Université Mohamed Khider de Biskra
Faculté des Sciences et de la Technologie
Département de génie électrique

MÉMOIRE DE MASTER

Sciences et Technologies
Télécommunications
Réseaux et Télécommunications

Réf. :

Présenté et soutenu par :
Helala Fouad

Le : lundi 25 juin 2018

Identification des personnes par les empreintes digitales

Jury :

Mr	Benakcha Abdelhamid	**MCA**	Université de Biskra	**Président**
Mr	Ouafi abdelkrim	**Pr**	Université de Biskra	**Encadreur**
Mr	Hindaoui Mounira	**MAA**	Université de Biskra	**Examinateur**

Année universitaire : 2017/2018

Dédicaces

***C**'est tout plein de joies que je dédie ce*

modeste travail a ceux qui m'ont été une source d'inspiration et de volonté et encouragement durant toute période de mes études.ma très cher mère.

Mon exemple de vie mon très cher père pour sacrifices

Je dédie également à mes frères Abdeljalil, Younes, Nassim.

Et toutes mes sœurs avec leurs petites familles

Son oublier tous mes amis et amies de département de génieélectrique

Aussi à tous les enseignements de l'université de Biskra.

H. Fouad

Remerciements

Nous tenons à remercier tout d'abord dieu qui a aidé à réaliser ce modeste travail, et pour sa grâce toutes au longue de notre vie professionnelle et personnelle.

Nous remercions chaleureusement notre encadreur monsieur : OuafiAbdelkrim pour son aide, sa disponibilité, son sérieux ainsi que ses encouragements et ses conseils.

Je tiens aussi à remercier :

- *Tous les enseignants de département de génie électrique.*
- *Messieurs, Azzeddine Benlaamoudi, pour sa disponibilité, sa patience, son suivi constant de ce travail.*
- *Sans oublier qui ont contribué de près ou de loin à la réaffirmation de notre travail.*

H. Fouad

Sommaire

Chapitre 3: Résultats et discussion

Résumé

Dans cette décennie, les systèmes de sécurité sont de plus en plus utilisés avec le développement du monde moderne. Il semble qu'ils ont envahi tout, les téléphones mobiles, les maisons, les bureaux et même les magasins. Ils sont devenus la source de l'identification des personnes.

L'objectif principal de cetmémoire est d'étudier comment l'empreinte digitale fonctionne dans ses étapes et comment identifier la personne à travers ses empreintes. Cette caractéristique ou priorités est connue depuis l'antiquité qu'elle est spéciale à chaque personne.

Le système de reconnaissance à base des empreintes digitales, comme tous les systèmes biométriques est composé de trois étapes : prétraitement, extraction des caractéristiques et classification. Dans le cadre de ce mémoire, nous allons détailler ces différentes étapes et les appliquées sur une c1base de données réel.

الملخص

في هذا العقد، يتم استخدام الأنظمة الأمنية بشكل متزايد مع تطور العالم الحديث و يبدو أنهم غزوا كل شيء،الهواتف المحمولة،المنازل،المكاتب، وحتى المتاجر.كما صاروا مصدر التعرف على الأشخاص.

الهدف الرئيسي من هذه المذكرة هو دراسة كيفية عمل البصمة بمراحلها وكيفية التعرف على الشخص من خلال بصمات الأصابع وتعرف هذه الخاصية أو الميزة منذ العصور القديمة أنها خاصة لكل شخص.

يتكون نظام التعرف على بصمات الأصابع ، مثل جميع الأنظمة البيومترية ، من ثلاث خطوات: المعالجة المسبقة ، واستخراج المعالم ، والتصنيف. في سياق هذا ، سوف نفصل هذه الخطوات المختلفة ونطبقها على قاعدة بيانات حقيقية

Introduction générale

La sécurité des systèmes d'information est devenue un domaine de recherche d'une très grande importance.La conception d'un système d'identification fiable, efficace et robuste est une tâche prioritaire.

L'identification de l'individu est essentielle pour assurer la sécurité des systèmes et des organisations. Elle correspond à la recherche de l'identité de la personne qui se présente dans une base de données et peut servir à autoriser l'utilisation des services.

L'exemple de contrôle d'accès à une zone très sécurisée pour laquelle seul un nombre restreint de personnes (enregistrée dans une base de données) y ont accès. Elle peut être également utilisée par la police judiciaire.

En Chine, deux siècles avant JC, l'Empereur Ts-In-She authentifiait certains scellésavec une trace digitale. Cette technique a été appliquée jusqu'au XIXe sièclepar les Chinois mais aussi par les Japonais, notamment lors de la signature descontrats commerciaux.

En 1684, l'Anglais NehemiahGrew est le premier scientifique à écrire un traitédétaillé sur les empreintes digitales et leurs fameuses "innombrables petitesrides". Deux ans plus tard, l'anatomiste italien Marcello Malpighi est le premier àétudier les empreintes digitales sous un microscope [1].

C'est en 1823 que le physiologiste Tchèque, Johannes Purkinje, propose de classer les empreintes digitales en neuf catégories de motifs. Puis, en 1860, l'administrateur britannique aux Indes, William James Herschel,note que "les empreintes digitales sont formées avant la naissance et restentinchangées tout au long de la vie sauf en cas de blessures profondes". Il imaginealors de les utiliser pour signer des chèques.Le docteur Ecossais, Henry Faulds, travaille dans un hôpital japonais et observe que les Japonais et les Chinois authentifient couramment certains documents àl'aide de leur empreinte. Fort de cette observation, il affirme dans une publicationde 1880 que les empreintes sont uniques pour chaque individu.En 1892, l'anthropologue Anglais, Francis Galton, s'appuie sur toutes ces découvertespour décréter que les empreintes permettent l'identification d'un individu [2].

La biométrie s'impose, par excellence, de plus en plus aux yeux des États comme solution sécuritaire. Cependant, l'apparition de biométrie n'est plus récente, elle remonte au 19ème siècle. Au début de son apparition, cette biométrie a été appelée anthropométrie. Pour un besoin policier et pour une reconnaissance des criminelles, les empreintes digitales étaient parmi les premières biométries utilisées.

Ainsi, à cause de l'efficacité de la biométrie basée empreinte digitale, cette utilisation policière n'a jamais été abandonnée. La biométrie souffre d'ailleurs un peu de cette image policière et a du mal à se faire accepter par le grand public pour d'autres types d'applications.

Cependant, la biométrie n'est plus limitée aux empreintes digitales et à l'identification biométrique de personne. De nombreuses modalités sont aujourd'hui inventées pour des applications biométriques. On peut citer des modalités physiologiques comme : le visage, la voix, l'iris, la rétine, la forme de la main et d'autres comportementales comme : la frappe de clavier. Toute cette variété de modalités biométriques a donné naissance à divers produits commerciaux intégrant des systèmes biométriques, [3].

La biométrie, qui consiste àidentifier un individu à partir de ses caractéristiques physiques ou comportementales, connait depuis quelques années un renouveau spectaculairedans la communauté du traitement du signal. Elle a aussireçu une attention accrue de la part des medias depuis lestragiques événements du 11 septembre 2001.

Dans cemémoirenous introduisons tout d'abord la notion de biométrie.Nous décrivons l'architecture d'un système biométrique ainsi que les métriques utilisées pour évaluer leur performance.Nous donnons un bref aperçu des technologies biométriquesles plus courantes. Nous présentons enfin lesapplications possibles de la biométriepermettant d'identifier et d'authentifier une personne sur la base d'un ensemble de données reconnaissables et vérifiables, uniques et spécifiques à celles-ci.Le reste du mémoire est organisé comme suit :

- **Le chapitre1** ***:*** Dans ce chapitre, nous allons suivre l'évolution de lareconnaissance biométrique, mettre le point sur le concept et les bases de la reconnaissance automatique ainsi que sur les différentes modalités et une étude détaillée d'un système biométrique sera dressée avec sesdomaines d'application.
- **Le chapitre2*:*** Nous présentons l'empreinte digitale comme modalité biométrique, et ses caractéristiques exploitées dans les différents types de reconnaissance ainsi que le processus général de sa reconnaissance. On exposera aussi les méthodes utilisées pour le prétraitement, l'extraction des caractéristiques, et la classification desdonnées.
- **Le chapitre 3*:*** dansCe chapitre, nous donnons le principe de notre système de reconnaissance des empreinte digitales, les bases de données utilisées et les résultats obtenus ainsi que des discussions.

Chapitre 1 : Généralités Sur la Biométrie

1.1 Introduction

Devant la croissance exponentielle des communications tant physiques que virtuelles et les risques que cela peut représenter, il est apparu nécessaire de contrôler l'identité des acteurs de ces échanges. La biométrie permet de vérifier que l'usager est bien la personne qu'il prétend être. C'est une technologie qui utilise les caractéristiques physiques propres à chaque individu pour établir de façon aussi fiable que possible son identité. Jouissant actuellement d'un certain engouement dû, sans doute, aux différents gadgets d'identification que l'on a pu voir dans certaines productions cinématographiques, la biométrie tend à envahir notre quotidien. Devant cette déferlante, il était nécessaire de faire le point sur ce qu'est exactement la biométrie, quelles techniques existent vraiment et leur degré de fiabilité pour ensuite détailler les plus utilisées. [4,5]

1.2 Définition de la biométrie :

Le terme "biométrie" provient des mots grecs, « bios » qui veut dire la vie et du mot « métrique » qui veut dire mesure. La biométrie englobe les technologies utilisées pour mesurer et analyser les caractéristiques uniques d'une personne. Il existe deux types de biométrie: comportementales et physiques. La biométrie comportementale est généralement utilisée pour la vérification alors que la biométrie physique peut être utilisée soit pour l'identification ou la vérification. [6]

La biométrie peut être définie comme étant "la reconnaissance automatique d'unepersonne en utilisant des traits distinctifs". Une autre définition de la biométrie est "toutescaractéristiques physiques ou traits personnels automatiquement mesurables, robustes etdistinctives qui peuvent être utilisées pour identifier un individu ou pour vérifier l'identitéprétendue d'un individu"[7]

La biométrie s'invite progressivement dans notre vie quotidienne, elle fait partie des grands enjeux pour un monde plus sûr. Le marché des produits d'authentification et d'identification est en pleinecroissance, dû à la nécessité croissante du besoin de sécurité de chacun, dans les domaines privé, professionnel ou public.

La biométrie est de plus en plus utilisée pour les titres d'identité, dans les aéroports, les établissements pénitentiaires, l'accès à des locaux sécurisés, le vote électronique, la sécurité des paiements bancaires ou des transactions via Internet.

La biométrie est une alternative aux mots de passe et autres identifiants pour supprimer le doute sur l'identité. Elle permet de vérifier que l'usager est bien la personne qu'il prétend être.

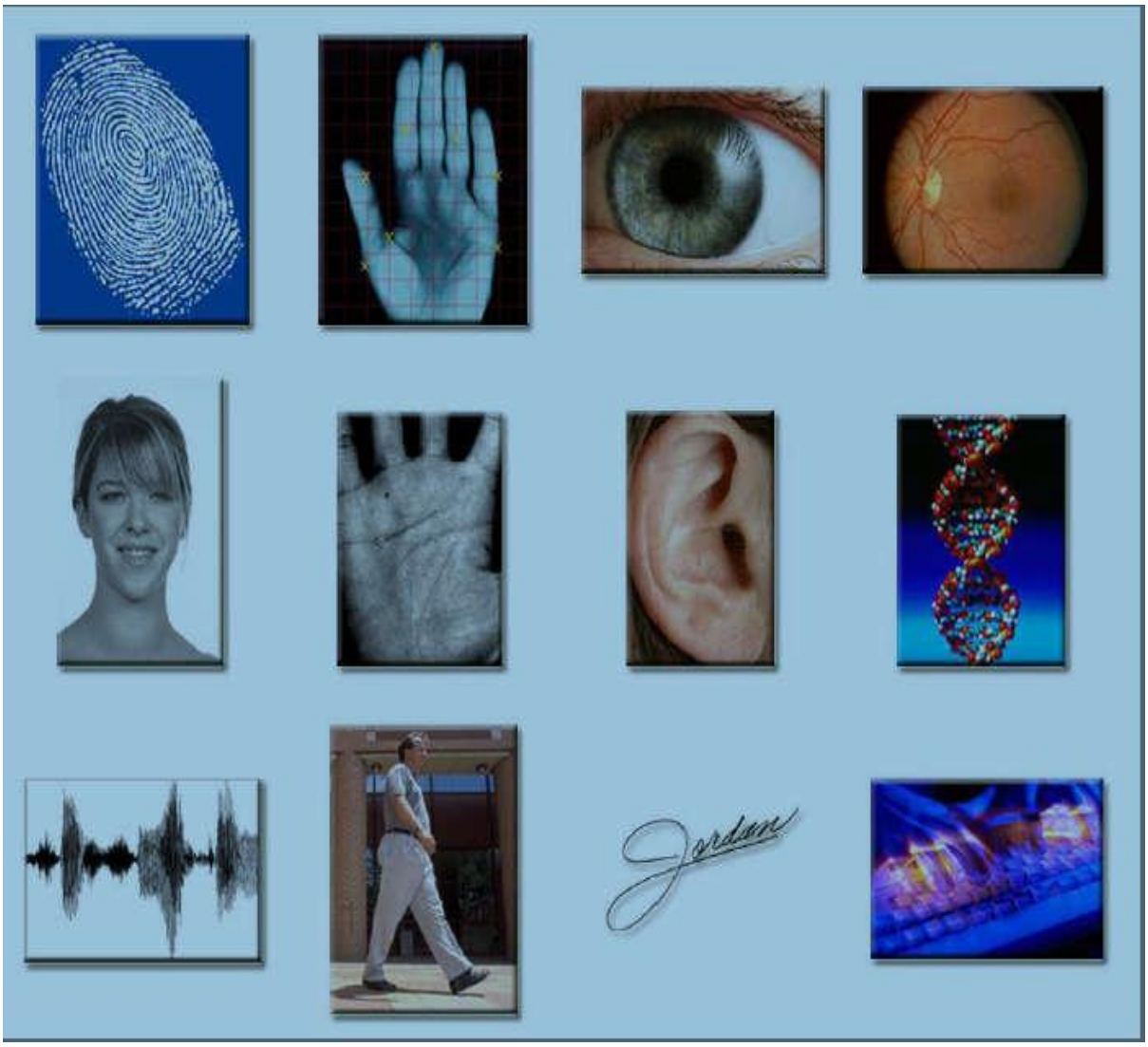


Figure 1.1 : Différentes modalités biométriques

C'est une technologie établie, avec plusieurs technologies (figure 1.1): empreintes digitales, visage 2D, Visage 3D, iris, rétine, voix, réseau veineux, forme de la main, comportemental (signature dynamique, frappe au clavier, navigation sur une tablette ou smartphone, façon de marcher).

Pour un système d'authentification encore plus robuste, on peut associer simultanément plusieurs méthodes biométriques (multimodale).

Les applications biométriques sont généralement associées à d'autres technologies de sécurité comme la carte à puce, le cryptage, l'anonymat des données stockées...etc, avec comme caractéristiques, [8] :

- **Sécurité** - Diminuer les tentatives de fraude. Supprimer le doute sur l'identité.
- **Confiance** - Augmente la confiance envers les systèmes, pour l'administrateur et pour l'utilisateur.
- **Facilité** - Satisfaction des utilisateurs grâce à la simplicité, d'utilisation et à l'élimination des contraintes.
- **Économie** - Réduction des coûts d'exploitation grâce à l'automatisation du processus d'identification [8].

1.3 Principaux modalités biométriques :

Il existe plusieurs modalités biométriques utilisées dans divers secteurs. On peut distinguer trois catégories (figure 1.2):

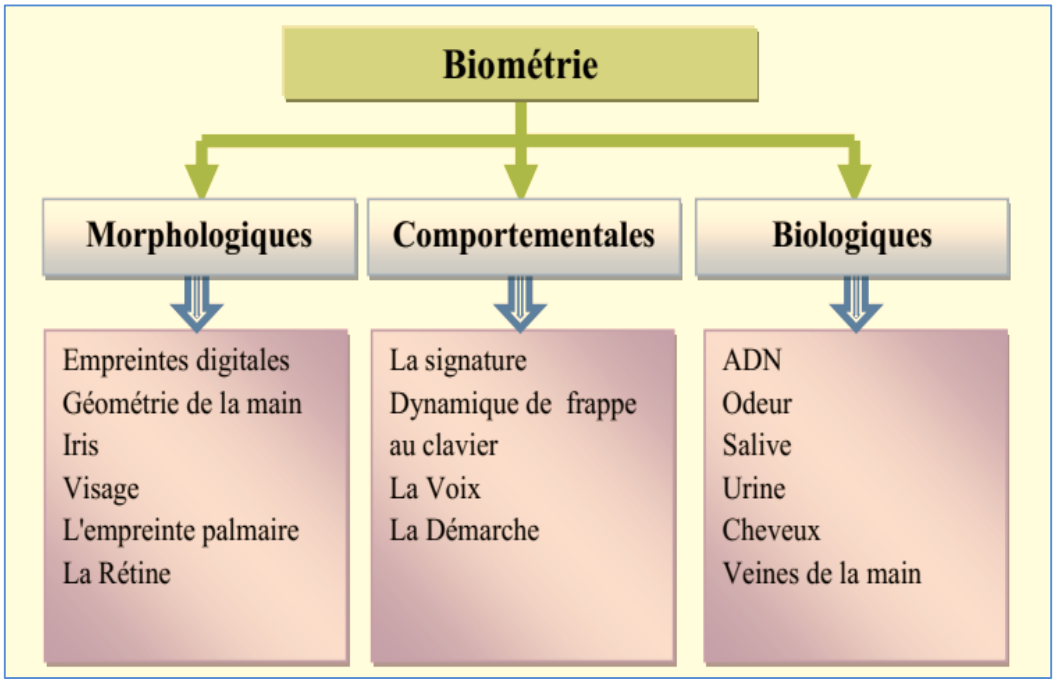


Figure 1.2 : Classification d'un certain nombre de modalités biométriques

1.4. Techniques biométriques :

Il existe plusieurs techniques biométriques utilisées dans plusieurs applications et secteurs, on peut en distinguer deux catégories :

1.4.Analyse morphologique (physiologique)

Elle est basée sur l'identification de traits physiques particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe l'iris de l'œil, le réseau veineux de la rétine la forme de la main, la cartographie thermique, les empreintes digitales, les traits du visage, les veines de la main, etc.

a) Reconnaissance de visage

On peut identifier un individu en fonction de ses caractéristiques faciales en effectuant des mesures: écartement des yeux, arêtes du nez, commissures des lèvres, oreilles, menton. Ces différentes caractéristiques sont analysées par les systèmes de reconnaissance faciale et comparées à une base de données existante. Cette méthode permet d'identifier une personne ou de vérifier une identité, [9].

Figure1.3: La Reconnaissance de visage

b) Empreintes digitales

Le procédé de reconnaissance anthropométrique le plus ancien, bien connu du grand public, est l'analyse des empreintes digitales, ce qui explique aujourd'hui son importance parmi les nombreux procédés d'identification sur la base de caractères physiologiques [10].

L'empreinte digitale est la caractéristique d'un doigt. On le croit que chaque empreinte digitale est unique. Chaque personne a ses propres empreintes digitales avec l'unicité permanente. Ainsi les empreintes digitales sont utilisées depuis longtemps pour l'identification et l'investigation juridique. Une empreinte digitale se compose de beaucoup

des rides et sillons. Ces rides et sillons présentent de bonnes similitudes dans chaque petite fenêtre locale [11].

Figure 1.4 : La reconnaissance de l'empreinte digitale

c) Géométrie de la main

Il consiste à mesurer plusieurs caractéristiques de la main (jusqu'à 90) telle que la forme de la main, longueur et largeur des doigts, formes des articulations, longueurs inter articulations, …etc. La technologie associée à cela est principalement de l'imagerie infrarouge.

Cette biométrie est Simple à mettre en œuvre, peu intrusive, cette technologie est appréciée des utilisateurs. Les images numérisées sont peu volumineuses, comparée à celles de l'empreinte digitale (10 à 20 octets contre 250 à 1000 octets).

La forme de la main est moins stable dans le temps que les empreintes digitales. Des déformations importantes des doigts peuvent en effet survenir avec l'âge. Le scanner est plus encombrant que pour les empreintes digitales, ce qui rend la technologie inaccessible aux systèmes portatifs [12].

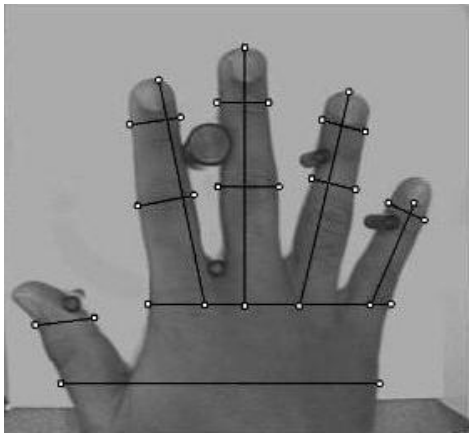


Figure 1.5 : Géométrie de la main

d) Œil

L'iris et la rétine de l'œil peuvent être utilisés pour la biométrie.

d.1Iris, est le disque coloré de la partie antérieure de l'œil, ne change pas après l'adolescence. Il comprend de très nombreux motifs distinctifs qui permettent d'affirmer son unicité. La texture de l'iris, avec ses crêtes et ses sillons, peut être facilement encodée pour comparaison. C'est un des procédés les plus fiables, car la fraude est très difficile : une copie de l'iris, présentée devant un lecteur, serait immédiatement décelée en raison de l'absence d'oscillation du diamètre de la pupille [13].

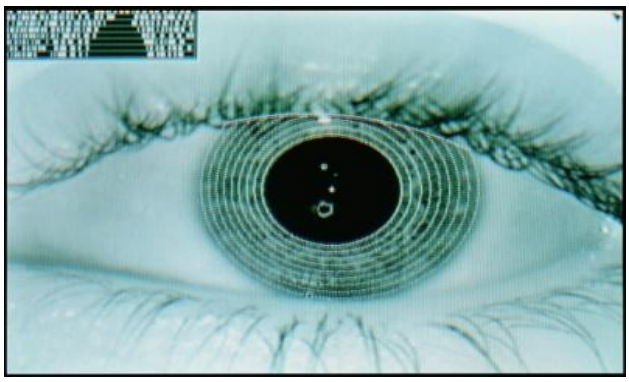


Figure 1.6 : L'iris

d.2 Rétine, c'est la membrane tapissant le fond de l'œil, est sans doute l'un des modes d'identification les plus précis. La carte rétinienne est tapissée de très nombreux vaisseaux sanguins. Elle est mise en évidence par éclairage, obligeant la personne à placer son œil très près du capteur, ce qui n'est pas le cas pour l'iris. C'est pourquoi, cette méthode est principalement employée pour les animaux (traçabilité des bovins, par exemple) [13].

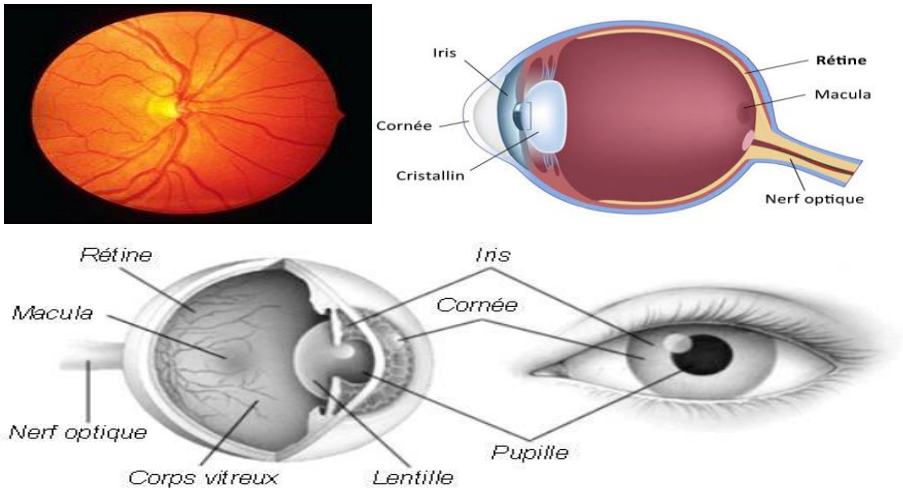


Figure 1.7 : La Rétine

1.4.2. Analyse comportementale :

Elle se base sur l'analyse de certains comportements d'une personne. Cette catégorie regroupe la reconnaissance vocale, la dynamique de frappe au clavier, la dynamique de la signature, l'analyse de la démarche, etc. Il existe, par ailleurs, une autre catégorie qui est l'étude des traces biologiques telles que : l'ADN, le sang, la salive, l'urine, l'odeur, …etc. [14].

a) **Signature**

Signer un document pour s'identifier est un geste naturel. Chaque personne a un style d'écriture unique. On peut donc définir, à partir de la signature d'une personne, un modèle qui pourra être employé pour effectuer une identification. De plus, elle est utilisée dans beaucoup de pays comme élément juridique ou administratif.

Figure 1.8: La signature

b) **Reconnaissance vocale**

Les données utilisées par la reconnaissance vocale proviennent à la fois des facteurs physiologiques (la sexe, l'âge, la tonalité, la fréquence, l'accent, l'harmonie,.....etc.) et comportementaux(la vitesse, le rythme,...etc.)

L'identification de la voix est considérée par les utilisateurs comme une des formes les plus normales de la technologie biométrique car elle n'est pas intrusive et n'exige aucun contact physique avec le lecteur du système.

Figure 1.9 : La reconnaissance vocale

c) **Frappe du 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 « SoftwareOnly ». Elle est appliquée au mot de passe qui devient ainsi beaucoup plus difficile à « imiter ». Lors de la mise en place de cette technique, il est demandé à l'utilisateur de saisir son mot de passe une dizaine de fois de suite.
A l'aide d'un algorithme qui exploite le temps d'appui sur chaque touche et le temps entre chaque touche, la dizaine de saisie est « moyennée » pour bâtir un Profil de frappe de l'utilisateur qui servira de référence.
Aux accès suivants, en suivant la même approche, la saisie du mot de passe donnera sera couplée à un profil de frappe qui sera comparé au profil de référence.
Le droit d'accès est alors accordé en fonction du niveau de ressemblance de ce profil avec la référence. Suivant le degré de filtrage qu'un administrateur aura défini, cet accès sera plus ou moins difficile [15].

Figure 1.10 : image de de frappe au clavier

d) **Démarche**

Après le développement des biométries, la recherche approfondit l'utilisation de la biométrie en créant un système de reconnaissance basé sur la silhouette d'un individu et sa façon de marcher.
Il s'agit de reconnaître un individu par sa façon de marcher et de bouger (vitesse, accélération, mouvements du corps…), en analysant des séquences d'images. La démarche serait en effet étroitement associée à la musculature naturelle et donc très personnelle, mais des vêtements amples, par exemple, peuvent compromettre une bonne identification [16].
Les paramètres communs de l'analyse de la marche sont:

- Paramètres cinématiques tels que le genou, les mouvements de la cheville et les angles
- Paramètres spatiotemporels tels que la longueur et la largeur des marches, la vitesse de marche [17].

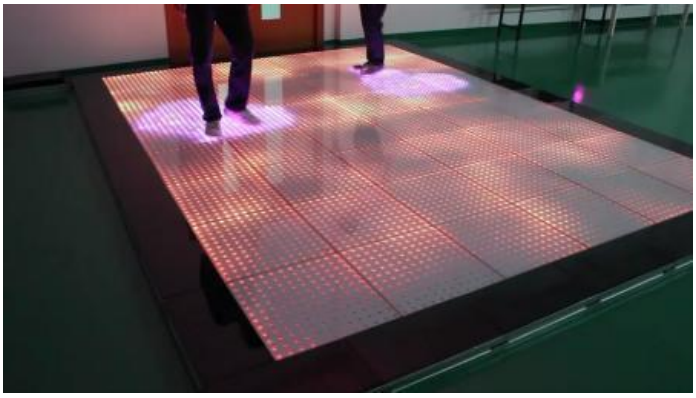


Figure1.11 : la démarche (capteur de sol)

1.4.3. Analyse biologique :

Elle est basée sur l'identification de traits biologiques particuliers.

a) ADN

L'empreinte génétique est la marque biologique la plus sure du monde. Dans le cas des tests de paternité, on atteint une fiabilité de 99,999%. Mais les analyses d'ADN nécessitent des délais de plusieurs semaines, ce qui interdit toutes les applications d'identification en temps réel [18].

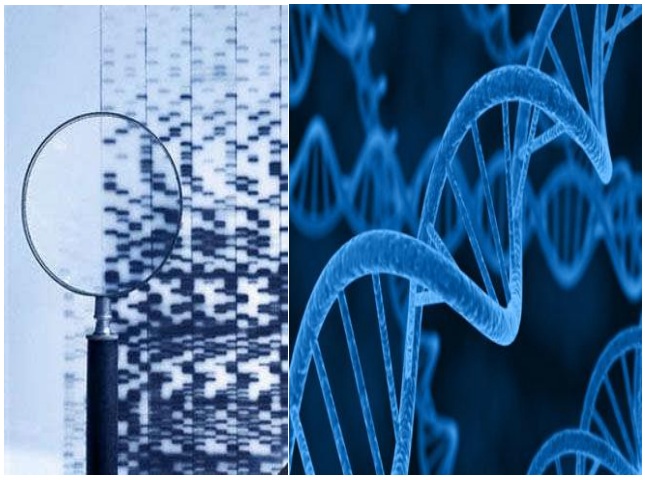


Figure 1.12 : L'ADN

b) Veines de la main

On a longtemps considéré que le modèle des veines dans l'anatomie humaine peut être unique aux individus. Le sang chargé en oxygène arrive dans les mains par les artères, puis repart vers le cœur par les veines. Le sang appauvri en oxygène n'a pas le même filtre d'absorption que le sang artériel : il absorbe la lumière à des longueurs d'onde proches de l'infrarouge (autour de 760 micromètres).

Quand la main est éclairée avec une lumière infrarouge, le réseau veineux apparaît en noir. Il est enregistré sous forme de "carte d'identité" dans une base de données, et pourra ensuite servir de comparaison lors de l'authentification [16].

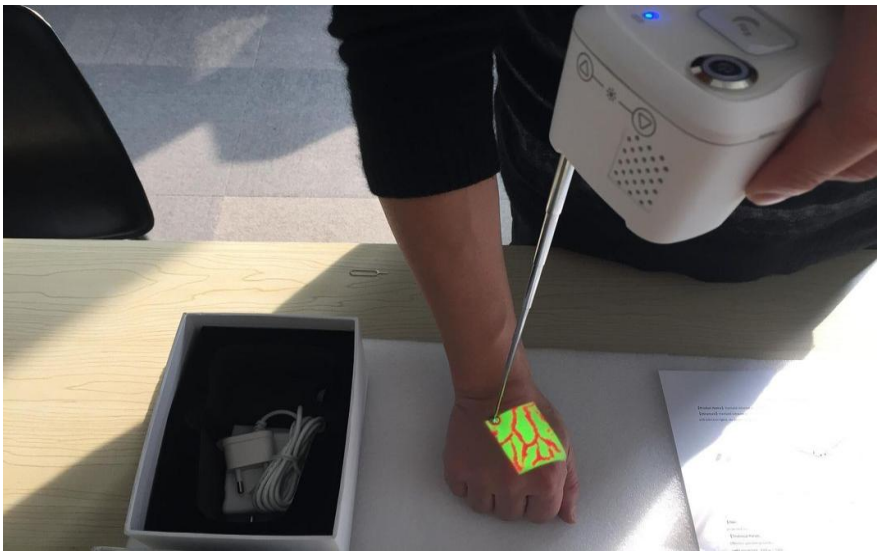


Figure 1.13 : Image de système configuration des veines

1.4.4. Modalité expérimental :

a) Cartographie thermique

Un cliché infrarouge du visage ou d'un membre (main, doigt) est réalisé par une caméra thermique. Il permet de mettre en évidence la répartition de chaleur qui caractérise chaque personne ou le réseau veineux de son visage. Ce système est encore expérimental [13].

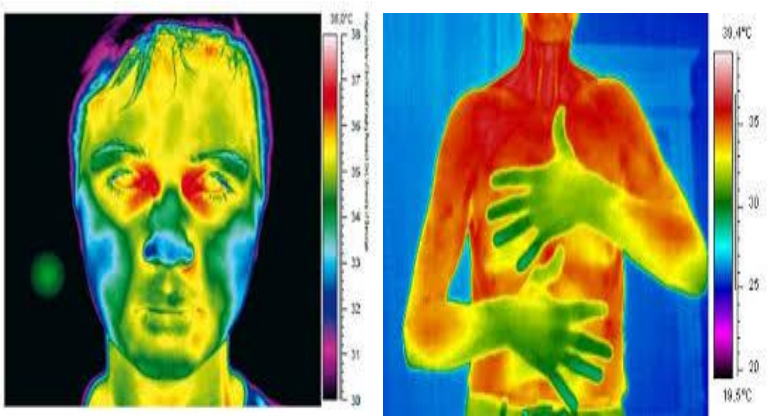


Figure 1.14Cartographie thermique de visage d'un homme - Thermographie infrarouge

1.5- Comparaison entre quelques Techniques Biométriques:

Techniques	avantages	inconvenants

Géométrique de main	-Très ergonomique -bonne acceptabilité	-Système coûteux et encombrant -perturbation possible par des blessures
L'empreinte digitale	-coût -ergonomie moyenne	- acceptabilité moyenne -possibilité d'attaque
La rétine	-fiabilité -pérennité	-acceptabilité très faible -contrainte d'éclairage
La voix	-facilité	-facile et falsifier (vulnérables aux attaques)
Le visage	-coût -bonne acceptabilité	-jumeaux, déguisement vulnérabilité aux attaques (faciles et falsifier)
L'iris	-fiabilité	-acceptabilité très faible -contrainte d'éclairage
La signature	-ergonomie	-dépendant de l'état émotionnel de la personne peu fiable
La frappe du clavier	-ergonomie	-dépendant de l'état physique de la personne peu fiable

1.6. Système biométrique :

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

Un système biométrique peut avoir deux modes opératoires [19] :

1.6.1. Authentification biométrique : est le processus consistant à comparer les données des caractéristiques de la personne au «modèle» biométrique de cette personne afin de déterminer la ressemblance. Le modèle de référence est le premier enregistré dans une base de données ou un élément portable sécurisé comme une carte à puce. Les données stockées sont ensuite comparées aux données biométriques de la personne à authentifier. Ici, c'est l'identité de la personne qui est vérifiée. Dans ce mode, la question posée est: "Êtes-vous en effet Monsieur ou Madame X?"[20]

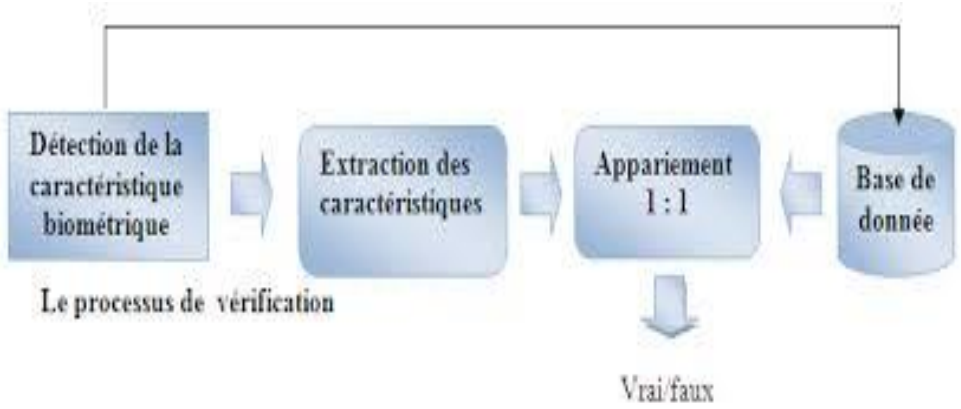


Figure1.15. Schéma d'authentification biométrique

1.6.2. Identification biométrique consiste à déterminer l'identité d'une personne. L'objectif est de capturer un élément de données biométriques de cette personne. Cela peut être une photo de son visage, un enregistrement de sa voix ou une image de son empreinte digitale. Ces données sont ensuite comparées aux données biométriques de plusieurs autres personnes conservées dans une base de données. Dans ce mode, la question est simple: "Qui es-tu?" [20]

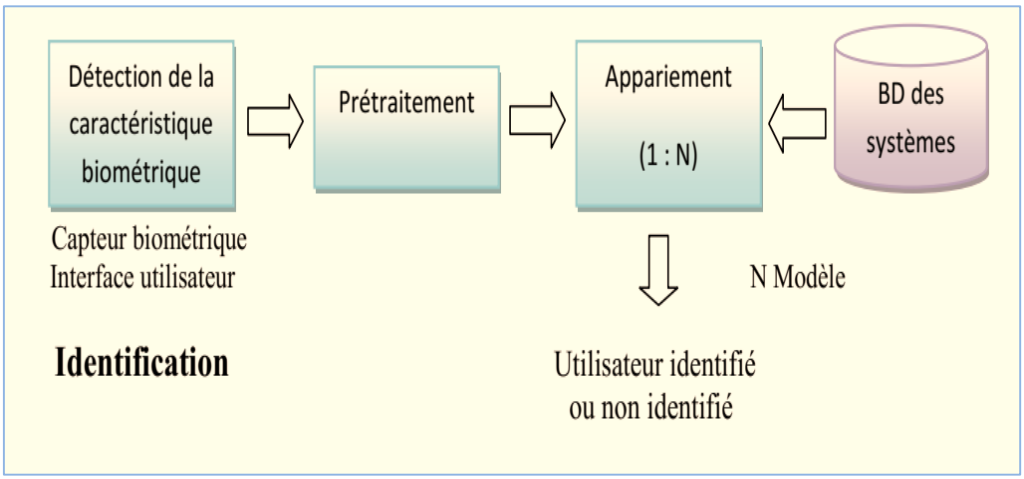


Figure1.15. Schéma d'identification biométrique

1.7. Conclusion

La biométrie est un ensemble des technologies (appelées les technologies biométriques) qui exploitent des caractéristiques humaines physiques ou comportementales telles que l'empreinte digitale, la signature, l'iris, la voix, le visage, la démarche, et un geste de main pour différencier des personnes.

Ces caractéristiques sont traitées par certains ordres des processus automatisés à l'aide des dispositifs comme des modules de balayage ou des appareils-photo. À la différence des mots de passe ou des PINs (numéros d'identification personnelle) qui sont facilement oubliés ou exposés à l'utilisation frauduleuse, ou des clefs ou des cartes magnétiques qui doivent être portées par l'individu et sont faciles à être volées, copiées ou perdues, ces caractéristiquesbiométriques sont uniques à l'individu et il y a peu de possibilités que d'autres individus puissentremplacer ces caractéristiques, donc les technologies biométriques sont considérées les plus puissantesen termes de sécurité.

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 nes'accompagne d'une atteinte généralisée à la vie privée des individus. Tout d'abord lemanque de fiabilité des systèmes biométriques inquiète.

Même si aujourd'hui les passagers sont prêts à faire des concessions pourgarantir leur sécurité, ils accepteront sans doute très mal ces erreurs à répétition. Et bienque des progrès constants soient enregistrés séparément pour chaque modalité, laperformance des systèmes à un seul mode est encore loin d'être satisfaisante ce quiplaide en faveur du développement de systèmes biométriques multimodaux [21].

Chapitre 02 :

Les systèmes d'identification des empreintes digitales

2.1. 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 [22].

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 ses caractéristiques.

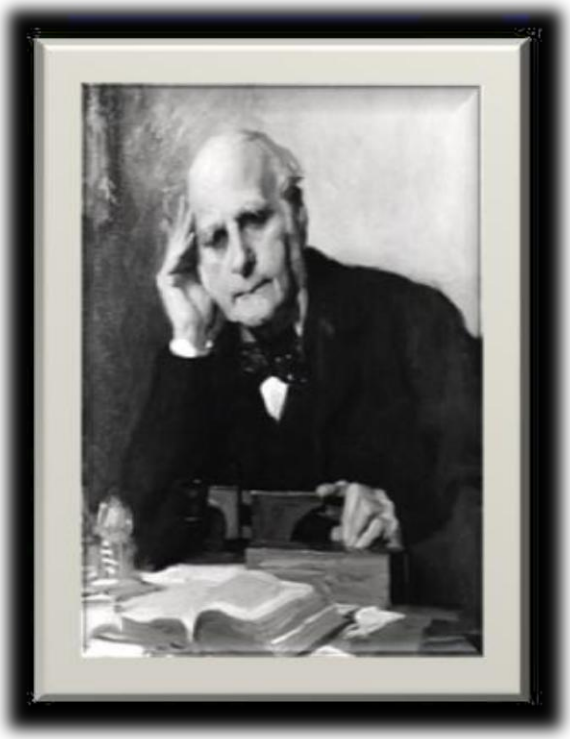


Figure 2.1 : Francis Galton.

L'empreinte digitale est l'une des techniques les plus connues du grand public. C'est grâce aux travaux d'Alphonse Bertillon, dans les années 1880, que l'on a commencé à pouvoir identifier des récidivistes sans avoir recours au marquage ou à la mutilation. L'idée d'en faire un instrument d'identification à part entière s'est imposée avec les recherches du Britannique Galton, qui démontra la permanence du dessin de la naissance à la mort, son inaltérabilité et son individualité.

La donnée de base dans le cas des empreintes digitales est le dessin représenté par les crêtes et sillons de l'épiderme. Ce dessin est unique et différent pour chaque individu. En

pratique, il est quasiment impossible d'utiliser toutes les informations fournies par ce dessin (car trop nombreuses pour chaque individu), on préférera donc en extraire les caractéristiques principales telles que les bifurcations de crêtes, les "îles", les lignes qui disparaissent, etc. Une empreinte complète contient enmoyenne une centaine de ces points caractéristiques (les "minuties"). Si l'on considère la zone réellement scannée, on peut extraire environ 40 de ces points. Pourtant, là encore, les produits proposés sur le marché ne se basent que sur une quinzaine de ces points (12 au minimum vis-à-vis de la loi), voire moins pour beaucoup d'entre eux (jusqu'à 8 minimum). Pour l'histoire, le nombre 12 provient de la règle des 12 points selon laquelle il est statistiquement impossible de trouver 2 individus présentant les mêmes 12 points caractéristiques, même en considérant une population de plusieurs dizaines de millions de personnes.

Les techniques utilisées pour la mesure sont diverses : capteurs optiques (camérasCCD/CMOS), capteurs ultrasoniques, capteurs de champ électrique, de capacité, de température...etc. Ces capteurs sont souvent doublés d'une mesure visant à établir la validité de l'échantillon soumis (autrement dit, qu'il s'agit bien d'un doigt) : mesure de la constante diélectrique relative de l'échantillon, sa conductivité, les battements de cœur, la pression sanguine, voire une mesure de l'empreinte sous l'épiderme.

2.2. Introduction :

La reconnaissance d'empreintes digitales fait partie du domaine de la biométrie. Cette méthode peut être utilisée dans plusieurs domaines tels que l'identification de personnes pour des raisons de sécurité [23].

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

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

Les techniques d'appariement des empreintes digitales peuvent être classées en deux catégories : les techniques basées sur la détection locale des minuties et les techniques basées sur la corrélation. L'approche basée sur les minuties consiste à trouver d'abord les points de minuties puis trace leurs emplacements sur l'image du doigt (**figure 2.2**). La figure suivante représente les étapes de l'extraction et de comparaison des caractéristiques d'empreinte (prétraitement, extraction, classification…).

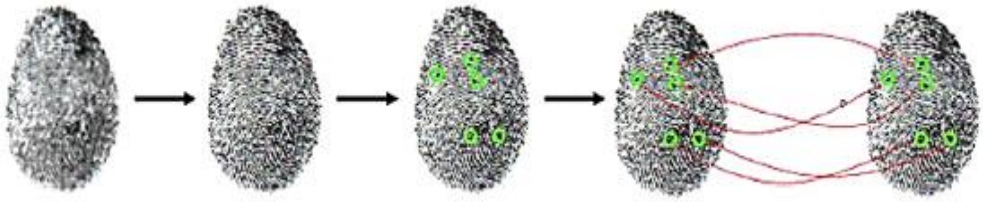


Figure 2.2. Le processus de reconnaissance par empreinte digitale.

Cependant, il y a quelques difficultés avec cette approche lorsque l'image d'empreinte digitale est d'une qualité médiocre, car l'extraction précise des points de minutie est difficile. Cette méthode ne tient pas en compte la structure globale de crêtes et de sillons. Les méthodes basées sur la corrélation sont capables de surmonter les problèmes de l'approche fondée sur les minuties. Ces méthodes utilisent la structure globale de l'empreinte, mais les résultats sont moins précis qu'avec les minuties. De plus, les techniques de corrélations sont affectées par la translation et rotation de l'image de l'empreinte. C'est pour cela que les deux approches sont en général combinées pour augmenter les performances du système [24].

2.3. Empreinte digitale

Dans ce contexte, nous donnerons une définition de l'empreinte digitale et nous montrons aussi comment cela fonctionne.

2.3.1. Définition d'une empreinte digitale

Les empreintes digitales sont les marques laissées par les sillons des pulpes. Le dessin qu'elles forment est propre à chacun d'entre nous, ce qui explique pourquoi les empreintes digitales servent à l'identification des personnes (figure 2.2).

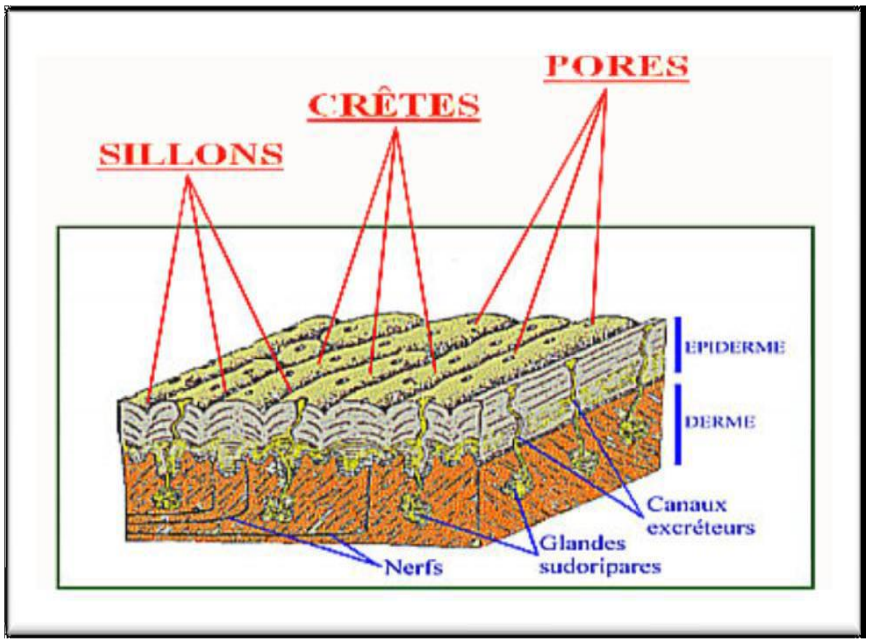


Figure 2.2 : Dessin d'une Empreinte.

2.3.2 Points caractéristiques de l'empreinte digitale :

Les éléments qui permettent de différencier deux empreintes digitales ayant le même motif sont :

a) **Points singuliers globaux**

Centre (le core) : c'est le noyau, est un courbure maximale de lignes dans le centre de l'empreinte. Lieu de convergences des stries.

Delta:S'il y a deux lignes différentes, où les lignes sont différentes, On le voit à l'œil en forme de triangle. Lieu de divergences des stries.(Voir la figure 2.3).

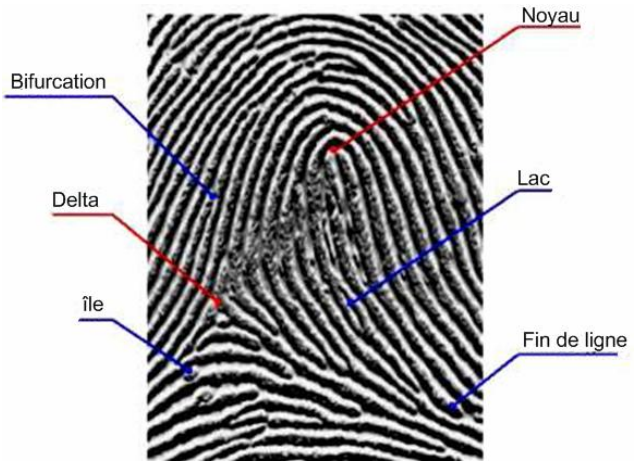


Figure 2.3 : points singuliers globaux

b) **Points singuliers locaux**

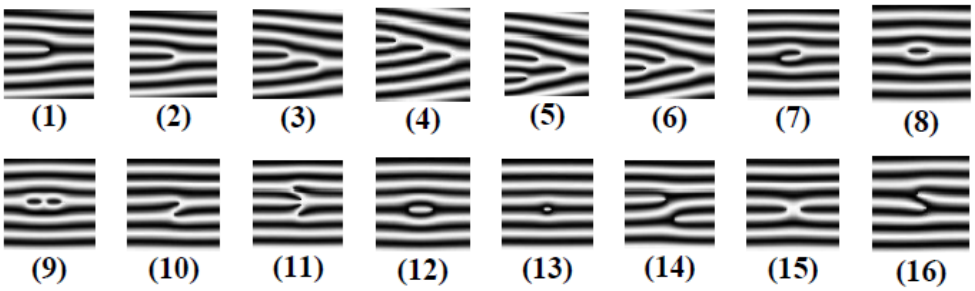
Minuties : points d'irrégularité se trouvant sur les lignes capillaires. On peut relever jusqu'à seize types de minuties mais dans les algorithmes on n'en retient que quatre types:

- Terminaison à droite ou à gauche (minutie située en fin de strie).
- Bifurcation à droite ou à gauche (intersection de deux stries).

On peut citer également :

- île : assimilée à deux terminaisons.
- Lac: assimilée à deux bifurcations.

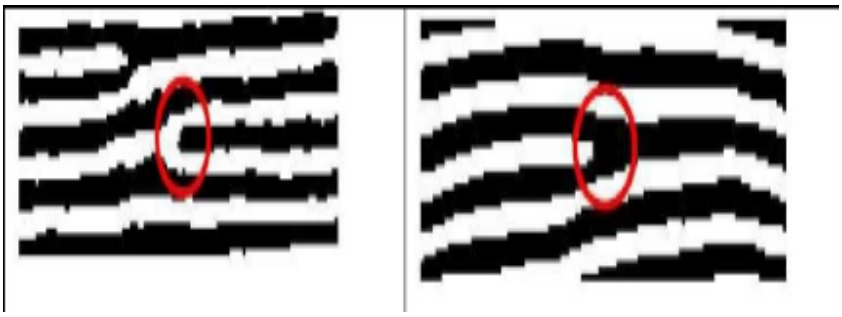
(voir la figure 2.4)



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

Fig2.4: Les différents types de minuties

Les bifurcations et les terminaisons sont les deux types de minuties les plus utilisés parce que ils sont facilement détectables (voir figure2.5)



a : Terminaison. ***b : Bifurcation.***

Fig2.5. La terminaison et la bifurcation

2.4. Architecture d'un système biométrique basé sur l'empreinte :

Le système biométrique sa fonctionne en deux étapes (figure 2.6) :

Apprentissage (Enrôlement) :à cette étape, nous traitons l'empreinte digitale contenus dans la base de données pour extraire les données et les caractéristiques de chaque empreinte digitale, puis l'enregistrer pour la comparer ultérieurement**.**

Test : à cette étape aussi, nous traitons l'empreinte de la personne à identifier ou à vérifier ensuite nous extrayons les données et les propriétés de cette empreinte. On compare ensuite l'empreinte que nous avons mise en place et les empreintesstockée dans la base de données. On arrive ainsi à une correspondance entre deux signatures à savoir que la personne proclamée soit identifiée ou non ou puisse passer ou non.

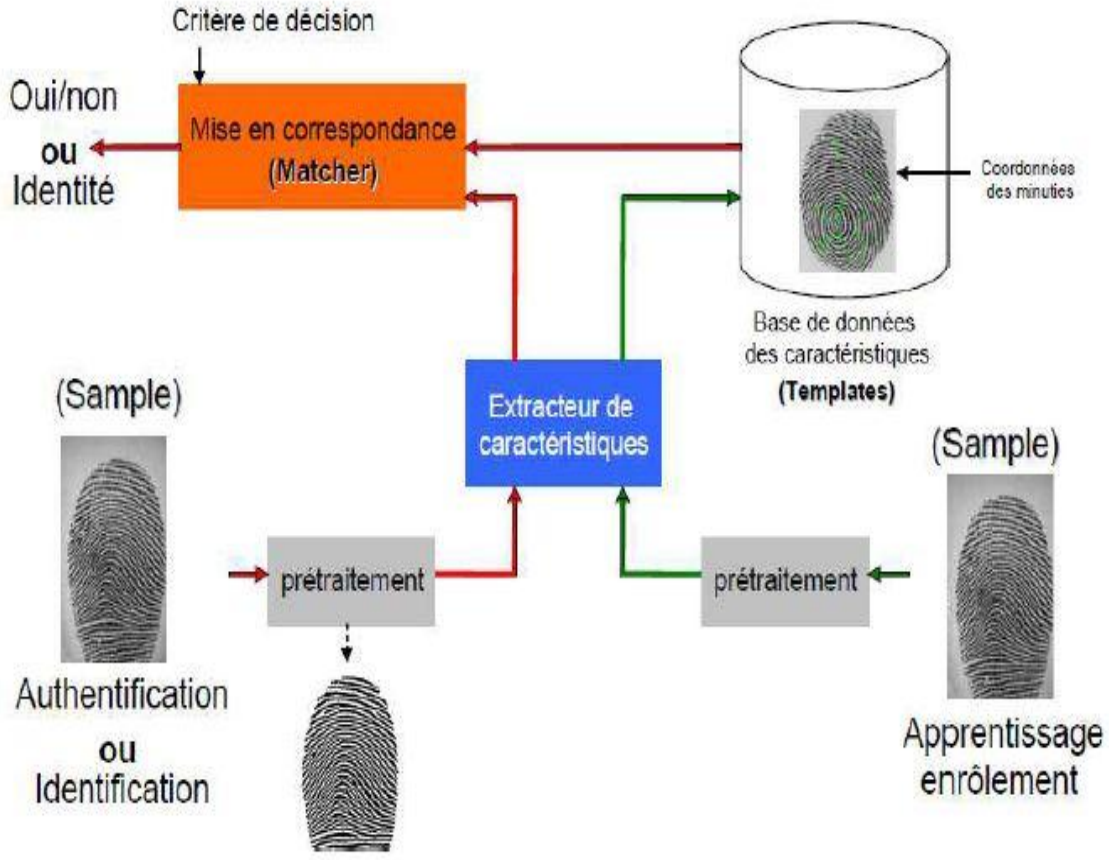


Fig2.6.Architecture d'un système biométrique basé sur l'empreinte

2.5. Méthodes de prétraitement d'empreinte digitale

Il existe plusieurs façons de traiter l'image d'une empreinte digitale. Nous allons présenter quelques-uns :

2.5.1. Conversion en niveaux de gris

L'image en niveaux de gris est une image de profondeur k=8 bits (figure 2.7). Alors ; chaque pixelprendre l'une des valeurs entre de l'intervalle [0 …..255], tel que le Noir représenter par le (0) et le Blanc représenter par (255).Dans les applications professionnelles 8 bits n'est pas suffisants, donc il ya d'autre type d'image de niveaux de gris de profondeur k=14 bits ou k=16 bits.

a : L'empreinte originale. b: L'empreinte en gris.

Fig2.7. Conversion Niveaux de gris

2.5.2. Seuillage (Binaraisation)

Dans cette étape, l'image est convertie en une image binaire à travers un processus de seuillage ou une méthode de binarisation adaptative (figure 2.8). Le but est le repérage des crêtes. Cette étape est aussi appelée dans la littérature **segmentation.** Toutefois, cela ne doit pas se confondre avec la segmentation de l'image entre région d'intérêt de fond lors de la génération du masquage des régions.

A)Image en niveaux de gris B) image Binarisée.

Fig2.8.Binarisation

2.5.3. 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. La squelettisation doit être faite sur une image binaire [25].Dans l'image binaire (noir et blanc), les lignes se voient clairement mais elles ont des tailles différentes. Pour pouvoir détecter rapidement les minuties (terminaisons, bifurcations), il est nécessaire d'obtenir une image plus schématique de l'empreinte, dans laquelle toutes les lignes ont la même épaisseur (1 pixel) comme le montre la figure 2.9.

Figure 2.9.Squelettisation de l'empreinte digitale.

2.6. Extraction de minuties

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

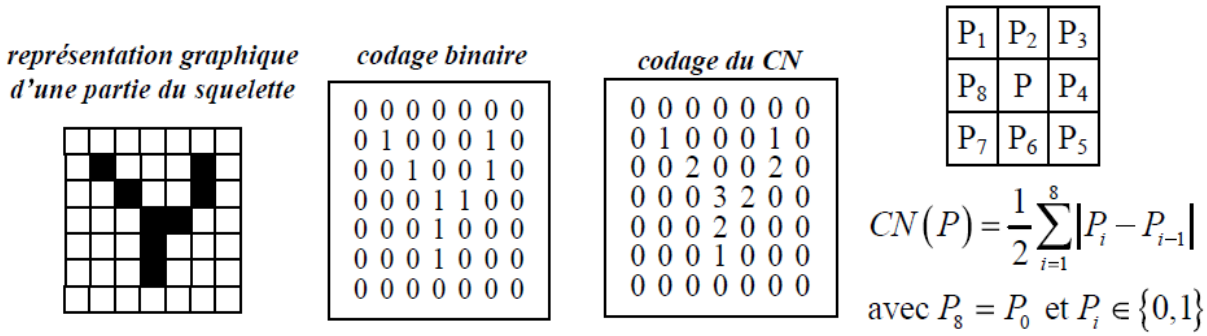


Figure 2.10. Calcule de minutie

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

- *CN(P)=0* : dans ce cas il s'agit d'un pixel isolé et nous n'en tenons pas compte car même si ce type de minutie existe il est très rare et à ce stade du traitement de l'image il est probablement du à un résidu de bruit.

- *CN(P)=1* : dans ce cas nous avons à faire à une minutie de type *terminaison.*

- *CN(P)=2 :* c'est le cas le plus courant, le pixel se situe sur une strie, il n'y a pas de minutie.

- *CN(P)=3 :* nous sommes en présence d'une *bifurcation* triple.

- *CN(P)=4 :* nous sommes en présence d'une *bifurcation* quadruple. Ce type de minutie étant assez rare il est probablement du à du bruit et nous l'ignorons.

La figure suivante (figure 2.11) illustre un exemple sur la détermination du type de minutie en fonction du calcul de *CN*

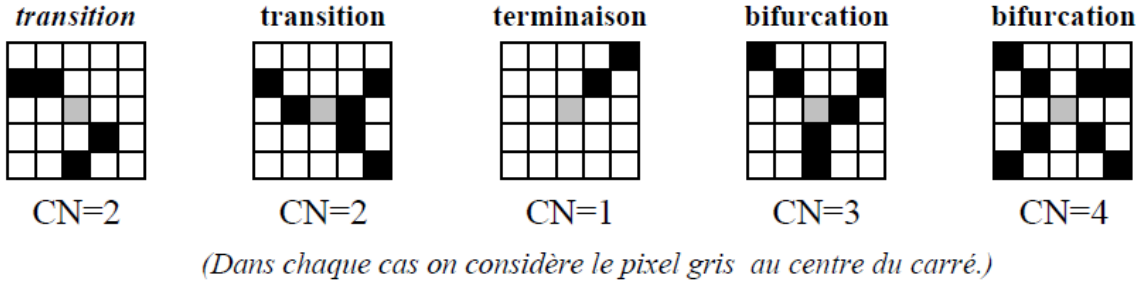


Figure 2.10. La reconnaissance du type de minutie à partir de CN

2.7. Classification

a) **Algorithme d'apprentissage (SVM mono classe)**

Le modèle de décision global obtenu contient en plus des paramètres des classes :

- les maximums et les minimums des attributs.
- le noyau utilisé.
- les paramètres du noyau.

b) **Distance**

Nous avons choisi la classification par le calcul de la distance euclidienne, pour la comparaison entre les vecteurs de caractéristiques (vecteur d'apprentissage et vecteur de teste) pour identifier la personne on utilisant la convergence entre les deux vecteurs

$$d(X,Y) = \sqrt{\sum_{i=1}^{n}(y_i - x_i)^2}$$

2.8. Conclusion

Dans ce chapitre, nous avons vu une introduction sur les différents processus informatiques utilisés pour identifier les empreintes digitales qui sont faciles à gérer en cours d'utilisation. Bien que la reconnaissance des empreintes digitales soit réussie aujourd'hui, ce domaine peut encore être amélioré. L'inefficacité des systèmes automatisés face aux empreintes digitales de mauvaise qualité et le temps nécessaire pour identifier les empreintes digitales du système font maintenant l'objet de nombreux projets de recherche.

Chapitre 3 :
Résultats et discussion

3.1 Introduction

L'étude expérimentale dans notre travail est basée sur la reconnaissance de personnes parleurs empreintes digitale en utilisant les méthodes décrites dans le chapitre 2. Nous avons testé notre programme sur la base de données de VeriFinger_Sample_DB (une base de données simple et amélioré). Dans ce chapitre nous allons détailler le fonctionnement de chaque bloc de notre système ainsi qu'une explication de la base de données utilisée et l'environnement de travail.

3.2 Base de données de l'empreinte digitale VeriFinger_Sample_DB:

La base de données que nous avons utilisée dans nos expérimentations est appelléeVeriFinger_Sample_DB obtenue par le Cross Match Vérifier 300 scanner d'empreintes digitales optique disponible avec une connexion USB ou analogique. Les caractéristiques de cette base de données sont :

- Fabricant Cross Match Technologies Inc.
- Connexion USB
- Système d'exploitation pris en charge Microsoft Windows (32 bits et 64 bits)
- La prise en charge du système d'exploitation 64 bits est limitée aux applications 32 bits uniquement
- Résolution 500 ppp
- Zone de capture d'image (taille de la plaque) 31 x 31 mm (1,2 "x 1,2")
- Type de capteur : Optique
- Taille de l'appareil 53 x 158 x 60 mm (2.1 "x 6.2" x 2.4 ")
- Poids de l'appareil 1,0 kg.
- Température de fonctionnement + 2 ° C ~ + 38 ° C
- Humidité de fonctionnement 10-95% (sans condensation, résistant aux éclaboussures)
- Contient 408 images de type (tif)
- Format du nom du fichier d'empreintes digitales: xxx_yyy_zzz.tif

. Où : xxx est ID de personne

yyy est l'identification des doigts.

zzz est le numéro de scan.

La figure 3.1 donne des exemples de cette base de données.

Figure 3.1 : Quelques images de la base de données VeriFinger_Sample_DB.

3.3 Séparation des bases de données :

Notre base de données est divisée en deux parties: une base pour effectuer l'apprentissage et l'autre pour le test. Il n'y apas de règle exactepour déterminer ce partage de manière quantitatif. Dans notre travail, nous avons pris 50% de la base comme base d'apprentissage et 50% comme base de test.

Dans les séries de test que nous avons effectué, la base de donnés a été scindée de la façon suivante :

3.3.1 Images d'apprentissages ;

Les quatre premièresimages de chaque personne servent pour laphase d'apprentissage. Cette partie d'apprentissage contient 51 personnes avec 4 images pour chaque personne donc 204 images.

3.3.2 Images de Tests ;

Les quatre dernières images par personne restantes de chaque individu nous ont servi pour la réalisation desdifférents tests.Cette partie de test contient aussi 51 personnes avec 4 images pour chaque personne donc 204 images.

3.4 Environnement du travail :

Dans cette section, nous allons fournir l'environnement de travail et ses caractéristiques ainsi que le logiciel adopté dans l'application.

3.4.1 Environnement matériel :

Afin d'accomplir notre travail nous avons fourni l'équipement suivant avec les caractéristiques suivantes:

Un ordinateur :***Lenovo*** avec les caractéristiques suivantes :

- Processeur : Intel® core(TM) **i3**-5005U@2.00GHZ
- RAM**: 4.00** Go de **RAM.**
- DisqueDure: **500 Go**.
- OS: Microsoft**Windows 7** 64bits.

3.4.2 Outils de développement :

Nous avons eu recours lors de l'élaboration de notre système au logiciel MatlabR2010b(7.11.0) que nous présenterons ci-dessous.

Matlab est un langage informatique technique à haut niveau et un environnement interactif pour le développement d'algorithmes. Ilest utilisé à des fins de calcul numérique. Matlab permet de manipuler des matrices, d'afficher des courbes et des données, de mettre en œuvre des algorithmes, de créer des interfaces utilisateurs, et peut s'interfacer avec d'autres langages comme le C, C++, Java, et Fortran. Il dispose de plusieurs boites à outils en particulier celle du traitement d'images.

3.5. Architecture globale du système :

Dans notre travail, on va suivre les étapes suivantes :

- **Prétraitement :** conversion on niveau de gris, égalisation de l'histogramme.
- **Extraction** : l'extraction des minuties.
- **Classification :** comparer les caractéristiques des images de test par les vecteurs de caractéristiques stockés dans la base de données d'apprentissage.

Figure 3.2:**Système de reconnaissance des empreintes digitale**

3.5.1 Prétraitement :

La base de données utilisée dans notre travail est déjà traitée. Nous allons faire directement la binarisation par seuillage ensuite la squelettisation avant de faire l'extraction des minuties.

a.1 **Seuillage (binarisation) :**

La binarisation est faite par un seuillage simple. Les niveaux de gris aux dessous du seuil serons misent à zéros. Le but est de garder que les traits utiles de l'empreinte.

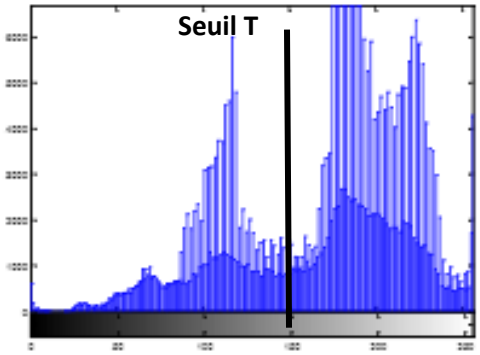


Figure 3.3 : Principe du seuillage

La figure suivante présente un exemple d'une image d'empreinte digitale avant et après seuillage.

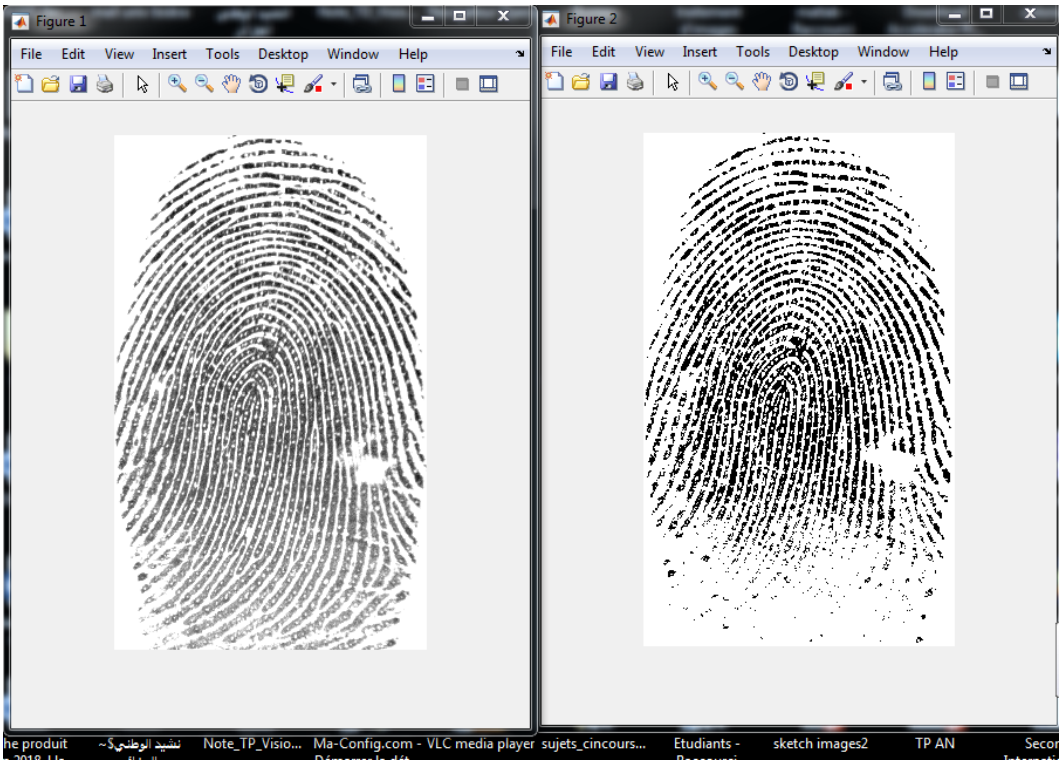


Figure 3.4 : Exemple d'une image en niveaux de gris et sa binarisation

a. Squelettisation

Permet de trouver un nombre une image d'empreinte avec des lignes d'épaisseur fixe égal à 1. La squelettisation doit être faite sur une image binaire.Le but est de pouvoir détecter rapidement les minuties. La figure suivante représente une image d'empreinte digitale avec sa squelettisation.

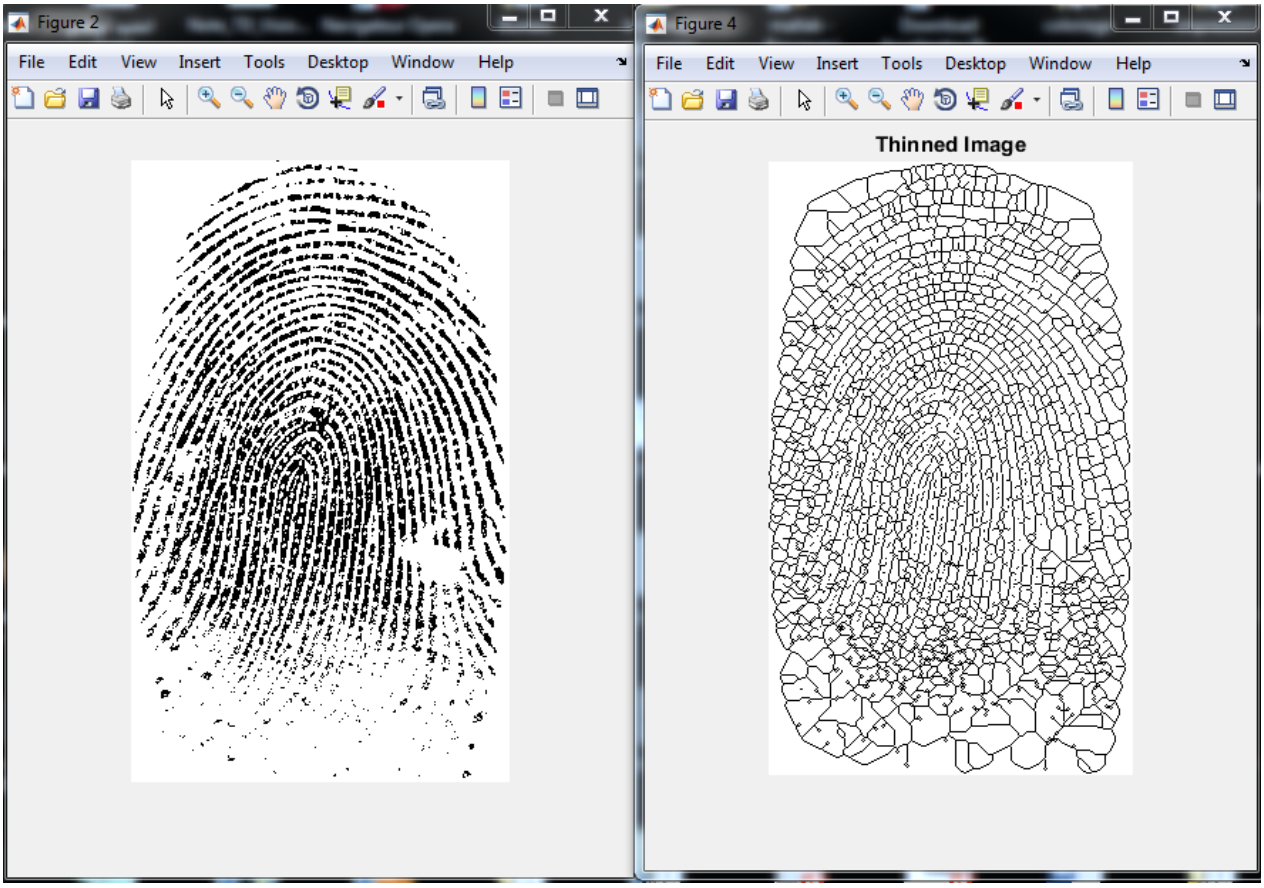


Figure 3.5 : Exemple d'une image binaire et sa squelettisation

3.5.2 Extraction des minuties

On calcule le nombre de transitions pour chaque point du squelette, on obtient le nombre de connectivité *CN* de strie partant de ce point pour déterminer le type de ce point.

La figure suivante illustre un exemple de détermination du type de minutie par le calcul des *CN* des points de l'image squelette.

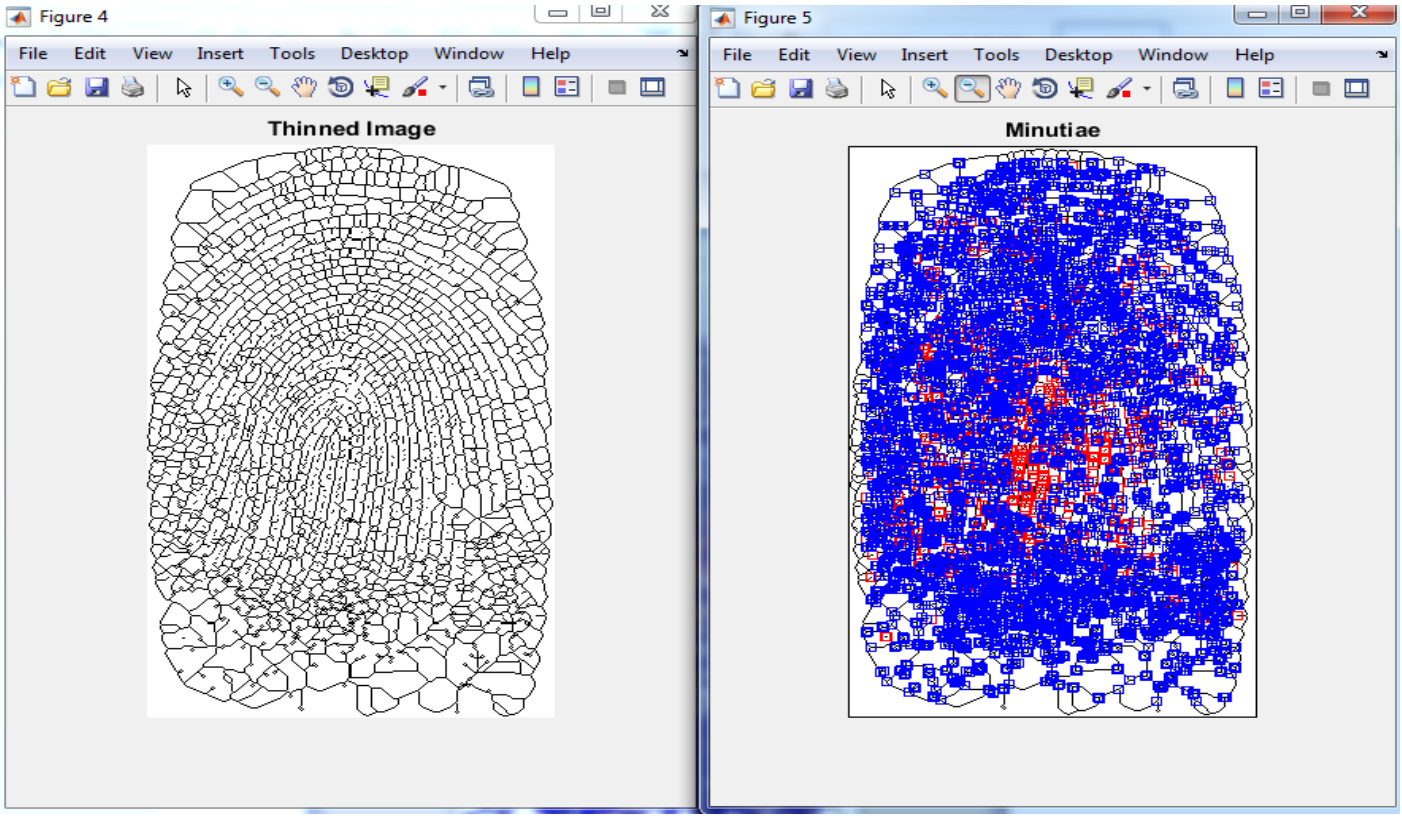
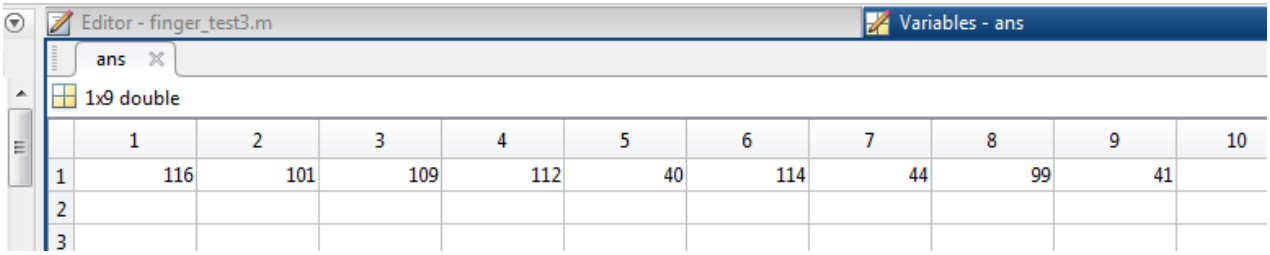


Figure 3.6: Exemple d'une image squelette et ses minuties

Un exemple de vecteur de caractéristique est donné comme suit :



	1	2	3	4	5	6	7	8	9	10
1	116	101	109	112	40	114	44	99	41	
2										
3										

Dans notre cas nous avons utilisé 9 types de minuties. Chaque valeur donne le nombre d'un type de minuties.

3.5.3 Classification

Dans notre cas, nous avons choisi la classification par le calcul de la distance euclidienne entre les vecteurs de caractéristiques.

$$d(X,Y) = \sqrt{\sum_{i=1}^{n}(y_i - x_i)^2}$$

3.6 Résultats et discussions

L'application de notre programme sur la base de données VeriFinger_Sample_DB qui contient 51 personnes dont, 8 images par personnes à donné les résultats suivants.

Images d'apprentissage	Images de test	Nombre total de personnes	Nombre de personnes reconnus	Taux de reconnaissance
204	**204**	**51**	**37**	**72.54%**

Les résultats obtenus sont intéressants. En effet on est arrivé à un taux de reconnaissance acceptable. Ce taux est intéressant ce qui rend notre système fiable et répond bien à l'objectif que nous nous sommes fixés au départ, à savoir la mise en œuvre d'un système permettant la reconnaissance d'individus.

3.7. Conclusion

Dans ce chapitre nous avons détaillé notre système de reconnaissance des empreintes digitale. Ce système est composé de trois étapes : prétraitement, extraction et classification. Dans la première étape, nous avons appliqué un seuillage pour binaires l'image ensuite une squelettisation pour avoir des lignes simples pour faciliter l'extraction de minuties. A partir des images squelettes, la deuxième étape permette l'extraction des minuties par le calcul des connexions de chaque point de l'image. Les vecteurs de caractéristiques sont ensuite classifier par le calcul de la distance minimal entre le vecteur de l'image de test et celles de la base de données.

Conclusion général

La reconnaissance biométrique est l'identification des personnes est basée sur l'utilisation de ses caractéristiques physiques ou comportementales ou biologies. Parmi les modalités les plus utilisées dans la reconnaissance biométrique est l'empreinte digitale par ce qu'elle est permanente et unique. Les chercheurs essayent toujours de développer les systèmes de reconnaissance à travers des outils mathématiques habituellement complexes pour faire la discrimination entre les individus.

Les objectifs suivis dans ce mémoire proposent une démarche qui consiste à améliorer la performance de l'identification et vérification biométriques via l'empreinte digitale par plusieurs méthodes avec un ensemble d'opérations. Notre système est constitué de trois étapes, le prétraitement, l'extraction des caractéristiques et la classification. Le prétraitement est fait par la conversion en niveaux de gris et l'égalisation de l'histogramme. L'extraction des minuties est faite par la squelettisation et le calcul du cross number CN des différents points de l'empreinte. Enfin, la classification est effectué par le calcul du distance euclidienne entres les vecteurs de caractéristiques des images de test et celle des images de la base de données.

En fin, le système proposé est appliqué sur une base de donnés connue dans le domaine des empreintes digitale et les résultats obtenus, sont intéressants. En effet on est arrivé à un taux de reconnaissance acceptable. Ce taux est intéressant ce qui rend notre système fiable où il répond bien à l'objectif que nous nous sommes fixés au départ, à savoir la mise en œuvre d'un système permettant la reconnaissance d'individus.

Comme travail futur, nous proposons de concentrée sur l'évaluation de la performance dans les deux phases (vérification et identification) en utilisant une base de données de grande taille et de l'intégration d'autres traits biométriques pour obtenir les performances du système avec une grande précision.

Bibliographie

1. **Ibtissam, BENCHENNANE.** Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus. *Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf.* 2016. https://www.univ-usto.dz/images/coursenligne/These_BENCHENNANE_I.pdf.

2. visiteplus. *BIOMÉTRIE LE CORPS IDENTITÉ.* [En ligne] 2005. www.visiteplus.net/generateur/biometrie/print/124fr.pdf.

3. **Guesmi, Hanêne.** Identification de personnes par fusion de différentes. *Université de Rennes.* 2014.

4. [En ligne] http://biometrie.online.fr/.

5. [En ligne] http://www-asim.lip6.fr/~marzouki/perso/publi/cnil-biometrie01.html.

6. **F.R.S, Francis Galton.** Personnal Identification and Description. *published on pp. 201-202 of the June 28,.* 1888 issue of Nature.

7. **John D. Woodward, Jr., Christopher Horn, Julius Gatune, and Aryn Thomas,.** Biometrics A Look at Facial Recognition. *documented briefing by RAND Public Safety and Justice for the Virginia State Crime Commission.* 2003.

8. [En ligne] https://www.biometrie-online.net/.

9. Biometrie--Wikipedia. *Wikipedia.* [En ligne] https://fr.wikipedia.org/wiki/Biom%C3%A9trie.

10. Histoire. *biometrie-online.* [En ligne] 2018. https://www.biometrie-online.net/biometrie/histoire.

11. **Abes, A. Ben Khalif et F.** Identification d'individus par reconnaissance. *Mémoire de fin d'étude, Université Kasdi Merbah, Ouargla.* Université Kasdi Merbah, Ouargla : s.n., 2008.

12. Biométrie - La géométrie de la main - L'Internaute. *linternaute.* [En ligne] http://www.linternaute.com/science/biologie/dossiers/06/0607-biometrie/main.shtml.

13. Encyclopédie Larousse en ligne - biométrie. *Larousse.* [En ligne] 2018. http://www.larousse.fr/encyclopedie/divers/biom%C3%A9trie/27110.

14. **Sofiane, BOUDJELLAL.** Détection et identification de personne par méthode.

15. biometrie-online-frappe-du-clavier. *biometrie-online.* [En ligne] https://www.biometrie-online.net/technologies/frappe-du-clavier.

16. *linternaute.* [En ligne] http://www.linternaute.com/science/biologie/dossiers/06/0607-biometrie/autres.shtml.

17. **Babich, Aleksandra.***Biometric authentication. Types of biomentric identifiers.* Helsinki : university of applied sciences, 2012.