



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



Projet soutenu dans le cadre de l'arrêté 1275



MEMOIRE

Présenté pour obtenir le diplôme de

MASTER EN ELECTRONIQUE

Option : électronique des systèmes embarqués

Par :

◆ Benaissa Abdel djallel Djilali

◆ Bendaouadji Sadek El amine

Intitulé du sujet

Réalisation d'un système de verrouillage Biométrique

Soutenu le 08/07/ 2023 devant le jury composé de :

Année Universitaire 2022/2023

Président :	Mr AZZEDINE Mohammed	FST GE Université de Mostaganem
Examineur 1:	Dr HEENI Sidahmed	FST GE Université de Mostaganem
Représentant de l'incubateur	Dr MEKHATRIA Djilali	FST GP Université de Mostaganem
Représentant de partenaire socioéconomique	Mm. ZINE el Houda	SETRAM Mostaganem
Rapporteur :	Pr MERAH Mostefa	FST GE Université de Mostaganem

Remerciements

Tout d'abord, nous aimerions exprimer notre gratitude envers notre créateur, qui nous a donné la force et la patience nécessaires pour mener à bien cette tâche.

Nous voudrions également remercier chaleureusement nos parents pour leur soutien constant et leurs encouragements tout au long de nos années d'études.

Nous tenons à exprimer notre profonde gratitude et notre reconnaissance respectueuse envers notre encadrant, Mr. Mostefa MFRATH, qui a généreusement accepté de superviser notre travail. Nous le remercions sincèrement pour son soutien et ses conseils inestimables.

Nous souhaitons également remercier tous nos enseignants, nos amis et toutes les personnes qui nous ont apporté leur aide et leur soutien tout au long de la réalisation de ce projet.

Leur contribution précieuse a été d'une importance capitale pour notre réussite, et nous leur sommes profondément reconnaissants.

Dédicace

Tout d'abord, je veux remercier Dieu Pour m'avoir donné la force et le courage de diriger Bon dans cet humble travail.

Nous dédions cet humble travail à :

nos chers parents qui ont un grand crédit pour leur patience et leurs encouragements tout au long de ces années d'études.

Nos sœurs et tous mes amis.

Et à tous ceux qui m'aiment et que j'aime

Sommaire

Introduction générale	1
------------------------------------	---

Chapitre 1 Les systèmes d'accès Biométrique

Introduction.....	4
1.1 Modes opératoires d'un système biométrique.....	7
1.2 Evaluation d'un système biométrique.....	8
1.3 Limites de la mono modalité et solution multimodale.....	12
1.4 Biométrie et multimodalité.....	14
1.4.1 Taxonomie des Systèmes biométriques multimodaux	14
1.4.2 Architectures d'un système multimodal.....	17
1.4.3 Niveaux de fusion multimodale	18
1.4.4 Fusion au niveau des scores	20
1.4.5 Normalisation des scores.....	23
Conclusion	26

Chapitre 2 Système biométrique de la main

Introduction.....	27
2.1 La biométrie de la main.....	27
2.2 Pourquoi utiliser La biométrie de la main?	28
2.3 Topographie et L'anatomie de la main.....	29
2.4 La géométrie de la main.....	30
2.5 Les doigts.....	30
2.6 La paume de la main.....	31
2.7 Caractéristiques de l'empreinte palmaire.....	32
2.8 Réseau veineux	33
2.9 Les dispositifs de la biométrie de la main	34
2.9.1 Dispositifs biométrique avec contact.....	34
2.9.2 Dispositifs biométrique sans contact.....	35
Conclusion.....	36

Chapitre 3 Conception et réalisation hardware et software du dispositif biométrique

Introduction.....	37
3.1 Partie hardware.....	38
3.1.1 RASPBERRY PI.....	39
3.1.1.1 Les caractéristiques dr Raspberry pi 3.....	40

3.1.2	Capteur Ultrason HC-SR04.....	40
3.1.2.1	Caractéristiques.....	41
3.1.2.2	Broche de connexion.....	41
3.1.2.3	Distance de l'objet.....	42
3.1.3	Caméra.....	42
3.1.4	Clavier.....	43
3.1.5	L'éclairage.....	44
3.1.6	Afficheur LCD.....	45
3.1.6.1	Caractéristiques.....	45
3.1.6.2	Fonction PIN sur l'interface.....	46
3.1.7	Router « modem »	46
3.1.8	Un PC serveur.....	47
3.2	Réalisation du boîtier.....	47
3.2.1	Utilisation du prototype.....	48
3.3	Partie software.....	51
3.3.1	Organigramme.....	51
3.3.2	RASPBERRY PI 3B+.....	52
3.3.3	Configuration.....	52
3.3.4	Logiciel Matlab	53
3.3.5	Python 3	54
3.3.5.1	Les principales utilisations de python par les développeurs sont	54
3.3.6	FTP serveur.....	55
3.3.7	Traitement d'image	56
3.3.7.1	Traitement d'image géométrie de la main.....	57
3.4	Résultats de la biométrie de la main.....	59
3.4.1	La Géométrie de la main	59
3.4.2	La texture de la paume de la main.....	63
	Conclusion.....	70

Conclusion

générale	71
-----------------------	----

ANNEXE Etude économique et cout du prototype Startup et BMC

Introduction.....	72
4.1 Business Model Canvas.....	73
4.2 Coût Prototype	74
4.3 L'annexe BMC.....	75
Conclusion.....	83
Références bibliographiques.....	84

Liste des figures

Figure 1. 1 Evolutions du marché biométrique mondial par technologies. A droite : parts de marché en 2009, à gauche : prévisions des parts de marché en 2017.	6
Figure 1. 2 Processus de fonctionnement d'un système biométrique.....	7
Figure 1. 3 Systèmes en mode d'identification en groupe ouvert et en groupe fermé.....	7
Figure 1. 4 Système en mode vérification.	8
Figure 1. 5 Illustration du FAR et du FRR (a) à travers leur variation en fonction du seuil de décision et (b) à travers les distributions des authentiques et des imposteurs.	10
Figure 1. 6 Courbes DET : FRR en fonction du FAR, (à gauche) en échelle linéaire et (à droite) en échelle logarithmique.	11
Figure 1. 7 Courbe ROC : TAR en fonction du FAR.	11
Figure 1. 8 Les multiples sources d'information dans un système biométrique multimodal.....	15
Figure 1. 9 Architectures d'un système multimodal (a) en série, (b) hiérarchique, (c) parallèle	18
Figure 1. 10 Les différents niveaux de fusion dans un système biométrique multimodal.....	20
Figure 2. 1 La géométrie de la main	28
Figure 2.2 Anatomie de la paume de la main droite	29
Figure 2.3 Dissection profonde palmaire	29
Figure 2.4 Les points caractéristiques dans la géométrie de la main.....	30
Figure 2.5 Surface des 5 doigts	31
Figure 2.6 La paume de la main.	32
Figure 2.7 L'empreinte palmaire.	32
Figure 2.8 Caractéristiques géométriques de l'empreinte palmaire	32
Figure 2.9 La biométrie du réseau veineux de la main.....	34
Figure 2.10 Le dispositif d'acquisition CCD bidimensionnel à base contact.....	35
Figure 2.11 Dispositif d'acquisition à base sans contact.....	36
Figure 3.1 Schéma synoptique.	38
Figure 3. 2 Logo Raspberry Pi.....	39
Figure 3.3 Raspberry Pi 3B+.....	40
Figure 3.4 Capteur Ultrason HC-SR04	41
Figure 3.5 Capteur Ultrason Broches de connection.	41
Figure 3.6 Capteur Ultrason Distance de L'objet.	42
Figure 3.7 La caméra utilisée	43
Figure 3.8 Clavier.....	43
Figure 3.9 Caplage interieur de Clavier 3x4.	44
Figure 3.10 L'éclairage.	44
Figure 3.11 Afficheur LCD 4x16.	45
Figure 3.12 Style D'affichage de LCD.....	45
Figure 3.13 Le modem utilisé.....	46
Figure 3.14 PC serveur.....	47
Figure 3. 15 Image de la maquette (vue extérieur).	47
Figure 3. 16 Image de la maquette (vue intérieur).	48
Figure 3. 17 Image de la maquette.	48
Figure 3. 18 Choix du mode.	48

Figure 3. 19 Choix du mode.	49
Figure 3. 20 Image de la main.....	49
Figure 3. 21 L'espace entre la main et le haut du boîtier.	49
Figure 3. 22 Glisser la main vers le haut.	50
Figure 3.23 Organigramme.....	51
Figure 3.24 Interface de Raspberry Pi 3B+.....	52
Figure 3.25 Logo de Matlab.....	53
Figure 3.26 Logo de Python.....	55
Figure 3.27 Console FTP serveur.....	55
Figure 3.28 Image noir et blanc	56
Figure 3.29 Image de la main avant le Traitement.....	57
Figure 3.30 Courbe Far et Frr et Courbe ROC de la Méthode.....	59
Figure 3.31 Courbe Far et Frr et Courbe ROC de la Méthode.....	59
Figure 3.32 Courbe Far et Frr et Courbe ROC de la Méthode.....	60
Figure 3.33 Courbe Far et Frr et Courbe ROC de la Méthode.....	60
Figure 3.34 Courbe Far et Frr et Courbe ROC de la Méthode.....	61
Figure 3.35 Courbe Far et Frr et Courbe ROC de la Méthode.....	61
Figure 3.36 Courbe Far et Frr et Courbe ROC de la Méthode.....	62
Figure 3.37 Comparaison des différentes courbes ROC des méthodes utilisées pour le matching...62	62
Figure 3.38 Courbe Far et Frr et Courbe ROC de la Méthode.....	63
Figure 3.39 Courbe Far et Frr et Courbe ROC de la Méthode.....	64
Figure 3.40 Courbe Far et Frr et Courbe ROC de la Méthode.....	64
Figure 3.41 Courbe Far et Frr et Courbe ROC de la Méthode.....	65
Figure 3.42 Courbe Far et Frr et Courbe ROC de la Méthode.....	65
Figure 3.43 Courbe Far et Frr et Courbe ROC de la Méthode.....	66
Figure 3.44 Courbe Far et Frr et Courbe ROC de la Méthode.....	66
Figure 3.45 Comparaison des différentes courbes ROC.....	67
Figure 3.46 EQUAL ERROR RATE (EER) en fonction de la taille de l'image en entrée.....68	68
Figure 3.47 EQUAL ERROR RATE (EER) de la texture de la main en fonction de la taille du ROI pour une taille de l'image de 510.....68	68
Figure 3.48 Taux de reconnaissance en fonction du seuil biométrique de matching de la géométrie de la main pour une taille de l'image de 510.....68	68
Figure 3.49 Taux de reconnaissance en fonction du seuil biométrique de matching de la texture de la paume de la main pour une taille de l'image de 510.....69	69

Introduction Générale

De nos jours, l'utilisation de la biométrie ne se limite plus aux empreintes digitales et son champ d'application dépasse largement le domaine de la loi et de l'ordre. Les avancées en matière de puissance de calcul des ordinateurs et de stockage de données, combinées à des programmes informatiques complexes, ont ouvert de nouvelles perspectives pour cette technologie. Ainsi, les gouvernements et le secteur privé s'engagent de plus en plus dans une politique visant à renforcer l'utilisation des technologies biométriques. Cette tendance s'explique par les enjeux sécuritaires et économiques considérables liés à la lutte contre le terrorisme et la fraude.

Les applications potentielles de la biométrie peuvent être regroupées en quatre catégories principales [1]. La première catégorie concerne les systèmes de sécurité ou les systèmes d'accès logique. Leur rôle est de surveiller, restreindre ou autoriser l'accès aux données ou aux informations. Dans ce cas, la biométrie remplace ou complète les codes PIN, les mots de passe et les jetons. L'industrie financière et bancaire, notamment à travers le commerce électronique, ainsi que la valeur des données personnelles sensibles stockées sur les réseaux et les ordinateurs, font de la biométrie un outil largement déployé pour sécuriser l'accès logique.

La deuxième catégorie d'applications concerne les systèmes d'accès physique ou les systèmes d'accès aux installations. Leur objectif est de contrôler, restreindre ou autoriser le mouvement des personnes à l'intérieur ou à l'extérieur d'une zone spécifique. Dans ce cas, la biométrie remplace ou complète les clés et les cartes d'accès, permettant aux utilisateurs autorisés d'accéder aux zones sécurisées. Les systèmes d'accès physique sont couramment utilisés dans des lieux publics très fréquentés tels que les aéroports, les musées, etc., ainsi que dans les installations frontalières, afin de surveiller et de restreindre les déplacements de personnes non autorisées ou suspectes. En outre, dans un contexte commercial, les systèmes d'accès physique peuvent également servir d'outil de gestion des ressources humaines en combinant la vérification d'accès à un endroit avec l'enregistrement des horaires de présence des employés.

La troisième catégorie concerne les systèmes biométriques qui garantissent l'unicité des individus. Ces systèmes sont principalement utilisés dans le secteur public, notamment dans les

programmes d'attribution d'aides sociales ou dans les systèmes de vote, pour prévenir les inscriptions multiples.

Enfin, les applications gouvernementales constituent la dernière et la plus importante catégorie d'applications biométriques. Elles englobent principalement les domaines militaires, de sécurité intérieure et judiciaires (criminologie, contrôle des établissements pénitentiaires). Elles couvrent également des secteurs civils tels que les services gouvernementaux, l'éducation, le transport et la santé.

Dans ce travail, nous proposons un système biométrique multimodal basé sur la géométrie et la texture de la paume de la main. La modalité de la main est largement acceptée par les utilisateurs en raison de sa commodité et de son caractère non intrusif. Afin d'augmenter le taux de reconnaissance, nous avons introduit une fusion des décisions provenant des deux modalités biométriques. Cette approche de fusion nous a permis de développer un système biométrique fiable. Nous avons réalisé un prototype fonctionnel qui peut être utilisé dans des environnements nécessitant un accès sécurisé. De plus, ce système peut également être utilisé comme dispositif de pointage dans les entreprises. Cette avancée technologique ouvre de nombreuses perspectives d'application, offrant une solution pratique et sécurisée pour les lieux nécessitant une authentification précise et fiable. Notre travail contribue ainsi au développement de nouvelles solutions biométriques et à l'amélioration des systèmes d'accès physique.

Le manuscrit de notre projet de fin d'études est structuré de la manière suivante :

Chapitre 1 : Introduction Ce chapitre offre une introduction générale aux systèmes d'accès biométriques, en mettant particulièrement l'accent sur les dispositifs biométriques utilisés dans ce contexte. De plus, il présente une revue de l'état de l'art des différentes techniques biométriques utilisées.

Chapitre 2 : État de l'art des systèmes biométriques de la main Ce chapitre est principalement consacré à une revue de l'état de l'art des systèmes biométriques de la main, nous permettant ainsi de situer notre travail par rapport aux travaux existants dans la littérature scientifique.

Chapitre 3 : Conception et réalisation du dispositif biométrique Dans ce chapitre, nous détaillons la conception et la réalisation matérielle et logicielle de notre dispositif biométrique. Les aspects

techniques de la réalisation de notre prototype y sont présentés, ainsi que les résultats obtenus grâce à la solution multimodale utilisant la géométrie et la texture de la paume de main. Nous abordons également la méthode de fusion des décisions qui a permis d'améliorer les taux de reconnaissance.

Chapitre 4 : Modèle économique détaillé de notre start-up Le dernier chapitre est consacré à la présentation d'un modèle économique détaillé de notre start-up. Nous y décrivons le Business Model Canvas (BMC) de manière approfondie, en mettant en avant les différents aspects de notre entreprise.

Chaque chapitre contribue à la compréhension globale de notre projet de fin d'études et nous permet de présenter de manière claire et structurée nos travaux, de l'introduction à la réalisation concrète du dispositif biométrique, ainsi que nos perspectives économiques avec notre start-up.

Les systèmes d'accès Biométrique

Introduction

La biométrie peut être définie de manière précise selon Jain et al. comme la science de l'identification automatique d'un individu sur la base de ses caractéristiques physiologiques ou comportementales [2]. Ainsi, la biométrie permet de vérifier l'identité d'une personne en se basant sur ce qu'elle est intrinsèquement, et non sur ce qu'elle possède (clé, carte d'accès, etc.) ou sur ce qu'elle sait (mot de passe). Cette caractéristique la rend moins vulnérable aux tentatives de contrefaçon par rapport aux méthodes d'identification traditionnelles.

En théorie, de nombreuses caractéristiques physiologiques ou comportementales humaines peuvent être utilisées en tant que modalités biométriques. Cependant, pour être utilisées dans un système biométrique précis, pratique et rentable, ces caractéristiques doivent également satisfaire à un ensemble de critères proposés dans [3]:

- Universalité: chaque individu doit posséder la caractéristique biométrique.
- Unicité: il doit y avoir une probabilité quasi nulle que deux personnes aient la même caractéristique biométrique.
- Permanence: la caractéristique biométrique doit rester stable dans le temps.
- Mesurabilité: la caractéristique biométrique doit pouvoir être quantifiée de manière pratique.
- Performance: précision et rapidité de reconnaissance à travers la caractéristique biométrique.
- Acceptabilité: acceptation de la mesure de la caractéristique par le public.
- Non-circonvension: degré de difficulté avec lequel le système peut être trompé en falsifiant la caractéristique biométrique.

Les modalités utilisées dans les systèmes biométriques possèdent ces propriétés, mais à des degrés différents. Le choix de la modalité biométrique est donc un compromis qui dépend des besoins spécifiques de l'application biométrique.

De nombreuses modalités biométriques ont été proposées et sont utilisées dans diverses applications. Les modalités physiologiques se basent sur des caractéristiques morphologiques ou biologiques, telles que le visage, l'oreille, l'iris, la rétine, les empreintes digitales et palmaires, la géométrie de la main, le réseau veineux, l'ADN, l'odeur de la peau, etc. Les modalités comportementales utilisent des traits personnels liés au comportement, tels que la voix, la dynamique de la signature, la démarche, la frappe au clavier ou encore les mouvements des lèvres. Certaines de ces modalités biométriques ont une longue histoire et sont considérées comme des technologies matures, tandis que d'autres sont encore au stade de la recherche.

Acuity Market Intelligence (Acuity MI), une entreprise mondiale de conseil en stratégies des technologies émergentes avec une expérience avérée dans l'anticipation de l'évolution du marché biométrique, fournit des données sur la répartition des parts de marché des différentes technologies biométriques [4]. Selon les données publiées par Acuity MI en 2009 et ses prévisions pour l'année 2017 (voir Figure 1.1), les empreintes digitales connaîtront une baisse au profit de l'iris, du visage, de la voix, de la signature et des veines.

Ces tendances démontrent une évolution dynamique du marché biométrique, avec un intérêt croissant pour certaines modalités biométriques telles que l'iris, le visage et la voix. Cette évolution est le résultat de l'amélioration des technologies, de la recherche continue dans le domaine et de l'adoption croissante des systèmes biométriques dans de nombreux secteurs, tels que la sécurité, la gestion des identités, les services financiers et bien d'autres.

En excluant le système gouvernemental AFIS (Automated Fingerprint Identification System), il est prévu que la modalité de l'empreinte digitale maintienne sa position dominante avec une part de marché de 25,4%. L'iris devrait prendre la deuxième place avec une part de marché de 18,8%, reléguant le visage à la troisième position avec une part de marché de 14,3%. Les modalités utilisant les veines et la voix suivront avec des parts de marché respectives de 5,8% et 5,5%. On s'attend à ce que la signature biométrique conserve

sa présence sur le marché avec une légère augmentation de sa part (1,57%), tandis que la modalité basée sur la main devrait perdre sa part de marché (0,0%).

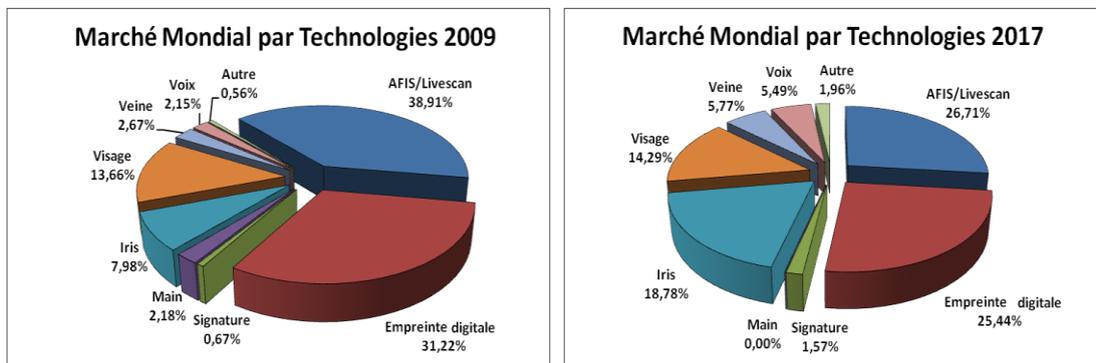


Figure 1. 1 Evolutions du marché biométrique mondial par technologies. A droite : parts de marché en 2009, à gauche : prévisions des parts de marché en 2017.

Un système biométrique fonctionne généralement en quatre étapes, constituant ainsi un processus de reconnaissance de formes. La première étape consiste à acquérir les données biométriques de l'utilisateur. Ensuite, les caractéristiques sont extraites à partir de ces données, éventuellement précédées d'une étape de prétraitement. La troisième étape consiste à comparer les caractéristiques extraites avec le modèle enregistré dans la base de données, afin de générer des mesures de similarité. Enfin, une étape de décision permet de conclure sur l'identité de l'utilisateur (voir Figure 1.2).

La phase d'enrôlement est le point de départ du système biométrique. Pendant cette phase, les données biométriques d'un utilisateur sont collectées et traitées pour créer un modèle. Ce modèle représente une forme mathématique des caractéristiques distinctives extraites par le système biométrique [2]. Il ne s'agit pas de données brutes ou d'images numérisées, mais plutôt d'une représentation abstraite des caractéristiques biométriques de l'individu.

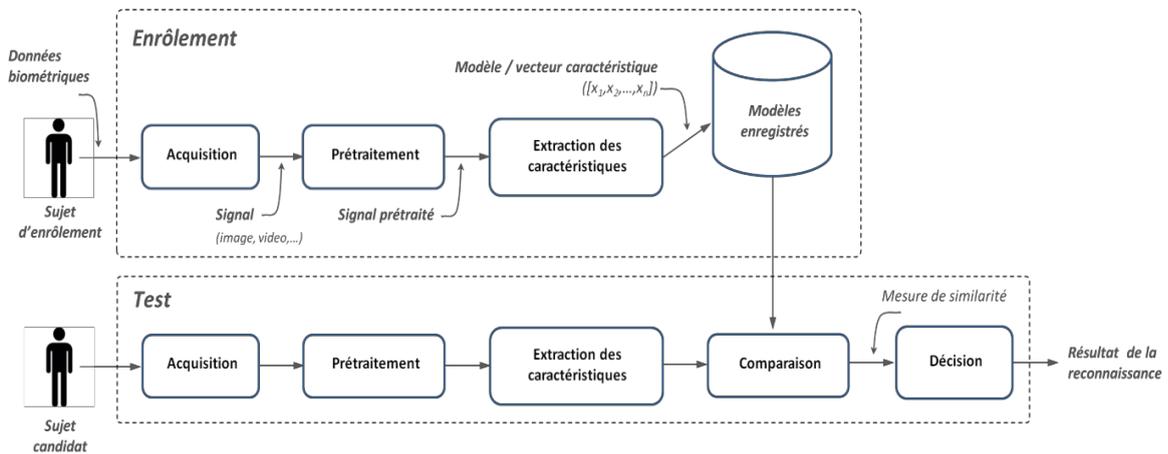


Figure 1. 2 Processus de fonctionnement d'un système biométrique

Les systèmes biométriques peuvent être conçus selon différents modes de fonctionnement, qui seront détaillés dans le paragraphe suivant. Ensuite, nous discuterons des outils d'évaluation utilisés pour évaluer les performances d'un système d'authentification biométrique. Nous aborderons également les différents aspects de la multimodalité, en mettant l'accent sur la fusion des scores. Enfin, nous présenterons la base de données IV² utilisée pour tester tous les systèmes biométriques proposés dans cette mémoire, ainsi que le protocole IV² utilisé pour les expériences monomodales et multimodales.

1.1 Modes opératoires d'un système biométrique

Il y a deux modes distincts pour un système biométrique : le mode d'identification, qui permet de répondre à la question "Qui suis-je ?", et le mode de vérification (ou d'authentification), qui permet de répondre à la question "Suis-je la personne que je prétends être ?" [2].

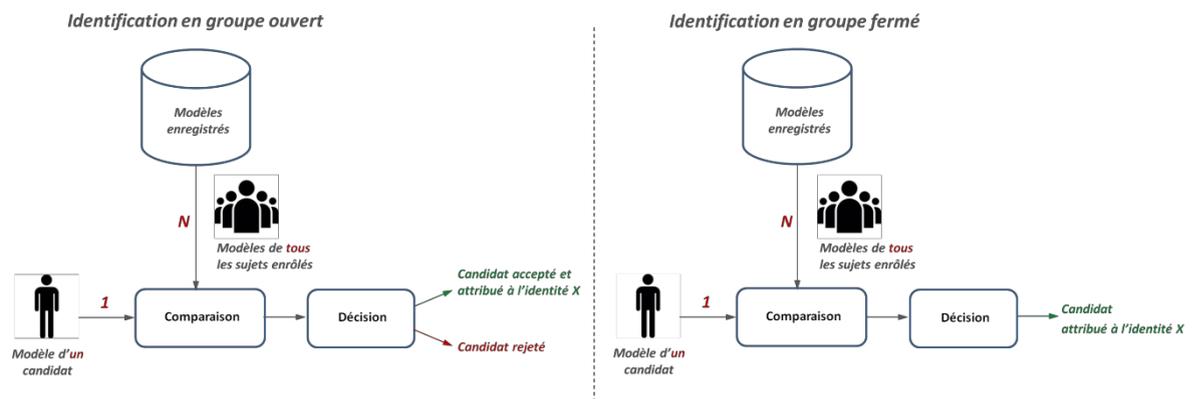


Figure 1. 3 Systèmes en mode d'identification en groupe ouvert et en groupe fermé.

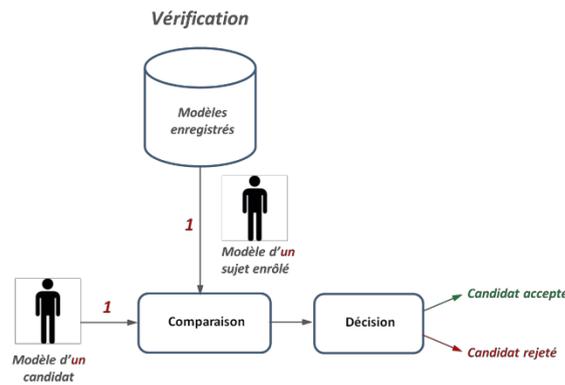


Figure 1. 4 Système en mode vérification.

Le mode d'identification, également connu sous le nom de reconnaissance "un-à-plusieurs", implique la comparaison du modèle biométrique du candidat avec les modèles de tous les utilisateurs enregistrés dans la base de données. Deux contextes sont possibles. Le premier est celui d'un groupe fermé, où l'on est certain que le candidat fait partie de la base de données des autorisés. Dans ce cas, le problème consiste à déterminer quelle identité correspond le mieux au candidat. Généralement, c'est ce contexte de groupe fermé qui est étudié dans les travaux de recherche. Le deuxième contexte est celui d'un groupe ouvert, où il est possible que le candidat soit un imposteur qu'il faut rejeter. Ainsi, le système peut prendre deux décisions : le rejet ou l'acceptation avec identification de l'identité du candidat (cf. Figure 1.3).

Dans le mode de vérification, également appelé authentification, le contexte reste toujours celui d'un groupe ouvert, c'est-à-dire qu'il n'y a aucune certitude que l'identité du candidat soit réellement connue par le système. En pratique, le candidat revendique l'identité d'une des personnes enregistrées dans la base de données. La comparaison se fait alors uniquement entre le modèle biométrique du candidat et les modèles de la personne annoncée. Il s'agit donc d'une reconnaissance "un-à-un" (cf. Figure 1.4). Tous les systèmes biométriques proposés dans le cadre de cette mémoire relèvent du mode de vérification.

1.2 Evaluation d'un système biométrique

Malgré les nombreux avantages des systèmes d'authentification biométrique, leur mise en œuvre comporte certains risques. Même le système biométrique le plus précis n'est pas parfait et générera des erreurs.

Dans cette mémoire, nous utiliserons des indicateurs de performance qui permettent de comparer différents algorithmes, en particulier dans le domaine de l'authentification d'identité. Nous ne nous intéresserons pas aux autres indicateurs de performance tels que la complexité de calcul et les ressources requises en mémoire. Les méthodes proposées dans ce travail de mémoire ont été testées au moyen d'une implémentation basique sur un ordinateur équipé d'un processeur Intel(R) Core(TM) i5, cadencé à 2,67 GHz, avec 4 Go de RAM et un système d'exploitation Windows 7 64 bits.

Un système d'authentification biométrique peut prendre deux décisions possibles : accepter ou rejeter un candidat. Deux types d'erreurs peuvent alors se produire :

- Les fausses acceptations : lorsque le système accepte des imposteurs en les considérant à tort comme des personnes autorisées.
- Les faux rejets : lorsque le système rejette des personnes authentiques en les considérant à tort comme des imposteurs.

La mesure de ces taux d'erreurs est effectuée à l'aide des équations (1.1) et (1.2), en fonction du seuil de décision τ . Le taux de fausses acceptations, ou FAR (False Acceptance Rate), est calculé en rapportant le nombre de fausses acceptations (c'est-à-dire le nombre d'imposteurs mal classés) au nombre total d'accès d'imposteurs dans la base de données. De même, le taux de faux rejets, ou FRR (False Reject Rate), est calculé en rapportant le nombre de faux rejets (nombre d'authentiques mal classés) au nombre total d'accès d'authentiques (selon le protocole suivi dans ce travail, un accès imposteur correspond à une comparaison entre deux images provenant de deux individus différents, tandis qu'un accès authentique correspond à une comparaison entre des images du même individu. cf. § 1.4).

$$FAR(\tau) = \frac{FA(\tau)}{N_{Imp}} \quad (1.1)$$

$$FRR(\tau) = \frac{FR(\tau)}{N_{Aut}} \quad (1.2)$$

On peut observer l'évolution de ces taux d'erreurs en fonction du seuil de décision en visualisant les distributions des scores pour les authentiques et les imposteurs, comme illustré sur la Figure 1.5-a. Alternativement, on peut représenter les valeurs de ces erreurs pour chaque seuil en traçant une courbe, comme montré dans la Figure 1.5-b.

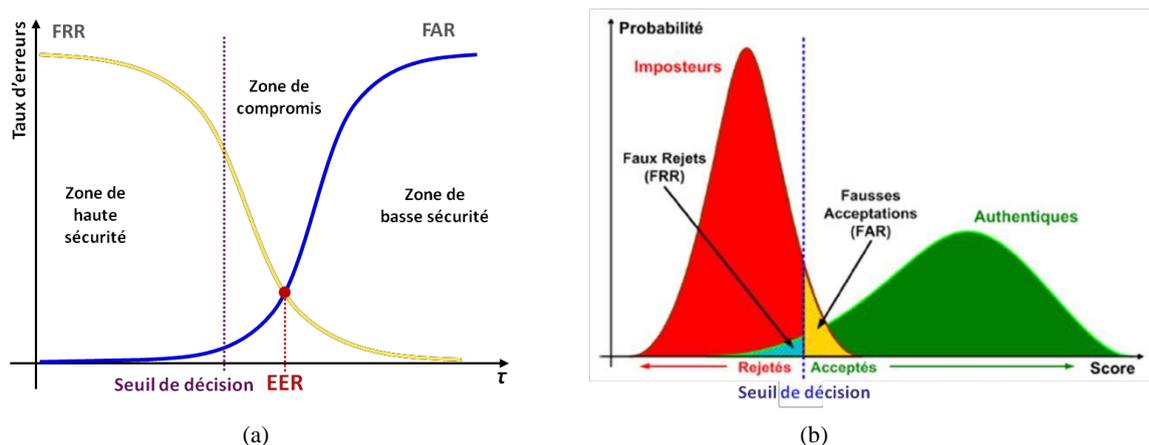


Figure 1. 5 Illustration du FAR et du FRR (a) à travers leur variation en fonction du seuil de décision et (b) à travers les distributions des authentiques et des imposteurs.

Idéalement, le choix du seuil de décision devrait correspondre à la valeur de τ qui minimise à la fois le taux de fausses acceptations (FAR) et le taux de faux rejets (FRR). Cependant, ces deux types d'erreurs ont des monotonies opposées, car le FAR est croissant tandis que le FRR est décroissant. Ainsi, le choix du seuil doit faire l'objet d'un compromis entre sécurité et confort, en fonction des besoins spécifiques de l'application.

Certaines applications exigent un taux de fausses acceptations (FAR) très faible, voire proche de zéro, par exemple lorsqu'il s'agit d'accéder à des documents confidentiels dans un contexte militaire. D'autres applications ne tolèrent pas un taux de faux rejets (FRR) élevé, comme l'accès à un téléphone portable. Dans les systèmes où ces deux types d'erreurs nécessitent un compromis, la performance du système biométrique est évaluée à plusieurs points de fonctionnement ou à travers des courbes de performance.

Un point de fonctionnement spécifique est le taux d'égaux erreurs (EER, Equal Error Rate), atteint lorsque le FAR et le FRR sont égaux. Ce point est souvent utilisé en raison de son caractère neutre et indépendant du type d'application.

Un autre point de fonctionnement est le FRR pour une valeur fixée du FAR. Par exemple, si le FAR est fixé à 1% ou 0,1%, le système nécessite un taux d'imposture relativement faible (1/100 ou 1/1000), et sa performance est mesurée par le FRR à cette valeur de FAR.

Par ailleurs, la courbe de performance la plus couramment utilisée dans la littérature est la courbe DET (Detection Error Tradeoff), qui trace le FRR en fonction du FAR pour différents seuils de décision τ [5]. Cette courbe est considérée comme meilleure lorsqu'elle est proche de l'origine du repère. L'EER peut être facilement détecté par l'intersection avec la première

bissectrice $y = x$. La courbe DET est généralement représentée sur une échelle logarithmique (cf. Figure 1.6). Elle diffère de la courbe ROC (Receiver Operating Characteristic), une autre courbe de performance couramment utilisée, qui trace le taux de rejet correct (TAR = 1-FRR) en fonction du FAR et est représentée sur une échelle linéaire (cf. Figure 1.7). Une courbe ROC est considérée comme meilleure lorsqu'elle se rapproche de l'angle supérieur gauche (FAR proche de zéro et TAR proche de 1).

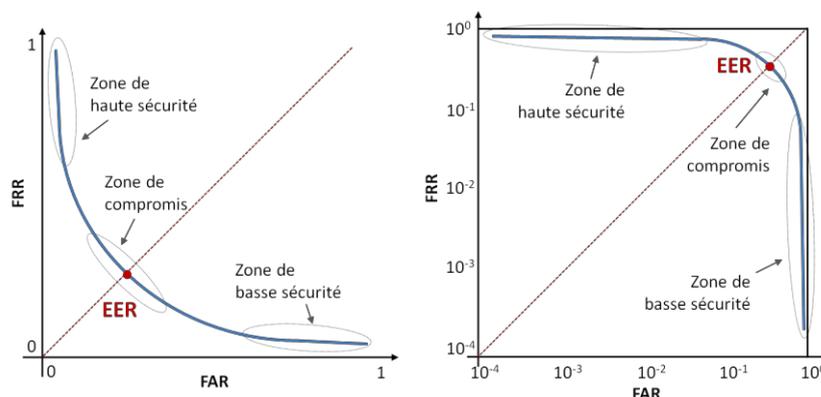


Figure 1. 6 Courbes DET : FRR en fonction du FAR, (à gauche) en échelle linéaire et (à droite) en échelle logarithmique.

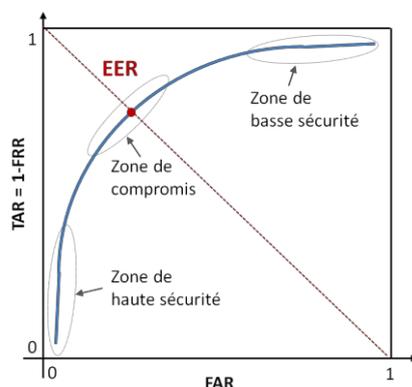


Figure 1. 7 Courbe ROC : TAR en fonction du FAR.

Lors de l'évaluation des méthodes monomodales proposées, nous présenterons les taux d'égaux erreurs (EER) ainsi que les courbes DET, suivies d'interprétations et de discussions. Dans l'évaluation des méthodes multimodales proposées, nous fournirons également les taux de faux rejets (FRR) aux deux points où le taux de fausses acceptations (FAR) est égal à 1% et 0,1%. Les taux d'erreurs seront accompagnés d'intervalles de confiance à 90% permettant d'évaluer leur signification statistique en termes de précision.

1.3 Limites de la monomodalité et solution multimodale

Les applications biométriques à petite et moyenne échelle, avec quelques centaines d'utilisateurs, peuvent encore utiliser des systèmes unimodaux, c'est-à-dire des systèmes biométriques basés sur une seule modalité. Cependant, ces systèmes présentent plusieurs limitations qui entravent leur utilisation lorsqu'il s'agit de construire un système de reconnaissance de haute précision pour des applications à grande échelle [6]. Parmi ces limites, on peut citer :

- Le bruit dans les données acquises : Les données biométriques peuvent être bruitées en raison de cicatrices sur une empreinte digitale ou d'une voix altérée par un rhume, par exemple. Cependant, le bruit dans les données est souvent dû à des capteurs défectueux ou mal entretenus, comme l'accumulation de poussière sur un capteur d'empreinte digitale ou un mauvais focus de la caméra entraînant du flou. Les conditions ambiantes défavorables, telles qu'un mauvais éclairage, peuvent également contribuer au bruit dans les données biométriques. Ce bruit peut conduire à des appariements incorrects entre les données acquises et les modèles de la base de données, entraînant ainsi le rejet incorrect d'un utilisateur autorisé (cf. Figure 1.1).
- Les variations intraclasse : Les données biométriques acquises d'un individu lors de l'authentification peuvent différer considérablement des données utilisées pour générer le modèle biométrique de cet individu lors de la phase d'enrôlement. Cette variation peut être causée par une mauvaise interaction entre l'utilisateur et le capteur, telle qu'un changement de pose, ou par des changements dans les caractéristiques du capteur, comme le passage à un capteur différent. De plus, les variations des conditions de l'environnement ambiant, telles que les changements d'éclairage, ainsi que les variations psychologiques de l'individu, peuvent également entraîner des variations intraclasse. Par conséquent, il peut y avoir des différences significatives entre les données biométriques acquises et les modèles enregistrés, ce qui peut affecter les performances du système biométrique.
- Le manque d'individualité : Bien qu'un trait biométrique soit censé varier considérablement d'un individu à l'autre, il peut y avoir de grandes similitudes entre les individus pour certains traits biométriques. Par exemple, les vrais jumeaux ont une apparence faciale quasi-identique. Cette limitation réduit la capacité de discrimination du système biométrique, augmentant ainsi les risques d'accepter des personnes qui ne devraient pas l'être.
- La non-universalité : L'utilisation d'un système biométrique unimodal suppose que chaque individu de la population ciblée possède la modalité biométrique en question. Cependant, cette hypothèse n'est pas toujours vérifiée, ce qui signifie qu'un sous-ensemble de la population peut être exclu par le système biométrique si aucune alternative ne lui est

proposée. Par exemple, une personne muette ne peut pas être enregistrée dans un système de reconnaissance vocale, et une personne présentant une paralysie de la main ne peut pas être enregistrée dans un système de reconnaissance de signature. Dans ces cas, les personnes ne possèdent pas la biométrie correspondante, ce qui génère des erreurs d'enrôlement (« Failure To Enroll » ou FTE). Un autre problème de non-universalité survient lorsqu'une personne possède le trait biométrique, mais de manière inexploitable par le système biométrique. Par exemple, une personne souffrant de cataracte oculaire ne fournira pas d'images d'iris de qualité suffisante pour une reconnaissance automatique, ou une personne présentant une sécheresse extrême des doigts ne fournira pas d'images d'empreintes digitales exploitables. Dans ce cas, le système générera une erreur de capture (« Failure To Capture » ou FTC).

- La sensibilité aux attaques : Bien que les traits biométriques soient plus difficiles à contrefaire que les méthodes d'identification classiques telles que les mots de passe et les cartes d'accès, ils restent sensibles aux attaques. Les modalités biométriques comportementales, telles que la signature et la voix, sont particulièrement vulnérables aux attaques d'usurpation. Les traits physiologiques sont également sujets aux attaques, par exemple, les empreintes digitales peuvent être reproduites à l'aide de silicone et le visage peut être contrefait à l'aide d'une photographie.

La multimodalité est une approche qui surmonte plusieurs limites rencontrées avec les systèmes biométriques unimodaux. Ces systèmes multimodaux utilisent simultanément plusieurs traits biométriques, tels que les empreintes digitales et le visage, pour renforcer les performances et répondre aux exigences strictes de diverses applications. Ils offrent une solution au problème de non-universalité en couvrant une plus grande partie de la population grâce à l'utilisation de plusieurs traits biométriques. De plus, la fiabilité des systèmes biométriques multimodaux est améliorée en raison de la présence de multiples preuves d'identité.

Même si deux individus différents peuvent être confondus en ce qui concerne un trait biométrique spécifique (problème de non-individualité), ils seront différenciés par rapport à d'autres traits biométriques. Ainsi, la combinaison de plusieurs traits biométriques permet de résoudre ce problème. De plus, les différents traits biométriques ne sont pas tous affectés de la même manière par le bruit ou les variations intraclasses dans les données acquises. Par exemple, un changement d'éclairage peut affecter la qualité de l'image d'un visage, mais pas celle d'une empreinte digitale. De même, une cicatrice sur un doigt peut affecter la reconnaissance d'une empreinte digitale, mais pas la reconnaissance par les veines.

Les systèmes biométriques multimodaux offrent également de nombreuses possibilités pour contrer les tentatives d'usurpation. Il est plus difficile pour un intrus d'usurper simultanément plusieurs traits biométriques d'un utilisateur légitime. De plus, ces systèmes permettent la mise en place d'un processus d'authentification question/réponse, qui garantit la présence physique de l'utilisateur lors de l'acquisition des données. Par exemple, l'utilisateur peut être invité à présenter un sous-ensemble aléatoire de caractéristiques biométriques spécifiques dans un ordre prédéfini (par exemple, l'index droit suivi du majeur droit).

1.4 Biométrie et multimodalité

Dans cette section, nous examinerons différents aspects de la multimodalité. Tout d'abord, nous aborderons les nombreuses sources d'informations utilisées par les systèmes multimodaux. Ensuite, nous détaillerons les différentes architectures possibles pour un système multimodal. Enfin, nous présenterons les divers niveaux de fusion multimodale, notamment la fusion des scores et la phase de normalisation qui l'accompagne.

1.4.1 Taxonomie des Systèmes biométriques multimodaux

Le concept de multimodalité consiste à combiner plusieurs sources d'information à partir de systèmes monomodaux [6]. Selon les sources d'information combinées, il existe cinq scénarios de multimodalité possibles (voir Figure 1.8) :

1. Systèmes multi-capteurs : Lorsque différents capteurs sont utilisés pour acquérir le même trait biométrique. Par exemple, l'utilisation d'une caméra digitale, d'une webcam et d'une caméra thermique pour la capture d'images du visage.
2. Systèmes multi-échantillons : Lorsque plusieurs échantillons du même trait/modalité sont associés. Par exemple, l'association des images des iris gauche et droit ou des empreintes digitales de l'index et du majeur.
3. Systèmes multi-instances : Lorsque plusieurs instances du même trait, provenant du même échantillon biométrique et acquises par un même capteur, sont associées. Par exemple, l'association de plusieurs images de visage prises avec des changements de pose (frontale ou de profil), d'expression ou d'éclairage [7].
4. Systèmes multi-algorithmes : Lorsque le traitement d'une image se fait par la combinaison de plusieurs algorithmes, que ce soit dans le module d'extraction de caractéristiques ou dans celui de comparaison.

5. Systèmes multi-biométries : Aussi appelés systèmes multi-traits ou systèmes multimodaux au sens strict du terme, ces systèmes combinent plusieurs modalités/traits biométriques. Par exemple, la combinaison de la voix et de la signature, ou du visage et de l'iris.

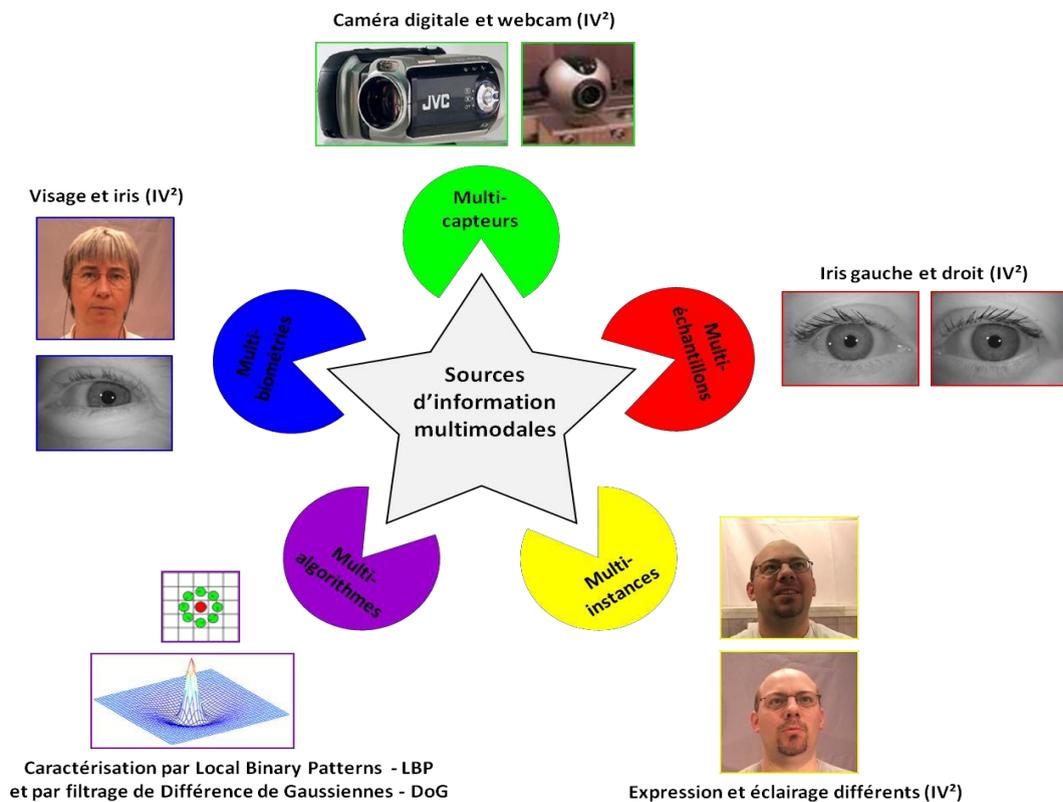
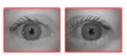


Figure 1. 8 Les multiples sources d'information dans un système biométrique multimodal.

Diverses combinaisons sont envisageables à partir de ces scénarios. Une étude comparative de l'utilité des scénarios multimodaux a été conduite par Tissé en 2003, en se basant sur trois critères essentiels (voir Tableau 1.1) : l'amélioration des performances, le coût matériel du système et la consommation de temps lors de l'acquisition ou du traitement numérique.

Table 1. 1 Comparaison des scénarios multimodaux suivant les critères de l'amélioration de la performance, du coût matériel et de la consommation du temps. +/- désigne le niveau de satisfaction (adapté à partir de [8]).

	multi-capteurs 	multi-échantillons 	multi-instances 	multi-algorithmes 	multi-biométries 
Performance en FRR et FAR	+	++	-	+	+++
Coût matériel	-	++	++	+	--
Consommation en temps	-	-	+	++	+

En réalité, aucun scénario ne peut répondre seul à toutes les exigences d'un système biométrique. Selon la comparaison présentée dans le Tableau 1.1, les scénarios multi-capteurs et multi-instances sont relativement moins satisfaisants que les autres scénarios (4+ ou plus) en termes d'exigences.

Le scénario multi-échantillons présente un inconvénient en termes de temps d'acquisition, car il nécessite la capture de plusieurs échantillons du même trait biométrique à partir d'un seul capteur. Cependant, l'utilisation d'un unique capteur est attrayante en termes de coût matériel, ce qui fait du scénario multi-échantillons un compromis intéressant pour améliorer les performances du système sans coût supplémentaire.

Le scénario multi-algorithmes améliore les performances du système, mais de manière moins significative que le scénario multi-échantillons. Cela est dû au fait que la performance de chaque algorithme combiné dépend fortement de la qualité d'un unique exemple initial acquis, à partir d'une même biométrie et via un même capteur. Le coût d'un tel système est davantage lié aux unités de calcul (plate-forme matérielle) qu'au capteur.

Le scénario de la multi-biométries est potentiellement celui qui atteint les meilleures performances en termes de FAR (taux de fausses acceptations) et de FRR (taux de fausses rejets). Cependant, ce scénario présente des inconvénients en termes de facilité d'utilisation et de coût. L'utilisation de plusieurs modalités biométriques peut entraîner un allongement du temps d'acquisition et du temps de traitement. Bien que la capture des multiples biométries et le traitement de l'information puissent être effectués de manière parallèle, l'utilisation de plusieurs capteurs implique inévitablement un coût matériel plus élevé. C'est pourquoi, en pratique, les systèmes multimodaux comprenant plus de deux modalités sont rarement utilisés. Si l'on considère d'autres critères liés aux problèmes de non-universalité et de tentatives d'usurpation d'identité, le scénario de la multi-biométries est le seul capable d'apporter des solutions. Les

quatre premiers scénarios combinent des informations provenant toutes d'un unique trait biométrique, ce qui ne leur permet pas de résoudre efficacement tous les problèmes rencontrés par les systèmes monomodaux, même s'ils parviennent à améliorer leurs performances.

En fin de compte, le choix d'un scénario, ou d'une combinaison de plusieurs, est une question de compromis entre les différents critères et les besoins de l'application.

1.4.2 Architectures d'un système multimodal

Il existe trois architectures possibles pour concevoir un système biométrique multimodal, comme décrit dans les références [6] [9] : l'architecture en série (ou en cascade), l'architecture en parallèle et l'architecture hiérarchique (ou en arbre). Une visualisation graphique des trois catégories est présentée dans la Figure 1.9.

L'architecture en série (Figure 1.9-a) consiste à invoquer les systèmes individuels de manière séquentielle. Certains systèmes ne sont utilisés que lorsque certaines conditions sont remplies après l'exécution des systèmes précédents, permettant ainsi de prendre une décision sans nécessairement impliquer tous les systèmes. Cette architecture peut être utilisée comme schéma d'indexation pour réduire le nombre d'identités possibles avant d'utiliser les données suivantes. Elle permet également d'améliorer l'efficacité en utilisant d'abord des systèmes moins coûteux et moins précis, puis en faisant appel à des systèmes plus coûteux mais plus précis.

Dans l'architecture hiérarchique (Figure 1.9-b), les différents systèmes individuels sont combinés dans une structure arborescente. Cette architecture est considérée comme la plus flexible et permet de faire face aux problèmes de données manquantes ou de mauvaise qualité souvent rencontrés dans les systèmes biométriques.

Dans l'architecture en parallèle (Figure 1.9-c), les informations provenant des différents systèmes sont utilisées simultanément pour effectuer la tâche de reconnaissance. L'utilisation de toutes les informations biométriques est alors requise pour prendre une décision, ce qui peut entraîner une amélioration plus significative par rapport à l'architecture en série. La plupart des méthodes proposées dans la littérature appartiennent à cette catégorie d'architecture, y compris les méthodes présentées dans cette mémoire.

Le choix de l'architecture d'un système dépend des besoins de l'application. Dans les applications conviviales et à faible risque, l'architecture en série est privilégiée en raison de ses avantages en

termes de coût en temps et en matériel par rapport à l'architecture en parallèle qui nécessite l'acquisition et le traitement d'un grand nombre de données biométriques. En revanche, dans les applications où la sécurité est d'une importance primordiale (par exemple, dans les applications militaires), l'utilisation d'une architecture en parallèle est plus appropriée. L'architecture hiérarchique est privilégiée dans les applications où il existe un risque accru d'acquisition de données biométriques de mauvaise qualité (par exemple, un système de contrôle d'assiduité avec plusieurs échantillons d'empreintes digitales dans un milieu hospitalier). Elle est également utilisée dans les applications où l'une ou l'autre des modalités biométriques risque d'être absente (par exemple, un système de contrôle d'assiduité avec plusieurs échantillons d'empreintes digitales dans une usine de bois).

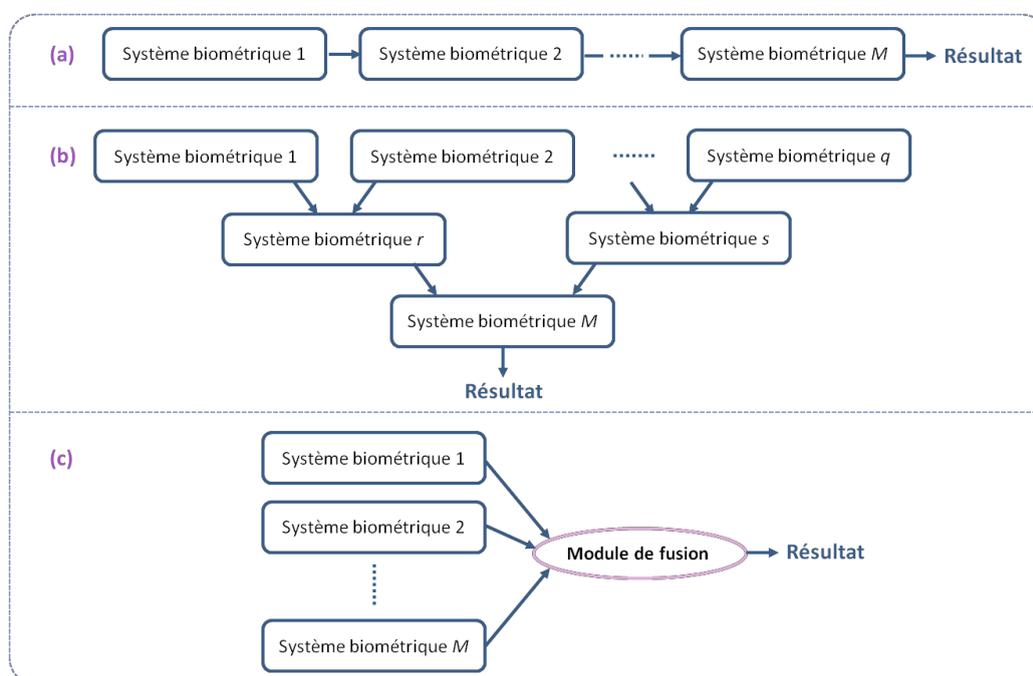


Figure 1. 9 Architectures d'un système multimodal (a) en série, (b) hiérarchique, (c) parallèle (adapté à partir de [9]).

1.4.3 Niveaux de fusion multimodale

Un système biométrique est principalement composé de quatre modules : un module d'acquisition des données, un module d'extraction de caractéristiques, un module de mise en correspondance (également appelé module de "classification" de manière erronée) et un module de décision. La fusion multimodale peut être effectuée à la sortie de n'importe lequel de ces modules, donnant ainsi lieu à quatre niveaux de fusion (voir Figure 1.10), qui peuvent être regroupés en deux grandes familles : la fusion pré-classification et la fusion post-classification [10].

La fusion pré-classification se fait avant le module de mise en correspondance, soit au niveau du capteur, soit au niveau des caractéristiques.

- La fusion au niveau des capteurs consiste à fusionner des données brutes provenant d'un ou de plusieurs capteurs. Ce type de fusion ne peut être effectué qu'entre différentes instances de la même biométrie et nécessite des données compatibles. Par exemple, il est possible de combiner plusieurs images du visage dans différentes poses pour former un modèle 3D.
- La fusion au niveau des caractéristiques consiste à combiner des vecteurs de caractéristiques provenant de différents capteurs ou obtenus après l'application d'algorithmes différents sur une même donnée biométrique. Lorsque les vecteurs de caractéristiques sont homogènes, par exemple plusieurs empreintes digitales d'un même doigt, une somme pondérée peut être utilisée pour obtenir un seul vecteur de caractéristiques. Si les vecteurs de caractéristiques sont hétérogènes, par exemple s'ils proviennent de différentes méthodes de caractérisation ou de différents traits biométriques, et s'ils sont compatibles (ce qui n'est pas toujours le cas, comme pour les minuties et les coefficients d'analyse en composantes principales d'une empreinte digitale), ils peuvent être concaténés en un unique vecteur de caractéristiques. La fusion au niveau des caractéristiques offre une information plus riche, mais elle est difficile à réaliser en pratique en raison de plusieurs raisons : i) La dépendance entre les espaces de caractéristiques à fusionner, qui est généralement inconnue et nécessite l'élimination des caractéristiques fortement corrélées. ii) La concaténation des vecteurs de caractéristiques peut conduire à un espace de caractéristiques excessivement grand. iii) Les vecteurs de caractéristiques générés par les systèmes biométriques commerciaux sont généralement la propriété des vendeurs et ne sont pas toujours accessibles.

L'une des approches classiques de reconnaissance faciale que nous proposons dans le prochain chapitre utilise une fusion au niveau des caractéristiques.

En raison des contraintes de la fusion pré-classification, la plupart des chercheurs se tournent vers l'étude de schémas de fusion post-classification, qui se produisent après le module de mise en correspondance, soit au niveau des scores, soit au niveau des décisions.

- La fusion au niveau des décisions consiste à combiner les décisions des systèmes biométriques, qui fournissent chacun une réponse (accepté : 1 ou rejeté : 0 dans le cas de la vérification) en fonction de l'entrée qui leur est présentée. Ce niveau de fusion peut être réalisé à l'aide de règles simples telles que ET, OU ou vote à la majorité, ainsi que de

règles plus complexes telles que le vote pondéré ou la classification dans l'espace des décisions [6]. La fusion au niveau des décisions est simple, mais elle utilise une information très limitée (0 ou 1).

- La fusion au niveau des scores consiste à combiner les scores provenant de chaque module de comparaison individuel. Les scores ont l'avantage d'être indépendants des systèmes biométriques et donc beaucoup plus faciles d'accès que les caractéristiques. Les scores contiennent l'information la plus riche sur le modèle d'entrée, après les vecteurs de caractéristiques. De plus, ils permettent de surmonter les contraintes de compatibilité et de grande dimension de l'espace des caractéristiques rencontrées avec la fusion au niveau des caractéristiques. Ainsi, la fusion au niveau des scores offre un meilleur compromis entre l'information riche et la facilité de mise en œuvre, ce qui en fait l'approche la plus répandue dans les systèmes biométriques multimodaux.

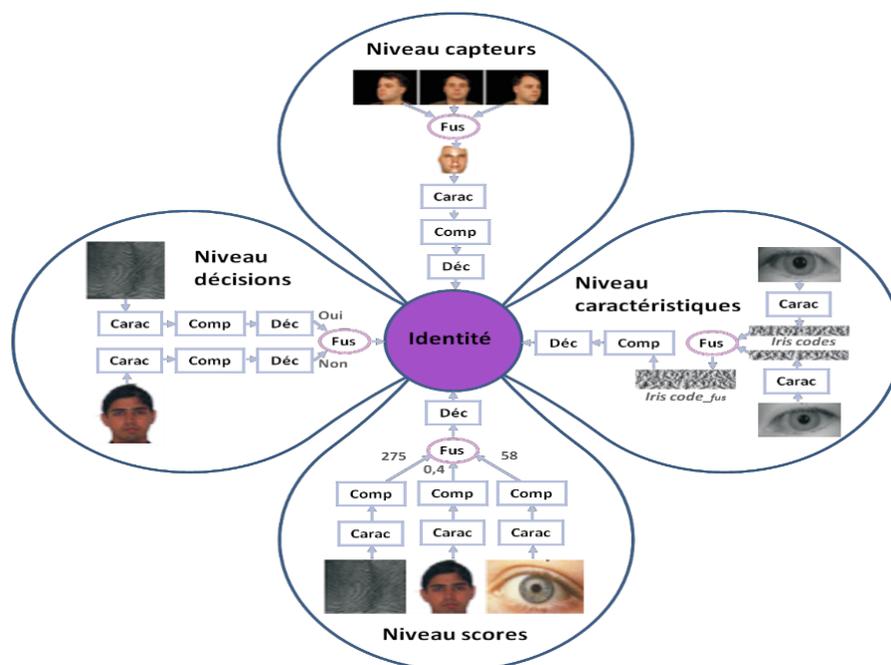


Figure 1. 10 Les différents niveaux de fusion dans un système biométrique multimodal (adapté depuis [11]).

1.4.4 Fusion au niveau des scores

Dans le contexte d'un système de vérification, deux approches sont envisageables pour fusionner les scores provenant des différents comparateurs ou matcheurs individuels : l'approche par classification et l'approche par combinaison de scores.

Dans l'approche par classification, un vecteur de caractéristiques est formé à partir des scores des matcheurs individuels, et il est attribué à l'une des classes "accepté" (également

appelée autorisé, authentique ou client) ou "rejeté" (imposteur). Le classifieur utilisé est généralement capable de prendre cette décision indépendamment de la manière dont le vecteur de caractéristiques des scores a été généré. Cela permet de fusionner des scores non homogènes provenant des différents matcheurs (distance ou similarité, différentes plages de scores, etc.) sans aucun traitement préalable avant de les passer au classifieur.

D'autre part, l'approche par combinaison combine les scores provenant des matcheurs individuels pour former un score unique qui sera utilisé par la suite pour prendre la décision finale. Par conséquent, les scores des différents matcheurs doivent d'abord être normalisés afin d'être transformés dans un domaine commun assurant la cohérence des données lors de la combinaison. Kittler et al. ont développé un formalisme mathématique pour consolider la combinaison de plusieurs classifieurs en utilisant des schémas évidents tels que la règle de somme, la règle de produit, la règle du maximum, la règle du minimum, entre autres [12]. Pour pouvoir utiliser ces schémas, les scores doivent d'abord être transformés en probabilités a posteriori conformément à un utilisateur autorisé ou imposteur. Kittler et al. considèrent le problème de classer un modèle d'entrée Z parmi m classes possibles (où $m = 2$ pour un système de vérification) en fonction des informations fournies par R matcheurs différents. Soit le vecteur de caractéristiques construit à partir du modèle d'entrée Z , et soit $P(\omega_j | \cdot)$ les sorties des matcheurs individuels, c'est-à-dire les probabilités a posteriori que le modèle Z appartienne à la classe ω_j sachant le vecteur de caractéristiques. Soit $c \in \{1, 2, \dots, m\}$ le numéro de la classe ω_c à laquelle le modèle d'entrée Z est finalement attribué ; c peut être déterminé en utilisant les règles suivantes [10]:

La règle du produit est une règle statistique qui repose sur l'hypomémoire d'indépendance des représentations. Cette hypomémoire est généralement vérifiée dans le cas de la multimodalité, où différentes caractéristiques telles que l'iris, le visage ou l'empreinte digitale sont utilisées. La règle du produit peut être exprimée par l'équation (1.3).

$$c = \arg \max_j \prod_{i=1}^R P(\omega_j | \vec{x}_i) \quad (1.3)$$

La règle de la somme est une autre règle statistique qui, en plus de l'hypomémoire d'indépendance statistique des représentations, suppose que les probabilités a posteriori calculées à partir des matchers individuels ne s'écartent pas beaucoup des probabilités a priori. Cette règle se révèle plus efficace que la règle du produit dans les cas où il y a un niveau élevé de bruit qui entraîne une ambiguïté dans le problème de classification. Selon l'équation (1.4), le modèle Z est assigné à la classe c en utilisant la règle de la somme.

$$c = \arg \max_j \sum_{i=1}^R P(\omega_j | \vec{x}_i) \quad (1.4)$$

La règle du maximum est une autre règle utilisée dans le contexte de la classification. Elle approxime la moyenne des probabilités a posteriori en prenant la valeur maximale parmi ces probabilités. Selon l'équation (1.5), la classe c du modèle d'entrée Z est déterminée en utilisant la règle du maximum.

$$c = \arg \max_j (\max_i P(\omega_j | \vec{x}_i)) \quad (1.5)$$

La règle du minimum est une autre règle de classification qui approxime la classe c du modèle Z en utilisant le minimum des probabilités a posteriori. Selon l'équation (1.6), la classe c est déterminée en utilisant la règle du minimum.

$$c = \arg \max_j (\min_i P(\omega_j | \vec{x}_i)) \quad (1.6)$$

La combinaison des scores peut également être calculée en utilisant une somme pondérée des scores provenant des matchers individuels. Certains travaux assignent des poids statiques aux scores des matchers individuels [13]. D'autres proposent d'utiliser des poids spécifiques à chaque utilisateur pour les différentes modalités [14]. D'autres encore présentent une approche adaptative de combinaison des scores en utilisant une somme pondérée, grâce à un processus d'apprentissage de poids hors ligne basé sur les taux d'erreur équivalents (EER) des matchers individuels, ainsi que des poids en ligne qui accordent une importance plus élevée aux scores de classement les plus élevés lors de l'identification [15].

Il est important de souligner que Ross et Jain ont démontré que l'approche de combinaison des scores est plus efficace que certaines approches de classification telles que les arbres de décision et l'analyse linéaire discriminante [16]. Cependant, ils affirment qu'il n'existe pas de schéma unique, que ce soit par classification ou par combinaison de scores, qui soit le meilleur dans toutes les circonstances. De plus, lorsque les sorties des matchers individuels sont simplement des scores, sans mesure de la qualité de l'échantillon, il est préférable de combiner directement les scores en utilisant la méthode appropriée plutôt que de les convertir en probabilités [16].

1.4.5 Normalisation des scores

Le choix d'une approche de fusion par combinaison de scores nécessite une étape préalable de normalisation avant la fusion proprement dite. Cette étape est essentielle pour les trois raisons suivantes :

1. Les sorties des modules de correspondance ou des matchers individuels peuvent être non homogènes, ce qui signifie qu'ils peuvent fournir des mesures de distances ou de similarités différentes.
2. Les scores peuvent se situer dans des intervalles différents, ce qui rend difficile leur comparaison et leur combinaison directe.
3. Les distributions statistiques des sorties de chaque matcher peuvent être différentes, ce qui peut affecter la manière dont les scores sont interprétés et comparés.

C'est pourquoi il est nécessaire de transformer les scores des matchers individuels dans un domaine commun avant de les combiner, en effectuant une normalisation. La normalisation implique un ajustement des paramètres de position (moyenne) et d'échelle (écart-type) des scores. Pour obtenir une bonne normalisation, il est important d'utiliser des estimateurs robustes et efficaces pour ces paramètres. La robustesse d'un estimateur se traduit par sa capacité à être insensible aux valeurs aberrantes ou "outliers", tandis que l'efficacité exprime la proximité de l'estimateur obtenu par rapport à l'estimateur optimal lorsque la distribution des données est connue. Une présentation détaillée des concepts de robustesse et d'efficacité des procédures statistiques se trouve dans [17].

Parmi les techniques de normalisation les plus couramment utilisées [10], on peut citer :

- La normalisation min-max : qui met les scores dans un intervalle prédéfini, généralement entre 0 et 1, en utilisant les valeurs minimales et maximales observées.
- La normalisation z-score : qui transforme les scores en utilisant la moyenne et l'écart-type des scores observés, ce qui les rend centrés autour de zéro et avec une dispersion standard.
- La normalisation par échelle logistique : qui utilise une fonction logistique pour répartir les scores dans un intervalle spécifique, généralement entre 0 et 1.

Il convient de noter que le choix de la technique de normalisation dépendra du contexte spécifique et des caractéristiques des données utilisées dans le processus de fusion des scores.

Min-Max : La technique de normalisation min-max est la plus simple et la plus adaptée lorsque les valeurs minimales et maximales des matchers individuels sont connues. Elle consiste à transformer les scores en les translatant vers une échelle allant de 0 à 1. Même si les scores des matchers ne sont pas bornés, il est possible d'estimer les bornes en utilisant un jeu de scores d'entraînement et de les appliquer par la suite. La normalisation min-max pour un score donné s_k peut être définie selon l'équation (1.7), où min et max désignent respectivement les scores minimal et maximal du matcher k.

$$s'_k = \frac{s_k - \min}{\max - \min} \quad (1.7)$$

Dans le cas de l'estimation des bornes min et max, la normalisation min-max n'est pas robuste aux valeurs aberrantes qui se trouvent en dehors de l'intervalle estimé par le jeu de scores d'entraînement. Cela signifie que si des valeurs aberrantes sont présentes dans les scores des matchers individuels et qu'elles se situent en dehors de l'intervalle estimé, elles peuvent avoir un impact significatif sur la normalisation min-max. Par conséquent, la normalisation min-max peut ne pas être adaptée dans ces situations où les valeurs aberrantes peuvent fausser la distribution des scores et introduire des biais dans le processus de fusion des scores.

Decimal-scaling : La méthode du "decimal scaling" peut être utilisée lorsque les scores des matchers individuels évoluent dans des intervalles à rapport logarithmique. Par exemple, les scores d'un matcher peuvent être dans l'intervalle [0, 1] tandis que les scores d'autres matchers peuvent être dans l'intervalle [0, 1000]. Dans ce cas, la normalisation peut être appliquée selon l'équation (1.8). Cependant, cette approche présente des défauts, tels que le manque de robustesse et l'hypomémoire selon laquelle les différents matchers varient selon un facteur logarithmique.

$$S'_k = \frac{S_k}{10^{\log_{10}(max)}} \quad (1.8)$$

zScores : La technique des "z-scores" est la plus couramment utilisée pour la normalisation des scores (équation (1.9)). Elle est calculée à partir de la moyenne arithmétique et de l'écart-type d'une distribution donnée. Son effet est de recentrer les scores des différents matchers autour de zéro. Cette approche est considérée comme bonne si l'on dispose de connaissances a priori sur la moyenne et les variations des scores du matcher. Dans le cas contraire, une estimation préalable de ces grandeurs est nécessaire à partir d'un ensemble de scores donné. Cependant, la normalisation des z-scores est sensible aux valeurs aberrantes, ce qui la rend non robuste.

Il est vrai que cette technique est optimale si la distribution des scores suit une distribution gaussienne, car la moyenne et l'écart-type sont des estimateurs optimaux des paramètres de position et d'échelle dans ce cas. Cependant, dans le cas d'une distribution arbitraire, ils restent des estimateurs raisonnablement bons selon [10], même s'ils ne sont plus optimaux.

$$S'_k = \frac{S_k - \mu}{\sigma} \quad (1.9)$$

Médiane et écart absolu médian MAD (Medium Absolute Deviation) : La normalisation par la médiane et l'écart absolu médian (MAD, pour Medium Absolute Deviation) est effectuée selon l'équation (1.10) et se révèle robuste car elle est insensible aux valeurs aberrantes. Cependant, contrairement à la moyenne et à l'écart-type, la médiane et le MAD sont considérés comme des estimateurs faibles de la position et de l'échelle lorsque la distribution des scores n'est pas gaussienne. En conséquence, cette technique est moins

efficace, ne préserve pas la distribution d'entrée en sortie et ne transforme pas les scores normalisés des différents matchers en un intervalle commun.

$$s'_k = \frac{s_k - \text{median}}{\text{MAD}} \quad \text{avec MAD} = \text{median}(|s_k - \text{median}|) \quad (1.10)$$

Fonction double sigmoïde : La normalisation par la fonction double sigmoïde est définie par l'équation (1.11), où t représente le point de référence, et r_1 et r_2 sont les bornes entre lesquelles la fonction double sigmoïde est linéaire.

$$s^k = \begin{cases} \frac{1}{1 + \exp(-2(s_k - \frac{t}{r_1}))} & \text{si } s_k < t \\ \frac{1}{1 + \exp(-2(s_k - \frac{t}{r_2}))} & \text{sinon} \end{cases} \quad (1.11)$$

La technique de normalisation par la fonction double sigmoïde garantit la transformation des scores dans un intervalle commun entre 0 et 1. Cependant, il est important de régler soigneusement les paramètres t , r_1 et r_2 pour obtenir une efficacité optimale. Les scores qui se trouvent dans l'intervalle $[t-r_1, t+r_2]$ correspondent à la zone de recouvrement des distributions des échantillons authentiques et imposteurs, et subissent une transformation linéaire. En revanche, les scores en dehors de cette plage sont transformés de manière non linéaire.

Estimateurs Tanh (Tangente hyperbolique)

Les estimateurs Tangente hyperbolique (Tanh) ont été proposés par Hampel et al. et sont réputés pour leur robustesse et leur efficacité [18]. Pour une distribution initiale des scores de développement située dans l'intervalle $[0, 1]$, une transformation préalable des scores est nécessaire pour les déplacer vers l'intervalle $[-1, 1]$. Cette transformation est similaire à celle du min-max et peut être réalisée en utilisant l'équation (1.12).

$$st_k = \frac{2s_k - (\min + \max)}{\min - \max} \quad (1.12)$$

La première étape consiste à appliquer la fonction d'influence de Hampel, définie par l'équation (1.13), aux scores de développement préalablement transformés dans l'intervalle $[-1, 1]$. Cette fonction réduit l'influence des points situés aux extrémités de la distribution (identifiés par a , b et c) lors de l'estimation des paramètres de position et d'échelle. Cela rend la méthode insensible aux valeurs aberrantes.

$$\psi(u) = \begin{cases} u & \text{si } 0 \leq |u| < a \\ a \operatorname{sign}(u) & \text{si } a \leq |u| < b \\ a \operatorname{sign}(u) \left(\frac{c - |u|}{c - b} \right) & \text{si } b \leq |u| < c \\ 0 & \text{si } |u| \geq c \end{cases} \quad (1.13)$$

La Table 1.2 présente un résumé des caractéristiques de chacune des techniques de normalisation mentionnées précédemment, en termes de robustesse et d'efficacité. Dans les fusions multimodales présentées dans cette mémoire, les techniques utilisées sont min-max pour sa simplicité, zScores pour son efficacité, et Tanh pour sa combinaison d'efficacité et de robustesse.

Table 1. 2 Récapitulatif des techniques de normalisation de score.

Technique de normalisation	Robustesse	Efficacité
Min-Max	Non	N/A
Decimal scaling	Non	N/A
Z-Score	Non	Elevée (optimale pour des distributions gaussiennes)
Médiane et MAD	Oui	Modérée
Double sigmoïde	Oui	Elevée
Estimateurs Tanh	Oui	Elevée

Conclusion

Dans ce premier chapitre, nous avons abordé les principes de fonctionnement et les outils d'évaluation d'un système biométrique. Nous avons également souligné que la conception d'un système biométrique multimodal dépend de plusieurs facteurs, tels que les sources d'informations fusionnées, l'architecture et le niveau de fusion. Il est important de prendre en compte ces aspects lors de la conception d'un système biométrique afin de garantir son efficacité et sa fiabilité. Les chapitres suivants exploreront plus en détail les différentes techniques et approches de fusion multimodale dans le contexte biométrique.

La Biométrie de la main

Introduction

La modalité biométrique de la forme de la main est utilisée pour identifier et caractériser une personne en se basant sur la silhouette de sa main et/ou des caractéristiques géométriques telles que la longueur et la largeur des doigts, les aires, les périmètres et les ratios. Comparée à d'autres traits biométriques, la mesure de la forme de la main est relativement simple à obtenir grâce à des calculs rapides. Les systèmes de reconnaissance basés sur la géométrie de la main ont une histoire d'implémentation plus longue que de nombreuses autres modalités biométriques, étant donné qu'ils ont été proposés pour la première fois par Ernst en 1971.

Ce chapitre présente les différentes étapes d'un système biométrique général basé sur la main, ainsi qu'un aperçu des modalités de forme de main, d'empreinte de paume et des approches multimodales combinant la forme de la main et l'empreinte de paume, telles que décrites dans la littérature.

2.1 La biométrie de la main

La biométrie basée sur la reconnaissance de la forme de la main, également connue sous le nom de morphologie biométrique, consiste à mesurer des caractéristiques telles que l'épaisseur, la longueur, la surface et la largeur des doigts de la main. Cette technologie est largement utilisée pour le contrôle d'accès physique et le suivi horaire, et elle est appréciée pour sa simplicité et son coût abordable.

Les systèmes biométriques basés sur la forme de la main offrent un niveau de précision raisonnable. Ils se concentrent uniquement sur la géométrie de la main et ne nécessitent pas de prendre en compte l'empreinte palmaire. Cette approche est simple à mettre en œuvre et bénéficie d'une forte acceptation de la part des utilisateurs, que ce soit pour le contrôle d'accès ou le suivi horaire. Elle est couramment utilisée pour l'authentification et a prouvé sa fiabilité au fil du temps.

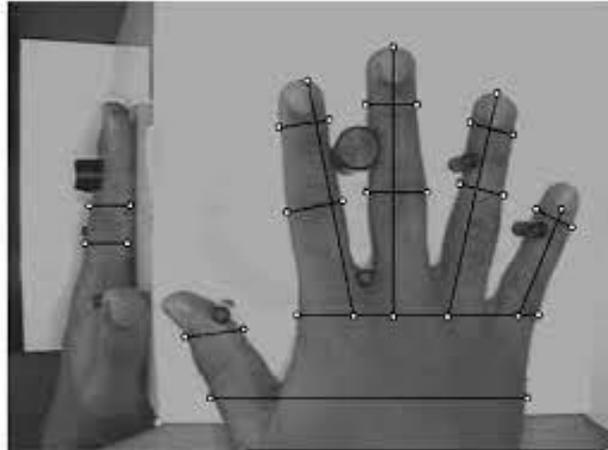


Figure 2. 1 La géométrie de la main [19].

2.2 Pourquoi utiliser La biométrie de la main?

La biométrie basée sur la forme de la main est considérée comme une "biométrie sans traces". En effet, l'utilisateur ne laisse aucune empreinte de l'épaisseur de ses doigts, préservant ainsi sa liberté et son anonymat. Cette approche est très conviviale et facile à mettre en place.

La biométrie de la forme de la main fonctionne même dans des conditions difficiles et avec des mains endommagées par leur utilisation. Contrairement aux empreintes digitales, la morphologie de la main ne nécessite pas de contact direct avec des surfaces potentiellement corrosives ou contaminantes, telles que le ciment, les produits chimiques ou la peinture.

Les technologies biométriques sont de plus en plus utilisées comme base pour de nombreuses solutions d'identification et de vérification personnelles. Des expériences ont montré que les caractéristiques physiques de la main humaine, telles que la longueur des doigts et la largeur des doigts, contiennent des informations capables de vérifier l'identité d'un individu.

La géométrie de la main est souvent utilisée pour le contrôle d'accès physique et le suivi horaire, en particulier dans les administrations. Cette forme de biométrie implique l'analyse de

90 caractéristiques de la main, telles que la longueur et la largeur des doigts, la forme des articulations et le tracé des lignes de la main [20].

2.3 Topographie et L'anatomie de la main

La main est une structure anatomiquement complexe, avec cinq doigts distincts, chacun ayant un nom spécifique.

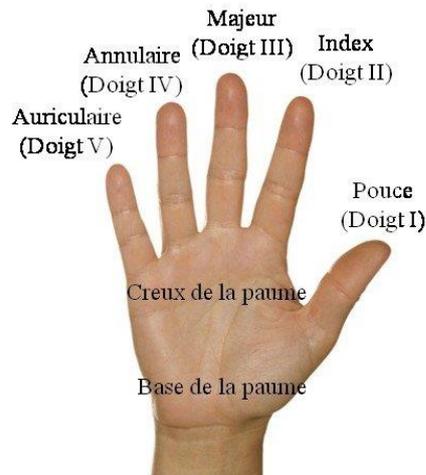


Figure 2.2 Anatomie de la paume de la main droite .

La main est composée de 27 osselets qui interagissent entre eux grâce à des articulations.

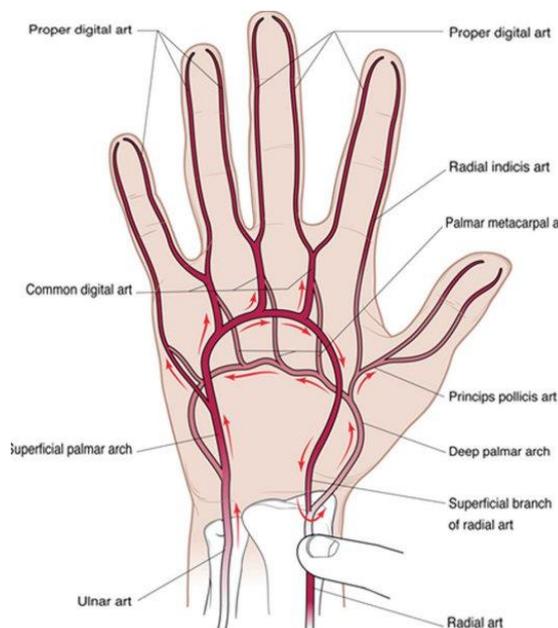


Figure 2.3 Dissection profonde palmaire .[21]

2.4 La géométrie de la main

La géométrie de la main est une branche de la géométrie qui se focalise sur l'étude de la structure et de la forme de la main humaine. Elle analyse les relations spatiales, les proportions et les mesures des différentes composantes de la main, telles que les doigts, les articulations, les os, les muscles et les tendons.

Cette discipline examine les lignes et les courbes formées par les doigts et les articulations lors des mouvements de flexion ou d'extension. Elle s'intéresse également aux angles formés par ces mouvements. De plus, elle explore les proportions entre les différentes parties de la main, comme la longueur des doigts par rapport à la paume, la largeur des articulations et la taille des os.

La géométrie de la main trouve des applications dans divers domaines tels que l'ergonomie, l'anatomie, la médecine, la robotique et même l'art. Par exemple, en ergonomie, les principes de la géométrie de la main sont utilisés pour concevoir des objets et des outils qui s'adaptent confortablement à la main humaine. En médecine, ces connaissances peuvent être exploitées pour diagnostiquer et traiter des problèmes liés à la main [22].

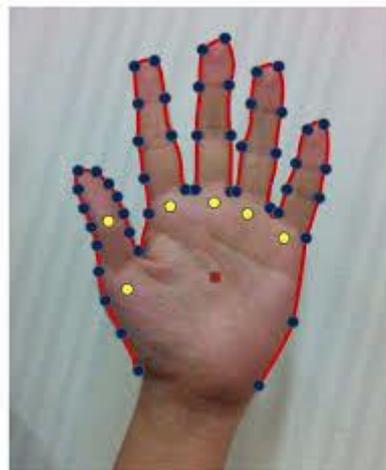


Figure 2.4 Les points caractéristiques dans la géométrie de la main

2.5 Les doigts

Pour modéliser la forme de la main, certains chercheurs ont suggéré de segmenter les doigts individuellement afin de représenter séparément leurs formes (voir figure 2.4). Une approche proposée par Oden consiste à modéliser la forme des doigts de chaque individu à l'aide de fonctions polynomiales implicites du quatrième degré. Ils ont également extrait les invariants

de Keren à partir des polynômes ajustés, qui servent d'invariants de caractéristiques pour les transformations affines.

Une autre approche, présentée par Ribaric et Fratric, segmente la main en six sous-images qui décrivent la région de la paume et les cinq surfaces des doigts. À partir de ces sous-images, les caractéristiques les plus importantes sont extraites en utilisant la transformée de Karhunen-Loève pour obtenir des "eigenfingers" (doigts propres) qui sont ensuite fusionnés avec des "eigenpalms" (paumes propres). Dans une autre étude, Xiong a identifié plusieurs doigts alignés selon un modèle elliptique à l'aide de transformations euclidiennes [23].

Ces approches illustrent différentes méthodes utilisées pour segmenter et modéliser la forme des doigts de la main dans le cadre de la reconnaissance biométrique.

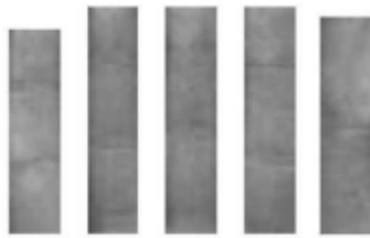


Figure 2.5 Surface des 5 doigts [23]

2.6 La paume de la main

Dans le domaine de la biométrie, la paume de la main désigne la surface interne de la main, incluant la zone entre la base des doigts et le poignet. La biométrie consiste à utiliser des caractéristiques physiques ou comportementales uniques pour l'identification des individus.

L'identification de la paume de la main est une technique biométrique qui exploite les caractéristiques spécifiques de la paume pour identifier et vérifier l'identité d'une personne. Ces caractéristiques peuvent comprendre les lignes de la main, les motifs des vaisseaux sanguins, les plis de la peau et d'autres détails propres à la paume.

Pour capturer ces caractéristiques, des dispositifs de reconnaissance de la paume, tels que des scanners ou des caméras spécialement conçus, sont utilisés. Ces dispositifs permettent de prendre une image ou une empreinte de la paume, qui est ensuite analysée pour extraire les caractéristiques biométriques uniques.

L'identification de la paume de la main présente certains avantages par rapport à d'autres méthodes biométriques telles que la reconnaissance faciale ou l'empreinte digitale. La paume de la main offre une plus grande surface de capture, facilitant ainsi l'acquisition des données biométriques. De plus, les caractéristiques de la paume sont moins susceptibles d'être altérées par des blessures ou des changements naturels par rapport à certaines autres parties du corps.

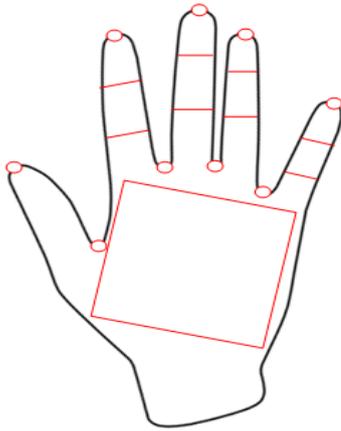


Figure 2. 6 La paume de la main.

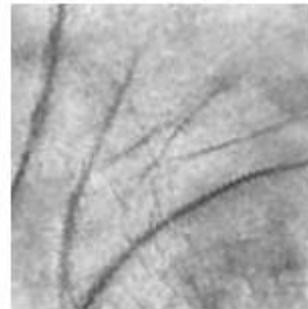


Figure 2. 7 L'empreinte palmaire.

2.7 Caractéristiques de l'empreinte palmaire

L'empreinte palmaire, tout comme toute autre image, présente des caractéristiques géométriques telles que la longueur, la largeur et la surface. Ces caractéristiques sont utiles pour une première vérification.

La capture de l'empreinte palmaire se fait généralement à basse résolution, ce qui permet un traitement d'image plus rapide et plus efficace.

En raison de la nature de l'empreinte palmaire, il y a peu de risques d'intrusion ou de falsification, ce qui en fait une méthode de vérification biométrique fiable.

De plus, l'utilisation de l'empreinte palmaire est souvent bien acceptée par les utilisateurs, ce qui se traduit par un taux élevé d'acceptation et de satisfaction.

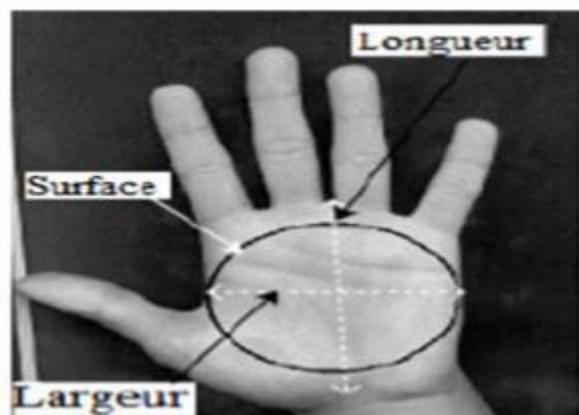


Figure 2.8 Caractéristiques géométriques de l'empreinte palmaire [24]

2.8 Réseau veineux

La biométrie du réseau veineux de la main est une technologie de reconnaissance qui se base sur les caractéristiques uniques des veines présentes dans la main d'une personne. Elle est utilisée comme méthode d'authentification ou d'identification biométrique.

Le réseau veineux de la main est composé d'un réseau de vaisseaux sanguins qui transportent le sang vers et depuis la main. Ces vaisseaux sanguins forment un motif unique pour chaque individu, similaire à une empreinte digitale. Les caractéristiques utilisées pour l'identification biométrique du réseau veineux de la main sont basées sur la disposition, l'espacement et la taille des veines.

Lors d'une vérification biométrique du réseau veineux de la main, un dispositif d'imagerie spécifique capture une image infrarouge ou proche infrarouge de la main de l'individu. Cette image permet de visualiser les veines et d'extraire les caractéristiques uniques du réseau veineux.

Les avantages de la biométrie du réseau veineux de la main sont les suivants :

- La technologie est non invasive, car elle ne nécessite pas de contact physique direct avec la main.
- Les veines sont situées à l'intérieur du corps, rendant la falsification plus difficile par rapport aux empreintes digitales ou aux iris.
- Les caractéristiques du réseau veineux sont stables et peu susceptibles de changer au fil du temps.

La biométrie du réseau veineux de la main est utilisée dans divers domaines, tels que la sécurité d'accès physique, l'authentification pour les transactions financières, l'accès aux systèmes informatiques et la gestion des identités. Cependant, il est important de noter que cette technologie peut varier en fonction des systèmes et des fournisseurs spécifiques.

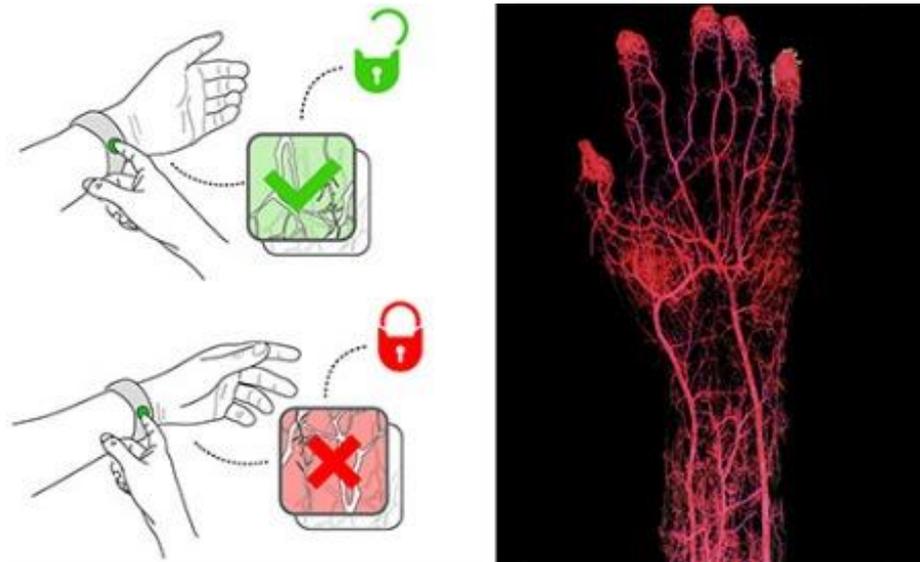


Figure 2.9 La biométrie du réseau veineux de la main[26]

2.9 Les dispositifs de la biométrie de la main

2.9.1 Dispositifs biométrique avec contact

Actuellement, la plupart des approches documentées utilisent des techniques de reconnaissance basées sur l'acquisition bidimensionnelle au contact à l'aide de scanners à plat ou de dispositifs basés sur des capteurs CCD. Les scanners à plat sont couramment utilisés dans les systèmes à faible coût, tandis que les dispositifs à base de CCD offrent des échantillons de meilleure qualité et des temps d'acquisition plus rapides. Certains dispositifs d'acquisition tridimensionnelle au contact, tels que les caméras CCD et les caméras, ont été proposés pour améliorer la précision de la reconnaissance, mais ils nécessitent une installation complexe et plus coûteuse.

Cependant, les méthodes basées sur le contact présentent des inconvénients majeurs. Tout d'abord, la pression inégale exercée par la main sur le capteur peut causer des déformations dans les images acquises. De plus, l'accumulation de saleté après des acquisitions répétées peut réduire la qualité des échantillons. Enfin, l'acceptabilité par les utilisateurs peut poser problème, car certaines personnes peuvent être réticentes à toucher des surfaces qui ont été en contact avec d'autres personnes par souci d'hygiène.

Ces inconvénients soulignent la nécessité de rechercher des solutions alternatives qui permettent une acquisition sans contact et qui répondent aux préoccupations d'hygiène et de confort des utilisateurs [27].



Figure 2.10 Le dispositif d'acquisition CCD bidimensionnel à base contact

2.9.2 Dispositifs biométrique sans contact

a. Reconnaissance des veines de la main : Ce type de dispositif utilise des capteurs infrarouges pour détecter les motifs uniques des veines présentes dans la main. Ces motifs sont utilisés pour créer une empreinte biométrique unique permettant d'identifier de manière précise une personne.

b. Reconnaissance des empreintes digitales sans contact : Contrairement aux scanners d'empreintes digitales traditionnels qui nécessitent un contact direct avec un capteur, les dispositifs sans contact utilisent des technologies telles que la reconnaissance d'images ou la détection capacitive pour capturer les empreintes digitales sans toucher la surface du capteur.

c. Reconnaissance de la forme de la main : Certains dispositifs biométriques analysent la forme et les caractéristiques générales de la main, telles que la taille, la forme des doigts, la longueur des phalanges, etc. Ces informations sont utilisées pour créer un modèle biométrique unique qui peut être utilisé pour l'identification ou la vérification d'identité.

d. Reconnaissance des mouvements de la main : Cette technologie utilise des capteurs tels que des caméras 3D ou des capteurs de mouvement pour capturer et analyser les mouvements de la main. Ces mouvements peuvent être utilisés comme une signature biométrique unique pour authentifier une personne.

Il est important de noter que l'utilisation de ces dispositifs biométriques sans contact de la main peut varier en fonction de leur application spécifique et des exigences de sécurité. De plus, d'autres méthodes biométriques de la main sans contact sont en cours de développement, mais celles-ci sont parmi les plus couramment utilisées à ce jour [28].



Figure 2.11 Dispositif d'acquisition à base sans contact[29]

Conclusion

À géométrie de la main, l'empreinte palmaire de la main et des doigts sont des méthodes physiques de reconnaissance relativement simples qui se basent sur des mesures telles que la taille de la paume, la largeur, la longueur et la courbure des doigts. Malgré la simplicité des méthodes d'extraction et de comparaison des caractéristiques, la géométrie de la main permet une reconnaissance relativement robuste, et de nombreux systèmes sont déployés pour des contrôles physiques.

L'avantage de cette technique est qu'elle est résistante aux facteurs environnementaux tels que l'humidité, ainsi qu'aux facteurs individuels tels que les coupures ou la peau sèche. Cela en fait une méthode de reconnaissance biométrique fiable dans des conditions variées.

Cependant, il convient de noter certaines limitations. Par exemple, il peut être difficile d'extraire des informations géométriques pertinentes lorsque les utilisateurs portent des bagues ou sont limités dans leurs mouvements en raison de problèmes tels que l'arthrite. De plus, la précision de la reconnaissance peut être affectée par la qualité de l'image capturée et par la variabilité naturelle des caractéristiques de la main d'une personne.

Malgré ces limitations, la géométrie de la main et l'empreinte palmaire restent des modalités biométriques populaires et largement utilisées dans diverses applications, offrant une solution pratique et robuste pour l'identification et la vérification des individus.



Réalisation Hardware et Software du dispositif Biométrique

Introduction

Les systèmes d'identification biométrique basés sur la géométrie de la main fournissent des estimations de certaines mesures de la main, telles que la longueur et la largeur des doigts. L'identification par la géométrie de la main repose sur le fait que chaque personne a une forme de main pratiquement unique et que cette forme ne change pas après un certain âge. En pratique, l'identification par la géométrie de la main repose généralement sur la détection de cinq points correspondant aux extrémités des doigts et de quatre points situés entre eux (points de vallée). La détection de ces points peut être difficile, notamment lorsque les doigts ne sont pas écartés. Des méthodes spécifiques doivent souvent être mises en œuvre lors des étapes d'acquisition et de prétraitement pour faciliter la détection de ces points. Une fois les points localisés, les caractéristiques biométriques nécessaires à l'identification sont extraites. La méthodologie utilisée dans ce projet pour la conception d'un système d'identification basé sur la géométrie de la main a été mise en œuvre dans l'environnement MATLAB. Les principales idées de ce système sont divisées en deux phases : l'enrôlement et l'identification. La réalisation du projet peut être considérée comme satisfaisante en fonction des objectifs visés et de leur concrétisation. Que le projet soit virtuel, nécessitant uniquement l'utilisation d'un ordinateur, comme les applications de simulation ou de modélisation, ou qu'il soit physique, utilisant des robots, des appareils électroniques, etc., il est important de prendre en compte les obstacles rencontrés au cours de cette phase et d'apporter les modifications nécessaires du côté matériel (équipements, dispositifs, etc.) ou du côté logiciel (logiciels informatiques, programmation, etc.).

3.1 Partie Hardware

Les principaux composants nécessaires pour la réalisation de ce projet sont :

- Raspberry Pi : Un ordinateur monocarte utilisé comme cœur du système pour le traitement des données et le contrôle des autres composants.
- Caméra : Une caméra compatible avec le Raspberry Pi pour capturer les images de la main et les utiliser dans les processus de reconnaissance et d'identification.
- Capteur Ultrason HC-SR04 : Un capteur de distance utilisé pour détecter la présence de la main et déclencher les actions du système en conséquence.
- Éclairage : Des sources lumineuses appropriées pour assurer un éclairage adéquat lors de la capture des images de la main.
- Afficheur LCD : Un écran LCD pour afficher les informations pertinentes, telles que les résultats de l'identification ou les instructions pour l'utilisateur.
- Clavier : Un clavier pour permettre à l'utilisateur d'interagir avec le système, par exemple pour entrer des commandes ou des informations supplémentaires.
- Modem : Un modem pour permettre la communication avec d'autres systèmes ou services, par exemple pour envoyer les données d'identification à un serveur distant.
- PC : Un ordinateur personnel utilisé pour le développement du logiciel, la configuration du système et l'analyse des données biométriques.

Ces composants jouent des rôles clés dans la création et le fonctionnement du projet, permettant la capture des images de la main, le traitement des données, l'affichage des informations, l'interaction avec l'utilisateur et la communication avec d'autres systèmes si nécessaire.

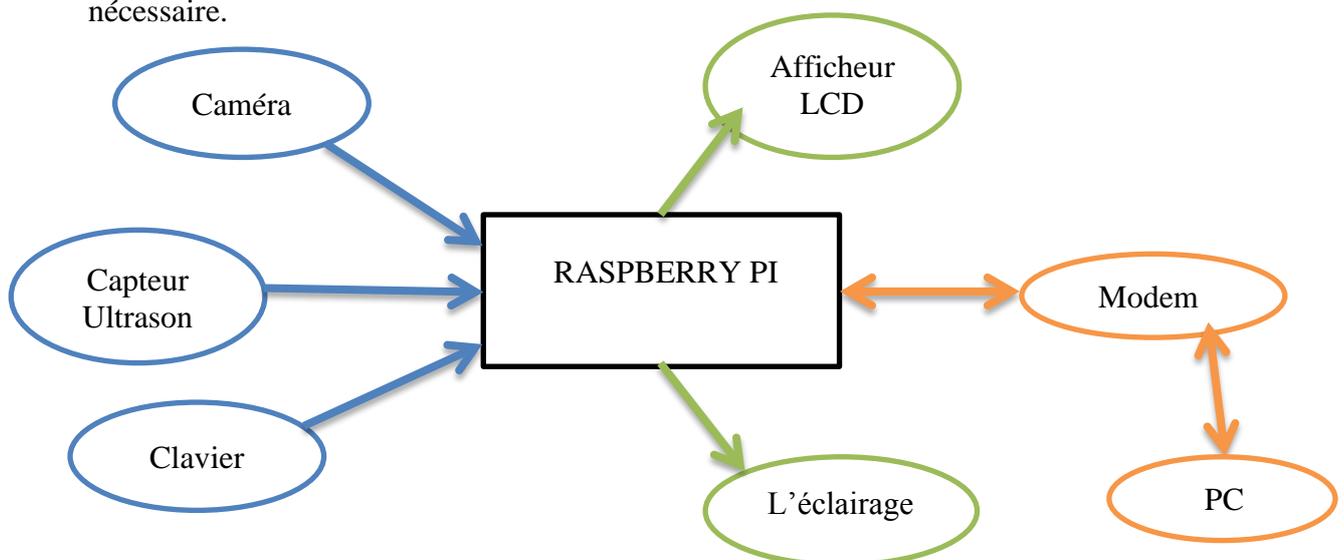


Figure 3.1. Schéma synoptique de notre projet.

3.1.1 RASPBERRY PI

Le Raspberry Pi est un nano-ordinateur monocarte à processeur ARM, créé par des professeurs du département informatique de l'université de Cambridge, dans le cadre de la fondation Raspberry Pi. Son objectif principal est de rendre l'accès à l'informatique et au digital making plus accessible et abordable. Grâce à son faible coût et à sa compatibilité avec des logiciels libres, le Raspberry Pi permet l'exécution de différentes variantes du système d'exploitation GNU/Linux, tels que Debian ou Ubuntu, ainsi que des logiciels compatibles.

Le Raspberry Pi est fourni nu, c'est-à-dire sans boîtier, câble d'alimentation, clavier, souris ni écran, dans le but de réduire les coûts et de permettre l'utilisation de matériel existant. Toutefois, des kits tout-en-un regroupant tous les éléments nécessaires sont disponibles à des prix abordables sur le web.

Son prix initial était estimé à 25 dollars américains, soit environ 19 euros, en mai 2011. Les premiers exemplaires ont été mis en vente le 29 février 2012 pour environ 25 euros. Depuis lors, de nombreuses versions ont été développées, avec des prix variant en fonction des fonctionnalités et des améliorations apportées. Le Raspberry Pi est devenu très populaire et a dépassé la barre des dix millions d'unités vendues en septembre 2016.

En plus de son faible coût, le Raspberry Pi est apprécié pour sa polyvalence. Il dispose de broches GPIO (General Purpose Input/Output) qui permettent la connexion de cartes d'extension ou d'autres composants électroniques pour la réalisation de projets personnalisés. De nombreux créateurs et passionnés du monde entier utilisent le Raspberry Pi en raison de sa facilité d'utilisation et de son attractivité économique.

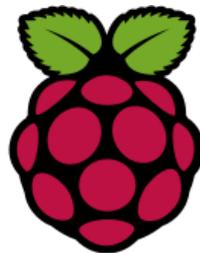


Figure 3. 2 Logo Raspberry Pi

3.1.1.1 Les caractéristiques de Raspberry Pi 3

- Processeur ARMv7 Broadcom BCM2837 – 4 Cœurs – 64 bits
- Fréquence d'horloge de 1.2Ghz (+33% par rapport au Pi 2)
- Port Ethernet 10/100
- 1GB RAM
- WiFi intégré à la carte 802.11 b/g/n (BCM43438)
- Bluetooth Low Energy intégré à la carte (BCM43438)
- HDMI 1.3a
- Une alimentation de 2.5 Ampères est vivement conseillée pour ce modèle

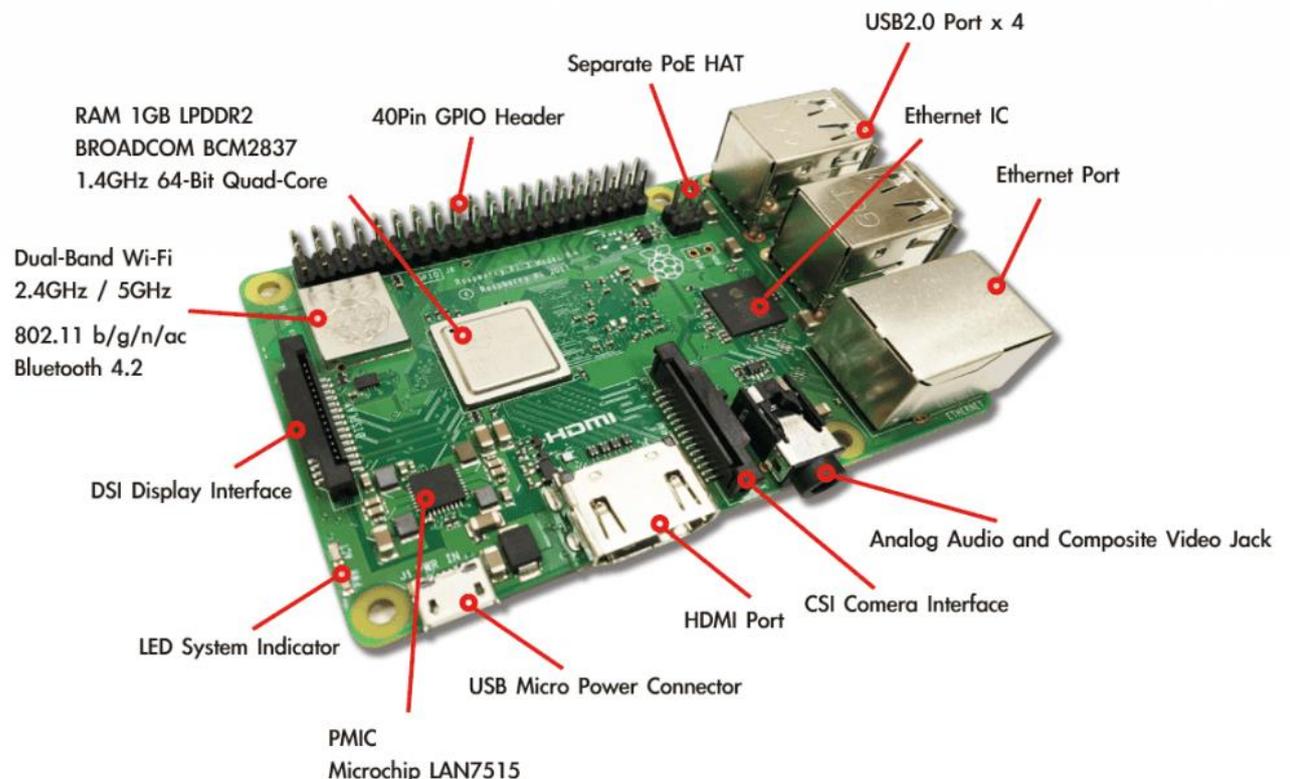


Figure 3.3 Raspberry Pi 3B+[30].

3.1.2 Capteur Ultrason HC-SR04

Le capteur HC-SR04 utilise la technologie des ultrasons pour mesurer la distance par rapport à un objet. Il offre une grande précision et une stabilité élevée dans la détection sans contact. Contrairement à d'autres capteurs qui peuvent être influencés par la lumière du soleil ou des matériaux sombres, le capteur HC-SR04 n'est pas affecté par ces facteurs. Cependant, il peut être plus difficile de détecter des matériaux tels que les vêtements, car ils peuvent absorber ou

réfléchir les ondes ultrasonores. Dans l'ensemble, le capteur HC-SR04 est largement utilisé pour des applications nécessitant des mesures de distance précises et fiables.

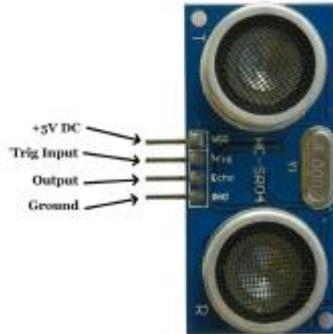


Figure 3.4 Capteur Ultrason HC-SR04 .

3.1.2.1 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 μ s

3.1.2.2 Broches de connexion

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

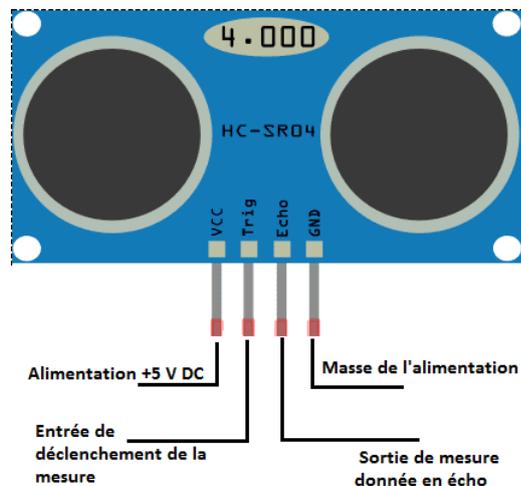


Figure 3.5 Capteur Ultrason Broches de connexion.

3.1.2.3 Distance de l'objet

La distance parcourue par un son peut être calculée en multipliant la vitesse du son (environ 340 m/s) par le temps de propagation. Pour convertir la durée d'impulsion fournie par le capteur HC-SR04 en temps de propagation, il faut multiplier la valeur par 10 μ s. Étant donné que le son fait un aller-retour, la distance réelle est la moitié de la valeur calculée.

La formule pour calculer la distance est donc : distance = (vitesse du son * temps de propagation) / 2

En utilisant les valeurs spécifiques pour la vitesse du son (340 m/s) et le temps de propagation (obtenu à partir de la durée d'impulsion en multipliant par 10 μ s), on peut calculer la distance.

Il est important de noter que la formule alternative $d = \text{durée}/58 \text{ cm}$ est également utilisée dans le manuel d'utilisation du capteur HC-SR04. Cependant, cette formule donne des résultats légèrement moins précis car la fraction 17/1000 est approximativement égale à 1/58.8235.

Il convient également de noter que pour des distances plus grandes, il est nécessaire que la surface de l'objet détecté mesure au moins 0.5 m² pour assurer une détection précise.

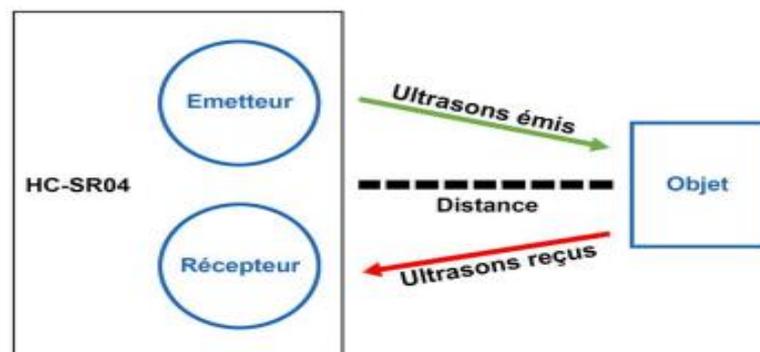


Figure 3.6 Capteur Ultrason Distance de L'objet [31].

3.1.3 Caméra

Une caméra est un dispositif utilisé pour capturer et enregistrer des images ou des vidéos successives. Elle peut être utilisée dans de nombreux domaines tels que le cinéma, la télévision, la recherche, la surveillance, l'imagerie industrielle et médicale, ainsi que pour des applications professionnelles ou domestiques.

Le terme "caméra" provient du latin "camera" qui signifie "chambre" en français. La "camera obscura", ou "chambre noire", est un dispositif optique connu depuis l'Antiquité qui permet de former une image inversée d'une scène sur un écran ou une toile.

Les premières caméras ont été développées aux États-Unis, puis en Europe, grâce à l'invention du support souple et transparent en nitrate de cellulose par John Carbutt en 1888 et sa commercialisation par George Eastman en 1889 sous la marque Kodak. Cela a conduit à la création de la première caméra de cinéma, le Kinétographe, par l'équipe de Thomas Edison.

Aujourd'hui, la grande majorité des caméras sont numériques, offrant une variété de caractéristiques telles que la résolution, la qualité d'image, la sensibilité, le support d'enregistrement, etc., adaptées aux besoins et aux domaines d'utilisation spécifiques.

Dans ce contexte, une caméra sport de 12 mégapixels au format H.264 a été utilisée, et une fois connectée au Raspberry Pi, elle peut être utilisée comme une webcam ou une caméra pour l'ordinateur.



Figure 3.7 La Caméra utilisée dans le dispositif Biométrique.

3.1.4 Clavier

Le clavier est généralement organisé en une matrice, où chaque touche est située à l'intersection d'une ligne et d'une colonne. Cela permet d'identifier la touche enfoncée en utilisant un système de détection. Dans le cas d'un clavier matriciel, le nombre de lignes d'entrée/sortie est égal à la somme du nombre de colonnes et du nombre de lignes.



Figure 3.8 Clavier

Il existe deux principales méthodes pour l'identification de la touche enfoncée :

1. **Balayage de colonne** : On génère un niveau bas sur la première colonne tandis que les autres colonnes restent au niveau haut. Ensuite, on décale le niveau bas sur la deuxième colonne tout en maintenant les autres colonnes au niveau haut. Ce processus de balayage des colonnes est répété en boucle et à une vitesse élevée. Le microcontrôleur surveille en permanence le niveau sur les lignes. Lorsqu'une touche est enfoncée, à la fois la colonne correspondante et la ligne correspondante sont au niveau bas. Des résistances de tirage sont utilisées sur les lignes pour maintenir un niveau haut lorsque aucune touche n'est enfoncée.
2. **Balayage de ligne** : Dans cette méthode, on envoie simultanément un niveau bas sur toutes les colonnes et on lit le niveau sur chaque ligne. Si une touche est enfoncée, un niveau bas sera détecté sur la ligne correspondante. Le code lu des lignes est ensuite renvoyé vers les colonnes, ce qui fait apparaître un niveau bas dans l'une d'entre elles. Les positions des deux "0" lus donnent les coordonnées de la touche recherchée. Cette méthode peut potentiellement être plus rapide que la précédente, car elle nécessite seulement deux étapes au lieu de N étapes (N étant le nombre de colonnes). Cependant, des résistances de tirage sont nécessaires à la fois pour les lignes et pour les colonnes.

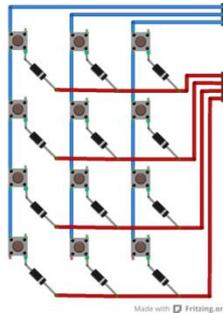


Figure 3.9 Câblage intérieur de Clavier 3x4 [32].

3.1.5 L'éclairage

L'éclairage englobe toutes les méthodes utilisées par l'homme pour créer les conditions de luminosité qu'il juge nécessaires pour ses activités ou son bien-être dans son environnement. Il implique l'utilisation d'une source de lumière, qu'elle soit naturelle ou artificielle, ainsi que divers dispositifs tels que des batteries, des luminaires ou des miroirs/puits de lumière, qu'ils soient fixes ou mobiles.



Figure 3.10 L'éclairage.

3.1.6 Afficheur LCD

Un afficheur LCD, également connu sous le nom d'écran à cristaux liquides, est un dispositif utilisé comme interface visuelle entre un système ou un projet et l'utilisateur. Son but principal est de fournir des informations pertinentes du système à l'utilisateur. L'afficheur LCD affiche donc des données qui peuvent être utilisées et interprétées par l'utilisateur d'un système donné.



Figure 3.11 Afficheur LCD 4x16.

3.1.6.1 Caractéristiques

- ▶ Afficheur alphanumérique 16x4
- ▶ 5x8 points incluant le curseur
- ▶ Alimentation en 5V (disponible également en 3V)
- ▶ WG16032D3 Option alimentation en 3V
- ▶ Taux de rafraîchissement 1/16 duty cycle
- ▶ Les Led se pilotent sur les broches 1, 2, 15, 16 or A et K
- ▶ Interface : 6800 (ST7066 IC ou équivalent), option SPI/I2C (RW1063 IC) [33]



Figure 3.12 Style D'affichage de LCD

3.1.6.2 Fonction PIN sur l'interface

Pin No.	Symbole	Description
1	V _{SS}	Ground
2	V _{DD}	Power supply for logic
3	V _O	Contrast Adjustment
4	RS	Data/ Instruction select signal
5	R/W	Read/Write select signal
6	E	Enable signal
7~14	DB0~DB7	Data bus line
15	A	Power supply for B/L +
16	K	Power supply for B/L -

3.1.7 Routeur « modem »

Un routeur "modem" est un dispositif électronique utilisé pour la transmission de données numériques sur un canal analogique. Le terme "modem" est un mot-valise formé à partir de "modulateur-démodulateur". Il peut être sous la forme d'un boîtier indépendant ou d'une carte insérée dans un ordinateur.

Le modem effectue la modulation des données numériques, c'est-à-dire qu'il les encode et synthétise un signal analogique qui est généralement une fréquence porteuse modulée. La démodulation, qui est l'opération inverse, permet au récepteur de récupérer l'information numérique.

Le terme "modem" est utilisé pour désigner les appareils qui permettent la communication entre différentes machines numériques, comme les ordinateurs et les systèmes embarqués. Il est également utilisé pour accéder à Internet, envoyer ou recevoir des télécopies, et même pour la téléphonie numérique, en utilisant un réseau analogique tel que le réseau téléphonique commuté, le réseau électrique ou les réseaux radio.



Figure 3.13 Le modem utilisé.[34]

3.1.8 Un PC serveur

Un PC serveur est un ordinateur spécialement conçu pour la gestion des opérations et le stockage de programmes liés au traitement d'images, aux logiciels, aux bases de données et au stockage des images provenant d'un boîtier, ainsi que pour les activités de retouche et de contrôle, entre autres. Ce type d'ordinateur est dédié à la gestion et à la manipulation de diverses tâches liées au traitement des images et aux opérations connexes.



Figure 3.14 PC serveur

3.2 Réalisation du boîtier

La figure 3.15 présente une image de la maquette montrant la vue extérieure, tandis que la figure 3.16 illustre la vue intérieure de la maquette. Ces deux images fournissent un aperçu détaillé de l'aspect extérieur et de l'aménagement intérieur de la maquette, offrant ainsi une compréhension complète de sa conception et de sa structure.



Figure 3. 15 Image de la maquette (vue extérieur).



Figure 3. 16 Image de la maquette (vue intérieur).

3.2.1 Utilisation du prototype :

La figure ci-dessus présente le prototype qui sera utilisé pour effectuer les acquisitions de la base de données nécessaires à notre travail. Cette illustration représente l'appareil ou l'équipement spécifique qui sera utilisé dans le processus de collecte des données nécessaires à notre étude.



Figure 3. 17 Image du prototype.

Lorsque nous commençons, nous devons d'abord sélectionner le mode : Administrateur (#) ou Utilisateur (*). Pour l'administrateur, l'écran LCD affiche deux messages lui permettant d'effectuer deux opérations distinctes : "Test (1)" ou "Enroll (2)".

En revanche, pour l'utilisateur, l'écran LCD affiche uniquement le message "Test".

Il est donc nécessaire de choisir le mode approprié et de suivre les instructions correspondantes affichées sur l'écran LCD en fonction de notre rôle, que ce soit en tant qu'administrateur ou utilisateur.



Figure 3. 18 Choix du mode.

Placez votre main droite dans le boîtier en veillant à maintenir une position droite avec l'avant-bras. L'objectif est de garantir un positionnement presque identique de la main lors de chaque test d'acquisition. Assurez-vous que votre main est maintenue dans une position stable et cohérente afin d'obtenir des résultats de test plus fiables et cohérents.



Figure 3. 19 Choix du mode.

Voici l'image de la main à l'intérieur du boîtier. L'objectif est de toucher le fond du boîtier avec le majeur, puis d'écarter les autres doigts une fois le contact établi. Cette action permet d'assurer un positionnement précis et reproductible lors de l'acquisition des données. En suivant ces instructions, vous pouvez obtenir une configuration optimale pour effectuer les tests nécessaires.



Figure 3. 20 Image de la main

Comme visible dans l'illustration, il y a un espace entre la main et le haut du boîtier.



Figure 3. 21 L'espace entre la main et le haut du boîtier.

Afin d'obtenir des résultats optimaux, il est important de maintenir une stabilité adéquate. Pour ce faire, faites glisser votre main de manière à ce qu'elle touche le haut du boîtier avec les doigts écartés. Une fois que votre main est positionnée, veillez à ne pas la déplacer jusqu'à ce que l'écran LCD affiche un message vous demandant de retirer votre main. Cette étape garantit une acquisition précise et cohérente des données.



Figure 3. 22 Glisser la main vers le haut.

3.3 Partie Software

3.3.1 Organigramme

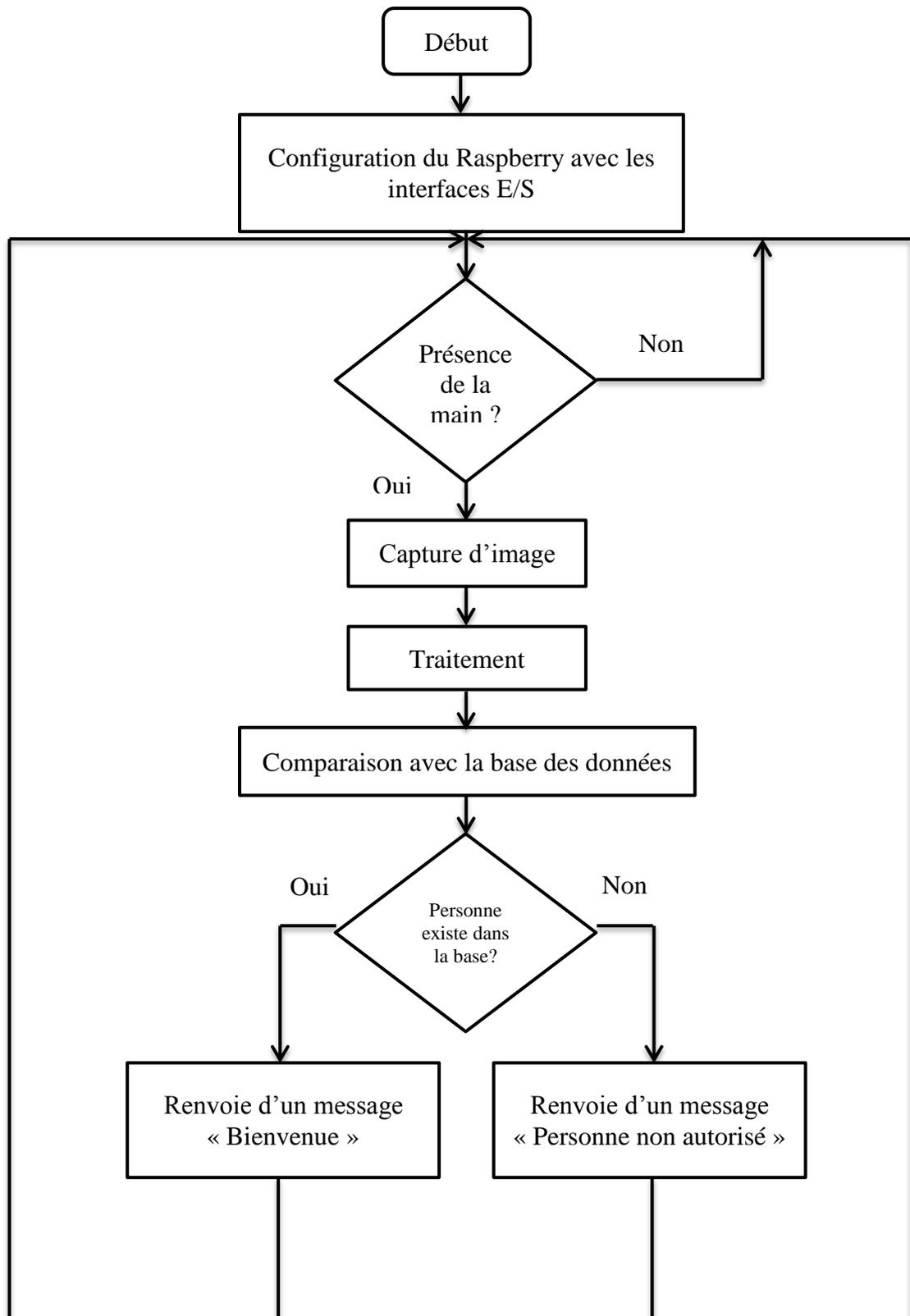


Figure 3.23 Organigramme

3.3.2 RASPBERRY PI 3B+ (Système d'exploitation)

Le système d'exploitation est essentiel pour exécuter des applications, des jeux et fournir une interface graphique conviviale sur votre Raspberry Pi. Raspbian, qui est maintenant connu sous le nom de Raspberry Pi OS, est le système d'exploitation de référence pour Raspberry Pi. Basé sur Linux Debian, il bénéficie de mises à jour régulières. Bien qu'il ait changé de nom en 2021, la nouvelle version de Raspberry Pi OS est plus facile à installer et à utiliser.

Spécialement optimisé pour Raspberry Pi, Raspberry Pi OS est une distribution polyvalente qui facilite la familiarisation avec le matériel. Il s'agit d'une distribution GNU/Linux basée sur la célèbre Debian, avec l'environnement de bureau LXDE choisi pour sa légèreté. Raspberry Pi OS est considéré comme la distribution la plus simple et la plus appropriée pour utiliser le Raspberry Pi [35].

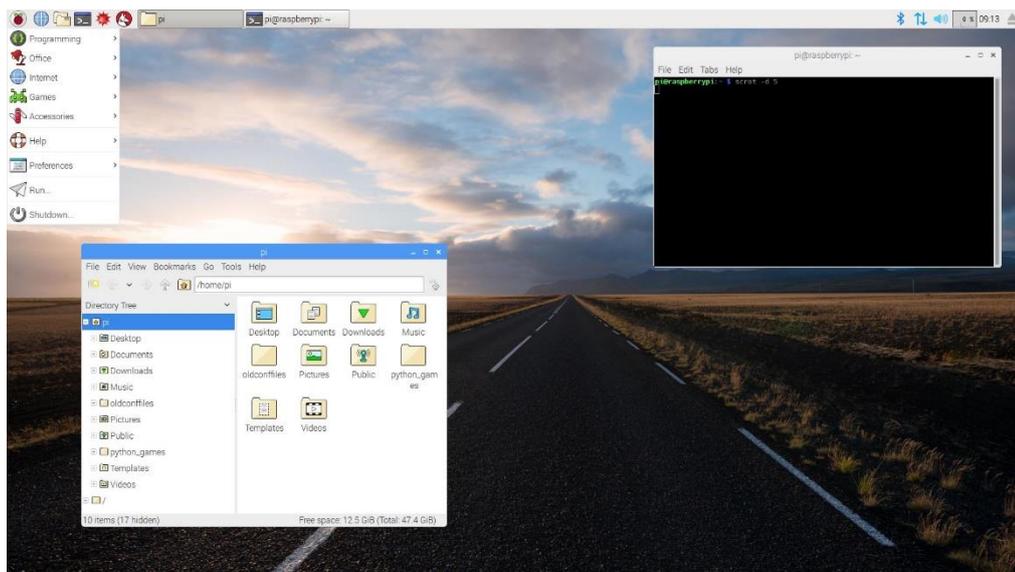


Figure 3.24 Interface de Raspberry Pi 3B+

3.3.3 Configuration

Vous pouvez configurer le système en utilisant un outil dédié, accessible via le menu « Préférences » → « Configuration du Raspberry Pi ». Cette interface conviviale vous permet de personnaliser des paramètres tels que la langue du système, la disposition du clavier, la date et d'autres options spécifiques au Raspberry Pi. Grâce à cet outil, vous pouvez facilement adapter le fonctionnement de votre Raspberry Pi selon vos besoins et préférences [36].

3.3.4 Logiciel Matlab

MATLAB est un logiciel de calcul numérique matriciel réputé pour sa syntaxe simple et conviviale. Il est largement utilisé dans les domaines de la finance et de l'ingénierie financière en raison de ses fonctionnalités avancées et de ses nombreuses boîtes à outils spécialisées. Grâce à sa vaste bibliothèque de fonctions pré-codées, MATLAB offre une prise en main rapide et efficace, à condition de suivre une approche rigoureuse.

Le langage de programmation utilisé dans MATLAB est similaire au langage C, avec l'avantage de reconnaître de nombreuses fonctions intégrées dans le logiciel. Contrairement au C ou au C++, il n'est pas nécessaire d'initialiser des bibliothèques avant d'exécuter du code MATLAB. De plus, MATLAB présente des aspects de programmation orientée objet similaires à ceux du langage C++. Il permet aux utilisateurs de créer leurs propres fonctions et de les appeler ultérieurement, offrant ainsi une grande flexibilité dans le développement de programmes personnalisés.

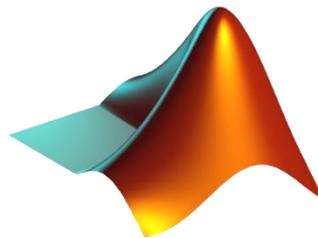


Figure 3.25 Logo de Matlab

Le logiciel MATLAB repose sur le langage MATLAB lui-même. Il dispose d'une interface en ligne de commande, qui fait partie intégrante de l'environnement MATLAB, et permet d'exécuter des commandes simples. Les séquences de commandes peuvent être sauvegardées dans des fichiers texte, généralement créés avec l'éditeur MATLAB, sous la forme d'un script ou encapsulées dans une fonction.

En plus de sa base logicielle, MATLAB est également complété par plusieurs boîtes à outils populaires, parmi lesquelles on retrouve :

- Communications Toolbox
- Control System Toolbox
- Simscape
- Image Processing Toolbox
- MATLAB Compiler
- Deep Learning Toolbox
- Optimization Toolbox

- Parallel Computing toolbox
- Real-Time Workshop, renommé commercialement Simulink Coder
- Robust Control Toolbox
- Signal Processing Toolbox
- Excel Link
- Simulink
- Statistics and Machine Learning Toolbox
- System Identification Toolbox
- Predictive Maintenance Toolbox
- Stateflow[19].

3.3.5 Python 3

Python est le langage de programmation open source le plus largement utilisé par les informaticiens. Il a gagné en popularité dans divers domaines tels que la gestion d'infrastructure, l'analyse de données et le développement de logiciels. L'une des principales qualités de Python est sa capacité à permettre aux développeurs de se concentrer sur ce qu'ils font plutôt que sur la manière de le faire. Il a libéré les développeurs des contraintes syntaxiques qui occupaient leur temps avec les langages plus anciens. Par conséquent, le développement de code avec Python est plus rapide que dans d'autres langages.

Python reste également accessible aux débutants, à condition de consacrer un peu de temps à son apprentissage. De nombreux tutoriels sont disponibles en ligne, sur des sites spécialisés et des chaînes YouTube. Les forums informatiques sont également des sources d'information précieuses, car de nombreux professionnels utilisent Python et peuvent fournir des réponses à des questions spécifiques.

Il convient de noter qu'il existe deux versions principales de Python : Python 2 et Python 3. Python 2, la version précédente, a cessé de recevoir des mises à jour en 2020. Python 3 est la version actuelle et offre des améliorations telles qu'un interpréteur plus efficace et un meilleur contrôle de la concurrence.

3.3.5.1 Les principales utilisations de Python par les développeurs sont :

- la programmation d'applications
- la création de services web
- la génération de code
- la métaprogrammation.

Techniquement, ce langage servira surtout pour le scripting et l'automatisation .



Figure 3.26 Logo de Python

3.3.6 FTP serveur

Le protocole de transfert de fichiers (File Transfer Protocol ou FTP) est une application installable sur un ordinateur qui permet le transfert de fichiers entre deux points, à savoir un serveur et un client. Son fonctionnement est similaire à celui d'un réseau local (LAN). L'avantage de cette application est qu'elle dispose d'une bibliothèque compatible avec Python, ce qui nous a permis de créer un client sur la Raspberry Pi et un serveur sur le PC serveur. Ainsi, lorsqu'une image est capturée, elle est automatiquement envoyée vers le PC serveur via FTP, et le fichier est stocké dans un emplacement spécifié par l'utilisateur. Cette approche facilite le transfert efficace des données entre les deux dispositifs et permet une gestion plus pratique des fichiers.

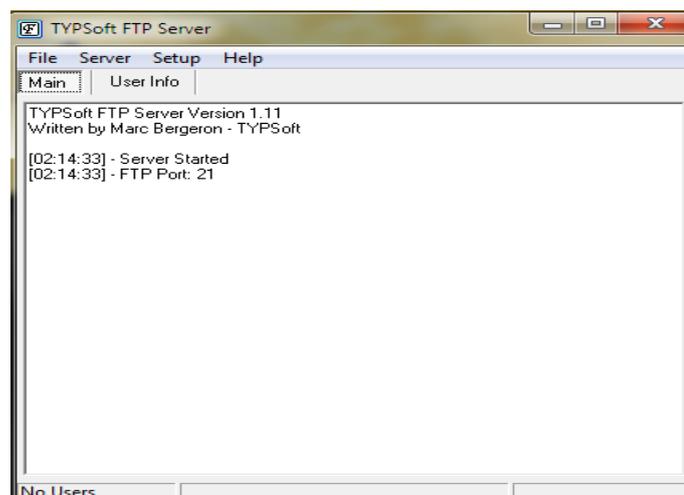


Figure 3.27 Console FTP serveur.

3.3.7 Traitement d'image

Le traitement d'images est une discipline de l'informatique et des mathématiques appliquées qui se focalise sur l'étude des images numériques et de leurs transformations dans le but d'améliorer leur qualité ou d'en extraire de l'information utile [38].

La compréhension du traitement d'images commence par une compréhension approfondie de ce qu'est une image. Les paramètres et les conditions d'acquisition et de numérisation des images jouent un rôle déterminant dans les opérations nécessaires pour extraire des informations pertinentes. Divers facteurs entrent en jeu, parmi lesquels :

- La résolution d'acquisition et le mode de codage utilisé lors de la numérisation, qui déterminent la précision des éventuelles mesures de dimensions effectuées sur l'image.
- Les réglages optiques utilisés, tels que la mise au point, qui influencent la netteté et la clarté de l'image.
- Les conditions d'éclairage, qui contribuent à la variabilité des images traitées.
- Le bruit provenant de la chaîne de transmission de l'image.

Tous ces éléments doivent être pris en compte lors du traitement des images afin d'obtenir des résultats précis et cohérents.

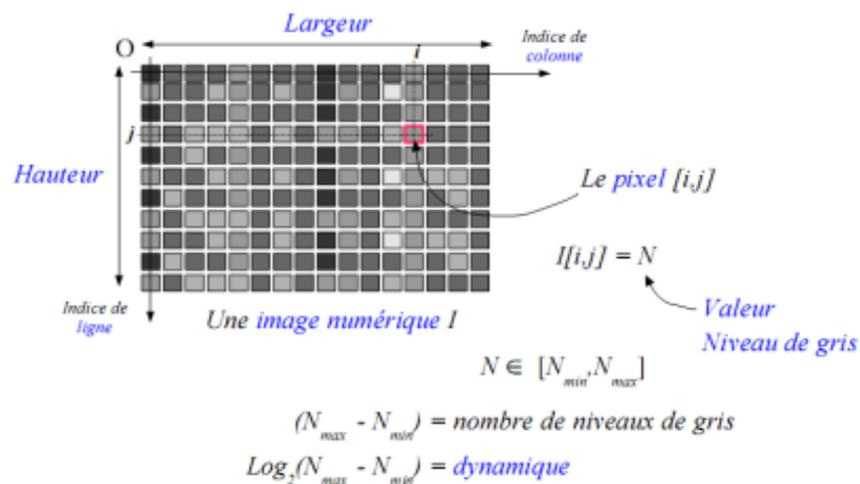


Figure 3.28 Image niveau de gris [39]

3.3.7.1 Traitement d'image Géométrie de la main

Le traitement des images nécessite une séquence d'étapes successives afin d'atteindre le résultat final souhaité. Parmi ces étapes essentielles figurent la segmentation, la squelettisation et l'extraction de points caractéristiques.

La première étape consiste en la segmentation, qui implique de diviser l'image en différentes régions ou objets distincts. L'objectif est de détecter et de délimiter avec précision les zones d'intérêt présentes dans l'image dans notre cas la main. Cette segmentation permet de séparer les objets du fond de l'image et de les isoler les uns des autres.

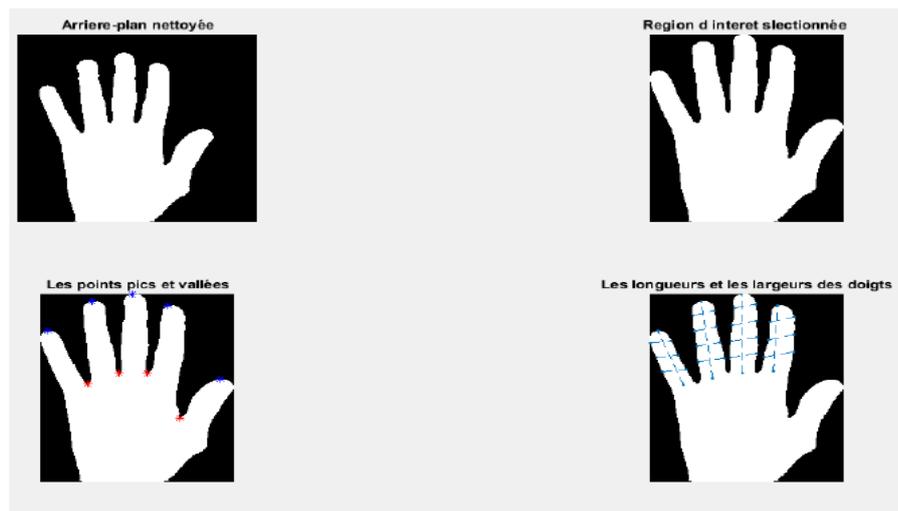
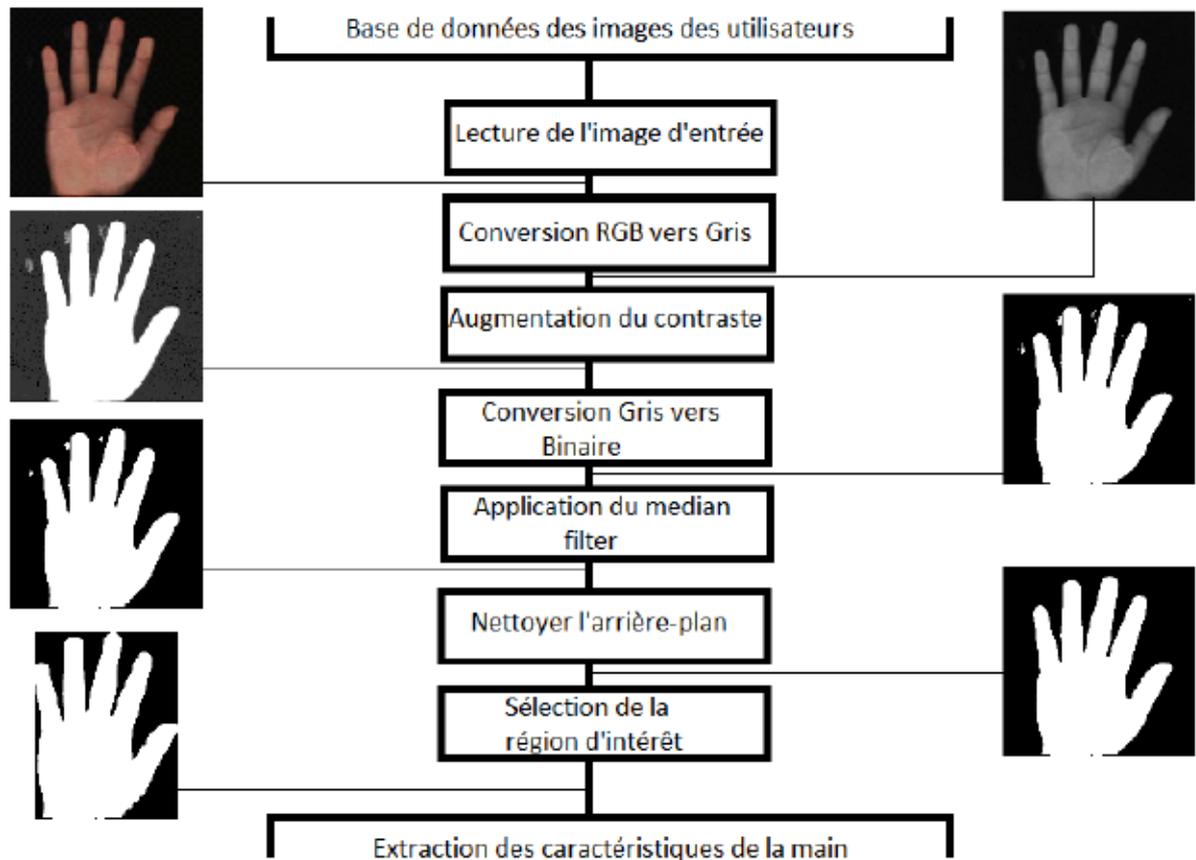
Une fois la segmentation effectuée, intervient la squelettisation. Cette étape vise à extraire la structure squelettique des objets présents dans l'image. Le squelette représente l'axe central de l'objet, réduit à une ligne fine qui capture l'essence de sa forme et de sa structure. La squelettisation permet d'obtenir une représentation simplifiée de l'objet, facilitant ainsi son analyse ultérieure.

Enfin, l'extraction de points caractéristiques se base sur le squelette obtenu précédemment. Les points caractéristiques sont des points d'intérêt ou des marqueurs significatifs qui représentent des informations clés sur l'objet ou la région analysée. Ces points peuvent comprendre des extrémités, des intersections ou d'autres caractéristiques distinctives permettant de décrire de manière concise et précise les objets présents dans l'image.



Figure 3.29 Image de la main avant le pré-traitement

Schéma synoptique du processus du prétraitement.



3.4 Résultats de la biométrie de la main

3.4.1 La Géométrie de la main

Résultats des différentes méthodes de distance et de similarités utilisées pour le matching de la géométrie de la main.

1-'euclidean';

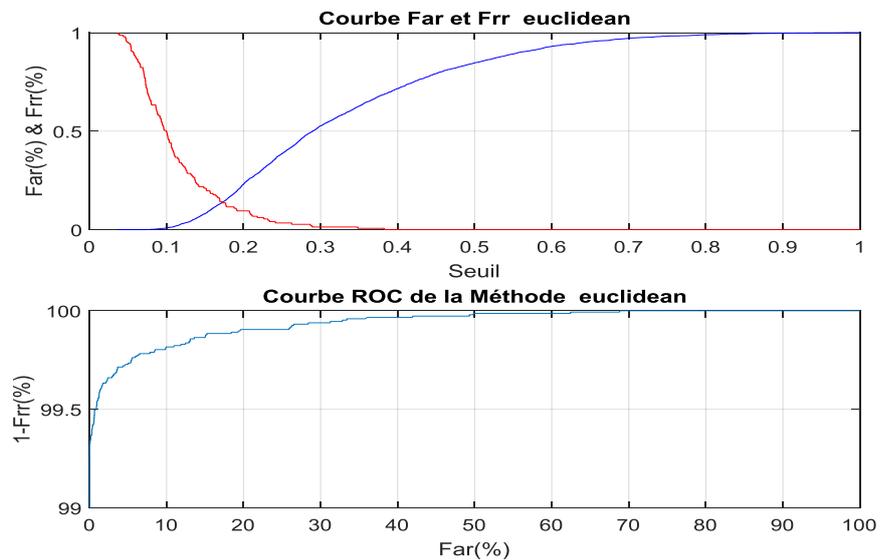


Figure 3.30 Courbe Far et Frr et Courbe ROC de la Méthode

2-'cityblock' ;

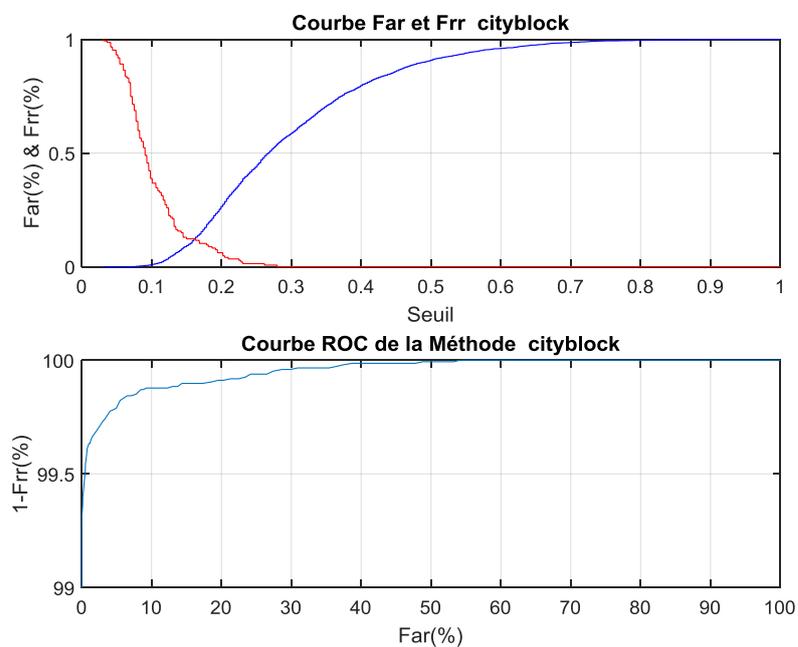


Figure 3.31 Courbe Far et Frr et Courbe ROC de la Méthode

3-'minkowski' ;

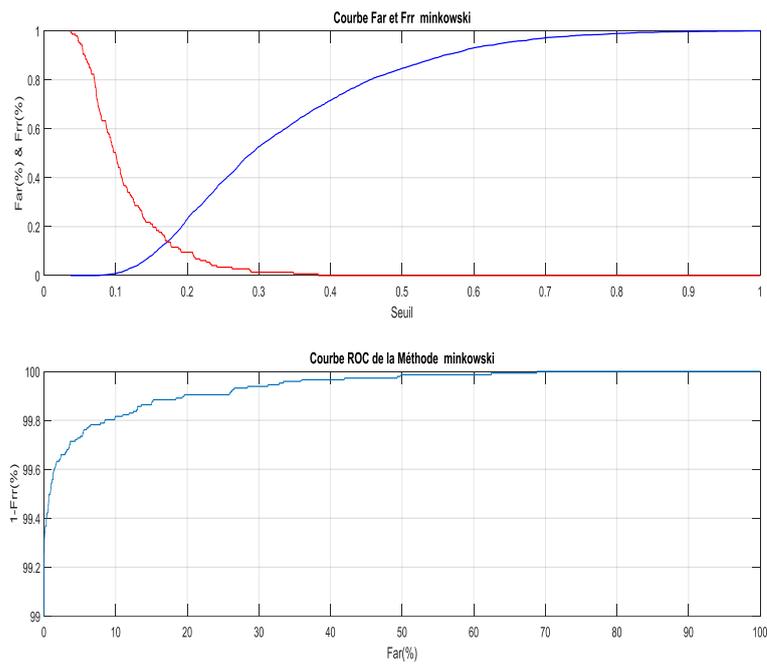


Figure 3.32 Courbe Far et Frr et Courbe ROC de la Méthode

4-'cosine' ;

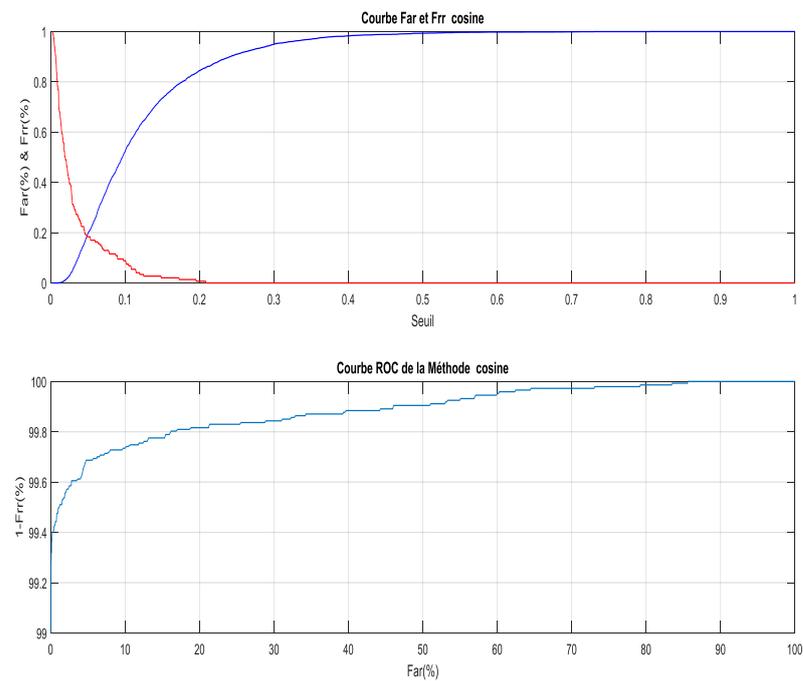


Figure 3.33 Courbe Far et Frr et Courbe ROC de la Méthode

5-'correlation';

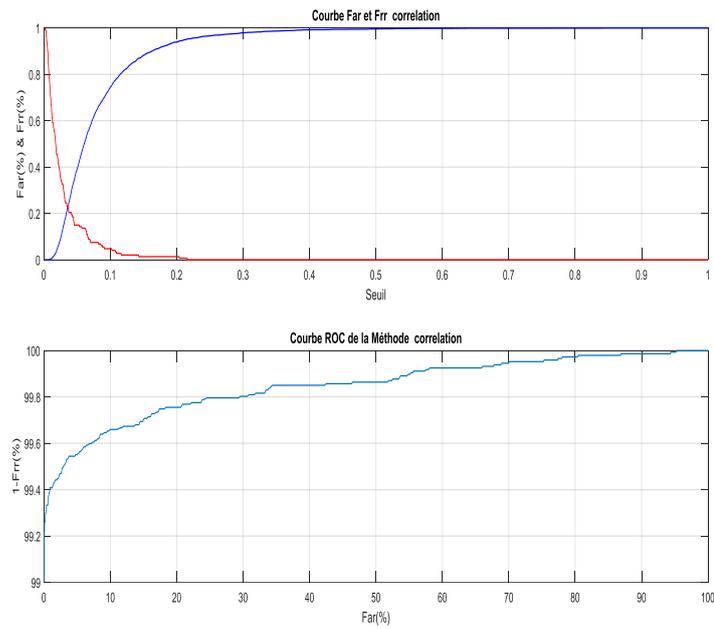


Figure 3.34 Courbe Far et Frr et Courbe ROC de la Méthode

6-'spearman' ;

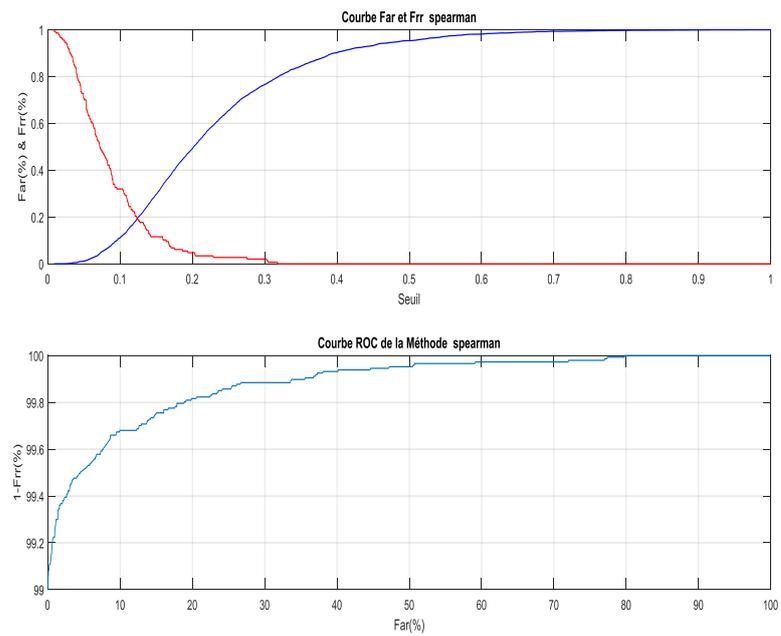


Figure 3.35 Courbe Far et Frr et Courbe ROC de la Méthode

7-'chebychev' ;

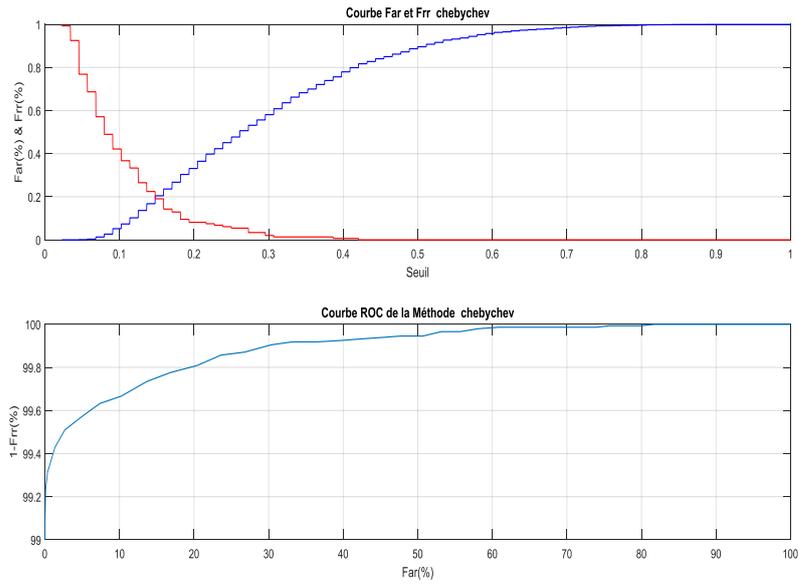


Figure 3.36 Courbe Far et Frr et Courbe ROC de la Méthode

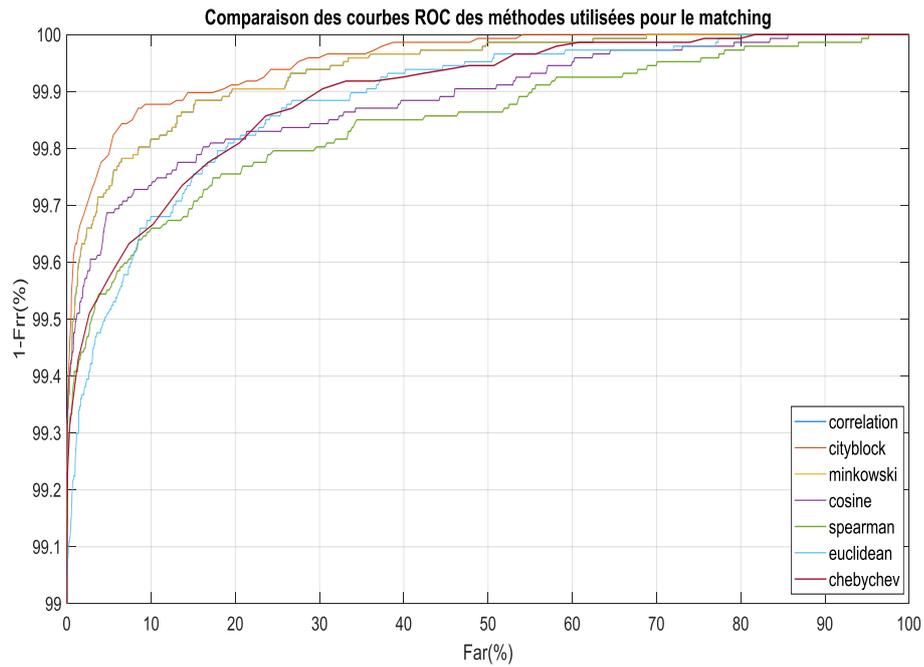


Figure 3.37 Comparaison des différentes courbes ROC des méthodes utilisées pour le matching

Tableau 3.1 comparatif des EER des différentes méthodes

Méthodes utilisées	euclidean	cityblock	minkowski	cosine	correlation	spearman	chebychev
Valeurs du EER	0.1361	0.1226	0.1361	0.1884	0.2241	0.1909	0.1976

Remarque

En analysant les données présentées dans le Tableau 3.1 et les courbes illustrées dans les Figures 3.30 à 3.37, il est observé que les méthodes Cityblock, Euclidean et Minkowski affichent une EER (Equal Error Rate) plus faible que les autres méthodes. De plus, la Figure 3.37 démontre que la courbe correspondant à la méthode Cityblock se rapproche le plus de l'angle supérieur gauche (Frr), ce qui en fait la méthode la plus performante pour le matching de la géométrie de la main

Résultat

La méthode de similarité la plus efficace pour la géométrie de la main est Cityblock, présentant un EER (Equal Error Rate) de 0.1226.

3.4.2 La texture de la paume de la main

Résultats des différentes méthodes de distance et de similarités utilisées pour le matching de la texture de la paume de la main.

1-'euclidean';

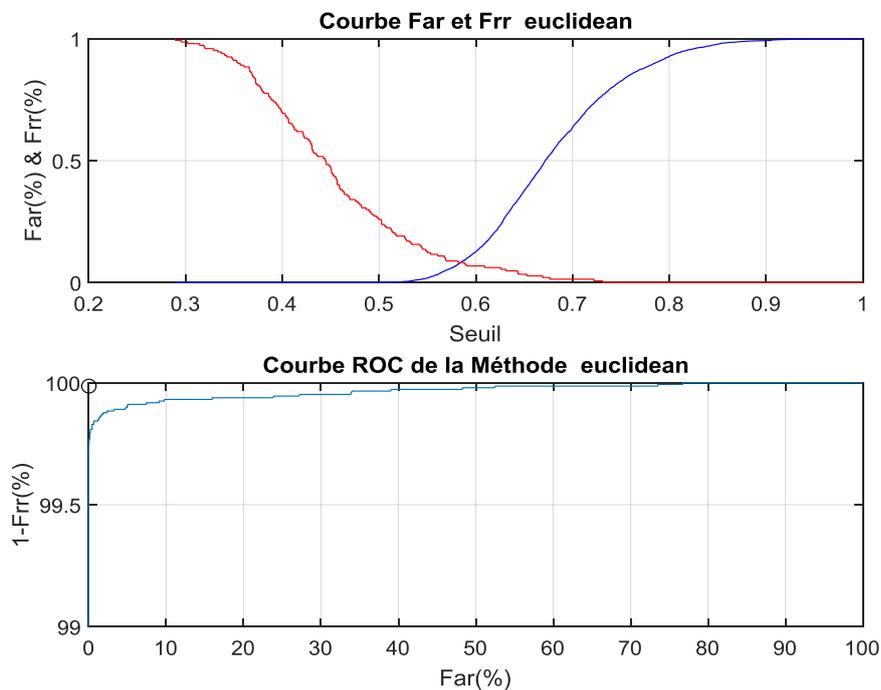


Figure 3.38 Courbe Far et Frr et Courbe ROC de la Méthode

2-'cityblock' ;

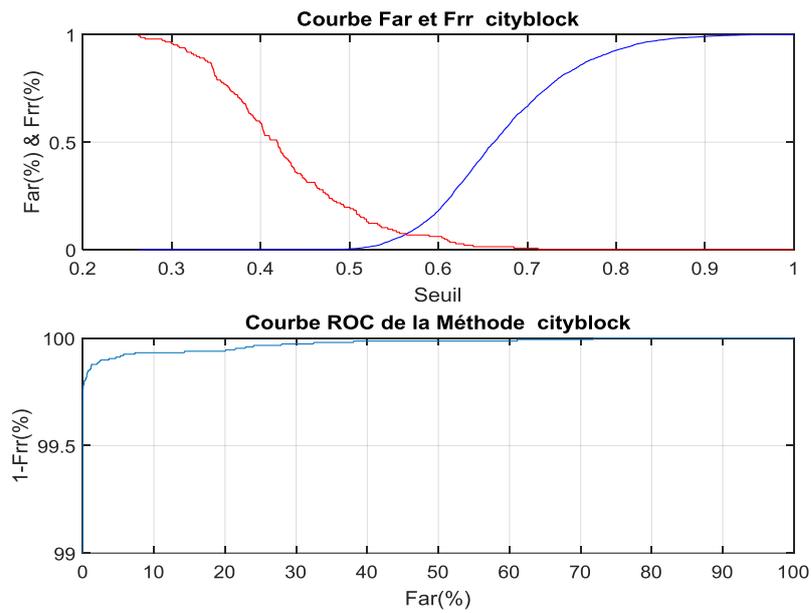


Figure 3.39 Courbe Far et Frr et Courbe ROC de la Méthode

3-'minkowski' ;

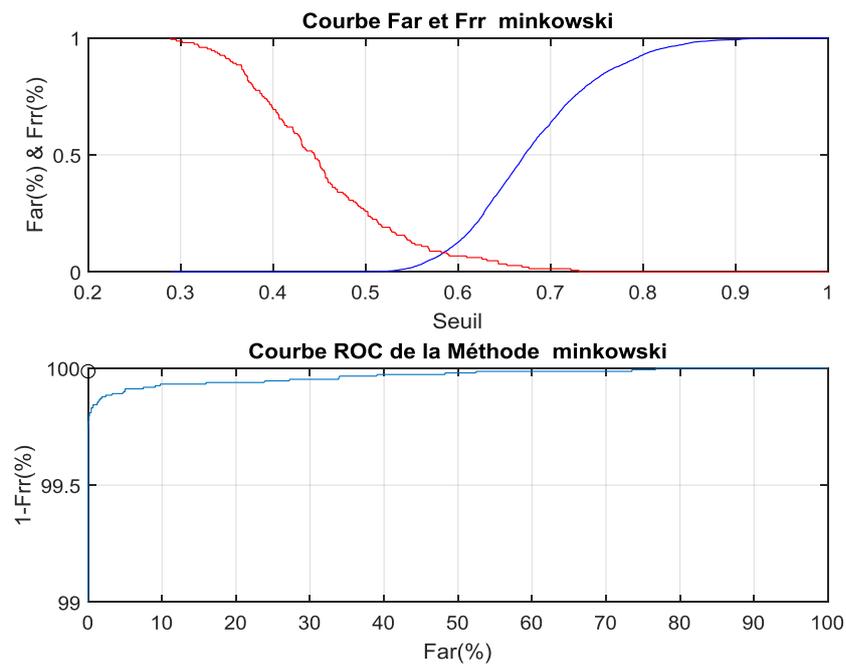


Figure 3.40 Courbe Far et Frr et Courbe ROC de la Méthode

4-'cosine' ;

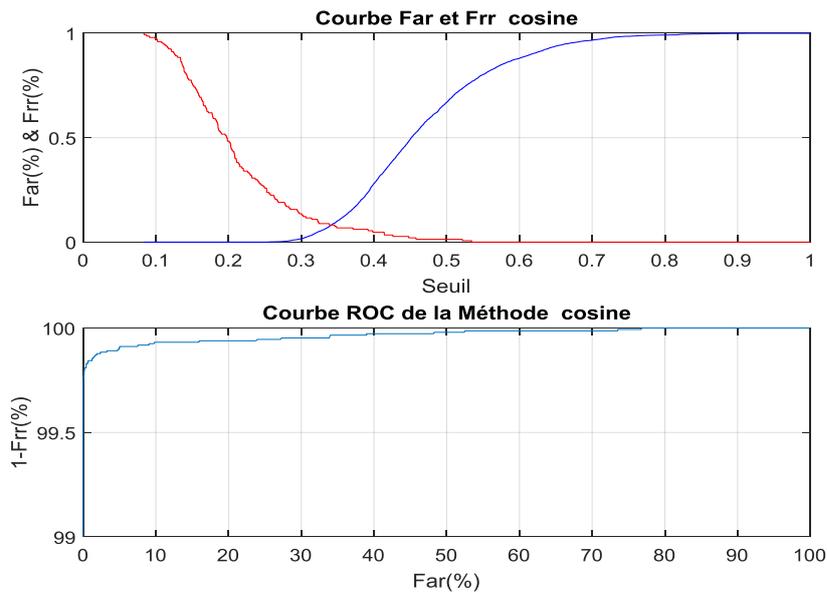


Figure 3.41 Courbe Far et Frr et Courbe ROC de la Méthode

5-'correlation';

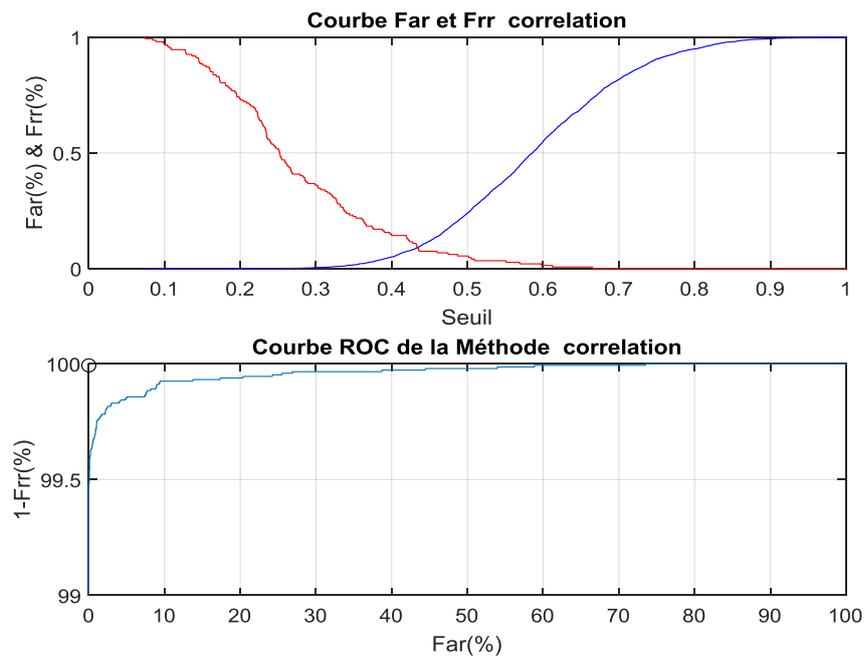


Figure 3.42 Courbe Far et Frr et Courbe ROC de la Méthode

6-'spearman' ;

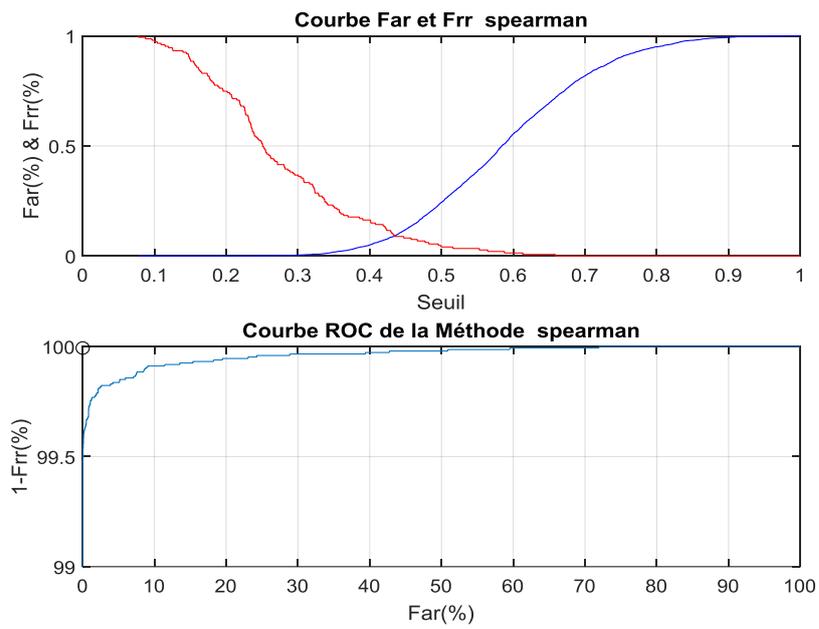


Figure 3.43 Courbe Far et Frr et Courbe ROC de la Méthode

7-'chebychev' ;

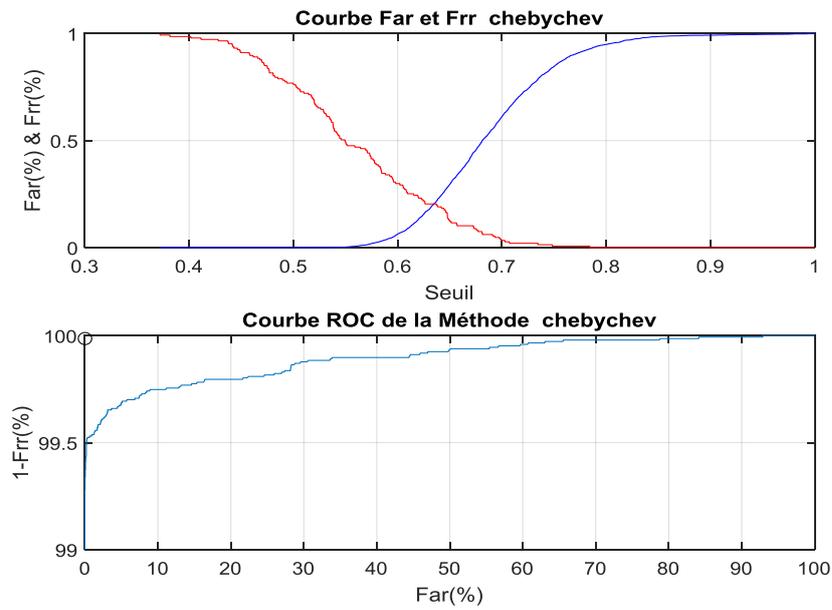


Figure 3.44 Courbe Far et Frr et Courbe ROC de la Méthode

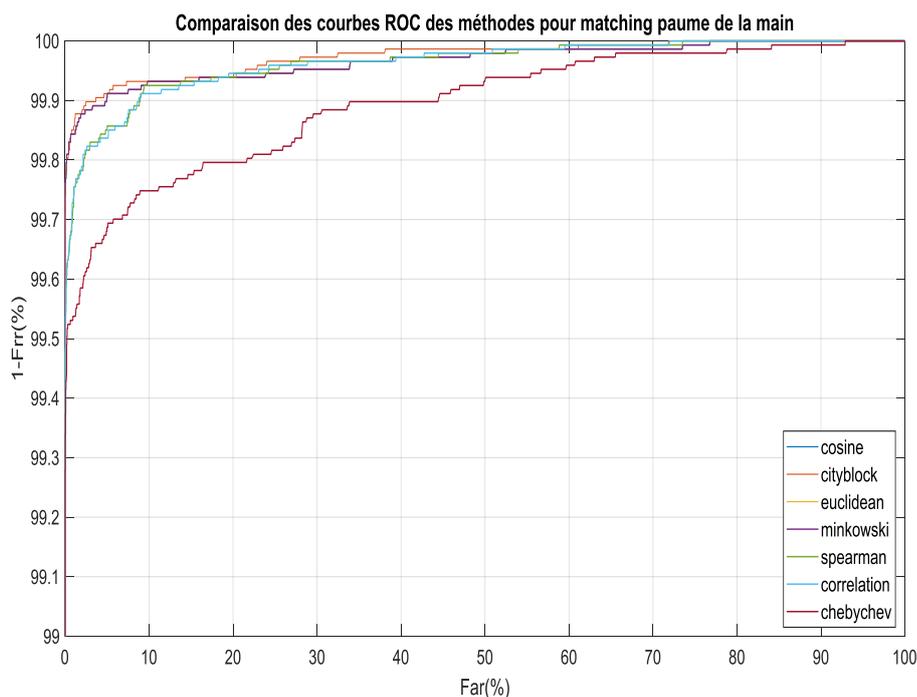


Figure 3.45 Comparaison des différentes courbes ROC

Tableau 3.2 comparatif des EER des différentes méthodes

Méthodes utilisées	euclidean	cityblock	minkowski	cosine	correlation	spearman	chebychev
Valeurs du EER	0.0815	0.0740	0.0815	0.0815	0.0891	0.0896	0.2042

Remarque

Après examen des données présentées dans le Tableau 3.2 et des courbes illustrées dans les Figures 3.38 à 3.45, il est constaté que les méthodes Cityblock, Euclidean, Cosine et Minkowski affichent une EER (Equal Error Rate) plus faible que la méthode Chebyshev. De plus, la Figure 3.45 révèle que la courbe ROC de la méthode Cityblock se rapproche de l'angle supérieur gauche, ce qui en fait la méthode la plus performante pour le matching de la texture de la paume de la main.

Résultat

Selon l'algorithme de HOG, la méthode de similarité la plus efficace pour l'empreinte palmaire est celle de Cityblock, avec un EER (Equal Error Rate) de 0.0740.

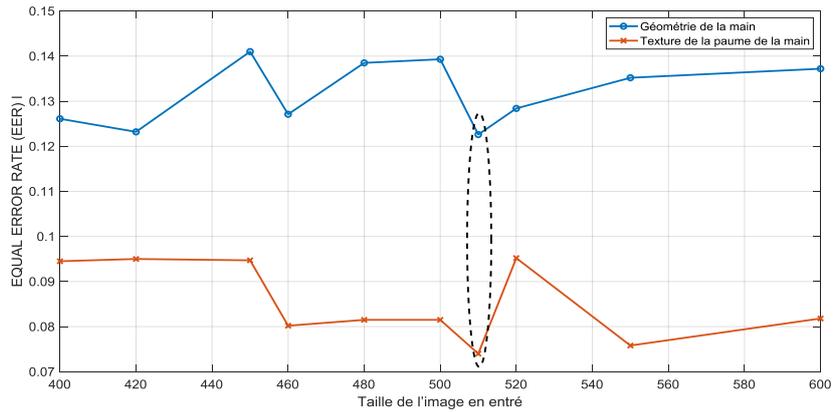


Figure 3.46 EQUAL ERROR RATE (EER) en fonction de la taille de l'image en entrée : Pour une taille du ROI de (50x50).

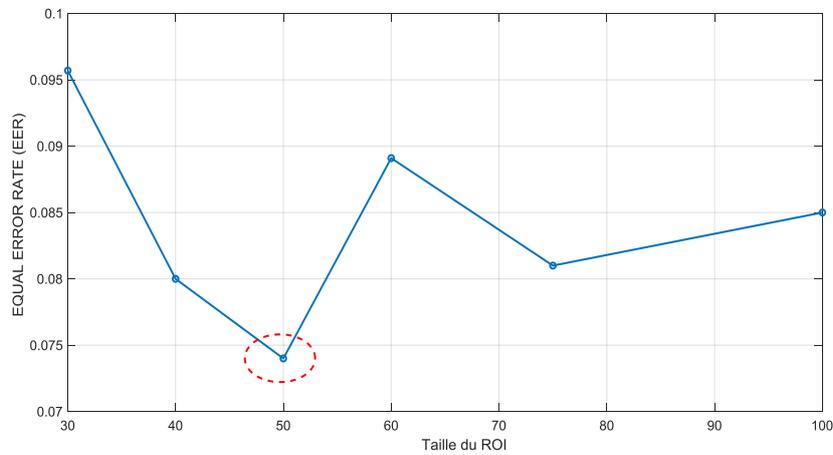


Figure 3.47 EQUAL ERROR RATE (EER) de la texture de la main en fonction de la taille du ROI pour une taille de l'image de 510.

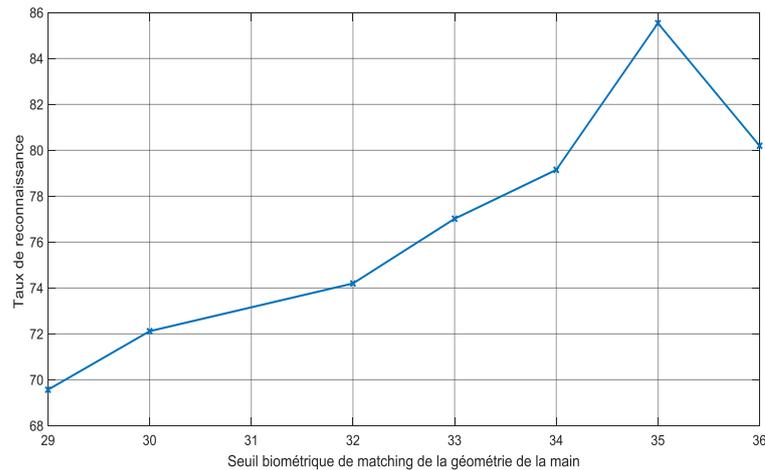


Figure 3.48 Taux de reconnaissance en fonction du seuil biométrique de matching de la géométrie de la main pour une taille de l'image de 510

Remarque :

D'après l'observation de la courbe de la Figure 3.48, le seuil biométrique optimal pour le matching de la géométrie de la main, pour une image de taille 510, est de 35.

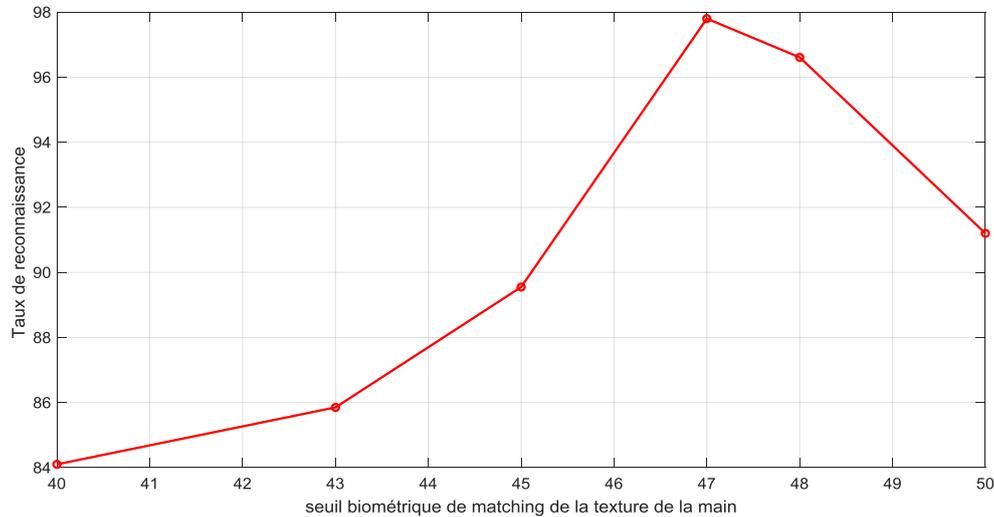


Figure 3.49 Taux de reconnaissance en fonction du seuil biométrique de matching de la texture de la paume de la main pour une taille de l'image de 510

Remarque :

D'après l'analyse de la courbe de la Figure 3.49, le seuil biométrique optimal pour le matching de la texture de la paume de la main, pour une image de taille 510, est de 47.

Résultat final

Voici une reformulation des points mentionnés :

- La méthode de similarité la plus performante pour la géométrie de la main est Cityblock, avec un EER (Equal Error Rate) de 0.1226.
- Selon l'algorithme de HOG, la méthode de similarité la plus efficace pour l'empreinte palmaire est également Cityblock, avec un EER de 0.0740.
- Lorsqu'on fusionne les scores de correspondance de la géométrie de la main et de la texture de la paume de la main, le taux de reconnaissance atteint 99.10%.

Conclusion :

Dans ce chapitre, nous avons abordé l'extraction des caractéristiques biométriques des individus, en particulier la longueur et la largeur des doigts. Nous avons conclu que la détection des points de repère est essentielle et dépend des conditions choisies lors des étapes d'acquisition et de binarisation des images. Pour mesurer la similarité entre les vecteurs caractéristiques, nous avons utilisé la distance Cityblock minimale, qui s'est avérée être une méthode de classification simple, rapide et précise, ne présentant pas de complexité majeure.

De plus, nous avons examiné les dispositifs (matériels et logiciels) utilisés dans notre étude, ainsi que les procédures d'acquisition de données et les traitements nécessaires pour obtenir les vecteurs caractéristiques. Nous avons également exploré plusieurs méthodes de traitement d'images.

Conclusion General

La réalisation de cette maquette de notre projet de fin d'études nous a permis d'explorer les différentes caractéristiques biométriques et d'évaluer leurs performances. Notre travail comprenait la conception à la fois d'une partie matérielle et d'une partie logicielle, en veillant à choisir judicieusement les dispositifs et les protocoles de communication sans fil pour assurer la transmission des données entre le kit d'acquisition et le PC serveur.

L'un des défis majeurs était de réduire l'encombrement du dispositif biométrique et d'utiliser un protocole de communication entièrement à distance. Malgré la limitation de la qualité d'image et de la résolution, nous avons obtenu de meilleurs résultats que les précédents projets de fin d'études. Tout au long de notre travail, nous avons exposé les procédures de traitement d'image et d'extraction des points caractéristiques, ainsi que les différentes méthodes de calcul de distance pour le matching. La méthode Cityblock s'est avérée être la plus performante dans notre cas.

Nous avons également démontré que la fusion des caractéristiques des deux modalités, à savoir la géométrie de la main et l'empreinte palmaire, après une réduction de la dimension du vecteur caractéristique, a considérablement amélioré les performances.

Cependant, malgré des performances biométriques satisfaisantes, notre travail reste vulnérable aux attaques frauduleuses, car une image de la main des utilisateurs pourrait être utilisée pour un accès non autorisé. En guise de perspectives pour ce travail, l'ajout d'une caméra infrarouge pour acquérir une nouvelle modalité biométrique, telle que le réseau veineux de la main, nous permettra d'améliorer la sécurité de notre dispositif biométrique à l'avenir.

Annexe

Etude économique et cout du prototype Startup et BMC

Introduction

Le Business Model Canvas (BMC) est largement adopté par les acteurs de l'entrepreneuriat tels que les incubateurs, les sociétés de capital-risque et les chambres de commerce et d'industrie. Il est considéré comme l'un des outils les plus utilisés par les start-ups. Développé par Alexander Osterwalder, le BMC permet de représenter de manière simple le modèle économique d'une entreprise. Il est particulièrement adapté à la phase de création, ainsi qu'au lancement de nouveaux produits ou services. Le BMC se compose de neuf composantes (les termes peuvent varier, mais le concept reste le même).

En utilisant le BMC, on peut obtenir des indications sur le financement de l'entreprise, sa proposition de valeur, son segment de clientèle cible ainsi que sa structure de coûts. Cet outil permet de cartographier les éléments clés d'un projet de start-up. Il est utile non seulement pour les start-ups en général, mais aussi pour les start-ups deeptech. Cependant, il doit être adapté pour être efficace. En effet, une start-up deeptech n'est pas une start-up ordinaire. Bien que le BMC soit globalement complet, l'un de ses défauts réside dans son application trop générale, sans distinction entre une start-up classique et une start-up deeptech. Chaque projet étant unique, les problèmes auxquels ils font face peuvent différer. Par conséquent, il est essentiel d'adapter le BMC à chaque cas spécifique [41].

L'avenir étant intrinsèquement incertain, il est risqué de fonder une vision à long terme sur une perception du présent. Les opportunités ne se concrétisent souvent que plusieurs années plus tard, et un phénomène appelé "exaptation" peut se produire (lorsqu'une capacité ou une caractéristique est détournée de sa fonction d'origine). Un exemple de cela est l'utilisation des couvertures de survie.

4.1 Business Model Canvas

Key Partners	Key Activities	Value Propositions	Customer Relationships	Customer Segments
<ul style="list-style-type: none"> - Fournisseur des composants électroniques. - Fournisseur de produit pour le boitement et structure du produit. - Fournisseur d'emballage. 	<ul style="list-style-type: none"> - Acquisition et achat de matières nécessaires - Montage de produit. - Emballage. - Installation -Maintenance et service après-vente. 	<ul style="list-style-type: none"> -Ce produit donne une utilisation facile au large public avec une matrise et de bon résultat. -Eviter le risque de la perte des clés. -Le produit est utilisable même dans le cas d'effacement de l'empreinte . -Le produit évite le risque de contamination lors de l'interconnexion humaine. -Le produit sert aussi come un système de pointage. 	<ul style="list-style-type: none"> - Service après vente (maintenance) - La mise à jour en cas ou. - Promotion - Variété du methode du paiments -Installation et livraison. - Essaie et garantie de produit. - La livraison disponible par un bon de commande. 	<ul style="list-style-type: none"> -Sociétés privés. -Sociétés étatiques. -Individus. -Commerçants. - Les banques.
	<p>Key Resources</p> <ul style="list-style-type: none"> -Ressources financières : (fonds de roulement) -Ressources matériels : (Composants, forex). -Ressources humaines : (programmeur, montage). 		<p>Channels</p> <ul style="list-style-type: none"> -Le produit est mediatisé à travers les diverses réseaux sociaux. - Le produit sera vendu aussi par les magasins de fournitures de bureaux. -le produit est vendu dans les magasins de matériels informatique. 	
	<p>Cost Structure</p> <ul style="list-style-type: none"> -charges d'investissement(équipement informatiques, outillagepour le montage) -Effectifs et employés, matières et composants et emballage. -Factures et charge (location de locale, énergie électrique, téléphone et internet...etc). 		<p>Revenue Streams</p> <ul style="list-style-type: none"> -Revenues des ventes. -Maintenance après la période garantie. 	

4.2 Coût Prototype

Matériels	Pris
Raspberry pi 3	25000 DA
Camera	5000 DA
Ultrason	450 DA
Clavier 3x4	300 DA
LCD afficheur 16x4	1600 DA
Spot éclairage	500 DA
Boitier forex	3000 DA
Total	35850 DA

4.3 L'annexe BMC

Fiche technique du projet

البطاقة التقنية للمشروع

Bendaouadji sadek elamine Benaissa abd eldjallel	الاسم واللقب Votre prénom et nom Your first and last Name
Système de verrouillage biométrique	الاسم التجاري للمشروع Intitulé de votre projet Title of your Project
0793470480 0799981511	رقم الهاتف Votre numéro de téléphone Your phone number
bendaouadjis@gmail.com benaissadjilali10@gmail.com	البريد الالكتروني Votre adresse e-mail Your email address
Mostaganem	مقر مزاولة النشاط (الولاية- البلدية) Votre ville ou commune d'activité Your city or municipality of activity

Nature de projet طبيعة المشروع

Vente de marchandises

المشكلة المراد حلها وتكون مدعمة بالبيانات (إحصائيات إن وجدت)



1- Value proposition:

1- القيمة المقترحة:

ما القيمة التي نقدمها للزبون؟

كيف نساعد الزبون على حل مشكلاته؟ (البحث عن حل وتحويله إلى نموذج تجاري)

ما طبيعة هذا الحل للمشكلة هل هي قيم نوعية أو كمية؟ (اختر من الرسم ما يوافق مشروعك)



1/1- القيمة التي نقدمها للعميل:

Ce produit apporte un plus-value dans la perspective d'améliorer la sécurité professionnelle matérielle et humaine.

Ce produit donne une utilisation facile au large public avec une maîtrise facile et de bon résultat.

Afin de préserver et sécuriser la santé public, le produit barre la voie pour toute contamination lors interconnexion humaine.

2/1- ما هي المشاريع الأخرى التي استهدفت نفس المشكلة والتي جرى تنفيذها؟

- Code pin ou clés : on peut toujours oublier nos clés ou bien nos mot de passe, dans ce cas notre système à régler ce problème car la main est toujours présente avec nous.

- Empreinte digitale : l'empreinte digitale risque facilement d'être endommagée par exemple :

Les personnes qui travaillent avec les produits chimiques risquent d'endommager leurs empreintes facilement.

Les personnes qui bricolent dans les ateliers peuvent endommager leurs empreintes.

L'empreinte digitale facilite la contamination des bactéries.

Notre système éviter toutes les contraintes précédent ainsi il réduit la contamination des bactéries.

2- Customer segments:



2- شرائح العملاء

- من أهم عملائنا؟ لمن نوجه القيمة؟ (حدد بالتفصيل)

نحاول تحديد عدد العملاء من خلال استبيان أو سير آراء إن وجد. بهدف تحديد السوق المحتمل. أو كيف العمل

لتحديد سوق مستهدف.

1. Les Sociétés privés et étatiques: tout les sociétés qui peuvent se bénéficier de l'utilité de la sécurité.

Les sociétés qui utilise le système de pointage.

2. Individus.

3. Commerçants: pour sécuriser le stock par exemple.

4. Les banques.

5. Laboratories

3- Customer Relationships



3- العلاقات مع العملاء:

كيف تجذب انتباه العملاء إلى منتجاتك أو خدماتك؟

كيف تشجع العميل لشراء منتجك أو خدمتك؟

كيف يستفيد العميل من منتجك أو خدمتك؟

ما هي الطرق المستعملة لخدمة ما بعد بيع منتجك أو خدمتك؟

Le contact et la relation entre les clients se faite avec le numéro du tel ou la boite email.

Le client profite aussi d'une page sur les réseaux sociaux pour commenter et donner son avis pour améliorer le système pour atteindre les besoins du client. Une garantie offerte du 6 mois après l'achat du produit.

Service de la maintenance.

Pour les clients important et potentiels prévoir le déplacement at home et prise en charge sur cite.

4- Channels :



4- القنوات:

كيف يعلم الجمهور بوجودنا أو منتوجنا أو خدمتنا؟
ما هي قنوات التوزيع التي يفضلها العملاء للتواصل معهم؟
ما هي القنوات الأكثر فعالية مقارنة مع تكلفتها

1/4- الآليات والطرق لإعلام بمنتوجنا أو خدمتنا:

- Le produit est mediatisé les diverses réseaux sociaux comme (Facebook,Instagram...)
- qui permet l'achat en ligne.
- Le produit se trouve aussi dans le secteur de fournitures de bureaux.
- Essaie et garantie de produit.
- La livraison disponible par un bon de commande.

2/4- قنوات التوزيع التي يفضلها العملاء:

Les réseaux sociaux

5- Key Partner:



5- الشركات الرئيسية:

- من هم الشركاء الرئيسيون الذين يمكن مساعدتنا في الانتاج أو الخدمة أو في تسويقها أو توزيعها؟ (الشركاء الذين أضع معهم عقد).
- من هم الموردون الرئيسيين؟ (الذين يقدمون لنا: المواد الأولية + الآلات للإنتاج + برنامج لتقديم خدمة + ...)
- قم بكتابة قائمة الشركاء الرئيسيين لمشروعك بالتفصيل مع ذكر الإسم، الهاتف، العنوان... إلخ

1/5- الشركاء الرئيسيون الذين يمكن مساعدتنا:

Service de livraison :

Nom : YALIDINE courrier express.

Numéro de tel : +213 770587106

Adresse : Salamandre en face la daïra

2/5-الموردين الرئيسيين:

- Fournisseur des composent électroniques :

Nom : dzduino

Numéro de tel : +213 (0) 550 323 025.

Adresse : 043 Cite Remila (Route du Port), Tigditt - Mostaganem

Site web : <https://www.dzduino.com/>

- Fournisseur de produit forex :

Nom : HDT pub

Numéro de tel : 05.61.49.36.82

Email : hdtpub27000@gmail.com

Site web : hdtpub

Adresse :

- Fournisseur d'emballage

6- Key activities:



6- الأنشطة الرئيسية:

ما هي أهم المراحل الرئيسية للإنتاج أو الخدمة؟ (نذكر المراحل من اقتناء المواد الأولية إلى المنتج النهائي)
هل هناك أنشطة ثانوية؟ (نذكر الأنشطة الثانوية التي تدخل في منتجنا أو خدمتنا)

1/6-المراحل الرئيسية:

1. Acquisition et achat de matière naicessaire à l'élaboration de produit.
2. Programmation de la carte.
3. Assemblage et montage des composants.
4. Emballage.
5. Maintenance et service après-vente

2/6-الأنشطة الثانوية

1. Emballage.
2. Maintenance et service après-vente
3. Service de livraison

7- Key Resources



7- الموارد الرئيسية:

نقوم بتحديد فقط الموارد دون ذكر التكلفة.

1/7- الموارد المادية:

الموردfournisseur	مصدر محلي أو أجنبي	المواردRessources
<ul style="list-style-type: none"> - DZduino - Fournisseur forex 	<ul style="list-style-type: none"> - National 	Composants électroniques : <ul style="list-style-type: none"> - Raspberry pi 3 B+ - Capteur ultrason - Afficheur LCD - Clavier 3x4 - Lampe Produit de coffrage : <ul style="list-style-type: none"> - Forex.

2/7-الموارد البشرية:

Pour les ressources humaines on a besoin d'un :

- Programmeur qui fait la partie software du prototype et tous ce qui est programmation.
- Un assembleur qui fait le montage et l'installation des composants électroniques.

العدد	صنف المورد البشري
1	Programmeur
1	Assembleur

3/7- الموارد المالية:

الاحتياج	المورد المالي
électricité	الكهرباء والغاز والماء
Petit atelier	كراء

	عناصر أخرى

8- Cost Structure



8- هيكل التكاليف:

■ 1/8: هيكل التكاليف structure Costs

/	تكاليف التعريف بالمنتج أو المؤسسة Frais d'établissement
/	تكاليف الحصول على العدادات (الماء- الكهرباء) Frais d'ouverture de compteurs (eaux-gaz-....)
/	تكاليف (التكوين- برامج الاعلام الالي المختصة) Logiciels, formations
/	Dépôt marque, brevet, modèle تكاليف براءة الاختراع و الحماية الصناعية و التجارية
/	Droits d'entrée تكاليف الحصول على تكنولوجيا او ترخيص استعمالها
/	Achat fonds de commerce ou parts شراء الأصول التجارية أو الأسهم
Louer un locale 20000 da par mois	Droit au bail الحق في الإيجار
/	
/	Frais de dossier رسوم ايداع الملفات
/	Frais de notaire ou d'avocat تكاليف الموثق-المحامي-.....
/	Enseigne et éléments de communication تكاليف التعريف بالعلامة و تكاليف قنوات الاتصال
/	Achat immobilier شراء العقارات
/	Travaux et aménagements الأعمال والتحسينات الاماكن
PC pour programmation : 70000 Da Outils : faire a soudure 1200 Da Visseuse 5000 Da	Matériel الألات- المركبات- الاجهزة
/	Matériel de bureau تجهيزات المكتب
/	Stock de matières et produits تكاليف التخزين
2000000 Da	trésorerie de départ التدفق النقدي (الصندوق) الذي تحتاجه في بداية المشروع.

المجموع = 2096200 Da

2/8 - نفقاتك أو التكاليف الثابتة الخاصة بمشروعك

/	Assurances التأمينات
2200da par mois	Téléphone, internet الهاتف و الانترنت
/	Autres abonnements اشتراكات أخرى
/	Carburant, transports الوقود و تكاليف النقل
/	Frais de déplacement et hébergement تكاليف التنقل و المبيت
Facture électricité :3000 da par trimestre	Eau, électricité, gaz فواتير الماء - الكهرباء- الغاز
/	Mutuelle التعاضدية الاجتماعية
35850 Da pour chaque prototype	Fournitures diverses لوازم متنوعة
/	Entretien matériel et vêtements صيانة المعدات والملابس
/	Nettoyage des locaux تنظيف المباني
/	Budget publicité et communication ميزانية الإعلان والاتصالات

المجموع = 41050 Da

3/8 - رواتب الموظفين و مسؤولين الشركة

/	رواتب الموظفين Salaires employés
	صافي أجور المسؤولين Rémunération nette dirigeant

9- Revenue Streams



9- مصادر الإيرادات

1/9-الإيرادات الاجمالية:

البيان	القيمة
عدد الوحدات المنتجة	1
سعر البيع	65000 Da
سعر البيع × عدد الوحدات المنتجة = الإيرادات الاجمالية	65000 Da

2/9-مصادر الدخل:

- Revenue de vente.
- Maintenance après garantie.

3/9-النسبة المئوية للزيادة في حجم الأعمال بين كل شهر لسنة الأولى؟ ثم لسنة الثانية؟

Conclusion :

L'adaptation du Business Model Canvas (BMC) permet aux start-ups deeptech de mieux appréhender leur environnement et de faire preuve d'agilité. Le BMC peut être utilisé lors de levées de fonds et de recherches de partenaires, offrant une vision claire et flexible. Il favorise également les synergies positives, en s'alignant sur les stratégies des investisseurs ou des grandes entreprises, et en anticipant les modes de transfert de technologies. Cette approche démontre une réelle action stratégique. Il est important de souligner que cette proposition d'adaptation ne doit pas être figée, mais plutôt évoluer selon les besoins spécifiques des entreprises. L'objectif principal est de faire progresser les start-ups deeptech, sans les enfermer dans des contraintes ou des généralisations abusives.

Références Bibliographiques

- [1] D. R. Lease, R. Guess, S. Lovaas, E. Solveggio. *Biometric Authentication*. In S. Bosworth and M. E. Kabay (Ed.), *Computer Security Handbook (Chapter 29)*, 4th Edition, John Wiley, New Jersey, 2009. 2
- [2] A. K. Jain, P. Flynn, A. Ross. *Handbook of Biometrics*. Springer, 2007. 2, 9
- [3] A. K. Jain, R. Bolle, S. Pankanti, editors. *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Publishers, 1999. 3
- [4] Acuity Market Intelligence. *The Future of Biometrics - Market Analysis, Segmentation & Forecasts, Insight into the Trends, Drivers & Opportunities that will Shape the Industry through 2020*. Rapport technique. Août 2009. 3
- [5] A. Martin, G. Doddington, T. Kamm, M. Ordowski, M. Przybocki. *The DET Curve in Assessment of Detection Task Performance*. In Proc. Eurospeech'97, 1895–1898, Rhodes, 1997. 12
- [6] A.K. Jain, A. Ross, S. Parabakar. *An Introduction to Biometric Recognition*. IEEE Trans. on Circuits and Systems for Video Technology, 14(1), Janvier 2004. 4, 13, 16
- [7] L. Allano. *La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles*. Mémoire de doctorat, Université d'Evry Val d'Essonne, Institut National des Télécommunications, 2009. 14, 165, 171, 189
- [8] C.L. Tissé. *Contribution à la vérification biométrique de personnes par reconnaissance de l'iris*. Mémoire de doctorat, Université de MontpellierII, 2003, France. 15
- [9] J. Fierrez-Aguilar. *Adapted Fusion Schemes for Multimodal Biometric Authentication*. Mémoire de thèse. Université Polytechnique de Madrid, 2006. 16, 17, 204
- [10] A.K. Jain, K. Nandakumar, A. Ross. 2005. *Score Normalization in Multimodal Biometric Systems*. Pattern Recognition, 38: 2270-2285. 18, 19, 21, 22, 23, 25, 169, 172
- [11] A. Ross, K. Nandakumar, A. K. Jain. *Handbook of Multibiometrics*. Springer, 2006.
- [12] J. Kittler, M. Hatef, R.P. Duin, J.G. Matas. *On combining classifiers*. IEEE Trans. PAMI, 20(3): 226–239, 1998. 20, 172
- [13] Y. Wang, T. Tan, A. Jain. *Combining face and iris biometrics for identity verification*. Proc. of 4th Int. Conf. on Audio and Video-Based Authentication – AVBPA, 805-813, Guildford, Juin 2003. 20, 21, 161
- [14] A.K. Jain, A. Ross. *Learning user-specific parameters in a multibiometric system*. Proceedings of Int. Conf. on Image Processing, 57–60, New York, 2002. 22, 204
- [15] W. Ben Soltana, D. Huang, M. Ardabilian, L. Chen, B.C Ben Amar. *Comparison of 2D/3D Features and Their Adaptive Score Level Fusion for 3D Face Recognition*. 3D Data Processing, Visualization and Transmission - 3DPVT, Paris, France. 2010. 22

- [16] A. Ross, A. K. Jain. *Information Fusion in Biometrics*. Pattern Recognition Letters, Special Issue on Multimodal Biometrics, 24(13): 2115-2125, Septembre 2003. 20, 22, 172
- [17] P. Huber. *Robust Statistics*. JohnWiley & Sons, 1981. 22
- [18] F. Hampel, P. Rousseeuw, E. Ronchetti, W. Stahel. *Robust Statistics : The Approach Based on Influence Functions*. John Wiley & Sons, 1986. 24
- [19] <https://www.biometrie-online.net/technologies/volume-de-la-main>
- [20] <https://www.abiova.fr/biometrie.html>
- [21] <http://www.thierryaimard.fr/anatomie-main.php>
- [22] http://biometrics.over-blog.com/pages/La_geometrie_de_la_main-2019729.html
- [23] Nesrine Charfi , l'Université Bretagne Loire , MÉMOIRE / IMT Atlantique le 23 janvier 2017
- [24] https://dspace.univguelma.dz/jspui/bitstream/123456789/10255/1/ZOUIED_NESREDDINE_Electronique.._Instrumentation.pdf
- [25] <https://www.zdnet.fr/actualites/biometrie-les-veines-de-la-main-comme-nouveau-point-de-reference-39241932.htm>
- [26] <https://www.techniques-ingenieur.fr/actualite/wp-content/uploads/2015/11/biowatch-2.jpg>
- [27] Rowe RK, Uludag U, Demirkus M, Parthasaradhi S, Jain AK (2007) A multispectral whole-hand biometric authentication system. In: Proceedings of biometric symposium. biometric consortium conference. Baltimore, September
- [29] <https://www.biometrie-online.net/technologies/reseau-veineux>
- [30] https://fr.wikipedia.org/wiki/Raspberry_Pi
- [31] <https://www.gotronic.fr/pj2-hc-sr04-utilisation-avec-picaxe-1343.pdf>
- [32] <https://pecquery.wixsite.com/arduino-passion/le-clavier>
- [33] <https://pijaeducation.com/arduino/keypad/keypad-with-arduino-without-using-keypad-library/>
- [34] <https://www.winstar.com.tw/fr/products/character-lcd-display-module/lcd-16x4.html>
- [35] <https://fr.wikipedia.org/wiki/Modem>
- [36] <https://www.raspberrypi-france.fr/guide/systeme-exploitation-raspberry-pi/>
- [37] <https://alexandre-laurent.developpez.com/articles/hardware/raspberry-pi>
- [38] https://www.hec.ca/cams/ateliers/Intro_Matlab.pdf
- [39] <https://www.techno-science.net/glossaire-definition/Traitement-d-images.html>
- [40] <http://fmi.univ-tiaret.dz/images/1GI/2020/S2/TAI/TAI COURS GI 2019 2020.pdf>
- [41] <https://eldorado.co/blog/2020/10/28/pourquoi-faut-il-adapter-le-business-model-canvas-aux-startups-deeptech>

الملخص

التحليل الحيوي لليد هو طريقة للاعتراف بالأفراد وتحديد همت بناءً على الخصائص الفريدة ليديهم. في هذا العمل، يعتمد على تحليل بصمات الكف وملامح اليد ونسبها. تُستخدم هذه التكنولوجيا على نطاق واسع في أنظمة الأمان والتحكم في الوصول، مثل مساحات بصمات الأصابع والأقفال الحيوية. في حالتنا، فإنها لا تعمل فقط كحل حيوي غير ملامس، ولكنها توفر أيضًا مستوى عالٍ من الدقة والموثوقية، حيث تعتبر ملامح اليد فريدة لكل فرد. علاوة على ذلك، فإنها غير غازية وسهلة الاستخدام.

RESUME

La biométrie de la main est une méthode de reconnaissance et d'identification des individus basée sur les caractéristiques uniques de leur main. Dans ce travail elle repose sur l'analyse des empreintes palmaires, et des contours et des proportions de la main. Cette technologie est largement utilisée dans les systèmes de sécurité et de contrôle d'accès, tels que les scanners d'empreintes digitales et les serrures biométriques. Dans notre cas en plus d'être une solution biométrique sans contact elle offre un niveau élevé de précision et de fiabilité, car les caractéristiques de la main sont uniques à chaque individu. De plus, elle est non invasive et facile à utiliser.

ABSTRACT

Hand biometrics is a method of recognizing and identifying individuals based on the unique characteristics of their hand. In this work, it relies on the analysis of palm prints, as well as hand contours and proportions. This technology is widely used in security systems and access control, such as fingerprint scanners and biometric locks. In our case, it not only serves as a contactless biometric solution but also offers a high level of accuracy and reliability, as hand features are unique to each individual. Furthermore, it is non-invasive and easy to use.

Mots clés :

Sécurité , Biométrie , Verrouillage , Géométrie de la main , sans contact , Empreint palmaire , La paume de la main.