وزارة البحث العلمي والتعليم العالي
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
جامعة عبد الحميد بن باديس مستغانم
Université Abdelhamid Ibn Badis Mostaganem
كلية العلوم و التكنولوجيا
Faculté des Sciences et de la Technologie
DEPARTEMENT DE GENIE ELECTRIQUE

N° d'ordre : M ……/GE/2019

MEMOIRE

Présenté pour obtenir le diplôme de

MASTER EN ELECTRONIQUE

Option : électronique des systèmes embarqués

Par

DEBBI Adlene Azzeddine

BENDAOUADJI Yacine

Système d'accès sécurisé multimodal à base de « géométrie et empreinte palmaire » de la main

Soutenu le 14/07/2019 devant le jury composé de :

Président :	ABED Mansour	MCA	Université de Mostaganem
Examinateur 1:	BENTOUMI Mohamed	MCB	Université de Mostaganem
Rapporteur :	MERAH Mostefa	MAA	Université de Mostaganem
Co-rapporteur :	REBHI Mustapha	MAA	Université de Mostaganem

Année Universitaire 2018/2019

Remerciements

Tout d'abord, la louange entière est à ***Allah*** *pour l'énergie et le courage qu'il nous a donné pour terminer notre travail et notre étude.*

Nous tenons à remercier nos deux encadreurs monsieur ***Mostefa MERAH*** *et monsieur* ***Mustapha REBHI*** *pour leur constante disponibilité à notre égard et leur aide précieuse pour mener à bien ce modeste travail, ainsi de nous avoir donné l'envie d'investir dans l'univers d'électronique et traitement d'image.*

Nous remercions aussi tous les enseignants de la Faculté des Sciences et de la Technologie, en général, et ceux du département de Génie électrique, en particulier, qui ont contribué à notre formation.

On remercie vivement l'ensemble des étudiants de notre faculté et surtout nos camarades de classe avec qui nous avons passé cinq merveilleuses années.

Enfin, permettez-nous d'adresser nos sincères remerciements à nos amis, proches, et toute personne qui nous ont encouragé et cru a nous dès le début.

Nous sommes heureux d'être des électroniciens sur cette planète.

Dédicace

Nous dédions ce travail qui n'aura jamais pu voir le jour sans les soutiens indéfectibles et sans limites de nos chers parents qui ne cessent de nous donner avec amour le nécessaire pour que nous puissions arriver à ce que nous somme aujourd'hui.

Que Dieu vous protège et que la réussite soit toujours à notre portée pour que nous puissions vous combler de bonheur.

Nous dédions aussi ce travail à :

- *Nos sœurs.*
- *nos oncles, mos tantes.*
- *Tous nos cousins et cousines.*
- *Tous nos amis, nos collègues.*

Table des matières

Introduction générale.....1

Chapitre I Les systèmes d'accès sécurisé

I.1 Introduction.....3

I.2 Type d'accès.....4

I.2.1 Ce que l'on sait.....4

a. Mot de passe.....4

b. Nom et prénom.....4

I.2.2 Ce que l'on a.....5

a. Code à barres.....5

b. Les RFID.....6

I.2.3 Ce que l'on est.....7

a. Reconnaissance faciale.....7

b. Empreinte digitale.....9

c. Biométrie oculaire « Iris ».....10

d. Reconnaissance de la voix.....10

e. La géométrie de la main.....11

I.3 Conclusion.....11

Chapitre II qu'est-ce que c'est la biométrie ?

II.1 Introduction.....13

II.2 La biométrie.....13

II.3 Classification des caractéristiques biométriques.....14

II.4 Les performances d'un système biométrique.....14

II.5 Marché mondial de la biométrie.....15

II.6 Les parts de marché par technologie.....16

II.7 La biométrie de la main.....17

II.7.1 Anatomie de la main.....18

II.7.2 Description.....18

II.8 Conclusion.....19

Chapitre III Software et hardware du dispositif biométrique

III.1 Introduction.....21

III.2 Partie hardware.....21

III.2.1 La carte électronique utilisées « RASPBERRY PI 3B+ »....21
a. Historique de Raspberry pi....21
b. Définition du Raspberry pi 3 B+....22
c. Caractéristiques de Raspberry pi 3 B+....23
III.2.2 L'éclairage....23
III.2.3 Webcam....23
III.2.4 L'affichage « LCD »....24
III.2.5 Capteur Ultrason HC-SR04....24
III.2.6 Router « modem »....26
III.2.7 Un pc server....26
III.2.8 Keypad....26
III.2.9 Réalisation du boitier....27
III.3 Partie software....29
III.3.1 Système d'exploitation du RASPBERRY PI 3B+ « Raspbian »....29
III.3.2 Python 3....30
III.3.3 FTP server....32
III.3.4 Logiciel Matlab....33
III.3.5 Traitement d'image....33
III.3.6 Fonctions de similarités....35
a. La distance de Minkowski....35
b. La distance de Manhattan « City block »....35
c. La distance de Tchebychev....36
d. La distance de Hamming....36
e. La distance Euclidienne....36
f. La similarité cosinus....36
g. Le coefficient de corrélation γ....37
h. Le coefficient de corrélation de rang Spearman....37
III.3.7 La méthode HOG « Histogram of Orientes Gradient »....38
III.3.8 La fusion....38
III.3.9 Evaluation de la vérification....38
III.4 Conclusion....40

Chapitre IV Résultats expérimentaux

IV.1. Introduction....41

IV.2. Traitement des images acquises par la caméra.....41
IV.3. Résultats expérimentaux.....42
IV.3.1. La géométrie de la main.....42
IV.3.2. L'empreinte palmaire méthode HOG.....47
IV.3.3 Fusion des deux modalités utilisant la méthode ACP.....51
IV.4 Conclusion.....53

V. **Conclusion générale**.....55
Références bibliographiques.....56

Liste des figures

Figure 1.1. Mot de passe.....4
Figure 1.2. Nom et prénom.....4
Figure 1.3. Code à barres.....5
Figure 1.4. Les composants du RFID.....6
Figure 1.5. Schéma de fonctionnement du RFID.....6
Figure 1.6. La reconnaissance faciale.....8
Figure 1.7. Échantillon d'empreinte.....9
Figure 1.8. Un dispositif d'empreinte.....9
Figure 1.9. L'iris.....10

Figure 2.1. La marge d'erreur autorisée/ EER.....15
Figure 2.2. Evolution du marché international de la biométrie.....16
Figure 2.3. Parts de marché des différentes méthodes biométriques.....16
Figure 2.4. Points caractéristique de la main.....17
Figure 2.5. Anatomie de la paume de la main droite.....18
Figure 2.6. Dissection profonde palmaire.....19

Figure 3.1. Schéma synoptique.....21
Figure 3.2. Raspberry Pi 3 B+.....22
Figure 3.3. Spot LED.....23
Figure 3.4. Webcam utilisé.....24
Figure 3.5. Afficheur LCD 4x16 avec I2C.....24
Figure 3.6. Capteur Ultrason HC-SR04.....25
Figure 3.7. Schéma de fonctionnement du Capteur Ultrason HC-SR04.....25
Figure 3.8. Test pratique de performance. Meilleur on angle de 30°.....25
Figure 3.9. Le modem utilisé.....26
Figure 3.10. Keypad 4x3.....27
Figure 3.11. Image de la maquette (vue d'extérieur).....27
Figure 3.12. Image de la maquette (vue d'intérieur).....27
Figure 3.13. Image de la maquette.....28

Figure 3.14. Choix du mode.....28
Figure 3.15. Entrée la main.....28
Figure 3.16. Ecartement des doigts.....28
Figure 3.17. L'espace entre la main et le haut du boitier.....29
Figure 3.18. Glisser la main vers le haut.....29
Figure 3.19. Console FTP server.....32
Figure 3.20. Le logo de MATLAB.....33
Figure 3.21. Les points caractéristiques de la main.....33
Figure 3.22. Organigramme des différentes étapes du traitement « prise d'image +traitement d'image avec Matlab…….....34
Figure 3.23. Trajets suivis par deux points.....36
Figure 3.24. Evolution des taux de FAR et FRR en fonction du seuil de similitude.....39
Figure 3.25. Taux de vraisemblance des utilisateurs légitimes et des imposteurs.....39
Figure 3.26. La courbe ROC.....40
Figure 4.1. Image originale de la main.....41
Figure 4.2. Image segmentée de la main.....41
Figure 4.3. Squelette + rotation de la main.....41
Figure 4.4. Contour et points caractéristiques.....41
Figure 4.5. Contour + cadre pour la paume.....42
Figure 4.6. Masquage et image de la paume.....42
Figure 4.7. La courbe Far, Frr et ROC de la méthode euclidienne.....43
Figure 4.8. La courbe Far, Frr et ROC de la méthode Manhattan (City block).....43
Figure 4.9. La courbe Far, Frr et ROC de la méthode Minkowski.....44
Figure 4.10. La courbe Far, Frr et ROC de la méthode Cosine.....44
Figure 4.11. La courbe Far, Frr et ROC de la méthode Corrélation.....45
Figure 4.12. La courbe Far, Frr et ROC de la méthode Spearman.....45
Figure 4.13. La courbe Far, Frr et ROC de la méthode Tchebychev.....46
Figure 4.14. La courbe Far, Frr et ROC de la méthode Euclidienne.....48
Figure 4.15. La courbe Far, Frr et ROC de la méthode Manhattan (City block).....48
Figure 4.16. La courbe Far, Frr et ROC de la méthode Minkowski.....49
Figure 4.17. La courbe Far, Frr et ROC de la méthode Cosine.....49
Figure 4.18. La courbe Far, Frr et ROC de la méthode Corrélation.....50
Figure 4.19. La courbe Far, Frr et ROC de la méthode Spearman.....50
Figure 4.20. La courbe Far, Frr et ROC de la méthode Tchebychev.....51

Liste des tableaux

Tableau 2.1. Les grandes familles de caractéristiques biométriques.....14

Tableau 3.1. Caractéristique Raspberry Pi 3 B+.....23
Tableau 3.2. Les ports de connexion entre l'écran LCD et le Raspberry Pi.....24

Tableau 4.1. Différentes méthodes de similarité sur la modalité de **la géométrie de la main**.....41
Tableau 4.2. Différentes méthodes de similarités sur la modalité de **l'empreinte palmaire**.....47
Tableau 4.3. Différentes méthodes de similarités sur la modalité de **fusion « méthode ACP»**.....51
Tableau 4.4. Différentes méthodes de similarités sur la modalité de **la géométrie de la** main.....52
Tableau 4.5. Différentes méthodes de similarités sur la modalité de **l'empreinte palmaire**.....52
Tableau 4.6. Différentes méthodes de similarités sur la modalité de **l'empreinte palmaire et la géométrie de la main « fusion » avec ACP**.....53

Liste des abréviations

ACP : *Analyse en Composantes Principales*

AFIS : *Automated Fingerprint Identification System*

EER : *Equal Error Rate*

FA : *False Accepting*

FAR : *False Acceptance Rate (TFA)*

FR : *False Rejection*

FRR : *False Rejection Rate (TFR)*

FTP : *File Transfer Protocol*

GPIO : *General Purpose Input/Output*

HOG : *Histogram of Orientes Gradient*

IBG : *International Biometric Group*

LAN : *Local Area Network*

LCD : *Liquid Crystal Display*

LED : *Light Emetting Diode*

PCB : *Printed circuit board*

PIN : *Numéro d'Identification Personnel*

RFID : *Radio Frequency Identification*

ROC : *Receiver Operating Characteristic*

USB : *Universal serial bus*

Introduction générale :

Un monde plein de mouvement, plein de vitalité et plein des richesses, l'être humain était souvent à la recherche des nouvelles qui l'entourent et qui peuvent fournir une meilleure qualité de vie et un confort qui ne connait pas de limite. Sa curiosité était souvent un paramètre primordial pour son développement. Mais comme la curiosité de l'être humain était un avantage pour sa progression et son développement, elle était aussi pour certaines personnes un paramètre indésirable par le fait du vol, l'espionnage et l'intrusion et autres comportement similaires. Donc, la technologie, par son rôle, était toujours présente du fait qu'elle réduisait de ces comportements non souhaités et essayait de les éliminer pour un meilleur confort sécuritaire des personnes et leurs patrimoines.

La technologie des systèmes de sécurité a vécu une chronologie et une diversité, depuis que l'homme était responsable de lui-même et de sa sécurité commençant par le recours au chien de garde, passant par la création des mécanismes de sécurité…, jusqu'à l'avènement de l'électronique. L'apparition de l'électronique dans notre vie quotidienne nous a apporté assez d'avantages, la réalisation des systèmes de sécurité électroniques se caractérise par la fiabilité, la rentabilité, un cout moins cher et des dimensions petites. Ces systèmes-là ont prouvé leur rôle, leur efficacité et la disparition presque totale du taux d'erreur.

Les chercheurs scientifiques ont montré que chaque personne sur cette planète à ses propres traces biologiques ou biométriques (géométrie des mains et leurs textures, iris, ADN). Toutes ses modalités sont devenues l'essence de l'identification reposant sur les indices de diversité entre les personnes dans leurs vies et cela grâce à la technique d'identification et d'authentification utilisée dans les endroits privés ou sensibles et ceci sera le cas de ce modeste travail qu'est la réalisation d'un système d'accès sécurisé multimodal.

Dans notre projet de fin d'études, on a abordé le thème d'un système d'accès sécurisé multimodal qui acquiert l'image d'une main droite prise par une caméra. L'image est, ensuite, traitée dans un logiciel et cela grâce à des protocoles utilisés qui assurent la liaison entre le milieu de la prise d'image (boitier) et l'autre milieu (PC-server) qui reçoit l'image et la fera passer vers « Matlab » pour la traiter. Une fois que le traitement est terminé, le logiciel fournira une réponse de reconnaissance ou non, sous forme d'un message, selon que l'utilisateur de ce système existe ou non dans la base des données.

Chapitre I

« Les systèmes d'accès sécurisé »

I.1 Introduction :

"La droite dit : la première liberté, c'est la sécurité. Nous disons au contraire : la première sécurité, c'est la liberté." [1]

La sécurité est une ressource indispensable à la vie quotidienne qui permet à l'individu et à la communauté de réaliser ses aspirations. C'est un état où les dangers et les conditions pouvant provoqué des dommages d'ordre physique, psychologique ou matériel sont contrôlés de manière à préserver la santé et le bien-être des individus et de la communauté.
Étymologie : c'est un mot latin "securitas" veut dire absence de soucis, tranquillité de l'âme, dérivé de securus, sans soucis, sans crainte, tranquille.

Pour obtenir un niveau de sécurité optimal, ceci nécessite que les individus, communautés, gouvernements et autres intervenants, créent et maintiennent les conditions suivantes, et ce, quel que soit le milieu de vie considéré [2]:

- Un climat de paix sociale ainsi que d'équité protégeant les droits et libertés, tant au niveau familial, local, national et international;
- La prévention et le contrôle des blessures et autres conséquences ou dommages causés par des accidents;
- Le respect des valeurs et de l'intégrité physique, matérielle ou psychologique des personnes;
- L'accès à des moyens efficaces de prévention, de contrôle et de réhabilitation pour assurer la présence des trois premières conditions.

Qu'est-ce que la sécurité au travail ?

Le concept de sécurité au travail appuie son existence sur un postulat de départ assez simple : Dans l'activité professionnelle y a-t-il des risques pour la sécurité d'un travailleur, à des degrés plus ou moins élevés ?
La sécurité au travail ne cesse de donner naissance à de nouvelles règlementations, de nouvelles mesures, des innovations. Cependant, les chiffres de la sécurité au travail révèlent que l'homme est en cause dans plus des accidents de travail. La tâche des dirigeants d'entreprises est de réduire au maximum les risques afin de protéger leurs salariés et de préserver leurs intégrités physique et morale [3].

I.2 Types d'accès :

Il y a plusieurs types pour accéder à un système de sécurité. Parmi lesquels, on citera :

I.2.1 Ce que l'on sait :

C'est-à-dire le mot de passe, la signature, le nom, le prénom ; mais ils peuvent être détournés, ou piratés très facilement par un hacker.

a. Mot de passe :

Un mot de passe, ou password est une séquence de caractères ou mot privé pour authentification, validation ou vérification. Un mot de passe fort permet davantage de sécurité.

Actuellement, les mots de passe sont très présents dans nos quotidiens, et cela est dû notamment à notre forte utilisation d'Internet et des systèmes bancaires …etc. la (**Figure1.1**) montre un champ pour nom d'utilisateur avec du mot de passe.

Figure 1.1. Mot de passe.

b. Nom et prénom :

C'est l'identité avec laquelle on peut différencier entre les sujets dans un environnement donné (classe, service, local, etc.). Voici un tableau de plusieurs personnes avec son nom et prénom (**Figure1.2)**

Nom	Prénom		Nom et Prénom
Nom1	Prénom1		Nom1 Prénom1
Nom2	Prénom2		Nom2 Prénom2
Nom3	Prénom3		Nom3 Prénom3
Nom4	Prénom4		Nom4 Prénom4
Nom5	Prénom5		Nom5 Prénom5

Figure 1.2. Nom et prénom.

I.2.2 Ce que l'on a :

Ce sont tous les objets que nous avons, tel que la clé, le badge, les puces RFID, les cartes bancaires qui contiennent un ensemble d'informations stockées dans des mémoires internes. Cependant, il y a la possibilité de perdre sa carte, sa clé.

a. Code à barres :

Le code à barres est un système de traçabilité des produits d'entreprises dans tous les secteurs. Il représente la codification d'une information relative à un produit.

La représentation de la codification est évoluée afin de pouvoir être lue par un lecteur optique.

La Figure1.3 représente un code à barres d'un produit algérien.

Pays de fabrication du produit
613 =fabrication Algérienne

Figure 1.3. Code à barres.

L'utilisation du code à barres est largement déployée à travers toutes les filières.

Ainsi, il est possible d'extraire ces utilisations principales du code à barres [4]:

- entrer un produit en stock,
- connaître l'origine du produit,
- faciliter l'approvisionnement,
- aiguiller facilement un produit en fonction de ses caractéristiques,
- avoir des informations sur le produit en continu, etc.

Parmi les principaux nombreuses qualités ou avantages du code à barres, on cite :

- Lecture rapide et fiable,
- Suppression des erreurs de saisies manuelles,
- Facilité du système,
- Faible coût.

Le code à barres présente des inconvénients majeurs :

- leur résistance/durée de vie,
- ils ne peuvent être lus qu'au contact d'un lecteur,
- un stockage d'informations restreint.

b. Les RFID :

Le système RFID (Radio Frequency Identification) est une technologie qui offre la possibilité d'une gestion automatique du nombre conséquent d'informations à traiter dans l'entreprise. Ce système permet de synchroniser les flux physiques avec les flux d'informations par des équipements adaptés au RFID.

Le système RFID permet de mémoriser et de récupérer des informations à distance grâce à une étiquette RFID qui émet des ondes radio, marqueur ou tag (**Figure1.4.)**

Figure 1.4. Les composants du RFID.

Pour équiper les entreprises avec un système RFID, elles doivent donc mettre en place un équipement de base bien spécifique composé de (**Figure1.5)** :

- un support RFID : étiquette, carte RFID ou badge RFID composé d'une puce + d'une antenne RFID,
- un lecteur : avec antenne intégrée ou externe,
- une infrastructure informatique qui sert à collecter et à exploiter les données (Arduino, Raspberry ou microcontrôleur).

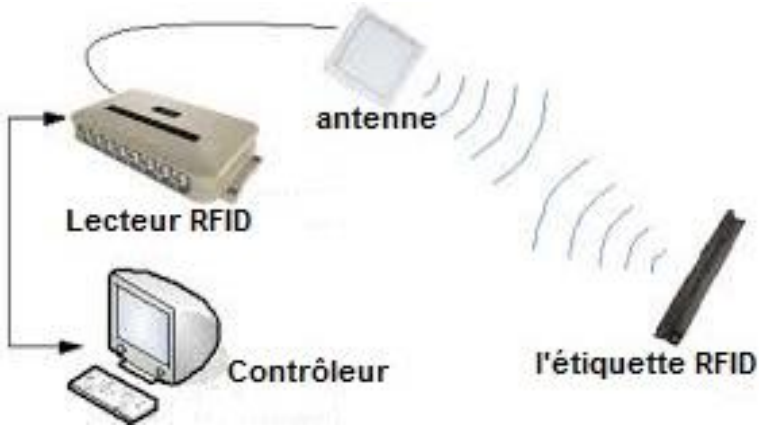

Figure 1.5. Schéma de fonctionnement du RFID.

La radio identification peut s'appliquer à des différents domaines et son intégration au sein des entreprises est en augmentation constante.

La RFID s'offre de multiples avantages, voici les principaux [5]:

- pas besoin de contact visuel comme les codes-barres,
- éviter les erreurs de saisie et de collecte des données,
- possibilité de lire plusieurs étiquettes en même temps,
- stockage d'informations beaucoup plus important que les codes barres,
- augmente la vitesse et l'efficacité de la traçabilité,
- les données sont fiables,
- une longue durée de vie de la puce (plus de 10 ans),
- un retour très rapide sur investissement,
- des gains de productivité,
- une discrétion totale du système d'identification,
- offre plus de sécurité et un gage de qualité à l'entreprise.

Malgré certains avantages, la radio identification présente certaines contraintes liées notamment à ces facteurs :

- le coût de la mise en place du système RFID : les étiquettes RFID et son lecteur plus l'infrastructure informatique sont plus coûteuses que les codes à barres,
- une technologie complexe à mettre en place,
- le fait de ne pas perturber les autres ondes radio (anticollision),
- l'impact des ondes radio sur la santé,
- le besoin de formation RFID du personnel à ces techniques.

I.2.3 Ce que l'on est :

Chaque personne possède plusieurs caractéristiques biologiques, que nous pouvons identifier avec précision et en toute sécurité et parmi ces caractéristiques:

a. Reconnaissance faciale :

Cette technique consiste à "reconnaître" chaque personne par sa photo. L'image du visage est capturée par une webcam, qui l'envoie à un logiciel pour la numériser (**Figure1.6**.)

Le logiciel repère d'abord la position des yeux pour procéder à un "alignement". En fonction de cet alignement, on prendra différents points caractéristiques du visage (ailes du nez, forme du menton, écartement des yeux). Un tracé géométrique personnel (par les points

caractéristiques qui se trouvent dans l'image suivante) est ensuite enregistré comme gabarit (chaque visage est codé sous forme de fichier de 84 octets), et c'est sur ce dernier que s'effectueront ensuite les recherches.

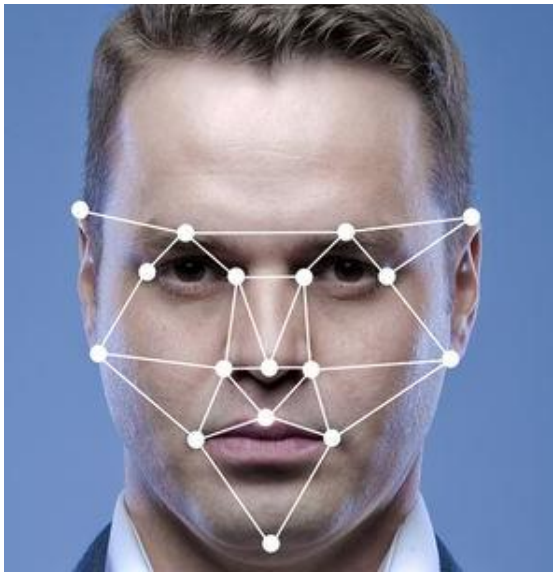

Figure 1.6. La reconnaissance faciale.

Une des technologies les plus utilisées est celle de "l'Eigenface", développée par le MIT (Massachusetts Institute of Technology) à partir d'analyses statistiques de milliers de visages. La technologie consiste à décomposer le visage en plusieurs images en nuances de gris, chacune mettant en évidence une caractéristique particulière. Le système des réseaux de neurones est encore plus performant, surtout dans des conditions difficiles de capture. Ils emploient un autre algorithme pour déterminer la similarité entre des captures d'images de visage et des gabarits [6].

Avantages :

Cette technologie est non intrusive, et peut même se dérouler à l'insu de la personne concernée. D'après les progrès accomplis ces dernières années sont considérables au point que les systèmes sont aujourd'hui capables de reconnaître des individus même avec des artifices (fausses moustaches, barbe, lunettes…). Seule une chirurgie importante du cartilage du visage pourrait tromper le système.

Inconvénients :

À condition d'avoir un bon éclairage, les taux de reconnaissance sont très élevés, mais en vidéo, la technique n'est pas encore améliorée. En fait, le visage est trop changeant au fil du temps pour être un repère biométrique suffisamment fiable.

b. Empreinte digitale :

Depuis longtemps, on a à mettre notre doigt à l'encre pour la signature. Aujourd'hui pour passer à l'électronique, une petite cellule scanne par des dispositifs l'extrémité du doigt (**Figure1.7**.) Les plus simples dispositifs se contentent d'un capteur optique (**Figure1.8**.)

La transmission des données se fait par Ethernet, GSM ou ondes radio. Sur une base de données classique, on peut préenregistrer des milliers de personnes avec leurs données.

Figure 1.7. Échantillon d'empreinte.

Figure 1.8. Un dispositif d'empreinte.

Avantages :

Cette technique est facile à utiliser et la plus fiable. Une étude a montré qu'une chance sur 17 milliards de trouver deux empreintes avec plus de 17 points de similitude. Les scanners sont peu encombrants (de nombreux fabricants proposent des lecteurs portatifs). Dernièrement, deux pirates allemands ont quand même réussi à tromper un système avec une fausse empreinte fabriquée sur ordinateur, et imprimée sur un faux doigt en latex.

Inconvénients :

Il n'est pas évident de faire un système de pointage avec l'empreinte digitale dans une entreprise, car les empreintes digitales sont associées à une image "policière". Il y a aussi certains problèmes d'hygiène, en milieu hospitalier par exemple.

c. Biométrie oculaire « Iris » :

L'iris est la surface colorée de l'œil. Elle est constituée d'un réseau de tubes très fins. Les tubes ne varient que très peu durant la vie de l'individu.

On met l'œil en face à une caméra proche des infrarouges qui prendra une photo de l'iris. Elle relève les caractéristiques particulières du relief (sillons de contraction, anneaux, etc. comme désigné sur la (**Figure 1.9**.). On peut distinguer jusqu'à 244 points de comparaison.

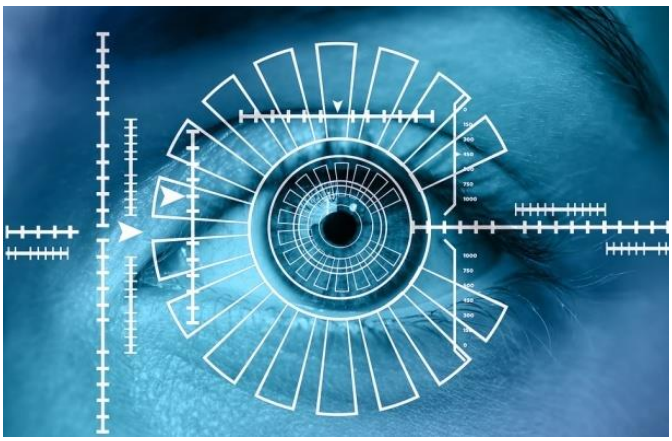

Figure 1.9. L'iris.

Avantage :

La probabilité de trouver 2 iris identiques sur les produits disponibles sur le marché serait de 1 sur 10^{72} donc le taux d'erreur est quasi nul. La texture de l'iris est parfaitement stable au cours du temps. Selon Sagem, la vérification de l'identité prend aujourd'hui moins de 4 secondes. La technique reste extrêmement fiable même à travers des lunettes ou des lentilles.

Inconvénients :

La taille de l'iris est très variable suivant la lumière ambiante ou l'état de fatigue. D'autre part, la fiabilité diminue proportionnellement à la distance entre l'œil et la caméra. Le cout est plus élevé (compter 12 000 euros pour un équipement de base).

d. Reconnaissance de la voix :

C'est-à-dire analyser et identifier la voix des personnes par des systèmes de reconnaissance vocale automatisés (Ordinateurs ou téléphone). Ces systèmes sont capables d'identifier avec précision les individus de leur voix avec un taux d'erreur inférieur à 1%.

e. Géométrie de la main :

L'identification avec la surface de la main repose sur le même principe que l'empreinte digitale. Dans ce cas, c'est toute la surface de main qui est analysée.

I.3 Conclusion :

Dans ce chapitre, nous avons indiqué différents types d'accès sécurisés qui existent. Vu que ceci nécessite trop de littérature pour citer les détails on n'a fait que relater l'essentiel.

Dans le prochain chapitre, nous nous focaliserons sur la biométrie, en général, et sur la biométrie de la main, en particulier.

Chapitre II

« Qu’est ce que c’est la biométrie ? »

II.1 Introduction :

La biométrie est une technique générale permettant de prouver l'identité d'une personne en mesurant l'une de ses propriétés physiques. Il existe plusieurs types de ces caractéristiques, différentes les unes des autres en termes de fiabilité, où elles doivent toutes être fiables et uniques pour un individu. D'autre part, nous verrons que les propriétés physiques sont loin d'être idéales et très précises, et nous atteignons bientôt les limites de ces techniques.

II.2 La biométrie :

La biométrie est un ensemble des technologies qui utilise les caractéristiques physiques et comportementales de l'être humain. Les caractéristiques sont traitées par ensembles de commandes automatiques utilisant plusieurs dispositifs, tels que les scanners et les appareils-photo. Les caractéristiques comprennent les empreintes digitales, la signature, l'iris, la voix, le visage et les gestes pour distinguer les personnes.

Contrairement aux mots de passe ou des PINs (numéros d'identification personnelle) qui sont facilement oubliés, ou des cartes magnétiques qui doivent être portées par l'individu et sont faciles à être volées, copiées ou perdues ; les caractéristiques biométriques sont uniques à l'individu, car elles se distinguent des autres et il n'ya aucune possibilité de remplacer ces caractéristiques, Les technologies biométriques sont donc considérées comme les plus puissantes en termes de sécurité.

Un système biométrique peut fonctionner en deux modes :

- **Vérification :** Le système vérifie l'identité de la personne à partir de la comparaison des données biométriques saisies avec la base de données. Dans le système, la personne qui souhaite s'identifier est requise généralement via un numéro d'identification personnel (PIN), un nom d'utilisateur ..., et le système effectue la comparaison un à un pour déterminer si ces données dynamiques appartiennent-elles à cette personne ou non.

- **Identification :** Le système détermine l'individu en recherchant les signatures pour tous les utilisateurs dans la base de données. Le système effectue plusieurs comparaisons pour établir l'identité de la personne (ou échoue si le sujet n'est pas enregistré dans la base de données de système).

II.3 Classification des caractéristiques biométriques :

Dans la biométrie, il y a des caractéristiques propres à chaque personne. Il existe trois grandes familles de caractéristiques biométriques :

- Caractéristiques biologiques
- Caractéristiques comportementales
- Caractéristiques morphologiques

Le tableau2.1 suivant résume les grandes familles de caractéristiques biométriques :

Caractéristiques biologiques	Caractéristiques comportementales	Caractéristiques morphologiques
sang ADN urine odeur salive, …	dynamique de signature dynamique de frappe sur un clavier parole démarche …	empreintes digitales forme de la main forme du visage forme de l'iris ou de la rétine …

Tableau 2.1. Les grandes familles de caractéristiques biométriques.

II.4 Les performances d'un système biométrique [7]:

Lorsque des systèmes biométriques sont utilisés, il est difficile d'obtenir des résultats 100% exempts d'erreur. La raison est peut-être à chercher dans des différences d'environnement lors de l'acquisition de données (éclairage, température, etc.) et dans les différences dans le matériel utilisé (caméras, scanners, etc.). Les paramètres d'évaluation des performances les plus souvent utilisés sont le taux de fausses acceptations (**FAR**) et le taux de faux rejets (**FRR**), qui peuvent être adaptés en fonction du système utilisé :

• **FRR :** taux de faux rejet

Le taux de faux rejets (**FRR** ou **TFR**) est la probabilité qu'un système produise un faux rejet. Un faux rejet se produit lorsqu'aucune correspondance n'est établie entre une personne et son modèle biométrique. Il est également connu sous le nom de «taux de faux négatifs».

• **FAR :** taux de fausse acceptation

Le taux de fausses acceptations (**FAR** ou **TFA**) est la probabilité qu'un système biométrique identifie de manière incorrecte une personne ou ne réussisse pas à rejeter un imposteur. Il mesure le pourcentage d'intrants non valides qui sont acceptés à tort.

Il est également connu sous le nom de «taux de faux positifs».

FR : nb faux rejets. **FA** : nb fausses acceptations.

NL : nb total légitime. **NI** : nb total imposteurs.

À partir du **FR** et **FA** on calcule : FRR=FR/NL et FAR=FA/NI.

Le delta (Δ) sur la figure représente la marge d'erreur autorisée/ERR.

EER : Equal Error Rate

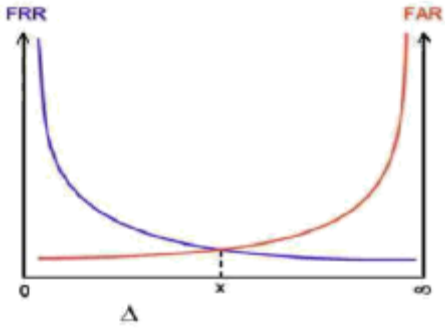

Figure 2.1. La marge d'erreur autorisée/ EER.

Avec un réglage correct du système et un bon ajustement de la configuration, les erreurs critiques des systèmes biométriques peuvent être minimisées au niveau permis pour l'utilisation opérationnelle en réduisant les risques d'évaluation incorrecte. Un système parfait présentera un FAR et un FRR de zéro, mais ces taux ont le plus souvent une corrélation négative. L'augmentation du FAR réduit souvent le niveau du FRR.

Il est important d'évaluer la finalité du traitement, le TFA et le TFR ainsi que la taille de la population au moment de déterminer si la précision d'un système biométrique particulier est acceptable ou non. Par ailleurs, l'évaluation de la précision d'un système biométrique peut également tenir compte de la capacité à détecter un échantillon vivant.

Par exemple, les empreintes digitales latentes peuvent être copiées et utilisées pour créer des faux doigts. Un lecteur d'empreintes digitales ne doit pas être mystifié et donner une identification positive dans ce type de situation.

II.5 Marché mondial de la biométrie :

Un groupe international qui s'appelle IBG (International Biometric Group) a édité un rapport sur le marché de la biométrie (**Figure 2.2.**). Ces études concernent les chiffres d'affaires, les tendances de croissance, et les développements industriels pour le marché de la biométrie actuel et futur [8].

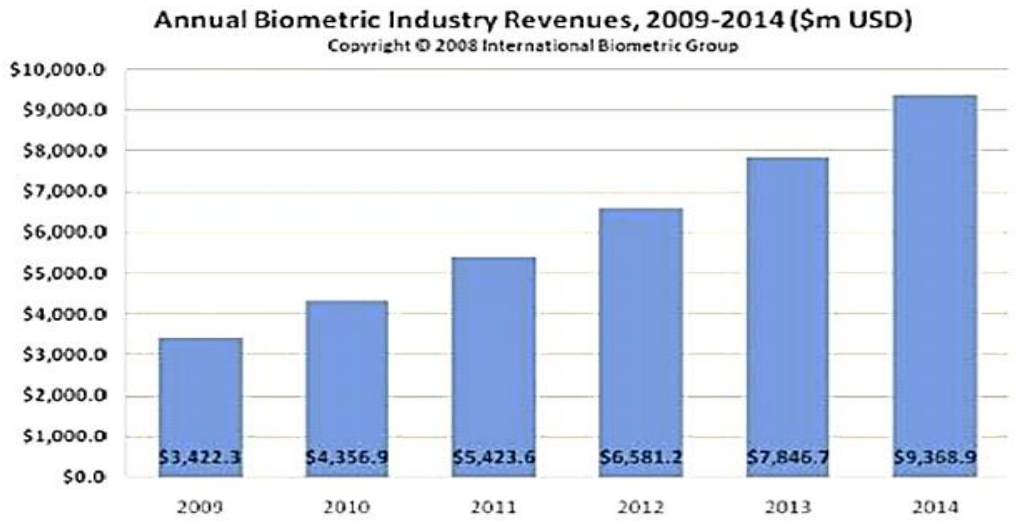

Figure 2.2. Évolution du marché international de la biométrie.

Les établissements déployant la technologie biométrique, les investissements dans les entreprises biométriques, ou les développeurs de solutions biométriques. Il y a un développement rapide sur le chiffre d'affaires de l'industrie biométrique incluant les applications judiciaires et celles du secteur public.

Malgré que les applications du secteur public continuent à être une partie essentielle de l'industrie, une grande partie de la croissance sera attribuable au contrôle d'accès aux systèmes d'information (ordinateur/réseau) et au commerce électronique.

II.6 Les parts de marché par technologie :

En termes, de part de marché (**Figure2.3)**, les empreintes digitales avec AFIS (Automated Fingerprint Identification System) restent toujours la principale technologie biométrique, plus de 50% du chiffre d'affaires total, dépasse la reconnaissance de la main et l'iris [8].

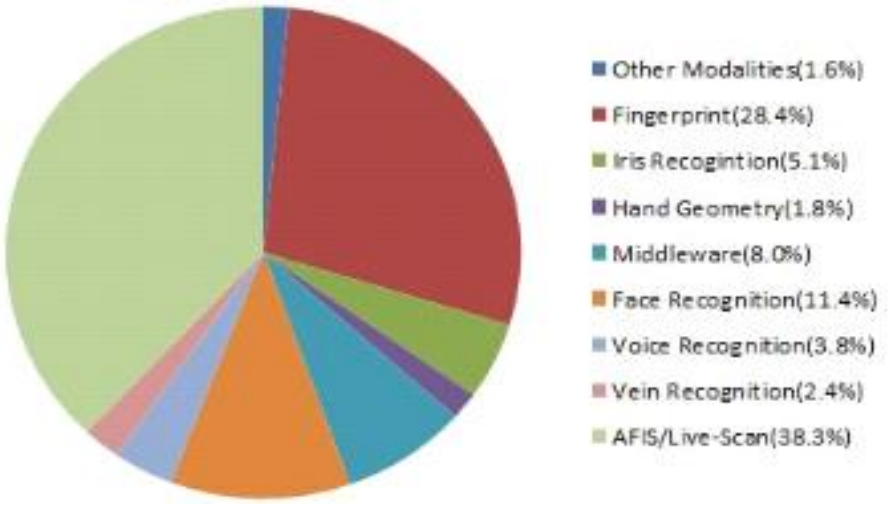

Figure 2.3. Parts de marché des différentes méthodes biométriques.

II.7 La biométrie de la main :

Cette technique de reconnaissance biométrique (handscan) est une des plus répandus à ce jour. Ce système fait appel à la forme de la main : longueur et épaisseur des doigts, largeur de la paume, forme des articulations (**Figure2.4**.)

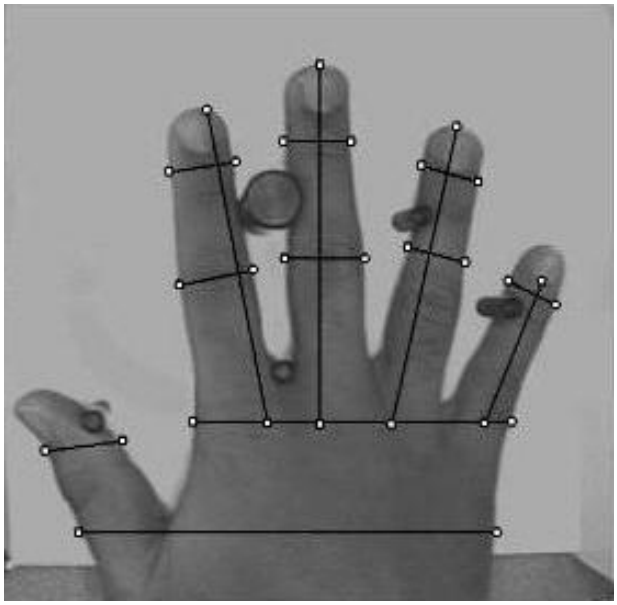

Figure 2.4. Points caractéristiques de la main.

Comme pour les empreintes digitales, on vérifie la validité de la mesure par la conductivité ou la température de la main. On peut aussi l'associer à l'empreinte du réseau veineux.

Avantages :

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

Inconvénients :

La forme de la main est moins stable dans le temps. 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.

Applications :

Moins associée à la police que les empreintes digitales, cette technologie est particulièrement appréciée dans les cas où aucun motif de sécurité n'est nécessaire. Coca-Cola, Pfizer, ou TWA par exemple l'utilisent déjà.

Lors des Jeux Olympiques de 1996, c'est la solution qui avait été retenue pour accéder au

village olympique. C'est aussi la solution qu'a retenue le service des migrations américain pour identifier les travailleurs frontaliers, qui effectuent des allers-retours fréquents entre les États-Unis et les autres pays. Au Musée de Louvre, l'accès à certaines salles est réservé pour le nettoyage, l'ouverture se fait par identification palmaire. Et avec la baisse des coûts, la biométrie palmaire s'implante de plus en plus dans les quartiers résidentiels réservés [9].

II.7.1 Anatomie de la main :

L'anatomie de la main est très complexe comme l'est sa fonction, elle est composée de 5 doigts chacun à un nom (**Figure 2.5.)**.

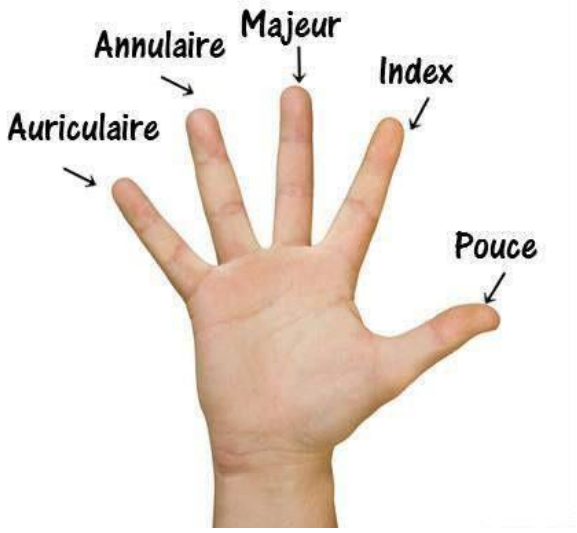

Figure 2.5. Anatomie de la paume de la main droite.

II.7.2 Description :

Les OS :

La main est constituée de 27 petits os qui s'articulent les uns aux autres **Figure2.6**.

- Le carpe est constitué de 8 os.
- Les métacarpiens sont constitués de 5 os.
- Les phalanges sont constituées de 14 os.

Les muscles :

- 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.

Les artères, veines et nerfs :

Les trois nerfs principaux de la main sont :

- le nerf médian,
- le nerf radial,
- le nerf cubital.

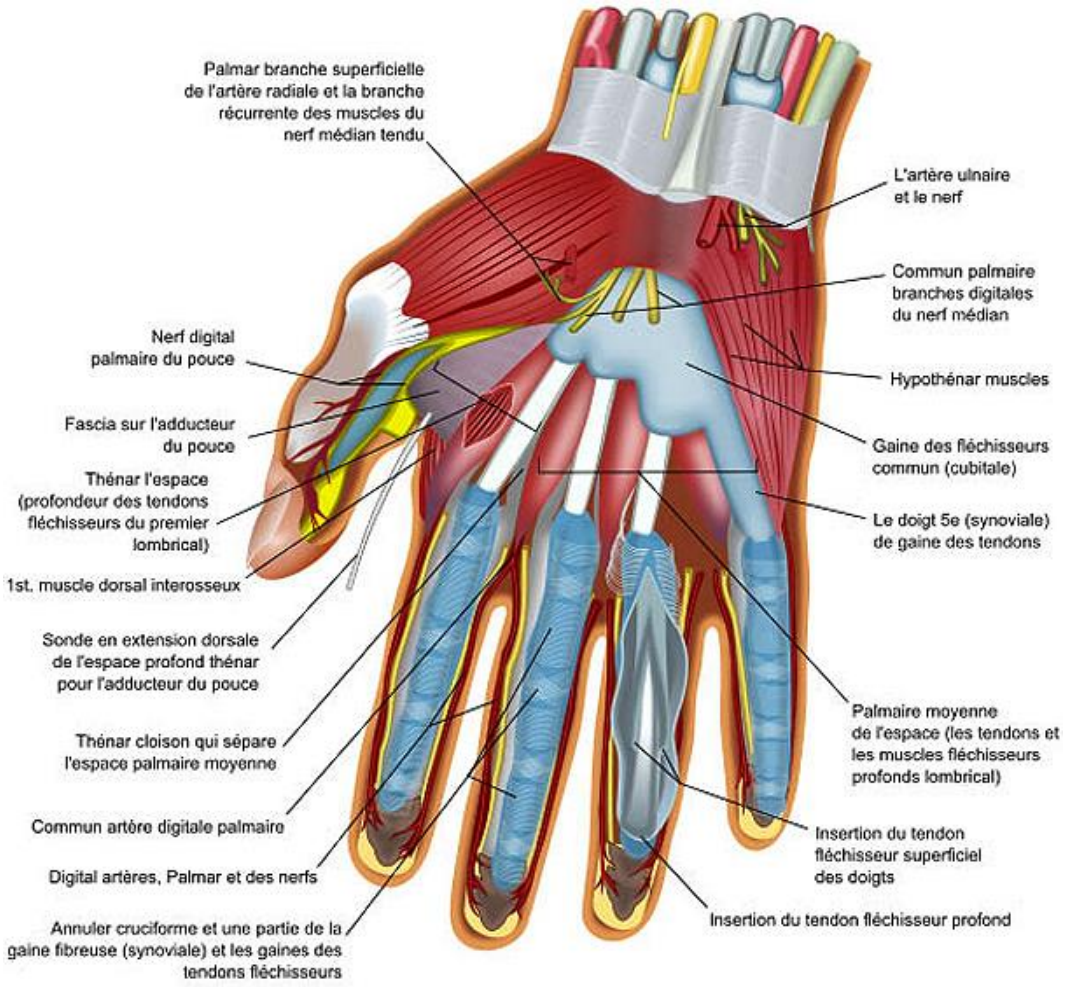

Figure 2.6. Dissection profonde palmaire [10].

II.8 Conclusion :

La biométrie tend à réaliser deux buts importants dans notre vie courante. Le premier but et de réaliser la sécurité en éliminant le doute sur l'identité d'une personne et le second but est de faciliter l'identification des individus.

Chapitre III

« Hardware et software du dispositif biométrique»

III.1 Introduction :

Pour la réalisation de projets dans le domaine de l'électronique des systèmes embarqués, une étude théorique est nécessaire et qui sera suivie par une concrétisation pratique. Un cahier des charges établi en premier temps, implique un suivi et un respect des clauses de ces deux étapes suscitées.

Le volet de la réalisation du projet est estimable selon les objectives cibles et leurs concrétisations. Que les projets soient virtuels, nécessitant seulement et basiquement l'utilisation d'un ordinateur tel que "les applications de simulation ou de modélisation" ou physique tels que ceux utilisant les robots, les appareils électroniques…etc., en tenant compte des obstacles rencontrés durant cette phase et les changements à apporter dans le projet du côté hardware (matériels, équipements, dispositifs…), ou du côté software (logiciels informatiques, programmations…).

Pour notre projet, nous avons déjà entamé l'étude théorique dans les deux chapitres précédents. Dans ce chapitre, on va aborder la partie pratique avec ses deux volets : hardware et software tout en ciblant comme objectif l'obtention des résultats escomptés qui garantiraient des tests positifs autant que faire se peut.

III.2 Partie hardware :

Le schéma synoptique du système d'accès sécurisé réalisé et rapporté sur la (**Figure 3.1.**).

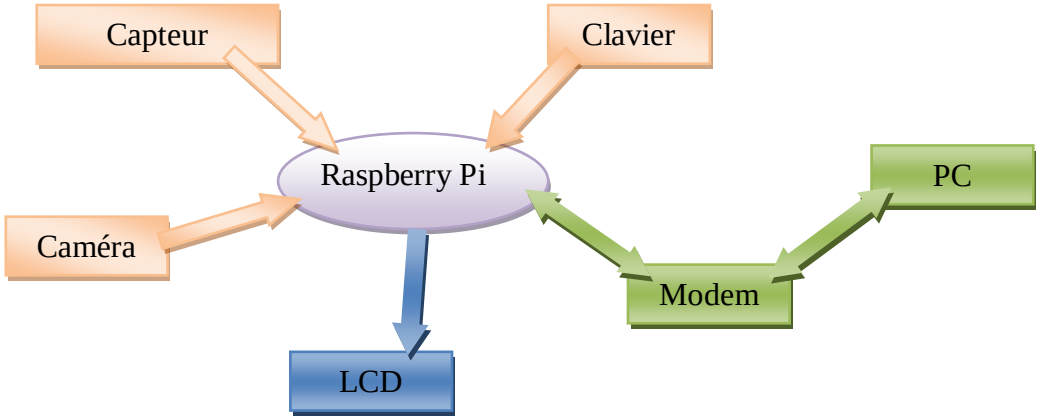

Figure 3.1. Schéma synoptique du système d'accès sécurisé.

III.2.1 La carte électronique utilisée « RASPBERRY PI 3B+ » :

a. Historique de Raspberry pi [11]:

L'histoire commence en 2006, quand une équipe d'universitaires du Laboratoire d'Informatique de Cambridge a commencé à s'inquiéter de la baisse du nombre et de la qualité des étudiants en informatique. La faute, pour eux, est due à l'absence de hardware

programmable utilisable par des jeunes voire des enfants, contrairement à ce qui était le cas dans les années 80.

Eben Upton, Rob Mullins, Jack Lang et Alan Mycroft se sont alors associés avec David Braben, créateur du jeu vidéo Élite qui avait révolutionné le genre en 1984 [11]. Ils ont sorti en 2011 la première version du Raspberry Pi : un PCB au format d'une clé USB avec un processeur à 700 MHz et 128 Mo de RAM, le tout pour la maudité somme de 25 $. Depuis, l'association caritative a multiplié les versions, dans des prix allant de 5 $ pour le Pi Zero à 35 $ pour un beau Model B. des processeurs atteignant 1,2 GHz et une RAM allant jusqu'à 1 Go.

b. Définition du Raspberry pi 3 B+ :

Raspberry Pi 3 B+ est considérée comme une carte mère, d'après ses dimensions elle a pris le nom d'un nano PC puisqu'elle possède les mêmes caractéristiques d'un ordinateur (système d'exploitation, interfaces E/S : HDMI, Ethernet, camera, affichage, Wifi, SD carte pour le stockage, pin GPIO). Cette carte a vécu un développement et une variété de modèles depuis sa première version en 2011 jusqu'à ce jour, et cela grâce aux chercheurs et aux développeurs des deux domaines informatiques et électroniques. Au début, la carte était destinée aux jeunes étudiants, mais avec le temps elle a connu une ampleur d'utilisation à même de la trouver dans les industries (contrôle, commande, traitement, régulation, serveurs …etc.).

Donc le Raspberry Pi 3 B+ (**Figure 3.2.)** a donné un avantage pour tout le monde par son petit prix qui ne dépasse pas les 50$, et cela a permis aux développeurs dans les domaines d'électronique et d'informatique de réaliser des projets avec des budgets réduits et raisonnables.

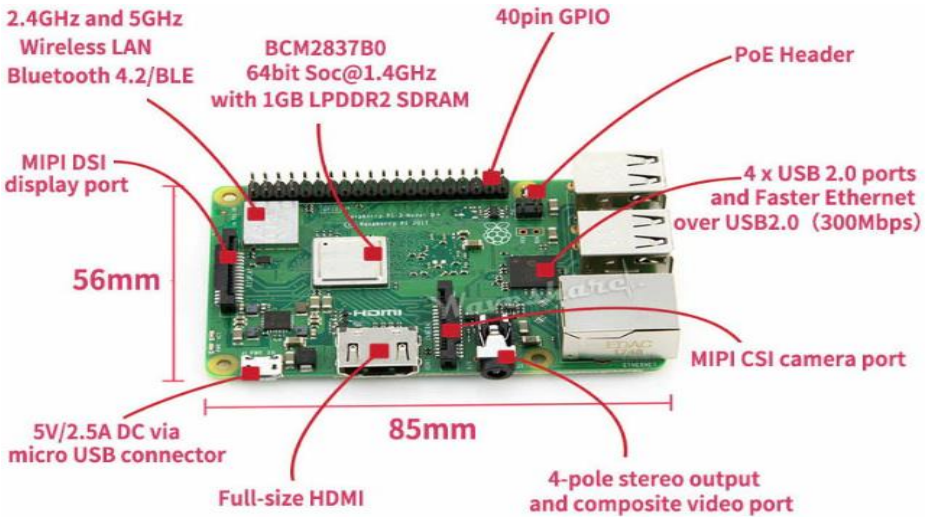

Figure 3.2. Raspberry Pi 3 B+.

c. Caractéristiques du Raspberry Pi 3 B+ [12]:

Processeur	Broadcom BCM2837B0, Cortex-A53 64-bit SoC @ 1.4GHz.
Mémoire	1GB LPDDR2 SDRAM.
Connectivité	2.4GHz and 5GHz IEEE 802.11.b/g/n/ac wireless LAN, Bluetooth 4.2, BLE. Gigabit Ethernet over USB 2.0 (maximum throughput 300Mbps). 4 x USB 2.0 ports.
Access	Extended 40-pin GPIO header.
Support de carte SD	Micro SD format for loading operating system and data storage.
Multimédia	H.264, MPEG-4 decode (1080p30); H.264 encode (1080p30); OpenGL ES1.1, 2.0 graphics.
Vidéos et sons	1 x full-size HDMI. MIPI DSI display port. MIPI CSI camera port. 4 pole stereo output and composite video port.
Alimentation	5V/2.5A DC via micro USB connector. 5V DC via GPIO header. Power over Ethernet (PoE)–enabled (requires separate PoE HAT).
Température	Operating temperature, 0–50°C.

Tableau 3.1. Caractéristiques du Raspberry Pi 3 B+ [12].

III.2.2 L'éclairage :

Un meilleur éclairage derrière un appareil photo ou une webcam nous délivre une très bonne qualité d'image, donc nous avons opté à utiliser un spot (**Figure 3.3.)** dans notre projet pour un meilleur traitement d'image. Un spot LED à lumière blanche.

Figure 3.3. Spot LED.

III.2.3 Webcam :

La webcam est un élément clé dans la réalisation de notre projet, sa qualité et sa résolution nous aident à obtenir une image claire et nette à une distance réduite.

Nous avons utilisé une caméra sport 5 mégas pixel, format H.264 (**Figure 3.4.)**. Donc, une fois la caméra est reliée au Raspberry Pi elle devient une webcam ou pc-Cam.

Figure 3.4. Webcam utilisée.

III.2.4 L'affichage « LCD » :

Dans cette réalisation nous avons utilisé un afficheur LCD (Liquid Crystal Display) de 16x4 c'est-à-dire seize (16) colonnes et quatre (4) lignes connectées au module I2C. Ce dernier permet directement d'avoir quatre (4) sorties au lieu de seize (16) pour le LCD_16x4 (**Figure 3.5.**).

Figure 3.5. Afficheur LCD 4x16 avec I2C.

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

Raspberry Pi	LCD I2C
3.3 V (PIN N°1)	VCC
SDA (PIN N°3)	SDA
SCL (PIN N°5)	SCL
GND (PIN N°6)	GND

Tableau 3.2. Les ports de connexion entre l'écran LCD et le Raspberry Pi.

III.2.5 Capteur Ultrason HC-SR04 :

Le capteur ultrason HC-SR04 (**Figure 3.6.)** est un dispositif électronique dédié à la mesure des distances. Il offre une meilleure plage de détection sans contact. L'utilité de ce dispositif dans notre projet et de capter la présence de la main dans le boiter d'après un calcul de la distance entre le capteur et la main.

Figure 3.6. Capteur Ultrason HC-SR04.

La durée entre l'instant de l'émission et l'instant de la réception peut être mesurée. Le signal ayant parcouru 2 fois la distance entre le capteur et la surface (un aller-retour) (**Figure 3.7.)**, on peut la calculer ainsi : $$distance = \frac{vitesse\ du\ son}{2} \times durée \ldots(1)$$

Remarque : La vitesse du son est environ égale à 340 m/s [13].

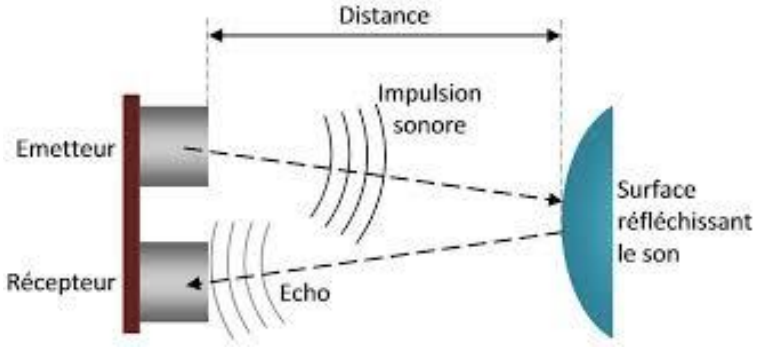

Figure 3.7. Schéma de fonctionnement du Capteur Ultrason HC-SR04.

Caractéristiques

- Dimensions : 45 mm x 20 mm x 15 mm ;
- Plage de mesure : 2 cm à 400 cm ;
- Résolution de la mesure : 0.3 cm ;
- Angle de mesure efficace : 15 ° ;
- Largeur d'impulsion sur l'entrée de déclenchement : 10 µs (Trigger Input Pulse Width).

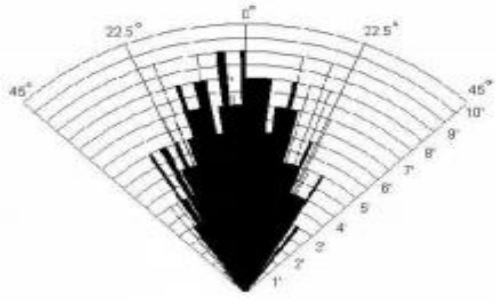

Figure 3.8. Test pratique de performance. Meilleur on angle de 30° [14].

Broches de connexion :

- Vcc = Alimentation +5 V DC ;
- Trig = Entrée de déclenchement de la mesure (Trigger input) ;
- Écho = Sortie de mesure donnée en écho (Echo output) ;
- GND = Masse de l'alimentation.

III.2.6 Modem [15]:

Le modem (mot-valise, pour modulateur-démodulateur) est un dispositif électronique (**Figure 3.9.)**, en boîtier indépendant ou en carte à insérer dans un ordinateur, qui permet de faire circuler (réception et envoi) des données numériques sur un canal analogique. Il effectue la modulation : codage des données numériques, synthèse d'un signal analogique qui est en général une fréquence porteuse modulée. L'opération de démodulation effectue le traitement inverse et permet au récepteur d'obtenir l'information numérique.

On parle de modem pour désigner les appareils destinés à faire communiquer des machines numériques entre elles (ex : ordinateurs, systèmes embarqués), à accéder à Internet, à envoyer ou recevoir des télécopies, à faire de la téléphonie numérique, et ce à travers un réseau analogique (réseau téléphonique commuté, réseau électrique, réseaux radio…).

Figure 3.9. Le modem utilisé.

III.2.7 Un PC serveur :

Un PC serveur est un ordinateur désigné aux gestions des manipulations et la contenance des programmes du traitement des images, logiciels, base des données et le stockage des images venant du boitier, retouche, contrôle, etc.…

III.2.8 Keypad 4x3 :

Le clavier numérique est plus aisé et plus pratique à utiliser, il présente la communication Homme-Machine. On propose d'implémenter un clavier matriciel, pour le choix entre les deux modes mode d'enregistrement et mode d'accès.

Le clavier de 12 touches est équipé de touche numérique 0 à 9, * et #. Le clavier est un ensemble de boutons, organisé en matrice.

Figure 3.10. Keypad 4x3.

III.2.9 Réalisation du boitier :

- Image de la maquette (vue d'extérieur) (**Figure 3.11.**).

Figure 3.11. Image de la maquette (vue d'extérieur).

- Image de la maquette (vue d'intérieur) (**Figure 3.12.**).

Figure 3.12. Image de la maquette (vue d'intérieur).

- Utilisation de la maquette

Cette partie concerne les étapes à suivre pendant l'acquisition :

La (**Figure3.13)** est celle de la maquette finale avec laquelle ont été effectuées les acquisitions des bases de données propres à notre travail.

Figure 3.13. Image de la maquette.

On commence le test par un appui sur le clavier numérique
« 1=> test »
« 2=> Enroll »
On obtient sur l'afficheur un message Test ou Enroll. Donc le système est prêt à recevoir ses clients « main droite » (**Figure3.14)**.

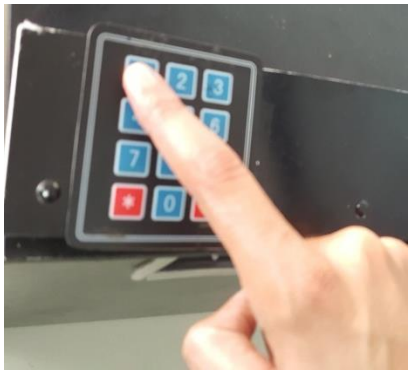

Figure 3.14. Choix du mode.

Mettez la main droite dans le boitier et l'objectif est de garder la main linéaire avec l'avant-bras pour que l'acquisition garde presque le même positionnement pour chaque test (**Figure3.15)**.

Figure 3.15. Entrer la main.

Voici une image d'une main dans l'intérieur du boitier. Le principe est de toucher le fond du boitier par un des doigts, une fois toucher, vous écartez vos doigts tous (**Figure3.16)**.

Figure 3.16. Écartement des doigts.

Comme vous voyez dans la figure il y a un espace entre la main et le haut du boitier (**Figure3.17)**.

Figure 3.17. L'espace entre la main et le haut du boitier.

Pour une meilleure stabilité de l'acquisition, il faut faire glisser la main telle qu'elle est vers le haut avec des doigts écartés et ne pas bouger jusqu'à ce que vous entendiez un bip sonore puis vous retirez la main (**Figure3.18)**.

Figure 3.18. Glisser la main vers le haut.

III.3 Partie software :

III.3.1 Système d'exploitation du RASPBERRY PI 3B+ « Raspbian » :

Raspbian est un système d'exploitation libre qui s'appuie sur la distribution GNU / Linux Debian, optimisée pour la Raspberry Pi.

Raspbian fournit non seulement le système d'exploitation de base, mais également plus de 35000 paquets logiciels précompilés livrés dans un format amélioré - pour une installation plus facile sur Raspberry Pi via des gestionnaires de paquets [16].

La première version des 35000 paquets Raspbian, optimisés pour la Raspberry Pi, a été achevée en juin 2012. Cependant, Raspbian est toujours en développement, dont l'objectif est l'amélioration de la stabilité et des performances pour autant de paquets Debian que possible.

Pourquoi utiliser Raspbian avec la Raspberry Pi ?

Raspberry Pi a toujours moins de puissance qu'un ordinateur moderne. Par conséquent, il est préférable d'installer un système amélioré pour Raspberry. Raspbian a été créé dans cet esprit et convient donc particulièrement à Raspberry. De plus, en tant que distribution dérivée de Debian, elle répond à la plupart des documents volumineux de Debian. Enfin, Raspbian est

sans doute la distribution la plus utilisée pour la Raspberry, bénéficiant ainsi d'une communauté nombreuse et active.

III.3.2 Python 3 :

Python est un langage de script de haut niveau, structuré et open source. Il est multiparadigme et multi-usage. Développé à l'origine par Guido van Rossum en 1989, il est, comme la plupart des applications et outils open source, maintenu par une équipe de développeurs un peu partout dans le monde. Conçu pour être orienté objet, il n'en dispose pas moins d'outils permettant de se livrer à la programmation fonctionnelle ou impérative, c'est d'ailleurs une des raisons qui lui vaut son appellation de « langage agile ».

Parmi les autres raisons, citons la rapidité de développement (qualité propre aux langages interprétés), la grande quantité de modules fournis dans la distribution de base ainsi que le nombre d'interfaces disponibles avec des bibliothèques écrites en C, C++ ou Fortran. Il est également apprécié pour la clarté de sa syntaxe, ce qui l'oppose au langage Perl [17].

Code :

```
import time
import os
import sys
import RPi.GPIO as GPIO
import ftplib as ftp
import socket
from time import sleep
import I2C_LCD_driver
from pad4pi import rpi_gpio
mylcd = I2C_LCD_driver.lcd()
mylcd.lcd_display_string("BIENVENUE",1,4)
mylcd.lcd_display_string("ACCES  => 1",2,0)
mylcd.lcd_display_string("ENROLL => 2",3, -4)

def processKey(key):
  if (key=="1"):
                while True:
                    mylcd.lcd_clear()
                    mylcd.lcd_display_string("ACCES", 2,5)
                    ultrason()
                    pygametest()
                    mylcd.lcd_clear()
                    mylcd.lcd_display_string("MERCI, RETIREZ", 1)
                    mylcd.lcd_display_string("VOTRE MAIN SVP", 2)
                    #time.sleep(3)
                   # mylcd.lcd_clear()
                    os.system('python server.py')
                   # key=""
                    return processKey(key)
                    print("####################################")
  if(key=='2'):
              for i in range (1,4):
                          mylcd.lcd_clear()
                          mylcd.lcd_display_string("ENROLL ",2,5)
                          ultrason()
                          pygameenroll()
```

```
COL_PINS = [21,24,27] #BCM NUMBERING

factory=rpi_gpio.KeypadFactory()

keypad=factory.create_keypad(keypad=KEYPAD, row_pins=ROW_PINS, col_pins=COL_PINS)

keypad.registerKeyPressHandler(processKey)
def ultrason():
    import RPi.GPIO as GPIO
    import time
    GPIO.setmode(GPIO.BCM)
    Trig=23
    Echo=18
    GPIO.setup(Trig,GPIO.OUT)
    GPIO.setup(Echo,GPIO.IN)
    GPIO.output(Trig,False)
    time.sleep(2)
    GPIO.output(Trig,True)
    time.sleep(0.00001)
    GPIO.output(Trig,False)
    while GPIO.input(Echo)==0:
        debutImpulsion=time.time()
    while GPIO.input(Echo)==1:
        finImpulsion=time.time()
    distance=round((finImpulsion - debutImpulsion) * 340 * 100 / 2, 1)
    print("la distance est de :",distance,"cm")
    if (distance < 21.7):
                    print(" hand ok ")
                    mylcd.lcd_clear()
                    mylcd.lcd_display_string("ECARTER VOS",1)
                    mylcd.lcd_display_string("DOIGTS SVP.",2)
                    print("ecarter vos doigts svp ")
                    time.sleep(3)
                    mylcd.lcd_display_string("NE BOUGEZ PAS",3,-4)
                    print("ne bougez pas svp")
                    time.sleep(2)
    else:
          print("no hand")
          return ultrason()
```

```
                    pygametest()
                    mylcd.lcd_clear()
                    mylcd.lcd_display_string("MERCI, RETIREZ", 1)
                    mylcd.lcd_display_string("VOTRE MAIN SVP", 2)
                    #time.sleep(3)
                   # mylcd.lcd_clear()
                    os.system('python server.py')
                   # key=""
                    return processKey(key)
                    print("###################################")
  if(key=='2'):
              for i in range (1,4):
                          mylcd.lcd_clear()
                          mylcd.lcd_display_string("ENROLL ",2,5)
                          ultrason()
                          pygameenroll()
                          mylcd.lcd_clear()
                          mylcd.lcd_display_string("MERCI, RETIREZ",1)
                          mylcd.lcd_display_string("VOTRE MAIN SVP",2)
                          time.sleep(3)
                          mylcd.lcd_clear()
                          print("###################################")
              #mylcd.lcd_display_string("OPERATION",1)
              #mylcd.lcd_display_string("TERMINER MERCI",2)
              #time.sleep(2)
              mylcd.lcd_clear()
              mylcd.lcd_display_string("BIENVENUE",2,4)
              #keypad.cleanup()
              return processKey(key)

KEYPAD=[
        ['1','2','3'],
        ['4','5','6'],
        ['7','8','9'],
        ['*','0','#']
 ]
```

```
    pygame.camera.init()
    pygame.camera.list_cameras()
    cam=pygame.camera.Camera("/dev/video0",(720,480))
    cam.start()
    img=cam.get_image()
    print("snapshot...")
    pygame.image.save(img, 'imagetest.jpeg')
    print("image stockee")
    host="192.168.1.109" #PC YACINE
    port=21
    user="ramy"
    password="yacinehooo"
    obj_ftp= ftp.FTP()
  ## connexion
    obj_ftp.connect(host, port)
  ##login
    obj_ftp.login(user, password)
    file=open('/home/pi/imagetest.jpeg','rb')
    obj_ftp.storbinary('STOR imagetest.jpeg',file)
    print("image envoyee")
   # buzzer()
    file.close()
    cam.stop()
    obj_ftp.quit()

while True:
    time.sleep(1)
```

III.3.3 FTP serveur :

File Transfer Protocol c'est une application installable sur ordinateur, elle permet le transfert des fichiers entre deux points « serveur-client » c'est le même principe qu'un réseau local LAN. L'avantage de cette application est qu'elle a une librairie quand peut utiliser avec Python et cela nous a permis de créer un client sur la Raspberry Pi et le serveur sur le PC-server pour qu'une image prise soit envoyée automatiquement vers le PC-server et le fichier sera stocké dans un emplacement spécifié par l'utilisateur.

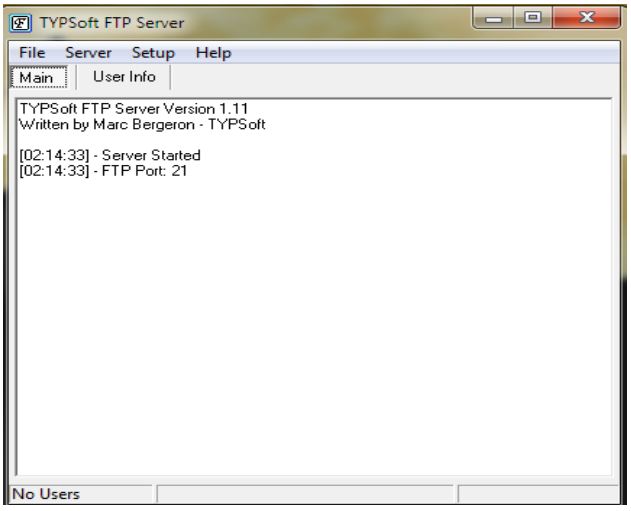

Figure 3.19. Console FTP serveur.

III.3.4 Logiciel Matlab :

MATLAB « Matrix Laboratory » est un logiciel informatique comportant des milliers de fonctions mathématiques développées par des programmeurs de la société MathWorks. Ces fonctions-là aident les utilisateurs de Matlab à générer des programmes dans les différents domaines comme le traitement de signal, traitement d'image, calcul matriciel simple et complexe, méthode numérique, les fonctions de transfert des systèmes, l'asservissement, mécanique…

Matlab est utilisé pour développer des solutions nécessitant une très grande puissance de calcul. Il permet de réaliser des simulations numériques basées sur des algorithmes d'analyse numérique. Il peut donc être utilisé pour la résolution approchée d'équations différentielles, d'équations aux dérivées partielles ou de systèmes linéaires, etc.… [18].

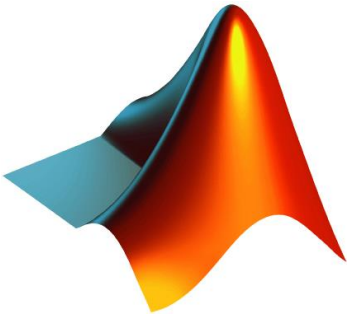

Figure 3.20. Le logo de MATLAB.

III.3.5 Traitement d'image :

On a développé un algorithme d'extraction de 18 points (**Figure 3.20.)** représentée par un vecteur appelé vecteur caractéristique et l'affiche sous forme matricielle.

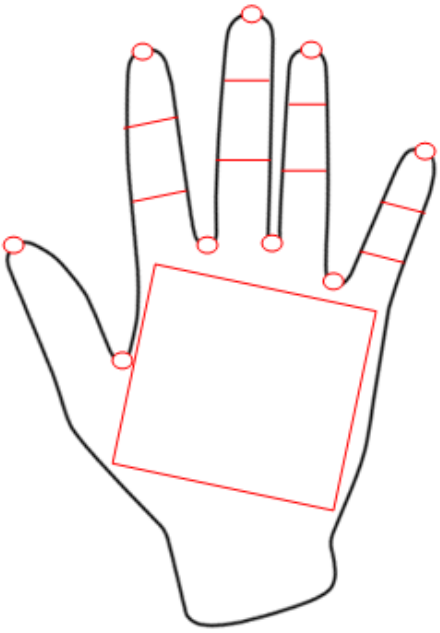

Figure 3.21. Les points caractéristiques de la main.

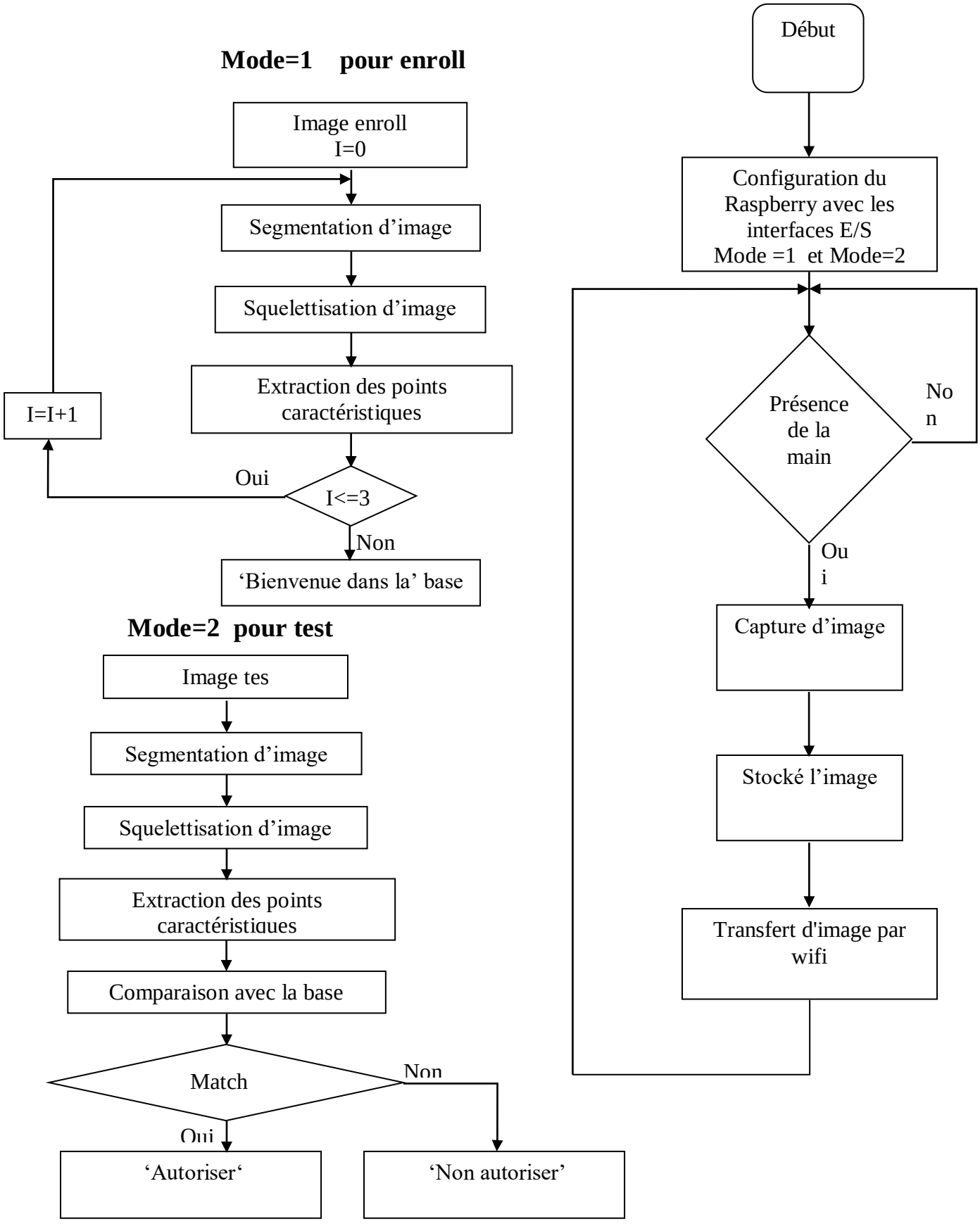
Début
Configuration du Raspberry avec les interfaces E/S Mode =1 et Mode=2
Présence de la main
Non
Oui
Capture d'image
Stocké l'image
Transfert d'image par wifi
Mode=1 pour enroll
Image enroll I=0
Segmentation d'image
Squelettisation d'image
Extraction des points caractéristiques
I<=3
Oui
I=I+1
Non
'Bienvenue dans la' base
Mode=2 pour test
Image tes
Segmentation d'image
Squelettisation d'image
Extraction des points caractéristiques
Comparaison avec la base
Match
Non
Oui
'Autoriser'
'Non autoriser'

Figure 3.22. Organigramme des différentes étapes du traitement « prise d'image + traitement d'image avec Matlab ».

III.3.6 Fonctions de similarités :

Notre système est basé sur la reconnaissance des personnes existantes dans la base de données pour les autorisées d'accès aux personnes et surtout rejeter ceux qui n'en font pas partie de la base. Pour cela plusieurs méthodes de calculs. Il s'agira d'une étude de similarité entre deux vecteurs caractéristiques ou bien de divergences provenant des vecteurs caractéristiques de notre base. Parmi les fonctions de similarités, on a :

a. La distance de Minkowski

La distance de Minkowski est l'approche la plus simple pour mesurer la similarité entre deux images, considérons deux vecteurs **x** et **y**, cette distance $\boldsymbol{D_{\text{Minkowski}}}$ est définie par :

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

Où, $\mathbf{p} \geq \mathbf{1}$ est le facteur de Minkowski, **n** la dimension de l'espace caractéristique.

Les métriques de Minkowski représentent un bon compromis entre efficacité et performance. Pour cette famille de distances, plus les paramètres p augmentent, plus la distance **D(x, y)** aura tendance à favoriser les grandes différences entre coordonnées, ces distances sont rapides à calculer et simples à implémenter, par contre leur calcul est réalisé en considérant que chaque composant de vecteur apporte la même contribution à la distance.

Pour **p = 1**, on obtient la distance Manhattan.

b. La distance de Manhattan « City block »

Elle est aussi appelée « **city block** », cette méthode définit la distance entre 2 vecteurs sur le plan cartésien (**Figure 3.22.**). Entre deux points A et B, de coordonnées respectives (X_A,Y_A) et (X_B,Y_B), la distance de Manhattan est définie par [19]:

$$\mathrm{D}(\mathrm{A},\mathrm{B}) = |X_B - X_A| + |Y_B - Y_A|$$

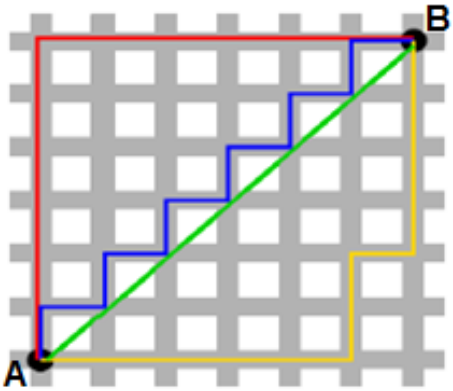

Figure 3.23. Trajets suivis par deux points.

c. La distance de Tchebychev

Est un cas particulier de la distance de Minkowski. Appelé aussi distance de Tchebychev, c'est la distance entre deux points donnée par la différence maximale entre leurs coordonnées sur une dimension. Cette distance est donnée par la formule suivante [20]:

$$\mathrm{D}(\mathrm{A},\mathrm{B}) = \max_{i\in[[0,n]]}(|A_i - B_i|)$$

d. La distance de Hamming

Elle est utilisée généralement dans le codage de canal dans une chaine de transmission. 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 $\boldsymbol{x}$ **=** $\boldsymbol{(x1, \ldots, xn)}$ et $\boldsymbol{y}$ **=** $\boldsymbol{(y1, \ldots, yn)}$ tel qu'on notera $\boldsymbol{\mathrm{D}(x, y)}$ étant le nombre d'indices $\boldsymbol{i}$ tels que $\boldsymbol{xi \neq yi}$

La distance minimale du code C est le minimum des $\boldsymbol{\mathrm{D}(x, y)}$ pour $\boldsymbol{x}$ et $\boldsymbol{y}$ 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. $\boldsymbol{C(n, k, d)}$.

Exemple 1 : Considérons les suites binaires suivantes :

C1= (0 0 0 1 1 1 1) et **C2= (1 1 0 1 0 1 1),** C'est un code de longueur **7** et de distance **d=1+1+0+0+1+0+0=3**

Exemple 2 : Considérons les suites binaires suivantes :

a= (1 0 1 1 1 0 1) et **b= (1 0 0 1 0 0 1)** La distance de Hamming entre **a** et **b** est **2**.

Notons que le poids de Hamming correspond au nombre d'éléments non nul (≠ 0) dans une chaîne d'élément [21].

e. La distance Euclidienne

C'est le type de distance qui nous utilisons depuis la 2eme année moyenne et la plus couramment utilisée. Il s'agit d'une distance géométrique dans un espace multidimensionnel (2D, 3D…). On calcule la distance par la formule suivante :

$$D(X,Y) = \sqrt{\sum_{i=1}^{n} (xi - yi)^2}$$

f. La similarité cosinus

La mesure cosinus sert à calculer la similarité entre deux vecteurs à n dimensions en déterminant l'angle entre eux. Cette métrique est souvent utilisée en fouille de textes.

Soit deux vecteurs A et B, cos θ s'obtient par le produit scalaire et la norme des vecteurs :

$$\cos\theta = \frac{A.B}{||A||.||B||}$$

g. Le coefficient de corrélation γ

Le coefficient de corrélation linéaire **γ** donne une mesure de l'intensité et du sens de la relation linéaire entre deux variables. On utilise souvent la calculatrice ou un logiciel pour faire le calcul du coefficient car il est assez complexe [22]. Le coefficient de corrélation est compris entre -1 et 1. Ce coefficient est déterminé par la formule suivante :

$$\gamma = \frac{cov(x,y)}{\delta x \delta y} = \frac{E\big((x - E(x))(y - E(y))\big)}{\delta x \delta y} = \frac{E(xy) - E(x)E(y)}{\delta x \delta y}$$

Où **Cov(X,Y)** désigne la covariance des variables **x** et y, $\boldsymbol{\delta x}$ *et* $\boldsymbol{\delta y}$ leurs écarts types et **E** désignent l'espérance mathématique.

- Plus **γ** est proche de 1, plus la relation linéaire positive entre les variables est forte.
- Plus **γ** est proche de -1, plus la relation linéaire négative entre les variables est forte.
- Plus le coefficient est proche de 0, plus la relation linéaire entre les variables est faible.

h. Le coefficient de corrélation de rang Spearman

Le coefficient de corrélation de rang (appelé coefficient de Spearman) examine s'il existe une relation entre le rang des observations pour deux caractères X et Y, ce qui permet de détecter l'existence de relations monotones (croissante ou décroissante), quelle que soit leur forme précise (linéaire, exponentielle, puissance ...). Ce coefficient est donc très utile lorsque l'analyse du nuage de points révèle une forme curviligne dans une relation qui semble mal ajustée à une droite [23].

Le coefficient de Spearman est fondé sur l'étude de la différence des rangs entre les attributs des individus pour les deux caractères **X** et **Y** :

$$\gamma(X,Y) = 1 - \frac{6 \times \sum_{i=1}^{N} (r(X_i) - r(Y_i))^2}{N^3 - N}$$

$r(X_i)$: rang de X_i dans la distribution $X_1 \ldots X_N$

$r(Y_i)$: rang de Y_i dans la distribution $Y_1 \ldots Y_N$

III.3.7 La méthode HOG « Histogram of Orientes Gradient » :

Un histogramme de gradient orienté (**HOG**) est une caractéristique utilisée en vision par ordinateur pour la détection d'objet. La technique calcule des histogrammes locaux de l'orientation du gradient sur une grille dense, c'est-à-dire sur des zones régulièrement réparties sur l'image. Elle possède des points communs avec les SIFT (Scale-Invariant Feature Transform), les Shape contexts et les histogrammes d'orientation de contours (ce sont des algorithmes pour la détection d'objet ou de reconnaissance de caractères), mais en diffère notamment par l'utilisation d'une grille dense.

La méthode **HOG** est particulièrement efficace pour la détection de personnes [24].

III.3.8 La fusion :

Ajouter une modalité à un système biométrique, c'est ajouter une nouvelle source d'information. C'est pourquoi les systèmes multimodaux permettent d'obtenir de meilleurs résultats que les systèmes monomodaux.

La fusion de données consiste essentiellement à confronter et intégrer des informations multiples dans le but de compenser la faible qualité de l'acquisition et de réduire l'incertitude sur l'information résultante.

Dans notre projet on fait la fusion entre deux modalités, la modalité de la géométrie et la modalité de l'empreinte palmaire. On fait cette fusion par une méthode qui s'appelle **ACP** (**A**nalyse en **C**omposantes **P**rincipales), cette dernière est une méthode très utilisée en statistique. Sa principale idée est de réduire la dimension d'un jeu de données tout en gardant un maximum d'informations. Cela est réalisé grâce à une projection qui maximise la variance tout en minimisant l'erreur quadratique moyenne de la reconstruction.

III.3.9 Évaluation de la vérification :

Pour évaluer la performance d'un système de biométrie il faut étudier des paramètres parmi eux le **FRR** (**F**alse **R**ejection **R**ate) c'est le rejet d'un utilisateur légitime et le **FAR** (**F**alse **A**cceptance **R**ate) c'est l'acceptation d'un imposteur. Ils sont deux données qui évoluent de façon inversement proportionnelle (**Figure 3.24.**).

Si la sécurité du système est privilégiée, le FAR devra être bas, tandis qu'un système plus convivial aura un FRR bas.

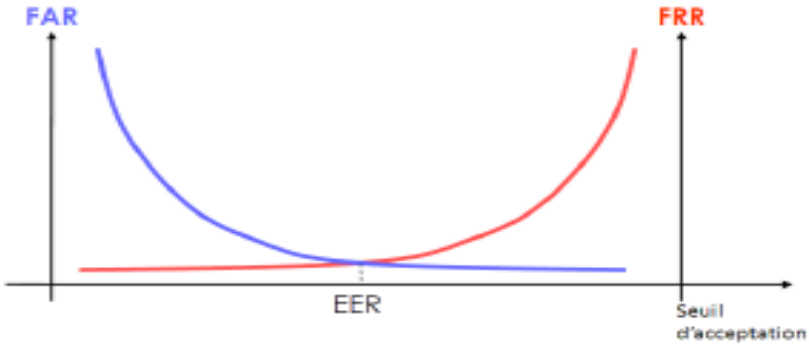

Figure 3.24. Évolution des taux de FAR et FRR en fonction du seuil de similitude.

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.

D'après la loi de Bayes en prenant C comme l'image provient d'un utilisateur légitime donc $(H1/C) > (H0/C)$ ce qui donne :

$$\frac{\mathrm{P(C/H1)\ P(H1)}}{\mathrm{P(C)}} > \frac{\mathrm{P(C/H0)\ P(H0)}}{\mathrm{P(C)}} \Rightarrow \frac{\mathrm{P(C/H1)}}{\mathrm{P(C/H0)}} > \frac{\mathrm{P(H0)}}{\mathrm{P(H1)}}$$

On compare ce taux $\frac{\mathrm{P(C/H1)}}{\mathrm{P(C/H0)}}$ par un seuil de décision nommée θ nous permet de dresser la figure suivante (**Figure 3.25.**) qui donne le taux de vraisemblance en fonction de la probabilité des FAR et FRR [21].

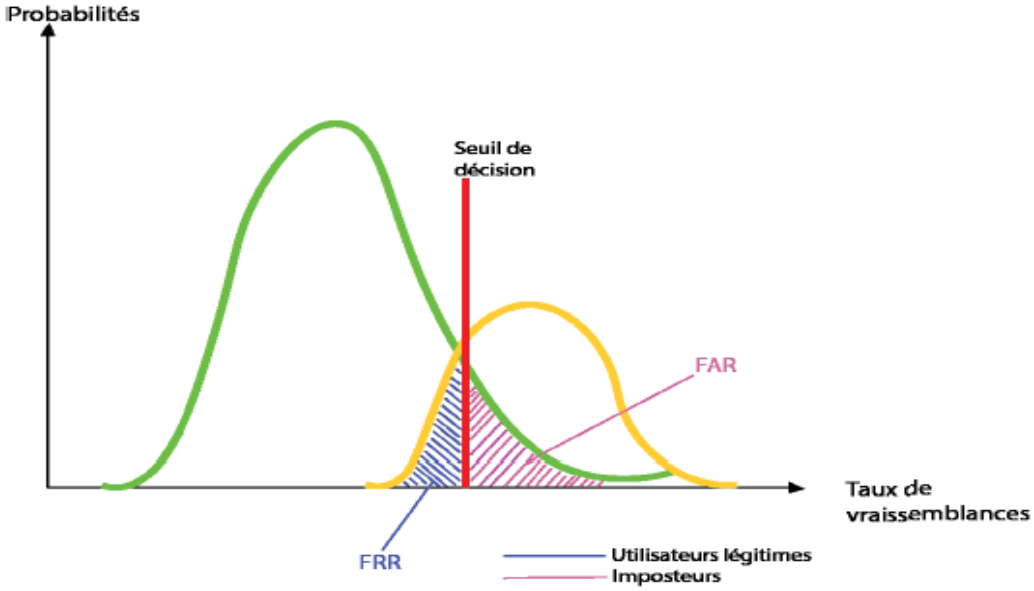

Figure 3.25. Taux de vraisemblance des utilisateurs légitimes et des imposteurs.

Le taux de faux rejet en fonction du taux de fausse acceptation nous donne une courbe qui s'appelle **ROC** (**R**eceiver **O**perating **C**haracteristic) (**Figure 3.26.**) représente la performance pour les différentes valeurs de θ.

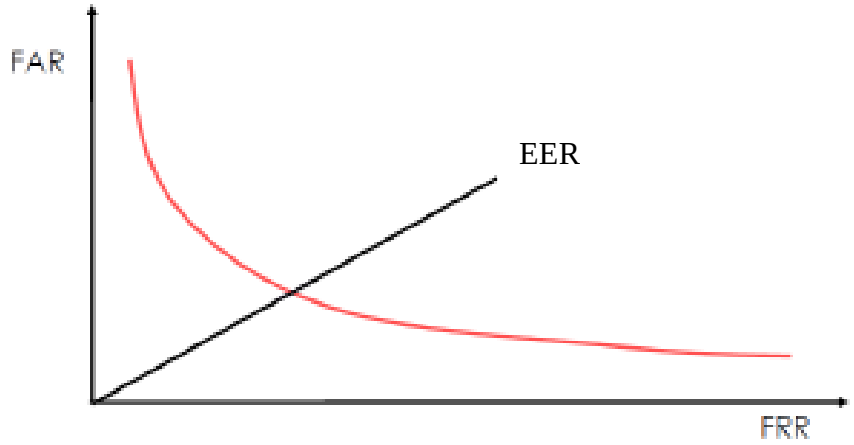

Figure 3.26. La courbe ROC.

Le taux d'erreur d'égal (**E**qual **E**rror **R**ate ou **EER**) correspond au point **FAR** = **FRR**, c'est-à-dire graphiquement à l'intersection de la courbe ROC avec la première bissectrice. Ce taux est fréquemment utilisé pour donner un aperçu de la performance d'un système biométrique.
Quand **EER** tend vers **0**, le système est très performant.

III.4 Conclusion :

Ce chapitre nous a permis de connaitre les différents dispositifs (hardware et software) qu'on utilisé dans notre réalisation puis l'acquisition des données et les traitements nécessaires pour produire les vecteurs caractéristiques. on a vu aussi un certain nombre de méthodes de traitement d'image.

Chapitre IV

« Résultats expérimentaux »

IV.1 Introduction :

Ce chapitre, présente les étapes essentielles du traitement d'image avec démonstration, sous Matlab, des résultats expérimentaux obtenus par traitement d'images appliqué à notre base de données avec les différentes modalités géométrique et palmaire de la main et l'extraction des points caractéristiques des deux modalités et cela grâce aux méthodes mathématiques de calcul des distances concernant la modalité géométrique, algorithmes HOG (Histogram of Oriented Gradient) pour la modalité palmaire et l'algorithme ACP (Analyse en Composante Principale) pour la fusion entre les deux modalités.

Le choix d'une méthode mathématique se fait par rapport à l'erreur EER. Et pour renforcer les résultats et minimiser de l'erreur EER on a fusionné les deux modalités pour une amélioration accrue et un renforcement de notre système d'un point de vue authentification.

Des courbes Far, Frr et ROC sont incluses dans ce chapitre pour une meilleure interprétation des résultats.

IV.2 Traitement des images acquises par la caméra :

Pour le traitement des images, il faut que l'image passe par des étapes successives pour aboutir au résultat final en passant par la segmentation et la squelettisation et puis l'extraction de points caractéristiques.

Initialement, on segmente l'image originale **(Figure 4.1.)** par une conversion de l'image couleur en image binaire pour que l'image devienne à deux couleurs, noir et blanc en passant par les niveaux de gris intermédiaires. Le fond choisi, intentionnellement, noir de notre maquette nous facilite l'étape de la segmentation d'image (**Figure 4.2.)**.

Figure 4.1. Image originale de la main.

Figure 4.2. Image segmentée de la main.

Après la segmentation, on extrait le contour et le squelette puis une rotation de la main est opérée (**Figure 4.3.)** de la main segmentée par une angle φ pour que le doigt majeur de la main soit perpendiculaire avec l'axe des abscisses pour faciliter l'extraction des points caractéristiques et les points caractéristiques sont déterminés (**Figure 4.4.)** pour être utilisés dans la suite du traitement.

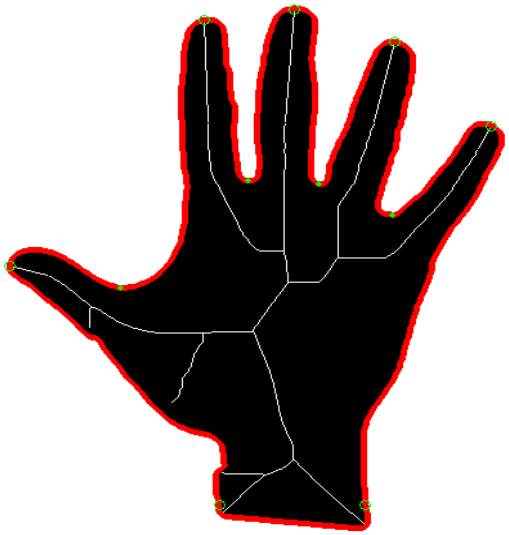

Figure 4.3. Squelette + rotation de la main.

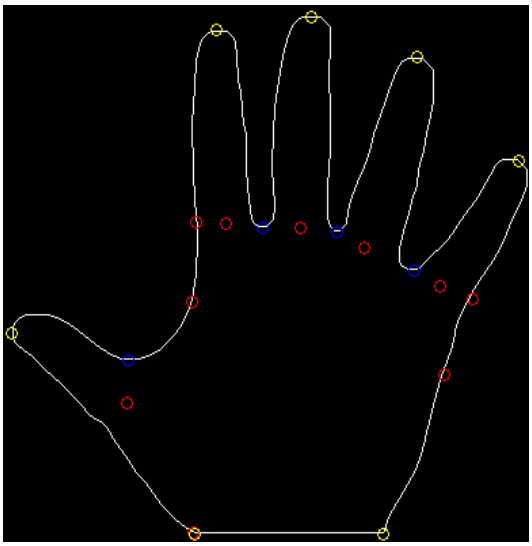

Figure 4.4. Contour et points caractéristiques.

Les différents points caractéristiques générés dans la figure précédente renseignent sur les coordonnées de la dimension de la main, la largeur, la longueur, la paume de la main (**Figure 4.5.**).

Ensuite, on applique un cadre qui servira au masquage de l'image originale de la main sur le contour pour obtenir une image de l'empreinte palmaire (**Figure 4.6.**).

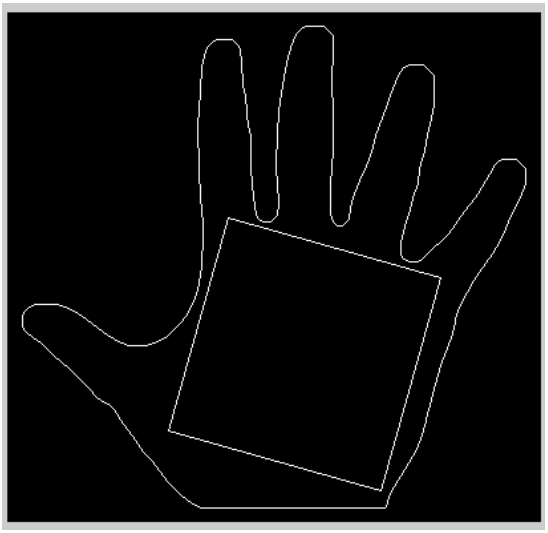

Figure 4.5. Contour + cadre pour la paume.

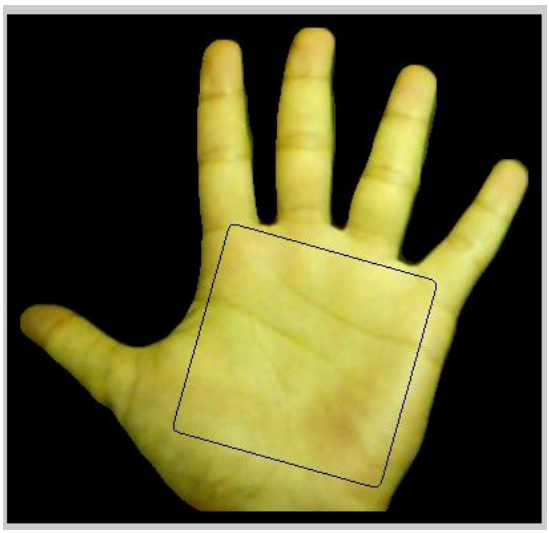

Figure 4.6. Masquage et image de la paume.

IV.3 Résultats expérimentaux :

Avant de discuter les résultats expérimentaux des différentes modalités, il convient de signaler que ces résultats sont obtenus avec une base de données contenant 35 personnes.

IV.3.1 la géométrie de la main :

Différentes méthodes	Moy inter-classe **myint**	Max inter-classe **maxin**	Min inter-classe **minin**	Écart type inter-classe **etint**	Moy extra-classe **Myex**	Min extra-classe **Minex**	max extra-classe **Maxex**	Écart type extra-classe **etext**	**EER**
Euclidien	9,085	57,349	0	7,917	32,722	7,348	104,680	16,264	0.085
Cityblock	26,990	119	0	18,222	93,392	24	322	44,198	0.069
Minkowski	9,085	57,349	0	7,917	32,722	7,348	104,680	16,264	0.085
Cosine	0,001	0,033	0	0,004	0,003	0,0002	0,047	0,005	0.113
Corrélation	0,002	0,069	0	0,009	0,006	0,0006	0.110	0,011	0.151
Spearman	0,034	0,409	0	0,055	0,071	0,003	0,617	0,072	0.287
Tchebychev	5,533	38	0	5,487	21,021	4	57	10,454	0.108

Tableau 4.1. Différentes méthodes de similarité sur la modalité de **la géométrie de la main.**

Les résultats des différentes des méthodes sont présentés graphiquement dans les (**Figures 4.7., 4.8., 4.9., 4.10., 4.11., 4.12., 4.13.)** (Courbes Frr, Far et courbe ROC).

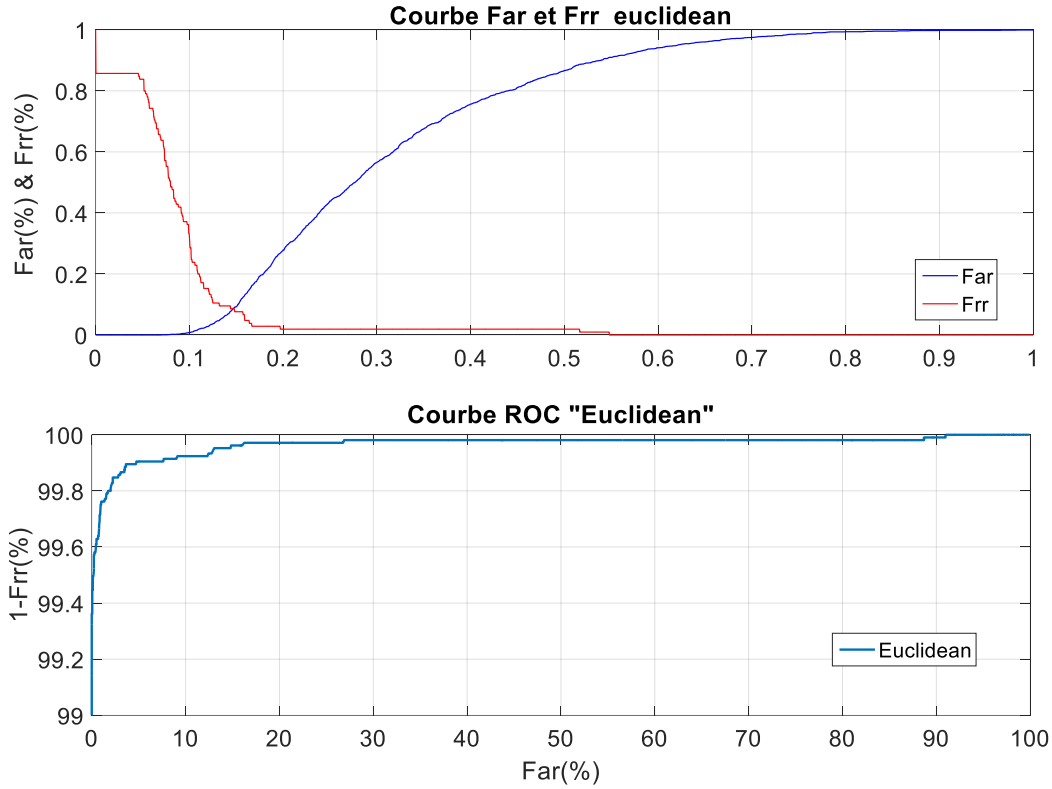

Figure 4.7. La courbe Far, Frr et ROC de la méthode euclidienne.

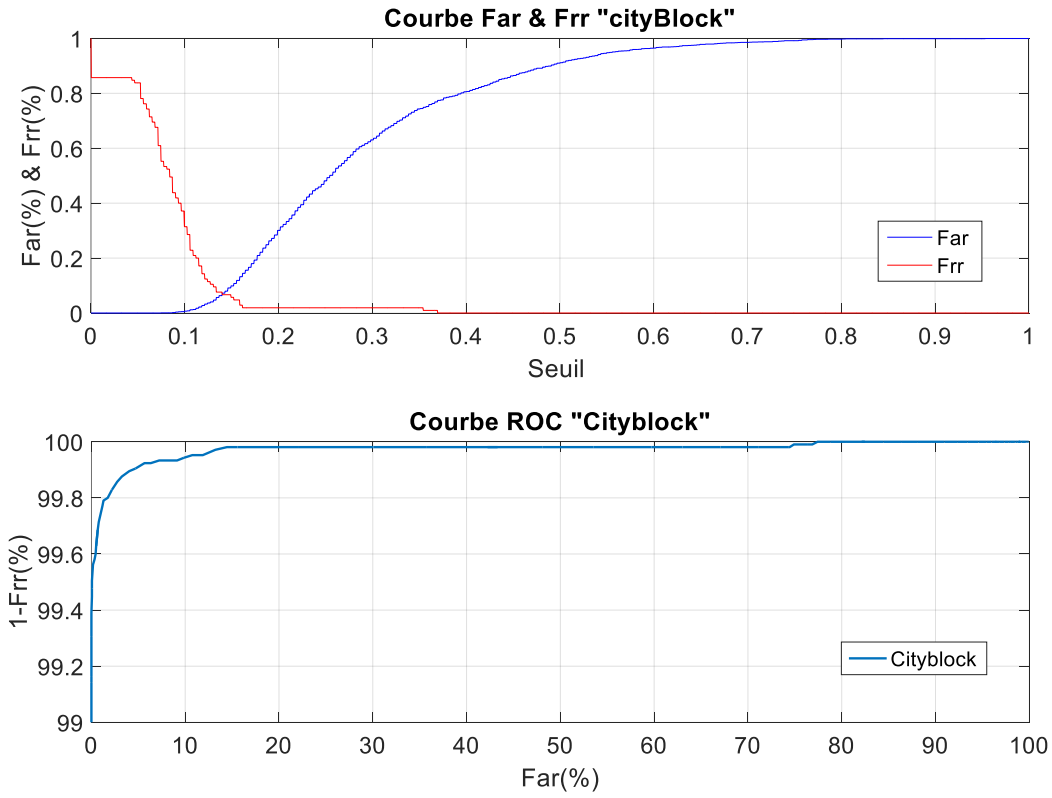

Figure 4.8. La courbe Far, Frr et ROC de la méthode Manhattan (City block).

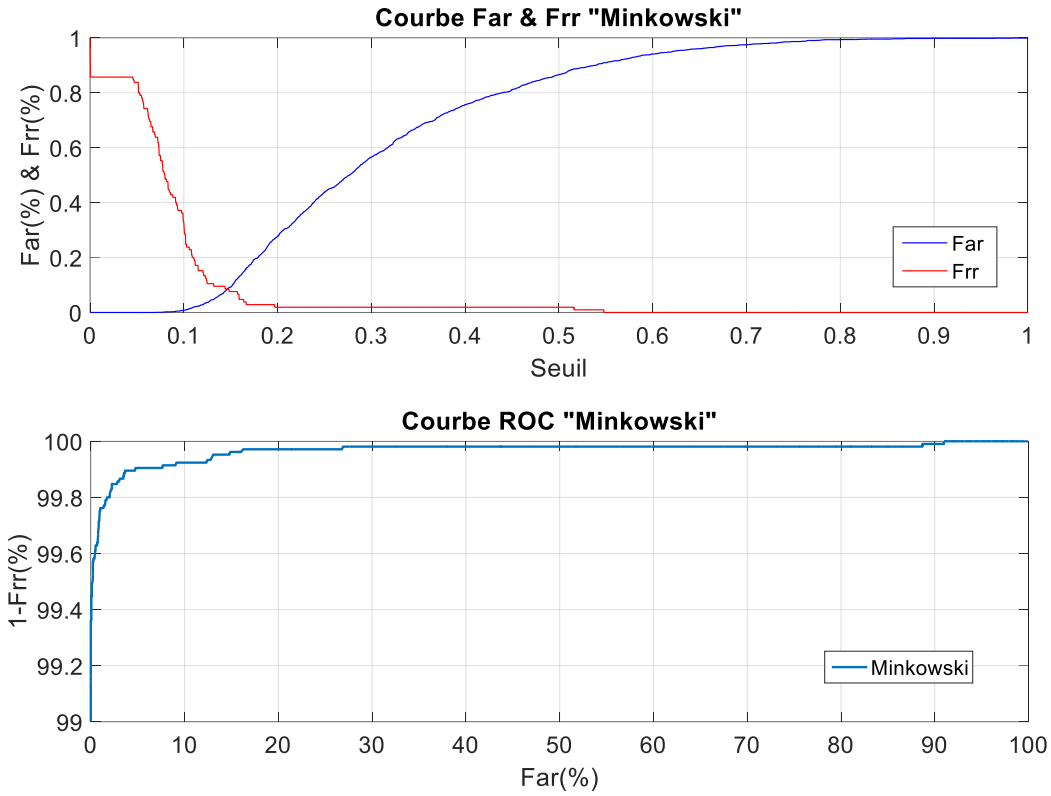

Figure 4.9. La courbe Far, Frr et ROC de la méthode Minkowski.

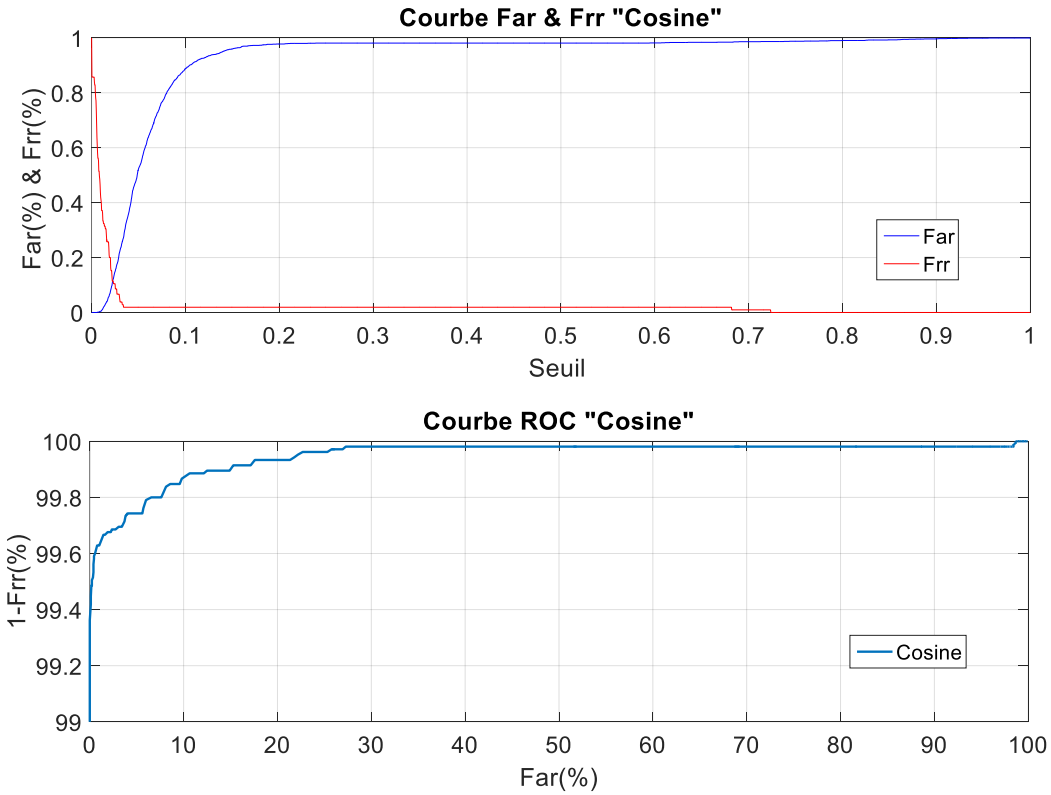

Figure 4.10. La courbe Far, Frr et ROC de la méthode Cosine.

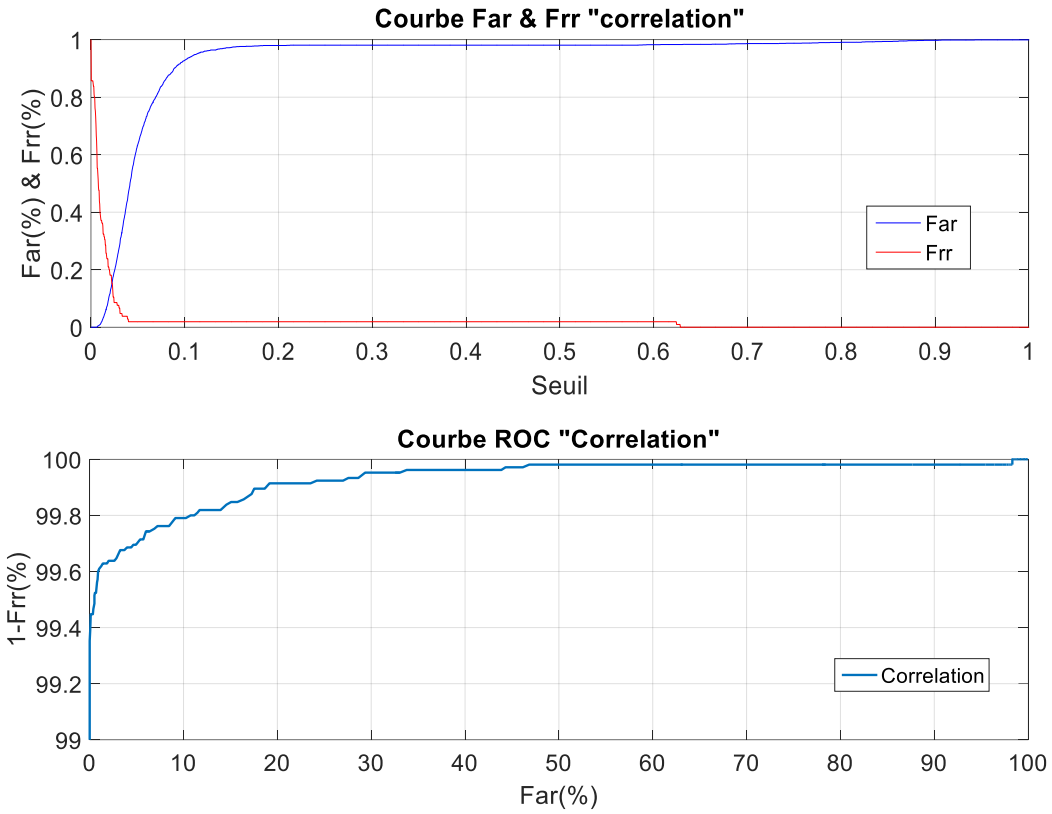

Figure 4.11. La courbe Far, Frr et ROC de la méthode Corrélation.

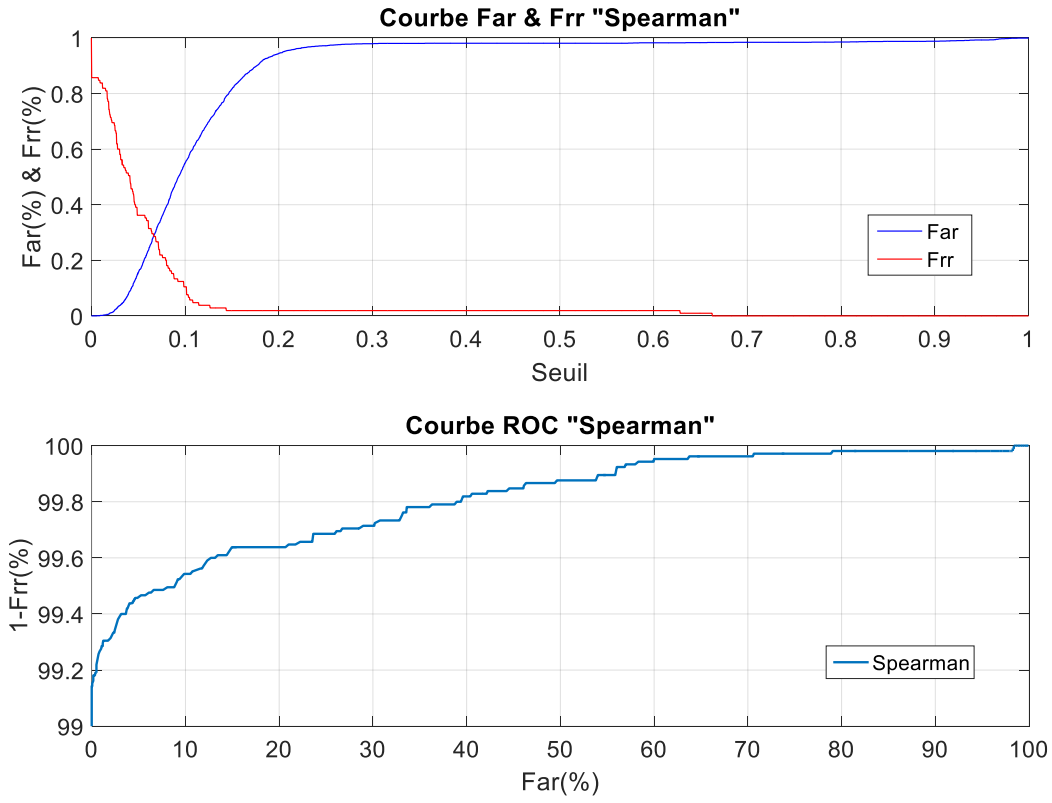

Figure 4.12. La courbe Far, Frr et ROC de la méthode Spearman.

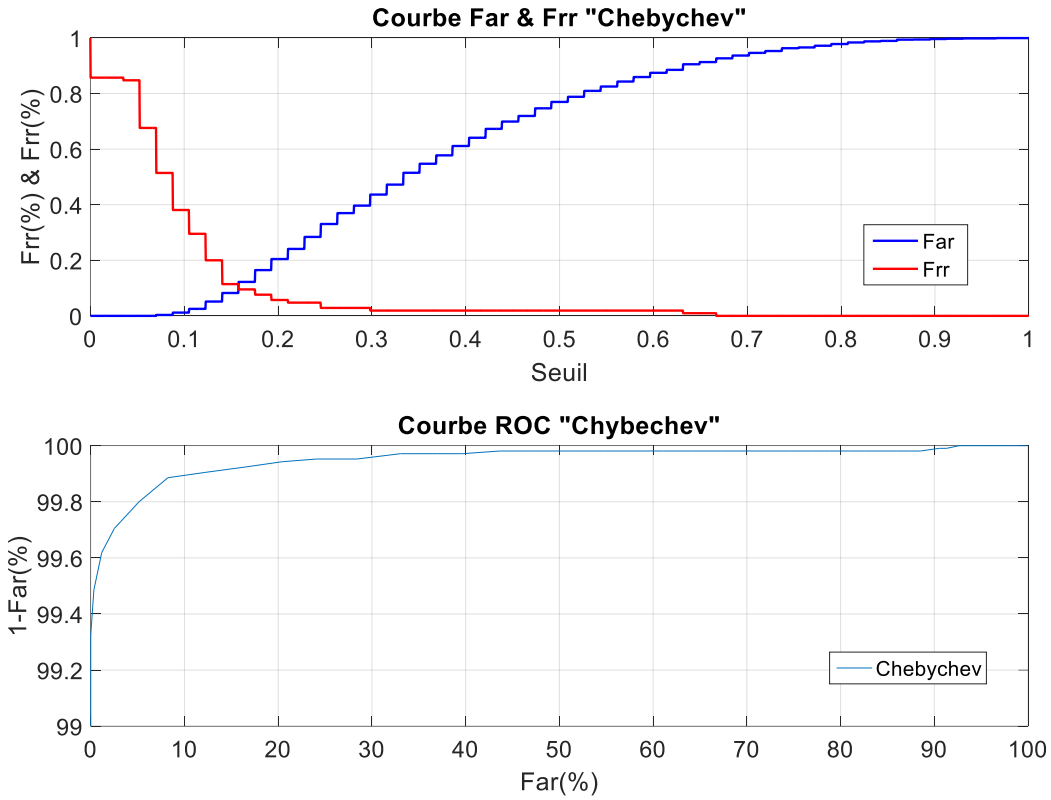

Figure 4.13. La courbe Far, Frr et ROC de la méthode Tchebychev.

Les résultats figurant dans le **tableau 4.1.,** et les courbes des (**Figures 4.7., 4.8., 4.9., 4.10., 4.11., 4.12., 4.13.),** montrent que la meilleure méthode de similarité pour la géométrie de la main est celle de City block (Manhattan) avec un EER = 0.069.

IV.3.2 L'empreinte palmaire méthode HOG :

Différentes méthodes Pour n	**n**	Moy inter-classe **myint**	Max inter-classe **maxin**	Min inter-classe **minin**	Ecart type inter-classe **etint**	Moy extra classe **Myex**	Min extra-classe **Minex**	max extra classe **Maxex**	Écart type extra classe **etext**	**EER**
Euclidien	**20**	0,203	0,510	0	0,098	0,414	0,153	0,774	0,093	0,100
	34	0,729	1,153	0	0,324	1,393	0,913	2,292	0,208	0,037
	60	1,881	3,025	0	0,818	3,181	2,257	4,156	0,291	0,057
City block	**20**	0,922	2,634	0	0,464	1,994	0,650	4,143	0,518	0,096
	34	9,858	16,389	0	4,447	19,784	12,273	36,019	3,365	0,038
	60	51,637	85,197	0	22,704	91,098	62,673	124,652	9,311	0,056
Minkowski	**20**	0,203	0,510	0	0,098	0,414	0,153	0,774	0,093	0,100
	34	0,729	1,153	0	0,324	1,393	0,913	2,292	0,208	0,037
	60	1,881	3,025	0	0,818	3,181	2,257	4,156	0,291	0,057
Cosine	**20**	0,025	0,130	0	0,018	0,090	0,011	0,300	0,041	0,100
	34	0,035	0,073	0	0,018	0,110	0,046	0,291	0,034	0,037
	60	0,058	0,127	0	0,029	0,141	0,070	0,239	0,026	0,057
Corrélation	**20**	0,176	0,771	0	0,139	0,591	0,046	1,549	0,280	0,135
	34	0,185	0,519	0	0,115	0,548	0,173	1,292	0,171	0,114
	60	0,279	0,582	0	0,152	0,661	0,326	1,089	0,128	0,076
Spearman	**20**	0,183	0,740	0	0,138	0,596	0,075	1,569	0,276	0,143
	34	0,189	0,516	0	0,114	0,550	0,198	1,281	0,168	0,105
	60	0,281	0,588	0	0,152	0,662	0,322	1,078	0,127	0,076
Chybechev	**20**	0,085	0,164	0	0,042	0,156	0,070	0,237	0,028	0,145
	34	0,137	0,216	0	0,060	0,211	0,137	0,302	0,022	0,133
	60	0,181	0,266	0	0,077	0,251	0,191	0,353	0,022	0,180

Tableau 4.2. Différentes méthodes de similarités sur la modalité de **l'empreinte palmaire.**

n : résolution du nombre de pixels du cadre de l'empreinte palmaire.

Les résultats des différentes méthodes sont présentés graphiquement dans les (**Figures 4.14.**, **4.15.**, **4.16.**, **4.17.**, **4.18.**, **4.19.**, **4.20.)** (Courbes Frr, Far et courbe ROC) pour une valeur de **n=34**.

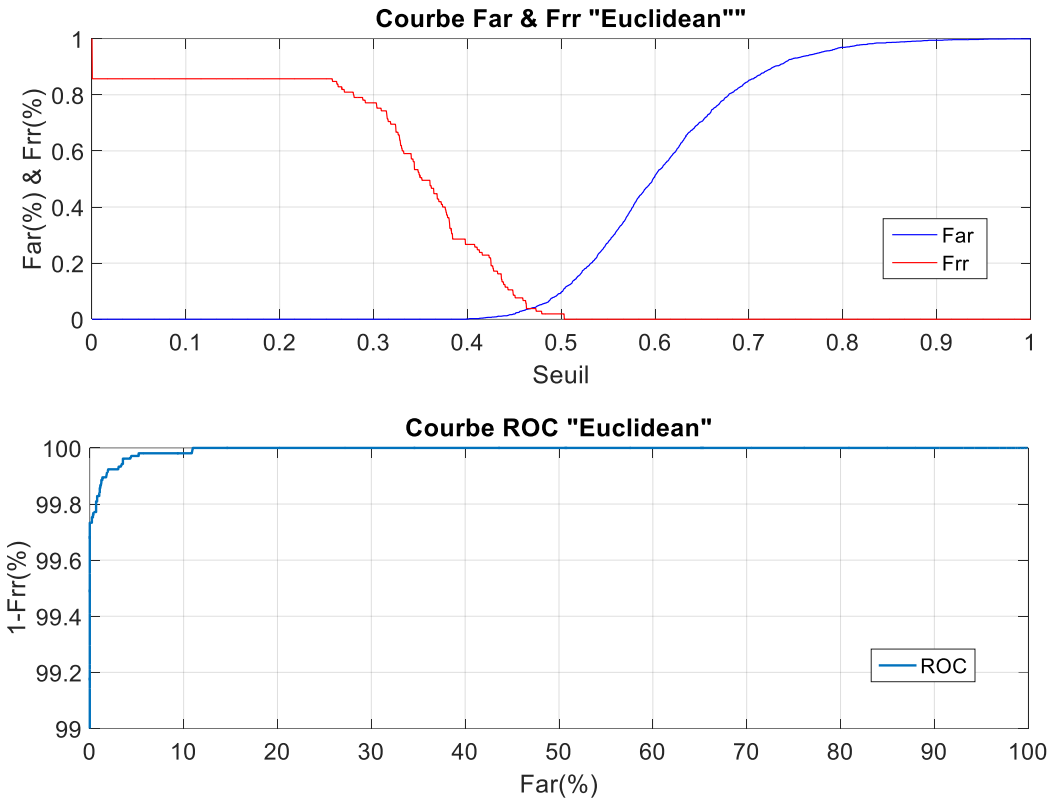

Figure 4.14. La courbe Far, Frr et ROC de la méthode euclidienne.

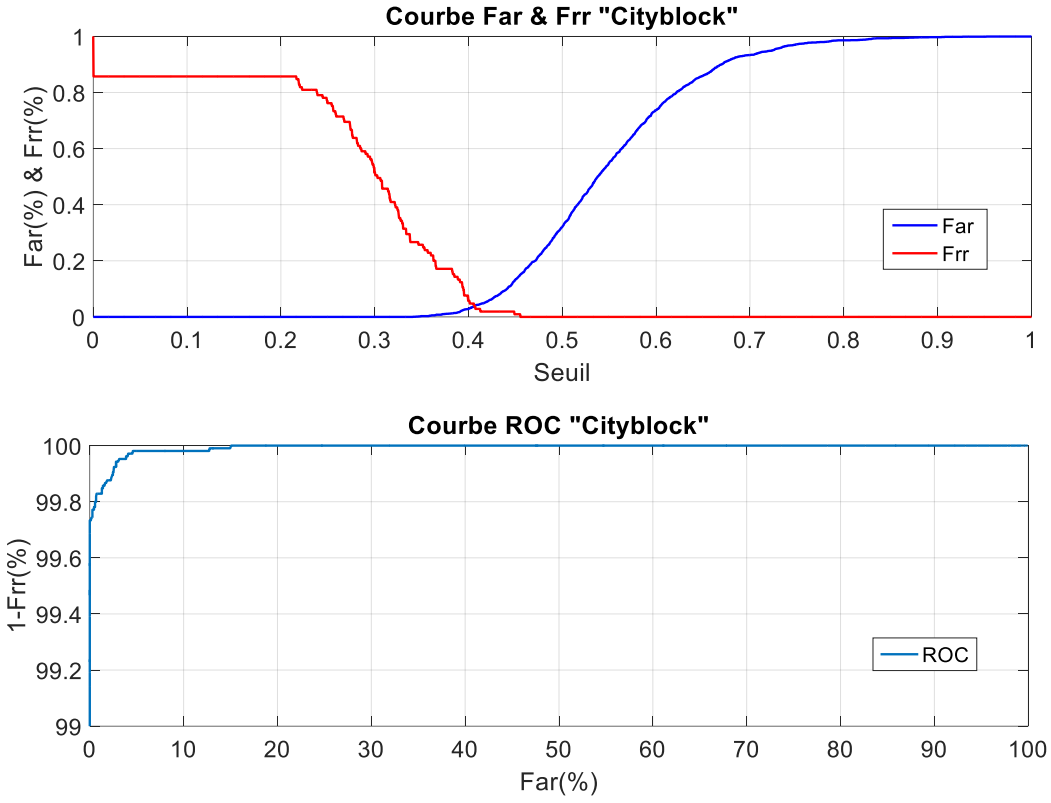

Figure 4.15. La courbe Far, Frr et ROC de la méthode Manhattan (City block).

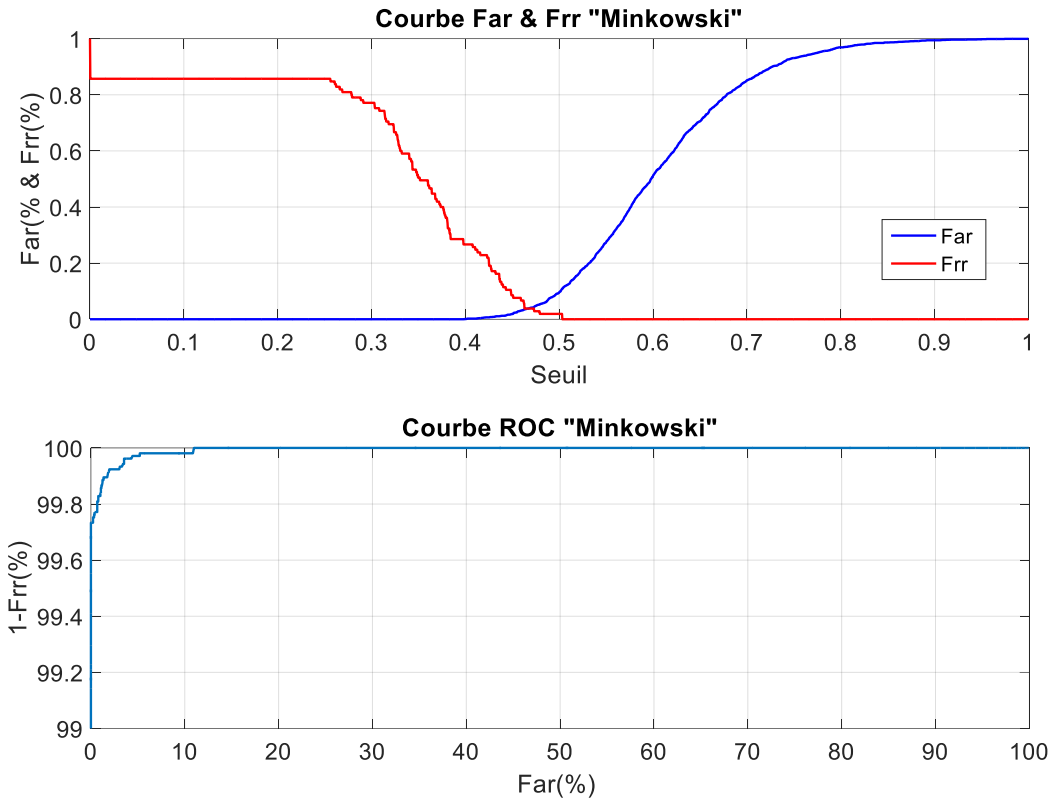

Figure 4.16. La courbe Far, Frr et ROC de la méthode Minkowski.

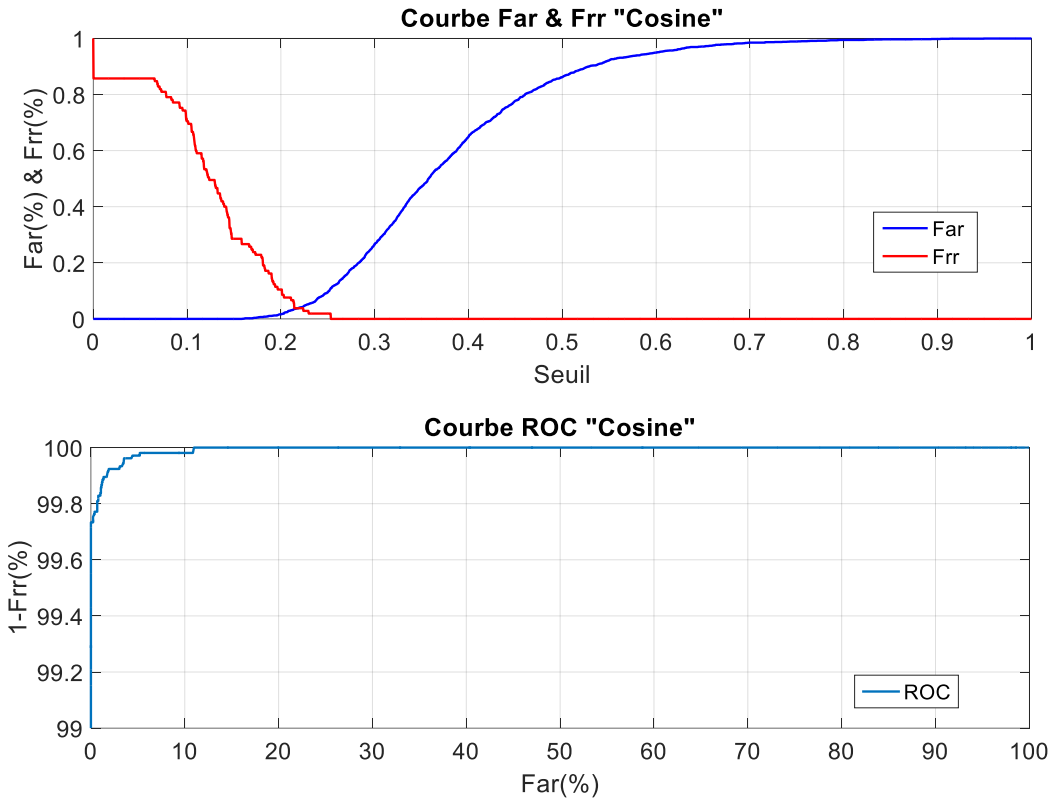

Figure 4.17. La courbe Far, Frr et ROC de la méthode Cosine.

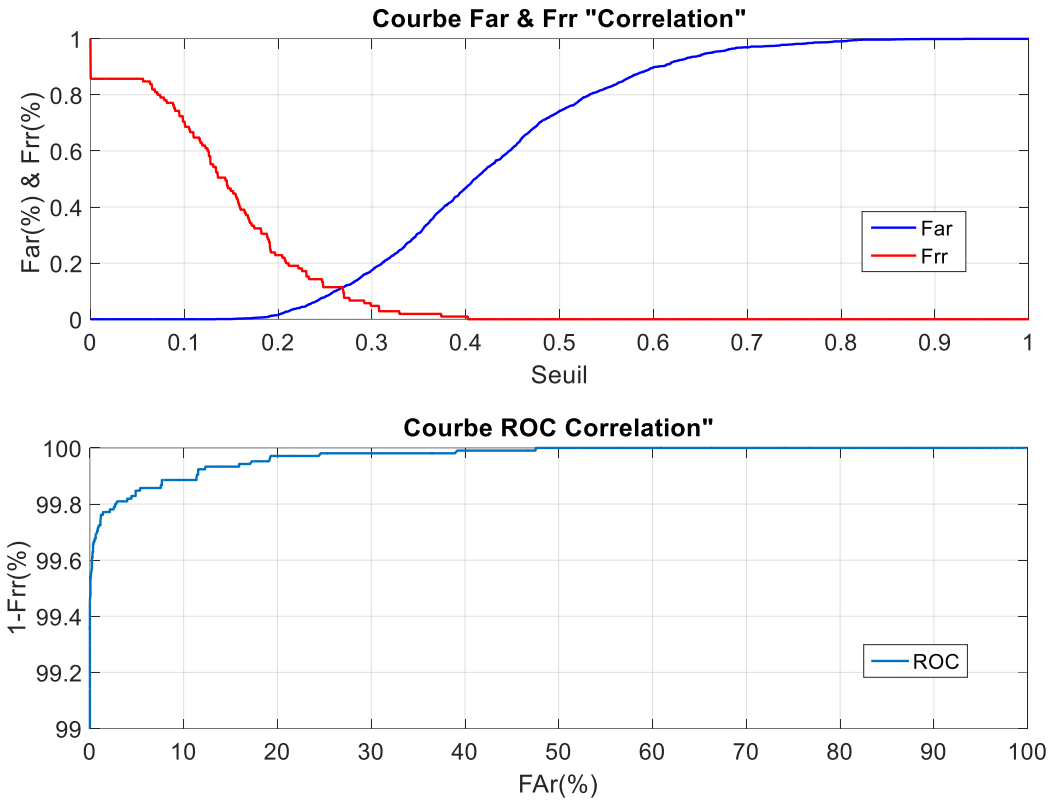

Figure 4.18. La courbe Far, Frr et ROC de la méthode Corrélation.

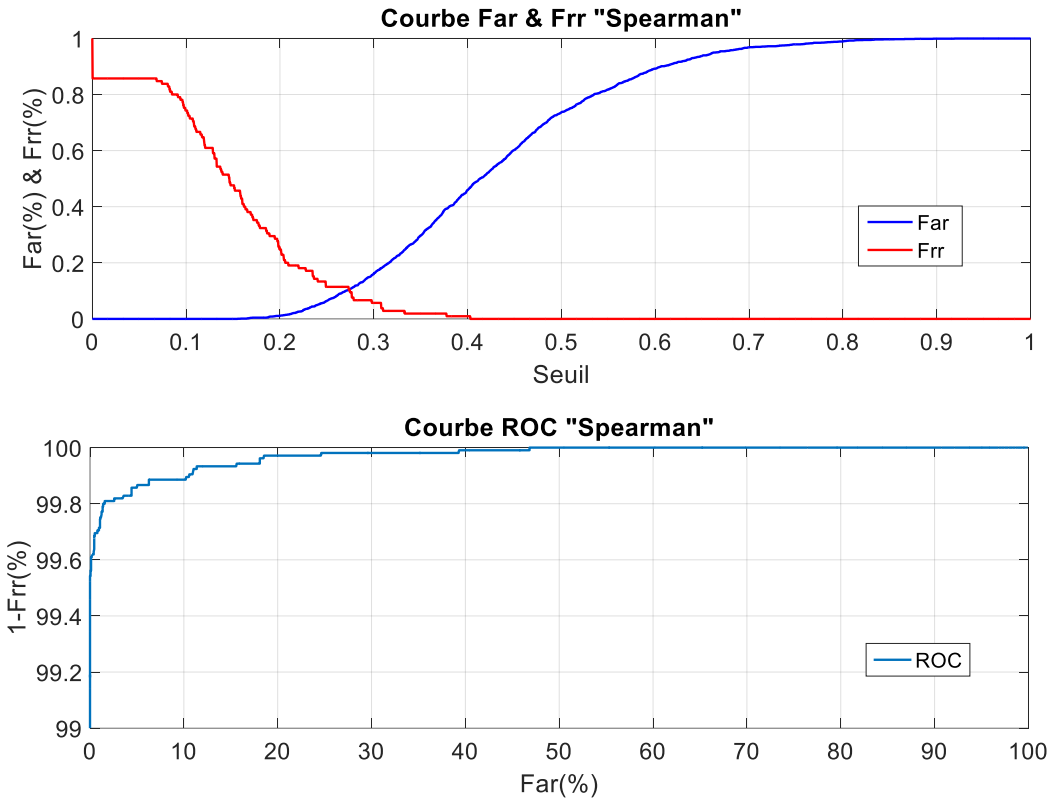

Figure 4.19. La courbe Far, Frr et ROC de la méthode Spearman.

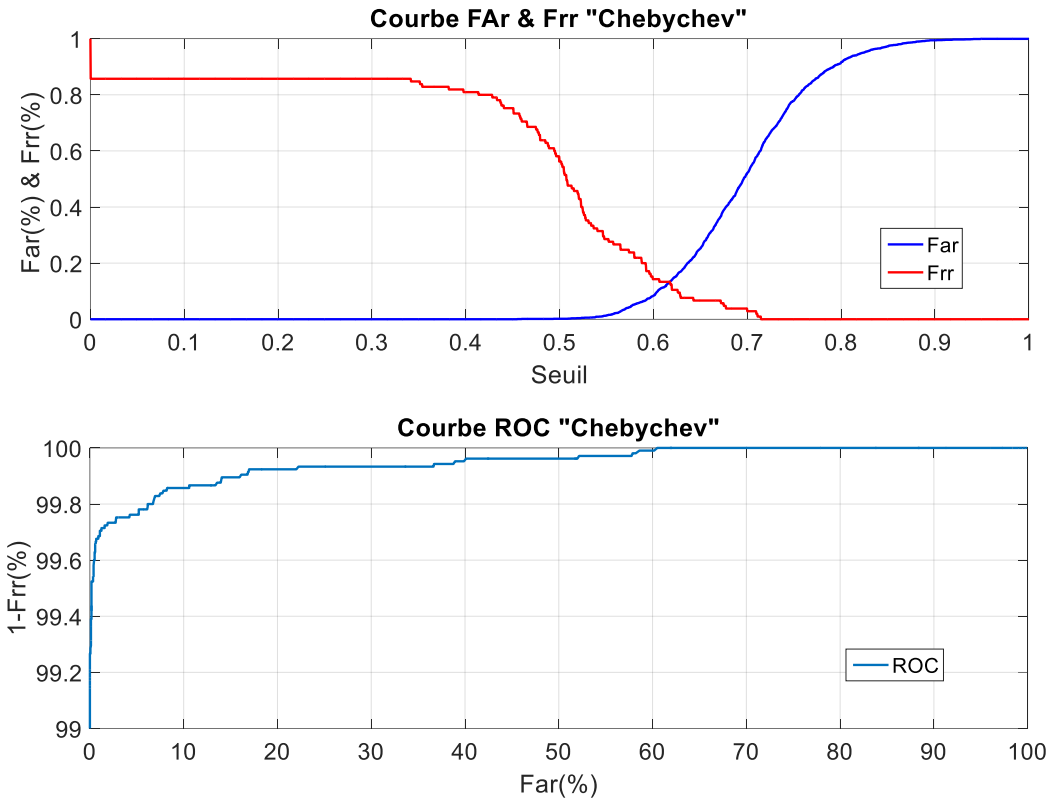

Figure 4.20. La courbe Far, Frr et ROC de la méthode Tchebychev.

Les résultats figurant dans le **tableau 4.2.**, et les (**Figures 4.14.**, **4.15.**, **4.16.**, **4.17.**, **4.18.**, **4.19.**, **4.20.),** montrent que la meilleure méthode de similarité pour l'empreinte palmaire est celle de Minkowski, Euclidean, Cosine avec un EER = 0.037 selon l'algorithme de HOG.

IV.3.3 Fusion des deux modalités utilisant la méthode ACP:

Différentes méthodes	Moy inter-classe **myint**	Max inter-classe **maxin**	Min inter-classe **minin**	Ecart type inter-classe **etint**	Moy écart extra classe **Myex**	Min écart extra-classe **Minex**	max écart extra classe **Maxex**	Écart type extra classe **etext**	**EER**
Euclidien	10,040	20,760	0	5,127	24,447	13,715	43,264	3,968	0.028
City block	48,643	104,953	0	24,819	106,939	63,735	154,79	12,174	0.041
Minkowski	10,040	20,760	0	5,127	24,447	13,715	43,264	3,968	0.028
Cosine	0,219	0,926	0	0,166	1,020	0,187	1,664	0,204	0.030
Corrélation	0,218	0,936	0	0,166	1,020	0,194	1,664	0,207	0.038
Spearman	0,314	0,796	0	0,196	1,018	0,445	1,549	0,135	0.019
Chybechev	4,010	11,746	0	2,152	12,960	4,990	37,228	4,748	0.036

Tableau 4.3. Différentes méthodes de similarités sur la modalité de **fusion « méthode ACP»**.

Les résultats figurant dans le **tableau 4.3.,** montrent que la meilleure méthode de similarité pour la fusionne des deux modalités est celle de Spearman avec un EER = 0.019 selon la méthode ACP.

À la fin de ces expériences nous avons formé une base de données secondaire pour faire les mêmes expériences, mais dans ce cas-là l'objectif était le 'sans contact' cela veut dire qu'une fois la main est introduire dans le boitier ne touche rien (main en l'air) jusqu'au le bip sonore, mais les résultats étaient défavorables.

Différentes méthodes	**EER**
Euclidien	0,304
City block	0,293
Minkowski	0,304
Cosine	0,183
Corrélation	0,170
Spearman	0,245
Tchebychev	0,322

Tableau 4.4. Différentes méthodes de similarités sur la modalité de **la géométrie de la main.**

EER des résultats des mains non stables (en l'air).

Différentes méthodes	**EER**
Euclidien	0.103
City block	0.097
Minkowski	0.103
Cosine	0.103
Corrélation	0.124
Spearman	0.123
Tchebychev	0.171

Tableau 4.5. Différentes méthodes de similarités sur la modalité de **l'empreinte palmaire.**

EER des résultats des mains non stables (en l'air).

Différentes méthodes	EER
Euclidien	0,097
City block	0,118
Minkowski	0,097
Cosine	0,029
Corrélation	0,038
Spearman	0,057
Tchebychev	0,114

Tableau 4.6. Différentes méthodes de similarités sur la modalité de **l'empreinte palmaire et la géométrie de la main « fusion » avec ACP.**

EER des résultats des mains non stables (en l'air).

IV.4 Conclusion :

Après avoir passé en revue les étapes du traitement d'image ainsi que les différentes méthodes qu'on a utilisées pour l'extraction des points caractéristiques, servant à développer un système fiable et à avoir de bons résultats pour aboutir à une bonne authentification 'sans' erreur (taux d'erreur le plus réduit), nous sommes arrivés à définir les correspondances appropriées qui lient chaque méthode à son application, à savoir City block (Manhattan) pour le calcul des distances (géométrie de la main), euclidean pour l'empreinte palmaire et Spearman pour la fusion des deux modalités par la méthode ACP.

V.1 Conclusion générale :

La réalisation maquette issu de notre projet de fin d'études, nous a permis d'aborder différentes caractéristiques biométriques ainsi que leurs performances.

Cette réalisation consistait à concevoir deux parties : une matérielle et l'autre logicielle garantissant un choix judicieux des dispositifs et des protocoles de communication sans fils permettant une transmission de données entre le kit d'acquisition et le PC-server.

Un des enjeux était la réduction de l'encombrement du dispositif biométrique et en particulier ses dimensions comparé à celui de l'année dernière. La caméra utilisée, quant à elle, bien que limitée en qualité d'image et en résolution, ne nous a pas empêchés d'obtenir un meilleur résultat que ceux obtenus lors des PFE des années précédentes.

Dans les différentes étapes de ce travail, on a exposé les procédures du traitement d'image et de l'extraction des points caractéristiques, ainsi pour le matching nous avons expérimenté plusieurs méthodes de calcul de distance, la méthode la plus performante dans notre cas étant celle du Spearman.

Il a étais aussi démontré que la fusion des caractéristiques entre les deux modalités, celle de la géométrie et de l'empreinte palmaire, passant par une réduction de la dimension du vecteur caractéristique par la méthode ACP, nous a permis une nette amélioration des performances.

Bien que notre travail a donné des résultats plus que satisfaisante en termes de performances biométrique, il reste néanmoins sensible à des attaque frauduleuse, puisque une image de la main des utilisateurs pourra être utilisé pour un accès non autorisé. Ainsi comme perspective a ce travail un ajout d'une caméra infrarouge pour l'acquisition d'une nouvelle modalité biométrique tel que le réseau veineux de la main nous permettra a l'avenir d'accroitre la sécurité de notre dispositif biométrique.

Références bibliographiques

[1] : Pierre Mauroy - L'Express - 13/09/2001 : "Sécurité: la gauche s'endurcit"

[2] : https://www.inspq.qc.ca/publications/149

[3]:https://www.chefdentreprise.com/Definitions-Glossaire/Securite-au-travail-245262.htm#Ly74s2Ed98UqZXXQ.97

[4] : https://rfid.ooreka.fr/comprendre/code-a-barres

[5] : https://rfid.ooreka.fr/comprendre/radio-identification

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

[7] : ZEMMIT Saad, « Identification d'un individu par l'EMG (L'électromyogramme) » Master Académique de l'UNIVERSITE MOHAMED BOUDIAF - M'SILA, 2018

[8] : https://www.memoireonline.com/03/15/8967/m_Conception-et-mise-en-place-dune-plateforme-de-securisation-par-synthese-et-reconnaissance-biom3.html

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

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

[11] : https://www.numerama.com/startup/raspberry-pi

[12] : https://static.raspberrypi.org/files/product-briefs/Raspberry-Pi-Model-Bplus-Product-Brief.pdf

[13] : http://www.orbit-dz.com/produit/scanner-automobile-2/arduino-compatibles/shields-et-accessoires/sons-voix-p-shields/hc-sr04-detail

[14] : https://kychem.wordpress.com/2015/09/18/the-hc-sr04-ultra-sonic-distance-sensor/

[15] : https://fr.wikipedia.org/wiki/Modem

[16] : https://raspbian-france.fr/

[17] : https://fr.wikibooks.org/wiki/Programmation_Python/Introduction

[18] : https://www.mathworks.com

[19] : https://fr.wikipedia.org/wiki/Distance_de_Manhattan

[20] : https://fr.wikipedia.org/wiki/Distance_de_Tchebychev

[21] : Maman Lourwana Issaka, «Etude et conception d'un système de pointage biométrique» Master 2 de Université Abdelhamid Ibn Badis de Mostaganem, 2018

[22]:https://fr.khanacademy.org/math/statistics-probability/describing-relationships-quantitative-data/scatterplots-and-correlation/a/correlation-coefficient-review

[23] : http://grasland.script.univ-paris-diderot.fr/STAT98/stat98_6/stat98_6.htm

[24] :https://fr.wikipedia.org/wiki/Histogramme_de_gradient_orient%C3%A9