désignées sous le terme de bruit d'image (provenant essentiellement de l'imperfection de la peau et des poussières entre le doigt et le capteur), mais aussi de mettre en évidence l'information relative aux sillons en les synthétisant sous forme filaire par leur squelette[17].

La binarisation consiste à utiliser un seuil global *S*. La procédure peut être définie comme suit :

$$I(x,y)=\begin{cases}1\ si\ I(x,y)\geq S\\ 0\ si\ I(x,y)<S\end{cases}$$

Où *I(x,y)* représente le pixel dont les coordonnés sont *x* et *y* .

III.5.4 Extraction des minuties

La prochaine étape consiste à extraire les minuties de l'image d'empreinte. Après la squelettisation, l'image sera composée de crêtes. Le but principal est d'extraire les terminaisons et les bifurcations. C'est le processus final qui complète l'obtention de la "signature" de l'empreinte[8]. A partir d'une image de l'empreinte préalablement traitée, on extrait grâce à différents algorithmes une structure de données (ou signature). La signature retenue pour caractériser l'empreinte est basée sur un ensemble suffisant et fiable de minuties (environ 14). Il est alors possible d'identifier une empreinte parmi plusieurs millions d'exemplaires. Lors du processus d'extraction[18], on détecte initialement 100 minuties en moyenne, parmi lesquelles environ 60 % correspondent à de fausses minuties qui seront identifiées lors d'un processus ultérieur. La recherche de minuties ne se fait que sur des images binarisées et squelettisées. Il existe deux types de minuties :

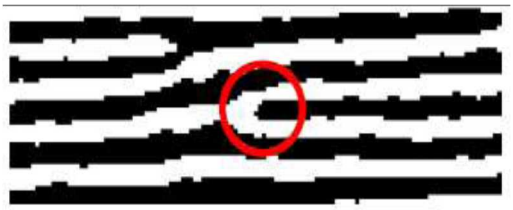

Figure III.11 Exemple d'arrêt de ride ou fin de ligne

Figure III.12 Exemple de bifurcation

Un algorithme va donc parcourir l'image à la recherche de telles situations. Pour cela, on utilise une matrice 3x3 qui va détecter si un pixel noir est entouré de un, deux ou plus de deux pixel noirs, s'il y en a qu'un, c'est une fin de ligne, s'il en a deux, c'est une ligne normale, sinon, c'est une bifurcation.

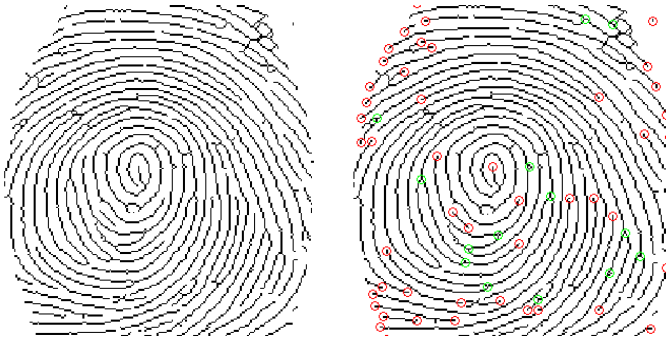

Figure III.13 Extraction des minuties.

III.5.5 Comparaison des minuties

La comparaison de minuties s'appuie sur le principe de graphe. En effet avec les coordonnées de chaque minutie, il est possible de calculer la distance entre chacune d'entre elles, ainsi que l'angle formé par trois minuties. Grâce à ces informations, il est possible de construire un graphe complet pondéré par les distances entre les minuties. L'angle existant entre chaque minutie sera calculé en temps voulu grâce à ces distances. Une fois ce graphe complet créé, il ne reste qu'à comparer les graphes des deux images pour savoir si elles sont identiques[9].

Pour comparer deux graphe de minuties, un algorithme est mis en œuvre, il prend en compte un seuil d'acceptation, ainsi qu'un seuil de refus, il prend aussi en compte un éventuel écart entre deux minuties, c'est-à-dire qu'il est possible de comparer deux distance avec une marge d'erreur en pourcentage.

Il existe 3 types de comparaison d'empreinte [4]:

- deux images identiques d'empreinte de la même personne (cas n°1)
- deux images différentes d'empreinte, mais venant de la même personne (cas n°2)

- deux images d'empreinte venant chacune d'une personne différente (cas n°3)

L'objectif de la comparaison est d'avoir des résultats dans le 2eme et 3ème cas, vu qu'en théorie, il ne sera jamais possible, via un capteur d'empreintes, d'obtenir la même image contenue dans la base de données.

III.6 Conclusion

La biométrie par l'empreinte digitale est la technologie la plus employée à travers le monde. Et on voit fleurir des solutions de plus en plus abordables et performantes. D'ici à quelques années, les lecteurs d'empreintes digitales n'étonneront plus personne et seront rentrés dans les mœurs au même titre que le téléphone portable. on peut donc dire qu'il est impossible que deux individus présentent des empreintes similaires. L'identification par les empreintes digitales est la méthode biométrique la plus utilisée à travers le monde, même si les gens la perçoivent comme « intrusive », car elle reste très simple. Bientôt, elle fera partie de notre quotidien : on la trouve déjà dans des systèmes de sécurité comme dans les aéroports ou même certaines entreprises[12]. Même les passeports aujourd'hui contiennent des informations biométriques, dont nos empreintes on les appelle « passeports biométriques ».

CHAPITRE IV: CONCEPTION ET IMPLEMENTATION

IV.1 Introduction

Notre travail consiste à réaliser un système qui a pour but la reconnaissance d'empreintes digitales (identification et authentification d'empreintes), nous présentons la démarche et toutes les étapes qui nous ont permis d'atteindre notre objectif.

La première étape consiste à implémenter les différents algorithmes de traitement d'images (filtrage , binnarisation, squelettisation , extraction des minuties et puis la comparaison entre les deux motifs de points). l'ensemble de ce système vise plus particulièrement des application embarquées et mono utilisateur qui nécessitent une authentification (téléphone cellulaire , ordinateur portable , contrôle de présence, assistance numérique, etc.).

IV.2 Environnement du travail

Dans cette section. Nous présenterons l'environnements de travail pour réaliser notre système.

IV.2.1 Environnement matériel

Afin de mener à bien ce projet. Il a été mis à notre disposition un ensemble de matériels dont les caractéristiques sont les suivantes :

Un ordinateur TOSHIBA SATILITE C670/C670 avec les caractéristiques suivantes :

- Processeur : Intel ® Core ™ i3CPU M 380@ 2.53GHz
- Ram : 4.00 Go de RAM
- Disque Dur :620 Go
- System d'exploitation : Microsoft Windows 7
- Type de système : System d'exploitation 64 bits
- Modèle de système :damasGate AIO Lited Edition

IV.2.2. Outils de développement logiciel :

La plate-forme de développement utilisée dans notre projet, permet de dérouler et d'exécuter des programmes écrits en langage JAVA, indépendamment de toute architecture matérielle et de tout type système d'exploitation. Ces applications logicielles sont portables et flexibles[13].

IV.2.2.1 le langage JAVA (Netbeans 6.8) :

Java est un langage de programmation récent (les premières versions datent de 1995) développé par Sun Microsystems. Il est fortement inspiré des langages C et C++.

NetBeans est un environnement de développement intégré (EDI), placé en open source par Sun en juin 2000 sous licence CDDL et GPLv2 (Common Développent and Distribution License). En plus de Java, NetBeans permet également de supporter différents autres langages.comme C, C++, JavaScript, XML, Groovy, PHP et HTML de façon native ainsi que bien d'autres (comme Python ou Ruby) par l'ajout de greffons. 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 Développent KitJDK 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 plateforme.

Les principales raisons du succès de Java :

Java a rapidement intéressé les développeurs pour quatre raisons principales : C'est un langage orienté objet dérivé du C, mais plus simple à utiliser et plus « pur » que le C++. On entend par « pur » le fait qu'en Java, on ne peut faire que de la programmation orienté objet contrairement au C++ qui reste un langage hybride, c'est-à-dire autorisant plusieurs styles de programmation. C++ est hybride pour assurer une compatibilité avec le C ;

Il est doté, en standard, de bibliothèques de classes très riches comprenant la gestion des interfaces graphiques (fenêtres, boites de dialogue, contrôles, menus, graphisme), la programmation multi-threads (multitâches), la gestion des exceptions, les accès aux fichiers et au réseau … L'utilisation de ces bibliothèques facilitent grandement la tâche du programmeur lors de la construction d'applications complexes ;

Il est doté, en standard, d'un mécanisme de gestions des erreurs (les exceptions) très utile et très performant. Ce mécanisme, inexistant en C, existe en C++ sous la forme d'une extension au langage beaucoup moins simple à utiliser qu'en Java ; Il est multi plates-formes :

les programmes tournent sans modification sur tous les environnements où Java existe (Windows, Unix, Linux,…) .

IV.2.2.2 Base de données "DERBY".

Apache Derby est un moteur de base de données relationnelle écrit en langage Java qui peut être embarqué dans des programmes écrits en Java. Étant multiplateforme et de très petite taille (2MB), il s'intègre particulièrement bien dans toute application Java.

Apache Derby est un projet open source sous licence Apache 2.0.Derby est aussi connu sous les noms IBM Cloud scape et Sun Java DB[15].

Derby a la particularité de pouvoir être utilisé comme gestionnaire de base de données embarqué dans une application Java. Ce qui rend inutile l'installation et la maintenance d'un serveur de base de données autonome. A l'inverse Derby supporte aussi un mode de fonctionnement client-serveur.

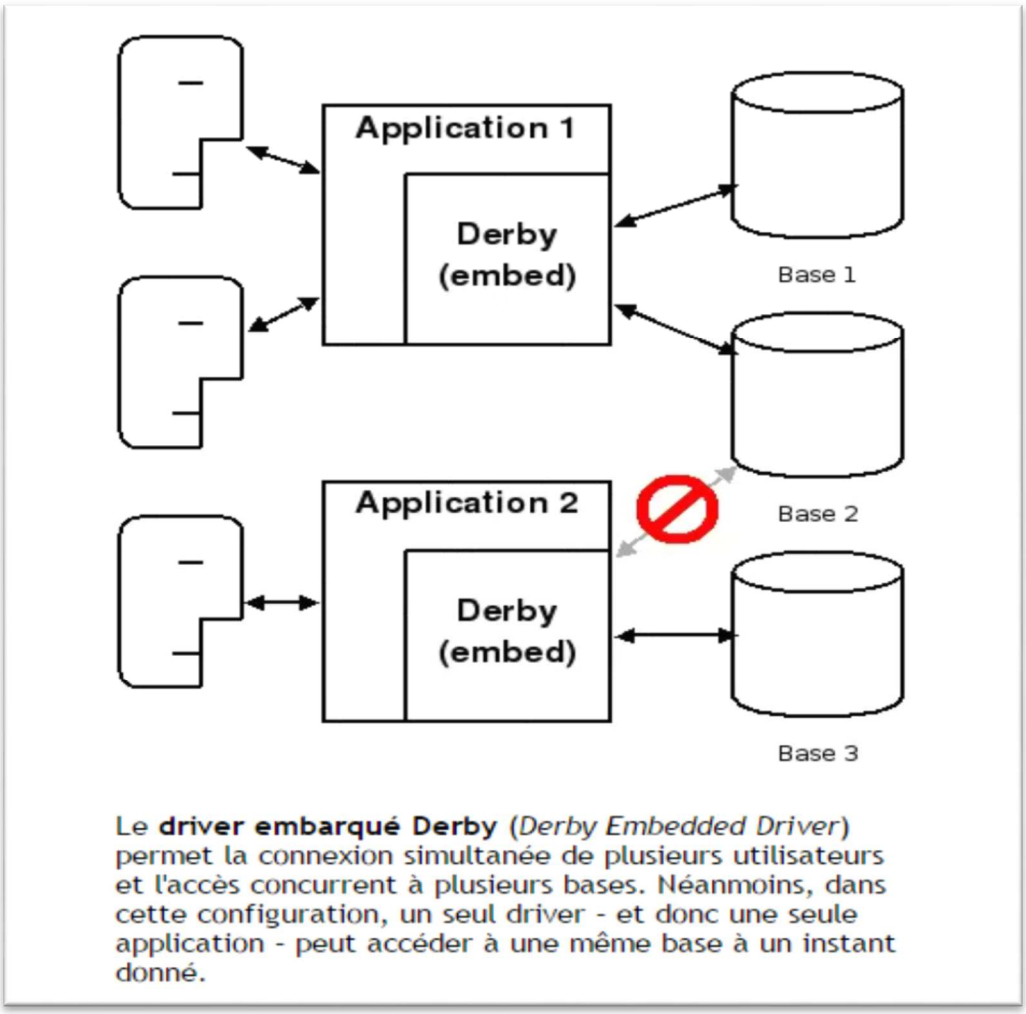

Figure IV.1 Connexion entre apache derby avec netbeans

Pour nos expérimentations, et en vue, d'analyser les performances de notre système nous avons utilisé une base de données d'empreintes téléchargée à partir du site Fingerprint Vérification Competition [25]. Les empreintes sont prises sur plusieurs individus.

IV.3 L'architecture générale de notre application :

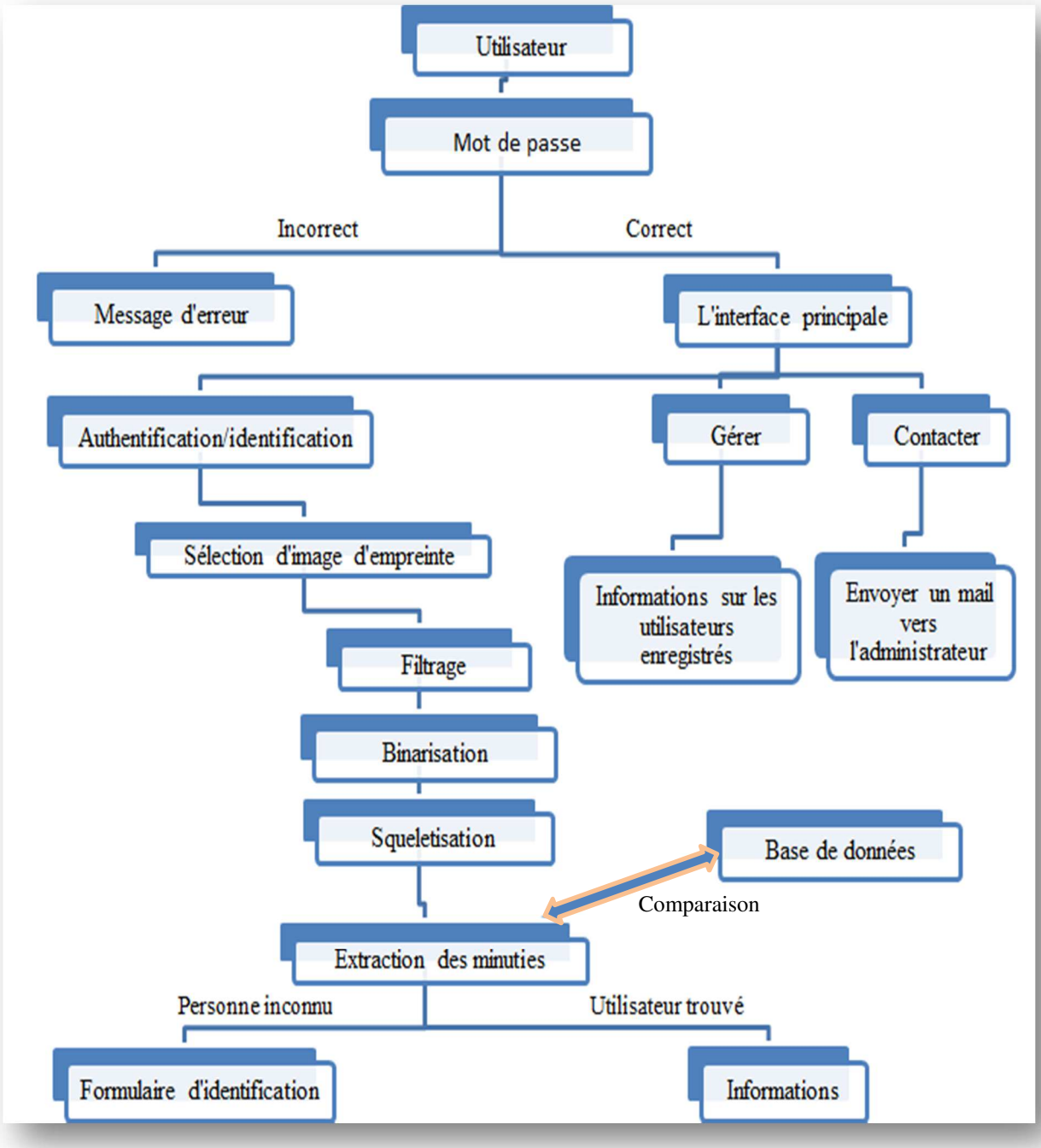

Figure IV.2 L'architecture générale de notre application.

Le système doit répondre à certaines caractéristiques :

- Une interface intuitive et simple à utiliser.
- Rapidité d'exécution.
- Une bonne performance des résultats.
- Un minimum d'erreur.

IV.4 Expérimentation :

Le système permet la reconnaissance et la vérification d'empreintes, il permet de confirmer ou infirmer l'identité d'une personne (*suis-je celui que je prétends être?*) par rapport à un enregistrement de référence. On distingue alors deux opérations, l'enregistrement et la vérification.

Lors de l'enregistrement, la signature S_P extraite de l'empreinte est stockée en mémoire. Lors de la vérification la signature S_Q de l'utilisateur est comparée à S_P. Bien entendu ces deux signatures ne seront jamais strictement identiques car l'empreinte ne sera jamais acquise de manière similaire (vitesse, poussière, pression).

L'authentification de la personne consiste alors à calculer le degré de similarité entre les deux Signatures S_P et S_Q. Cette similitude quantifiée est ensuite comparée à un seuil défini par avance en fonction de l'application choisie (voir chapitre I) pour déterminer si c'est la bonne personne ou non.

IV.4.1Les interfaces de notre application :

IV.4.1.1 La fenêtre principale d'accès au système :

A partir de cette fenêtre, l'administrateur doit introduire un nom d'utilisateur et un mot de passe valides pour pouvoir utiliser le système.

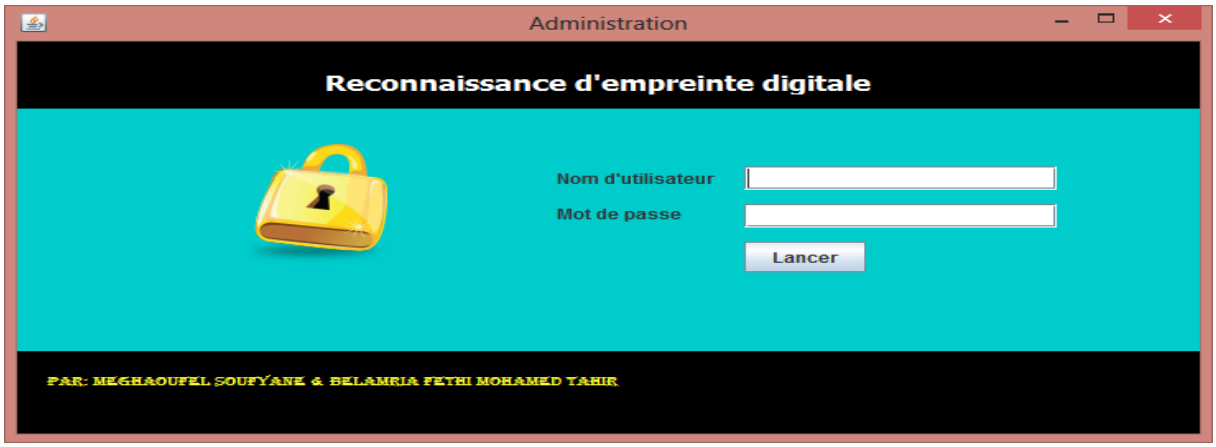

Figure IV.3 Interface d'accès aux système.

IV.4.1.2. L'authentification et l'identification :

A partir de cette onglet l'administrateur sélectionne une image d'empreinte pour le traitement, le système réalise les opérations suivantes sur l'image sélectionnée.

Figure IV.5 Sélection d'empreinte.

a. Filtrage et binarisation :

Pour permettre l'authentification/l'identification, l'image doit être filtrée et 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 filtrage et de la binarisation d'images, Nous avons choisi d'utiliser une méthode de seuillage simple comme suit[17] :

1- Conversion de l' image en niveaux de gris.

Pour chaque pixel $p(i, j)$, on a $gris(p) = \frac{rouge + vert + bleu}{3}$

2- Le système divise l'image en bloc de taille NxN.

3- Le système calcule la moyenne de niveaux de gris MB_i pour chaque bloc B_i.

Exemple pour le premier bloc :

$$MB1 = \frac{\sum_{I=1}^{N}\sum_{J=1}^{N} gris(I,J)}{N^2}$$

4- Si *gris*(p) ≥ MB_i alors p(i,j) prend la valeur de 1 et 0 dans l'autre cas.

Figure IV.6 Résultats de l'étape de filtrage et binarisation.

b. Squelettisation :

L'algorithme de Zhang-Suen a été utilisé pour la squelettisation des images, les étapes principales de cet algorithme sont les suivantes :

Répéter

Supprimer en parallèle les points P de l'image vérifiant les conditions suivantes :

$2 \leq B(P) \leq 6$ (A.1)

$A(P) = 1$ (A.2)

$P_4 = 0$ ou $P_6 = 0$ ou $P_2 = P_8 = 0$ (itérations impaires) (A.3)

$P_2 = 0$ ou $P_8 = 0$ ou $P_4 = P_6 = 0$ (itérations paires) (A.4)

Jusqu'à ce qu'il n'y ait plus de point supprimé durant 2 sous-itérations successives.

La condition (A.1) permet la préservation des points extrémités (points 8-adjacents à un point de l'image). Elle est telle que les points supprimés sont 4-adjacents au complémentaire et 4-adjacents à l'objet[20]. La condition (A.2) jointe à la condition (A.1) cible alors des points à la fois 4-simples et 8-simples. La condition (A.3) s'attache à retirer les points de bord *Est* ou *Sud* et les coins *Nord–Ouest*. La condition (A.4) s'attache à retirer les points de bord *Nord* ou *Ouest* et les coins *Sud –Est*.

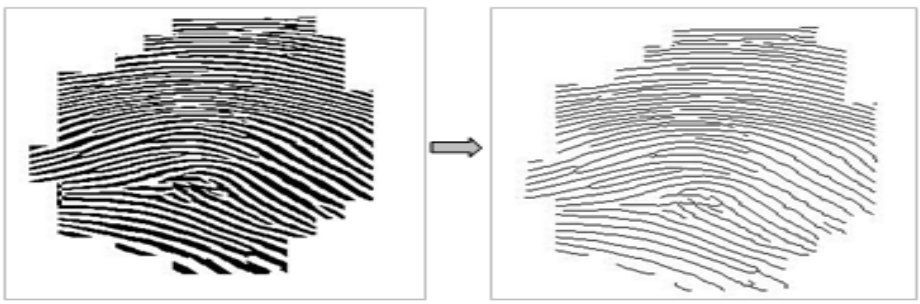

Figure IV.7 Squelette de l'image binaire de l'empreinte**.**

c. La détection des minuties :

Les deux étapes de préparation à l'extraction (binarisation et squelettisation) ont grandement facilité cette phase. En effet nous disposons maintenant d'une image binaire squelettisée: un pixel noir prend la valeur *1*, un pixel blanc prend la valeur *0* et la largeur des stries est égale à 1 pixel. Si on calcule le nombre de transitions divisé par *2* entre un pixel blanc et un pixel noir pour chaque point du squelette, on obtient le nombre *CN*(*Crossing Number*) de stries partant de ce point et nous pouvons donc déterminer simplement le type d'un pixel[16].

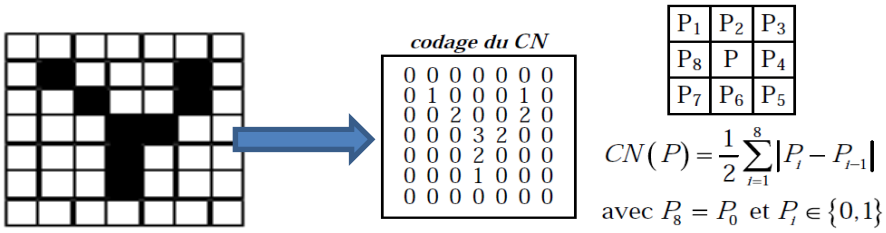

Figure IV.8 Représentations du squelette selon la méthode de (CN).

Ainsi pour chaque pixel *P* appartenant à une strie (c'est-à-dire pour chaque pixel ayant une valeur de 1 le calcul de *CN* peut prendre cinq valeurs:

1- CN(P)=0 :Dans ce cas il s'agit d'un pixel isolé.
2- CN(P)=1 :Une minutie de type terminaison.
3- CN(P)=2 :c'est le cas le plus courant, le pixel se situe sur une strie, il n y a pas de minutie.
4- CN(P)=3 :Une minutie de type bifurcation.
5- CN(P)=4 : nous sommes en présence d'une *bifurcation* quadruple. Ce type de minutie étant assez rare il est probablement dû à du bruit et nous l'ignorons[21].

d. Le fichier signature :

Le fichier signature correspond à l'information utile minimum contenue dans l'image qui est nécessaire à l'identification. Dans notre cas il s'agit de la liste des minuties détectées *et* validées associées de leurs caractéristiques.

Pour chaque minutie détectée et validée on extrait trois caractéristiques.

1- Le type de minutie: *bifurcation* ou *terminaison*.
2- La position de la minutie dans l'image: *coordonnées (x, y)*.

3- La direction du minutie.

e. Comparaison des signatures :

Dans ce stade le système compare le fichier généré a partir de cette image avec les fichier enregistrés dans la base.

Figure IV.9 Cas d'un utilisateur trouvé**.**

Si l'utilisateur n'a pas été retrouvé nous devons passer à l'étape d'identification.

Figure IV.10 Formulaire d'identification.

IV.4.1.3. L'interface de gestion de la base de données :

A partir de cette interface l'administrateur peut avoir accès à toutes les informations sur les utilisateurs déjà enregistrés dans la base.

Figure IV.11 Interface de gestion.

IV.4.1.4. Interface de contact :

Cette interface permet de contacter l'administrateur de cette application par un mail.

Figure IV.12 Interface de contact.

IV.5 Conclusion

Dans ce chapitre, nous avons vu détaillé le concept générale de la réalisation de notre système. Nous avons présenté la structure globale et détaillé les différentes étapes de notre application, on a également décrit les fonctions utilisées, qui consistent en la transformation l'image en une image binaire et ensuite en procédant à sa squelettisation. La dernière étape consiste à la détection des minuties pour procéder par la suite à la comparaison.

Dans le but d'illustrer notre travail, nous avons accompagné ce chapitre d'un ensemble d'exemples sur les opérations essentielles.

CONCLUSION GENERALE

Le projet de la reconnaissance d'empreintes digitales nous a permis d'approcher les différentes méthodes de traitement d'images et de comprendre les possibilités et les limites de la reconnaissance d'empreintes digitales. De nos jours la biométrie par l'empreinte digitale est considéré comme moyen le plus sûr pour la sécurité. Elle est la plus employée à travers le monde. Et on voit fleurir des solutions de plus en plus abordables et performantes grâce à ses avantages. Ses application sont divers : applications de contrôle d'accès, applications dans les téléphone portables, application dans l'e-commerce etc.

Nous pouvons conclure par les affirmations qui sont que les systèmes biométriques sont de plus en plus utilisés pour vérifier ou déterminer l'identité d'un individu. Compte tenu des enjeux liés à leur utilisation, notamment pour des applications dans le domaine de commerce électronique, il est particulièrement important de disposer d'une méthodologie d'évaluation de tels systèmes. Les systèmes conçus doivent se baser sur une méthodologie générique visant à évaluer le système biométrique.

Cette méthode doit être de qualité sans référence pour prédire la qualité d'une donnée biométrique, elle doit être d'usage pour évaluer l'acceptabilité et la satisfaction des usagers lors de l'utilisation des systèmes biométriques et elle doit assurer l'analyse sécuritaire du système biométrique afin de mesurer sa robustesse aux attaques

La biométrie présente malheureusement un inconvénient majeur, en effet aucune des mesures utilisées ne se révèle être totalement exacte car il s'agit bien là d'une des caractéristiques majeurs de tout organisme vivant : on s'adapte à l'environnement, on vieillit, on subit des traumatismes plus ou moins importants, bref on évolue et les mesures changent.

Le principal biais de la biométrie réside dans «la confusion entre identification et authentification. En résumé, s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité», ce qui se traduit généralement au travers du couple identifiant (ou "login") et mot de passe. Or, la biométrie aurait tendance à confondre login et mot de passe: alors que la solution classique requiert la validation des deux paramètres, les procédés biométriques n'en demandent trop souvent qu'un seul

Dans un futur proche, les systèmes biométriques vont être utilisés pour les ordinateurs, les voitures, les accès contrôlés à des bâtiments ou à Internet. Les systèmes qui rencontreront le plus de succès seront ceux qui offriront l'interface la plus simple et la moins contraignante à l'utilisateur, tout en garantissant un bon niveau de sécurité. Finalement, l'authentification biométrique contribuera à rendre l'utilisation de certains systèmes plus simple et plus conviviale.

Bibliographies

[1] John D. Woodward, Jr., Christopher Horn, Julius Gatune, and Aryn Thomas “Biometrics

A Look at Facial Recognition” Published 2003 by RAND.

[2] Loubna BEDOUI, « Authentification de visages par la méthode d'analyse discriminante linéaire de Fischer » Ingénieur d'état en Automatique, Université Mohamed Kheider de Biskra 2008.

[3] Simon Liu and Mark Silverman , “A Practical Guide to Biometric Security Technology ” IT Pro January, February 2001.

[4]Anil Jain, Lin Hong and Sharath Pankanti, “ Biometrics : Promising Frontiers for Emerging Identification Market”, Communications of the ACM, pp. 91-98, [February 2000].

[5] Duane M. Blackburn, Mike Bone, P. Jonathon Phillips. “Face recognition vendor test 2000”, Evaluation Report February 16, 2001.

[6] D. Saigaa, N. Benoudjit, K. Benmahamed, S. Lelandais, « Authentification d’individus par reconnaissance de visages », courrier du savoir – n°06, Juin 2005, pp.61-66.

[7] SOUHILA GUERFI ABABSA, « Authentification d’individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D » Thèse, UNIVERSITE D’EVRY VAL D'ESSONNE, 2008.

[8] Florent Perronnin et Jean-Luc Dugelay, « Introduction à la Biométrie Authentification des

Individus par Traitement Audio-Vidéo, (Revue Traitement du Signal, volume 19, numéro 4,

2002).

[9] Y. Belgnaoui, J-C. Guézel et T. Mahé. La biométrie, sésame absolu. Industries et techniques, Juillet 2000.

[10] J. Goy, “Study, conception and fabrication of an APS image sensor in standard CMOS technology for low light level applications such as star trackers”, Ph.D. dissertation, INPGTIMA Laboratory 2002.

[11] Arcelli C. and Baja G.S.D., “A Width Independent Fast Thinning Algorithm,”

IEEE Transaction on pattern Analysis and Machine Intelligence, vol. 4, no. 7, pp. 463-474.

[12] Nalini Ratha, Ruud Bolle Automatic Fingerprint Recognition Systems, Springer, New York,2004

Webographie

[13] http://biometrics.over-blog.com/pages/La_geometrie_de_la_main-2019729.html (2014)

[14] http://biometrics.over-blog.com/pages/Liris-2019780.html(2014)

[15] http://www.biometrie-online.net/technologies/voix (2014)

[16] http://www.biometrie-online.net/technologies/visage (2014)

[17] http://db.apache.org/derby/(2013)

[18] http://fr.scribd.com/doc/7045082/Les-Empreintes-Digitales (2012)

[19] http://www.extpdf.com/emprientes-digitale-pdf.html#pdf (2012)

[20] http://biometrie.online.fr/Dossiers_index.htm (2012)

[21] http://biometrie.scan-r.eu/

[22] file:///C:/Users/intissar/Desktop/works/mini%20projet/divers/Biom%C3%A9trie%20-%20Gestion%20du%20temps%20et%20de%20pr%C3%A9sence%20%E2%80%93%20Synel%20France.htm (20114)

[23]http://lhe.epfl.ch/enseignement/index.php?option=com_content&view=article&id=82%3Atraitement-dimages-avec-matlab&catid=6%3Amatlab&Itemid=13&lang=fr(2012)

[24]file:///C:/Users/intissar/Desktop/works/mini%20projet/divers/Lecteur%20biom%C3%A9trique%20-%20Lecteurs%20biom%C3%A9triques%20-%20Empreinte%20digitale%20-%20Capteur%20biom%C3%A9trique%20-%20Biometrics%20-%20D%C3%A9veloppement%20-%20Ing%C3%A9nierie%20%20%20Biom%C3%A9trie%20Lorraine%20Nancy%2054%20Biometrie%20-%20Scan-r.eu%20Biometrie%20-%20Scan-r.eu.htm(2014)

[25]http://bias.csr.unibo.it/fvc2002/databases.asp(2012)