وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة عبدالحميد ابن باديس مستغانم
Université Abdelhamid Ibn Badis de Mostaganem
كلية العلوم و التكنولوجيا
Faculté des Sciences et de la Technologie

N° d'ordre : M...../GE/2018

MEMOIRE DE FIN D'ETUDES

MASTER ACADEMIQUE

Filière : Génie Electrique

Spécialité : Systèmes des Télécommunications

Thème

ETUDE ET CONCEPTION D'UN SYSTEME DE POINTAGE BIOMETRIQUE

Présenté par :

MAMAN LOURWANA ISSAKA Issaka

Soutenu le 01/07/2018 devant le jury composé de :

Président : Mr BAHOUS. H

Examinateur : Mr OULD MAMMAR. M

Examinateur : Mr BENACHENHOU. A

Encadreur : Mr Mostefa MERAH

Année Universitaire : 2017/2018

Remerciements

Nous remercions tout d'abord, Allah (SWT) de nous avoir donner le courage mais surtout le temps d'accomplir ce travail.

Mes remerciements vont directement dans un premier temps à mon encadreur Monsieur Mostefa MERAH qui était là à ma disposition et surtout de l'aide qu'il m'a apporté afin d'aboutir à ce travail et que Dieu le bénisse davantage.

Ensuite je tiens à remercier et à témoigner mes reconnaissances à tout le corps professoral de l'Université Abdel Hamid Ibn Badis de Mostaganem (Algérie) en particulier celui du département de génie électrique de la faculté des sciences et techniques qui m'ont enseigné durant mon cursus et plus précisément à ceux qui ont accepté d'examiner mon travail.

Sans oublier bien évidemment mes camarades avec lesquels nous avions su mettre en valeur le travail d'équipe durant nos recherches et réalisations mais surtout de l'attention, l'hospitalité et aussi la considération qu'il ont démontré à mon égard durant ces cinq (5) années.

Enfin, la liste ne pouvant pas être exhaustive, permettez-moi d'adresser mes sincères remerciements à mes amis, proches et toute personne qui m'ont encouragé et cru en moi dès le début.

Dédicace

A ma famille.

Table des matières

Chapitre III *Software et Hardware du dispositif proposé*

Chapitre IV *Résultats expérimentaux*

Liste des figures

Liste des tableaux

Introduction générale

Durant plusieurs décennies, la sécurité faisait partie de la vie quotidienne de l'homme sous différentes formes. Mais ce n'est qu'au début du 21^{ième} siècle qu'une nouvelle forme de sécurité est apparue, celle qui permet d'utiliser certaines parties du corps de l'être humain pour des identifications nommée « biométrie » qui est dérivée du mot composé latin « *métri* » qui signifie mesure et « *bio* » issu du mot vivant donc mesure du vivant. Ensuite, la science c'est intéresser à plusieurs parties du corps humain seules ou combinées entre eux, comme le visage, l'œil (l'iris), la main, l'empreinte digitale, la signature, le réseaux veineux de la main, la forme de la main, etc.

L'utilisation des parties citées ci-haut sont possibles mais la différence réside dans le processus de l'acquisition afin de fournir des résultats acceptables et performants, ceux d'une bonne identification. C'est dans cette optique que dans notre travail, nous nous sommes consacrés à l'étude et la conception d'un système à base de la géométrie de la main pour le pointage au sein des entreprises, laboratoires, écoles, cantines scolaires, maisons, bref tout ce qui demande un accès réglementé.

Tout au long de ce mémoire, nous nous efforcerons d'élaborer, d'expliquer et d'argumenter les techniques utilisées, les difficultés rencontrées et aussi les solutions utilisées pour la réalisation de ce système de pointage biométrique par la géométrie de la main. C'est pour cela que dans le premier chapitre, nous évoquerons l'importance des systèmes d'accès sécurisés avant d'aborder dans le deuxième chapitre la biométrie d'une manière plus détaillée. Le troisième chapitre quant à lui est consacré à la réalisation hardware et software, le quatrième chapitre s'articulera autour des résultats expérimentaux sur la base ainsi obtenus et le dispositif de pointage réalisé.

Et en dernière position, nous clôturons par une conclusion générale sur les différents aspects de ce travail.

I.1 Introduction

La sécurité dérive du latin *securitas* (« *exemption de soucis ; tranquillité d'esprit* »). Physiquement, la sécurité est l'état d'une situation présentant le minimum de risque ou l'état d'esprit d'une personne qui se sent tranquille et confiante. Il nous revient tout de même de spécifier que le fait de sécuriser une entité (donnée, objet, personne, entité politique, juridique, intellectuelle, écologique…, informatique) revient à étudier individuellement ou collectivement ses objectifs (objectif de sécurité) sous plusieurs formes [1] :

- En tant que droit (droit à la sécurité),
- En tant que valeur (la sécurité est la première des libertés),
- En tant qu'état de ce qui est sécurité,
- En tant que fonction ou activité qui vise à sécuriser cette entité.

Quant à l'accès, il désigne toute sorte d'action, possibilité ou moyen nous permettant d'accéder à un lieu, une interface, une base de données. Nous détaillerons l'importance de la sécurité d'accès dans la suite de notre travail en utilisant la biométrie la forme de la main.

I.2 L'importance de la sécurité

Il s'agit d'abord d'un point très important dont chaque jour en moyenne il y'a une conférence qui est organisée sur lequel nous risquerons de passer le plus de temps là-dessus, car les raisons sont énormes, mais tout de même nous essayerons de citer les plus essentielles. Plusieurs aspects ou du moins raisons, nous poussent a sécurisé des données personnelles, locaux (aéroports, supermarchés, entreprises), des sites internet d'où l'enjeu à prendre devient majeur. Notons que la sécurité est une affaire de confiance. Nous pouvons tout de même avancer trois (3) critères essentiels qui nous pousserons à sécuriser un accès telles que :

- La fiabilité
- L'authenticité
- L'intégrité

Afin d'anticiper les risques de pertes de données, d'usurpation d'identité ou piratage des données. Notons que de nos jours la sécurité est inévitable dans tous les secteurs d'activité, car il y'a crainte de cyberattaque comme celle de l'année passée qui a infecté beaucoup d'entreprises, hôpitaux, ordinateurs à travers le monde à l'aide juste d'un virus

« WANACRY » qui a fait vibrer la terre ce qui a poussé les gens à prendre conscience du danger qui existe dans ce domaine s'il est mal protégé.

Dans notre cas nous allons nous pencher sur la sécurité biométrique comme accès sécurisé qui révolutionne le monde depuis plusieurs années dans plusieurs domaines qui se sont focalisés dans les banques, services, magasins, aéroports, cantine pour aider à filtrer les personnes qui sont habilitées à avoir accès à un service ou pas.

I.3 Types d'accès

Nous pourrions nous référer sur ces trois (3) hypothèses qui nous registrent l'ensemble des accès possibles que nous avoir à faire :

3.1 Ce que l'on sait

C'est-à-dire tout ce que nous savons comme le mot de passe, le nom, le prénom ; qui peuvent toutefois nous être volé, usurpés ou pirater très facilement par un hacker.

3.1.1 Mot de passe

Il s'agit d'une méthode qui est utilisée pendant plusieurs décennies, elle permet à l'utilisateur de saisir un ensemble de caractères des chiffres ou bien des lettres et des caractères à travers un clavier. C'est l'une des méthodes les plus utilisées à l'heure actuelle que ça soit dans le web, le quotidien (porte de maison, téléphone, ordinateur). Mais son défaut ce qu'il peut être facilement hacké en une fraction de seconde vu que le chiffrement n'est pas trop solide.

3.1.2 Nom et prénom

C'est l'identité que l'on affecte à une personne afin de le différencier des autres personnes dans un environnement donné (classe, service, local, etc.).

3.2 Ce que l'on a

Tout ce dont nous possédons physiquement à notre possession telle que la clé, le badge, les puces RFID, les cartes bancaires qui sont un ensemble d'informations stockées dans un support en plastique, bracelets connectés là surgit la possibilité de perdre sa carte, sa clé ou d'être volée.

3.2.1 Les puces RFID

Comme son sigle l'indique *Radio frequency identification* et aussi appelé « tag ». Ce sont des cartes constituées d'une antenne reliée à une puce électronique permettant d'envoyer et recevoir les informations à travers des antennes émettrices et réceptrices. C'est un transfert d'énergie électromagnétique entre une étiquette radio et un émetteur RFID.

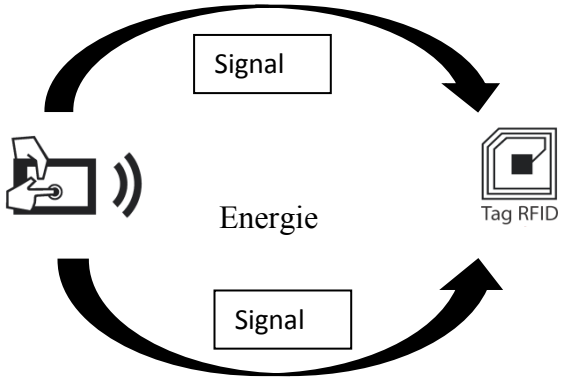


Figure 1.1 Fonctionnement du principe du RFID

Elle était d'abord conçue pour les militaires bien avant d'être au service du civil dans les années 2000 [2] dans la conception des objets connectés. La plus répandue est la Mifare fabriquée par l'entreprise NXP qui est technologie sans contact. Elle se trouve sous quatre (4) technologies qui se différencient à travers leurs stockages comme ayant toutes la même fréquence de service tournant autour de 13.56Mhz. Nous avons :

- La Mifare ultralight qui a un stockage de 512 bits c'est-à-dire 64 caractères ;
- La Mifare classique 1K cette fois-ci avec 768 octets ce qui correspond aux 768 caractères ;
- La Mifare classique 4K, 4ko équivalent à 4096 caractères
- La Mifare DESfire Ev1 qui varie de 2ko, 4ko ou 8k, la taille du fichier est choisie lors de la création.

Il existe plusieurs types sur le marché tel que :

Tableau 1.1 : Types des RFID sur le marché

Types de supports	**Objectifs**
Cartes et badges 	○ Identification des personnes ○ Paiement sans contact ○ Contrôle d'accès en entreprise ○ Transports ○ Cartes de fidélité
Étiquettes et stickers 	○ Identification des biens ○ Stockage et inventaire ○ Lutte contre la contrefaçon ○ Traçabilité des produits ○ Promotion dans les évènements
Bracelets 	○ Identification des personnes ○ Paiement sans contact ○ Promotion dans les évènements
Bracelets et tags 	○ Accès à des résidences, locaux et parking ○ Badges d'accès en entreprise
Puces sous-cutanées 	○ Identification d'animaux ○ Traçabilité

De nos jours, elle est même implémentée dans le corps humain pour faciliter l'identification dans les services afin de remplacer les badges d'accès. Notons aussi que les RFID ont des limites, car il y'a risque de la perdre à n'importe quel moment ou être volée, ce qui devient plus dangereux puisque les informations peuvent être copiables et modifiables par un tiers. Ce qui nécessite une mise en sécurité des données personnelles, c'est-à-dire protéger la vie privée de l'utilisateur en les changeants régulièrement afin d'améliorer le chiffrement comme le font certaines entreprises ou banques qui exigent aux clients de changer leurs cartes après un certain temps d'utilisation.

3.3 Ce que l'on est

Notre propre personne, des traits morphologiques comme les empreintes digitales, l'ADN, l'iris, l'architecture de la main, la manière de taper sur le clavier, la voix dans ce cas c'est quelque chose qui nous appartient, qui est très difficile d'être piraté, d'être volé et moins d'être confié à quelqu'un, car il fait partie de nous-mêmes.

3.3.1 L'empreinte digitale

Il s'agit d'une architecture que possède nos mains qui ont été développées à l'état embryogénique, ce qui les rend uniques en chacun de nous. [3] Elle apparaît donc durant la grossesse où nous observons des atténuations sur le gonflement ce qui donne la création des plis qui sont incrustés ensuite formant l'empreinte digitale dans le derme.

Nous disposons trois types d'empreintes digitales : [4]

3.3.1.1 Empreinte en arc : il s'agit de celle qui recouvre le doigt d'un côté à l'autre.

3.3.1.2 Empreinte en boucle : son dessin *entre* et *sort* du même côté du doigt. Elle est dite *radiale* ou *cubitale* selon le côté du doigt d'où émerge l'empreinte.

3.3.1.3 Les spires ou tourbillons

Figure 1.2 : Les types d'empreintes digitales

3.3.2 L'ADN

L'acide désoxyribonucléique, ou ADN, est une macromolécule biologique présente dans toutes les cellules ainsi que chez de nombreux virus. L'ADN contient toute l'information génétique, appelée génome, permettant le développement, le fonctionnement et la reproduction des êtres vivants. Il s'agit là d'un trait qui est vraiment unique chez une personne à part les *vrais* jumeaux qui en possèdent le même. Avec ceci nous avions une excellente performance et une certitude qu'il s'agira d'une seule personne qui aura accès excepté les *vrais* jumeaux.

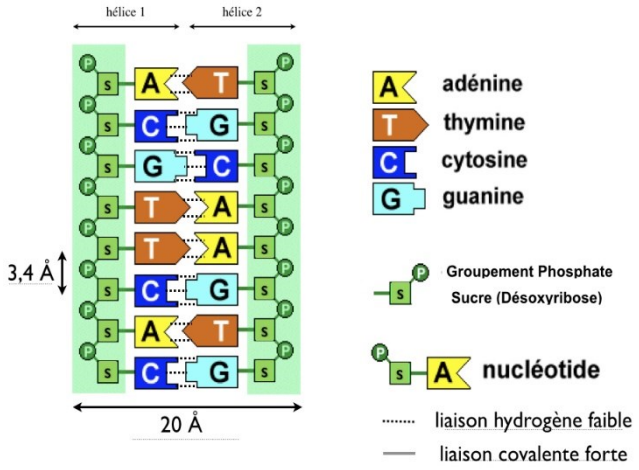


Figure 1.3 : Composition de l'ADN

Figure 1.4 : Forme de l'ADN

3.3.3 Le visage

Elle était basée initialement en 1970 sur certains traits du visage comme les lèvres, la forme du menton, les sourcils ou encore la distance entre deux yeux. C'est l'extraction de certaines caractéristiques du visage pour l'authentification des individus. Mais il faut que le sujet soit bien positionné devant le système. Ensuite ces traits seront comparés à base de données pour voir la similitude des deux. Mais notons aussi qu'elle possède des inconvénients tels que le déguisement ce qui le rend vulnérable aux attaques, les vrais jumeaux aussi causent un souci vu qu'ils ont les mêmes traits.

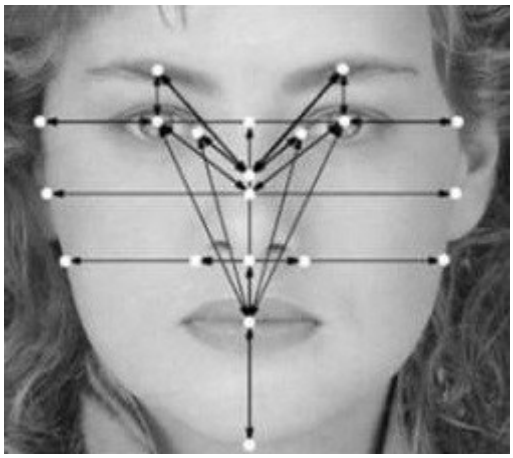


Figure 1.5 : Les parties possibles du visage

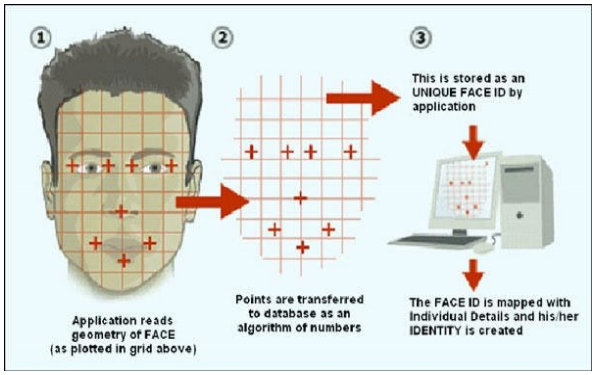


Figure 1.6 : Exemple d'application utilisée

3.3.4 L'iris

C'est la membrane colorée du Sil. Une caméra proche des infrarouges photographie une tranche de l'iris, elle relève les caractéristiques particulières du relief. Il est fiable, mais les gens se méfient trop puisqu'il y'a des lasers qui vont passer.

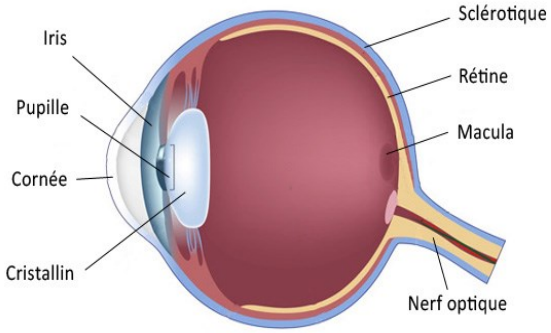


Figure 1.7 : Schéma de l'œil

Figure 1.8 : Analyse de l'iris par biométrie

3.3.5 La voix, signal vocal

Il s'agit d'une reconnaissance par la voie utilisant les caractéristiques vocales aidant à l'identification des individus utilisant des phrases codées. On utilise généralement un téléphone ou un microphone pour l'acquisition favorisant ainsi le faible coût de sa réalisation, mais elle est très vulnérable aux attaques et se confronte aux perturbations extérieures (échos, bruits, tec.)

Figure 1.9 : Authentification vocale.

3.3.6 La manière de taper le clavier

Les premières recherches de cette technique remontent aux années 1980 lorsque le gouvernement américain voulait savoir s'il est possible de distinguer les personnes e fonction de leurs manières de taper le clavier tel que les télégraphes. [5] Cette technique se réfère à la manière dont un individu tape les touches d'un clavier qui fait partie de la biométrie comportementale communément appelée dynamique de frappe au clavier (DDF). Le choix de cette méthode se repose principalement sur le coût et sa simplicité puisqu'il suffit juste d'un clavier du PC et aussi les utilisateurs ne sont pas retissant. Par ailleurs cette méthode varie facilement donc sa non-fiabilité puisqu'elle dépendra de l'humeur de l'utilisateur, sa manière de taper le clavier peut changer est en fonction de comment il l'a apprise. Ces facteurs nous prouvent un peu la limite de cette technologie. [6]

Figure 1.10 : Dynamique de frappe au clavier

Notons que ces trois (3) hypothèses citées plus haut sont la base même de l'accès sécurisé, mais la dernière requière beaucoup plus notre attention à cause de son unicité au cours

du temps. Notre corps humain possède des parties qui ne changent pas en fonction du temps tel l'ADN, les empreintes digitales ou bien encore le l'iris. Mais précisons qu'avec la forme de la main on arrive à un système d'autant plus robuste puisqu'avec l'empreinte de la main elle peut s'effacer ou bien la personne peut faire allusion à des procédures judiciaires comme la police, etc. Par ailleurs, la forme de la main ne gênera pas l'utilisateur lors de l'accès et mieux encore même si un usurpateur prend possession il ne pourra pas faire grand-chose par rapport à une empreinte digitale qui peut être reconstituée et utilisée à d'autres fins telles que les faux papiers, etc.

C'est en ce sens que dans la suite de notre travail nous allons la développer cette technique d'accès.

I.4 Conclusion

En somme, nous avions détaillé dans ce chapitre l'importance des accès sécurisés, mais aussi les différents types qui en existent. Par ailleurs, détailler tout prendra du temps, c'est pour cela c'est ne que l'essentiel qui a été développé. Nous nous focaliserons sur la biométrie en général dans le prochain chapitre.

II. 1 Introduction

Elle regorge les techniques permettant d'identifier des personnes à l'aide des traits biologiques (ADN, salive, odeur, sang), comportementaux (dynamique de frappe au clavier, signature, parole, démarche) ou morphologiques (empreintes digitales, forme de visage, de la main, de l'iris ou de la rétine). La biométrie dérive du latin « bio » qui signifie humain et « métrie » qui veut dire mesure, donc la mesure des caractéristiques de l'être humain. Ces dernières années, elle se trouve présente dans notre vie quotidienne comme nous pouvons le constater, les fabricants des téléphones les équipes des capteurs d'empreintes digitales ou reconnaissance faciale. Il s'agit d'un ensemble de traitement qui se fera par des processus afin de restreindre les ressemblances de ces traits pour deux individus, ce qui nous pousse à dire que cette méthode possède des limites aussi.

Dans la suite de ce travail, nous détaillerons le principe de la biométrie basée sur la géométrie de la main.

II.2 Fonctionnement du système biométrique

2.1 Définition

C'est un système d'identification des personnes qui se base sur l'étude des différents caractères physiologiques ou morphologiques des contours de leurs mains obtenues après la phase de l'acquisition d'une personne et par la suite elles seront comparées avec ceux qui existent déjà dans une base de données dédiée à cet effet afin de faire ressortir la similarité.

Ce système se base sous deux aspects généraux qui sont les suivants :

2.1.1 Identification

Cette phase permet de faire le *one to many*, c'est-à-dire comparer les données (l'empreinte ou la forme de la main de l'individu) avec ceux qui existent dans la base de données. Si ces derniers s'avèrent identiques alors on valide cette étape et on conclut que cette donnée existe. Et, on peut avoir plusieurs personnes ayant les mêmes identités, seule cette dernière étape va les différentier.

2.1.2 Authentification

Elle permet quant à elle de voir si réellement il s'agit de la bonne personne. Ainsi, après l'acquisition des données de la personne, celles-ci seront étudiées pour vérifier si elles sont liées à cette personne. Quand le test est validé alors là on peut dire que la personne est authentifiée c'est-à-dire qu'il s'agit de la bonne personne.

II.3 Description d'un système biométrique

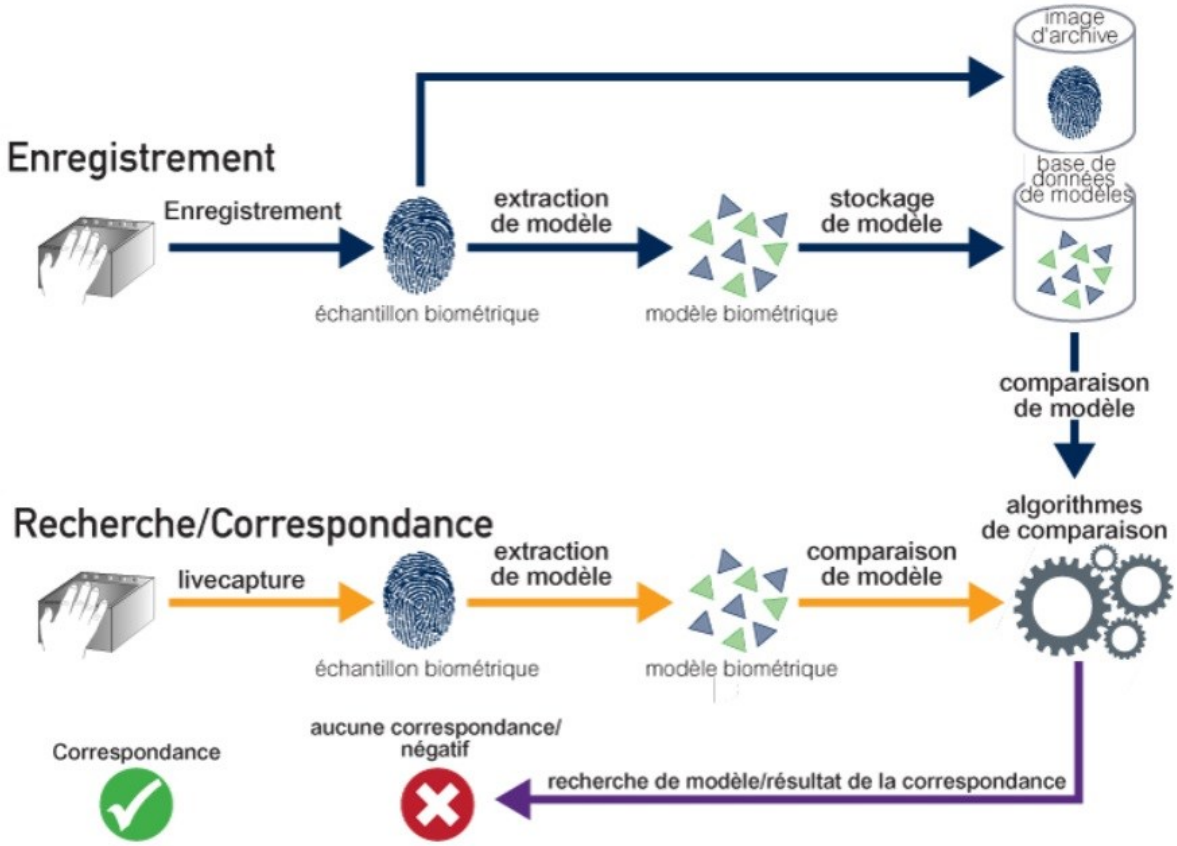


Figure 2.1 Descriptions d'un système biométrique

La phase d'enregistrement sert à l'acquisition des caractéristiques et l'archive de l'échantillon biométrique afin d'être numérisée pour une utilisation ultérieure [7]. C'est une étape primordiale par laquelle passera un utilisateur déjà enregistrer et un nouveau aussi qui sera enregistré dans la base de données, là on parle d'enroulement qui consiste à enregistrer une nouvelle personne dans la base de données existante déjà.

La comparaison se fera avec des modèles déjà sauvegardés dans la base de données afin de voir s'il y'a ressemblance ou non avec l'acquisition que nous avions faite. Mais n'oublions pas que la phase d'extraction nécessite un traitement d'image/son tout dépend de ce qu'on fait entrer dans le système. Ce traitement permettra d'obtenir des données numériques et diminuer

le temps lors de la comparaison, et cette comparaison se fait à travers un algorithme qui recherchera les points caractéristiques de ressemblances. Si les caractéristiques sont différentes alors le test s'avère négatif ce qui échoue l'accès.

Pour tous les systèmes biométriques, les processus sont identiques et automatisés leur permettant d'agir rapidement lors du traitement malgré que d'autres sont multimodales c'est-à-dire une combinaison de deux ou plusieurs caractères biométriques. On peut avoir l'empreinte digitale avec le réseau veineux, ou bien la forme de la main et le visage et l'iris, etc.

Ce système se focalise sur des propriétés suivantes :

1. Faible taux de duplication par des usurpateurs
2. Performant
3. Simplicité d'utilisation
4. Universalité
5. Efficacité

Dans cette partie , nous nous focaliserons sur la biométrie de la forme de la main

Cette technique se base sur l'étude de la forme de la main, la longueur des doigts, l'épaisseur, la position relative font l'objet de l'étude. Tous ces paramètres sont ensuite comparés avec ceux qui existent déjà dans la base de données. Les utilisateurs sont plus attirants à cette méthode que celle des empreintes digitales qui a un aspect retissant, celui de la police. Malgré son coût qui est raisonnable elle reste encombrante lors l'installation dans l'environnement dédiée.

Elle est de nos jours employée pour les contrôles d'accès comme dans les services, certains aéroports internationaux, mais aussi dans les systèmes de pointage qui permettront de savoir les horaires auxquelles les employeurs par exemple d'une société sont venus et répartie, ce qui est d'ailleurs notre objectif principal du début jusqu'à la fin de ce travail.

II.4 Biométrie de la main

4.1 Raisons du choix de la main

Elle permet une acquisition moins couteuse, simple d'usage, favorable aux écosystèmes, mais surtout donne une bonne performance lors de la vérification puisqu'il n'y a pas beaucoup de traits à étudier. Les gens se sentent beaucoup plus à l'aise avec une telle technologie que celle de l'empreinte qui fait référence à la police.

4.1.1 Avantages

Cette technique permet d'avoir des fichiers moins volumineux que pour une base de données servant à comparer des empreintes digitales. Nous prenons le cas de la numérisation d'une image d'une main, cette dernière ne représente qu'un espace d'environ 15 octets alors que l'image de l'empreinte a une taille avoisinant les 500 octets, voire plus. Mais aussi les facteurs comme l'humidité de la peau, la saleté, petites lésions, brûlures sur la main n'empêche pas une bonne prise de la mesure [8].

4.1.2 Inconvénients

Tant qu'il y'a des avantages, il y'aura bien évidemment des inconvénients comme des maladies liées à vieillesse comme l'arthrite qui peut engendrer la déformation des doigts qui agit sur la forme de la main favorisant une mauvaise détection. Mis à part ça, le problème se focalise surtout chez les membres d'une même famille pouvant tromper ce système biométrique, car ils présentent beaucoup de traits physiques semblables. Le système est un peu encombrant pour être transporté [9].

4.2 Utilisation

Par ailleurs, il s'agit d'une technologie qui a été choisie pour le village Olympique en 1996 à Atlanta, au niveau des postes de migration, identification d'électeurs, au parc d'attractions Walt Disney World afin de s'assurer que les tickets sont utilisés par la même personne d'un jour à l'autre[10] au musée de Louvre en France pour accéder à certaines pièces et aussi par des grandes sociétés comme coca cola qui l'utilise afin de permettre à ses employés d'utiliser ses mains à leurs arrivées et sorties, mais aussi le pointage et de présence qui facilitera la tâche à la direction des ressources humaines. Dans plusieurs établissements comme le Collège public Salagou de Clermont-L'Héreault, l'utilisent à la cantine ou l'entrée de l'école évitant de refaire des cartes à chaque fois, car les élèves ne sont pas vigilants vis-à-vis d'une carte qui se perd facilement. Cette technique de la géométrie de la main est très fiable lorsqu'elle est conjuguée à d'autres formes d'identification comme la carte, l'iris, l'empreinte ou encore le mot de passe comme dans notre cas pour avoir un système multimodal.

4.3 Anatomie de la main

Elle est subdivisée en deux faces, la face palmaire, c'est-à-dire antérieure, et une face dorsale dite postérieure. Ces deux faces sont structurées en plusieurs parties en autres nous avons : la partie distale, latérale, médiale et proximale où réside les cinq (5) structures cylindriques divisées en 3 sous parties :

- L'éminence thénar, latérale
- Le creux de la main, central

- L'éminence hypothénar, médiale

Ces cinq (5) doigts sont décrits comme suit :

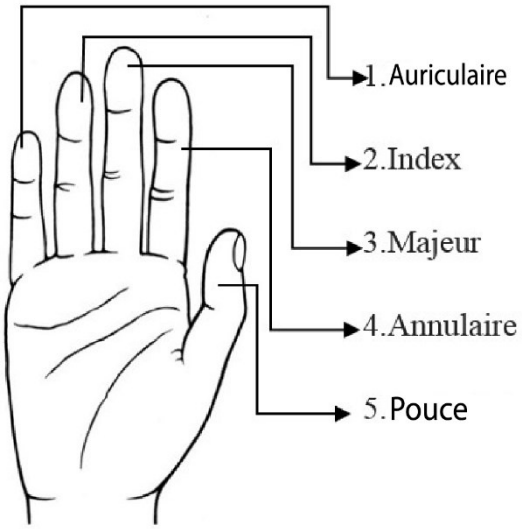


Figure 2.2 Anatomie de la paume de la main droite

4.3.1 Description

Celle-ci comprend 27 os dont :

- Huit (8) du carpe constituent le poignet et sont alignés sur deux rangées : la proximale (près du bras) avec le scaphoïde, le semi-lunaire, le pyramidal et le pisiforme, et distale (près des doigts) avec le trapèze, le trapézoïde, le grand os et l'os crochu.
- Cinq (5) du métacarpe, un par doigt, sont les os longs qui forment la structure élargie de la main.
- Quatorze (14) phalanges se séparent en trois catégories : les proximales, prolongées par les médianes (le pouce n'en a pas), et les distales qui forment l'extrémité des doigts.

Et quant aux muscles nous avons plusieurs types comme suit[14] :

- Les muscles extrinsèques. Situés dans l'avant-bras, ils transmettent les mouvements, aux mains et aux doigts, par l'intermédiaire de longs tendons qui cheminent soit sur la paume (tendons fléchisseurs), soit sur le dos de la main (tendons extenseurs).
- Les muscles extrinsèques. Situés dans la main, ils transmettent les mouvements précis des doigts. Les muscles interosseux, se distinguent selon leur situation, en dorsaux (dos de la main) ou palmaires (paume), et permettent respectivement d'écarter et de rapprocher les doigts. Les muscles lombricaux, présents entre chacun des 5 doigts, participent à la flexion et à l'extension tandis que les muscles thénariens servent à la mobilisation du pouce et les muscles hypothénariens à celle de l'auriculaire [11].

À propos des doigts, nous distinguons qu'ils possèdent que des ligaments et des tendons, provenant des muscles de la main et de l'avant-bras. Les quatre derniers doigts comportent ainsi chacun deux tendons longs, de flexion et d'extension, provenant des muscles de l'avant-bras. Le pouce est contrôlé par des tendons de muscles, extenseurs et fléchisseurs, et deux ligaments principaux (latéral interne et latéral externe).

Ensuite vient le tour de l'innervation qui est assurée que par trois nerfs principaux issus du plexus brachial, enchevêtrement de fibres nerveuses provenant du rachis cervical :

- Le médian innerve les muscles de l'avant-bras et de la main,
- Le radial, les muscles de la paume,
- Le cubital (ou ulnaire), les muscles du dos de la main.

Ces nerfs se terminent par de petits faisceaux donnant à la main une capacité de mouvements très précis et une perception sensitive très fine.

Et enfin nous entamons l'irrigation gérant le flux vasculaire se fait par l'intermédiaire des artères radiale et cubitale, accompagnées par deux veines profondes, dites « satellites ». Les veines superficielles, développées sur la face dorsale des doigts, forment un réseau allant de l'ongle à la phalange proximale. Elles sont très nombreuses et infiniment variables d'un individu à l'autre, mais aussi d'une main à l'autre [12].

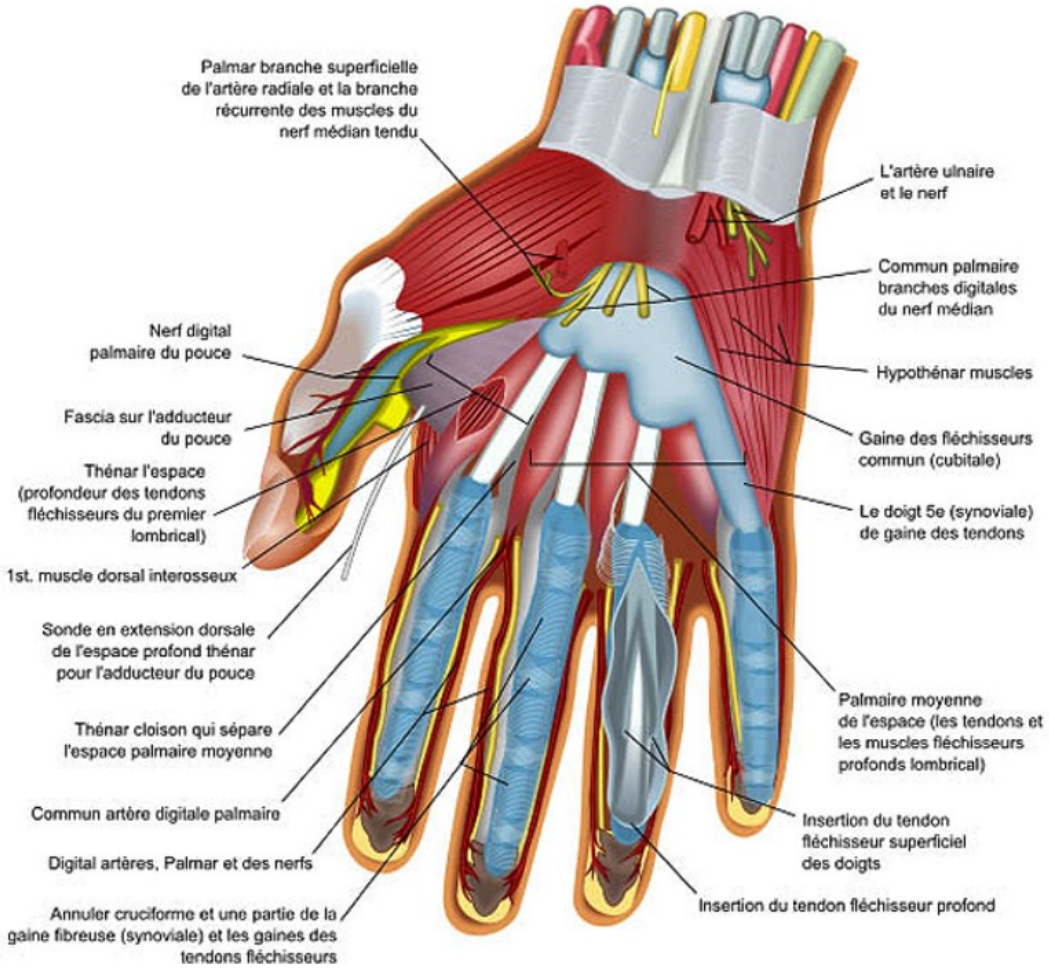


Figure 2.3 Dissection profonde palmaire [13]

4.4 Procédés de l'acquisition

Nous avons utilisé un boîtier dont le fond est noir pour faciliter la segmentation qui est un procédé qu'on détaillera par la suite dans la partie traitement contenant une webcam de 5MP en bas d'un verre qui est éclairé par une lampe LED. Un capteur de proximité donnera un signal à la webcam afin de prendre une capture de la main pour la suite du processus de traitement. Cette phase prendra quelques secondes.

II.5 Traitement

Dans cette partie nous allons développer le processus à suivre afin d'obtenir l'usage de la forme de la main et jusqu'à l'identification.

5.1 Acquisition

Il s'agit d'un boîtier contenant une ampoule LED permettant d'éclairer ce dernier, dont à côté il y'a une webcam de 24Mpx qui prendra la capture de la main. La main est posée sur une vitre transparente dont le haut de la main est surmonté d'une planche de couleur noire qui permettra l'optimisation du temps lors du traitement surtout la phase de la segmentation. Mais aussi, nous

avons placé des capteurs TOR (Tout Ou Rien) qui permettront une acquisition automatique dès que l'utilisateur l'appui. En ce temps nous aurons une faciliter lors de la détection de la forme de la main uniformément pour tout le monde. Une fois les capteurs détectent la forme approximative de la main l'utilisation saisira un mot passe qui sera rattaché à sa géométrie de la main afin de valider sa présence. Le système devient alors multimodal ce qui nous fournira un système plus performant, sûr, et, mais aussi l'exploitation de plus du processus de vérification d'identité comme le bruit d'acquisition [14]. Lui-même est subdivisé en plusieurs types à savoir :

- Systèmes multialgorithmes, le traitement des données biométriques acquises se fait avec plusieurs algorithmes, mais on a le temps de traitement qui s'avère un long, et aussi l'utilisation n'a pas beaucoup d'interaction avec ces genres de systèmes puisque c'est en une seule prise.
- Systèmes multicapteurs, l'acquisition de plusieurs informations du même donnée biométrique est primordial dans ces systèmes c'est la raison pour laquelle plusieurs capteurs saisissent cette capture afin de ne rien laisser.
- Systèmes multi-instances, il choisit de prendre une donnée biométrique plusieurs fois comme la main gauche et la main droite, mais l'utilisateur ne l'adore pas puisqu'il faut faire le mouvement plusieurs fois, c'est ennuyant et fatigant si on peut le dire ainsi.
- Systèmes multiéchantillons, celui-là favorise une bonne robustesse contre les bruits qui prend plusieurs données biométriques d'une manière répétitive. Mais nous constatons que les utilisateurs n'adhèrent pas bien ces systèmes à cause de la manière répétitive
- Systèmes multicaractères utilisant plusieurs caractères afin d'identifier une personne, mais le coût est important vu le capteur à mettre en place. Comme la combinaison entre le visage et l'iris ou bien l'empreinte et la forme de la main
- Systèmes hybrides qui sont eux composés de plusieurs scénarios à l'image des autres systèmes ce qui le rend plus informatif que les autres systèmes d'ailleurs [15].

En ce temps la capture d'image suivra un traitement pour être stockée dans la base de données pour une prochaine utilisation lorsque l'utilisateur se pointera. Nous utiliserons le logiciel MATLAB pour le traitement que l'on détaillera dans la partie suivante.

II.6 Conclusion.

En somme, cette technologie de la main entraine une facilité lors de son usage et est moins onéreuse que d'autres outils de contrôle d'accès puisqu'elle aide plusieurs entreprises surtout la direction des ressources humaines sur le plan de pointage des employés. Tout de même, bien que plusieurs sociétés font usage de cette technique, elle ne semble pas être partout pour des raisons de sécurité pointue qu'exigent certaines entreprises afin de mieux protéger les informations de leurs bases de données .

III.1 Introduction

La réalisation d'un prototype se base essentiellement sur deux parties : la partie hardware et la partie software permettant le fonctionnement des différents dispositifs de la carte entre eux afin qu'ils nous fournissent un parfait résultat. C'est ainsi que dans la suite de ce chapitre nous allons nous baser sur le processus qui nous a permis à mettre en place ce prototype à travers une description assez claire des composants, cartes et logiciels utilisés lors de cette réalisation, mais surtout les résultats et interprétations ayant été obtenus à la fin de ce test du début jusqu'à la fin.

III.2 La partie Hardware

2.1 La carte utilisée « Genuino UNO »

2.1.1 Historique

Le projet de l'invention de cette carte est basé sur la licence libre dans la pittoresque ville d'Ivrea, qui chevauche la rivière bleue verte Dora Baltea au nord de l'Italie, est connu pour ses rois déchus. En l'an 1002, le roi Arduin (Arduino en italien) devint le seigneur du pays, pour être détrôné par Henri II d'Allemagne, deux ans plus tard. Aujourd'hui, le *Bar di Re Arduino*, un bar dans une rue pavée de la ville, honore sa mémoire, et c'est là qu'un nouveau roi inattendu naquit. Ainsi c'est là que commence la révolution de l'univers de l'électronique à travers le monde entier [16].

C'est à l'honneur de ce bar où Massimo Banzi a pour habitude d'étancher sa soif que fut nommé le projet électronique Arduino (dont il est le cofondateur). Arduino est une carte microcontrôleur à bas prix permettant même aux novices de faire des choses époustouflantes. Vous pouvez connecter l'Arduino à toutes sortes de capteurs, lampes, moteurs, et autres appareils, et vous servir d'un logiciel facile à appréhender pour programmer le comportement de votre création. Vous pouvez construire un affichage interactif, ou un robot mobile et bien plus que ça. [17]. Il s'agit d'une petite carte (5,33 x 6,85 cm) carte électronique dont à partir d'elle on peut détecter des obstacles par des capteurs, de programmer et commander des actionneurs d'où l'interfaçage programmable.

Les cartes ARDUINO sont de plusieurs modèles et ces derniers se différentient par leurs fonctionnalités comme les Mega/2560, Yun, Nano, Esplora, Fio, NG/Older, Pro/Pro Mini, Gemma Mega ADK, Leonardo, Duemilanove/Decimila, Mini, Ethernet et bien d'autres. Nous

avons choisi l'Arduino Genuino UNO dans la suite de notre réalisation puisqu'il est assez suffisant dans notre conception ce qui nous permet de réduire aussi le coût.

2.1.2 Architecture de la carte « Genuino UNO »

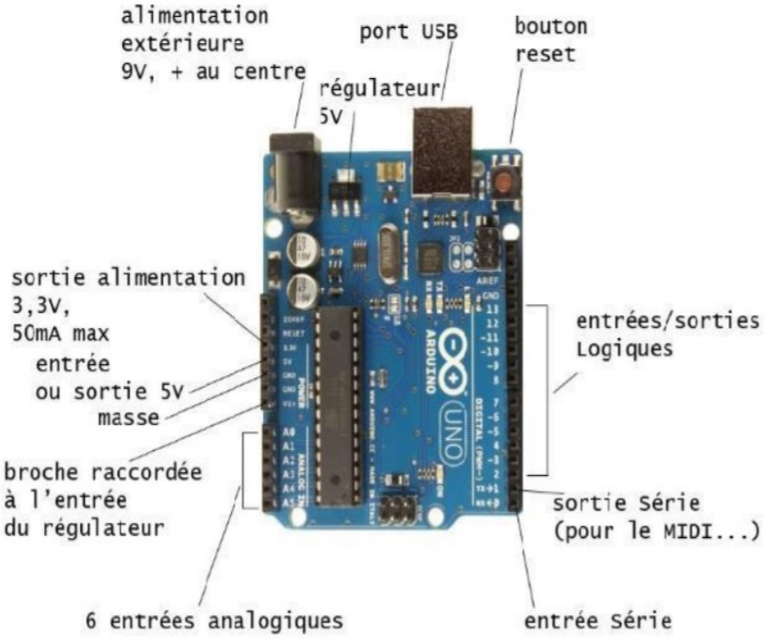


Figure 3.1 Description de l'architecture de la carte Arduino UNO

La conception matérielle (schémas électroniques et typons) [18] est distribuée sous licence *Creative Commons Attribution Share-Alike 2.5*. En plus, le code source de l'environnement de programmation et les bibliothèques embarquées sont disponibles sous licence LGPL. C'est ce qui permet à beaucoup d'amateurs et programmeurs d'enrichir les applications à travers le partage en libre accès aux novices.

Cette interface nous permettra de programmer n'importe quels capteurs, composants à travers les menus qu'elle compose. Nous détaillerons le contenu de chaque menu ici-bas.

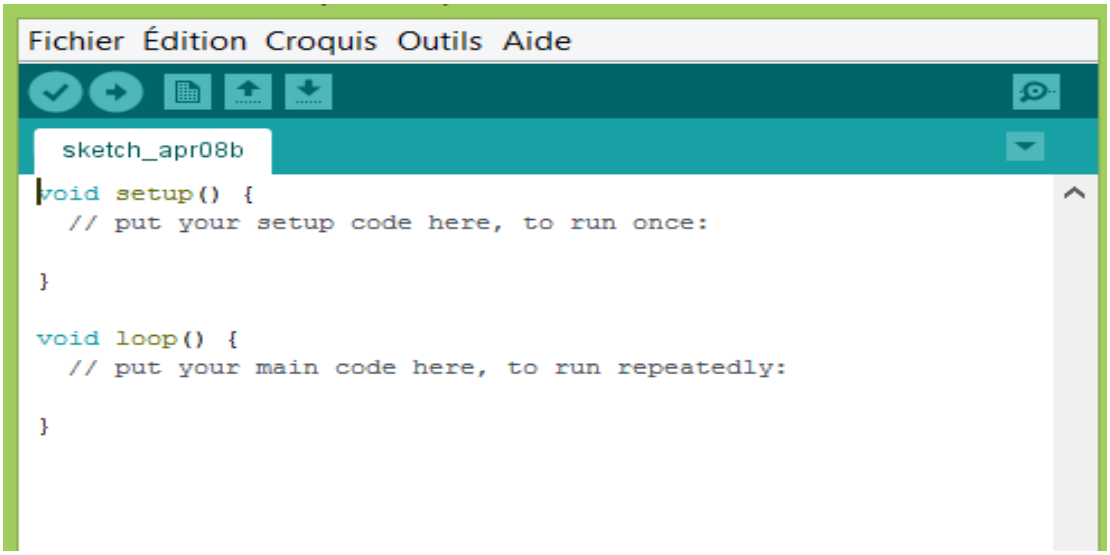


Figure 3.2 Interface du logiciel Arduino

Pour tous les programmes, il est nécessaire de poser les deux fonctions de base comme

- void setup () : la fonction d'initialisation et de configuration de l'état des
- broches (Entrées ou sorties) en utilisant la fonction pinMode (nom, état).
- void loop () : dans laquelle on mit nos instructions

La compilation permet de voir les éventuelles erreurs dans le programme avant de le charger au niveau de la carte et le téléversement permet de charger le programme après correction des erreurs sur la carte en la connectant à l'ordinateur via un câble USB, celui qui ressemble à celui de l'imprimante.

(a)

(b)

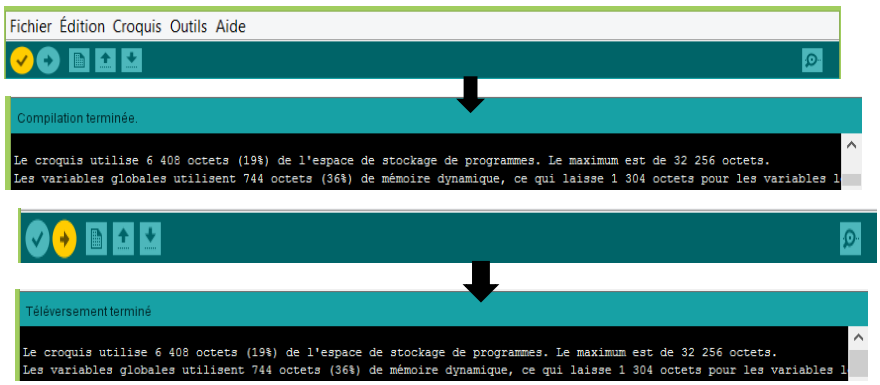


Figure 3.3 (a) Statut d'un programme bien compilé (b) Statut d'un programme bien téléversé

2.1.3 Programmation de la carte ARDUINO UNO R3

Le langage de programmation d'une telle carte est basée sur le C et C++.Pour cela ce programme est structuré est trois (3) grandes parties essentielles à savoir : la structure, les valeurs (variables et constantes) et les fonctions.

Nous l'utilisons pour l'interfaçage avec le bouton poussoir et l'écran LCD.

2.1.3.1 Structures

Il est impératif de définir deux fonctions de bases ci-dessous :

Void setup () qui fera l'initiation et la configuration des états des broches

Void loop () s'en charge de nos instructions.

Mais aussi nous dénombrons d'autres structures telles que celles de contrôles (if, else, for, while, break,…), de

- Comparaisons

Tableau 3.1 Symboles des structures de comparaison

= =	**Egal**
! =	Différent
< , >	Inférieur, supérieur
<= , >=	Inférieur ou égal, supérieur ou égal

- Composés

Tableau 3.2 Symboles des structures composées

+ +, - -	**Incrémentation, décrémentation**
+ =, - =	Addition composée, soustraction composée
*=	Multiplication composée
/ =	Division composée

2.1.3.2 Variables

Comme dans les autres langages de programmation, nous avons ici aussi des constantes prédéfinies à savoir :

- **HIGH, LOW** : Haut, Bas
- **INPUT, OUTPUT** : Entrée, Sortie
- **TRUE, FALSE** : Vrai, Faux
- **Constantes décimales**

Les différents types de données et leurs conversions sont les suivantes :

- **Void** : fonctions
- **Char** : caractère
- **Long** : réel long
- **Int** : entier
- **Float** : réel

Il y'a par ailleurs des fonctions utilisées pour faire certaines conversions des nombres réels, entiers, réels longs vers un caractère dans la programmation telle que : char (), byte (), int (), float (), long ().

2.1.3.3 Fonctions

Dans cette partie nous allons voir deux types d'entrées/sorties en fonction de l'utilisation à savoir [19] :

- **Entrées/sorties analogiques de A0-A5**
  - **AnalogRead (broche)** : elle permet la lecture d'une broche analogique
  - **AnalogWrite (broche, valeur)** : Elle permet quant à elle l'écriture d'une valeur sur une broche analogique généralement les 9, 10 ou 11.
- **Entrées/sorties numériques de D0-D13**
  - **digitalRead (broche)** : sert à la lecture de l'état assigné à la broche
  - **digitalWrite (broche, valeur)** : assignation d'une valeur sur une broche
  - **pinMode (broche, état)** : définition par écriture d'un état sur la broche
  - **unsigned long pulseIn (broche, état)** : lecture d'une impulsion au niveau de la broche.
- **Temps**
  - **delay (ms)** : temps d'attente en millisecondes
  - **delayMicroseconds (us)** : attente en millisecondes
  - **Unsigned long millis ()** : période d'activité du programme

2.1.3.4 Bibliothèque

Dans cette partie nous décrirons comment se structure la bibliothèque d'arduino, sa gestion, son intégration et ses différentes fonctionnalités.

Tout d'abord, commençons par dire que cette dernière dépendra du projet à réaliser puisqu'on n'a pas des ressources standards fonctionnant avec tous les montages.

L'interfaçage de notre carte et des dispositifs ou composants (capteurs, keypad, webcam, …) se fera par cette librairie . La plus importante est celle qui permet de faire la communication entre la carte et le programme (qui est un code) qu'on établira à travers les broches qui se nomment : SoftwareSerial. Ce code se trouve sous forme généralement avec le symbole « # » devant comme ceci :

- **Structure d'une librairie :**

```
#include <Keypad.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
```

L'écriture en verte permet juste d'inclure la librairie et celle en orange désigne le nom de la librairie, 'keypad' est celle liée au keypad à titre d'exemple.

Elle permet enfin par la suite les rôles suivants à travers les fonctions :

SoftwareSerial (rx Broche, tx Broche)

- **begin ():** sert de fixer la vitesse de la communication série
- **read ():** Lire un caractère sur la broche en réception sur le port série logiciel
- **print ():** sert d'afficher dans une fenêtre Terminal les données émises par la broche d'émission du port série logiciel.
- **println ():** sert d'afficher dans une fenêtre Terminal les données émises par la broche d'émission du port série logiciel, avec un saut de ligne [20].

2.2 La caméra

Le choix de la camera a gagné la majeure partie de notre réalisation, car ayant débuté avec celle de 5 Mpx nous avons atteint jusqu'à celle de 24 Mpx du coup on a essayé jusqu'à 5 webcams avant de tombées sur la bonne. Le problème ne se situait pas en fait au niveau de la résolution, mais de la qualité des webcams lors de l'acquisition des images. Nous avons utilisé une webcam de la marque Mac Tech de Modèle MT-WC404.

2.3 L'éclairage

L'éclairage est un facteur très important dans le traitement d'image puisqu'elle agit sur les pixels afin de les rendre plus clairs ou sombre. Nous avons utilisé une ampoule LED de 4W blanc extra plat de 12mm d'épaisseur afin d'être repartis un peu partout dans la maquette, mais l'ajustement du paramètre de luminosité a été un casse-tête durant cette réalisation.

Figure 3.4 Image de la LED 5W blanche utilisée

2.4 L'afficheur LCD

L'afficheur LCD (Liquid Crystal Display) utilisé dans cette réalisation est celui de 16x4 c'est-à-dire seize (16) colonnes et quatre (4) lignes connectées au module I2C afin de réduire le câblage lors du montage, car le module I2C permet directement d'avoir quatre (4) sorties au lieu de seize (16) pour le LCD_16x4. Ci-dessous le montage

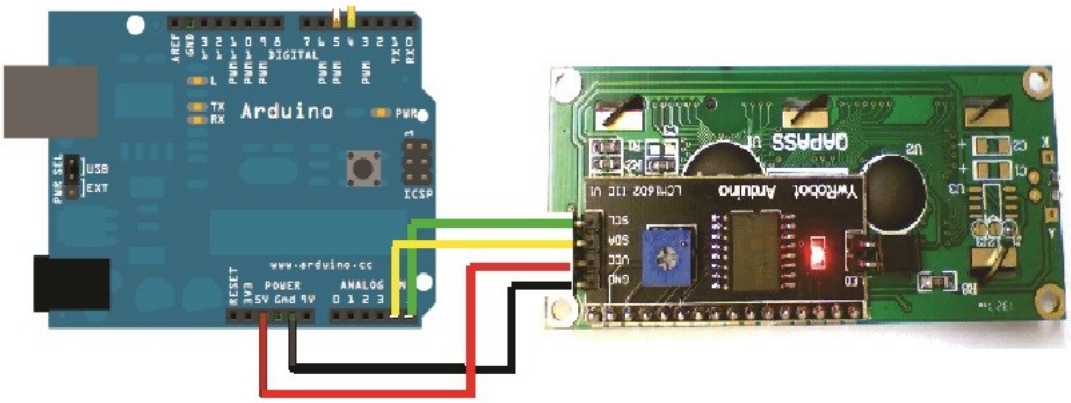


Figure 3.5 Schémas du montage du LCD avec le I2c à la carte arduino

Les différents ports de liaison de l'écran LCD avec l'arduino sont résumés dans le tableau ci-dessous :

Tableau 3.3 les ports de connexion entre l'écran LCD et l'arduino

Broches Arduino	Broches LCD_I2C 16 x 4
5V	**VCC**
GND	**GND**
A4	**SDA**
A5	**SCL**

2.5 Réalisation de la maquette

Il s'agit d'un boîtier fait en planche de bois d'une hauteur de 57cm qui permet de prendre une bonne image de la main via la webcam qui est implémentée au fond du boîtier et une circonférence de 22,5 cm carrés qui correspond avec la largeur maximale de la main humaine. Ce dernier est peint avec une peinture noire, car celle-ci nous facilitera le temps de traitement de l'image donc le temps d'accès sera aussi minimum. En plus il possède une fenêtre rectangulaire avec un rideau noir favorisant le presque le noir absolu dans le boitier permettant à l'utilisateur d'insérer sa main lors des deux (2) étapes. La première permettant d'insérer les utilisateurs dans la base de données et la seconde lui autorisant l'utilisation de ce dispositif, ci-dessous les étapes de réalisations en images :

Figure 3.6 Les étapes de la réalisation de la maquette

❶ Dimensionnement des planches chez le menuisier
❷ Choix des clous afin de fixer les différentes parties
❸ Fixation des clous terminée
❹ Choix du bonbon de peinture de couleur noire
❺ L'intérieur est devenu noir après la peinture
❻ Choix du tissu de couleur noire couvrant le background de la maquette
❼ Finition de la maquette enfin prête

Figure 3.7 : Image de la maquette

III.3 La partie Software

3.1 Le logiciel MATLAB

L'acronyme désigne tout simplement « *matrix laboratory* » reconnu et utilisé dans plusieurs domaines tels que la télécommunication, la médecine, l'aéronautique, l'électronique, imagerie, l'économie et bien d'autres domaines assez vastes pour des calculs numériques. C'est un algorithme de dernière génération qui a été développé par la société The MathWorks et accepte les environnements actuels qu'on utilise à savoir Linux, Unix, Mac OS, Windows qui explique son utilisation sous licence. Notons que plusieurs fonctions présentes dans les avions ont été codées par ce dernier [21].

Il possède un environnement assez chargé, mais pour des bonnes raisons vues les fonctionnalités qu'il offre et peut être utilisé avec la boîte à outils communément appelée « *TOOLBOX* » dans matlab ou bien seul comme dans notre cas.

3.2 Traitement de l'image

Nous avons développé un algorithme qui aide à faire ressortir 24 éléments de la main d'une personne appelée vecteur caractéristique et l'afficher sous forme matricielle de [24,1] c'est-à-dire une colonne et 24 lignes après avoir détecter les contours et les coordonnées de cette main.

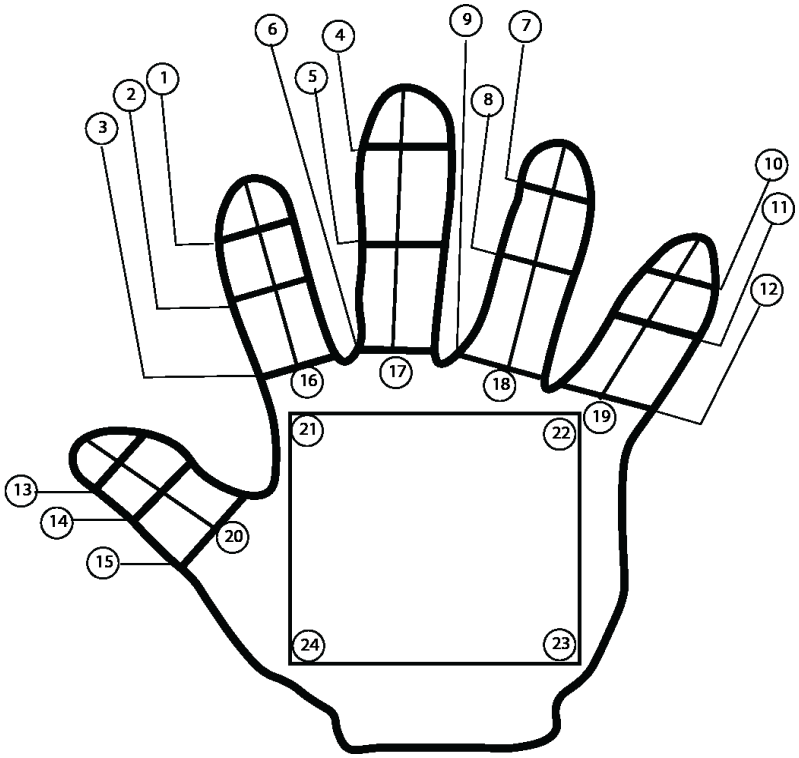


Figure 3.8 : Les éléments caractéristiques de la main

3.2.1 L'acquisition de l'image

Dans cette première partie, l'utilisateur est amené à insérer sa main dans le boîtier tout en écartant sa main, mais aussi en touchant le bouton qui est juste au-dessus de la paume de sa main afin que ça soit automatique lors de son accès. Ce geste sera fait trois (3) fois afin qu'on ait de valeurs assez larges de la forme de sa main pour une reconnaissance assez rapide lors de l'utilisation. Nous avons décidé de créer une base afin d'être sûr de notre dispositif comportant 60 images différentes provenant de 20 sujets entre autres des enseignants, des étudiants, des camarades, mais surtout des deux sexes et dont la tranche d'âge varie entre 18 - 55ans. Avant d'avoir une telle position, nous avions dû adopter une rotation de ladite main afin d'avoir une

bonne normalisation. Il s'agit de faire pivoter l'image de seconde diagonale et ça se fait par la syntaxe suivante : $X1 = symmus(X, ps)$ avec 'X1' étant l'image originale et 'ps' la symétrie à choisir qui est 'D2' dans notre cas. L'affection de l'heure de pointage s'effectue avec la fonction MATLAB comme suit : *DateString = datestr(t)*, il suffit de définir le « *t* » comme étant le temps de l'acquisition donc par le mot « now » qui signifie « maintenant » en anglais. Nous avons l'organigramme ci-dessous qui explique le processus de cette étape

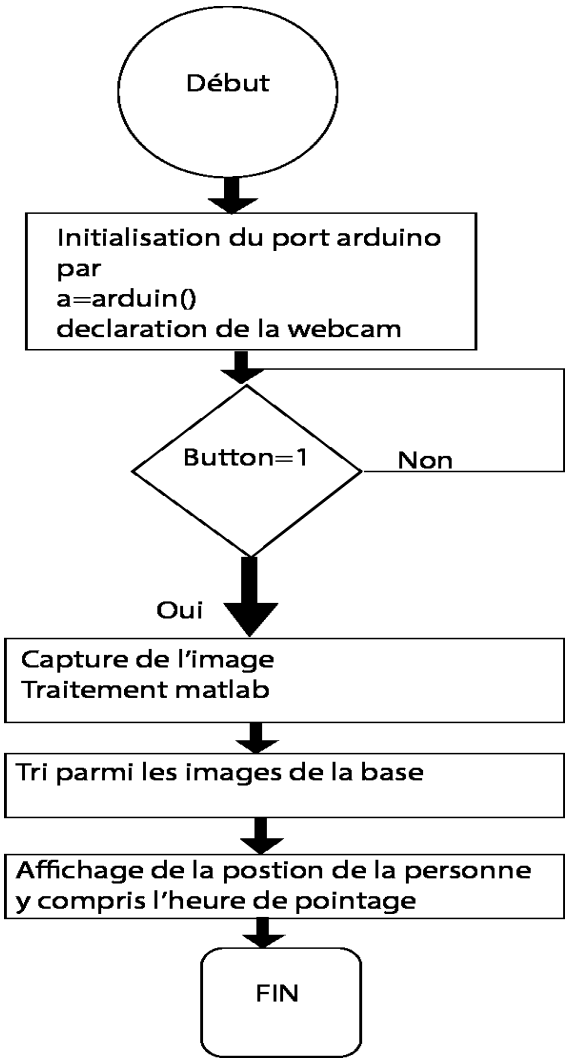


Figure 3.9 : Organigramme sur Matlab du traitement

Les images provenant de la base que nous avions créée

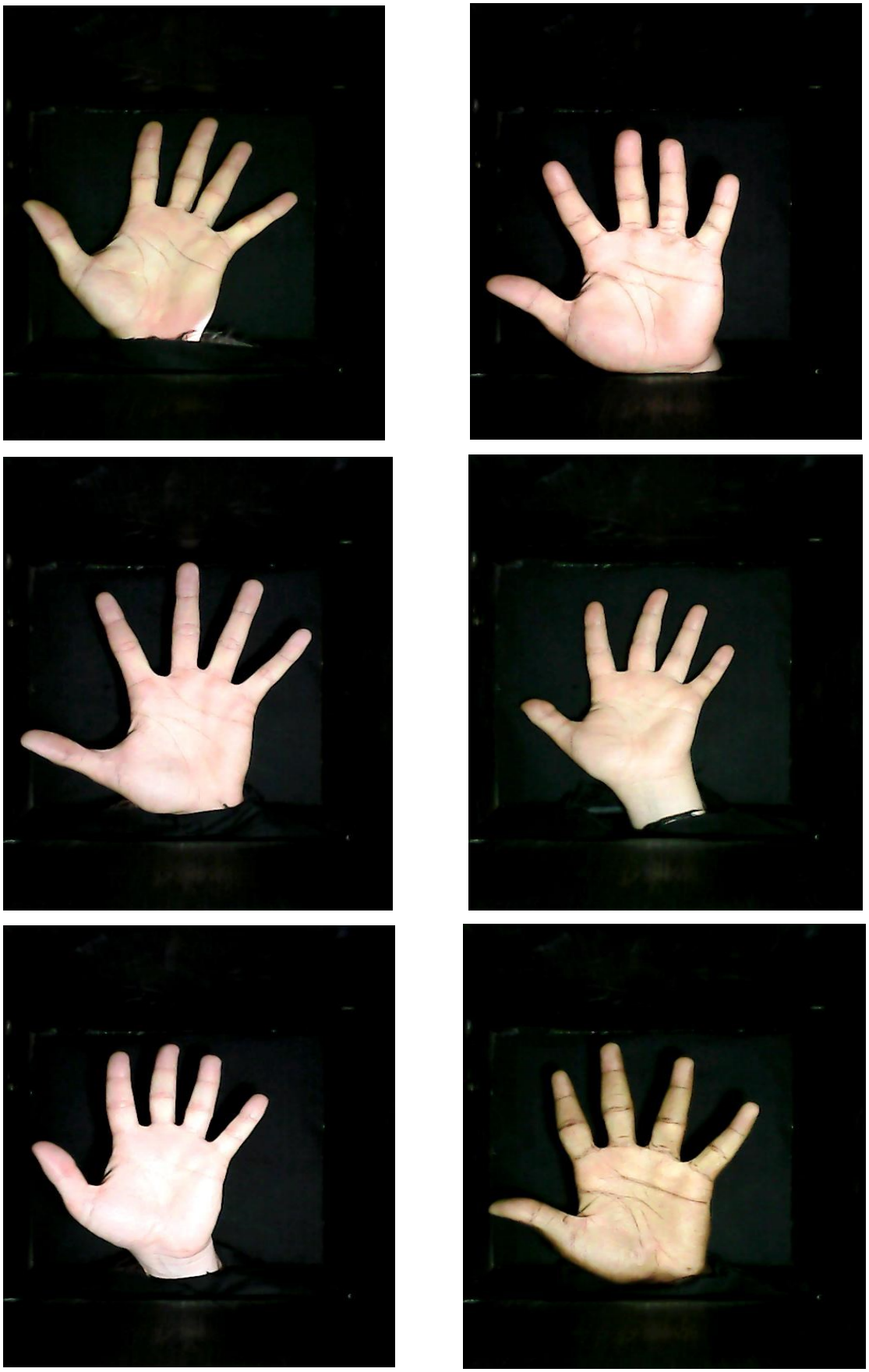


Figure 3.10 les échantillons des images des mains provenant de la base créée.

3.3 Fonctions de similarités

Notre système est sensé reconnaitre les personnes existantes dans la base afin de les donner accès au moment voulu, mais surtout de pouvoir rejeter ceux qui n'en font pas partie de cette dernière. Pour cela plusieurs méthodes de calculs nous permettent de faire le bon choix de la marche à choisir lors de cette implémentation. Il s'agira d'une étude de similarité entre deux vecteurs caractéristiques ou bien de divergences provenant des vecteurs caractéristiques de notre base [22].

3.3.1 La distance de Manhattan :

Elle est aussi appelée taxi-distance à cause des chemins suivis, est tout simplement une distance entre deux points A et B de coordonnées respectives (X_A, Y_A) et (X_B, Y_B) définies ainsi par :

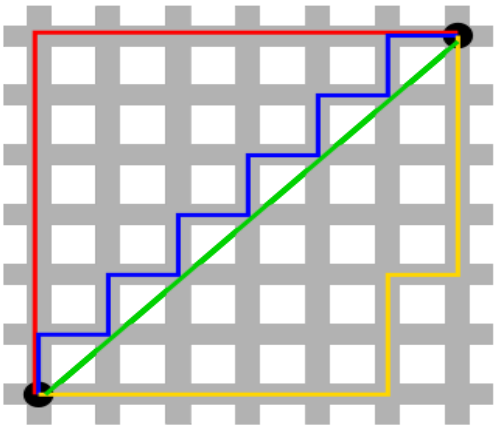


Figure 3.11 Trajets suivis par deux points

$$d(A,B) = |X_A - X_B| + |Y_B - Y_A| \qquad \textbf{(3.1)}$$

Cette égalité se traduit par la somme des valeurs absolues des deux différences entre les coordonnées du point A et celles du point B.

3.3.2 La distance de Minkowski :

Il s'agit d'une distance concernant l'ordre p entre deux points qui se définit par la formule suivante :

$$D(\mathrm{X},\mathrm{Y}) = (\sum_{i=1}^{n}|x_i - y_i|^p)^{1/p} \qquad \textbf{(3.2)}$$

Avec $X = (x_1, x_2, \dots, x_n)$ et $Y = (y_1, y_2, \dots, y_n) \in \mathbb{R}^2$ où quand le p ≥ 1, la distance entre le point (0,0) et (1,1) équivaut à $2^{1/p} > 2$. Toutefois, elle présente un inconvénient et ceci s'explique par le côté défavorisant lors de l'augmentation du p entraine aussi entre les points une augmentation de cette différence entre les coordonnées.

3.3.3 La distance de Tchebychev

On peut aussi l'appeler distance de Chebychev. Elle représente la distance maximale des coordonnées de deux points sur une dimension donnée.

Nous pouvons le voir dans la formule suivante :

On considère deux points respectifs

$(A_0, \dots, A_n)$ et $(B_0, \dots, B_n)$ tels que

$$d(A,B) = \max_{i\in[[0,n]]}(|A_i - B_i|) \text{ Qui est une distance des normes} \quad \textbf{(3.3)}$$

infinies et en même temps à ce niveau elle équivaut à la distance de Minkowski.

3.3.4 La distance de Hamming

Elle est utilisée généralement dans le codage de canal dans une chaine de transmission afin de prendre en compte certaines erreurs lors du transport. Les messages transmis sont supposés découpés en blocs (ou mots) de longueur n écris avec l'alphabet {0,1}. On dit que n est la longueur de C. Cette distance se calcul entre deux mots $x = (x_1, \dots, x_n)$ et $y = (y_1, \dots, y_n)$ tel qu'on notera $d(x,y)$ étant le nombre d'indices i tels que $x_i \neq y_i$

La distance minimale du code C est le minimum des $d(x,y)$ pour x et y des mots différents de C (on suppose que C a au moins 2 mots). On la notera toujours d. Le code linéaire est ainsi noté. $C(n,k,d)$.

Exemple : Considérons C = $C = \{C_0C_1C_2C_3\}$ avec C_0= (00000); C_1= (10110); C_2= (01011); C_3= (11101). C'est un code de longueur 5 et de distance. $d = 3$.

Notons que le poids de hamming correspond au nombre d'éléments non nul ($\neq 0$) dans une chaîne d'élément.

3.3.5 La distance euclidienne

On s'adapte généralement à l'utilisation de cette distance vu son intérêt dans nos différents traitements dans plusieurs types de plans à savoir le 2D, le 3D puisqu'il fournit une distance géométrique, car son p vaut 2 (p étant l'ordre de la distance) qui est la norme euclidienne. Elle s'exprime sous cette forme :

$$d(X,Y) = \sqrt{\sum_{i=1}^{n}(y_i - x_i)^2} \quad \textbf{(3.4)}$$

3.3.6 La similarité Cosinus

Il s'agit là d'un facteur très important, car elle est utilisée généralement dans la fouille de texte pour relever les ressemblances entre ces derniers. Elle facilite le calcule de similarité entre deux vecteurs à. n dimensions par la détermination bien évidemment de l'angle séparant les deux vecteurs par cette expression :

$$\cos\theta = \frac{A.B}{||A||\,.\,||B||} \qquad \textbf{(3.5)}$$

Nous remarquons à travers cette expression que plus l'angle est petit plus la similarité entre ces deux-points A et B est grande c'est-à-dire s'approchant de 1.

3.3.7 Le coefficient de corrélation

Permettant d'étudier le rapport existant entre deux ou plusieurs variables de manière générale. Ainsi il peut être négatif ou positif, car il est compris entre -1 et +1. C'est une fonction utilisée fréquemment en statistiques. Nous avons un petit tableau qui peut résumer ses états ci-dessous [23] :

Tableau 3.4 Types de corrélation et leurs valeurs

Type de corrélation	Forte	Faible
Négative	**-1,0 à -0,5**	**-0,5 à 0,0**
Positive	**0,5 à 1**	**0,0 à 0,5**

Ce coefficient est déterminé par la formule suivante :

$$r = \frac{Cov(X,Y)}{\sigma_X \sigma_Y} \qquad \textbf{(3.6)}$$

Avec la $Cov(X,Y) = \frac{E(XY)-E(X)E(Y)}{\sigma_X \sigma_Y}$ désigne tout simplement la covariance **(3.7)**

des variables $X, Y, \sigma_X \; et \; \sigma_Y$ muni de leurs écarts types et E() qui signifie l'espérance mathématique.

3.3.8 Le coefficient de corrélation de rang Spearman

Elle est communément appelée rho (ρ) ou r_s et permet surtout de faire l'étude des liens existants entre deux variables quantitatives sans que ces dernières n'aient pas la même forme affine, mais généralement curviligne c'est-à-dire permet d'observer leurs rangs d'observations. Il est compris entre 1 qui est le maximum signifiant qu'il s'agit d'une variation simultanée dans le même sens et -1 indiquant une variation simultanée en sens inverse [24] on peut le déterminer par cette expression :

$$\rho = 1 - \frac{6\sum D^2}{n(n^2-1)} \qquad \textbf{(3.8)}$$

Avec n étant la taille de l'échantillon et $\sum D^2$ Qui est la somme des différences au carré. Nous avons ci-dessous un récapitulatif qui illustre la signification des valeurs [25].

- ✓ $0{,}0 < \rho < 0{,}5$: Très faible
- ✓ $0{,}5 < \rho < 0{,}7$: Faible
- ✓ $0{,}7 < \rho < 0{,}8$: Modéré
- ✓ $0{,}8 < \rho < 0{,}9$: Élevé
- ✓ $0{,}9 < \rho < 1{,}0$: Très élevé

Soulignons qu'il ressemble à celui de PEARSON, mais la différence réside aux nouvelles valeurs numériques en d'autres termes le coefficient de PEARSON est calculé avec des données brutes alors que celui de Rho Spearman sur les rangs d'échelles ordinaires comme sur l'organigramme suivant :

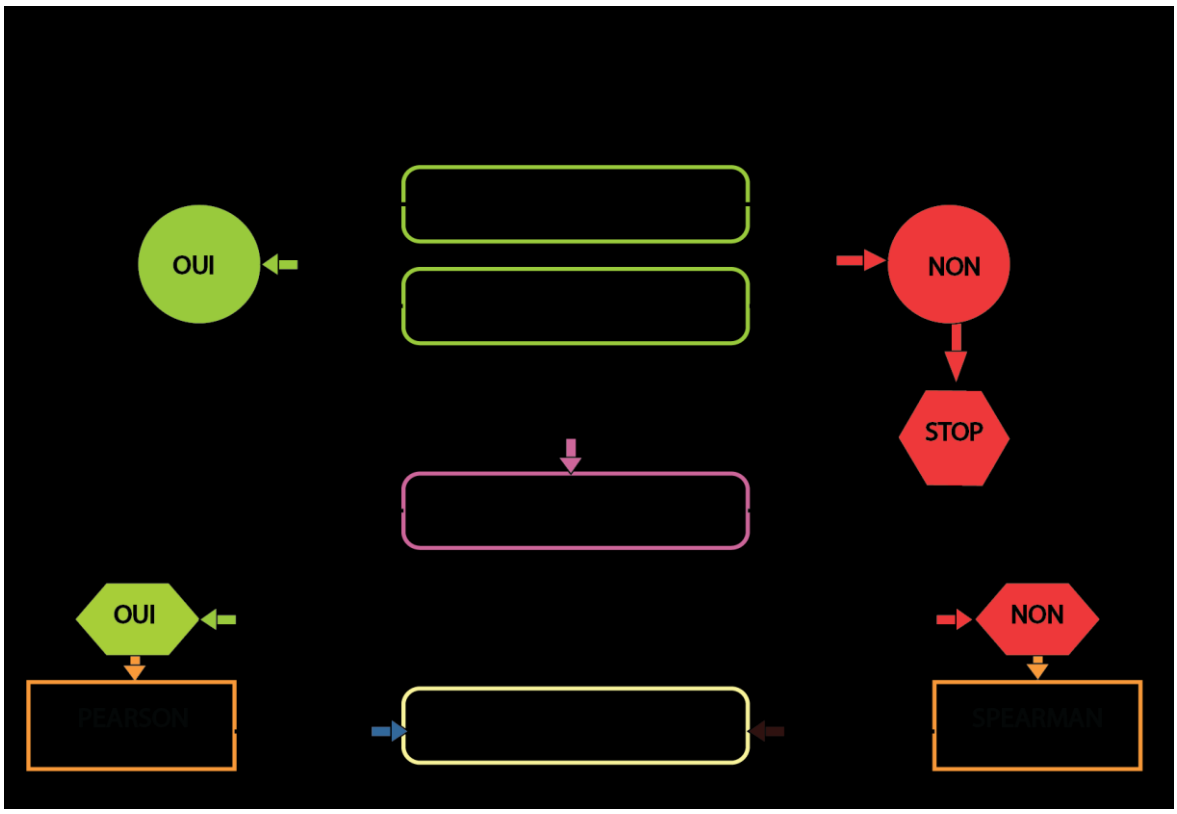


Figure 3.12 Différences entre PEARSON et SPEARMAN

3.4 Évaluation de la vérification

Généralement lors de la vérification effectuée par un système nous nous confrontons à deux types de situations :

- Rejeter un utilisateur légitime, là on parle de faux rejet (false rejection)
- Accepter un imposteur (intrus au système), là il s'agit de fausse acceptation.

Pour mesurer la performance d'un système on fait recours à deux (2) taux celui du faux rejet (False Rejection Rate ou FRR) et celui de fausse acceptation (False Acceptance Rate ou FAR) [26].

Du coup les hypothèses suivantes peuvent être évoquées :

$H0$: l'image de la main provient d'un imposteur

$H1$: l'image de la main provient de la personne légitime c'est-à-dire appartenant à notre base.

Ceux-ci nous permet d'établir la loi de Bayes en prenant C comme l'image provient d'un utilisateur légitime donc $P(H_1/C) > P(H_0/C)$ ce qui donne

$$\frac{P(H_1/C)\,\mathrm{P}(H_1)}{P(C)} > \frac{P(H_0/C)\,\mathrm{P}(H_0)}{P(C)} \Rightarrow \frac{P(C/H_1)}{P(C/H_0)} > \frac{P(H_0)}{P(H_1)} \qquad \textbf{(3.9)}$$

On compare ce taux $\frac{P(H_1)}{P(H_0)}$ par un seuil de décision nommée θ nous permet de dressé la figure suivante qui donne le taux de vraisemblance en fonction de la probabilité des FAR et FRR.

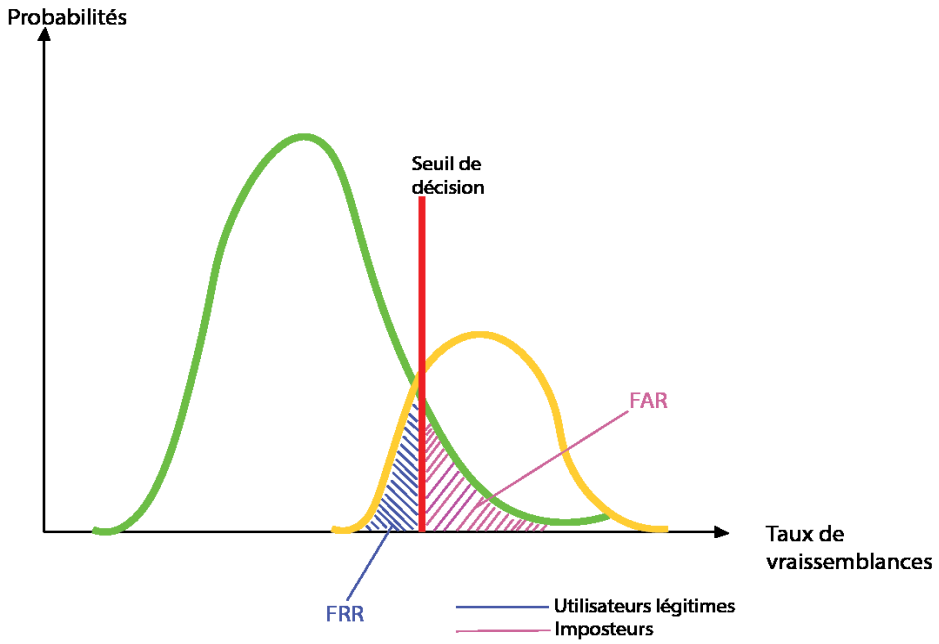


Figure 3.13 : Taux de vraisemblance des utilisateurs légitimes et des imposteurs

Nous choisissons un compromis entre le FAR et le FRR comme il est impossible en pratique d'avoir la valeur 0 pour les deux paramètres, donc si on augmente l'un des taux l'autre diminue et vice versa.

Cette performance est représentée par la courbe ROC (Receiver Operating Charactristic) pour les différentes valeurs de θ , le taux de faux rejet en fonction du taux de fausse acceptation ci-dessous :

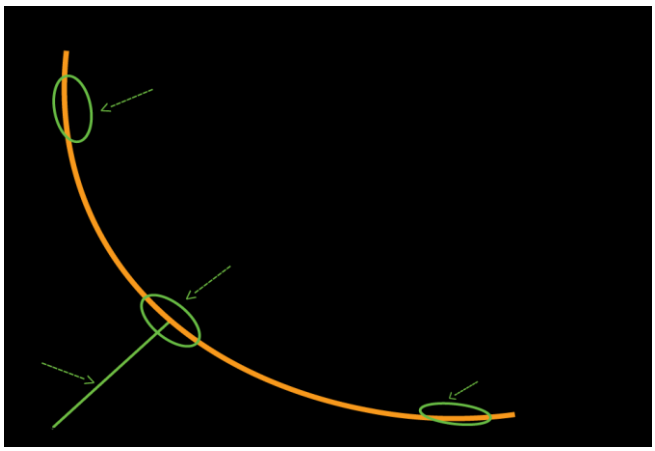


Figure 3.14 : Courbe ROC

En analysant cette courbe ROC, on remarque que plus la courbe tente de toucher le repère plus le système est performant, donc un taux assez considérable. Le taux d'erreur EER (Equal Error Rate) correspond au point où FAR=FRR.

III.4 Conclusion

Dans ce chapitre, nous avons eu à élaborer les différentes étapes de la réalisation en passant par la partie software de notre système biométrique, mais aussi une description brève des différentes distances qu'on utilisera dans le chapitre. Toutefois, gardons que la méthode d'évaluation du système biométrique est d'une importance capitale, car le choix du seuil θ se repose essentiellement sur le type de système qu'on veut obtenir, c'est-à-dire par niveau de sécurité.

IV.1 Introduction

Après la réalisation de notre maquette, nous passons dans la suite de ce travail aux ‘analyses des résultats issus des traitements effectués sur notre base de données issu de la biométrie de la forme de la main. Ces résultats proviennent essentiellement, de différentes méthodes de calcul de distance ayant été évoquées dans le chapitre précédent, ainsi que différentes dispositions des vecteurs caractéristiques.

IV.2 Traitement des images acquises par la webcam

À ce niveau notons qu’il va y avoir un prétraitement afin de mettre l’image en question dans les conditions d’être bien utilisé par la suite du programme pour aboutir au résultat final en passant par l’extraction de points caractéristiques. Les images ci-dessous illustrent les phases suivies par une image.

Figure 4.8 Image de la main originale

Figure 4.9 Image de la main segmentée

Le passage de l’image de la main originale vers l’image segmentée permet un meilleur traitement dans la suite des analyses. Par ailleurs, nous constatons toutefois comme énoncé ci-haut que le fond noir de la maquette nous facilite la segmentation qui est une transformation de l’image couleur vers une image binaire c’est-à-dire une image qui comporte uniquement de la noire et blanche tout en passant par le niveau de gris.

Il permet quant à lui de transformer l'image couleur c'est-à-dire remplacer chaque pixel représentant les couleurs RGB (Red Green Blue) ou en français RVB (Rouge vert bleu) par une seule valeur de luminosité en utilisant simplement la fonction « *rgb2gray* () » comme sur cette image ci-dessous :

Figure 4.10 Image au niveau de gris

IV.2.1 Détection des points caractéristiques

Après l'acquisition et le traitement suivi par l'image elle sera dans cette étape utilisée dans le but de faire ressortir les points caractéristiques qu'on utilisera dans la suite du travail. Ils sont la base de notre travail, car tous ces eux qui représentent les personnes physiques au niveau de matlab pendant tout le traitement du début jusqu'à la fin.

Figure 4.11 Squelettes de la main +rotation

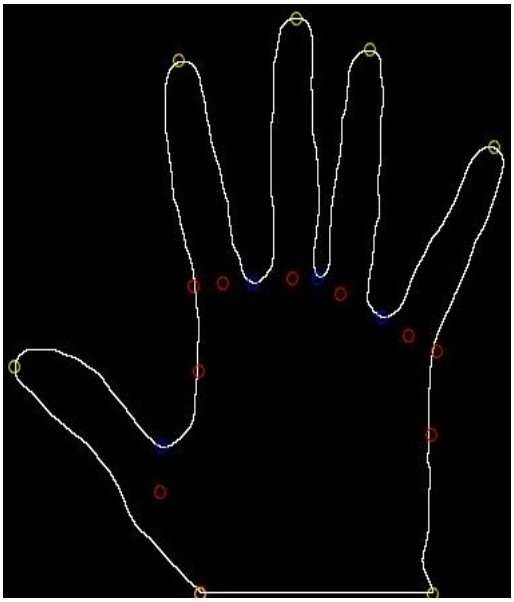


Figure 4.12 Contour de la main + points caractéristiques

L'image (**Figure 4.11**) nous décrit le squelette de la main après avoir suivie une rotation et une éventuelle normalisation pour qu'elle soit adaptée à toutes les mains.
Pour celle de (**Figure 4.12**), comporte en elle le contour en trait blanc et les différents points caractéristiques qui sont en points jaunes, bleu et rouges donnent les coordonnées de la dimension de la main, la largeur, la longueur, les aspects de doigts de la paume de la maison et plusieurs informations. Nous choisissons les points qui nous mèneront à notre but.

IV.3 Résultats expérimentaux

Dans cette partie, nous détaillerons les différents résultats issus de l'application méthodes de calcul sur la base choisies après le traitement sur MATLAB à propos des similarités des distances citées ci-haut qui sont appliquées sur notre base des données pour la géométrie de la main et voir si les nous sommes dans la même longueur d'onde que la description faite.

Tableau 4.1 Les résultats des différentes méthodes de similarités appliquées à notre propre base

Différentes méthodes	myint	maxin	minin	stdint	myex	minex	maxex	stdext	EER
Euclidien	30,2005	81,4248	7,0711	15,8037	72,3507	22,1359	171,3359	23,8071	0,1333
City Block	102,6000	284	24	57,3583	240,2509	80	600	79,8492	0,1496
Minkowski	30,2005	81,4248	7,0711	15,8037	72,3507	22,1359	171,3359	23,8071	0,1333
Cosine	5,0316e-04	0,0018	1,44e-04	4,2703 e-04	0,0041	3,4869e-04	0.0174	0,0027	0,0539
Corrélation	0,0013	0,0040	3,31e-04	0,0011	0,0098	8,3670e-04	0,0411	0,0065	0,0829
Spearman	0,0086	0,0222	0,0031	0,0058	0,0283	0,0052	0,0877	0,0130	0,1351
Chebychev	16,8167	47	4	8,9053	41,3035	10	88	14,3339	0,1439

Avec :

(myint) : Moy.Intra Classe
(maxin) : MaxIntra Classe
(minin) : MinIntra Classe
(stdint) : Écart type Inter class
(myex) : Moy.Extra Classe
(minex) : MinExtra Classe
(maxex) : MaxExtra Classe
(stdext) : EcartTypeExtra Class

Nous présenterons par la suite juste ci-dessous les résultats de nos différentes utilisations des méthodes sous forme graphique.

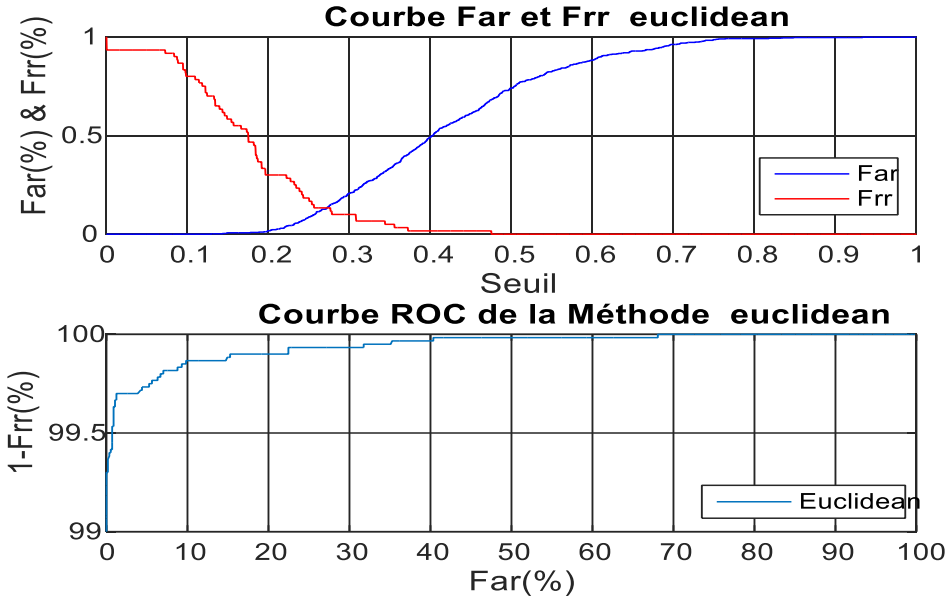


Figure 4.1 La courbe Far, Frr et ROC de la méthode euclidienne

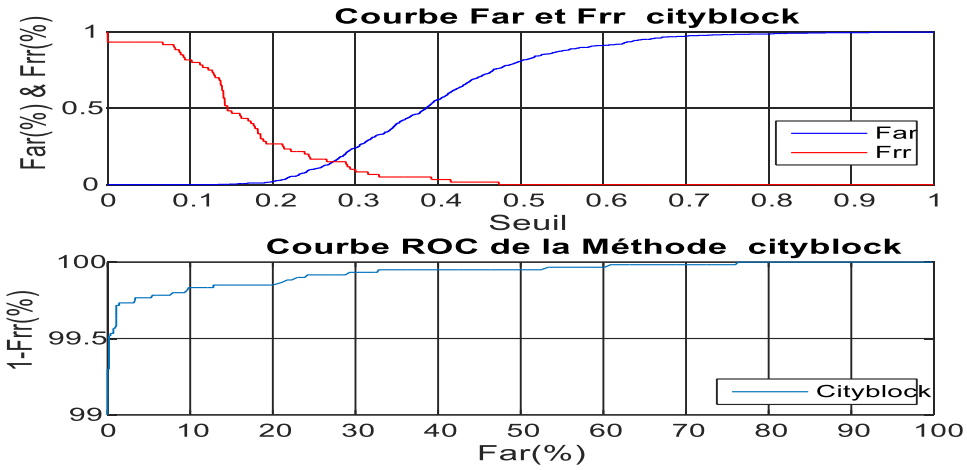


Figure 4.2 La courbe Far, Frr et ROC de la méthode City Rock c'est-à-dire celle de Manhattan

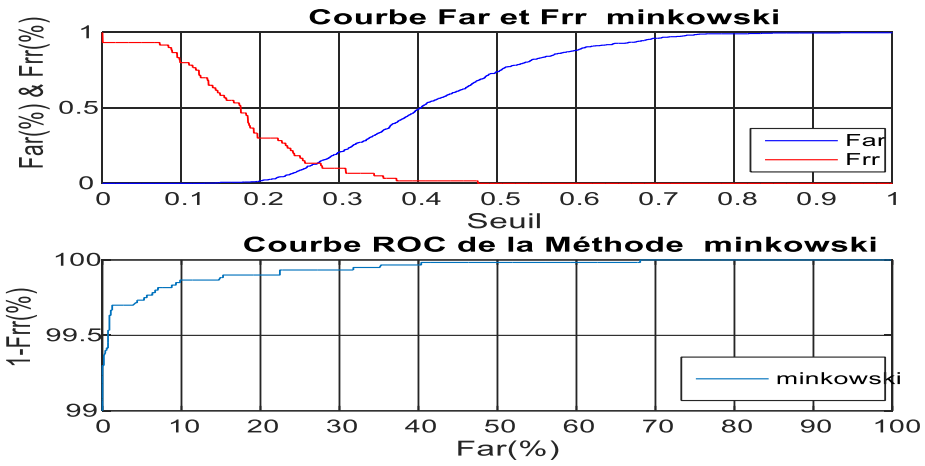


Figure 4.3 Courbes Far, Frr et ROC de la méthode de Minkowski

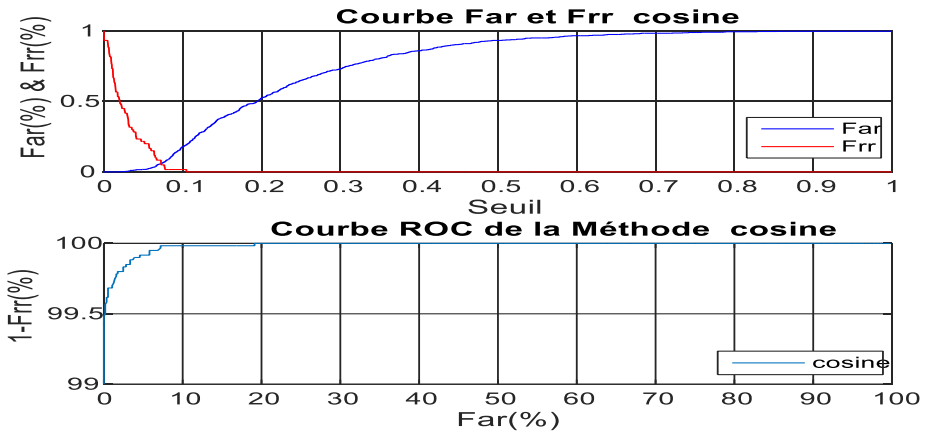


Figure 4.4 Courbes Far, Frr et ROC de la méthode de cosine

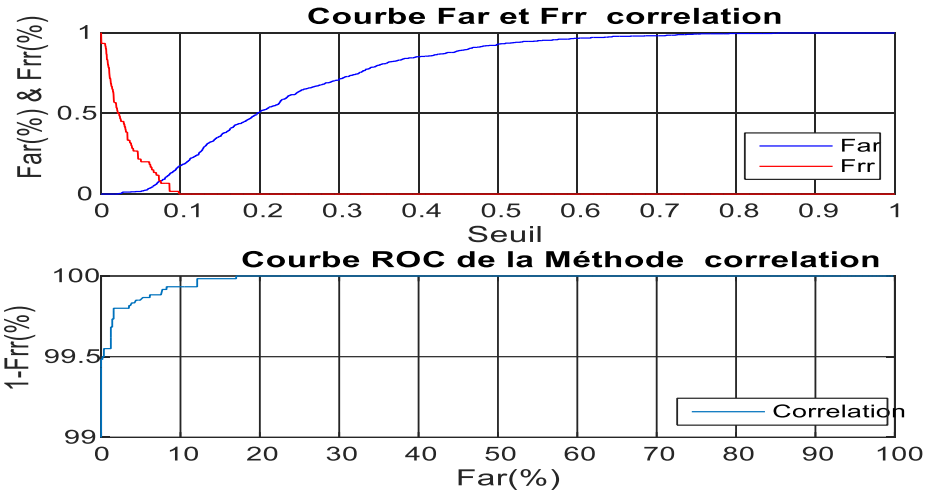


Figure 4.5 Courbes Far, Frr et ROC de la méthode de Corrélation

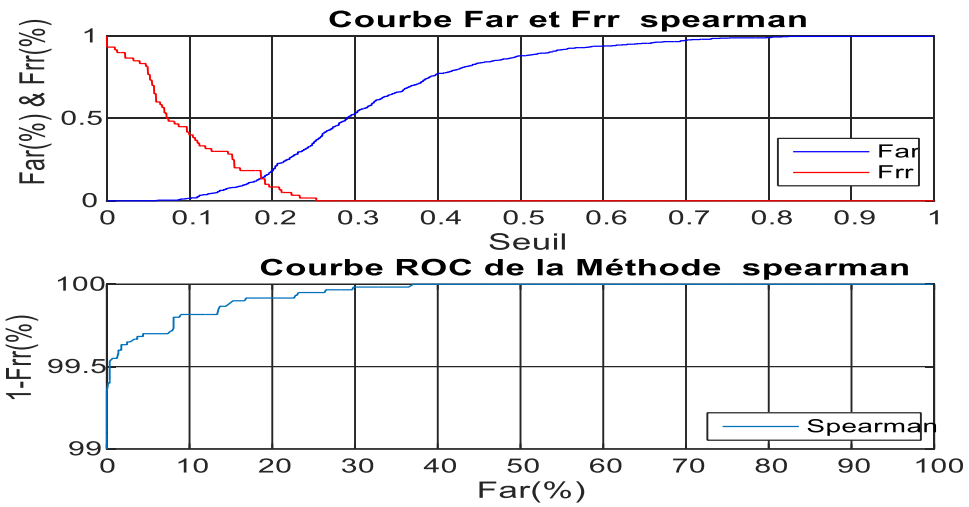


Figure 4.6 Courbes Far, Frr et ROC de la méthode de Spearman

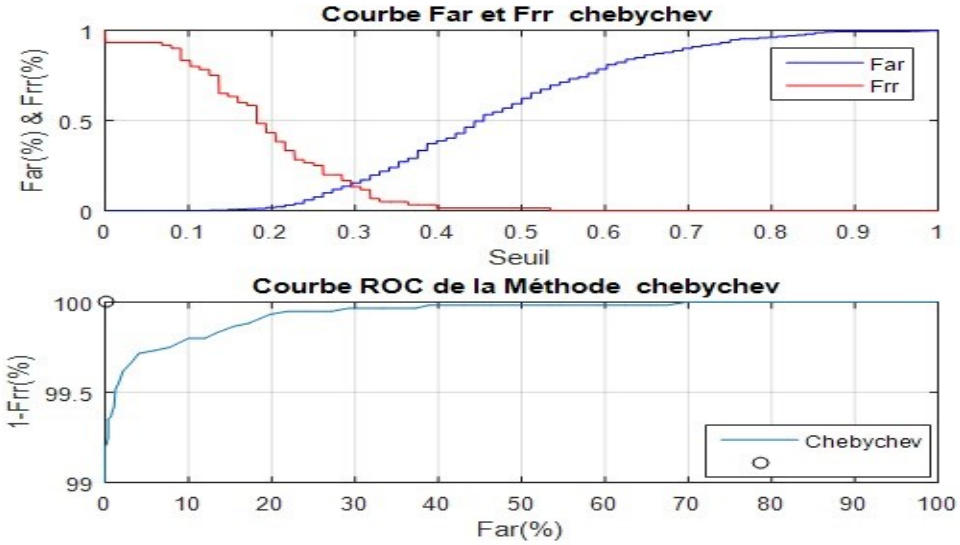
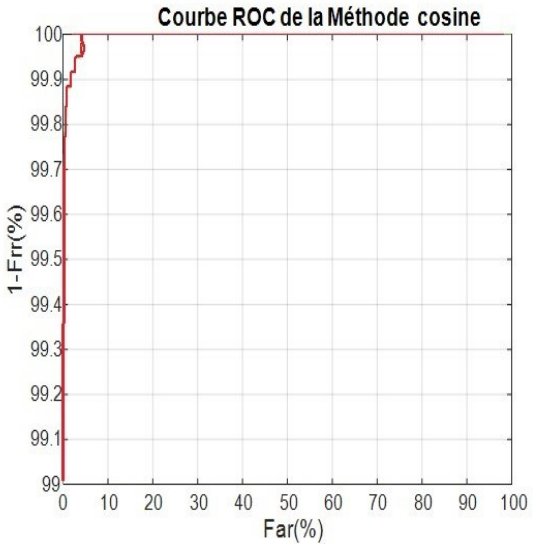


Figure 4.7 Courbes Far, Frr et ROC de la méthode de Chebychev

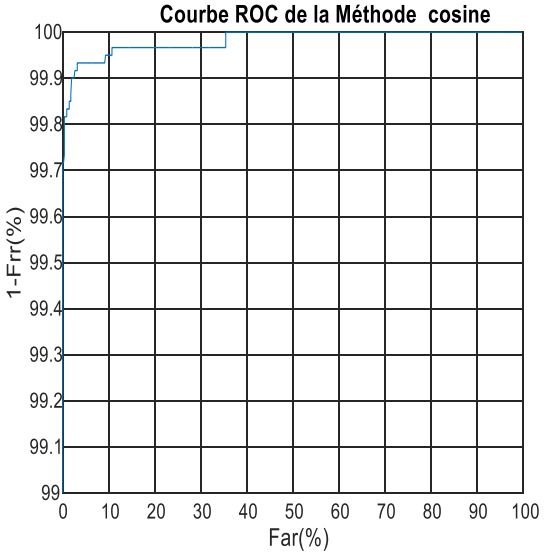
Notons que la méthode de Cosine offre la meilleure performance 0,0539 et aussi nous constatons qu'à travers aussi ses représentations comme nous l'avons énoncé ci-haut que les méthodes de Cosine et Spearman sont presque les mêmes.

IV.3.2 Application des méthodes de calcul sur des positions différentes :

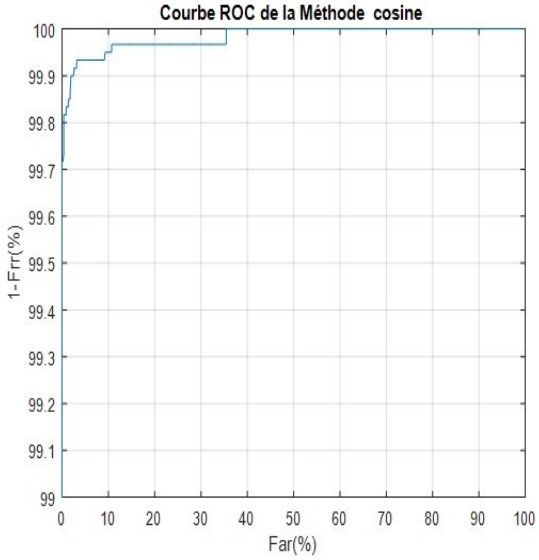
Au niveau de cette étape, on a simulé différentes positions de distances afin de voir la variation du taux d'erreur EER dans la main, ce qui permettra dans l'avenir de faciliter la conception d'un tel système à des services bien définis. Puisque nous devrons garder à l'esprit que l'être humain est soumis à plusieurs tentations au cours de la vie, telle que des maladies (cancers), des accidents qui le prive de certaines parties de son corps à savoir la main. Il peut perdre une partie un ou plusieurs doigts donc avec cette méthode on peut aussi l'inclure dans même système avec des personnes sans handicapes.



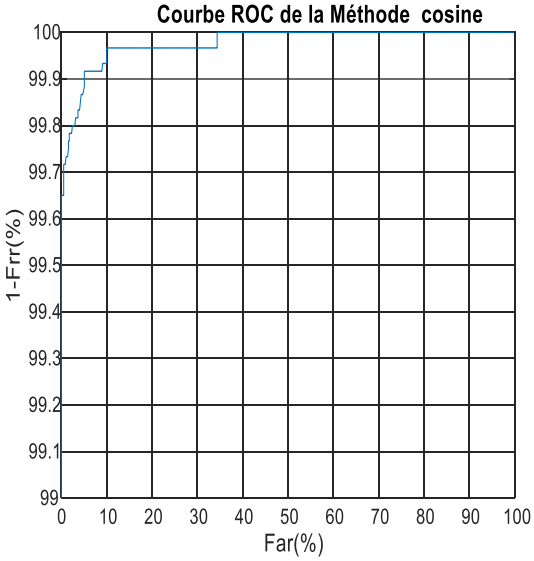
(1)



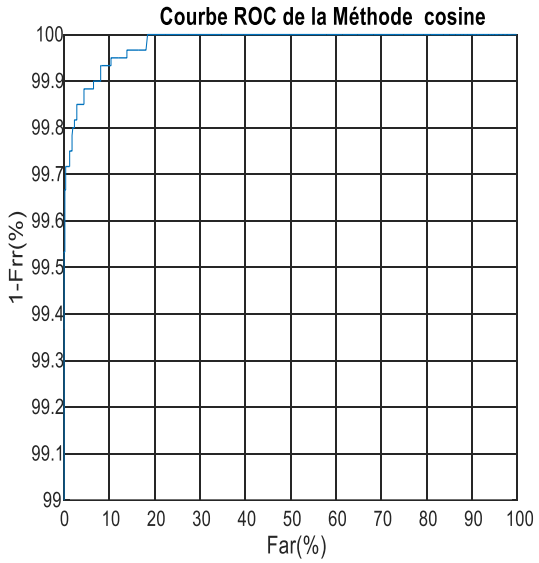
(2)



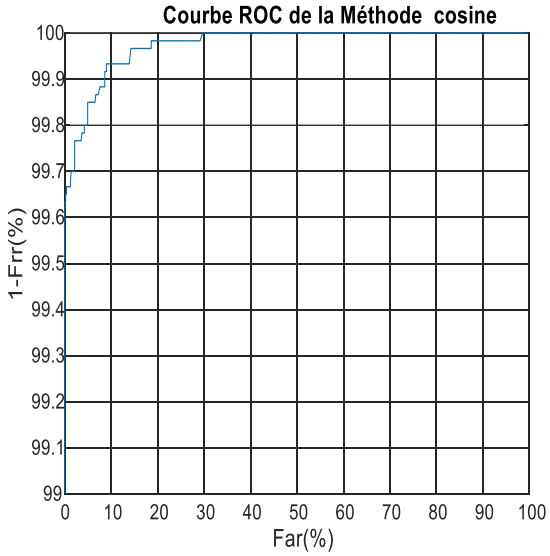
(3)



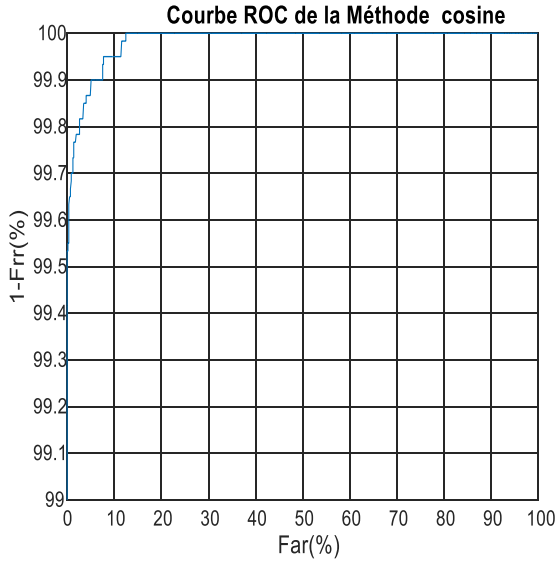
(4)


Courbe ROC de la Méthode cosine
1-Frr(%)
Far(%)

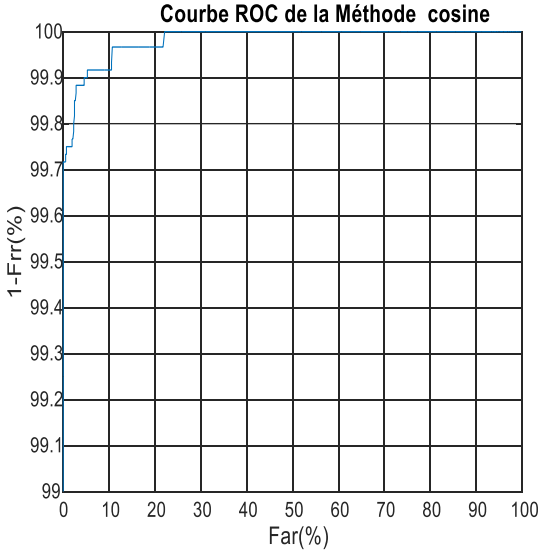
(5)


Courbe ROC de la Méthode cosine
1-Frr(%)
Far(%)

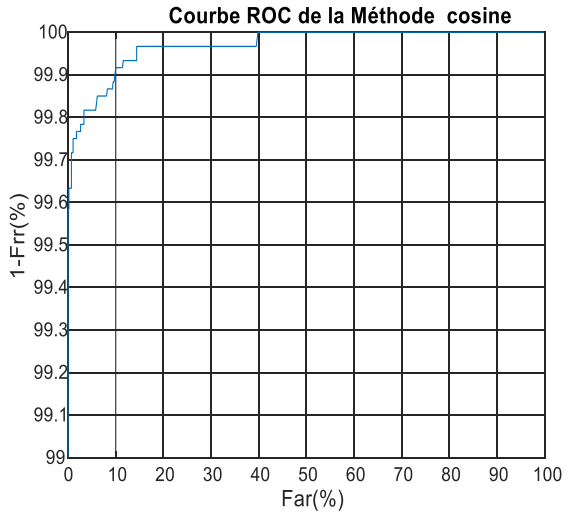
(6)


Courbe ROC de la Méthode cosine
1-Frr(%)
Far(%)

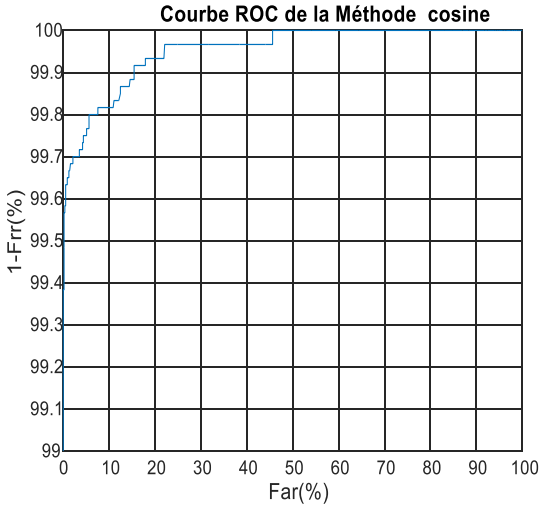
(7)


Courbe ROC de la Méthode cosine
1-Frr(%)
Far(%)

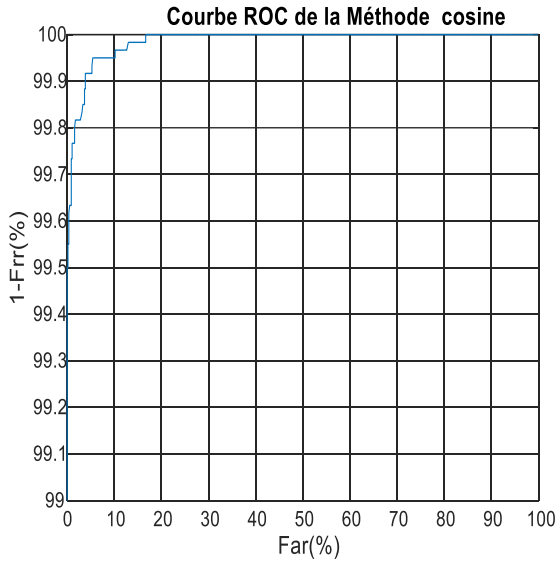
(8)


Courbe ROC de la Méthode cosine
1-Frr(%)
Far(%)

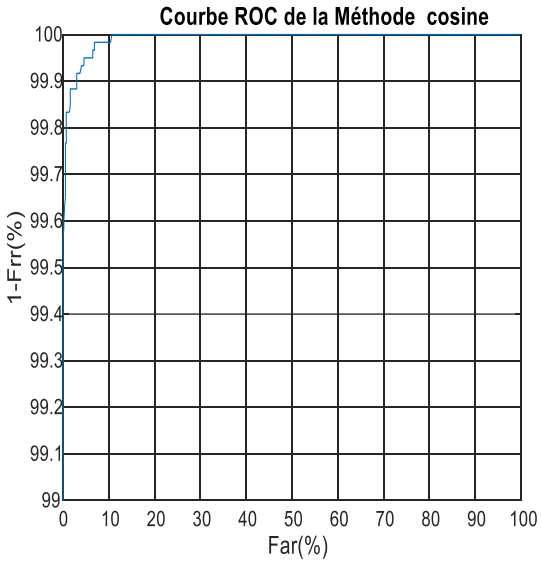
(9)


Courbe ROC de la Méthode cosine
1-Frr(%)
Far(%)

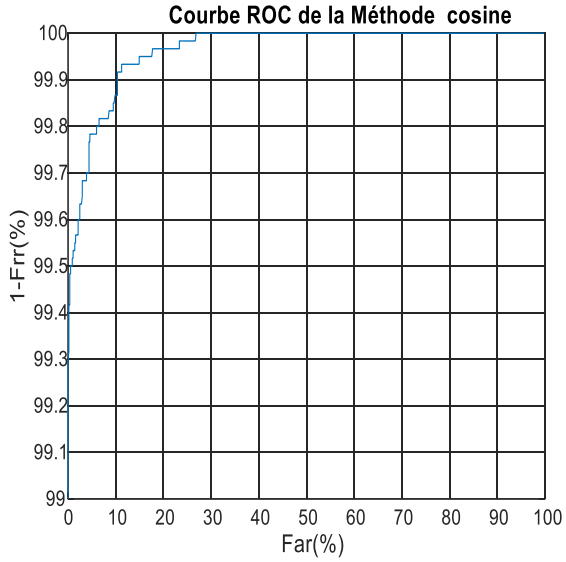
(10)



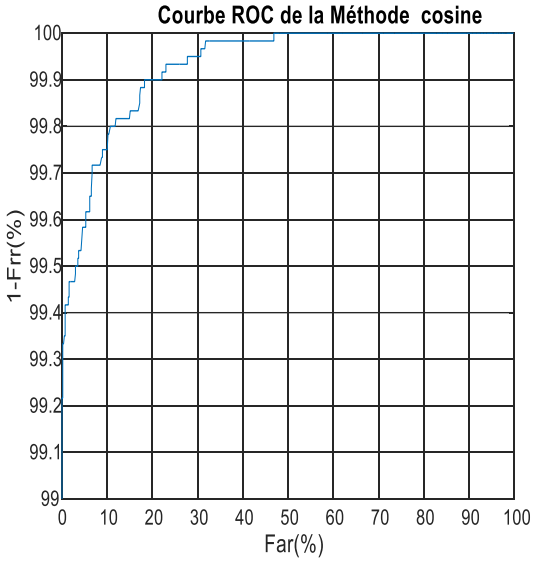
(11)



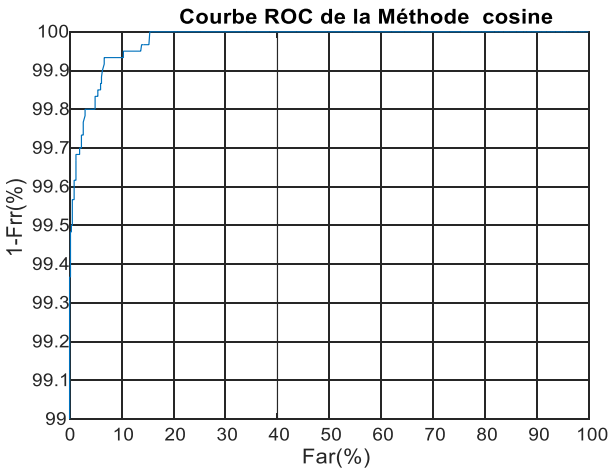
(12)



(13)



(14)



(15)

Figure 4.13 : (1) à (15) les différentes positions de la courbe ROC en fonctions des distances choisies.

Tableau 4.2 : Taux d'erreur en fonctions des positions de distances prises

Positions de calcul par méthode de cosine pour les graphes de ROC	Taux d'erreur
(1)--15 premières valeurs	0,1000
(2)--18 premières valeurs	0,0368
(3)--19 premières valeurs	0,0667
(4)--20 premières valeurs	0,0838
(5)--21 premières valeurs	0,0737
(6)-- 20 premières valeurs +21^{ième}-22^{ième}	0,0846
(7)-- 20 premières valeurs +21^{ième}-24^{ième}	0,0711
(8)-- 20 premières valeurs +21^{ième}-23^{ième}	0,0838
(9)-- 12 premières valeurs +13^{ième} -17^{ième} et 16^{ième}-20^{ième}	0,0917
(10)--12 premières valeurs +13-17^{ième} ,16^{ième} - 18^{ième}	0,1325
(11)--16 valeurs	0,0522
(12)--17 valeurs	0,5044
(13)--12 valeurs	0,1101
(14)--9 valeurs	0,1667
(15)--9 premières valeurs +16^{ième} ,17^{ième} et 18^{ième}	0,0667

Nous remarquons qu'avec la position qui correspond à la courbe ROC (2) nous obtenons un meilleur taux d'erreur celui de 0,0368 en prenant en compte que seulement dix-huit (18) valeurs de la main sur les 24 valeurs.

IV.4 Conclusion

En résumé par rapport à ces expériences faites avec notre propre base, nous obtenons des résultats vraiment intéressants et nous permet de nous mettre en confiance qu'il a été réalisé en tenant compte de plusieurs facteurs. Mais aussi l'application des méthodes nous a donné une idée sur leurs différences du point de vue calcul et la marge d'erreur qu'on peut obtenir et la meilleure restera toujours celle de cosine.

V. Conclusion générale

En somme, lors de la conception de ce système, nous nous sommes tout d'abord rendu compte que, lorsqu'il s'agit d'une réalisation, il y a toujours un compromis entre ce que l'on s'est fixé au début et ce que l'on obtient à la fin. Ceci dit, le choix de la webcam ainsi que le taux de lumière ont pris énormément de temps lors de cette réalisation. Leur influence réside essentiellement dans le problème qu'elle pose lors de la segmentation des images de la main des différentes personnes conduisant à des erreurs de matching. Mais aussi notons que la création de la base de données n'était pas simple, car il fallait convaincre les gens que, tout d'abord il ne s'agissait pas d'acquérir leurs empreintes digitales pouvant être utilisé à leur insu mais seulement la forme de leur main et aussi que même.

Ensuite, différents tests ont été effectués en utilisant différentes distances pour le matching, cela nous a permis d'avoir un taux d'égal erreur EER très intéressant pouvant être appliqué dans des systèmes d'accès sécurisé.

Aussi, ce travail nous a donné une opportunité de nous essayer et de nous familiariser à certains softwares et hardwares, méconnue ou mal maîtriser pour nous jusqu'à lors.

Notons surtout que nous avons développé un système de pointage innovant, car on donne le libre choix à l'utilisateur de mettre sa main sans "plugs" juste en écartant ses doigts chose qui n'a pas encore été développé ailleurs d'après nos recherches. D'où un système sans contact, c'est-à-dire sans risque de contamination des maladies puisque la main est source de 90% des infections et de contaminations.

Références bibliographiques

[1] : https://fr.wiktionary.org/wiki/securitas

[2] : Hélène Molinari, 24 avril 2017, faut-il avoir peur des puces RFID ?,Tech,Tech-numerama.com,11/02/18

[3] : https://www.futura-sciences.com/fr/definition/t/medecine-2/d/empreintes-digitales_3302/

[4]:https://infoscience.overblog.com/pages/La_reconnaissance_des_empreintes_digitalesFingerprint_recognition-4408216.html

[5] : Romain Giot, « Contributions à la dynamique de frappe au clavier : multibiométrie, biométrie douce et mise à jour de la référence », Thèse de doctorat de l'université de Caen Basse-Normandie, 2006

[6] : Régis Bigot et Patricia Croutte: « La diffusion des technologies de l'information et de la communication dans la société française », rapport technique, Centre de recherche pour l'étude et l'observation des conditions de vie, 2011

[7] : www.aware.com/quest-ce-que-la-biometrie/processus-biometriques/

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

[9] : http://www.linternaute.com/science/biologie/dossiers/06/0607-biometrie/main.shtml

[10] : www.tryengineering.org/technologique de la main

[11] : http://www.thierryaimard.fr/anatomie-main.php

[12] : http://www.lecorpshumain.fr/corpshumain/1-main.html

[13] : http://www.thierryaimard.fr/anatomie-main.php

[14] : AMINE NAÏT-ALI., RÉGIS FOURNIER., « *traitement du signal et de l'image pour la biométrie* », p.202

[15] : DAUGMAN J., « Combining Multiple Biometric », The Computer Laboratory, Cambridge University, Cambridge, Royaume-Uni, 2000

[16] : « The making of arduino », sur IEEE Spectrum, 26 octobre 2011 (consulté le 13 février 2018)

[17] : https://framablog.org/2011/12/10/arduino-histoire/

[18] : http://www.hb9g.ch/site/images/documents/CoursArduino.pdf, 28/03/18

[19] : www.techmania.fr

[20] :http://www.mon-club-elec.fr/pmwiki_reference_arduino/pmwiki.php?n=Main.Librairies

[21] : www.mathworks.com

[22] : L. LAGROUME & M. SAAD, « Contrôle d'accès biométrique multimodale », Mémoire de Master 2 en Génie électrique d'Informatique industrielle de l'université AbdelHamid Ibn Badis de Mostaganem, 2017

[23] : http://eric.univ-lyon2.fr/~ricco/tanagara/fichiers/fr_Tanagra_KMO_Bartlett.pdf

[24] : www.modalisa.com/support/lexique/correlation-rangs-spearman.php

[25] : staps.univ-lille2.fr/fileadmin/correlation

[26] : S. BOUDJELLAL, « Détection et identification de personne par méthode biométrique », Mémoire de Magister en Électronique en télédétection de l'université Mouloud MAMMERI de TIZI-OUZOU (UMMTO).

[27] : Romain Scotto (04/05/14), « Hygiène : Les mains, ce vecteur de maladies insoupçonné ,20minutes.fr,sur :https://www.google.com/amp/s/m.20minutes.fr/amp/a/1366777, 14/04/18