Université Abou Bekr Belkaid
Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Master en Informatique

Option: *Génie Logiciel (G.L)*

Thème

Reconnaissance des Empreintes Digitales

Réalisé par :

- **Ben Hamed Amina**
- **Medjadji Omar**

Présenté le 17 juillet 2015 devant le jury compose de MM.

-Mme Iles(Présidente)
-Mme Didi Fadoua (Encadreuse).
-Mr Bel housine(Examinateur)
-Mr Ben Ziane (Examinateur)

Année 2015-2016

Remerciement

Louange à Dieu qui ma donné la force, le courage, et l'espoir nécessaire Pou accomplir ce travail et surmonter l'ensemble des difficultés.

Je tiens tout d'abord à remercier mon encadreuse **Mme Didi Fadoua** pour ces conseils et sa disponibilité et son encouragement qui nous ont permis de réaliser ce travail dans les meilleures conditions.

J'exprime également ma reconnaissance à **Iles** D'avoir accepté de présider le jury.

Mes remercîments à **Bel housine**Pour avoir bien voulu juger ce travail Mes remercîments s'adressent également à **Ben Ziane** Pour avoir bien voulu juger ce travail Mes vifs remercîments A tous mes enseignants durant mon cursus universitaire.

Je remercie aussi les personnes qui m'ont aidé en la Police Scientifique de Tlemcen.

Dédicace

Je tiens à dédier ce travail à mes très chers parents, à la mémoire de ma mère qui m'a toujours encouragé dans mes études,

A mon frère Aissa et ma belle-sœur Houda qui m'ont toujours soutenu,

A mes grands-mères et mes grands-pères a la mémoire du défunt,

A mon cher binôme sans qui ce travail n'aurait pas été réalisé

A tous les membres du département informatique,

A tous mes amis qui m'aime

Ben Hamed Amina

Dédicace

A

Mes parents Pour les sacrifices déployés à nos égards ; pour leur patience Leur amour et leur confiance en moi

Ils ont tout fait pour mon bonheur et mon réussite.
Qu'ils trouvent dans ce modeste travail, le témoignage de mon Profonde affection et de mon attachement indéfectible. Nulle dédicace ne puisse exprimer ce que je leur deviens Que dieu leur réserve la bonne santé et une longue vie.

A

Mes chers frères Mohamed, Illyés pour leur encouragement leur soutenir et leur aide pendant tout long année et a mes chers sœur

A

Mes amis surtout Islam, Nadjib, Ali, Osemma

En témoignage de nos sincères reconnaissances pour les efforts Qu'ils ont consentis pour leurs soutenir au cours de mes études.
Que dieu nous garde toujours unis

A toute personne qui aide moi à faire notre projet.

Medjadji Omar.

Table des matières

Introduction Générale

Contexte

La biométrie a une longue histoire même si beaucoup ne le réalisent pas. Depuis des temps immémoriaux, l'Homme reconnaît ses semblables en scrutant leurs visages, leurs voix et leur morphologie. Mais ce n'est pas de ce processus naturel qu'il est question ici, mais bien de la technologie biométrique en tant que telle.

Les Chinois authentifiaient des actes de propriétés par empreintes digitales. Les potiers égyptiens savaient que leurs empreintes marquées dans la glaise permettaient de reconnaître leur production. L'épistémologie est friande d'inventions retrouvées : il faudra attendre la seconde partie du XIX e siècle pour trouver enfin une réflexion biométrique construite avec la démarche de William Herschel qui eu l'idée, au Bengale en 1858, de sécuriser des engagements contractuels par l'impression d'empreintes palmaires. C'est ainsi que naquit la technique d'identification la plus connue et sans conteste la plus démontrée et la plus éprouvée : l'identification par empreinte digitale.

Il fut suivi quelques temps après, en 1883, par Alphonse Bertillon qui, introduisit les techniques anthropométriques pour identifier des criminels n récidivistes. Cette même année, la technique d'identification par empreinte digitale était récupérée dans un roman « The life of the Mississipi » écrit par un certain Longhorn Clemens plus connu sous son nom de plume de Mark Twain.

Avec la conquête de l'Ouest, et l'essor du télégraphe, on découvrit que les télégraphistes avaient un « doigté » caractéristique qui permettait de les reconnaître. Cette technique fut communément utilisée pendant la dernière guerre mondiale pour authentifier les opérateurs de radiotélégraphie. C'est dans le milieu des années soixante,

alors même que l'identification de criminels récidivistes à l'aide d'empreintes digitales était reconnue et utilisée depuis plusieurs décennies par l'ensemble des polices du monde, qu'enfin le FBI lançait un vaste programme de recherche sur le traitement automatique des empreintes digitales. C'est aussi à la même époque que l'université de Sandford démontrait qu'il était possible de « discriminer » une population d'environ 5 000 personnes grâce à la mesure de la longueur des doigts d'une main. Cette technique biométrique fut utilisée expérimentalement pour contrôler l'accès aux salles d'examen. Cela donna naissance au premier système de contrôle d'accès biométrique connu sous le nom d'Identimat.

Problématique

Notre objectif est de mettre en œuvre un système de reconnaissance d'individus à base d'empreintes digitales.

Contribution

On a réalisé les étapes suivantes :

- Les empreintes digitales dans un dossier
- Amélioration de l'empreinte digitale (Niveau de gris, Binaraisation, Squelettisation).
- Les points caractéristiques de l'empreinte digitale
- Reconnaissance de l'individu à partir de ces minutiers de leur empreinte digitale.

PLAN DU MEMOIRE :

Notre mémoire est présenté en trois chapitres décrit comme suit :

Dans le premier chapitre, nous introduisons quelques définitions de la biométrie, puis nous détaillons les différentes modules dans un système biométrique (module d' apprentissage, reconnaissance et module d'adaptation) et les différentes moyennes

biométriques (Moyens biométriques physiques, comportementaux et expérimentaux).

Ensuite, le deuxième chapitre est consacré de prendre l'empreinte digitale comme une image numérique et faire un traitement sur cette image, c'est là où on va définir les traitements les plus utiles pour l'amélioration de la qualité d'une image l'extraction de l'information à partir de l'image (le seuillage, squelettisation et l'extraction des minutiers).

En fin, nous terminons ce travail par une description de notre système, on définit les différentes fenêtres à partir de chargement de l'empreinte jusqu'au l'extraction des minutiers… etc. Et une conclusion des résultats obtenus et les problèmes rencontrés durant le développement de l'application.

La Biométrie

1. Introduction

La biométrie est une alternative aux deux précédents 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. La voix, l'écriture, le rythme de frappe sur un clavier, etc. sont des caractéristiques comportementales. Ces caractéristiques, qu'elles soient innées comme les empreintes digitales ou bien acquises comme la signature, sont attachées à chaque individu et ne souffrent donc pas des faiblesses des méthodes basées sur une connaissance ou une possession.

En effet, un attribut physique ou comportemental ne peut être oublié (cf. le slogan de Nuance **[1]** : « No PIN to remember, no PIN to forget ») ou perdu. En général, ils sont très difficiles à « deviner » ou à « voler » ainsi qu'à « dupliquer » **[2]**.

Savoir déterminer de manière à la fois efficace et exacte l'identité d'un individu est devenu un problème critique dans notre société. Notre identité est vérifiée quotidiennement par de multiples organisations : lorsque nous utilisons notre carte bancaire, lorsque nous accédons à notre lieu de travail, lorsque nous nous connectons à un réseau informatique, etc.

Il existe traditionnellement deux manières d'identifier un individu :

- La première méthode est basée sur une connaissance (knowledge-based). Cette connaissance correspond par exemple au mot de passe utilisé au démarrage d'une session Unix ou au code qui permet d'activer un téléphone portable.

- La seconde méthode est basée sur une possession (token-based). Il peut s'agir d'une pièce d'identité, une clef, un badge, etc. Ces deux modes d'identification peuvent être utilisés de manière complémentaire afin d'obtenir une sécurité accrue comme pour la carte bleue.

Cependant, elles ont leurs faiblesses respectives. Dans le premier cas, le mot de passe peut être oublié par son utilisateur ou bien deviné par une autre personne. On estime ainsi qu'une personne sur quatre écrits directement sur sa carte bleue son code secret afin de ne pas l'oublier **[3]**. Dans le second cas, le badge (ou la pièce d'identité ou la clef) peut être perdu ou volé.

2. Les débats sur la biométrie

Si la biométrie est un sujet récent, il reste néanmoins que le débat sur les technologies de sécurité et les libertés ne date pas d'hier, c'est en fait un souci que les intellectuels ont depuis longtemps. Ici seront présentées les principales contributions sur le sujet.

Il faut cependant noter que puisque que la biométrie est une technologie extrêmement récente et évolue rapidement, il est normal que l'internet soit une importante source d'information sur le sujet, surtout afin d'être à jour dans la compréhension de la biométrie et de ses impacts. **[4]**

3. Définition

La biométrie est composé de deux termes : bio / métrie c'est la « mesure du vivant ». [5]

Elle est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiologiques ou comportementales. Il peut y avoir plusieurs types de caractéristiques, les unes plus fiables que d'autres, mais toutes

doivent être ***infalsifiables*** et ***uniques*** pour pouvoir être représentatives d'un et un seul individu.

3.1. Pourquoi la biométrie ?

Les arguments pour la biométrie se résument en 2 catégories:
Praticité : Les mots de passe comme les cartes de crédit, les cartes de débit, les cartes d'identité ou encore les clés peuvent être oubliés, perdus, volés et copiés.
En plus, aujourd'hui tous et chacun doivent se rappeler une multitude de mots de passe et avoir en leur possession un grand nombre de cartes. De son côté la biométrie serait immunisée contre ce genre de maux en plus qu'elle serait simple et pratique, car il n'y a plus ni cartes ni mots de passe à retenir.

La biométrie serait capable de réduire, sans l'éliminer, le crime et le terrorisme car, à tout de moins, elle complique la vie des criminels et des terroristes. **[4]**

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

- **L’analyse morphologique :** les empreintes digitales, l’iris, la forme de la main, les traits du visage, le réseau veineux de la rétine.
- **L’analyse biologique :** l’ADN, le sang, la salive, l’urine, l’odeur, la thermographie.
- **L’analyse comportementale :** la reconnaissance vocale, la dynamique de frappe au clavier, la dynamique de signature, la manière de marcher. [5]

4. Architecture d’un système biométrique

Il existe toujours au moins deux modules dans un système biométrique :
Le module d’apprentissage et celui de reconnaissance [3]. Le troisième module (facultatif) est le module d’adaptation. Pendant l’apprentissage, le système va acquérir une ou plusieurs mesures biométriques qui serviront à construire un modèle de l’individu.

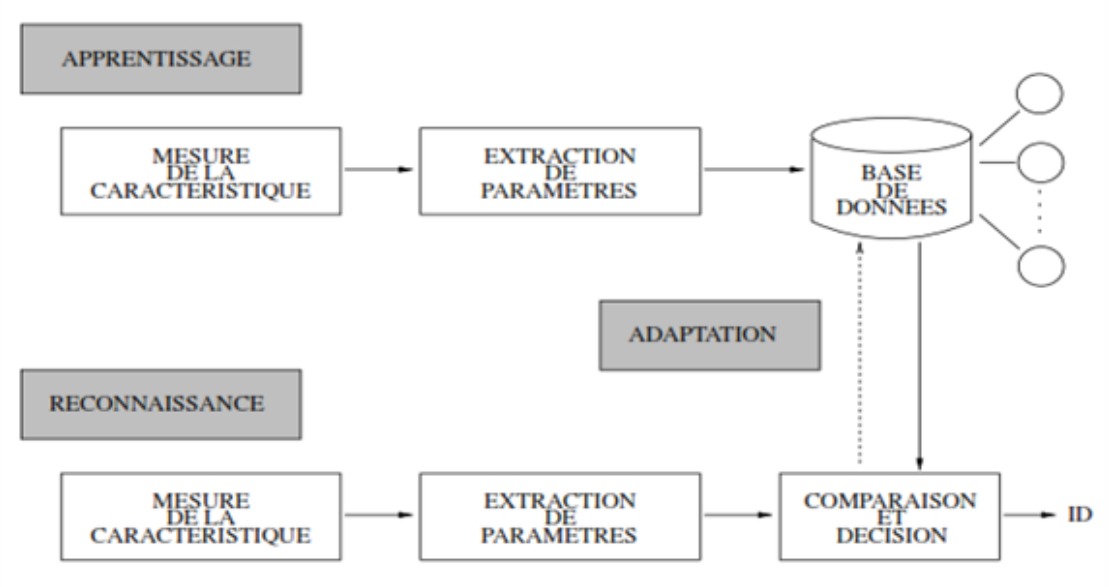


Figure 1.1: Architecture d'un système biométrique.

4 .1. Module d'apprentissage

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

4.2. Module de reconnaissance

Au cours de la reconnaissance, la caractéristique biométrique est mesurée et un ensemble de paramètres est extrait comme lors de l'apprentissage. Le capteur utilisé doit avoir des propriétés aussi proches que possibles du capteur utilisé durant la phase d'apprentissage.

Si les deux capteurs ont des propriétés trop différentes, il faudra en général appliquer une série de prétraitements supplémentaires pour limiter la dégradation des performances.

La suite de la reconnaissance sera différente suivant Le mode opératoire du système identification ou vérification.

En mode identification, le système doit deviner l'identité de la personne. Il répond donc à une question de type : « Qui suis-je ? ». Dans ce mode, le système compare le signal

mesuré avec les différents modèles contenus dans la base de données (problème de type 1:n).

En général, lorsque l'on parle d'identification, on suppose que le problème est fermé, c'est-à-dire que toute personne qui utilise le système possède un modèle dans la base de données.

4.3. Module d'adaptation

Pendant la phase d'apprentissage, le système biométrique ne capture souvent que quelques instances d'un même attribut afin de limiter la gêne pour l'utilisateur. Il est donc difficile de construire un modèle assez général capable de décrire toutes les variations possibles de cet attribut.

De plus, les caractéristiques de cette biométrie ainsi que ses conditions d'acquisition peuvent varier. L'adaptation est donc nécessaire pour maintenir voire amélioré la performance d'un système utilisation après utilisation.

5. Les moyens biométriques :

5.1 Moyens biométriques physiques :

5.1.1 L'empreinte digitale

Définition :

Les empreintes digitales sont le dessin formé par les lignes de la peau des doigts, ils appelées aussi dermatoglyphes - sont une signature que nous laissons derrière nous à chaque fois que nous touchons un objet. Les motifs dessinés par les crêtes et plis de la peau sont différents pour chaque individu ; c'est ce qui motive leur utilisation par la police criminelle depuis le 19è siècle.

On distingue deux types d'empreintes : *l'empreinte directe ou visible* qui laisse une marque visible à l'œil nu et l'empreinte *latente ou invisible* qui est composée de lipides, de sueur et de saletés déposés sur un objet touché. [5]

Une empreinte digitale se compose principalement de crêtes (Ridges) et de vallées (Valleys). On regroupe ces points clés de l'empreinte sous le terme de

minuties. C'est l'étude des minuties qui permet d'identifier de façon certaine un individu.

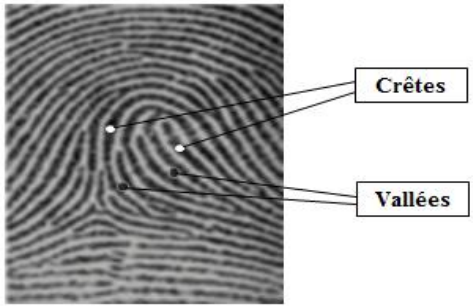


Figure 1.2 : Empreinte digitale

5.1.2 La forme de la main

Définition :

La biométrie par la forme de la main est une technologie populaire qui est largement employée pour le contrôle d'accès physique ou le pointage horaire.

Le système prend une photo de la main et examine 90 caractéristiques, y compris la forme tridimensionnelle de la main, de la longueur et de la largeur des doigts et de la forme des articulations.

Pour utiliser la géométrie de la main, l'utilisateur place sa main sur une platine possédant des guides pour positionner les doigts.

Les lecteurs du contour de la main offrent un niveau très raisonnable d'exactitude, mais peuvent avoir des taux de fausse acceptation élevée pour des jumeaux ou d'autres membres de la même famille.

Figure 1.3 : Lecteur de la forme de la main

5.1.3 Le visage

5.1.3 .1 Définition :

Rien n'est plus naturel qu'utiliser le visage pour identifier une personne. Les images faciales sont probablement la caractéristique biométrique la plus communément employée par l'homme pour effectuer une identification personnelle.

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

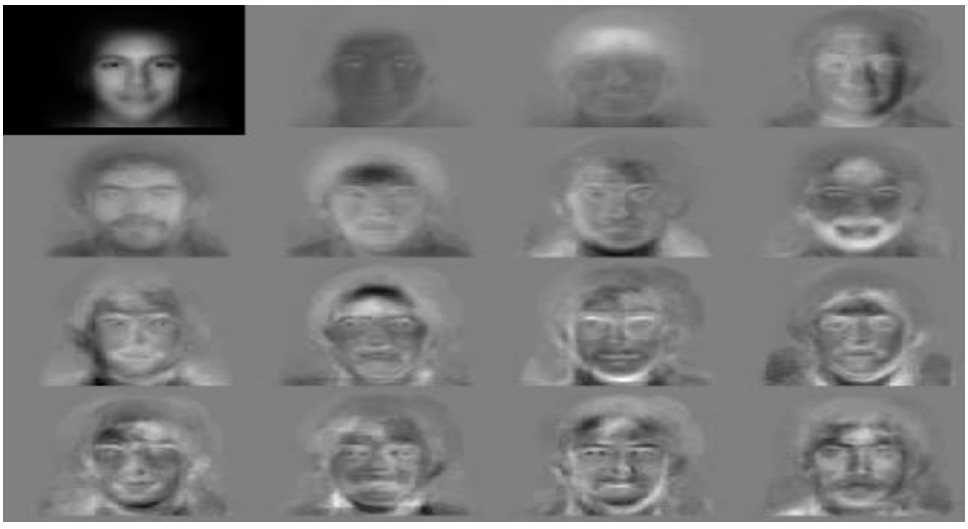


Figure 1.4 : Caractéristiques du visage

5.1.3.2 Les modes de fonctionnement (Surveillance ou Recherche)

5.1.3.2.1.Mode Surveillance

Le système peut détecter automatiquement la forme d'un visage, en extraire l'image, exécuter l'identification en s'appuyant sur une base de données d'individus préenregistrés.

Il calcule rapidement le degré de recoupement entre l'empreinte du visage réel qui vient d'être capté et ceux associés aux individus connus enregistrés dans une base de données biométrique d'images faciales.

Il peut retourner une liste d'individus possibles triée par score décroissant (images ressemblantes) ou il peut simplement retourner l'identité du sujet (résultat le plus haut) et un niveau de confiance associé. Ceci paramétrable au choix de l'opérateur.

En mode Surveillance il fonctionne en temps réel et dans le même temps, capte les images et recherche dans la base de données. L'architecture technique mise en place pour cela est fonction des besoins de l'application (nombre d'individus enregistrés, vitesse de défilement devant la caméra, flux…)

Une autre fonction du mode Surveillance permet de trouver des visages humains n'importe où dans le champ de vision du système et à toute distance. Il peut les suivre de façon continue et les extraire de l'image, en comparant le visage ainsi isolé avec une liste de visages stockés.

5.1.3.2.1.Mode Recherche

Le mode Recherche peut être utilisé en mode IDENTIFICATION (un à plusieurs) ou en mode VERIFICATION (un à un).

5.1.4 L'iris

Définition :

L'iris est la région annulaire située entre la pupille et le blanc de l'œil. Les motifs de l'iris se forment au cours des deux premières années de la vie et sont stables. Les iris sont uniques et les deux iris d'un même individu sont différents. Dans l'iris de l'œil, il est possible de compter plus de 200 paramètres indépendants. [5]

La capture de l'iris se fait par une caméra standard.

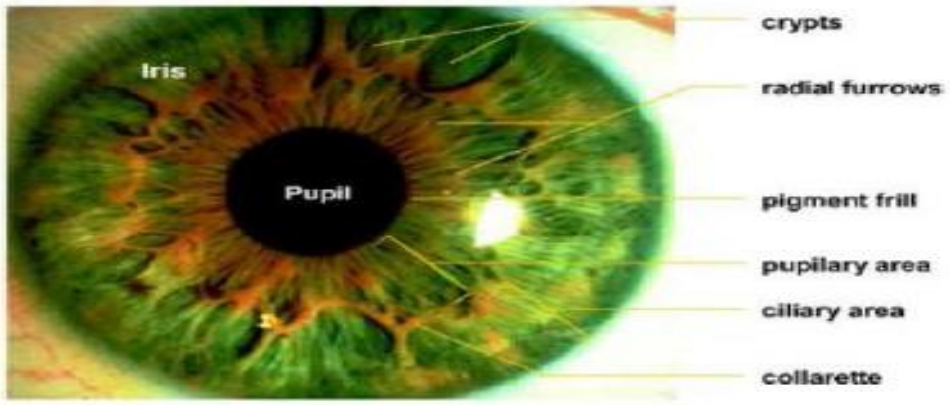


Figure 1.5 : Vue détaillée de l'œil humain

2

5.1.4 La rétine

Définition :

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 vasculariser les cellules qui permettent la vision.

La grande variété de configurations des vaisseaux sanguins présenterait 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. [5]

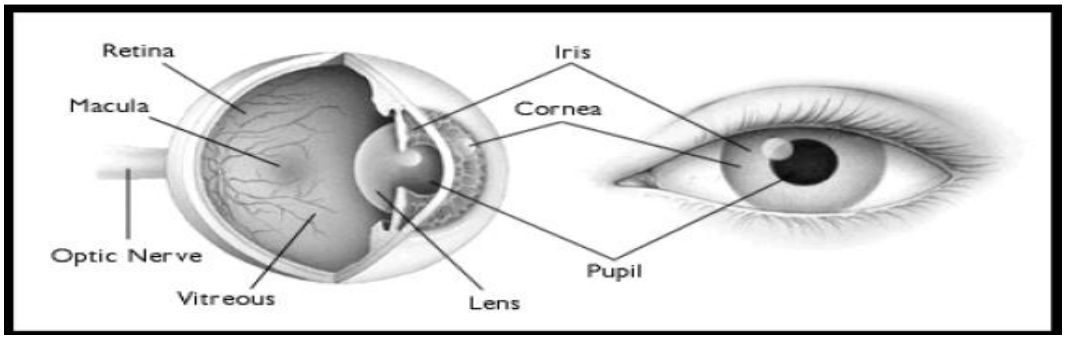


Figure 1.6. : Détail d'une rétine

La reconnaissance de la rétine est actuellement considérée comme une des méthodes biométriques les plus sûres. L'image est obtenue en projetant sur l'œil un rayon lumineux de faible intensité dans les fréquences visibles ou infrarouges. L'œil doit être situé très près de la tête de lecture et l'utilisateur doit fixer son regard sur un point déterminé pendant plusieurs secondes ce qui demande une grande coopération de sa part.

5.2 Moyens biométriques comportementaux :

5.2.1 La voix

Chaque personne possède une voix propre caractérisée par une fréquence, une intensité et une tonalité et que l'on peut analyser par enregistrement avec un microphone. Même si deux voix peuvent sembler similaires pour l'oreille, le traitement informatique permet de les isoler.

La reconnaissance du locuteur vise à déterminer les caractéristiques uniques de la voix de chaque individu. Cette biométrie est en général très bien acceptée car la voix est un signal naturel à produire.

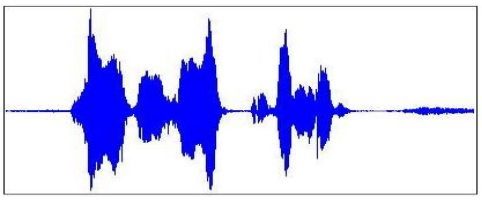


Figure 1.7 : Signal de la voix

5.2.2 La signature dynamique

Cette technique est encore peu répandue, et peu de constructeurs la proposent. La vérification dynamique de signature est basée sur la différentiation entre les parties d'une signature qui sont habituelles et celles qui changent avec presque chaque signature. Les systèmes d'authentification de signature incluent habituellement un crayon lecteur et une tablette à digitaliser électronique. [6]

Figure 1.8 : Dynamique de signature

5.2.3 La dynamique de frappe au clavier

Il s'agit d'une technique de reconnaissance des personnes basée sur le rythme de frappe qui leur est propre. C'est une solution biométrique « Software Only », car elle consiste uniquement en un relevé de données basées sur la dynamique de frappe des utilisateurs. Elle est appliquée au mot de passe qui devient ainsi beaucoup plus difficile à imiter.

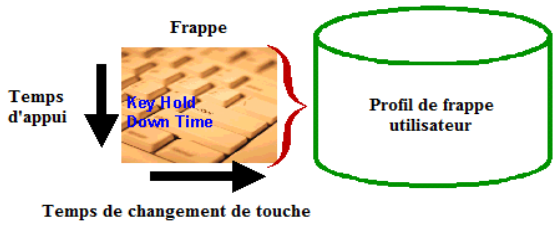


Figure 1.9 : Dynamique de frappe au clavier

5.3 Moyens biométriques expérimentaux :

5.3.1 La thermographie

Une caméra thermique est utilisée pour réaliser un cliché infrarouge du visage. Cela permet de faire apparaître une répartition de la chaleur unique à chaque individu, voire de cartographier le réseau veineux du visage invisible à l'œil nu. L'avantage est que l'on peut distinguer de vrais jumeaux. Très cher, ce système reste expérimental.

Figure 1.10. La thermographie

5.3.2 L’oreille

Cette technique consiste à comparer les empreintes d’oreille que peuvent laisser certains individus dans le cadre d’un délit.

Cette méthode est uniquement utilisée par la police, mais est admissible devant une cour de justice. [5]

5.3.3 L'ADN

L'analyse des empreintes génétiques est une méthode extrêmement précise d'identification, issue directement de l'évolution de la biologie moléculaire.

- L'information génétique d'un individu est unique car aucun membre de l'espèce ne possède la même combinaison de gènes codés dans l'acide désoxyribonucléique (ADN).
- Trace individuelle unique : l'ADN est l'outil d'identification par excellence.
- L'analyse ADN : l'analyse des empreintes génétiques est devenue en quelques années l'un des outils majeurs de la criminalistique, la science de l'identification des indices matériels. 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. [5]

6. Conclusion :

La recherche en biométrie est donc un domaine à très fort potentiel. Cependant, nombreuses sont les personnes qui craignent que l'essor de la biométrie ne s'accompagne d'une atteinte généralisée à la vie privée des individus. Tout d'abord le manque de fiabilité des systèmes biométriques inquiète.

Même si aujourd'hui les passagers sont prêts à faire des concessions pour garantir leur sécurité, ils accepteront sans doute très mal ces erreurs à répétition. Et bien que des progrès constants soient enregistrés séparément pour chaque modalité, la performance des systèmes à un seul mode est encore loin d'être satisfaisante ce qui plaide en faveur du développement de systèmes biométriques multimodaux. Un problème très différent est le stockage de données personnelles dans des bases de données biométriques et l'utilisation malveillante qui pourrait en être faite.

La Reconnaissance des Empreintes Digitales

1. Introduction

Depuis longtemps, le public sait que : Une image veut mieux que mille mots. Combinée avec la parole, l'image constitue un moyen essentiel dans la communication homme-machine. C'est un moyen de communication universel dont la richesse du contenu permet aux êtres humains de tout âge et de toute culture de se comprendre.

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

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

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

Le principe de la Reconnaissance des Empreintes Digitales consiste à comparer 2 empreintes fournies au système à une ou plusieurs autres empreintes aussi appelé « Template» ou signatures, le système biométrique renvoie un résultat positif au cas où l'empreinte fournie à l'entrée correspond à l'un des Template, et un résultat négatif dans le cas contraire.

2. Historique

La prise d'empreinte digitale est la plus ancienne des techniques biométriques, dans l'histoire « la Dactyloscopie » ce terme signifie l'étude des empreintes papillaires digitales en générale [7] .

En 1892 L'anthropologue anglais Francis Galton étudie les empreintes digitales, il établit une classification expérimentale de plus de 2500 séries d'empreintes, et en 1898 Edward Richard Henry inspecteur générale de la police londonienne a mis en place un système de classification des empreintes.

Dans ce système le classement repose sur la topographie générale de l'empreinte digitale et permet de définir des caractéristiques.

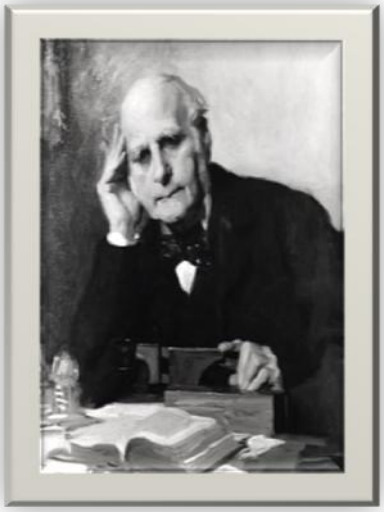


Figure 2.1 : Francis Galton.

3. L'empreinte Digitale

L'empreinte digitale est très efficace pour l'identification d'un individu, car il est impossible de trouvé deux empreintes similaires, Les jumeaux venant de la même cellule, auront des empreintes très proches mais pas semblables, et aujourd'hui les empreintes sont reconnues comme méthodes d'identification fiable [8].

3.1. Définition de l'empreinte digitale

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

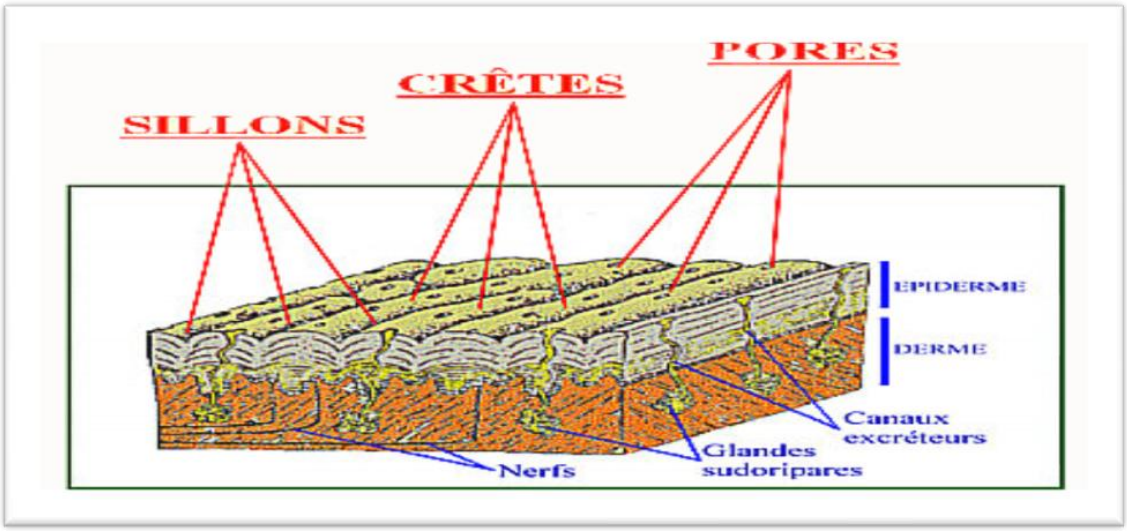


Figure 2.2 : Etude du dessin digital.

3 .2. Les points caractéristiques de l'empreinte digitale

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 .2 .1 .Les points singuliers globaux

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

- **Le Core :** centre ou le noyau contient de courbure maximale des lignes de l'empreinte.
- **Le Delta :** est proche du lieu où se deux lignes, aussi est le lieu de divergence des lignes les plus internes. (voir Figure 2 .3)

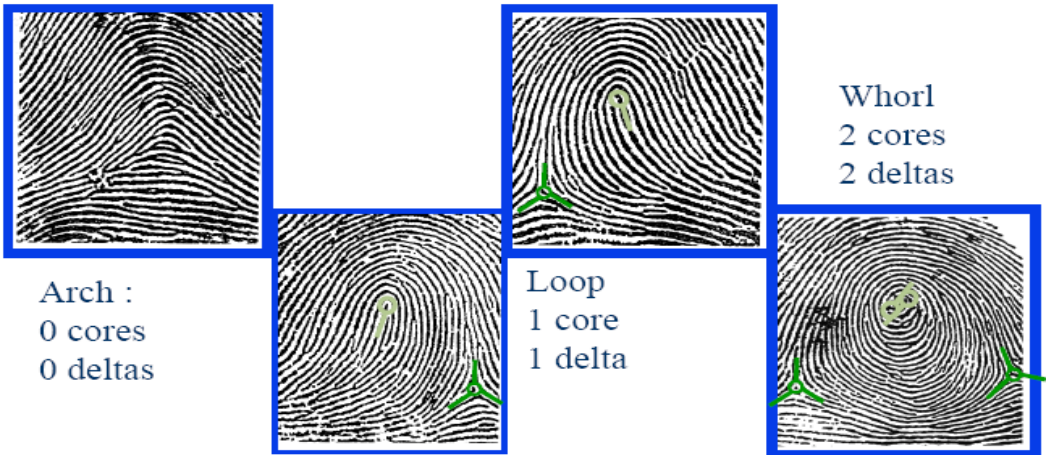


Figure 2.3: Différents positions de Delta.

3 .2.2. Les points singuliers locaux (minutiers)

En chaque empreinte il y a des minuties spécifiques permettent de différencier et classer les empreintes, et il ya plusieurs formes des minutiers généralement on a quatre types :

- **Les coupures :** terminaison à droite ou à gauche, minuties située en fin de stries. (voir Figure2.4)
- **Les divisions :** Bifurcation à droite ou à gauche, intersection de deux stries. (voir Figure 2.5)

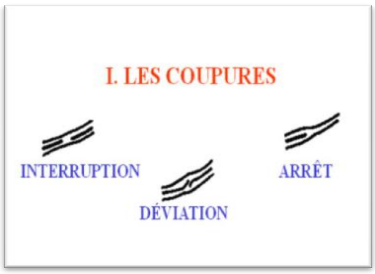
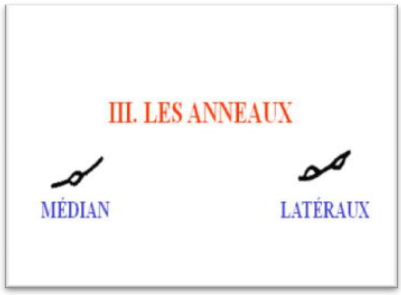


Figure 2.4: Les Coupures. **Figure 2.5:** Les Divisions**.**

- **Les anneaux :** Lac, assimilée à deux bifurcations. (voir Figure 2.6)
- **Les ilots:** assimilés à deux terminaisons. (voirII.Figure2.7)



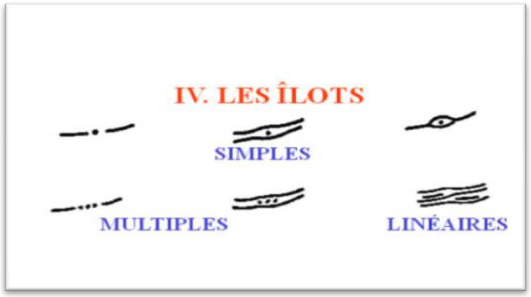


Figure 2.6: Les Anneaux **Figure 2.7**: Les îlots**.**

3 .3 .Les classes de l'empreinte digitale

Français Galton (1822-1916) ont été faites les premières études scientifiques sur les classifications des empreintes digitales, ces études ont affiné par Edward Henry (1850-1931), il est classé les empreintes en cinq classes : arc, arc tendu, boucle à gauche, boucle à droite, et spire.

- **Classe 1**:il contient en maximum un Delta et au moins une crête montre une courbure élevée, est une classe poubelle. [7]
- **Classe 2**:il contient un Delta à droite et des boucles situé en côté à gauche de l'empreinte.
- **Classe 3**:il contient un Delta à gauche et des boucles situé en côté à droite de l'empreinte.
- **Classe 4**:il contient un Delta à gauche et d'autre à droite avec un centre spirale. [9]
- **Classe 5**:il contient trois Delta autour de forme besace

- **Classe 6**:il contient des empreintes invisibles.

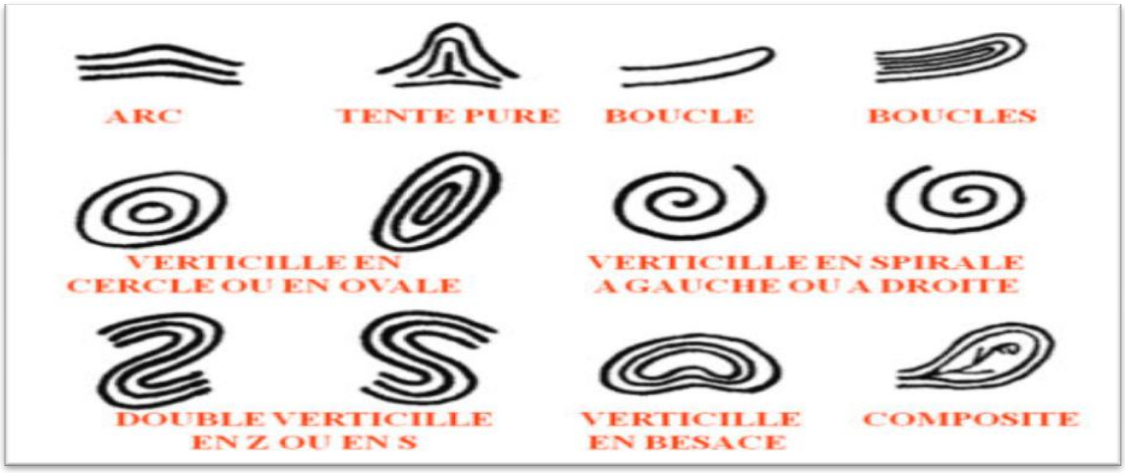


Figure 2.8: Les formes des crêtes à la zone centrale de l'empreinte.

4. Amélioration de l'empreinte digitale

Pour améliorer la reconnaissance des empreintes digitales il faut d'abord faire un traitement l'empreinte, cette traitement prendre l'empreinte digitale comme une image numérique .Dans un côté informatique c'est quoi une image numérique ? .

On peut représenter l'image numérique comme une interface divisé dans ensembles des cellules appelée pixels de tailles fixes et chaque pixel a une couleur correspond à l'image réal. Et on générale l'image numérique définie par un ensemble de pixels situé dans un espace limité par une hauteur et largeur.

Le dynamique de l'image chaque pixels pendre teintes de gris ou des couleurs [10].

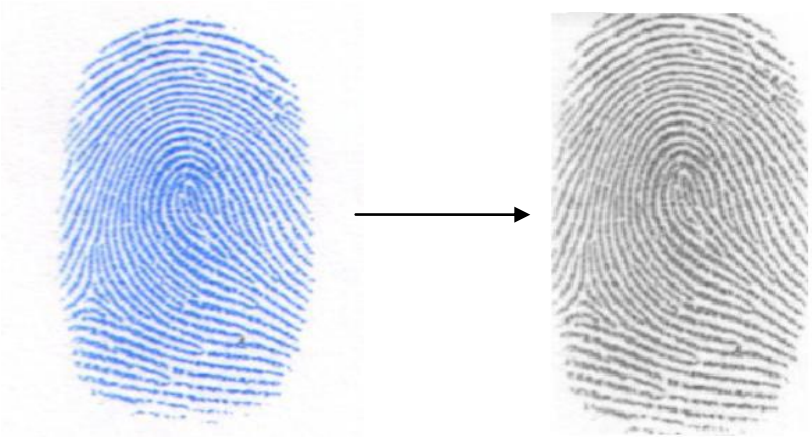
4.1. Quelques traitements sur l'image de l'empreinte digitale

Il ya plusieurs techniques de traitement d'image d'un empreinte digitale, nous allons présenter quelques-uns :

4 .1.1.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.

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.

Figure 2.9: L'empreinte digitale en gris.

4 .1.2.Seuillage (Binaraisation)

Le seuillages est une technique simple et efficace pour séparer les objets au fond, la difficulté apparaitre dans le choix des seuils optimaux pour une séparation optimal, le seuillages permet de trouver une image binaire à partir d'une image d'origine en niveau de gris.

Soit l'image I(X, Y), supposons que f(x, y) représente le niveau de gris du pixel aux coordonnées (x, y), $0 \leq x < X$, $0 \leq y < Y$ et S est le seuil choisi.

On choisit un seuil : c'est un niveau de gris qui va nous permettre de prendre une décision. On parcourt l'image en niveaux de gris. Si le pixel sur lequel on se trouve est plus clair que le seuil, il devient blanc. Sinon, il devient noir. Pour le seuillage inverse, c'est le contraire : si le pixel est plus clair que le seuil, il devient noir, sinon, il devient blanc.

L'image I est déterminée par les pixels(x, y) dont la valeur est :

$$I(x,y) = \begin{cases} 0 \, si \, f(x,y) < S \\ 255 \, si \, f(x,y) \geq S \end{cases}$$

```
seuil = (Integer.valueOf(reponse));
int X = transfert.getWidth();
int Y = transfert.getHeight();
int  colB=new Color(255,255,255).getRGB();
int  colN=new Color(0,0,0).getRGB();
int  colMoyen=new Color (seuil,seuil,seuil).getRGB();
        for (int x=0; x<X; x++) {
            for (int y=0;y<Y; y++) {
               int k = transfert.getRGB(x, y);
               if (k >=colMoyen )
               transfert.setRGB(x, y,colB);
               if (k <colMoyen)
               transfert.setRGB(x,y,colN);
            }
        }
```

Figure 2.10: Code source de binarisation.

L'empreinte originale l'empreinte en gris

Figure 2.11: Binarisation de l'empreinte digitale.

5 .1.3.Squelettisation

Squelettisation permet de trouver un nombre minimal de l'information,

sous une forme qui soit à la fois simple à extraire et commode à manipuler.et il faut effectuer la squelettisation sur une image binaire. [11]

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

Figure 2.12: Squelettisation de l'empreinte digitale.

5. Caractérisation par minutie

5.1. Introduction

Le traitement de l'image de l'empreinte, il est effectué par un ensemble des algorithmes qui sont permettent de trouver des caractéristiques spécial à chaque empreinte digitale. Parmi de ces algorithmes on trouve algorithme de Marthon, algorithme de Zhang et Suen

5.2 .Algorithme de Marthon

C'est un algorithme de suppression de points.

Soit le point M considéré de coordonnées (x, y). Soit l'ensemble M_i (x_i, y_i) 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 :

$$X = (x_1-x) + (x_2-x) +...+ (x_n-x)$$

$$Y = (y_1-y) + (y_2-y) +...+ (y_n-y)$$

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. [12]

5.2 .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 2.1**)

A la 2ème itération les conditions (1) et (2) ne changent pas plus les conditions suivantes dans (t) sont réalisées.(voir **Table 2.1**)

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 2.1 : Table des conditions à chaque itération

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]

5.2 .Extraction minutier

Les *minuties* de l'empreinte digitale sont extraites à partir de son squelette en calculant la « connectivité » *CN* en chaque point de l'image *P* de la manière suivante :

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

```
int CN =((Math.abs( filtre[i-1][j-1]-filtre[i-1][j])/255)+
      Math.abs((filtre[i-1][j]-filtre[i-1][j+1])/255)+
       Math.abs ((filtre[i-1][j+1]-filtre[i][j+1])/255)+
        Math.abs((filtre[i][j+1]-filtre[i+1][j+1])/255)+
        Math.abs((filtre[i+1][j+1]-filtre[i+1][j])/255)+
        Math.abs((filtre[i+1][j]-filtre[i+1][j-1])/255)+
         Math.abs((filtre[i+1][j-1]-filtre[i][j-1])/255)+
       Math.abs((filtre[i][j-1]-filtre[i-1][j-1])/255))/2;
```

Figure 2. 13: Code source de la connectivité CN.

En effet le coefficient *CN* présente des caractéristiques (tableau 2) qui permettent d'identifier la nature d'une *minutie* en fonction du résultat obtenu lors du calcul de *CN*.

CN	Nature de la minutie en P
0	Erreur ====> point isolé
1	Terminaison
2	Erreur ====> point appartient sillon
3	Bifurcation
4	Erreur ====> minutie à 4 branches

Table 2.2 : Identification d'une minutie à partir du calcul de CN

```
if (CN==1)
 {
        int rgb = new Color(255,0,0).getRGB();
  pixel[i-1][j-1]=rgb;pixel[i-1][j]=rgb;pixel[i-1][j+1]=rgb;pixel[i][j-1]=rgb;
  pixel[i][j+1]=rgb;pixel[i+1][j-1]=rgb;pixel[i+1][j]=rgb;pixel[i+1][j+1]=rgb;

  cord[0][nbr_point]=i;
  cord[1][nbr_point]=j;
  cord[2][nbr_point]=-1;
  nbr_point++;
  nbr_fin++;
       }
```

Figure 2. 14: Code source des minuties en fin de ligne(Terminaison).

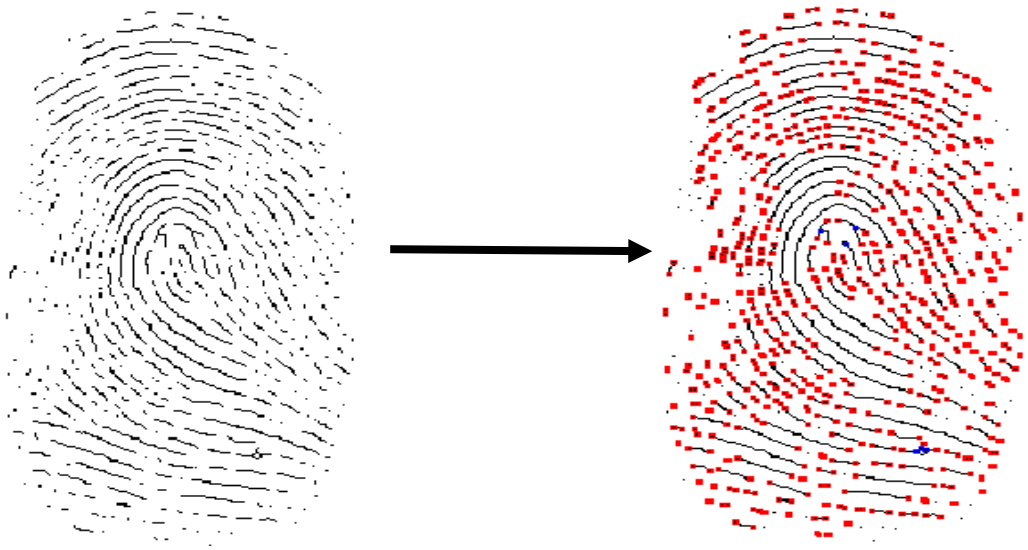
```
    else if (CN==3)
{
int rgb = new Color(0,0,249).getRGB();

    pixel[i-1][j-1]=rgb;pixel[i-1][j]=rgb;pixel[i-1][j+1]=rgb;pixel[i][j-1]=rgb;
    pixel[i][j+1]=rgb;pixel[i+1][j-1]=rgb;pixel[i+1][j]=rgb;pixel[i+1][j+1]=rgb;

      cord[0][nbr_point]=i;
      cord[1][nbr_point]=j;
      cord[2][nbr_point]=0;
      nbr_point++;
      nbr_bifurcation++;
            }
```

Figure 2. 15: Code source des minuties d'intersection de deux lignes (Bifurcation).

Le résulta obtenu :



Empreinte squelette

Figure 2. 16: Les minuties en empreinte digitale.

Les points rouges : fin de ligne (Terminaison).

Les points blues : intersection de deux lignes (Bifurcation).

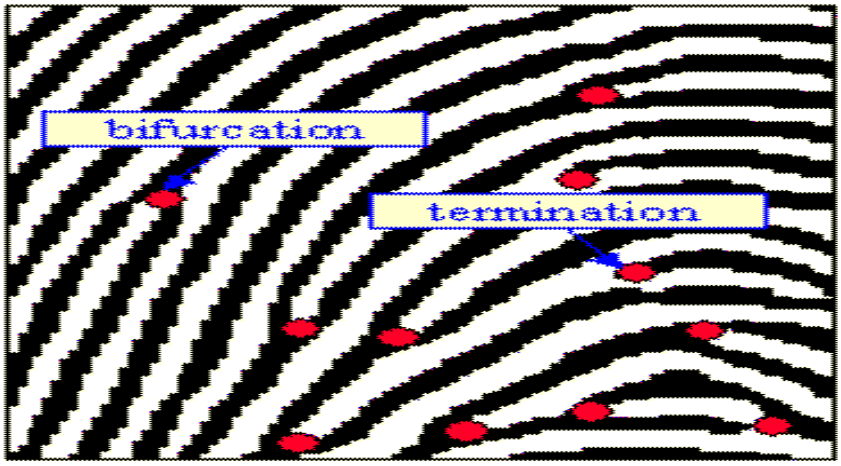


Figure 2.17: Les terminaisons et les bifurcations.

Les *minuties* présentes au sein de l'image de l'empreinte digitale, que l'on sauvegarde dans un liste *L1* en associant à chacun d'entre eux la position absolue (xP,yP) correspondante et le type de *minutie* dont il s'agit (*terminaison* ou *divergence*).

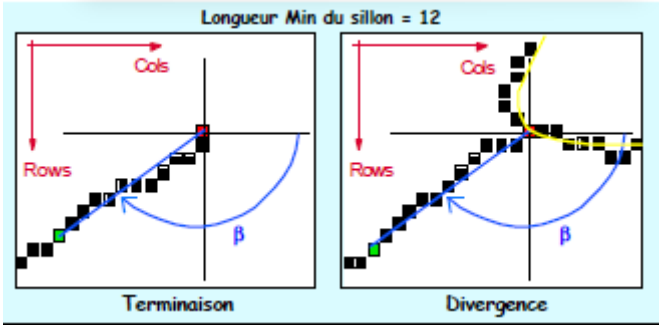


Figure 2.18: Détermination de la direction des minuties.

5. Conclusion

Bien que la reconnaissance des empreintes digitales fasse ses preuves aujourd'hui, des améliorations doivent encore être apportées dans ce domaine. L'inefficacité des systèmes automatiques face aux empreintes de mauvaise qualité et le temps nécessaire au système pour identifier une empreinte font actuellement l'objet de plusieurs recherches.

Conception et Implémentation

1. Introduction

Notre application consiste à développer un système biométrique de reconnaissance des individus par leurs empreintes digitales.

Dans ce dernier chapitre, nous présentons les différentes étapes réalisées durant le développement de notre application, nous commençons tout d'abord par la collection de la base de données (nous avons utilisées une base de donnée sous forme d'un fichier .XML) ensuite, nous définissons les fonctionnalités de notre application avec des captures de l'interface, aussi nous décrivons les différentes diagrammes (diagramme de cas d'utilisation, diagramme de classe et diagramme de séquence) et enfin nous discutons les résultats obtenus.

2 .Conception de l'application

2 .1.Modélisation avec UML

UML (Unified Modeling Language) : se définit comme un langage de modélisation des systèmes d'information graphique et textuel destiné à comprendre et décrire des besoins, spécifier, concevoir des solutions et communiquer des points de vue.

UML est un langage visuel pour comprendre un système communiquer et travailler à plusieurs individus, aider à spécifier, concevoir et développer un système d'information avec différents modèles et différentes vues.

UML ne propose pas de méthode de réalisation. UML est totalement indépendant des langages objet de développement. Une fois la problématique modélisée, une méthode de conduite de projet axée sur la qualité est généralement suffisante pour mener à bien le projet. [AA]

UML propose plusieurs types de diagrammes parmi lesquels, nous avons présenté trois types :

2.1.1 Diagrammes de cas d'utilisation

Un diagramme de cas d'utilisation (use case) représente un ensemble de séquences d'actions réalisées par le système et produisant, un résultat observable intéressant pour un acteur particulier, et modélise un service rendu par le système. Il exprime les interactions acteurs/système et apporte une valeur ajoutée « notable » à l'acteur concerné, et permet de structurer les besoins des utilisateurs et les objectifs correspondants d'un système. (Voir Figure 3.1)

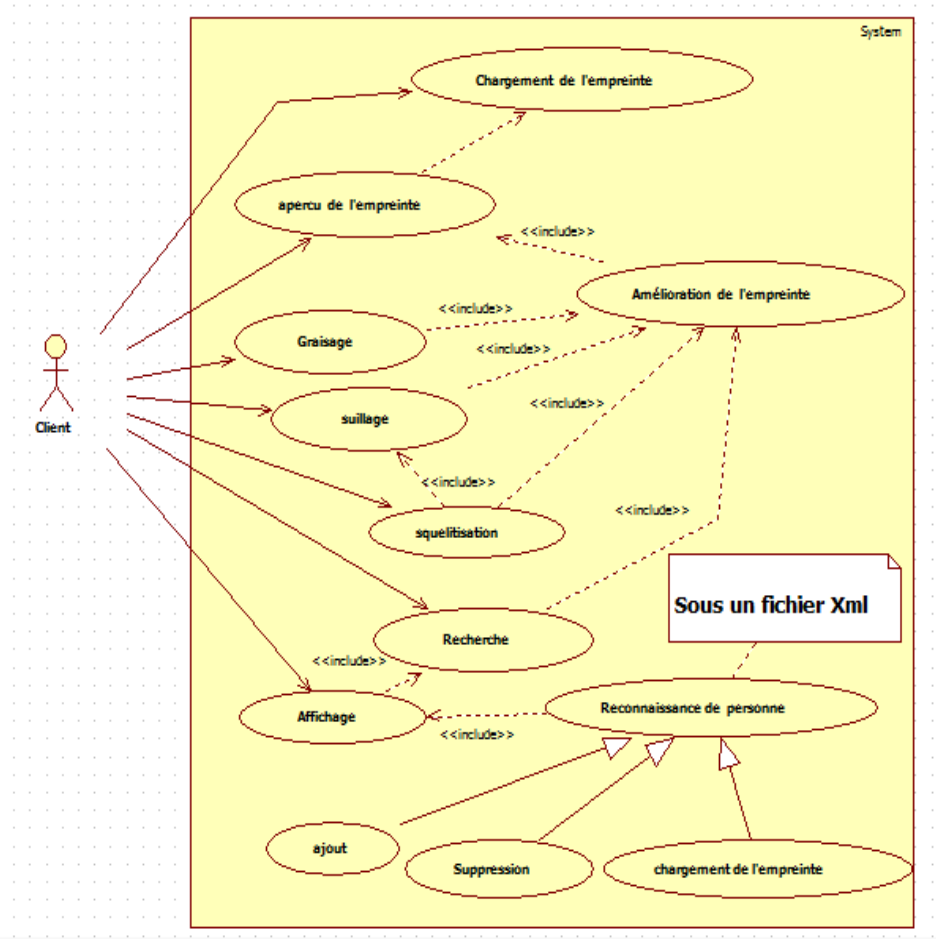


Figure 3.1 : Diagramme de cas d'utilisation.

2.1.2 Diagramme de séquence

Un diagramme de séquence permet de représenter des collaborations entre objets selon un point de vue temporel. Les objets communiquent en échangeant des messages représentés sous forme de flèches. Il peut servir à illustrer un cas d'utilisation, L'ordre d'envoi d'un message est déterminé par sa position sur l'axe vertical du diagramme, le temps s'écoule "de haut en bas" de cet axe.

Voici un exemple de diagramme de séquence de notre application :

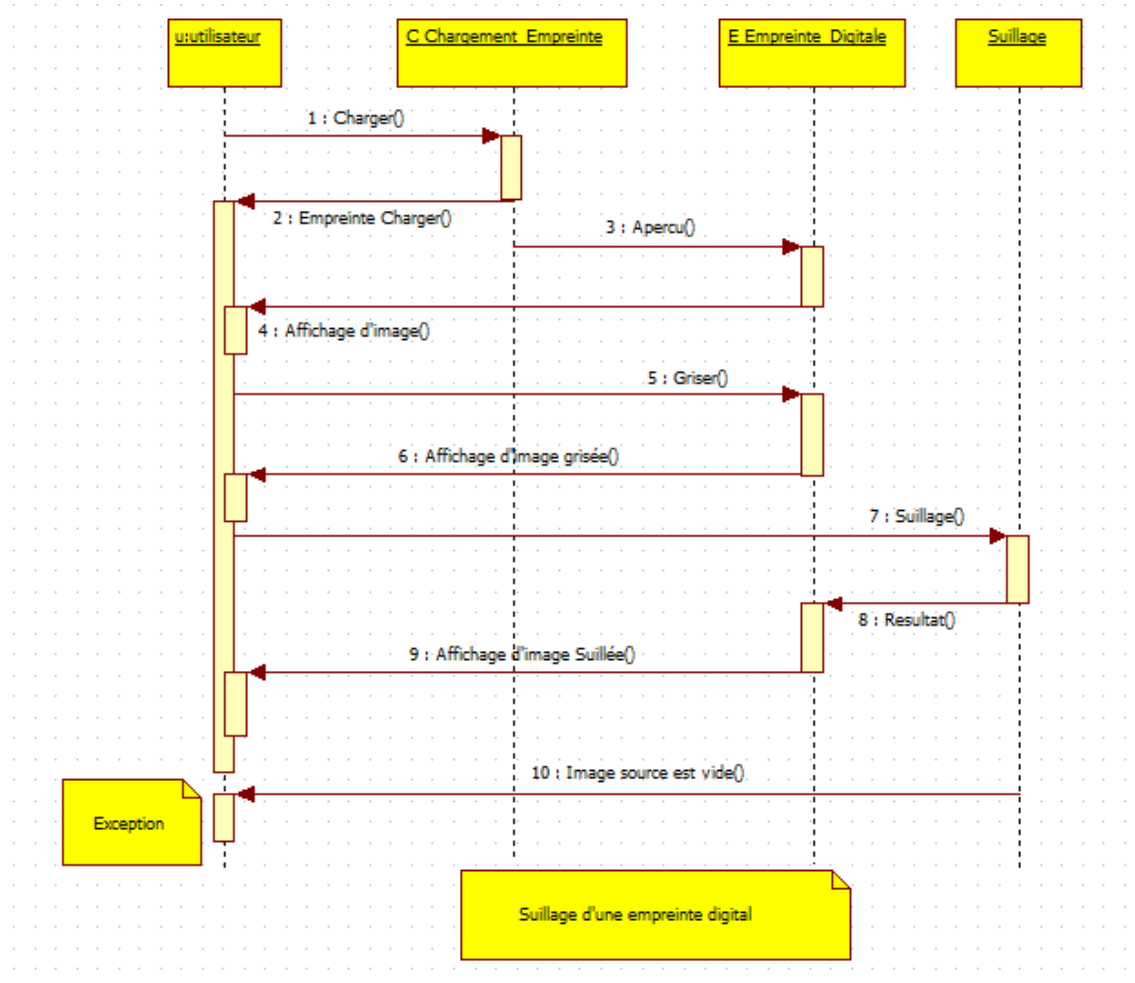


Figure 3.2 : Diagramme de séquence (exemple de Seuillage d'une image de l'empreinte digitale)

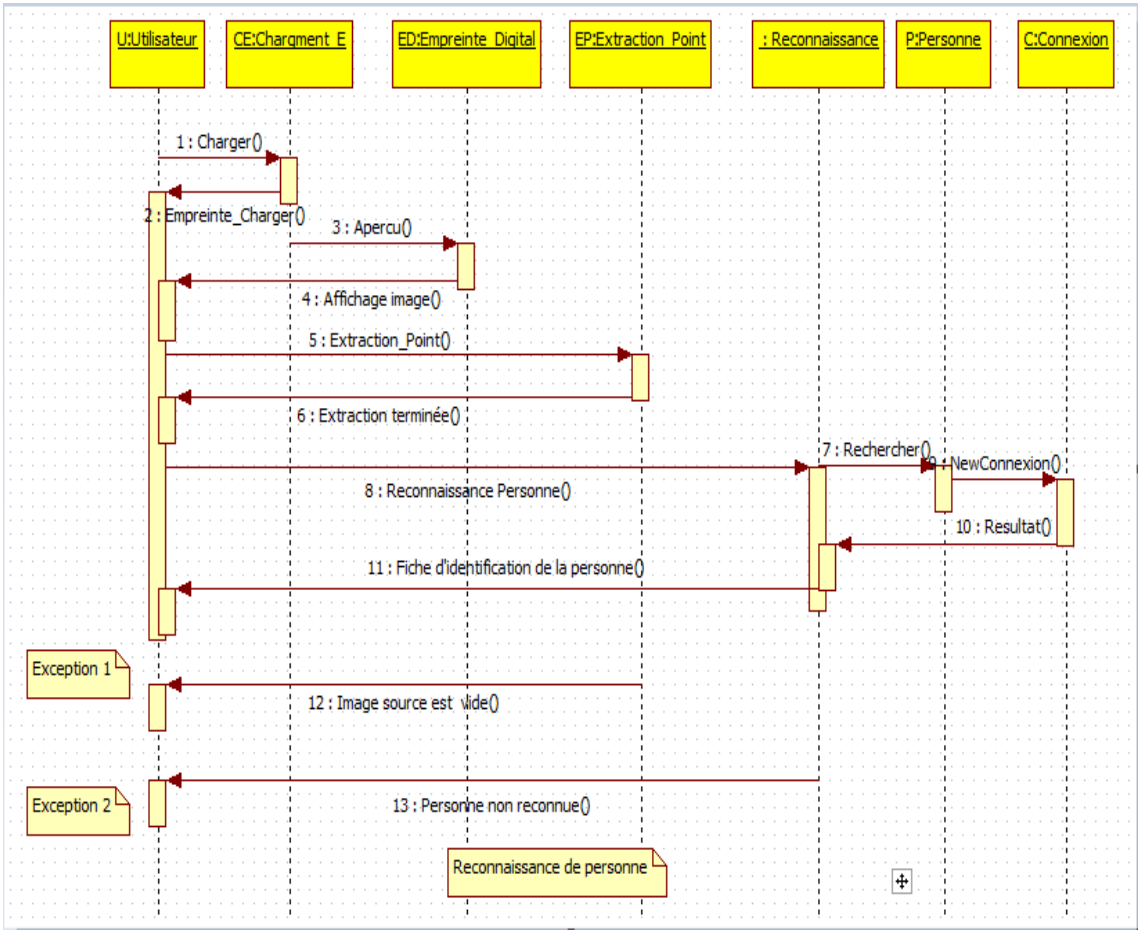


Figure 3.3 : Diagramme de séquence (exemple de reconnaissance d'une personne)

2.1.3 Diagramme de classes

Un diagramme de classes est une collection d'éléments de modélisation statiques (classes, paquetages...), qui montre la structure d'un modèle de données, il fait abstraction des aspects dynamiques et temporels.

Il constitue un élément très important de la modélisation et permettre de définir quelles seront les composantes du système final. Il permet de structurer le travail de développement de manière très efficace. (Figure 3.4) représente le diagramme de classes de notre application.

Pour réussir un diagramme de classes:

- identifier les entités (ou classes) pertinentes
- identifier leurs interactions (relations et cardinalités)
- utiliser les designs patterns (singleton, héritage…)

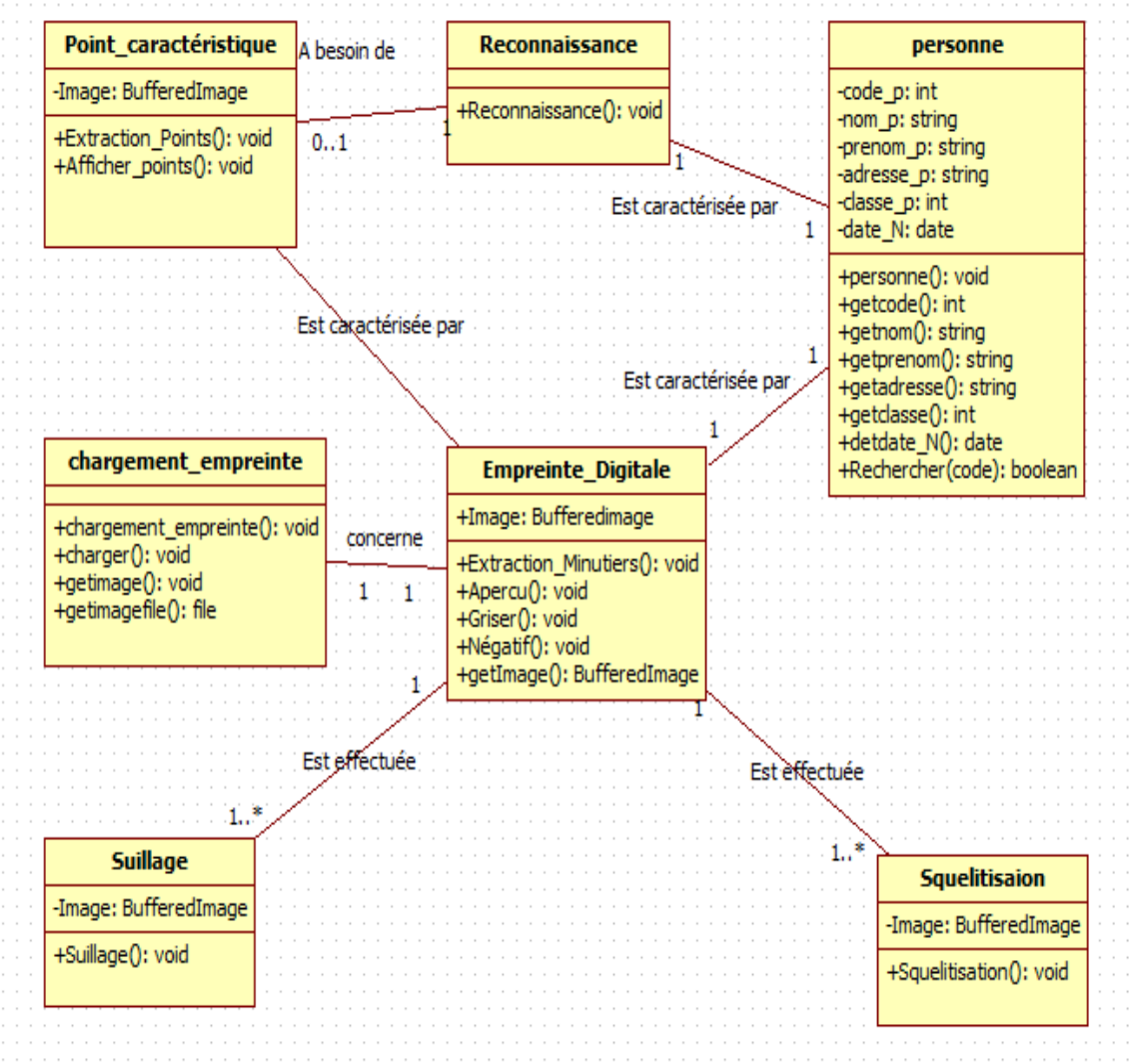


Figure 3.4 : Diagramme de classe

3. Présentation du prototype

Nous avons données une vue globale sur les différentes traitements réalisées et le déroulement de notre système, donc nous avons décri les grandes démarches réalisées, et les principes suivies pour le bon fonctionnement de notre application.

4. Réalisation de travail:

Nous avons utilisés le langage java puisqu'il est caractérisé par les avantages qu'offre la programmation orienté objet, java facilitent l'internationalisation et augmentes les performances d'entrée/sortie,

4.1. Environnement de travail :

Notre logiciel est écrit en Netbeans version 6.8 sous Windows. Le choix de Netbeans par ce qu'il permet principalement le développement des applications en java, et facilite la création des interfaces graphiques.
on utilisant Netbeans peut intégré des codes en Matlab a l'intérieur des codes java.

4.2. Présentation de l'interface homme-machine :

Notre prototype est constitué de deux parties distinctes, la première représente le traitement d'image à utilise : les opérateurs de filtrage (graissage, seuillage, squelettisation) pour simplifier en maximal l'empreinte digitale.

La deuxième partie est utilisée pour la présentation de la base donnée de l'application sous forme d'un fichier XML.

4.2.1 Partie de traitement d'image :

4.2 .1.1 fenêtre principale de l'application (Accueil)

Elle se compose en 6 parties :

1. Zone pour chargement de l'empreinte digitale après zoom.
2. Zone pour l'image zoomer (ou on fait les traitements principale)
3. Les traitements faits sur l'image ou l'empreinte
4. Zone pour affichage les caractéristiques des individus
5. Extractions des points et reconnaissance de l'individu
6. Zone pour les traitements nécessaire dans la base de données (ajouter, supprimer, afficher)

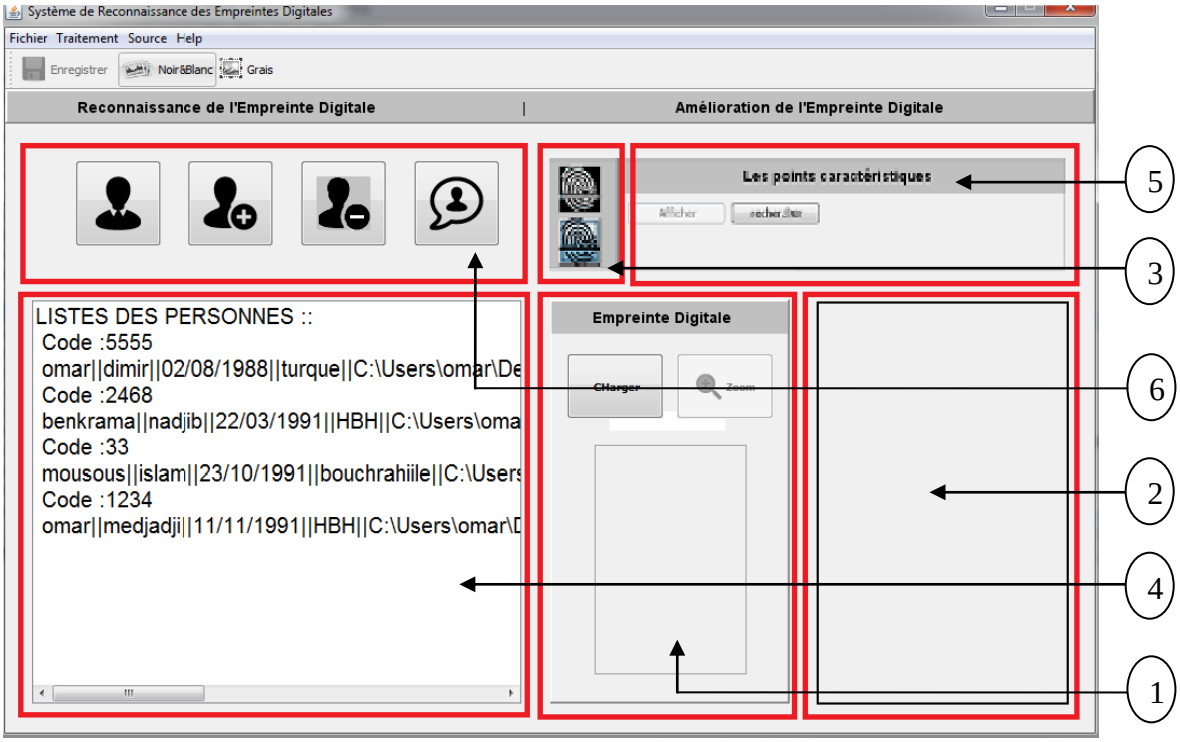


Figure 3.5 : fenêtre principale de l'application (Accueil)

4.2 .1.2 Chargement de l'empreinte digitale :

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

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

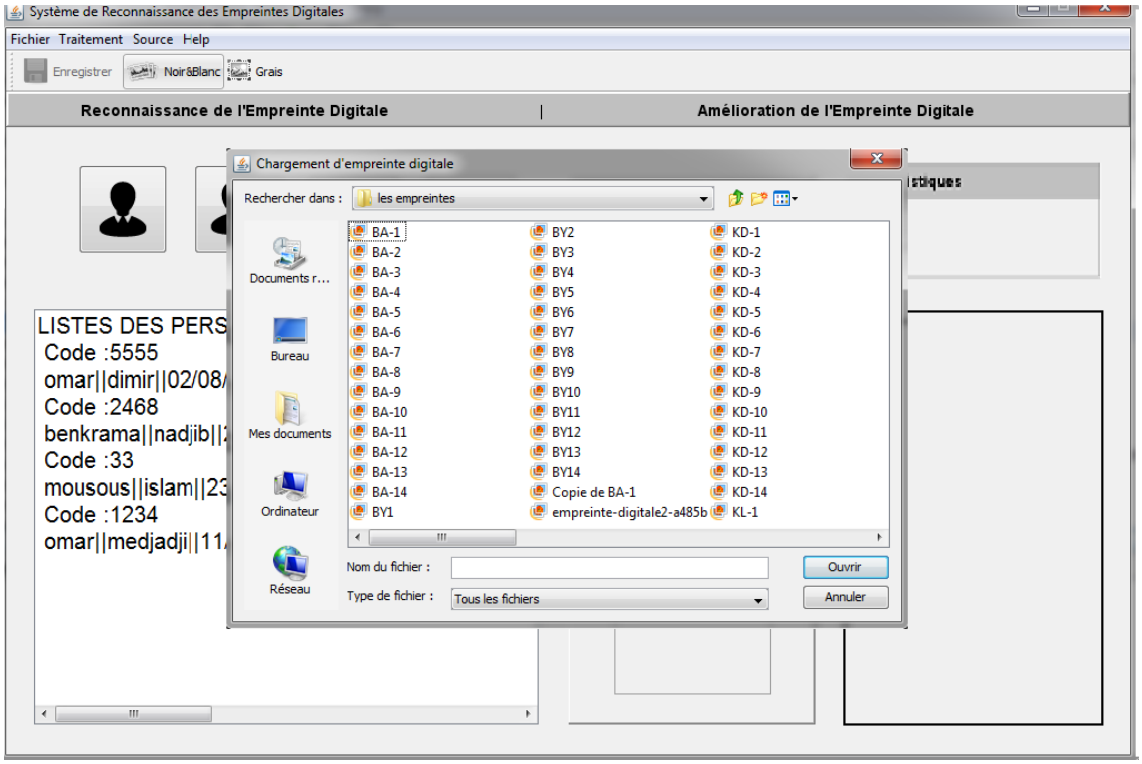


Figure 3.6 : Chargement d'une image d'empreinte digitale

Après une boite de dialogue qui informe que l'image est chargée.

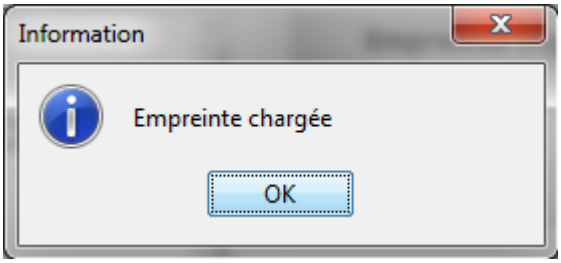


Figure 3.7 : Boite de dialogue (information)

4.2 .1.3 Aperçu de l'empreinte chargée

Après avoir chargé l'image, on clique sur le bouton [***Aperçu***] qui se trouve dans la zone (1) pour afficher l'image avec une grande dimension.

Figure 3.8: Aperçu de l'empreinte charger

4.2 .1.4 Transformation en niveaux de gris

Dans cette étape, on transforme l'image en niveaux de gris. Pour cela, on clique sur le bouton [***Griser***] qui se trouve dans le menu en haut.

Figure 3.9 : Grisage de l'empreinte charger

4.2 .1.5 Segmentation (Seuillage ou binarisation)

Dans cette étape de binarisation où les pixels de l'image sont partagés par un seul seuil s en deux classes : ceux qui appartiennent au fond et ceux qui appartiennent à la scène (l'objet). Pour effectuer cette opération on clique sur le bouton [***Binariser***] ou [***seuillage***]. Une boite de dialogue nous s'affiche pour faire saisir le seuil de binarisation.

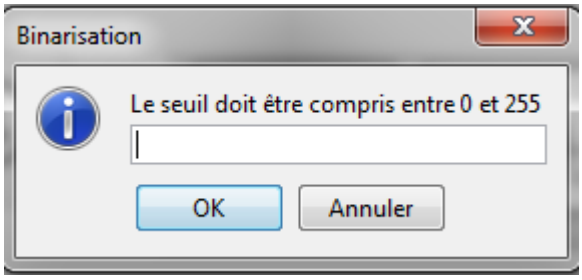


Figure 3.10: saisir le seuil de binarisation

Lorsque on appuyé sur le bouton ok on obtient le schéma suivant :

Figure 3.11 : Binarisation de l'empreinte

4.2 .1.6 Segmentation (squelettisation) :

La squelettisation est un traitement nécessaire qui suivre l'étape de binarisation.

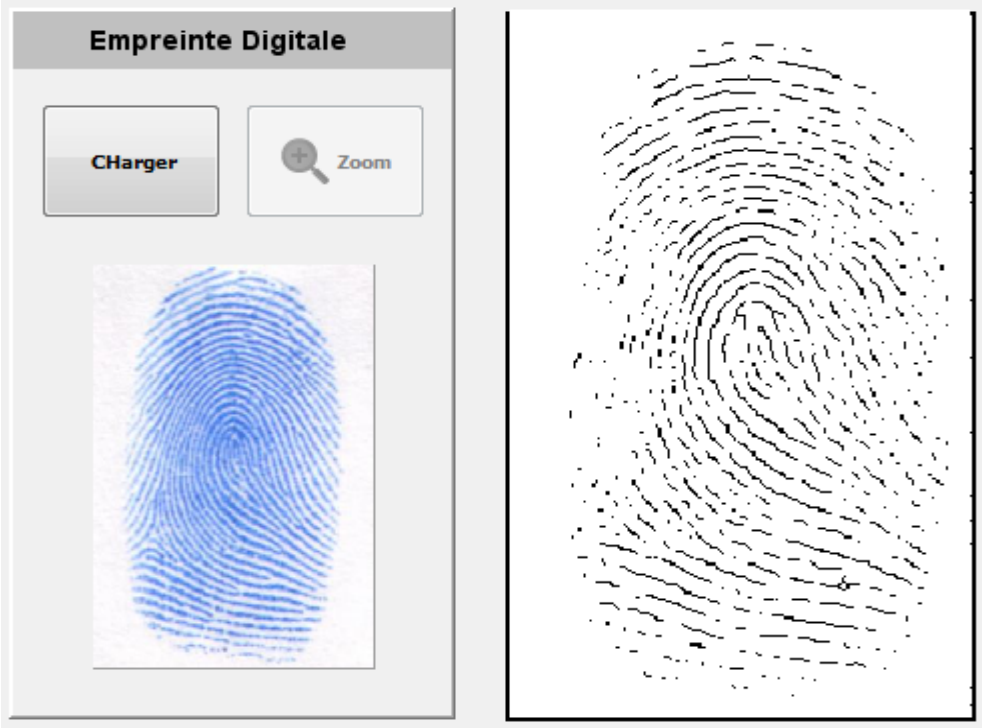


Figure 3.12 : squelettisation de l'empreinte

4.2 .1.7 Extraction des points :

Dans cette étape, on clique sur le bouton [***rechercher***] pour faire extraire les points associés à l'image d'empreinte digitale chargée, on sépare l'mage on 12 zones et dans chaque zone on calcule le nombre des points qui présentes les arrêts des nœuds.

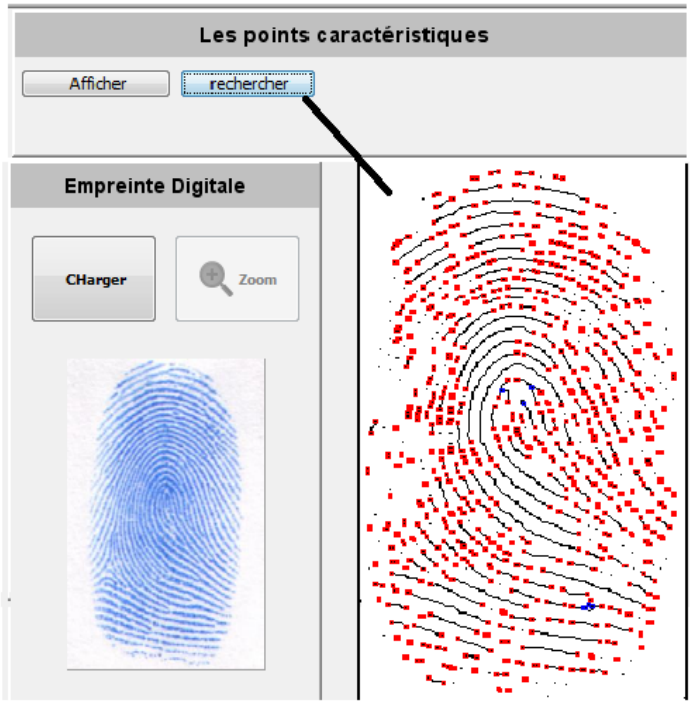


Figure 3.13 : Extraction des points minutiers de l'empreinte

Après l'extraction des points minutiers, si l'empreinte digitale est déjà enregistrer dans la base de données donc lorsque l'utilisateur clique sur le bouton [***Afficher***] on affiche les caractéristique de cette personne.

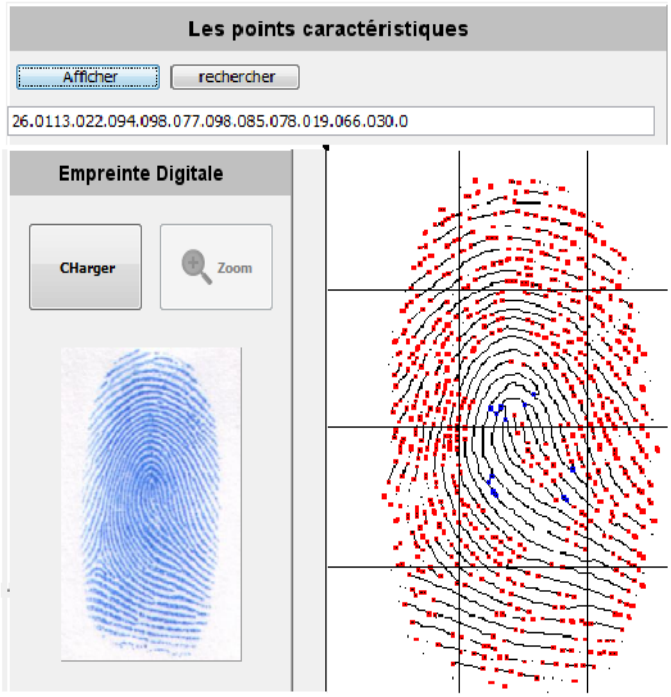


Figure 3.14 : Nombre des points dans chaque zone.

Figure 3.15 : **Les informations de cette personne (coté serveur)**

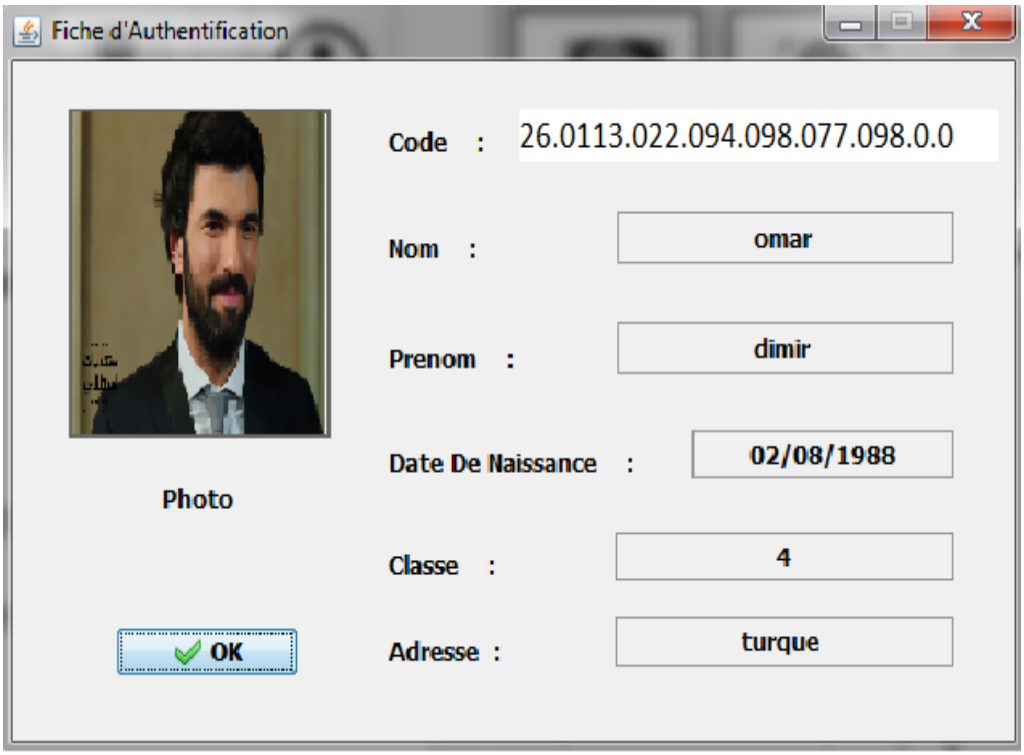


Figure 3.16 : Fiche d'authentification de la personne

Sinon on affiche une boite de dialogue « cette personne n'existe pas », et après on ajoute les caractéristiques dans la BDD.

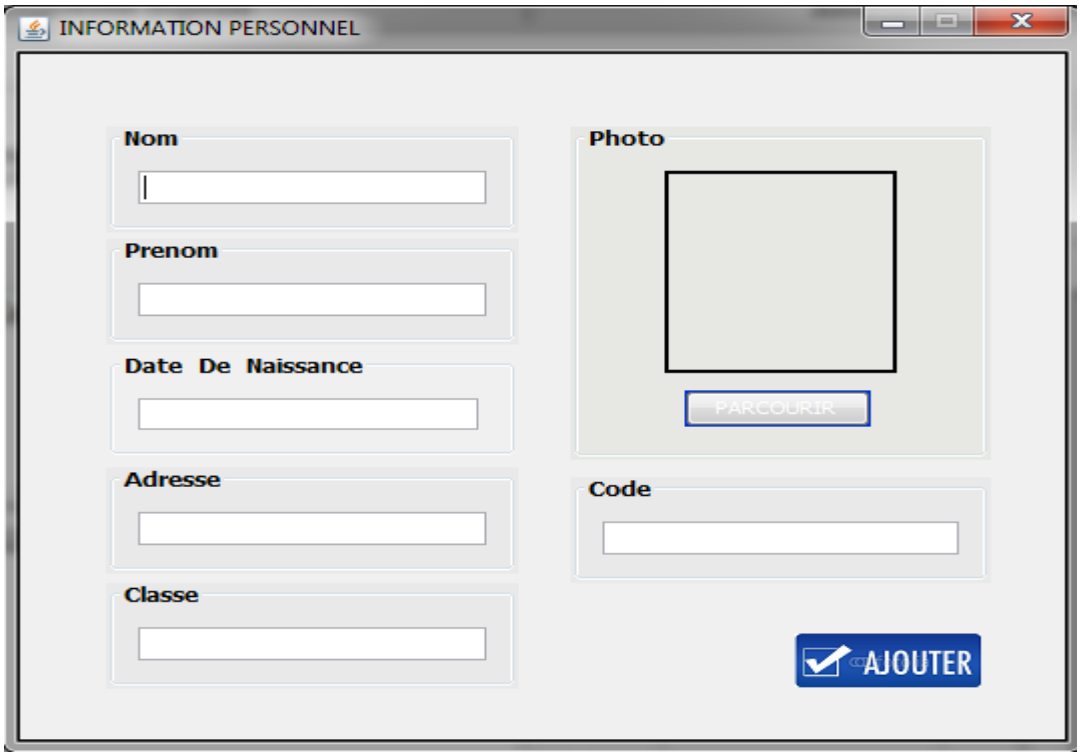


Figure 3.17 : Formulaire d'identification de la personne

4.2.2 Partie de base de données :

Nous avons prévu une base de données pour les individus, elle est constituée d'une seule table Personne qui contient des caractéristiques nécessaires sur chaque personne, telles que le code, le nom le prénom, la date de naissance, l'adresse, classe ainsi que son image. Pour la création de cette base, nous avons utilisé un SGBD XML avec la bibliothèque Jdom.

```
<?xml version="1.0" encoding="UTF-8"?>
<personnes>
  </personne>
  <personne ID="1234">
    <nom>omar</nom>
    <prenom>medjadji</prenom>
    <adresse>HBH</adresse>
    <classe>1</classe>
    <photo>C:\Users\omar\Desktop\prjet pfe\NV8.png</photo>
    <datenaissance>11/11/1991</datenaissance>
  </personne>


  <personne ID="33">
    <nom>mousous</nom>
    <prenom>islam</prenom>
    <adresse>bouchrahiile</adresse>
    <classe>3</classe>
    <photo>C:\Users\omar\Desktop\prjet pfe\NV1.png</photo>
    <datenaissance>23/10/1991</datenaissance>
  </personne>
</personnes>
```

Figure 3.18: Fichier .XML de la BDD

4. L'environnement de développement

5.1 .L'environnement matériel :

Pour développer cette application j'ai utilisé une machines, configurées comme suit :

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

5.2. Environnement Logiciel :

Lors du développement de cette application, nous avons utilisé, les outils logiciels suivants:

- netbeans. Version 8.0.1
- matlab. Version 18.0
- StarUml. Version 5.0.2

6. Conclusion

Dans ce chapitre, nous avons présenté les différentes interfaces de l'application ainsi que les diagrammes principaux tels que le diagramme de cas d'utilisation, diagramme de classe, et diagramme de séquence.

La partie de réalisation détermine une idée plus claire sur les taches qui sont réalisé dans cette application par la présentation des interfaces graphiques. Enfin avec ce chapitre presque on termine la phase de développement de notre application.

Conclusion Générale

Notre projet fin d'étude consiste à concevoir une application de Reconnaissance des empreintes digitales qui permet de réaliser un système biométrique qui fait l'authentification des individus selon leurs empreintes digitales.
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.

C'est une application presque finalisée et accompagnée de tous les documentations technique et conceptuelle nécessaire à sa bonne évolution.

Dans ce mémoire, nous nous sommes intéressés au problème de la reconnaissance biométrique des empreintes digitales. Nous avons souligné durant l'influence néfaste des principales difficultés lors de la reconnaissance biométrique des empreintes digitales et pour cela, nous avons proposé quelques solutions qui ont été évaluées durant la phase de test.

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

Enfin, la réalisation de ce projet de travail en équipe sur une durée limitée est un bon entraînement pour ce futur métier.

Bibliographie

Référence	Détail Bibliographique
[1]	Nuance, http://www.nuance.com
[2]	S. Liu, M. Silverman, « A Practical Guide to Biometric Security Technology », IEEE Computer Society, IT Pro-Security, Janvier-Février 2001.
[3]	A. Jain, R. Bolle, S. Pankanti, « Biometrics: Personal Identification in Networked Society », Kluwer, New York, 1998
[4]	Mémoire Présenté Comme Exigence Partielle De La Maîtrise En Science Politique. La Biométrie, Sa Fiabilité Et Ses Impacts Sur La Pratique De La Démocratie Libérale Université Du Québec À Montréal Par : Frédéric Massicotte Promotion : Novembre 2007
[5]	] http://www.biometrie-online.net
[6]	http://xpose.avenir.asso.fr/viewxpose.php?site=3

[7]	DGSN :la Police scientifique de Tlemcen
[8]	N. GALY, " *Etude de système complet de reconnaissance d'empreintes digitales pour un capteur microsystème à balayage*", Thèse de Doctorat, Institut National Polytechnique de GRENOBLE, 2005.
[9]	H. V. DANG, " *Biométrie pour l'Identification*". Rapport final du tipe, Institut de la Francophonie pour l'Informatique, 2005.
[10]	Titre de l'ouvrage : Analyse d'images : filtrage et segmentation Auteur : Jean-Pierre Cocquerez & Sylvie Philipp Maison d'édition : Masson Année : 1995
[11]	Mémoire de fin d'étude : Traitement d'images par réseau de neurones Présenté par : BOUAFIA Zoheyr, BENHLIMA Mustafa Université de : Abou Bakr Belkaid, Tlemcen. Faculté : des sciences de l'ingénieur Département : informatique. Promotion : 2005
[12]	http://www.tsi.enst.fr/tsi/enseignement/ressources/mti/skel_4_8/algo.html
[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

Table des figures

Liste des tableaux

RESUME:

La biométrie, qui consiste à identifier un individu à partir de ses caractéristiques physiques ou comportementales,
Dans cet article nous introduisons tout d'abord la notion de biométrie. Nous décrivons l'architecture d'un système biométrique ainsi que les biométriques utilisées pour évaluer leur performance.

La reconnaissance d'empreintes digitales est une technique biométrique mature pour toute application d'identification ou de vérification d'individus. Dans ce travail, nous décrivons la conception et le développement d'un système automatique d'identification d'identité à l'aide des empreintes digitales.

Mots Clés :

Biométrie, empreinte digital.

ABSTRACT:

Biometrics, which is to identify an individual from physical or behavioral characteristics,

In this article we first introduce the concept of biometrics. We describe the architecture of a biometric system and biometric used to assess their performance.

The fingerprint recognition is a mature biometric technology for any application identification or verification of individuals. In this work, we describe the design and development of an identity automatic identification system using fingerprints.

Keywords:

Biometric, fingerprint

الـــمـلـــخـــص:

البيومتري ، والتي تعني تحديد الفرد من خلال خصائصه الفيزيائية أو السلوكية،

في هذه المقالة ونحن نقدم لأول مرة مفهوم البيومتري . نحن نصف بنية نظام التحقق من الهوية البيومترية واستخدامها لتقييم أدائها.

والتعرف على بصمات الأصابع هي التكنولوجيا الحيوية الناضجة لأي تحديد تطبيق أو التحقق من الأفراد. في هذا العمل وصفنا تصميم وتطوير نظام التعرف الآلي الهوية باستخدام بصمات الأصابع

الكلمات المفتاحية :

البيومتري ، البصمات.