République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Ghardaïa

Faculté des Sciences et Technologie

Département des Mathématiques et Informatique

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

LICENCE

Domaine : Mathématiques et Informatique

Spécialité : Informatique

THEME

Application de reconnaissance biométrique

PAR :

Brahim CHEIKH AISSA

Khaled KERBOUCHE

Jury:

M^{r}: Slimane OULAD NAOUI	Maitre Assistant A Univ. Ghardaia	**Examinateur**
M^{me}: Nacéra BRAHIM	Maitre Assistant B Univ. Ghardaia	**Encadreur**

ANNEE UNIVERSITAIRE: 2013/2014

Remerciements

Aux termes de ce travail nous voulons remercier infiniment toutes les personnes qui nous ont aidées, de près ou de loin, à la réalisation et l'aboutissement de ce travail.

C'est avec un grand plaisir que nous réserverons ces lignes en termes de gratitude et de profonde reconnaissance envers tous les enseignants de la faculté d'informatique particulier, et spécialement, notre encadreur Madame **Brahim Nacéra** pour son soutien moral, ses précieux conseils et son encouragements pour effectuer ce travail.

Résumé

Les empreintes digitales humaines sont riches en détails appelés les minuties, qui peuvent être utilisés comme marques d'identification des individus.

Le but de ce mémoire est d'étudier la biométrie avec les différentes modalités qui existent pour pouvoir développer une application de reconnaissance en se basant sur l'empreinte digitale. Pour cela il est nécessaire de faire l'extraction et l'appariement des minuties.

Mots clés : authentification – biométrie – empreinte digitale – minutie

Abstract

Human fingerprints are rich in details called minutiae, which can be used as identification marks for fingerprint verification. The goal of this thesis is to develop a java application for fingerprint recognition through extracting and matching minutiae after studying biometric approaches.

Key words: authentication – biometric – fingerprint – minutiae – extraction

Table des Matières

Liste des figures

Liste des tableaux

Introduction

La reconnaissance biométrique se réfère à l'utilisation des identificateurs comportementaux et anatomiques distinctives pour reconnaître automatiquement une personne.

Parce que les caractères biométriques d'une personne ne peuvent pas être facilement perdus, modifiés, ou partagés, ils sont considérés comme plus fiables pour la reconnaissance des personnes que les jetons traditionnels (par exemple, les clés ou les cartes d'identité) ou les méthodes à base de connaissance (par exemple, un mot de passe ou code PIN).

La reconnaissance biométrique fournit une meilleure sécurité, une plus grande efficacité, plus de commodité de l'utilisateur. C'est pour ces raisons, les systèmes de reconnaissance biométrique sont de plus en plus déployés dans un grand nombre de gouvernement (par exemple, passage des frontières, carte d'identité nationale, passeports électroniques) et dans les applications civiles (par exemple, accès au réseau informatique, téléphonie mobile, accès à l'internet, carte à puce).

Un certain nombre des technologies biométriques ont été développées et plusieurs d'entre eux ont été déployés avec succès. Parmi celles-ci, les empreintes digitales, le visage, l'iris, la voix, et la géométrie de la main sont les plus couramment utilisées.

Chaque caractéristique biométrique a ses forces et ses faiblesses et le choix d'un caractère particulier dépend généralement des besoins de l'application. Les divers identifiants biométriques peuvent être également comparés selon les facteurs suivants: l'universalité, l'unicité, la permanence, la recouvrabilité, l'acceptabilité et la circumvention.

À cause de la spécificité bien connue (individualité) et la persistance des propriétés d'empreintes digitales ainsi que le coût et la maturité des produits, les empreintes digitales sont les caractéristiques biométriques les plus largement déployés.

Chapitre I

L'authentification : Concepts et techniques.

I.1. Introduction

Aujourd'hui, la sécurité informatique devient un sujet vital, de plus en plus d'entreprise ouvrent leur système d'information à leurs partenaires et leurs fournisseurs, Alors que tous les systèmes d'information (d'une société, d'une entreprise, …) doit protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur internet.

Ce chapitre présent une introduction à la sécurité informatique et certains notions et techniques de base sur l'authentification.

Pour bien cerner les enjeux de notre étude on va tout d'abord introduire quelques concepts relatifs à la sécurité informatique

I.1.1. Définitions

La sécurité informatique est une collection des outils automatiques et est un ensemble des techniques mis en œuvre pour **protégé** l'information et ses éléments essentiels, y compris les systèmes et le matériel qui utilisent, stockent et transmettent ces informations, **contre** les menaces accidentelles ou intentionnelles.

La sécurité informatique utilise un vocabulaire bien défini. Les définitions de certains termes sont les suivant :

- **La vulnérabilité** : Toute faille ou faiblesse dans un system de défense qui pourrait être exploitée par une menace pour créer un impact sur les assets (personne, objet physique, processus, technologies ou tout autre ressource de valeur) d'une organisation.[1]
- **Les menaces** : Le potentiel qu'un événement (malveillants ou autrement) ce serait endommagé ou compromettre une asset (ressource de valeur).

  Les **menaces** contre un système d'information entrent dans une des catégories suivantes : atteinte à la disponibilité des systèmes et des données, corruption ou falsification de données, vol ou espionnage de données, usage illégal d'un système ou d'un réseau, usage d'un système compromis pour attaquer d'autres cibles.

  Les menaces engendrent des **risques** comme: la perte de confidentialité des données, l'indisponibilité des infrastructures et des données, les dommages pour le patrimoine intellectuel et la notoriété. Les risques peuvent se réaliser si les systèmes menacés présentent des vulnérabilités [4]
- **Les contre-mesures** : ce sont les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique (auquel cas il peut exister d'autres attaques sur la même vulnérabilité).

La norme ISO 7498-2 définit autre termes. [3]

I.1.2. Les services principaux de la sécurité informatique

Des normes ont été définies pour les services de sécurité pour atteindre les objectifs de sécurité et de prévenir les attaques de sécurité. Figure I.1 montre les principaux services de sécurité.

- **Confidentialité:** La confidentialité garantit que seuls ceux qui ont les droits d'accès à l'information sont capables de faire, Lorsque des individus ou des systèmes non autorisés peuvent consulter les informations, la confidentialité est violée.
- **Intégrité d'information :** empêcher la modification non-autorisée de données pendant le transfert ou le stockage.
- **Authentification :** pour vérifier l'identité de l'utilisateur/ordinateur.
- **Non-répudiation :** pour assurer que l'utilisateur/serveur ne peut pas nier avoir participé à une transaction plus tard.
- **Contrôle d'accès** : pour être en mesure de dire : qui peut faire quoi avec quelle ressource.
- **Disponibilité:** pour s'assurer que les services sont toujours disponibles pour les utilisateurs légitimes.

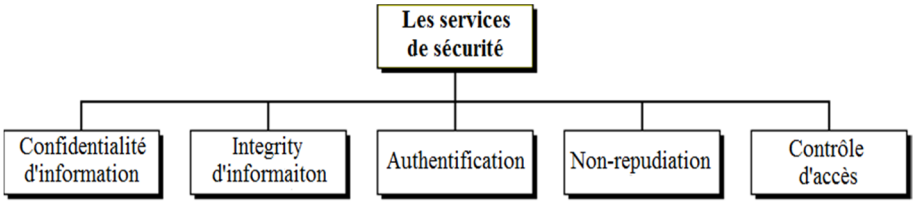


Figure I.1 Les services de la sécurité informatique [3]

I.3.Concepts de bases de l'authentification

I.3.1. Contrôle d'accès

I.3.1.1. L'identification

L'identification est un mécanisme par lequel une personne ou un ordinateur cherche avoir accès à une ressource, propose son identifiant (ID) par lequel il est connus pour le système [5]

L'identification nécessite la comparaison d'identifiant avec chaque identifiant (1pour plusieurs) de référence contenue dans une base de données, afin de trouver une correspondance si elle existe. [6]

I.2.1.2. L'authentification

L'authentification est le processus de vérification et validation d'une identité proposé par une entité, et la détermination que cette personne est bien celle qu'elle prétend d'être. [5]

L'authentification généralement peut se réalisé par :

a. Un identifiant connu par l'entité (ce qu'il sait) comme les mots de passe et le code PIN.
b. Un identifiant possédé par l'entité (ce qu'il possède) comme les smartes cardes et les cartes magnétiques.

c. Un identifiant propre à l'entité (ce qu'il est) représenté par une caractéristique biométrique comme l'empreinte digitale et la voix.

Le mot authentification à une relation avec deux contextes dans le domaine de la sécurité informatique :

a. L'authentification d'origine d'une information : corroborer la source de l'information (c'est-à-dire l'authentification demandée dans une association en mode connexion).
b. L'authentification de l'entité homologue: corroborer l'identité d'une entité (c'est-à-dire l'authentification dans une association en mode sans connexion) [7]

I.2.1.3. L'autorisation

L'autorisation est l'acte de déterminer si une entité authentifiée a le droit d'effectuer certaines activités, par une association entre une liste de ressources d'information et des niveaux d'accès correspondants. [5]

I.2.1.4. L'audit

Garanti que toutes les actions sur un système (autorisée ou non) peuvent être attribuées à une identité authentifiée, elle est souvent réalisée par les journaux système (logs ou audit) qui enregistre des informations spécifiques tel que les tentatives d'accès échouées et les modifications sur les systèmes. Ils ont nombreux usages, tels que la détection d'intrusion, la détermination de la cause d'une défaillance du système, ou simplement surveiller l'utilisation d'une ressource particulière [5]

I.2.2. Les systèmes d'authentification

I.2.2.1. L'authentification multi-facteurs (forte)

La combinaison entre deux facteurs d'authentification (ou plus), est un système utilisé pour augmenter la fiabilité de mécanisme de l'authentification, exemple d'application de ce système c'est la combinaison entre la carte magnétique et le code PIN.

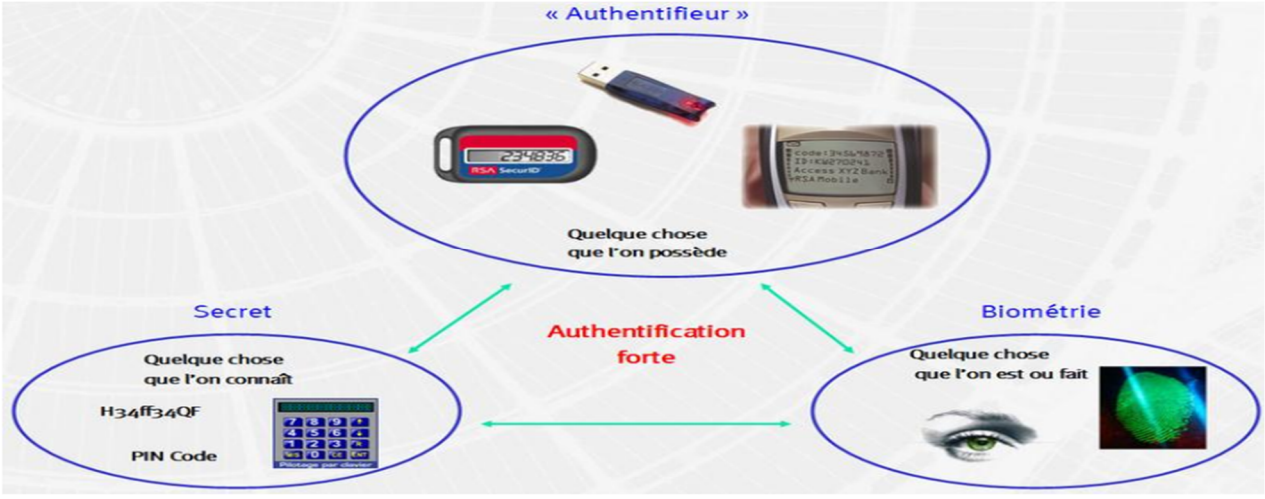


Figure I.2 Le principe de l'authentification forte

I.2.2.2. L'authentification devisée

L'utilisation des trois facteurs d'authentification en même temps n'est pas suffisante pour certain type d'ultra-haute sécurité, la solution c'est de distribuer l'authentification entre plusieurs entités, par exemple : pour contrôler un system de lancement des missiles nucléaire, deux personnes (ou plus) utilise leur identifiant unique (clé physique, mot passe, empreint…) simultanément pour lancer un missile.

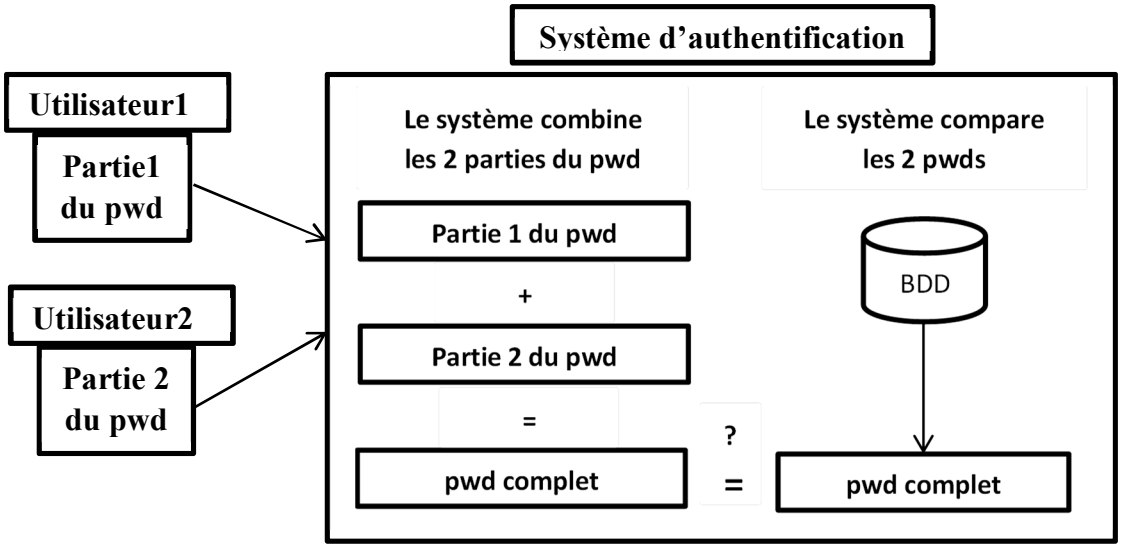


Figure I.3 Le principe d'authentification devisée (pwd = mot de passe)

I.2.3. Vérifier l'identité d'un individu, Pourquoi ?

a. Si l'identité d'un utilisateur est correctement vérifiée, seulement les utilisateurs légitimes peuvent avoir l'accès au système, et par la suite, ils ne peuvent pas nier leur activité, ce qui garantit la non-répudiation.

b. La protection de la propriété individuelle, (habitation, compte bancaire, données informatiques, messagerie, ...).

c. Assurer l'accès limité.

I.2.4. Dans l'absence de l'authentification, Qu'est-ce qui se passe ?

Dans l'absence du service d'authentification, le système informatique peut être face au plusieurs problèmes, citons quelques-uns :

a. Perte de la confidentialité : Lorsque l'information est lue ou copiée par une personne non authentifié ou non autorisé, le résultat est connu par la perte de la confidentialité.

b. Perte de l'intégrité des données : La perte de le l'intégrité est un résultat des modifications non autorisé sur l'information.

I.3. Techniques et méthodes d'authentification

I.3.1. Techniques à base de Connaissance

Les techniques d'authentification les plus utilisées sont basées sur ce que l'entité sait, par exemple: mot de passe, numéro d'identification personnel (PIN),

Leur but est d'avoir un code unique pour qu'un attaquant ne puisse l'obtenir par prédiction, brute force ou autre manière, malheureusement c'est la plus faible approche [5]

I.3.1.1. Les mots de passe à base de texte

Le mot de passe est une combinaison de caractères, utilisé pour authentifier l'utilisateur [5], ils ne sont pas vraiment sécurisés, et pour cela ils doivent être:

- Difficiles à deviner ;
- Changés fréquemment ;
- Différent sur différents comptes d'un même utilisateur;
- Chiffré lors de leur stockage dans la base de données.

Satisfaire toutes ces exigences est pratiquement impossibles pour les utilisateurs, par conséquent, ils les ignorent et utilisent des mots de passe faibles.

I.3.1.2. Les mots de passe graphiques

Le problème de l'incapacité suffisant pour les utilisateurs de se souvenir d'une chaîne de caractères de longueur et de complexité important, conduit à des nouvelles techniques comme les mots passe graphiques et la connaissance cognitive [6]

Il existe deux technique basés sur les images : à base d'une reconnaissance et à base de rappel :

a. **A base d'une reconnaissance**: l'utilisateur passe l'authentification par la reconnaissance d'une image (depuis une série d'images) qu'il choisit lors la phase d'enregistrement
b. **A base de rappel :** faire reproduire quelque chose qu'il a créé lors de la phase d'enregistrement [6]

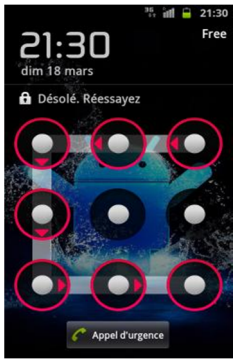


Figure I.4 Le mot de passe graphique à base de rappel

I.3.1.3. La connaissance cognitive

Cette technique basée sur un fait connu par l'utilisateur. En général cette technique repose sur le fait de poser certaines questions à l'utilisateur qui ont une relation avec son histoire personnelle, aime / n'aime pas, films, dates importants et les opinions [6]

I.3.2. Facteur de jeton (Token)

Le concept de cette approche (quelque chose détenu par l'entité), a été utilisé avant la création des ordinateurs, Les clés d'une maison ou d'une voiture utilisés pour vérifier l'accès physique, mais l'accès électronique n'est plus vérifier par une clé physique. Ce qui nécessite l'utilisation d'une clé électronique.

Mécanisme : le jeton est présenté au système d'authentification. Une conversation a aura lieu entre le jeton et le système par des moyens filaires ou sans fil. Pour passer ce système d'authentification, le jeton doit avoir un mot de passe correct.

Cette approche fonctionne en toute sécurité si les personnes légitimes (et seulement les légitimes) ont la possession de jeton.

Pour qu'un jeton soit parfait il doit être unique, pas cher et facilement remplaçable en cas de perte ou vol, difficile à reproduire et a une forme portable et pratique.

Les jetons peuvent être classés selon la nature fondamentale de leur fonctionnement : passive et active [6]

a. **Les jetons passifs** Les jetons passifs simplement stockent un secret, ils sont présenté à un système de traitement et de validation externe, les plus fameux sont les cartes magnétique et les cartes de proximité.
b. **Les jetons actifs** Les jetons actifs stockent également un secret, mais ce n'est jamais sorti à un system externe, en plus ce genre des jetons capable de traiter le secret avec d'autre information, le résultat c'est un mot de passe jetable qui n'est valable que pour une seule utilisation.

   Le system crée une empreinte en appliquent une fonction de hachage sur nombre aléatoire avant d'être envoyé au jeton, ce dernier combine son secret avec le nombre aléatoire et applique une fonction de hachage pour créer une empreinte unique, qui sera envoyé vers le system, ou les deux empreint seront comparé, si elles correspondent, le jeton est authentifié.

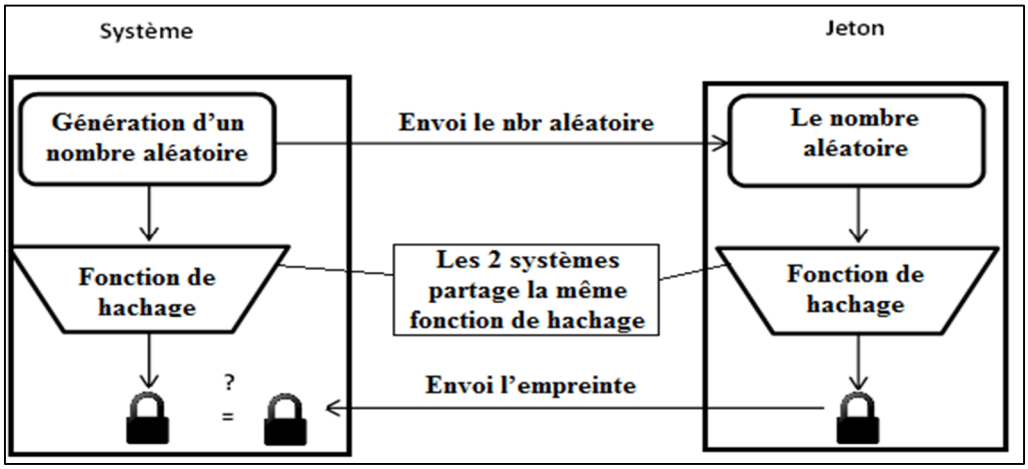


Figure I.5 Le principe d'authentification d'un jeton actif

Ce mécanisme est appliqué sur certains type de jeton comme : Les clés USB qui sont des clés physique contient des programmes chiffrée, et les smartes cardes qui contient des clés cryptographie basé sur une clé public infrastructure (PKI) et d'un code PIN, cela utiliser sur divers entrepris et surtout les entreprise commerciale. [6]

I.3.3. La cryptographie asymétrique et la signature numérique

Une approche puissante pour vérifier l'authentification d'un expéditeur d'une information via une zone non sécurisé est la signature numérique qui est basée sur l'utilisation conjointe d'une fonction de hachage et de chiffrement asymétrique, elle garantit l'intégrité des données, l'authentification de l'expéditeur, et la non répudiation.

L'expéditeur génère deux clés qui ne contiennent pas des informations liées au système

a) Une clé privée : équivalant à un mot de passe, elle est utilisée pour chiffrer l'empreinte (qui est le résultat de l'application de la fonction de hachage sur le message à envoyer) pour obtenir une signature digitale.

b) Une clé publique : envoyée avec le message et la signature, elle est utilisée par le destinataire pour authentifier l'expéditeur, par la comparaison entre l'empreinte du message (qui est le résultat de la même fonction de hachage que l'expéditeur) et le résultat du déchiffrement de la signature avec cette clé publique (qui dépend mathématiquement de la clé privé de l'expéditeur), si elles sont égales alors l'authentification est vérifier. [7] [8]

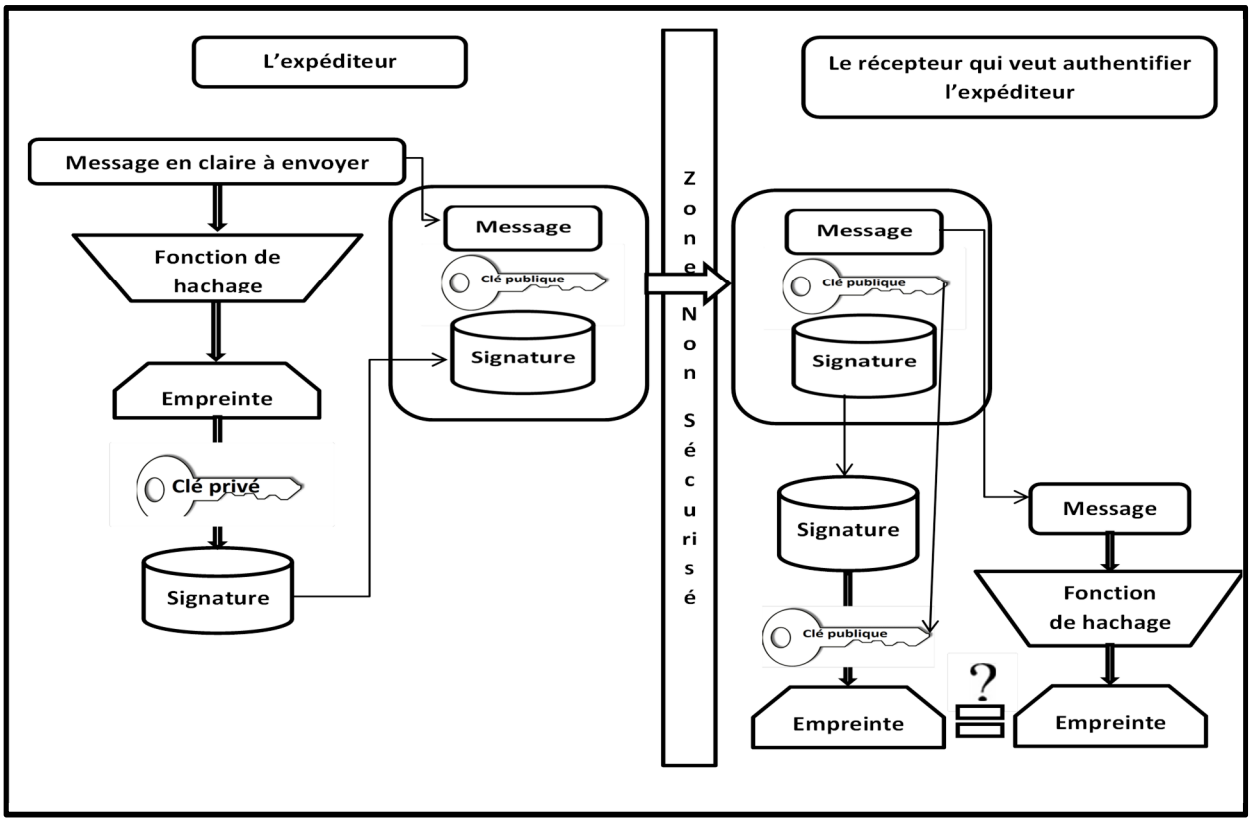


Figure I.6 l'authentification par cryptographie asymétrie

I.3.4. Facteur d'Inhérence (La biométrie)

La biométrie est l'utilisation automatisée des caractéristiques physiologiques ou comportementales pour déterminer ou vérifier une identité [6]

Ce facteur est détails dans le chapitre qui suit.

I.3.5. Classification des méthodes d'authentification :

Les méthodes et les techniques d'authentification sont actuellement disponibles, mais chacun a des avantages et inconvénients. Le tableau suivant présents une comparaison entre les différentes méthodes d'authentification (tableau 1).

Authentification à base de :	**Avantages**	**Inconvénients**
Connaissance	+ Bonne acceptabilité et fortement répandu. + Les photos sont plus faciles à retenir. + Les mots de passe graphiques sont difficiles à deviner par l'attaquant. + Facile à communiquer. + Peu coûteux	- Vulnérable aux attaques de dictionnaire, brute force, et les attaques d'observation. - Difficile à retenir ou facilement prévisible. - Peut-être oublié et facilement surpable. - Partageable.
Token	+ Reconnu partout. + Robuste.	- Peut être perdus ou volés. - Observable et possible de reproduire.
Biométrie	+ Haut niveau de sécurité. + L'identification positive et précise. + Sûr et facile à utiliser. +Pas d'oubli ou de vol possible.	- Sensible à rejouer de capture de données et de réutilisation. - Coût élevé. - Menaces sur la confidentialité. - Technologie encore immature.

Tableau I.1 Les avantages et Inconvénients des méthodes d'authentification

Toutes les technologies d'authentification fournissent un niveau de protection contre l'accès non autorisé. Le schéma au-dessous présente la relation entre le niveau de sécurité, le coût et la facilité d'utilisation :

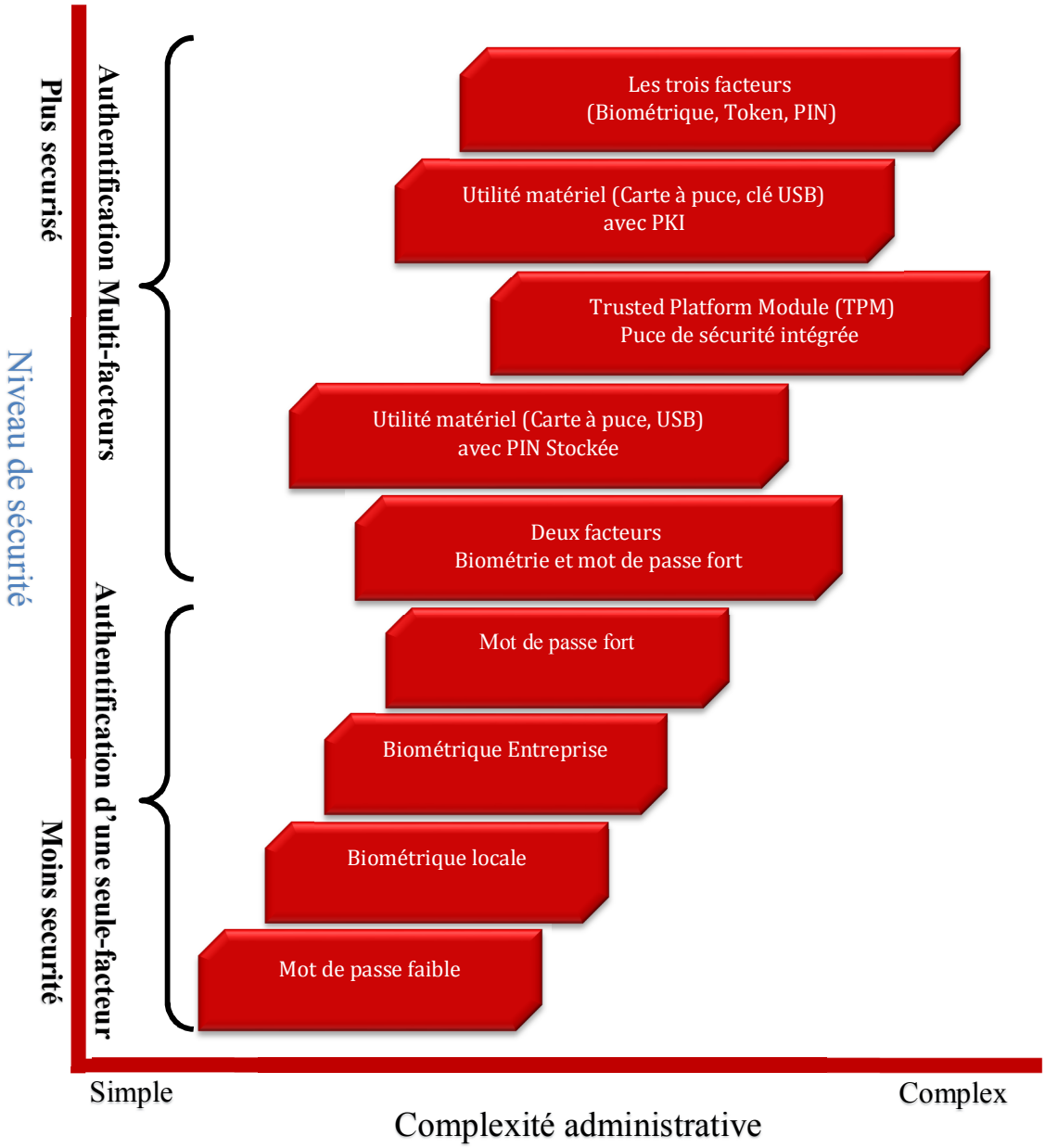


Figure I.7 Les techniques d'authentification entre le niveau de sécurité et la complexité d'administration

I.4. Conclusion

L'authentification est une action fondamentale de tout système de contrôle d'accès, cette opération permet de maintenir la confidentialité, l'intégrité et la disponibilité des systèmes.

Les approches d'authentification sont généralement catégorisées en trois types: la connaissance, les jetons, la biométrie.

Il existe différentes méthodes d'authentification, solutions et moyens d'implémentation qui dépend au type de d'application ou l'environnement, les besoins des utilisateurs et le budget disponible.

Chapitre II

La biométrie : modalités et systèmes

II.1. Introduction

Les systèmes biométriques sont de plus en plus utilisés depuis des années dans le domaine de la sécurité et de contrôle d'accès au sein des infrastructures et des systèmes informatiques. La biométrie est l'un des moyens les plus fiable et les plus utilisés pour la reconnaissance et l'authentification des individus. Elle est basée sur les attributs biologique, physiques ou comportementaux des personnes, tels que l'ADN, l'urine, la forme de visage, la forme des mains, les empreintes digitales, la voix, la démarche…etc. Ces attributs sont traitées par certain ordre des processus automatisés à l'aide des dispositifs comme des modules de balayage ou des appareils-photo. Car les attributs biologiques sont des techniques très couteuses, difficiles à mettre en œuvre et pas complétement automatisées, ce chapitre présent que les méthodes basées sur les attributs physiques et comportementaux.

II.2. Concepts de base sur la biométrie

II.2.1. Définition

Le terme de « biométrie » est une traduction de l'anglais "biométrics" qui correspond au mot anthropométrie [10] Elle vient du grec : bios « vie » et metron « mesure » [11] et selon le dictionnaire[1] c'est « la science qui étudie, à l'aide des mathématiques (statistiques, probabilités) les variations biologiques à l'intérieur d'un groupe déterminé ».

Techniquement, la biométrie est l'ensemble des techniques (appelées les technologies biométriques) qui déterminent ou vérifient automatiquement l'identité des personnes en comparant leurs caractéristiques physiques ou comportementales avec des modèles informatiques numériques préenregistrés de ces caractéristiques, Ces modèles numériques sont produits à partir des algorithmes complexes, puis encodés à l'aide des algorithmes cryptographiques. [6] [12]

La principale différence est dans le terme **automatisé.** Alors que de nombreuses caractéristiques biométriques peuvent exister, ils deviennent biométrique si le processus d'authentification peut être réalisé de manière automatisée. Par exemple, tandis que l'ADN est peut-être l'une des caractéristiques biométriques uniques plus connus, elle échoue actuellement considérée comme une biométrique car il n'est pas un processus entièrement automatisé. Cependant, d'importantes recherches sont actuellement menées pour qu'il en soit ainsi.

L'objectif principal de la biométrie est de fourni des alternatives et des solutions plus sécurisée pour pallier les problèmes et les faiblesses reconnue dans les systèmes de contrôle d'accès actuels, par exemple: la faiblesse des mots de passe, la perte ou vol des cartes magnétiques [11]

[1] Petit Robert, 2003

II.2.2. Les systèmes biométriques

Un system biométrique peut :

- **Enrôler une identité** : créer un modèle de référence numérique d'une caractéristique d'une personne et l'enregistrer dans une base des données.
- **Identifier une identité** : L'identification nécessite un échantillon à comparer avec chaque échantillon de référence (1 pour plusieurs), contenue dans une base de données, afin de trouver une correspondance si elle existe.
- **Vérifier une identité** : comparaison (1 pour 1) entre un échantillon capturé récemment et un échantillon de référence.

II.2.2.2. Les attributs d'un système biométrique :

Chaque type de mesure biométrique peut être classé avec un certain nombre de caractéristiques qui devraient être considérés dans le processus de sélection. Le choix de la technique biométrique à utiliser n'est pas une simple décision à faire.

La biométrie s'appuie sur l'unicité, mais aucune caractéristique biométrique n'est 100% unique, même si elle est unique, parfois le système ajoute des erreurs dans l'échantillon de référence lors le processus d'extraction.

L'unicité, n'est pas le seul critère utilisé pour décider la technique à mettre en œuvre. Plusieurs autres caractéristiques ou facteurs sont utilisés :

- **Unicité** : Le trait doit être suffisamment différent d'une personne à une autre, par exemple : l'empreinte digitale.
- **Universalité** : toute les personne ayant accès à l'application doit posséder le trait.
- **Permanence**: le trait biométrique d'une personne doit être suffisamment invariant au cours d'une période de temps.
- **Mesurabilité** : La possibilité d'acquérir et de numériser les données biométriques à l'aide d'un dispositif approprié.
- **Acceptabilité** : les individus doivent être disposés à présenter leurs traits au système.
- **Contournement :** la facilité d'imité d'un trait biométrique en utilisant des objets (faux doigt par exemple) [6] [17]

II.2.2.3. Les composants d'un système biométrique

Tous les systèmes biométriques peuvent être décrits par un modèle général. Un système biométrique complet comprend plusieurs sous-systèmes distincts (voir Figure II.8): la capture biométrique, le traitement de signal et l'extraction des caractéristiques biométriques, le stockage de

l'information biométrique, la comparaison biométrique et, enfin, le processus de pris la décision en se basant sur cette comparaison si elle est la bonne personne.

a. **Acquisition :** processus de collecte d'un échantillon biométrique d'un utilisateur en utilisant un dispositif électronique permettant d'obtenir une représentation numérique d'un élément du corps humain (par exemple: scanner d'empreintes digitales, tablette de signature).

b. **Extraction :** le traitement de l'échantillon capturé. Ce processus fait appel à trois opérations:

- Le contrôle de qualité : si l'élément capturé a une faible qualité alors le ré-enrôlement est nécessaire.
- L'extraction des informations biométriques uniques (Template ou modèle de référence), qui a pour but de recueillir des points particuliers dans l'échantillon.
- L'enlèvement de bruit et le fond inutile. Le résultat de ce processus est la création d'un modèle de référence unique.

c. **Stockage :** permet de stocker le modèle de référence au cours de l'étape d'enregistrement dans une base de données.

d. **Appariement :** Un algorithme biométrique compare les caractéristiques du modèle de référence mémorisée et les caractéristiques extraites à partir de l'échantillon capturé, Le résultat de ce processus est une valeur (typiquement, est une valeur entre 0 et 1 où 1 présente un match parfait) indique le degré de similitude entre les deux échantillons.

e. **Décision :** phase de décider d'accorder ou de refuser l'accès [6] [13]

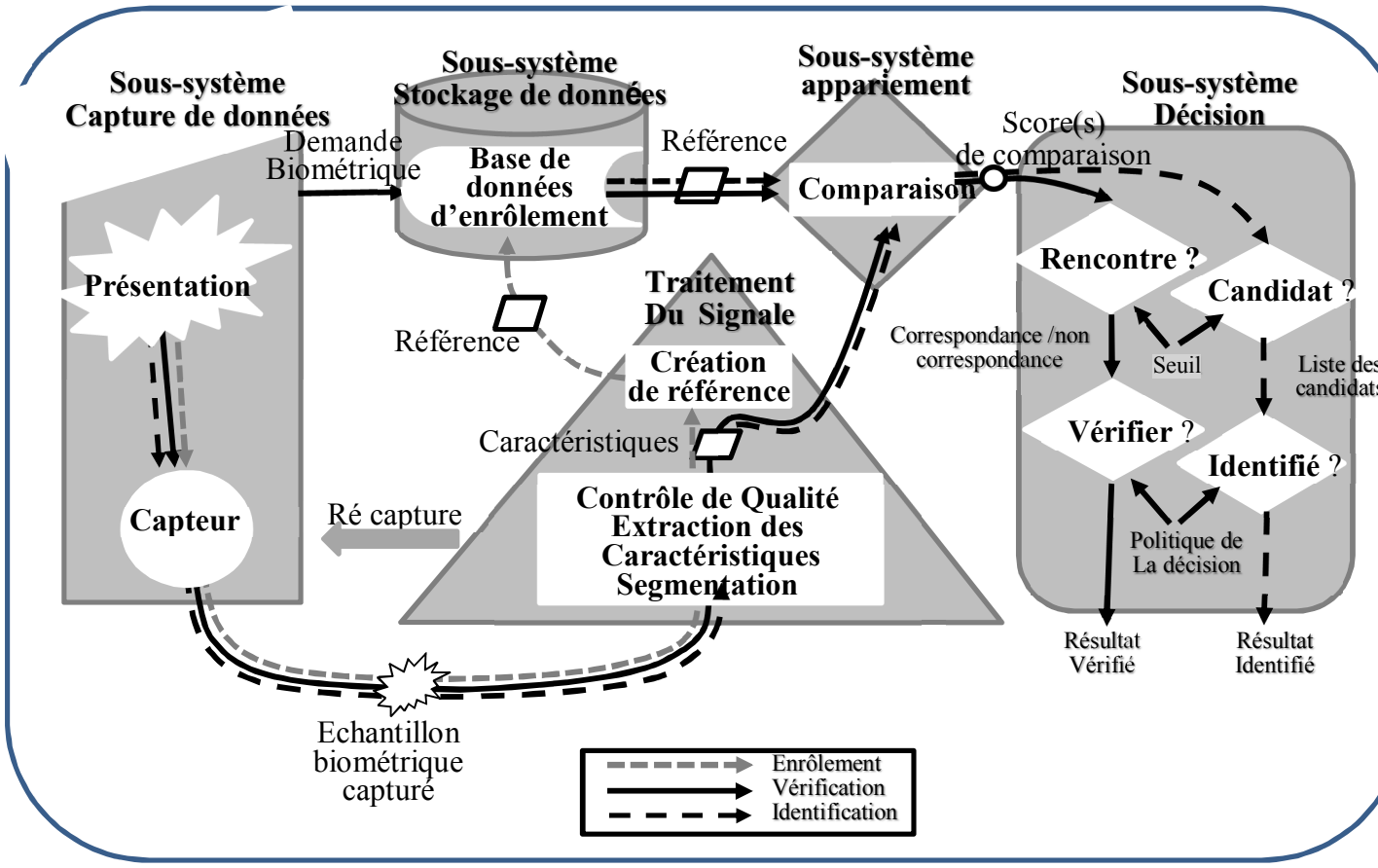


Figure II.8 Les composants généraux d'un système biométrique [13]

II.3. Les modalités biométriques

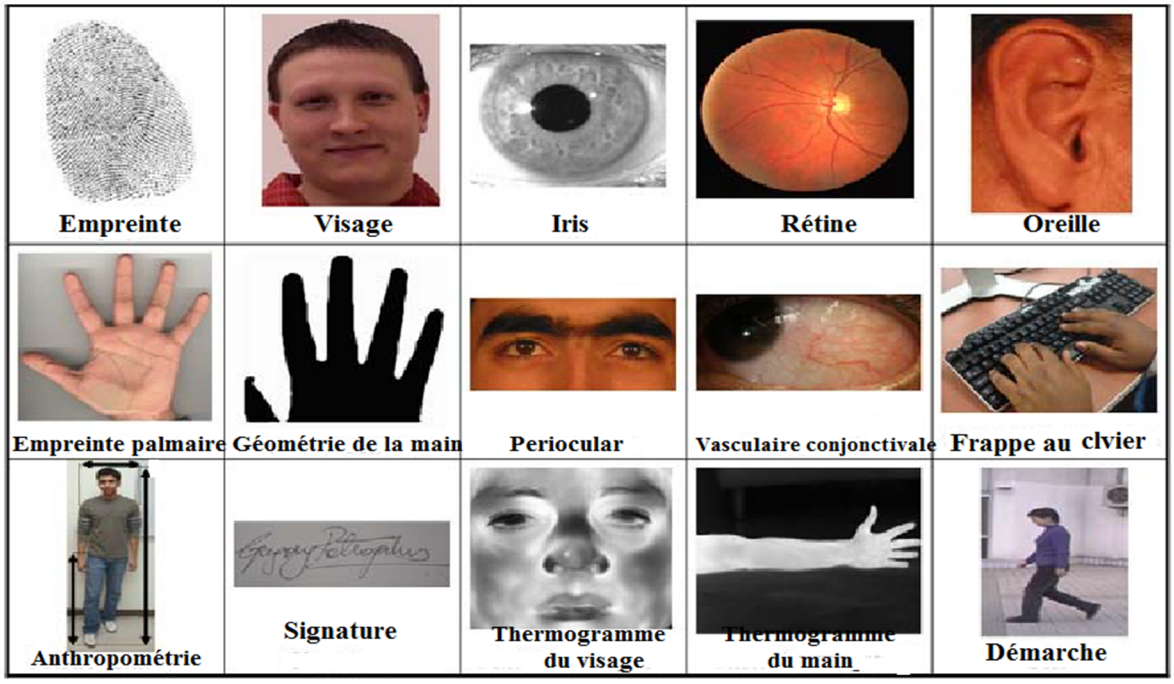


Figure II.9 un ensemble de traits biométriques couramment utilisés [18]

Il existe deux catégories de technique de reconnaissance biométrique:

- Les techniques d'analyse de la morphologie humaine : il s'agit d'un type de biométrie défini par des caractéristiques physiques.
- Les techniques d'analyse du comportement : il s'agit d'un type de biométrie caractérisées par un trait d'attitude qui est appris et acquis au fil du temps.

II.3.1. Les approches par biométrie physiologique

Ces approches généralement ont des caractéristiques invariantes, et souvent utilisés à la fois dans les systèmes de vérification et d'identification.

Cette section fournit brièvement une introduction aux approches physiologiques, citons : Les empreintes digitales, la main, le visage, l'œil…etc.

II.3.1.1. Les empreintes digitales

Une empreinte digitale est une impression ou une reproduction laissée sur tout objet, formée par le frottement de la peau du doigt avec l'objet, elle se compose de beaucoup des rides et sillons. Les empreintes digitales ne sont pas bien distinguées par leurs rides et sillons, mais par des minuties qui sont des points anormaux sur les rides.

La reconnaissance d'empreinte digitale est la technique la plus ancienne et la plus couramment utilisée, elle est basée principalement sur trois approches :

- La corrélation des pixels d'image de deux empreintes digitales.
- L'extraction des minuties à partir des images de deux empreintes digitales et les stockées sous forme d'un ensemble de points dans un plan de deux dimensions pour l'alignement entre les minuties du motif et les minuties d'entrée. Le résultat est le nombre maximum des paires de minuties.
- Les rides : cette approche utilise des caractéristiques extraites des rides (orientation, forme de ride, etc...) pour comparer les empreintes digitales.

Figure II.10Les différents capteurs d'empreinte digitale

L'acquisition des données se faite par un capteur électronique de type optique, thermique, capacitif ou à ultrasons.

L'empreinte digitale est unique pour chaque individu et garde la même forme tout au long de la vie [6]

Cette approche est détaillée dans le chapitre qui suit.

II.3.1.2. La forme de la main

La géométrie de la main implique l'utilisation d'un scanner spécialisé, qui prend un certain nombre de mesures telles que la longueur, la largeur, l'épaisseur et la surface des doigts et de la main.

Des différents systèmes prennent différents mesures, mais tous les systèmes sont généralement fondés sur le même ensemble de caractéristiques. Malheureusement, ces caractéristiques n'ont pas tendance à être assez unique pour les systèmes d'identification à grande échelle, mais sont souvent utilisés pour les systèmes de pointage.

Le capteur et le matériel nécessaires pour capturer l'image est grande et probablement pas approprié pour plusieurs applications telles que le login à un ordinateur [6]

II.3.1.3. La reconnaissance par visage

La reconnaissance faciale qui utilise les traits de visage a trouvé une popularité croissante dans la sécurité informatique et les applications de surveillance, grâce à l'augmentation des performances des algorithmes les plus récents et sa nature secrète (c'est à dire l'authentification de l'individu peut se faire sans leur interaction explicite avec un dispositif ou un capteur). Cette approche biométrie satisfait deux caractères, il s'agit de l'universalité et de l'acceptabilité (dans la plupart des scénarios).

Les techniques actuelles s'appuient sur le traitement des différences entre les caractéristiques des échantillons qui contiennent des mesures comme les couleurs des yeux, la distance entre les yeux et le nez. Les recherches les plus récents sont concentrées sur l'imagerie en trois dimensions (3D).

Les algorithmes d'extraction des paramètres de visage peuvent être classés en trois grandes catégories :

- **Méthodes local basées sur un modèle**: des propriétés et des relations géométriques sont utilisés comme descripteurs pour la reconnaissance du visage tels que les zones, les distances et les angles entre les points caractéristiques du visage.
- **Méthodes basées sur l'apparence globale du visage:** Elles utilisent directement des valeurs d'intensité des pixels de l'image entière du visage comme caractéristiques sur lesquelles la décision de reconnaissance sera fondée.

Ces algorithmes généralement procéder en calculant des vecteurs de base pour représenter les données de visage efficacement, dans l'étape suivante, les visages sont projetées sur ces vecteurs et des coefficients de projection peuvent être utilisées pour représenter les images de visage.

Il existe plusieurs algorithmes populaires basent sur l'apparence du visage, citons :

- L'analyse en composantes principales (PCA) : fut d'abord utilisé pour représenter efficacement des images de visages humains. La méthode classique détruire la structure géométrique de l'image de visage (par conséquent perdre les informations de voisinage) lors du passage de l'image en vecteurs. Pour éviter ce problème une méthode PCA bidimensionnelle (2-D PCA) (qui prend en entrée des images et non plus des vecteurs) a été étudiée.
- L'analyse discriminante linéaire (LDA) : Le LDA construis un sous-espace discriminant pour distinguer de façon optimale les visages de différentes personnes (PCA construit un sous- espace pour représenter seulement « l'objet » visage). Elle permet d'effectuer une véritable séparation de classes.

- **Méthodes hybrides:** Elles permettent de combinent la détection de caractéristiques géométriques avec l'extraction de caractéristiques d'apparence locales (i.e. associer les avantages des méthodes globales et locales) pour augmenter les performances lors de changements de pose, d'éclairement et d'expressions faciales. Exemple des algorithmes hybrides sont L'analyse des caractéristiques locales (LFA) et les caractéristiques extraites par ondelettes de Gabor (comme l'Elastic Bunch Graph Matchig, EBGM) [6] [14]

La performance des algorithmes de reconnaissance faciale peut varier considérablement selon le contexte (par exemple des images haute résolution par rapport à faible résolution, la position et de l'environnement) et les algorithmes d'extraction et de classification employées.

II.3.1.4. Le thermogramme du visage

Thermogramme du visage est une approche qui a évolué à partir de domaine de la reconnaissance faciale, et le problème de l'éclairage insuffisant pour l'appareil photo pour prendre une bonne qualité d'image. Elle utilise une caméra infrarouge pour capter la configuration de chaleur d'un visage provoquée par le flux sanguin sous la peau. L'unicité est présente à travers la structure de la veine et des tissus du visage d'un individu. Cependant, la plupart des recherches ont combiné les capteurs visibles avec les thermogrammes [6]

II.3.1.5. L'iris

L'iris est le tissu coloré sous forme d'anneau, située entre la pupille et le blanc de l'œil, il est unique et composée de motifs complexes avec de nombreux sillons et crêtes. L'iris est une approche biométrique idéale en termes de son unicité et de stabilité (variation avec le temps), avec des résultats extrêmement rapides et précises.

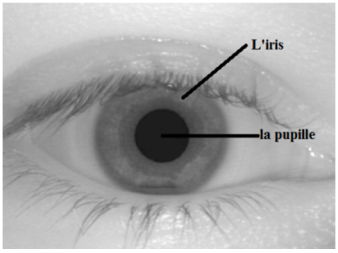


Figure II.11 L'iris

Traditionnellement, les systèmes nécessite une distance focale très courte pour capturer l'image, mais les nouveaux acquièrent des images à des distances allant jusqu'à 40 cm. les caméras sont encore sensible à l'alignement des yeux.

La reconnaissance de l'iris est donc adaptée à des scénarios d'identification et c'est là où la majorité des implémentations à ce jour ont été déployées. Par exemple, le Royaume-Uni utilisé reconnaissance de l'iris pour accélérer le contrôle des passeports dans les aéroports [6]

John Daugman est l'inventeur de la reconnaissance de l'iris, et ses algorithmes sous-tendent tous les déploiements publics de cette technologie dans le monde entier, ils sont devenus commercialisés dans les années 1990. Son algorithme reconnaît les personnes automatiquement et en temps réel, en codant des motifs aléatoires visible dans l'iris de l'œil d'une certaine distance, et en appliquant un test d'indépendance statistique. Il utilise une transformée en ondelettes de Gabor pour extraire la structure de l'iris. Ceci est codé en un train de bits très compact [15]

II.3.1.6. La rétine

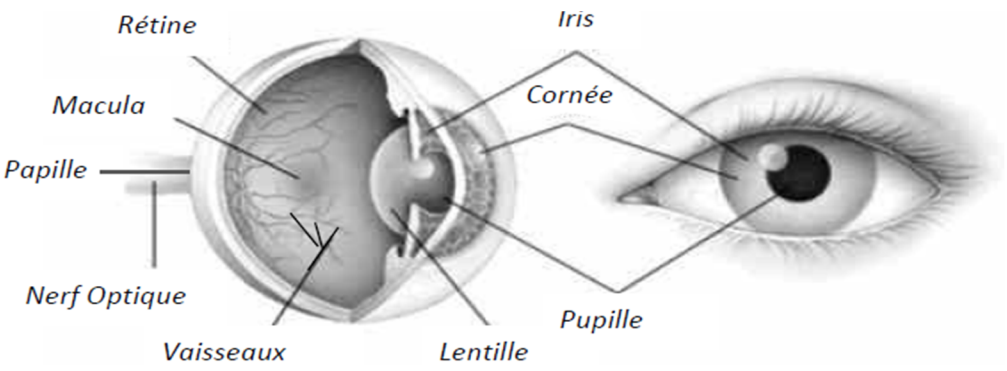


Figure II.12 Un illustration du fond d'œil [17]

Robert Hill est l'inventeur original de la technologie RI (Retinal Identification) et le fondateur de l'entreprise 'EyeDentify' [16]

Le scanner de rétine utilise les caractéristiques distinctives de la rétine pour l'identification et la vérification. Une caméra infrarouge est utilisée pour prendre une photo de la rétine, en illuminant le modèle unique des veines au fond de l'œil.

De même à la reconnaissance de l'iris, cette technique souffre de problème d'ennui les utilisateurs tels que l'individu est tenue de présenter soigneusement les yeux de la caméra à très grande proximité.

Cette technique souvent utilisé dans les solutions d'accès physique où l'exigence a la sécurité est très élevé. Elle présent une performance excellente dans la phase de l'extraction des caractéristiques produisant au maximum 400 points de données (30-40 points pour les minuties d'une empreinte digitale) [6]

Il existe plusieurs algorithmes pour l'extraction des caractéristiques de rétine, certains d'entre eux basées sur une comparaison des modèles formés par les points de bifurcation et le croisement des branches du réseau vasculaire [17]

II.3.1.7. La forme de l'oreille

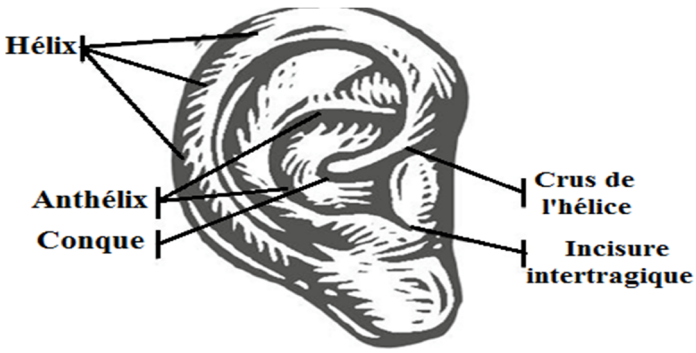


Figure II.13 L'anatomie de l'oreille [6]

Comme illustré dans la Figure II.13, l'oreille est constituée de plusieurs composants, y compris l'hélice, anthélix, conque et l'incisure intertragique, ce qui se traduit par un motif relativement unique.

Cette approche vérifier le critère d'universalité efficacement (peu de gens sont nés sans oreille) et comprendre son critère d'acceptabilité est difficile à établir, car aucun système biométrique commercial n'implémente la géométrie de l'oreille. Elle a été utilisée presque exclusivement dans le domaine juridique.

Tandis que recueillir l'échantillon de l'oreille peut avoir ses difficultés, des études ont affirmé que la géométrie de l'oreille ne souffre pas tellement de facteurs environnementaux tels que la

reconnaissance faciale, les mouvements faciaux ou les problèmes d'orientation et est suffisamment grande pour capturer à partir d'une distance contrairement à les approches de reconnaissance d'iris et de rétine [6]

II.3.2. Les approches par la biométrie comportementale

La biométrie comportementale classe une personne selon un comportement unique qui change au fil du temps en raison de l'environnement, la société et les variations de la santé. Elle est considérée comme moins sûre étant donné le caractère évolutif des comportements que la biométrie physique. Cette section présente brièvement quelques approches comportementales.

II.3.2.1. La reconnaissance de locuteur par la voix

La reconnaissance du locuteur par sa voix est une modalité biométrique qui utilise la voix d'un individu à des fins de reconnaître le locuteur (C'est une technologie différente de "reconnaissance vocale", qui reconnaît les mots comme ils sont articulés).

Le processus de reconnaissance du locuteur s'appuie sur les caractéristiques influencé à la fois par la structure physique du conduit vocal et les caractéristiques comportementales d'un individu.

Les échantillons de parole sont des formes d'onde avec : le temps sur l'axe horizontal et le volume sur l'accès vertical.

Le système de reconnaissance du locuteur analyse le contenu de fréquence de la parole et compare des caractéristiques telles que la qualité, la durée, l'intensité dynamique, et la hauteur tonale du signal. L'analyse peut être réalisée en deux modes, dépendant et indépendant du texte :

- En mode dépendant du texte, le texte prononcé par le locuteur est le même que celui qu'il a prononcé lors de l'apprentissage de sa voix.
- En mode indépendant du texte, le locuteur peut prononcer n'importe quelle phrase pour être reconnu [6]

II.3.2.2. La signature

Les systèmes de reconnaissance de signatures tentent d'authentifier une personne par l'analyse de la façon dont un utilisateur signe son nom, cette méthode a été utilisé depuis des années sur papier, mais en tant que biométrique elle est plus récente.

L'authentification de la signature peut être réalisée de manière statique et / ou dynamique :

- Dans la vérification de signature statique, seules les formes géométriques de la signature sont utilisées pour authentifier une personne,
- L'authentification dynamique utilise aussi des informations concernant la façon dont la signature a été produite, telles que la vitesse, l'accélération et la pression.

La signature évolue dans le temps et est influencée par les conditions physiques et émotionnelles de la personne.

Les taux de performance pour la reconnaissance de la signature sont mieux que la plupart des approches comportementales [6]

II.3.2.3. La démarche

Cette approche utilise la façon de la marche d'une personne pour déterminer son identité, il peut être réalisé d'une distance très loin plus que toute autre approche biométrique.

La chaussure, la surface de marche et les vêtements et d'autres facteurs comme l'âge et la maladie, jouent un rôle important dans la variance d'échantillons.

Un échantillon de la démarche inclut la marche d'une personne sur deux progrès. Selon les quels le processus de classification est basées. On distingue L'approche basée sur la forme qui s'intéresse sur la forme globale de l'image de l'individu pendant ce cycle, et l'approche de la dynamique qui s'intéresse sur le taux de transition dans le cycle [6]

L'inconvénient majeur de cette approche est que les attributs d'universalité et de permanence ne sont pas assurés.

II.3.2.4. La dynamique de frappe

La reconnaissance biométrique accueille une nouvelle technologie, basée sur la dynamique de frappe sur un clavier. En analysant la façon dont on tape un texte sur un clavier, cet outil biométrique remplacera peut être un jour le mot de passe graphique, et permettra de garantir la validité d'un mot de passe.

La façon dont une personne tape les touches d'un clavier a été utilisée pour démontrer certaines propriétés uniques. Ce processus d'authentification est connu comme l'analyse de frappe (ou dynamique).

L'authentification proprement dite peut être réalisée soit en mode statique (texte dépendant) ou dynamique (texte indépendant), la première approche est la plus fiable.

Les caractéristiques particulières utilisées pour différencier les personnes peuvent varier, mais elles incluent souvent le temps entre les frappes successives, aussi connu comme le temps de latence entre la frappe et le temps de maintien d'une pression sur une touche.

Les facteurs uniques d'analyse de frappe ne sont pas suffisamment discriminant pour l'utilisation au sein d'un système d'identification, mais peut être utilisé dans un système de vérification. [6]

II.4. Les approches multi biométriques

L'un des objectifs essential d'authentification est de fournir une plateforme qui permet d'utilisés une variété d'approches afin de couvrir le point faible d'utilisation les approches biométriques Individuellement (i.e. une seule approche biométrique ne fournit pas une vérification suffisante d'une population complète). Dans le secteur de la biométrie, l'accent a été mis sur multi-biométrie, capitalisant sur les points forts de deux ou plusieurs approches pour contourner les problèmes. Chaque approche multi-biométrique: multimodal, multi-instance et multi-algorithmique, a son propre ensemble d'avantages qui permettent d'atteindre à un ensemble particulier d'objectifs.
La Multi-biométrie peut être divisée en six catégories:

- **Multimodal**: l'utilisation de plusieurs méthodes biométriques.
- **Multi-échantillon**: l'utilisation de plusieurs échantillons de la même caractéristique biométrique.
- **Multi-algorithmique:** se réfère à l'utilisation de plus d'un algorithme lors de la phase de l'appariement.
- **Multi-instance** se référer à l'utilisation de plusieurs sous-types de la même caractéristique biométrique, par exemple, l'iris gauche et droit ou les empreintes des de la main gauche et droite. Cette approche est particulièrement utile dans les situations où la population des utilisateurs est particulièrement importante. Plutôt que de compter sur une seule instance biométrique pour fournir un caractère distinctif suffisant pour distinguer l'ensemble de la population, l'utilisation de multi-instances simplifie le problème.
- **Multi-capteurs:** ces approches utilisent plus d'un capteur pour capturer une seule traite biométrique. Cette approche est utile lorsque les différents capteurs sont en mesure d'apporter une information complémentaire au problème de classification.
- **Les approches hybrides** utilisent une combinaison des approches mentionnées ci-dessus, par exemple, la combinaison d'une approche multimodale et multi-algorithmique. Chaque technique individuelle utilise plusieurs algorithmes de classification pour optimiser la réponse individuelle, mais ces réponses sont également combinées avec d'autres techniques biométriques.
  Les systèmes hybrides, s'ils sont conçus correctement, représentent les plus robustes et les plus forts (en termes de performances de reconnaissance) des systèmes biométriques. Cependant, ils représentent aussi les plus complexes (nécessitant une augmentation du stockage et une architecture complexes).[6]

Comme la Figure II.14 illustre, dans un appareil mobile, il existe une possibilité de capturer le visage, la voix, les caractéristiques comportementales et d'autres caractéristiques en même temps.

Figure II.14 Un exemple d'un mobile inclus un system multi biométrique [6]

II.5. Avantages et inconvénient

Technique	Avantages	Inconvénient	Physique/ Logique
Empreinte digitale	Cout. Ergonomie moyenne. Facilité de mise en place. Taille du capteur.	Qualité optimale des appareils de mesure (fiabilité). Acceptabilité moyenne. Possibilité d'attaque.	P/L
Forme de la main	Très ergonomique. Bonne acceptabilité.	Système encombrant. Cout. Perturbation possible par des blessures et l'authentification des membres d'une même famille.	P
Visage	Cout. Peu encombrement. Bonne acceptabilité.	Jumeaux. Psychologie, religion. Déguisement… Vulnérable aux attaques.	P
Rétine	Fiabilité. Pérennité.	Cout. Acceptabilité faible. Installation difficile.	P

Iris	Fiabilité.	Acceptabilité très faible. Contrainte d'éclairage.	P
Voix	Facile	Vulnérable aux attaques.	P/L
Signature	Ergonomie	Dépendance de l'état émotionne de la personne. Fiabilité.	L
Dynamique de la frappe	Ergonomie.	Dépendant de l'état physique de la personne.	L

Tableau II.2 : Les avantages et inconvénient des modalités biométrique [22]

Rq : La colonne Physique/Logique précise l'usage le plus courant de chaque technique.

Propriété **Technique biométrique**	**Universalité**	**Unicité**	**Permanence**	**Recouvrabilité**	**Performance**	**Acceptabilité**	**Circumvention**
Visage	H	F	M	H	F	H	L
Empreinte digitale	M	H	H	M	H	M	M
Forme de la main	M	M	M	H	M	M	M
Iris	H	H	H	M	H	F	F
Dynamique de la frappe	F	F	F	M	F	M	M
Signature	F	F	F	H	F	H	H
Voix	M	F	F	M	F	H	H

Tableau II.3 Une comparaison entre diverses technologies biométriques [16].

H = Haut, M = moyenne, F = Faible

II.5. Conclusion

En résumé, l'exigence accrue pour des systèmes d'authentification fiables et commodes. La disponibilité des ressources informatiques peu couteuses, le bon marché de développement des capteurs biométriques, et les avancements dans le traitement du signal, ont contribué au déploiement rapide des systèmes biométriques dans les établissements s'étendant des épiceries aux aéroports. C'est seulement une question de temps avant que la biométrie puisse s'intégrer même dans le tissu de la société et s'imposer dans notre vie quotidienne

Par ailleurs, la biométrie n'est pas une science exacte: elle reste dépendante de la qualité des captures, du traitement de celles-ci, et donnes des réponses en termes de pourcentage de similitude.il faut donc tenir compte d'un facteur de risque.

La biométrie présente bien des avantages qui donnent un intérêt d'une grande importance dans la sécurité des infrastructures et des systèmes informatiques.

La reconnaissance d'empreintes digitales est le système biométrique le plus populaire et mature utilisé aujourd'hui, ils sont précis, rapides, robustes, acceptables pour le public, et ils sont difficiles à contourner

Dans le chapitre qui suit une étude détaillée de l’approche de reconnaissance par empreinte digitale sera présentée.

Chapitre III

La reconnaissance d’empreinte digitale

III.1. Introduction

Après l'invention de l'anthropométrie par Alphonse Bertillon et la découverte de la spécificité des empreintes digitales humaines, les empreintes digitales ont été utilisées dans différents domaines comme l'investigation juridique et la médecine légale.

Par la suite, des préoccupations croissantes concernant la sécurité ont créé un besoin croissant pour les empreintes digitales et d'autres technologies biométriques de reconnaissance des personnes dans un grand nombre d'applications non-judiciaires.

III.2. Généralité

III.2.1. Les champs d'application

Les deux méthodes les plus populaires pour classer les applications de reconnaissance biométrique sont la catégorisation horizontale et la catégorisation verticale.

a) **Catégorisation horizontale** : les catégories sont des applications qui ont des caractéristiques communes dont ils ont besoin à partir du système de reconnaissance d'empreinte digitale :

- Contrôle d'accès physique: l'accès est limité à certains aménagements comme les centrales nucléaires, banque.
- Contrôle d'accès logique: l'accès aux ordinateurs de bureau ou les serveurs et les bases de données distantes est limité aux utilisateurs autorisés. En plus, l'accès à des applications logicielles est également limité aux seuls utilisateurs autorisés.
- Contrôle d'accès de périphérique: les ordinateurs portables, les PDA, les téléphones cellulaires et autres appareils électroniques contiennent souvent des données personnelles et sensibles.
- Temps de présence: les systèmes de pointage sont utilisés pour garder une trace de salariés, les heures de travail et de calculer la masse salariale.
- Identification civile: application d'identification civile, l'objectif le plus important est d'empêcher les inscriptions multiples et à trouver des doublons.
- Identification judiciaire: les empreintes digitales latentes levée des scènes de crime sont comparées à une base de données criminelles pour identifier le suspect (et parfois les victimes).

b) **Catégorisation verticale :** basé sur les besoins d'un secteur particulier de l'industrie ou du gouvernement point:

- Les soins de santé.
- Financière.
- Jeux et hospitalité (casinos, hôtels, etc).
- Éducation.
- Fabrication.
- La haute technologie et des télécommunications.

- Voyage et transports.
- Fédérales, étatiques, les administrations municipales, ou d'autres.
- Militaire.

Chaque marché vertical peut avoir un besoin pour un certain nombre de différentes applications horizontales [19]

III.2.2. Caractéristiques et représentation des empreintes digitale

Pour bien distinguer les empreintes il est nécessaire de choisir des caractéristiques invariantes et uniques pour chaque doigt d'une personne.

Une empreinte digitale est la reproduction de l'apparence extérieure de l'épiderme du bout des doigts, elle est formée d'un ensemble de lignes sombres dessinées sur l'épiderme appelées stries (crêtes), et des espaces lumineux appelés vallées (voir figure III.15), Les empreintes digitales sont distinguées par les minuties, les points singuliers, l'épaisseur de rides, la séparation de rides, la profondeur de rides et les locations des points critiques.

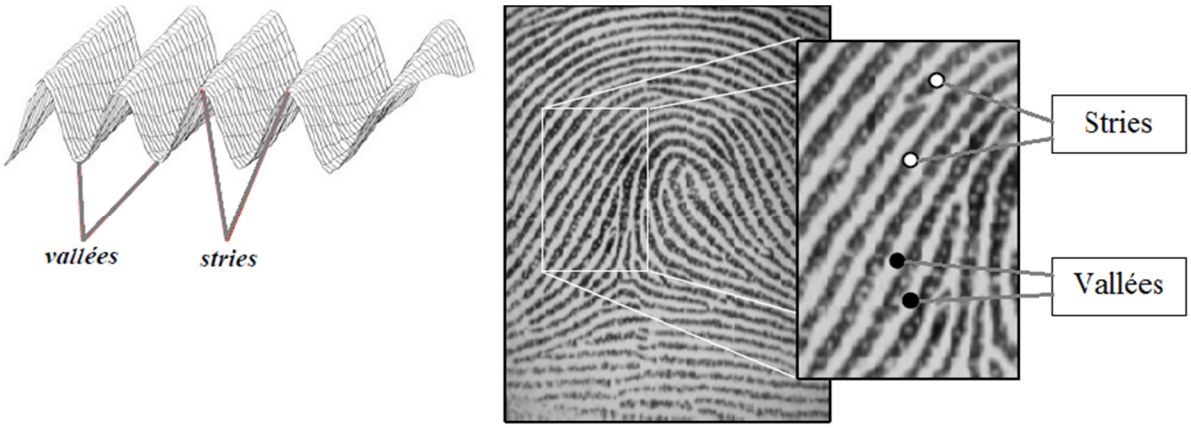


Figure III.15 Les Stries et Les vallées dans une image d'empreinte [19] [21]

Une bonne représentation d'empreintes digitales devrait avoir les deux propriétés suivantes:

a) la représentation devrait contenir des informations distinctive sur l'empreinte.
b) la représentation peut être facilement extrait, stocké dans un mode compact, et être utile pour l'appariement.

Plusieurs représentations des empreintes digitales sont proposées, elles sont classifiées en trois niveaux principaux: Niveau 1 : les points singuliers, Niveau 2 : les minuties, Niveau3: les pores, forme locale de bords d'arête, etc.)[19] [21]

III.2.2.1 Niveau 1 : Les points singuliers globaux

Dans certaines régions de l'empreinte les dessins de stries adoptent des formes distinctes. Ces régions s'appellent points singulières, elles sont classées en trois grandes catégories : boucle, delta (lieu de divergences des stries) et spires ou tourbillon, ils sont généralement utilisés dans la phase de classification des empreintes dans la base de données pour simplifier la recherche et la récupération.

Une autre caractéristique globale d'une empreinte utilisée dans certains algorithmes de comparaison d'empreintes digitales est le cœur (noyau) de l'empreinte. C'est le point où il y a le plus de convergences des stries.

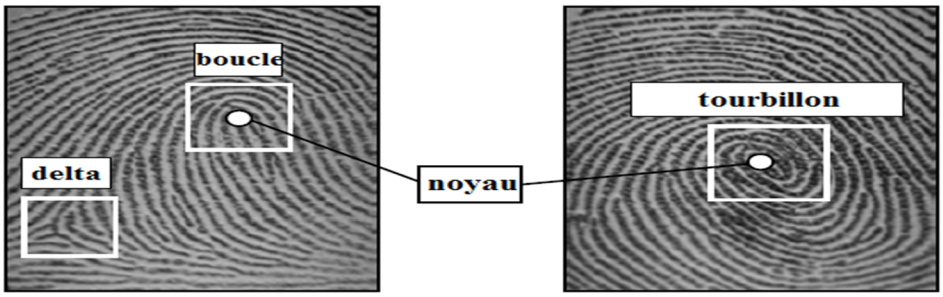


Figure III.16 Les points singuliers et le noyau dans une empreinte [19]

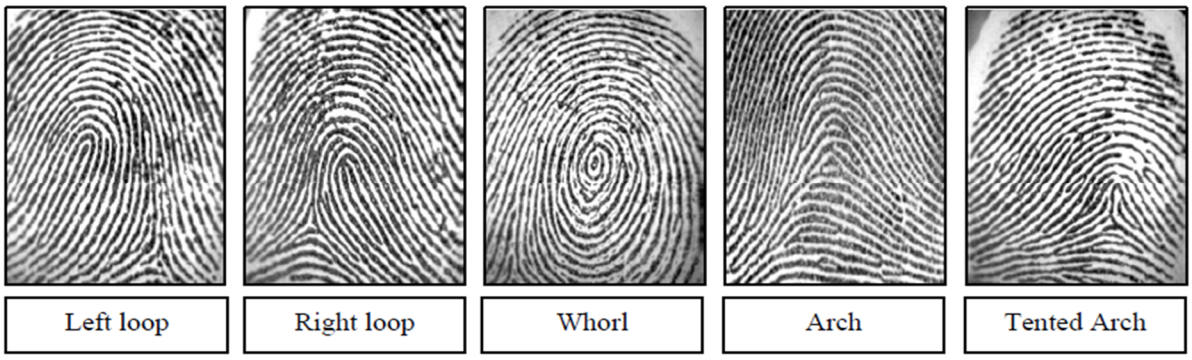


Figure III.17 Une empreinte pour chaque classe de subdivision d'Edward Henry (1900) [19]

III.2.2.2 Niveau 2 : les minuties

Les empreintes ne sont pas bien distinguées par leurs stries et vallées, mais par les minuties (littéralement : petits détails), qui sont des points anormaux sur les stries et les différentes discontinuités de lignes d'une empreinte. Parmi les types des minuties, deux types sont les plus utilisés car ils sont facilement détectables : la terminaison qui est l'arrêt (la fin) d'une crête, et la bifurcation, le point sur le strie dans lequelle deux branches dérivent, ces deux types permettent la

reconstitution de toutes les minuties, toute autre minutie peut se composer de combinaisons de bifurcations et de fins de crêtes.

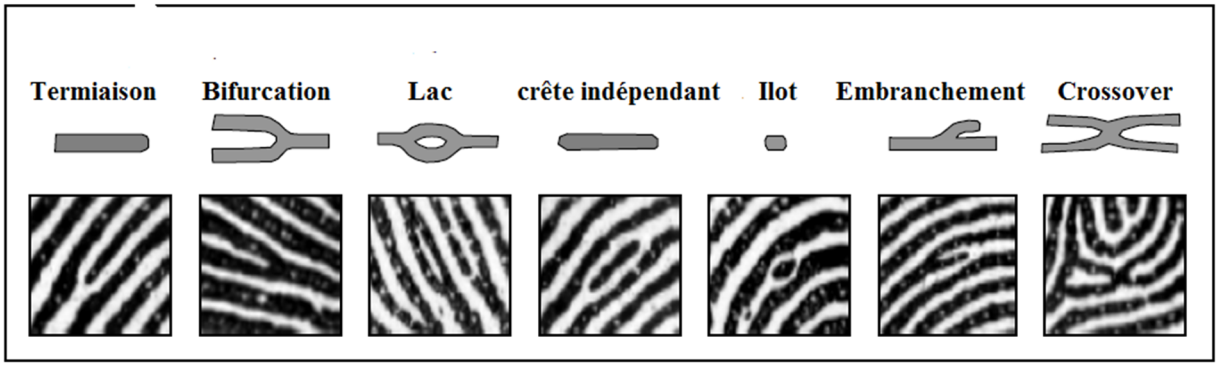


Figure III.18 Les types des minuties les plus fréquentes [19]

Figure III.19 montre une partie de l'image d'empreinte digitale où les lignes de crête apparaissent comme des traces noir sur un fond clair; deux terminaisons (1, 2) et une bifurcation (3) sont affichés. Remarque que sur l'image négative(b), les minuties correspondantes prennent les mêmes positions, mais leur type change : les terminaisons apparaissent comme des bifurcations et vice versa (cette propriété est connue comme terminaison/bifurcation dualité).

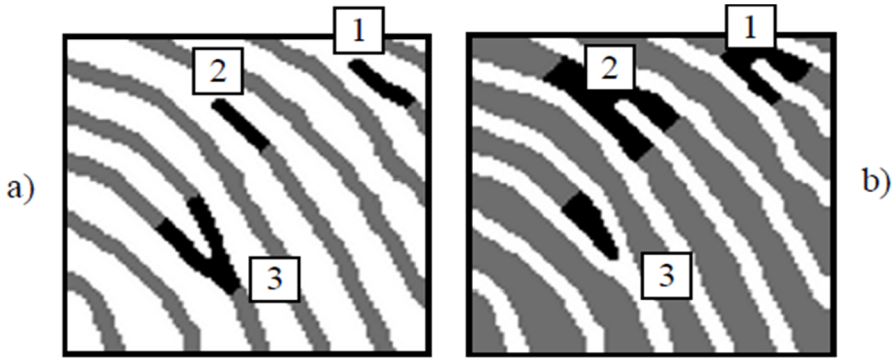


Figure III.19 La dualité des terminaisons/ bifurcations [19]
a) une image binaire et b) son image négative

La représentation des minuties la plus simple constituent une liste de points définis par leurs coordonnées spatiales, où chaque minutie est représentée par le vecteur : (type de minutie, x, y, θ) où θ est l'angle entre la tangente de la ligne de crête dans la position (x, y) de minuties et l'axe horizontal.

Dans la figure III.19 :

a) la terminaison est représenté par (terminaison, x, y, θ).

b) la bifurcation est représenté par (bifurcation, x_0, y_0, θ_0) θ_0 est défini par la tangente de la terminaison correspondant à la bifurcation origine qui existe dans l'image négative.

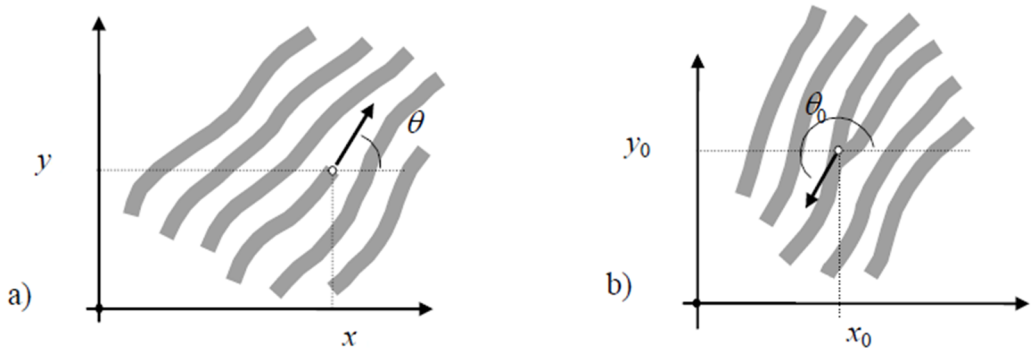


Figure III.20 La représentation d'une terminaison et une bifurcation [19]

III.2.2.2 Niveau 3 : le niveau très fin

Au niveau très fin, des détails intérieurs de crête peuvent être détectés. Elles comprennent tous les attributs dimensionnels des crêtes, tels que la largeur, la forme, les pores, les cicatrices, ainsi que d'autres détails permanents. L'une des plus importants détails de ce niveau est les pores sudoripares du doigt (voir figure III.21), dont les positions et les formes sont distinctif.

Toutefois, l'extraction des détails très-fins est possible seulement en haute résolution d'images d'empreintes digitales de bonne qualité et donc ce type de représentation n'est pas pratique pour les applications non-judiciaires.

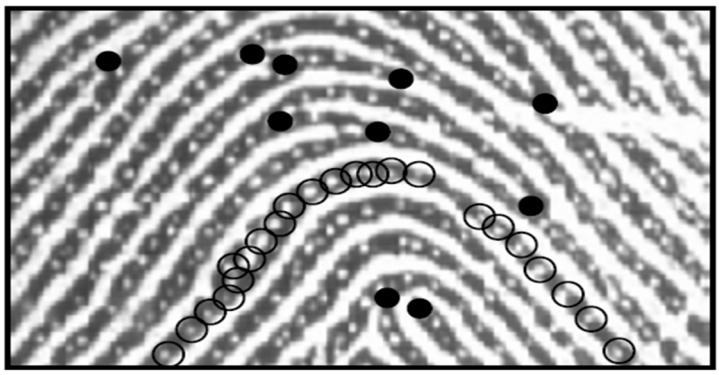


Figure III.21 Les minuties (cercles noir), Les pores sudoripares (cercles vide) sur les lignes de crête [19]

III.3. Processus de reconnaissance d'une empreint digitale

III.3.1. L'acquisition d'empreintes digitales

L'acquisition d'images d'empreintes digitales a été historiquement réalisée en étalant le doigt avec l'encre et le pressant contre une carte de papier. La carte papier est alors numérisée, résultant en une représentation numérique. Ce processus est connu comme l'acquisition hors ligne et est encore utilisé dans les applications de l'application de la loi. Actuellement, il est possible d'acquérir des images d'empreintes digitales en appuyant sur le doigt contre la surface plane d'un capteur d'empreinte digitale électronique. Ce processus est connu comme l'acquisition en ligne. Il existe

trois familles de capteurs d'empreintes digitales électroniques basés sur la technologie de détection [19] [20]:

III.3.1.1. Les capteurs de silicium

Les capteurs de silicium (ou les semi-conducteurs) consistent en une matrice de pixels, chaque pixel est un capteur lui-même. Les utilisateurs placent le doigt sur la surface du silicium, et quatre techniques sont généralement utilisés pour convertir les informations crête / vallée en signaux électriques: capacitive, thermique, champ électrique et piézoélectrique.

Les capteurs à semi-conducteurs n'utilisent pas des composants optiques, leur taille est considérablement plus petit et peut être facilement intégré. D'autre part, les capteurs de silicium sont chers, de sorte que la zone de détection d'un capteur à semi-conducteurs est généralement petite.

III.3.1.2. Les capteurs Optiques

Le doigt touche un prisme de verre et le prisme est éclairé par une lumière diffuse. La lumière est réfléchie sur les vallées et absorbé les crêtes. La lumière réfléchie est focalisée sur un capteur CCD ou CMOS. Ces Capteurs optiques offrent une bonne qualité d'image et une grande zone de détection, mais ils ne peuvent pas être miniaturisés, car tant que la distance entre le prisme et le capteur d'image est réduite, plus de distorsion optique est introduite dans l'image acquise.

III.3.1.3. Les capteurs échographie

Des signaux acoustiques sont envoyés, en capturant les signaux d'écho qui sont réfléchis à la surface de l'empreinte digitale. Les signaux acoustiques sont capables de traverser la saleté et l'huile qui peut être présente dans le doigt, donnant ainsi des images de bonne qualité. D'autre part, les échographes sont volumineux et coûteux, et de prendre quelques secondes pour acquérir une image.

Une nouvelle génération de dispositifs de scan sans contact direct qui génèrent une représentation 3D d'empreintes digitales comparaît [20].

Plusieurs images du doigt sont acquises à partir de différentes vues à l'aide d'un système multi-caméra, et une représentation 3D sans contact de l'empreinte digitale est construite. Cette nouvelle technologie de détection de surmonter certains problèmes qui apparaissent intrinsèque dans les capteurs à contacts tels que le placement incorrect du doigt, la déformation de la peau, le bruit du capteur ou de la saleté.

III.3.2. Le prétraitement et l'extraction des caractéristique

La représentation **en niveaux de gris** d'une image d'empreinte digitale est connue pour être instable pour la reconnaissance d'empreintes digitales. Bien qu'il existe des techniques d'appariement des empreintes digitales qui comparent directement des images grises en utilisant des méthodes à base de corrélation, la plupart des algorithmes de comparaison d'empreintes digitales utilisent les caractérisés qui sont extraites de l'image en niveaux de gris.

Pour faire cette extraction facile et fiable, un ensemble d'étapes de prétraitement est souvent réalisée: calcul de la fréquence locale et de l'orientation locale des crêtes, l'amélioration de l'image d'empreinte digitale, la segmentation de la zone d'empreinte digitale à partir de l'arrière-plan, et la détection des singularités.

III.3.2.1. L'orientation locale des rides

L'orientation locale des rides au niveau de pixel est définie comme l'angle des rides d'empreintes digitales qui forment avec l'axe horizontal [19]. La plupart des algorithmes ne pas calculer l'orientation locale des rides à chaque pixel, mais sur une grille à mailles carrées (Figure III.22).

Figure III.22 L'orientation locale de crête d'une image d'empreinte digitale, calculé sur une grille à mailles carrées [20]

L'approche la plus simple pour l'estimation de l'orientation locale des rides est basée sur le gradient de niveau de gris. Puisque l'angle de phase de gradient dénote le sens de la variation maximale de l'intensité de pixels, l'orientation de crête est orthogonale sur cet angle de phase.

Il existe essentiellement deux techniques d'estimation d'orientation: échantillonnage par direction de tenseur et spectrale tenseur discrétisation en utilisant des filtres de Gabor. Pour son efficacité de calcul, la première technique est la plus utilisé actuellement dans les applications d'empreintes digitales parce que l'approche spectrale besoin de plus de filtrage [20]

III.3.2.1.2. La fréquence locale de crête

La fréquence locale de crête au niveau du pixel est défini comme le nombre des crêtes par unité de longueur le long d'un segment présomptif centrée sur ce pixel et orthogonale à l'orientation locale

des crêtes [19]. Les méthodes existantes modélisent généralement la structure de crête-vallée comme une onde de forme sinusoïdale (Figure III.23), où la fréquence de crête est définie comme la fréquence de cette sinusoïde, et l'orientation est utilisée pour anglé l'onde [20].

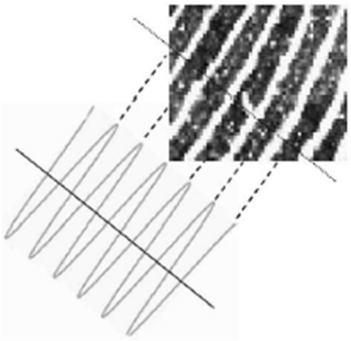


Figure III.23 La structure de crête et de vallée comme une onde de forme sinusoïdale [20]

III.3.2.3. L'Amélioration

Dans une image d'empreinte digitale, les crêtes et les vallées de couler en douceur dans une direction constant localement.

En pratique, cependant, il y a des facteurs qui influent sur la qualité d'une image d'empreinte digitale (Figure III.24): l'humidité ou la sécheresse de la peau, le bruit du capteur, et des coupures temporaires ou permanentes de la peau, la variabilité de la pression sur le capteur, etc.

Figure III.24 les images d'empreintes digitales avec différentes qualités [20]

Plusieurs algorithmes d'amélioration ont été proposés dans la littérature, dans le but d'améliorer la clarté de crêtes et de vallées. Les techniques d'amélioration d'empreintes digitales les plus largement utilisés appliquent un filtre contextuel, ce qui veut dire la modification des paramètres de filtrage selon les caractéristiques locales (contexte) de l'image. Les filtres sont réglés pour l'orientation de l'arête locale et / ou de la fréquence, supprimant ainsi les imperfections et de préserver les crêtes et les vallées (Figure III.25)

Figure III.25 Une image d'empreinte améliorée [20]

III.3.2.4. La segmentation

La segmentation consiste à séparer la zone d'empreinte digitale du fond [19]. Ceci est utile pour éviter l'extraction ultérieure de caractéristiques du fond d'empreintes, qui est la zone bruyante.

Les méthodes de segmentation qui utilisent un seuillage global ou local ne sont pas très efficaces. Des techniques plus robustes sont utilisées en exploitant l'existence d'un motif périodique orientée au premier plan et un modèle isotrope non orienté en arrière-plan (Figure III.26).

Figure III.26 Un exemple de segmentation d'une image d'empreinte [20]

III.3.2.5. La détection des singularités

Comme mentionné ci-dessus, le motif de crêtes et de vallées présente un certain nombre de formes particulières appelé singularités. Pour la détection des singularités, la plupart des algorithmes existants s'appuient sur les informations d'orientation de crête. L'algorithme le plus connu pour la détection de la singularité est basé sur l'indice de Poincaré [19]. Alternativement, la détection des singularités de type noyau et delta a été montré pour être efficace et précis en utilisant des techniques de filtrage différentes [20].

III.3.2.6. Extraction de caractéristiques

Une fois l'image d'empreinte digitale a été prétraitée, une étape d'extraction de caractéristiques est effectuée.

La plupart des systèmes de reconnaissance d'empreintes digitales existants sont basées sur l'appariement des minuties, par conséquent la phase d'extraction des minuties est une tâche extrêmement importante.

Généralement, l'image d'empreinte digitale prétraitée est convertie en une image binaire en deux couleurs (noir et blanc), qui est ensuite amincie en utilisant la morphologie.
L'étape d'amincissement réduit l'épaisseur de crête à un pixel, résultant une image squelette. Une analyse simple d'image permet alors la détection directe des pixels qui correspondent aux minuties. Au cours de l'étape d'amincissement, un certain nombre d'imperfections parasites peuvent apparaître et donc, une étape de post-traitement est parfois réalisée afin d'éliminer les imperfections de l'image amincie.

Figure III.27 La binarisation et l'amincissement d'images d'empreintes en utilisant des filtres contextuels [20]

Plusieurs approches pour la binarisation, l'amincissement et la détection des minuties ont été proposées dans la littérature [19]

Un algorithme pour la détection de minuties : (Crossing Number)
Soit un pixel sur une crête amincie (avec 8 voisins), il a une valeur de 0 ou 1. Le couple (x, y) dénote un pixel sur une crête amincie, et $N_0,...,N_7$ dénotent les 8 voisins.

Un pixel (x, y) est une fin de crête si ($\sum_{i=0}^{8} N_i$) = 1.

Un pixel (x, y) est une bifurcation si ($\sum_{i=0}^{8} N_i$) > 2

Le nombre ($\sum_{i=0}^{8} Ni$) s'appelle le nombre de connexions NC. [23]

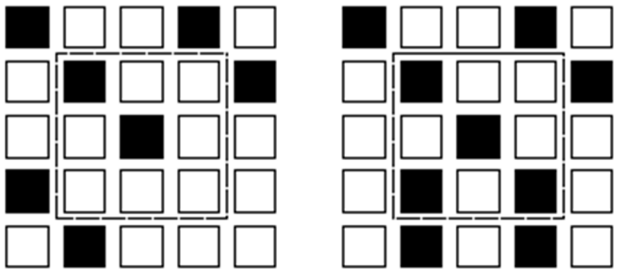


Figure III.28 La détection des minuties sur une carte amincie [19]

Cependant, binarisation et amincissement souffrent de plusieurs problèmes:
a) les imperfections parasites;

b) la perte de l'information structurelle ;

c) le coût de calcul;

d) le manque de robustesse dans les images d'empreintes digitales de faible qualité.

A cause de cela, d'autres approches qui extraient minuties directement à partir de l'image d'échelle de gris ont également été proposées [19].

III.3.3. La comparaison des empreintes digitale

Dans l'étape d'appariement, les caractéristiques extraites à partir de l'empreinte digitale d'entrée sont comparés à ceux qui sont dans le Template, ce qui représente un seul utilisateur (extraites de la base de données du système sur la base de l'identité revendiquée).

Le résultat d'une telle procédure est soit un degré de similitude (également appelé score de correspondance) ou une décision d'acceptation / rejet, Il existe des techniques d'appariement des empreintes digitales qui comparent directement les images en niveaux de gris en utilisant des méthodes à base de corrélation, de sorte que le modèle d'empreinte digitale coïncide avec l'image à échelle de gris. Cependant, la plupart des algorithmes d'appariement des empreintes digitales utiliser les caractéristiques qui sont extraites de l'image en niveaux de gris.

Un des plus grands défis de la reconnaissance des empreintes digitales est la grande variabilité trouvé entre les différentes impressions d'un même doigt. Les facteurs principaux responsables des variations d'intra-classe sont: déplacement, rotation, déformation non-linéaire, variation des pressions, changement d'état de peau, bruit, et erreurs d'extraction des caractéristiques …etc

La comparaison des empreinte digitale reste comme un problème de reconnaissance de motifs difficile en raison de la difficulté de comparaison des empreintes digitales affectées par un ou plusieurs des facteurs mentionnés [19].

Plusieurs approches de comparaison des empreintes digitales peut être trouvé dans la littérature. Ils peuvent être classés en:

a) les approches à base de corrélation.

b) les approches fondées sur les minuties.

c) caractéristique approches fondées sur les caractéristique des crêtes.

III.3.3.1 L'appariement basé sur la corrélation

Dans les approches basées sur la corrélation, les images d'empreintes digitales sont superposées et les images d'échelle de gris sont directement comparées en utilisant une mesure de corrélation.

En raison de la distorsion non linéaire, des impressions différentes du même doigt peuvent entraîner des différences de la structure globale, rendant la comparaison unifiables. Le calcul de la corrélation

entre les deux images d'empreintes digitales est coûteux. Pour traiter ces problèmes, la corrélation peut être calculée uniquement dans certains points locaux de l'image, qui peut être choisie suivant plusieurs critères. En outre, afin d'accélérer le processus, la corrélation peut être calculée dans le domaine de Fourier ou en utilisant des approches heuristiques, qui permettent de réduis le nombre d'opérations de calcul.

III.3.3.2 L'appariement basé sur les minuties

Les approches fondées sur les minuties sont les méthodes les plus populaires et largement utilisés pour la comparaison d'empreintes digitales, car ils sont analogues avec la façon dont les experts médico-légaux comparent les empreintes.

Les minuties sont extraites de deux empreintes, et représentées comme un ensemble de points dans un plan à deux dimensions selon le modèle de coordonnées. La comparaison consiste à trouver un bon alignement de minuties de deux empreintes (T et I) qui produit un nombre maximum de paires de minuties qui ont le même emplacement et la même orientation.

Les deux empreintes à comparer **I** et **T** sont des vecteurs de minuties, où chaque minutie **m** est représentée à son tour par un vecteur (x, y,θ) où x et y sont les coordonnées de l'emplacement de la minutie dans l'image de l'empreinte, et est l'orientation de la minutie, c'est le modèle de coordonnées [19]:

$$T = \{m_1, m_2, \dots, m_m\} \qquad m_i = \{x_i, y_i, \theta_i\} \qquad i = 1..\ m$$

$$I = \{m'_1, m'_2, \dots, m'_n\} \qquad m'_j = \{x'_j, y'_j, \theta'_j\} \qquad j = 1..\ n$$

Où m et n sont respectivement le nombre de minuties de T et I.

On considère qu'il y a un "match" entre une minutie m'_j de T et une minutie m_i de I lorsque la distance sd (pour spatial distance) qui les sépare est inférieure ou égale à une tolérance r_0, et la différence dd (pour direction difference) de leurs angles est inférieure ou égale à une certaine tolérance angulaire θ_0 :

$$\mathrm{Sd}(m'_j, m_i) = \sqrt{(x'_j - x_i)^2 + (y'_j - y_i)^2} \leq r_0$$

$$\mathrm{dd}(m'_j, m_i) = min(|\theta'_j - \theta_i|, 360^\circ - |\theta'_j - \theta_i|) \leq \theta_0$$

III.3.3.3 L'appariement basé sur les rides

Malheureusement, l'extraction des minuties depuis les images à faible qualité connue pour être peu fiable. Pour cette raison et d'autres, des caractéristiques alternatives ont été proposées dans la littérature comme une alternative aux minuties (ou pour être utilisé en conjonction avec les minuties) [19]. L'alternative la plus largement étudiée pour l'empreinte digitale est les informations de texture. La structure de l'empreinte digitale se compose d'une répétition périodiques d'un motif de crêtes et de vallées qui peut être caractérisée par son orientation locale, la fréquence, la symétrie, etc. les informations texture sont moins discriminante que minuties, mais plus fiable dans les conditions de faible qualité [20].

III.4. Conclusion

La reconnaissance des empreintes digitales est la méthode biométrique la plus ancien et la plus utilisée pour l'identification et l'investigation juridique. Les caractéristique d'une empreinte digitale est unique, universel et permanent.

Il convient d'élaborer des méthodes efficaces de détection de minuties, afin de mettre en place un système de reconnaissance fiable.

En faisant des recherches sur ce projet, nous avons acquis des connaissances sur les diverses caractéristiques de d'empreintes digitales, les techniques, les structures d'empreintes digitales, l'analyse des images d'empreinte digitale, comparaison et image filtres.

Chapitre IV
Implémentation

IV.1. Préliminaire

Dans ce dernier chapitre et après l'aperçu théorique des chapitres précédents, nous présentons le côté pratique de notre application .Notre but est la réalisation d'un système flexible et fiable qui authentifie un individu par son empreinte.

L'implémentation est faite sur un système d'exploitation Windows 7 qui est un système multitâche reconnu pour sa stabilité et ses performances.

Pour le langage de programmation, nous avons choisi d'utiliser le langage JAVA sous l'environnement de développement Eclipse, un kit de développement logiciel (SDK) et une base de données MySql, un choix qui se justifie par les nombreux avantages qu'ils offrent.

IV.2. Le langage de codage : JAVA

Java est un langage de programmation informatique orienté objet , créé par James Gosling et Patrick Naughton employés de Sun Microsystems présenté en 1995. La particularité et l'objectif central de Java est que les logiciels écrits sous ce langage doivent être très facilement portables sur plusieurs systèmes d'exploitation tels que UNIX, Windows, Mac OS ou GNU/Linux, avec peu ou pas de modifications. Pour cela, divers plateformes associés visent à guider, sinon garantir, cette portabilité des applications développées en Java.

Java peut être séparée en deux parties. D'une part, le programme écrit en langage Java et d'autre part, une machine virtuelle (JVM) qui va se charger de l'exécution de programme Java. C'est cette plateforme qui garantit la portabilité de Java. Il suffit qu'un système ait une machine virtuelle Java pour que tout programme écrit en Java puisse fonctionner. Sa syntaxe est proche de celle du C, mais Java n'est pas une surcouche du C et sa syntaxe est beaucoup plus claire que celle du C++.

Le langage Java, permet de développer des applications Desktop, des applets pour les sites web, et des applications pour les téléphones mobiles. Il présente beaucoup d'avantages: sécurisé, orienté objet, haut niveau, robuste, indépendant du matériel, portable, avec une JDK très riche, les applications sont plus sûres et stables, des IDE très bonne qualité et libres : Eclipse et Netbeans par exemple [24].

IV.3. L'environnement de travail : Eclipse

Eclipse est un environnement de programmation visuelle orientée objet très performant permettant le développement d'applications en vue de leur déploiement sous Windows ou sous Linux. Il trouve son origine au sein de la société IBM, qui a décidé de mettre, à disposition de la communauté Open Source, le projet d'une plateforme de développement ouverte entièrement écrite en Java et

capable d'intégrer des extensions adaptées à diverses activités (débogage, modélisation, interfaces graphiques...).

L'objectif étant de créer un environnement de développement intégré polyvalent, Extensible, capable de travailler avec n'importe quel langage de programmation. [24]

IV.4. Le SDK

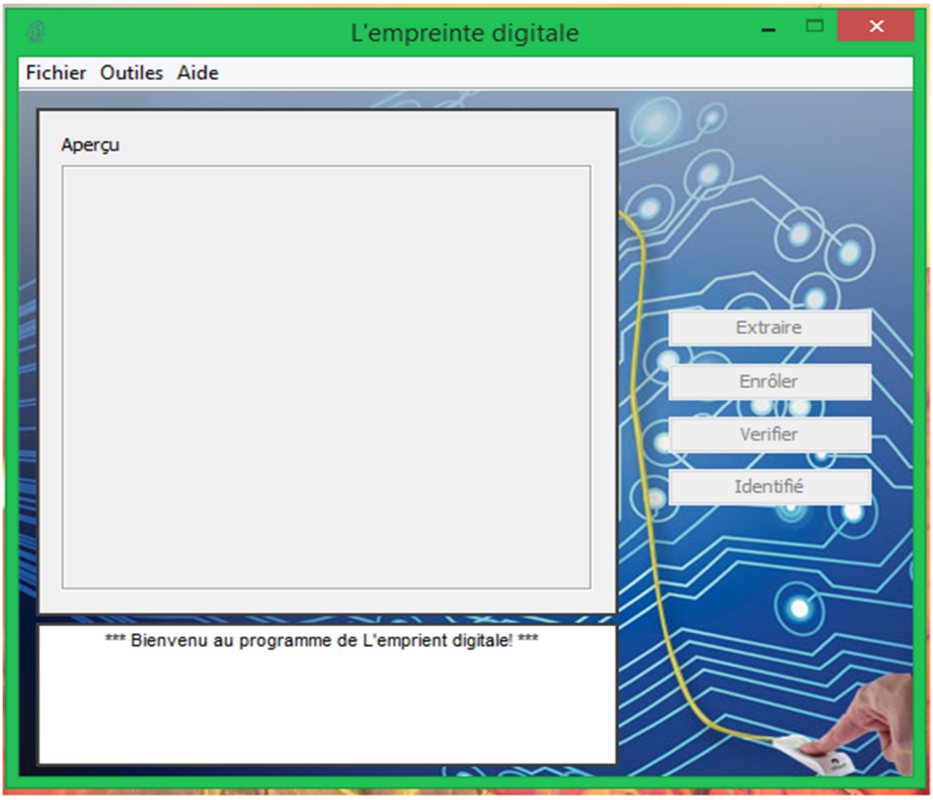
SDK (Software Development Kit) **:** Littéralement « kit de développement logiciel ». Est un ensemble de briques logicielles permettant d'intégrer une solution tierce (par exemple l'acquisition d'une empreinte digitale à l'aide d'un capteur) dans une autre application, sans pour autant posséder le code source de celle-ci. Il fournit une plate-forme flexible pour le développement et la programmation des systèmes biométriques complets de reconnaissance d'empreinte digitale.
(La source de SDK: http://www.griaulebiometrics.com)

IV.5. Le system de gestion de base de données (SGBD)

Un SGBD a pour rôle de stocker et de gérer une grande quantité de données en les organisant sous forme de tables, et de permettre la manipulation de ces données à travers le langage de requête SQL.
Il existe plusieurs SGBD tel que Oracle Database, Access de Microsoft, MySQL, mais nous avons choisie MySQL car il est devenue le SGBD open source le plus populaire au monde grâce à sa haute performance, sa fiabilité et sa simplicité d'utilisation. Non seulement MySQL est la base de données open source la plus populaire au monde mais elle est aussi devenue le choix privilégié pour la nouvelle génération d'applications développées sur la pile LAMP (Linux, Apache, MySQL, PHP / Perl / Python.). MySQL fonctionne sur plus de 20 plateformes incluant Linux, Windows, Mac OS.
Il existe plusieurs outils pour se connecter à distance à une base de données MySQL, nous pouvons citer entre autre : PhpMyAdmin, MysqlWorkbeng, Mysql administrat, SQL Yog… Nous avons utilisé MySql java connecter pour notre application

IV.6. Présentation de l'application

Cette partie présente les captures d'écran et les codes sources essentiels de notre application.
La figure qui suit présente la fenêtre principale.



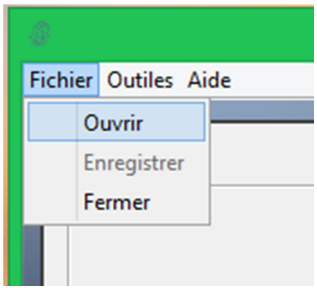
Vue l'indisponibilité du matériel d'acquisition des mesures (capteur d'empreinte), on a opté pour le choix d'une image à partir d'une grande base d'images téléchargées d'internet.

Donc le choix de l'image simule la présentation d'un individu au capteur pour faire l'acquisition de son empreinte.

Pour chaque individu il existe deux images (deux mesures différentes) l'une pour l'enrôlement tandis que l'autre est pour la vérification ou l'identification

IV.6.2. Le choix d'image d'empreinte digitale

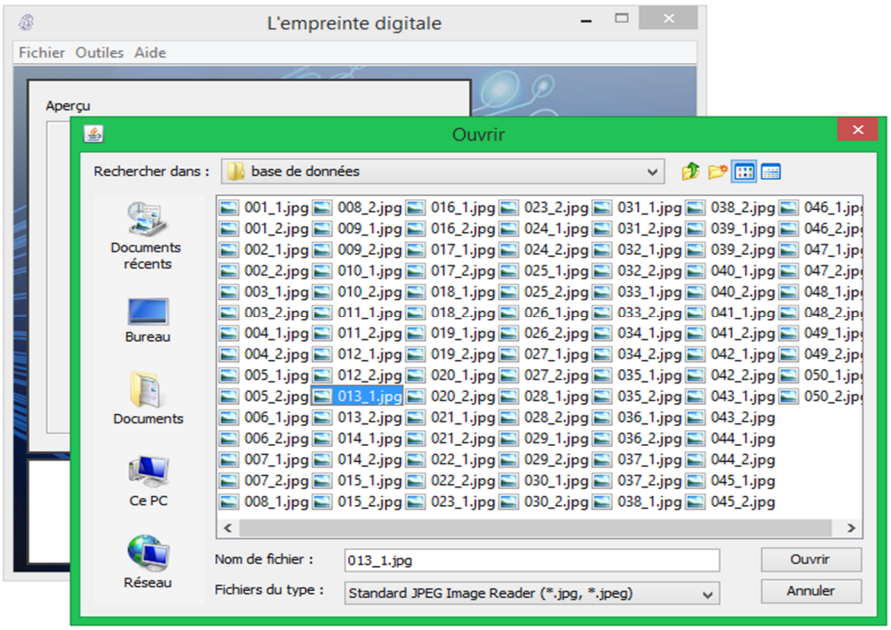
Pour choisir une image tous simplement on clique sur Fichier dans la barre de menu puis sur le Ouvrir. Une fenêtre apparait dans laquelle on choisit une image de l'empreinte digitale pour extraire ses minuties.



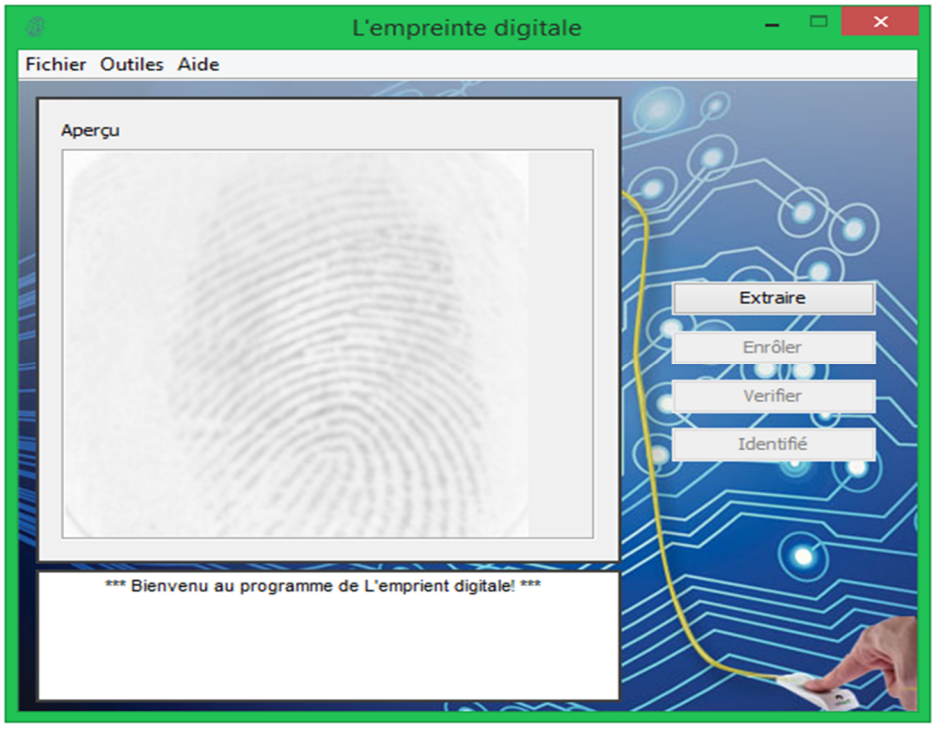
```
menuItem.addActionListener(new ActionListener() {
	public void actionPerformed(ActionEvent arg0) {
		AjouterImage(fingerprintSDKSample);
	}});
```

Figure IV.29 : L'action du menu ouvrir.

Le code source illustré par la figure IV.29 permet d'afficher la fenêtre suivante :

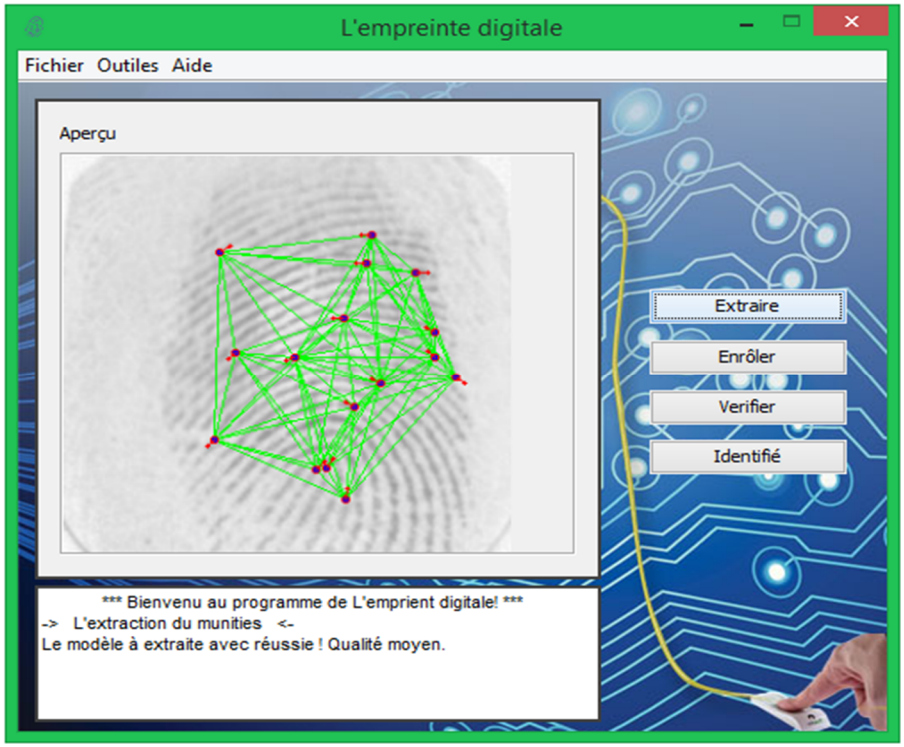


Un aperçu d'empreinte digitale (de l'image sélectionnée dans l'étape précédente).



IV.6.3 l'extraction des minuties

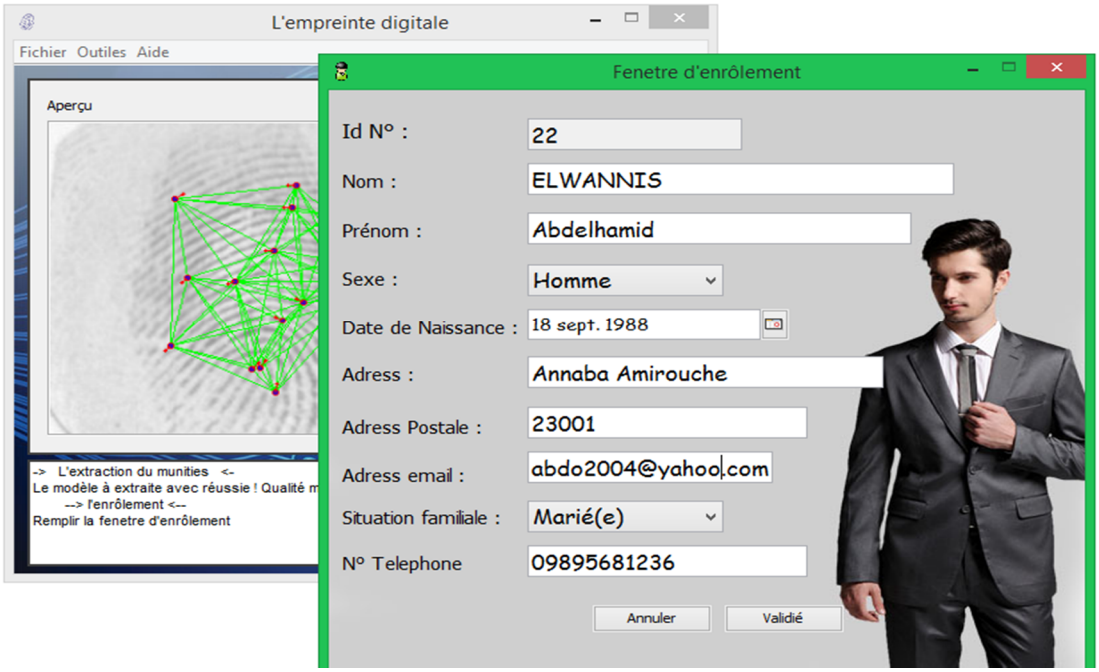
En cliquant sur le bouton Extraire , l'extraction des minuties se fait et il apparaissent sous formes de points rouges sur l'image



IV.6.4 l'enrôlement

Tel que cité auparavant l'enrôlement consiste à sauvegarder un modèle de référence dans la base de données contenant les renseignements relatifs à l'individu courant.

Cela et fait par le bouton «enrôler ».



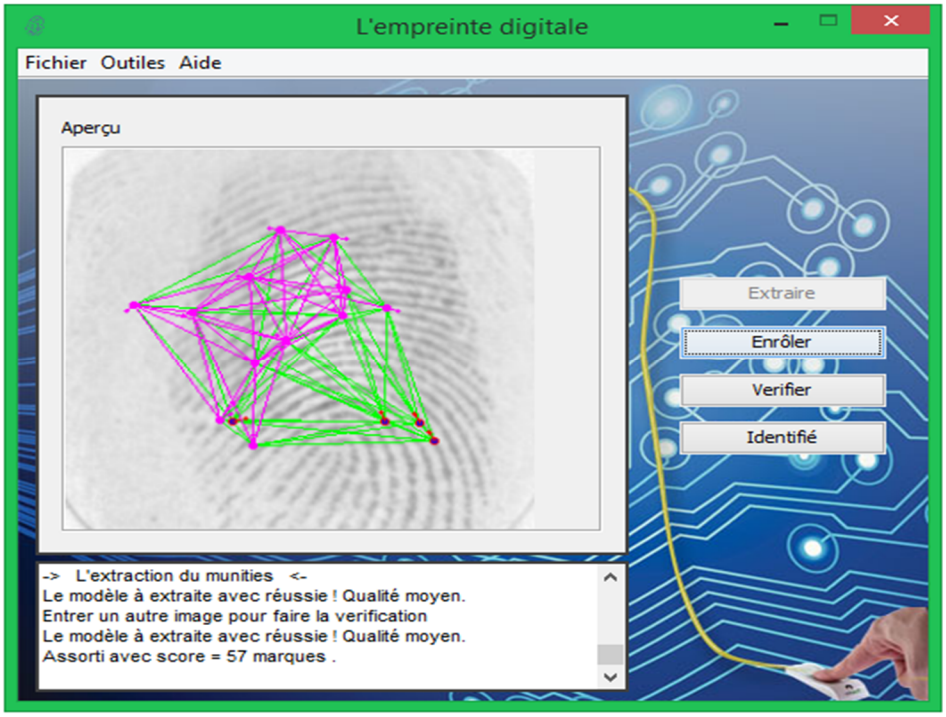
IV.5. Vérification

Cette phase permet de vérifier si le modèle de référence élaboré est en mesure d'identifier l'individu. pour cela une deuxième mesure est nécessaire(dans notre cas une deuxième image du même individu) sans oublier de fournir son ID.

C'est une comparaison un à un.

L'aperçu affiche les minuties qui correspondent aux deux images et la barre d'état affiche le score(le nombre des minuties qui sont en correspondance).

Les couleurs de minuties de la 1er image sont violets claires et vertes dans la 2eme.



IV.6.6 l'identification

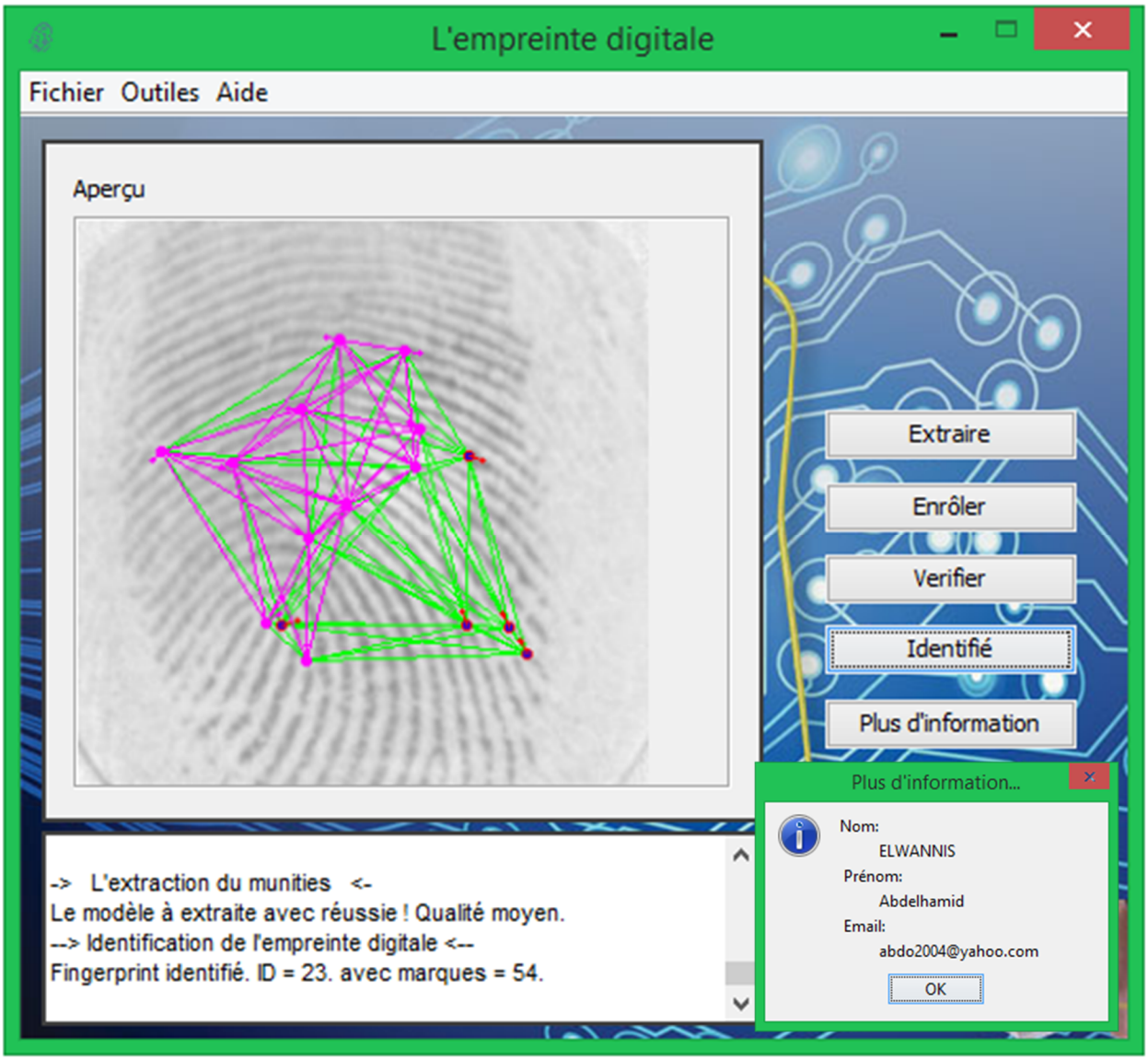
Pour identifier un individu (vérifier s'il existe dans notre base données) on choisit l'image d'empreinte digitale qui lui correspond on clique sur « Identifier ».

Le déroulement de cette étape et le même que celui de la vérification, néanmoins elle ne nécessite pas l'ID.

Elle parcourt toute la base de données pour comparer l'empreinte digitale avec les modèles de référence existants.

L'aperçu affiche les deux images (la mesure lors de l'identification et celle du Template) avec les minuties correspondantes entre eux. La zone d'état affiche si l'individu identifié ou non.

Les renseignements de l'individu identifié sont affichés sur la fenêtre« Plus d'information ».


L'empreinte digitale
Fichier Outiles Aide
Aperçu
Extraire
Enrôler
Verifier
Identifié
Plus d'information
-> L'extraction du munities <-
Le modèle à extraite avec réussie ! Qualité moyen.
--> Identification de l'empreinte digitale <--
Fingerprint identifié. ID = 23. avec marques = 54.
Plus d'information...
Nom:
ELWANNIS
Prénom:
Abdelhamid
Email:
abdo2004@yahoo.com
OK

Bibliographie

[1] Information Security Fundamentals, Second Edition. Thomas R. Peltier. 2014
[2] Introduction to information security. Dan Hutchison. http://arapaho.nsuok.edu/~hutchisd/
[3] Le Grand Livre de SecuriteInfo.com. http://www.securiteinfo.com .
[4] Sécurité Informatique Principes et Méthode. Laurent Bloch & Christophe Wolfhugel. 2007
[5] Principles of Information Security 4th edition, Michael E. Whitman & Herbert J.Mattord, 2011.
[6] Transparent User Authentication, Nathan Clarke, 2011.
[7] Cryptography, A Very Short Introduction ,Fred Piper & Sean Murphy, 2002.
[8] Mechanics of User Identification And Authentication ,Dobromir Todorov, 2012.
[9] Authentication technologies and suitability to task, HP ProtectTools, 2005.
[10] Thechniques de controle d'acces par boimetrie. Dossier technique. 2003
[11] Biometrics for Dummies. Peter Gregory, CISA, CISSP and Michael A. Simon 2008
[12] Biométrie pour l'Identification. Rapport final de type. Dang Hoang. Institut de la Francophonie pour l'informatique. 2005
[13]Biometric System and Data Analysis Design, Evaluation, Data Mining. Ted Dunstone.Neil Yager. 2009
[14] Détection et identification de personne par méthode biométrique. Mémoire de magister en électronique (Option: télédétection).Université UMMTO. boudjellal sofiane.
[15]How Iris Recognition Works. John Daugman. (http://www.cl.cam.ac.uk/~jgd1000/) 2004
[16]Personal identication in networked society. A.K. Jain,Ruud Bolle,Sharath Pankanti .Biometrics.2002
[17]Caractérisation de la rétine pour la reconnaissance biométrique des personnes .Mémoire de magister. Talib Hichem Betaouaf. Université Aboubakr Belkaid Tlemcen. 2011
[18]Introduction to Biometrics. Anil.K.Jain,Arun.A.Ross,Karthik.Nandakumar. 2011
[19] Handbook of Fingerprint Recognition. Davide.Maltoni, Dario.Maio, Anil.K.Jain, Salil.P. 2nd edition. 2009
[20] Bern Guide to Biometric Reference Systems and Performance Evaluation. Dijana.Petrovska-Delacretaz,Gerard.Chollet. 2009
[21] Etude d'un système complet de reconnaissance d'empreintes digitales pour un capteur microsystème à balayage. Nicolas Galy. Pour obtenir le grade Docteur de l'INPG 14 Avril 2005
[22] Techniques de contrôle d'accès par biométrie. Dossier technique. Juin 2003
[23] Contribution à la reconnaissance d'empreintes digitales par une approche hybride, RIMA BELGUECHI. Mémoire de magister. Université d'I.N.I. 14 Juin 2006
[24]Placement des tâches répétitives sur une architecture régulière embarquée. MOSTEFA MERIEM. Diplôme d'Ingénieur d'Etat. Université d'Oran.2009