REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de **T**echnologie

Département **I**ngénierie des **S**ystèmes **E**lectriques

Mémoire de Master

Présenté par

M^r^ YAKOUBI Yazid

M^r^ OUNNOUGHI Mohammed Badereddine

Filière : Électronique

Spécialité : Electronique des **S**ystèmes **E**mbarqués

Mise en œuvre d'un système de contrôle d'accès basé sur la reconnaissance faciale et l'empreinte digitale

Soutenu le 03/07/2022 devant le jury composé de :

RAHMOUNE	Fayçal	Prof	Université de Boumerdès	Président
BELKACEM	Samia	MCA	Université de Boumerdès	Rapporteur
MOUATSI	Abdelmalek	MCA	Université de Boumerdès	Examinateur
KESSAISSIA	Karima	MAA	Université de Boumerdès	Examinateur

2021/2022

Dédicaces

A nos mères adorées

A nos pères protecteurs

A nos frères et sœurs aimés

Et nos amis attentionnés

Yazid & Mohammed Badereddine

Remerciements

Nos remerciements vont premièrement à Dieu, le seul et unique qui nous a donné la volonté, la santé, et la patience durant cette année.

La première personne que nous tenons à remercier est notre encadreur de projet de fin d'études **Dr Samia BELKACEM**, pour son orientation, sa confiance et sa patience qui ont constitué un apport considérable pour bien mener ce travail.

Nous tenons également à remercier les membres du jury : Prof. RAHMOUNE Fayçal, Dr MOUATSI Abdelmalek et Mme KESSAISSIA Karima d'avoir accordé de leurs temps pour expertiser notre travail, nous espérons qu'ils en soient satisfaits.

Nous adressons également nos remerciements à l'UNIVERSITE M'HAMED BOUGARA-BOUMERDES d'avoir fait de nos cinq années d'études une expérience enrichissante est agréable à vivre, sans oublier un hommage à notre chef de département **Mr NE. MESSAOUDI**

Nous profitons de l'occasion pour remercier toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce projet.

Et on passe un grand merci à nos familles et nos amis qui par leurs prières et leurs encouragements, et leurs soutiens surtout durant cette période de la pandémie COVID-19, nous avons pu surmonter tous les obstacles et finir le travail à distance.

Liste des abréviations

B

BYOD: bring your own device

E

EEPROM: Erasable Programmable Read-Only Memory

F

FAR : false acceptance rate

FMR : Taux de fausse correspondance (false matche rate)

FNIR : false-négative identification-errer rate

FNMR : Taux de fausse non-correspondance (false non-matche rate)

FRR : false rejection rate

FPIR : false-positive identification-errer rate

FPS/IPS: Image par second

FTE: Failure-to-enroll rate

FTDI : Future Technology Devices International

G

GPIO: General Purpose Input/Output

H

HTML: HyperText Markup Language

I

I2C: circuit inter intégré

IDE/EDI : Environnement de Développement Intégré

IR : identification rate

ISO/CEI : (Organisation internationale de normalisation/Commission électrotechnique internationale)

L

LED: light emitting diode

LCD: Liquid Crystal Display

M

Mac: man, and machine

P

PIN: Personal Identification Number

PR : Taux de pénétration

PSRAM: pseudo static (random-access) memory

PWM : Pulse Width Modulation

R

RFID: Radio Fréquence Identification

RGB: red, green, blue

RX: Receive X

S

SD: Secure Digital

SDA: Serial Data OUT

SPI: Serial Peripheral Interface

SRAM: Static Random Access Memory

T

TFA : taux de fausse acceptation

T.F.R : Pourcentage de personnes rejetées par erreur

TTL: Transistor-Transistor Logic

TX: Transmit X

U

UART: Universal Asynchronous Receiver Transmitter

USB: Universal Serial Bus

UXGA: Ultra Extended Graphics Array

V

VCC: Common Collector Voltage

W

Web: World Wide Web

Y

YUV: Y représente la luma U et V, représentent la chrominance

Table des matières

Dédicaces i
Remerciements ii
Liste des abréviations iii
Table des matières v
Liste des Figures ix
Liste des tableaux xi
Introduction générale 1
I.1 Introduction 2
I.2 Concepts de base 2
I.2.1 Principe de fonctionnement d'un système biométrique 3
I.2.2 Les techniques biométriques 3
I.2.2.1 L'analyse morphologique (physiologique) 3
I.2.2.2 L'analyse comportementale 3
I.3 Les différents systèmes biométriques 4
I.3.1 Les empreintes digitales 4
I.3.2 Le système biométrique à base de l'iris 5
I.3.3. Le système biométrique à base de la reconnaissance faciale 5
I.4 Performance d'un système biométrique 7
I.4.1 Métriques 7
I.4.2 Les mesures des taux d'erreur 7
I.5 Application des systèmes biométriques 10
I.5.1 Sécurité biométrique 12
I.5.2 Contrôle frontalier / Aéroports 12
I.5.3 Biométrie résidentielle 13
I.5.4 Biométrie financière 13
I.5.5 Empreintes digitales et verrous biométriques 13
I.5.6 Biométrie de la santé 13
I.5.7 Justice 13
I.5.8 Contrôle d'accès logique 14
I.5.9 Biométrie mobile 14
I.5.10 Temps et pointage 14

I.6 Les principales exigences d'une application biométrique 14
I.7 Les Caractéristiques biométriques 15
I.8 États de l'art sur les méthodes de télésurveillance par systèmes biométriques 17
I.9 La reconnaissance d'empreinte digitale 18
I.9.1 Description des empreintes digitales 18
I.9.2 L'étude d'une empreinte 19
I 9.3 Authentification et vérification d'empreinte 20
I.9.4 Architecture de système d'empreinte digitale 21
I.9.5 Capteur d'empreinte digitale 22
I.9.5.1 Les capteurs d'empreintes digitales macroscopiques 22
I.9.5.2 Capteurs intégrés 23
I.10 La reconnaissance faciale 23
I.10.1 Le fonctionnement 23
I.10.2 Les classes des techniques de reconnaissance de visages 24
I.10.3 Systèmes biométriques basés sur la reconnaissance de visage 25
I.10.4 Les difficultés de reconnaissance faciale 26
I.10.4.1 Problème d'éclairage 26
I.10.4.2 Problème de posture 26
I.10.4.3 Problèmes d'expression 27
I.10.4.4 Changement d'âge 27
I.10.5 La multimodalité 28
1.11 Conclusion 28
Bibliographies 30
Webographie 30
II.1 Introduction 33
II.2 Carte Arduino Uno 33
II.2.1 Description 33
II.2.2 Caractéristiques 34
II.2.3 La partie logicielle 35
II.2.4 La partie matérielle 35
II.2.5 Schéma structurel 36
II.3 La carte ESP 32cam 37
II.3.1 Description 37
II.3.2 Caractéristiques de ESP 32 cam 37
II.3.3 Fonctionnement 38

II.3.4 Brochage de la carte ESP 32 cam 38
II.4 Module de capteur d'empreintes digitales avec Arduino (FPM10A) 40
II.4.1 Spécifications techniques 41
II.4.2 Brochages 42
II.4.3 Principe d'opération 42
II.4.4 Étape de comparaison d'empreintes digitales 42
II.4.5 Installation de la bibliothèque de capteurs d'empreintes digitales Adafruit 43
II.4.6 Enregistrement d'une nouvelle empreinte digitale 43
II.4.6.1 La reconnaissance d'empreinte 45
II.5 Unité de sortie et de communication (Afficheur LCD) 46
II.5.1 Brochage d'un afficheur LCD 47
II.5.2 Principe de fonctionnement d'un écran LCD 49
II.6 PCF8574 (I2C) 49
II.7 Relais 50
II.7.1 Avantages et inconvénients d'un Relais 51
II.7.2 Principe de fonctionnement d'un Relais 52
II.8 Buzzer 53
II.9 La serrure électrique 54
II.9.1 Min serrure éélectromagnétique 54
II.10 La diode électroluminescente LED 55
II.11 Présentation de l'Espace de développement Intégré software (EDI) Arduino 55
II.11.1. Software de l'Arduino 56
II.11.2 Description de la structure d'un programme 58
II.11.2.1 Description détaillée des parties 59
II.11.3 Téléversement du programme 60
II.11.3.1 Les étapes de téléversement du programme 60
II.12 Bibliothèques utilisées 61
II.12.1 La bibliothèque ESP32 61
II.12.2 La bibliothèque Arduinowebsockets 63
II.12.3 EEPROM 64
II.13 Les configuration de la carte ESP 32 cam 64
II.14 HTML 65
II.14.1 Interface graphique avec HTML 66
II.15. Conclusion 67

Bibliographie....68
Webographie....68
III.1 Introduction....71
III.2 Partie de la reconnaissance faciale....71
III.2.1 Logiciels et langages utilisés....71
III.2.1.1 Arduino IDE....71
III.2.1.2 Navigateur web utilisé....71
III.2.1.3 HTML....71
III.2.2 Montage de connexion de la carte ESP32CAM....72
III.2.3 Création de la liste des gens autorisés....75
III.2.5 Tests de la reconnaissance facial avec la carte ESP32CAM et Arduino....75
III 2.5.1 Test des cas possibles....76
Cas 1 : la personne est enregistrée....76
Cas 2 : La personne est non enregistrée....77
III.3 Partie d'empreinte digitale....78
III.3.1 Principe de fonctionnement....79
III.3.2 Schéma bloc....81
III 3.3 Test des cas possibles....81
Cas 1 : La personne est enregistrée....81
Cas 2 : La personne est non enregistrée....82
III.4 La conception générale....83
III.4.1 Schéma bloc....83
III.4.2 Organigramme général....83
III.4.3 Comparaison....84
III.5 Réalisation....85
III.5.1 Montage sur la maquette....85
III.5.2 Les étapes du fonctionnement de notre système....86
III.5.3 Test et résultats....89
III.5.4 Avantages et inconvénients de notre système de contrôle d'accès....90
III.6. Conclusion....90
Conclusion générale....93
Résumé....95
Abstract....95
ملخص....95

Liste des Figures

Chapitre I

Figure I. 1: Le processus de reconnaissance par empreinte digitale 4
Figure I. 2 : Photos d'iris 5
Figure I. 3: Schéma synoptique d'un système de reconnaissance faciale. [1] 7
Figure I. 4: Les performances des systèmes biométrique 9
Figure I. 5 : Taux de vraisemblance des utilisateurs légitimes et des imposteurs d'un système d'authentification biométrique 10
Figure I. 6 : Exemples d'application de la biométrie : 12
Figure I. 7 : Comparaison des sélections de technologies biométriques selon les critères effort. (Anouar Ben KHALIFA,2014) 15
Figure I. 8 : Exemples de caractéristiques biométriques 16
Figure I. 9 : Image d'une empreinte digitale. [1] 18
Figure I. 10 : La figure Reconnaissance d'empreinte digitale(a)Reconnaissance par encre sur papier (b)Reconnaissance par un capteur optique 19
Figure I. 11: Delta trépied, Delta triangle fermé, Delta triangle ouverte 19
Figure I. 12 :(a) adelte, (b) monodelte, (c) bidelte 20
Figure I. 13 : Diagramme de système en haute niveau 20
Figure I. 14 : Architecture d'un système d'authentification par empreinte digitale 21
Figure I. 15 : Architecture d'un capteur macroscopique 29 22
Figure I. 16 : Principe de fonctionnement de base d'un système de reconnaissance faciale 24

Chapitre II

Figure II. 1: Les compartiments avec description de la carte Arduino Uno [3] 34
Figure II. 2: Schéma électronique structurel de l'Arduino Uno [6] 36
Figure II. 3: Image réelle d'une ESP 32 cam.[7] 37
Figure II. 4: Brochage ESP 32 cam avec une FTDI 39
Figure II. 5: Branchement structurel Arduino UNO et ESP 32 cam.[11] 40
Figure II. 6: Capteur d'empreinte FPM10A 40
Figure II. 7: Brochage du FPM10A 41
Figure II. 8: Brochage de capteur FPM10A 42
Figure II. 9: Le numéro ID du serial monitor 44
Figure II. 10: Emplacement du doigt sur le capteur 44
Figure II. 11: Empreinte enregistrée avec succès 45
Figure II. 12: La reconnaissance d'empreinte 46
Figure II. 13: L'affichage de ID des empreintes autorisés 46
Figure II. 14: Afficheur LCD et accroires associées 47
Figure II. 15: Brochage d'un écran LCD 48
Figure II. 16: Principe de fonctionnement d'un écran LCD 49
Figure II. 17: PCF8574 (I2C) 50
Figure II. 18: Symbole de relais 51

Figure II. 19: Schéma interne de relais 51
Figure II. 20: Principe de fonctionnement d'un Relais 53
Figure II. 21: Buzzer 1. Électromécaniques, 2. piézo-électrique 53
Figure II. 22: Serrure Électromagnétique 54
Figure II. 23 Symbole de la LED 55
Figure II. 24: Présentation des éléments de l'ARDUINO software. (Jean- Noël ,2006) 57
Figure II. 25: Module TERMINAL SERIE.[30] 58
Figure II. 26: Fenêtre graphique de l'EDI qui représente le programme de base.[30] 59
Figure II. 27: Les étapes de téléchargement du code. (TAKHA AIMEN,2020) 61
Figure II. 28: Les étapes pour ajouter le lien de la bibliothèque.[31] 62
Figure II. 29: Installation de la bibliothèque ESP32 62
Figure II. 30: Bibliothèque Arduinowebsockets 64
Figure II. 31: Le type de carte utiliser 65
Figure II. 32: Exemple d'un texte avec le langage HTML.[33] 65
Figure II. 33: représente comment rédiger un paragraphe dans un HTML 66
Figure II. 34: exemple d'une interface graphique sur un navigateur web.[33] 66
Figure II. 35: Mode de diffusion 67
Figure II. 36: Mode détection des visages 67

Chapitre III

Figure III 1: Montage à base de esp32cam-MB 72
Figure III 2: Organigramme de la reconnaissance facial 73
Figure III 3: Etablissement de la connexion wifi avec la carte ESP32cam 74
Figure III 4: Interface de la plateforme 74
Figure III 5: Les noms enregistrés 75
Figure III 6: Brochage de la carte esp32cam avec la carte Arduino 76
Figure III 7: Reconnaissance de la personne enregistrée 77
Figure III 8: LED allumée (serrure ouverte) 77
Figure III 9: Personne non enregistrée 78
Figure III 10: L'organigramme de l'empreinte digitale avec la carte Arduino Uno 80
Figure III 11: Schéma bloc du capteur d'empreinte avec la carte Arduino 81
Figure III 12: LED allumée 82
Figure III 13: Personne non enregistrée 82
Figure III 14: Représente schéma bloc du circuit général 83
Figure III 15: Organigramme général 84
Figure III 16: Les différents composants de la maquette 85
Figure III 17: Démarrage du système « posez votre doigt » lors du 86
Figure III 18: Résultat de l'accès refusée 87
Figure III 19:Empreinte validée 87
Figure III 20: Visage reconnu 88
Figure III 21: Porte ouverte 88
Figure III 22: Accès non autorisé, porte fermée 89

Liste des tableaux

Tableau II. 1 : Rôle et nom de chaque broche d'un afficheur LCD 48

Tableau III. 1 : Rôle et nom de chaque broche d'un afficheur LCD..... 89

Introduction générale

Le contrôle d'accès biométrique est une technologie très utilisée et très répandue vu la fiabilité et la sécurité qu'elle apporte, et permet de gérer ou limiter l'accès physique a un bâtiment ou un site au quelle on veut contrôler ou limiter l'accès, les systèmes de contrôle d'accès sont très utilisés pour contrôler le flux dans les aéroports ou limiter l'accès à des sites ou des endroits très sensibles comme les banques.

Plusieurs systèmes d'identification et de vérification de caractéristiques biométriques sont développés et en amélioration constante, mais ça reste toujours insuffisants pour des besoins qui exiges une sécurité très fiable, la plupart de ces systèmes utilisent une seule méthode de sécurité biométrique, donc le système reconnait la personne avec une seule signature biométrique.

Dans le cadre de ce projet, nous nous intéressons au concept du contrôle d'accès par biométrie. Notre objectif consiste à proposer un système pour le contrôle d'accès permettant d'assurer une fiabilité et une sécurité très élevé. Pour cela nous avons jugé que le choix le plus judicieux en matière de contrôle d'accès est de combiner deux systèmes biométriques très sécurisés, pour notre cas nous allons combiner deux modalités : l'empreinte digitale et la reconnaissance faciale.

Ce présent mémoire est structuré en trois chapitres organisés comme suit :

- Le premier chapitre portera sur des généralités sur les systèmes biométriques, ses différents types, ses performances, ses caractéristiques ainsi que ses applications.
- Le deuxième chapitre sera consacré à la présentation du projet en introduisant et en faisant une étude des outils utilisés pour la réalisation de notre projet.
- Le troisième et dernier chapitre inclura la réalisation, la structure et la discussion des résultats d'expérimentation obtenus.

Chapitre I

Généralités sur la biométrie

I.1 Introduction

Les systèmes de contrôle d'accès sont devenus presque une nécessité de nos jours par les entreprises qui disposent de locaux ou bâtiments, considérés comme « sensibles » et qui nécessitent un niveau de sécurité optimal. Les solutions sont nombreuses de nos jours pour contrôler l'accès du personnel ou d'intrusions dans une entreprise, une nouvelle technologie de contrôle d'accès a fait son apparition et ne cesse de se développer depuis 1997. Nous allons présenter dans ce chapitre les différents types de système de biométrie.

I.2 Concepts de base

La biométrie peut être définie comme étant « la reconnaissance automatique d'une personne en utilisant des traits distinctifs ». Une autre définition de la biométrie est « toutes caractéristiques physiques ou traits personnels automatiques mesurables, robustes et distinctifs qui peuvent être utilisés pour identifier ou pour vérifier l'identité prétendue d'un individu » ;

La biométrie consiste en une analyse mathématique des caractéristiques physiques ou biologiques d'une personne et a pour objectif de déterminer son identité de manière incontestable ;

La biométrie surpasse toutes les méthodes existantes d'authentification ID (identifiant informatique), les badges magnétiques et les mots de passe. En effet, elle fournit plus de sécurité et de sûreté, ce qui engendre un énorme avantage économique et elle rectifie les grandes failles de sécurité d'authentification (ID) (John D, 2003).

I.2.1 Principe de fonctionnement d'un système biométrique

Les systèmes biométriques sont des systèmes de reconnaissance de formes qui traitent les données biométriques des individus. Ils présentent trois principaux modes de fonctionnement qui sont (Anouar Ben KHALIFA,2014) :

- **L'enregistrement :** Il s'agit d'une phase d'apprentissage durant laquelle les données biométriques des individus à reconnaître sont collectées par un capteur biométrique, puis représentées sous formes de signatures numériques pour être stockées dans une base de références ;
- **L'authentification :** le candidat décline son identité et le système vérifie alors si cette identité correspond bien à celle prétendue. Les caractéristiques sont mesurées et comparées à celles qui sont stockées à la base de référence ;
- **L'identification :** est une phase qui consiste à établir l'identité de l'utilisateur, L'utilisateur utilise un identifiant unique qui l'identifie et qui lui est attribué individuellement

I.2.2 Les techniques biométriques

Il existe plusieurs techniques biométriques utilisées dans plusieurs applications et secteurs, on peut en distinguer deux catégories [1] **:**

I.2.2.1 L'analyse morphologique (physiologique)

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

I.2.2.2 L'analyse comportementale

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

I.3 Les différents systèmes biométriques

Dans cette section, nous allons décrire les différents systèmes biométriques :

I.3.1 Les empreintes digitales

Parmi les systèmes biométriques les plus récents, la reconnaissance des empreintes digitales est l'une des méthodes biométriques les plus utilisées. Les empreintes digitales sont composées de lignes parallèles et constituent une forme unique, permanente et universelle. Pour obtenir une image de l'empreinte ou la composition d'un doigt, les avancées technologiques ont permis d'automatiser la tâche au moyen de capteurs intégrés, remplaçant l'ancienne méthode l'utilisation de l'encre et du papier. Ces capteurs fonctionnant avec différents facteurs de mesure (température, champ électrique, pression) permettent de mesurer l'empreinte positionné sur ce dernier.

L'image d'empreinte de la personne est capturée ou enregistrée à l'aide d'un lecteur d'empreinte digitale puis les caractéristiques et les traits sont extraites de l'image puis un modèle est créé. La **figure I.1** illustre les étapes d'extraction des traits de l'empreinte digitale ;

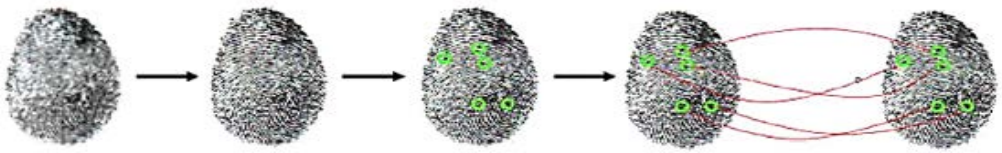


Figure I. 1: Le processus de reconnaissance par empreinte digitale

Cependant, lorsque la qualité de l'image d'empreinte digitale est médiocre, cette approche rencontre quelques difficultés, car l'extraction précise des points de minutie est difficile. Cette méthode ne tient pas en compte la structure globale de crêtes et de sillons. Les approches ou méthodes basées sur la corrélation sont capables de surpasser les problèmes de méthode fondée sur les minuties. Ces méthodes utilisent la structure globale de l'empreinte, mais les résultats sont moins précis qu'avec les minuties. De plus, les techniques de corrélations sont affectées par la translation et rotation de l'image de l'empreinte. C'est pour cela que les deux méthodes sont en général fusionnées pour avoir de meilleurs résultats du système (Florent Perronnin,2002).

I.3.2 Le système biométrique à base de l'iris

L'utilisation de l'iris comme caractéristique biométrique unique de l'homme a fait naître une technologie d'identification fiable et extrêmement précise. L'iris est sous forme d'anneau, situé entre le blanc de l'œil et la pupille, il est unique. L'iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque personne. Les algorithmes utilisés dans la reconnaissance de l'iris sont si précis que la planète toute entière pourrait être inscrite dans une base de données de l'iris avec peu d'erreurs d'identification ;

L'image de l'iris est généralement capturée à l'aide d'une caméra, Cependant, cette étape de capture implique une coopération de la personne. De plus, il existe plusieurs contraintes liées à l'utilisation de cette technologie. Par exemple, il faut s'assurer que l'iris de la personne comme représenté sur la **Figure I.2** est à une distance fixe et proche du capteur d'iris, ce qui rend moins pratique l'utilisation de cette technologie (Florent Perronnin,2002).

Figure I. 2 : Photos d'iris

I.3.3. Le système biométrique à base de la reconnaissance faciale

Nos visages sont des objets complexes avec des traits qui peuvent varier dans le temps. Cependant, les humains ont une capacité naturelle à reconnaître le visage d'une personne et de l'identifier d'un seul coup d'œil. Bien sûr, notre capacité de reconnaissance naturelle s'étend au - delà de la reconnaissance du visage, où nous sommes également en mesure d'identifier rapidement des objets, des odeurs ou des sons. Malheureusement, cette compétence n'existe

pas chez les machines. C'est ainsi qu'est né le besoin de simuler artificiellement la reconnaissance afin de créer des systèmes intelligents autonomes. Simuler la capacité naturelle de la reconnaissance faciale dans les ordinateurs est une tâche très compliquée mais pas impossible. Tout au long de notre vie, de nombreux visages sont vus et sauvegardés dans nos mémoires formant une sorte de base de données dans notre cerveau ;

La reconnaissance faciale par ordinateur a aussi besoin d'une base de données, qui est constituée en utilisant plusieurs images du visage, ou parfois des images différentes de l'individu pour tenir compte des variations dans les traits et les angles du visage. Les systèmes de reconnaissance de visage se composent d'un module pour capturer l'image avec une caméra. Tout d'abord, il procède à une détection du visage dans l'image acquise. Ensuite, l'image du visage détectée est normalisée pour être transmise au module de reconnaissance qui va la traiter en utilisant des algorithmes afin d'extraire une signature faciale ;

Finalement, cette signature est comparée, à l'aide d'un algorithme, avec les signatures déjà existantes dans une base de données locale, afin d'identifier la personne en question. Les différentes étapes de la reconnaissance faciale sont illustrées dans la **figure I.3.** Durant le dernier siècle de recherche, la performance des systèmes de reconnaissance faciale s'est décuplée, mais les résultats sont encore loin d'être parfaits. Ces systèmes peuvent être induits en erreur à cause des variations lumineuses et au pose non fixe ou non stable de la personne (OUAMANE,2012).

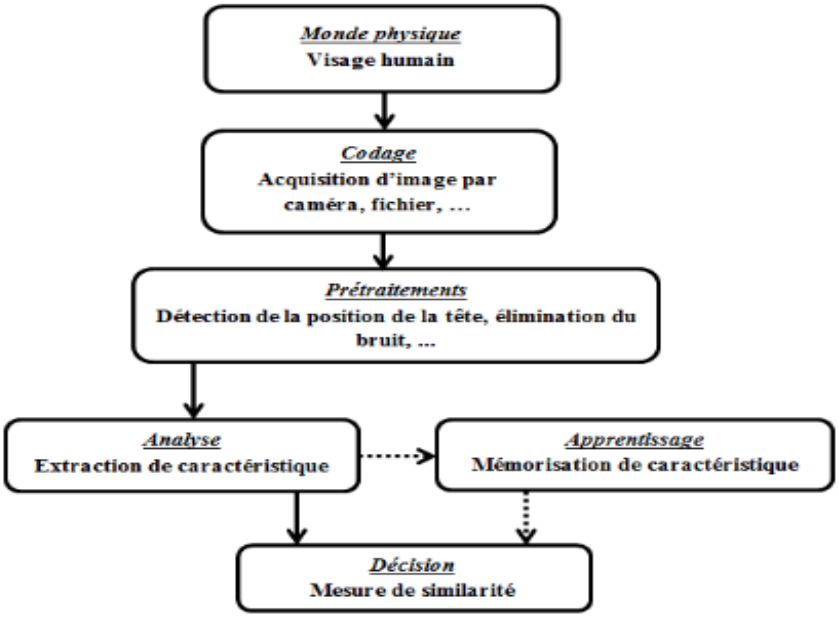


Figure I. 3: Schéma synoptique d'un système de reconnaissance faciale. [1]

I.4 Performance d'un système biométrique

La performance évalue l'efficacité et la fiabilité d'un système biométrique dans un cadre d'utilisation précis. Dans cette partie, nous allons débuter par les définitions d'une variété de mesure de ce qu'on appelle les taux d'erreurs utilisées dans le but de quantifier l'exploit d'un système biométrique. Par la suite, on va présenter la collection des bases de données essentielles, les plateformes d'évaluation, avec les compétences de comparaison de systèmes biométriques (OUAMANE Hanane, 2012).

I.4.1 Métriques

Il existe dans la littérature plusieurs métriques de diverses natures que sont les mesures des taux d'erreur, les mesures liées à la saturation de mémoire et temps de traitement, les courbes de performance et les points de fonctionnement associés ;

I.4.2 Les mesures des taux d'erreur

Selon l'Organisation Internationale de Normalisation ISO/IEC 19795-1, les mesures des taux d'erreur sont divisées en trois classes que sont les taux d'erreur fondamentale, taux

d'erreur de systèmes d'authentification et taux d'erreur de systèmes d'identification (El Abed, 2011).

- **Taux d'erreur fondamentale**

  - Taux d'échec à l'acquisition FTA : proportion des tentatives de vérification ou d'identification pour lesquelles le système biométrique n`a pas pu acquérir l'information biométrique requise.

  - Taux d'échec à l'enrôlement FTE : proportion des individus pour lesquels le système n'a pas pu générer le modèle biométrique durant la phase d'enrôlement. Prenons par exemple le cas des empreintes, il existe certaines personnes qui n'ont pas d'empreintes pour des raisons génétiques, ou des empreintes quasi-inexistantes pour des raisons médicales

  - Taux de fausse non-correspondance (false non-matche rate, FNMR) : proportion de fausses non-correspondances, par l'algorithme de comparaison, entre la donnée biométrique acquise et le modèle correspondant.

  - Taux de fausse correspondance (false matche rate, FMR) : proportion de fausse correspondance, par l'algorithme de comparaison, entre la donnée biométrique acquise et le modèle correspondant à un autre individu.

Les éléments d'origine (une image, un son...) utilisés pour les traitements informatiques ne peuvent jamais être reproduit à l'identique. Les performances des systèmes d'authentifications biométriques s'expriment par T.F.R, T.F.A, T.E.E schématisés sur la **figure (I.4)** :

- T.F.R : Pourcentage de personnes rejetées par erreur.
- T.F.A : Pourcentage d'acceptations par erreur.
- T.E.E : donne un point sur lequel le T.F.A. est égal au T.F.R. [2]

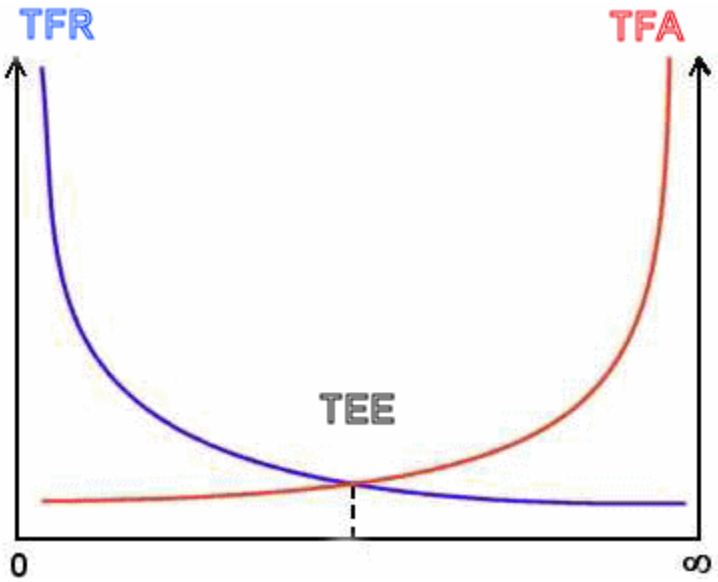


Figure I. 4: Les performances des systèmes biométrique

- **Taux d'erreur de systèmes d'authentification**

-Taux de faux rejets (false rejection rate, FRR) : proportion des transactions des utilisateurs légitimes rejetées par erreur. Ces transactions sont rejetées, par l'algorithme de correspondance, en raison de non-correspondance a tort ainsi que ceux rejetées en raison d'un échec à l'acquisition ;

-Taux de fausses acceptations (false acceptance rate, FAR) : proportion des transactions des imposteurs acceptés par erreur ;

La figure **I.5** représente la distribution théorique des taux de vraisemblance des utilisateurs légitimes et des imposteurs. Les deux taux d'erreurs, FAR et FRR, sont liés et dépendent d'un seuil de décision qui doit être ajustée en fonction de la caractéristique ciblée du système biométrique haute ou basse sécurité. En effet, plus le seuil est bas, plus le taux de fausses acceptations est élevé. Dans ce cas, le système biométrique acceptera des imposteurs. A l'inverse, plus le seuil s'est élevé, plus le taux de fausses acceptations est bas. Le système biométrique sera alors robuste aux imposteurs mais rejettera de vrais utilisateurs (M. Mohamad El Abed,2011).

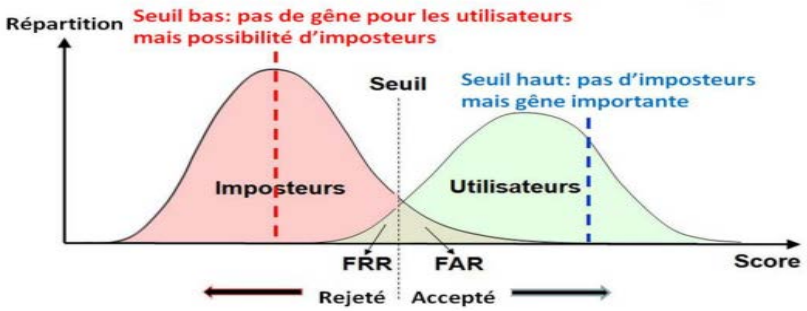


Figure I. 5 : Taux de vraisemblance des utilisateurs légitimes et des imposteurs d'un système d'authentification biométrique

- **Taux d'erreur de systèmes d'identification**

-Taux d'identification (identification rate, IR) : le taux d'identification au rang est la proportion de transactions d'identification, par des utilisateurs enrôlés dans le système, pour lesquels l'identifiant de l'utilisateur est dans les r identifiants retournes ;

-Taux de faux-négatif d'identification (false-négative identification-errer rate, FNIR) : proportion de transactions d'identification, par des utilisateurs enrôlés dans le système, pour lesquels l'identifiant de l'utilisateur ne figure pas dans la liste des identifiants retournée ;

-Taux de faux-positif d'identification (false-positive identification-errer rate, abrège par FPIR) : proportion de transactions d'identification, par des utilisateurs non enrôlés dans le système, pour lesquels la liste des identifiants retournée est non vide

-Taux de pénétration PR : mesure, en moyenne, le nombre de modèles biométriques présélectionnés par rapport au nombre total de modèles

I.5 Application des systèmes biométriques

La biométrie peut être appliquée pour l'authentification : vérifier qu'une personne est qui elle prétend être, et pour l'identification : déterminer qui est la personne ; ceci en fonction du facteur biométrique mesuré. Toute application nécessitant une authentification ou une identification peut utiliser la biométrie, cela ne signifie pas que l'utilisation de la biométrie

présente toujours un avantage par rapport aux autres techniques d'authentification et d'identification.

L'utilisation de la biométrie pourrait avoir plusieurs avantages : systèmes de gestion du temps, contrôle d'accès aux systèmes informatiques ou aux supports portables, contrôle d'accès physique et carte de fidélité ou autres systèmes de promotion pour les clients.

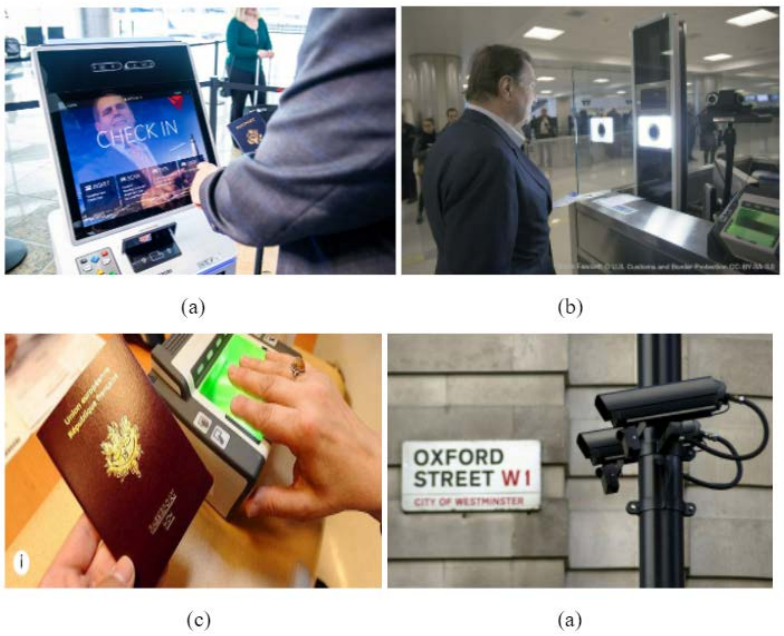
Les principaux objectifs de la biométrie sont d'accroître la sécurité et réduire l'obligation de garder les clés, de se souvenir des mots de passe, etc.

La technologie biométrique peut être utilisée pour un grand nombre d'applications. Les chances sont, si la sécurité est impliquée, la biométrie peut aider à rendre les opérations, les transactions et la vie quotidienne plus sûres et plus pratiques [3].

La biométrie peut être utilisée pour un grand nombre de domaines d'applications (Anouar Ben KHALIFA,2014) :

- La reconnaissance par l'iris à l'aéroport d'Amsterdam ;
- La reconnaissance faciale à l'aéroport d'Atlanta ;
- La reconnaissance faciale dans la ville de Nedham à Londres ;
- Le passeport biométrique en Europe qui comporte une puce RFID contenant des informations sur l'empreinte digitale et le visage de son propriétaire

Les exemples discutés sont montrés dans la **figure (I.6)** :



(a) (b)

(c) (a)

Figure I. 6 : Exemples d'application de la biométrie :

(a) Utilisation de l'iris à l'aéroport d'Amsterdam

(b) Machines de reconnaissance faciale à l'aéroport d'Atlanta

(c) Passeport biométrique

(d) Caméras pour reconnaissance faciale dans la ville de Nedham à Londres

I.5.1 Sécurité biométrique

Alors que la connectivité transparente tend à se répandre dans le monde entier, il est clair que les anciennes méthodes de sécurité ne sont pas assez solides pour protéger ce qui compte le plus. Heureusement, la technologie biométrique est plus accessible que jamais, prête à apporter une sécurité améliorée et une plus grande commodité à tout ce qui a besoin de protection [3].

I.5.2 Contrôle frontalier / Aéroports

Le contrôle aux frontières par identification biométrique dans les aéroports est un domaine d'application majeur de la technologie biométrique. Quiconque voyage en avion peut vous dire depuis les points de contrôle de sécurité que les passages frontaliers sont parmi les endroits les plus frustrants à traverser. Heureusement, la technologie biométrique permet d'automatiser le processus.

I.5.3 Biométrie résidentielle

Les innovations récentes en matière de mobilité et de connectivité ont créé un besoin de biométrie dans les maisons et les poches des consommateurs. Smartphones avec capteurs d'empreintes digitales, applications permettant la reconnaissance faciale et vocale, portefeuilles mobiles : ce sont des moyens de plus en plus populaires que les consommateurs du monde entier recherchent pour la biométrie dans leur vie.

I.5.4 Biométrie financière

Parmi les applications les plus populaires et les plus répandues de la technologie biométrique. L'identification financière, la vérification et l'authentification dans le commerce contribuent à rendre les opérations bancaires, les achats et la gestion des comptes plus sûrs, pratiques et responsables ;

I.5.5 Empreintes digitales et verrous biométriques

Verrouillage biométrique par empreintes digitales : Si vous avez quelque chose à protéger, pourquoi ne pas opter pour une solution de contrôle d'accès physique biométrique. Il s'agit d'une méthode d'authentification plus puissante que les clés, les cartes-clés et les codes PIN pour une raison simple : c'est qui vous êtes, pas ce que vous avez.

I.5.6 Biométrie de la santé

La biométrie offre non seulement sécurité et commodité partout où elle est déployée, mais dans certains cas, elle donne un coup de fouet à l'organisation. Dans le secteur de la santé, c'est particulièrement vrai. Les dossiers médicaux sont l'un des documents personnels les plus précieux et les médecins ont besoin d'un accès rapide.

I.5.7 Justice

La technologie biométrique et la justice ont une très longue histoire, et de nombreuses innovations très importantes dans la gestion de l'identité ont ravivé cette relation bénéfique. Aujourd'hui, la biométrie médico-légale est véritablement multimodale ; Les empreintes digitales, la reconnaissance faciale et la reconnaissance vocale jouent toutes un rôle important dans l'amélioration de la sécurité publique et l'identification des personnes recherchées**.**

I.5.8 Contrôle d’accès logique

Le contrôle d'accès logique est un domaine d'application majeur de la technologie biométrique. Lorsque nous disons "il est temps de tuer le mot de passe", c'est de la technologie dont nous parlons. Qu'il s'agisse de sécuriser les applications de votre smartphone, d'accéder à la messagerie professionnelle ou d'activer des politiques BYOD efficaces.

I.5.9 Biométrie mobile

Les solutions biométriques mobiles vivent à l'intersection de la connectivité et de l'identité. Ils intègrent une ou plusieurs méthodes biométriques à des fins d'authentification ou d'identification et tirent parti de la portabilité des smartphones, tablettes et autres types d'appareils portables.

I.5.10 Temps et pointage

Des solutions biométriques de gestion du temps existent pour suivre les mouvements des employés, avoir un reportage précis des heures de travail de chacun et optimiser la performance des ressources humaines. Et cela en installant des horodateurs biométriques au niveau des entités, sociétés, entreprises et autres organisations [3].

I.6 Les principales exigences d’une application biométrique

Selon une étude menée par une société américaine spécialisée dans le développement et l’industrie biométriques, une application biométrique doit répondre à quatre principales exigences qui sont (Anouar Ben KHALIFA,2014) :

1) Effort : la reconnaissance biométrique de l’identité d’un individu nécessite généralement une coopération et un effort développé par l’utilisateur. Cet effort doit être réduit le plus possible. Le visage, la voix, l’empreinte digitale, voir figure (I.7).

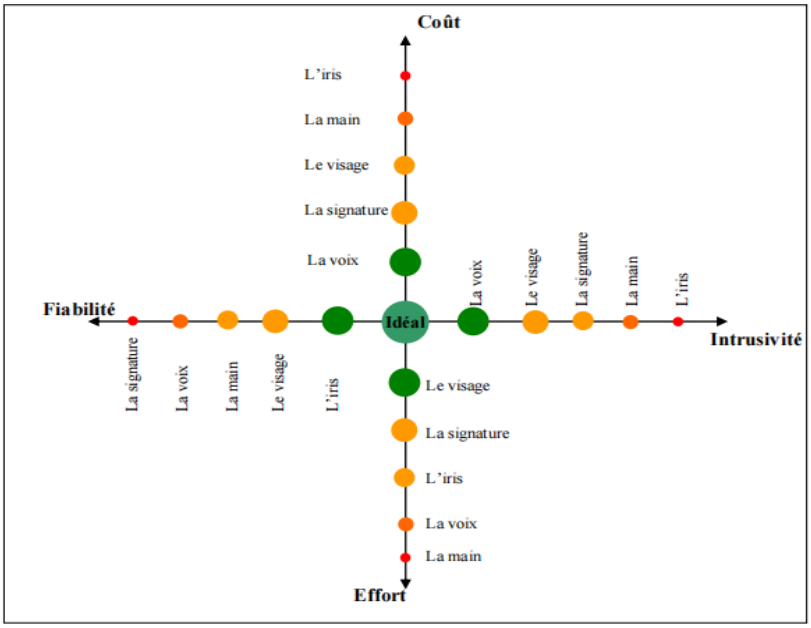


Figure I. 7 : Comparaison des sélections de technologies biométriques selon les critères effort.
(Anouar Ben KHALIFA,2014)

2) Coût : le coût d'un système biométrique dépend principalement de celui du matériel d'acquisition de la caractéristique biométrique ;
3) Intrusivité : ce critère est lié à l'acceptation des applications biométriques par les utilisateurs. Généralement les modalités biométriques qui ne nécessitent pas un contact entre l'utilisateur et le capteur telles que la voix, le visage ;
4) Fiabilité : ce critère qualifie les produits biométriques en termes d'efficacité et de précision de reconnaissance de l'utilisateur par le système biométrique. Il dépend essentiellement de l'environnement d'acquisition et surtout de la méthode de traitement de l'information. L'iris, la rétine et l'empreinte digitale sont les modalités biométriques les plus fiables selon les critères effort, coût, Intrusivité et fiabilité. La **figure I.3** illustre une comparaison entre L'iris, la main, le visage, la signature et la voix en termes des quatre principales exigences.

I.7 Les Caractéristiques biométriques

La biométrie est la science visant à identifier ou vérifier l'identité d'un individu à partir de caractéristiques morphologiques ou comportementales. La **Figure (I.8)** représente des exemples rassemblés sur les caractéristiques biométriques.

Une caractéristique physiologique, biologique ou bien comportementale est considérée comme une caractéristique biométrique (dite encore modalité biométrique) si elle répond aux critères suivants (Ben KHALIFA, 2014) :

• Universalité : présente chez tous les individus ;
• Unicité : spécifique à un seul individu ;
• Robustesse : difficile à imiter par un imposteur ;
• Acceptabilité : simple à acquérir de façon non intrusive ;
• Performance : permet une reconnaissance précise et rapide des Individus.

La figure ci-dessous représente les différentes caractéristiques de la biométrie :

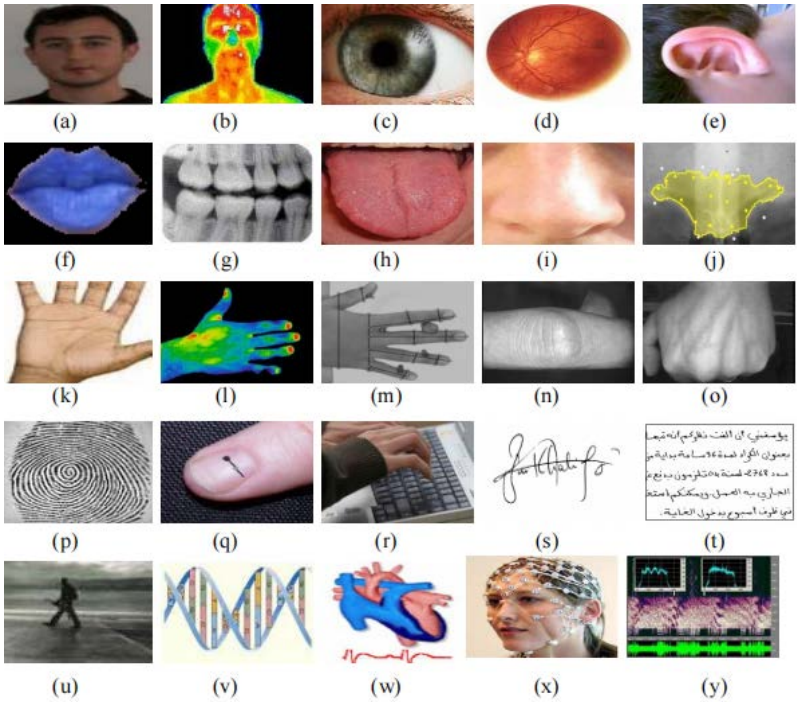


Figure I. 8 : Exemples de caractéristiques biométriques

(a). Visage, (b). Thermogramme facial, (c). Iris, (d). Rétine, (e). Oreille, (f). Formes des Lèvres, (g). Couronne dentaire, (h). Langue, (i). Nez, (j). Sinus frontal, (k). Empreinte Palmaire, (l). Thermogramme de la main, (m). Forme de la main, (n). Articulation des Doigts, (o). Veines de la main, (p). Empreinte digitale, (q). Ongles, (r). Dynamique de la Frappe sur le clavier, (s). Signature manuscrite, (t). Ecriture manuscrite, (u). Démarche, (v). ADN, (w). Electrocardiogramme, (x). Electro-encéphalogramme, (y). Voix. (Anouar Ben KHALIFA,2014)

I.8 États de l’art sur les méthodes de télésurveillance par systèmes **biométriques**

La biométrie est la science qui porte sur l'analyse des caractéristiques physiques ou comportementales propres à chaque individu. La biométrie signifie de façon simplifiée la "*mesure du corps humain*". Une surveillance de masse biométrique utilise des technologies numériques automatiques par intelligence artificielle pour la reconnaissance de caractéristiques physiques ou comportementales des personnes présentes dans les lieux publics, à des fins d'identification ou de prévention des risques. La reconnaissance faciale par caméras de rue est la surveillance biométrique la plus connue [4].

Les technologies biométriques constituent un assemblage de composants matériels (capteurs, ordinateurs, etc.) et logiciels (algorithmes, drivers des capteurs, etc.). Chacun de ces composants a des faiblesses et des limites. Certaines technologies sont plus fiables que d’autres et certains manufacturiers offrent des produits plus ou moins performants pour une technologie donnée. De plus, ces systèmes nécessitent l’acquisition des données biométriques de personnes, ceci à l’aide d’un capteur et dans un environnement qui est, dans la plupart du temps, non contrôlé. En conséquence, ces systèmes ne donnent pas une réponse précise sur l'identité d’une personne mais une réponse relative qui s’exprime par un indice de similarité qui n’atteint quasiment jamais 100% (M. Mohamad El Abed,2011).

Depuis peu, les technologies fondées sur la biométrie suscitent un grand intérêt pour ce qu'elles pourraient apporter à la recherche de criminels, à la lutte contre le terrorisme et comme méthode d'identification « infaillible ».

Aujourd'hui, des technologies fondées sur la biométrie sont utilisées pour restreindre l’accès à des installations et systèmes d’information à haute sécurité et faciliter l’enregistrement et l’authentification des usagers en ligne.

À mesure que les innovations technologiques et le désir de se simplifier la vie amènent les hommes à interagir avec des systèmes reliés à des réseaux (comme les distributeurs automatiques de billets , les distributeurs automatiques de journaux ainsi que les services bancaires, les achats, les votes, etc. par téléphone ou par Internet), et bien que ces technologies soient loin d'avoir atteint leurs maturités, les technologies fondées sur la biométrie pourraient

constituer la réponse à un problème qui s'oppose sérieusement à cette évolution, à savoir la possibilité d'authentifier quelqu'un à distance (Ben KHALIFA, 2014).

I.9 La reconnaissance d'empreinte digitale

Dans cette section on va étudier l'empreinte digitale :

I.9.1 Description des empreintes digitales

Les empreintes digitales consistent en un ensemble de lignes localement parallèles de la peau des doigts qui forment un motif unique pour chaque individu , et les crêtes et les rainures sont distinguables, elles contiennent un ensemble de trous régulièrement espacés en leurs centre , elles sont uniques et immuables ,elle ne se modifient donc pas au cours du temps(sauf par accident);on remarque que, sur une empreinte digitale, on peut repérer un grand nombre de minuties comme le montre la **figure (I.9)** suivante :

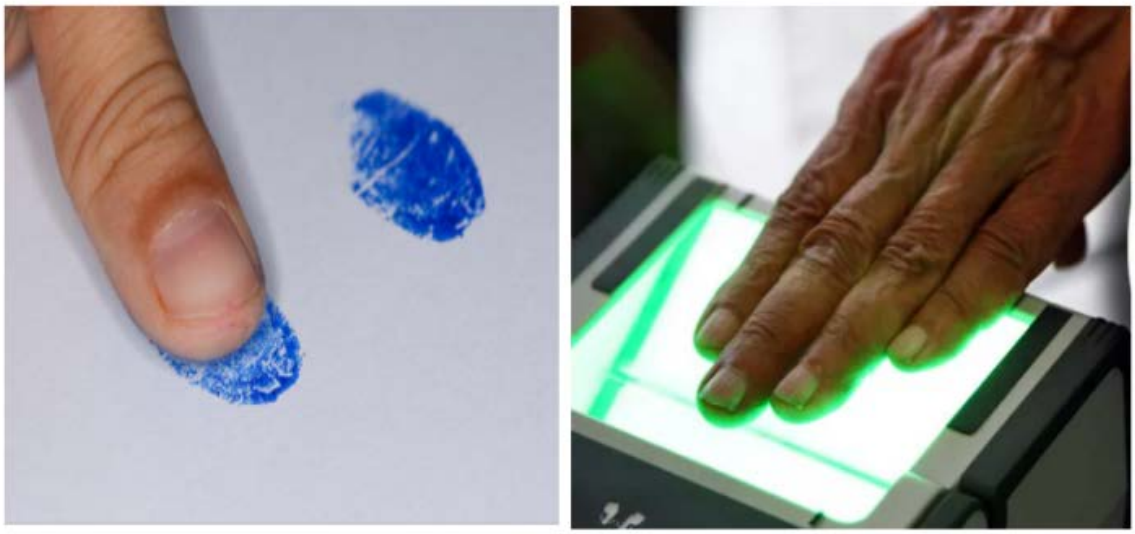
Figure I. 9 : Image d'une empreinte digitale. [1]

La reconnaissance d'empreinte digitale est la technique la plus ancienne et la plus répandue, les empreintes sont différentes pour chaque doigt d'une même personne. Il existe de nombreuses méthodes d'acquisition d'empreinte digitale (LAMRAOUI RAWIA,2016) :

La plus ancienne consiste à couvrir le bout du doigt d'une fine couche d'encre et à l'imprimer sur une feuille de papier ;

Les appareils d'acquisition numérique sont basés sur la capture optique, thermique, électromagnétique ou sur l'ultrason.

La **figure (I.10)** (a) présente une image de l'utilisation de l'ancienne méthode de reconnaissance d'empreinte digitale tandis que (b) représente une des nouvelles méthodes.



(a) (b)

Figure I. 10 : La figure Reconnaissance d'empreinte digitale(a)Reconnaissance par encre sur papier (b)Reconnaissance par un capteur optique

Les empreintes peuvent être classées, triées ou identifiées à l'aide de leur dessin général et de certaines particularités : on parle de lophoscopie. Une empreinte digitale est divisée en quatre zones : la zone centrale, la zone basale, la zone distale et les zones marginales (les côtés).

Pour décrire une empreinte la première particularité à observer est la présence de delta(s). Un delta est un point de convergence entre les zones centrales, basales et marginales. Le delta peut être en forme de triangle ouvert ou fermé, ou formé directement par une crête.

Quelques exemples de deltas sont représentés sur la **figure (I.11)** :

Figure I. 11: Delta trépied, Delta triangle fermé, Delta triangle ouverte

I.9.2 L'étude d'une empreinte

L'étude d'une empreinte s'effectue du général au particulier. La première observation qui peut être réalisée est l'absence ou la présence de deltas. En effet l'empreinte digitale peut

être : adelte (aucun delta), monodelte (un delta), bidelte (deux deltas) et plus rarement tridelte (trois deltas), qui sont représentés sur la **figure II.12** :

Figure I. 12 :(a) adelte, (b) monodelte, (c) bidelte

Ensuite, la forme du centre de figure permet de rattacher l'empreinte à une des familles des dessins digitaux : les arcs, les tentes pures, les composites, les boucles ou les verticilles. Enfin, une analyse plus minutieuse des minuties ou points caractéristiques permettra de comparer deux empreintes pour dire si elles sont identiques. Il existe de nombreuses minuties mais les plus fréquentes sont les arrêts de ligne et les bifurcations [5].

I 9.3 Authentification et vérification d'empreinte

Le système de l'authentification d'empreinte est divisé par trois étapes schématisées sur la **figure I.13** (LE Duc Bao) :

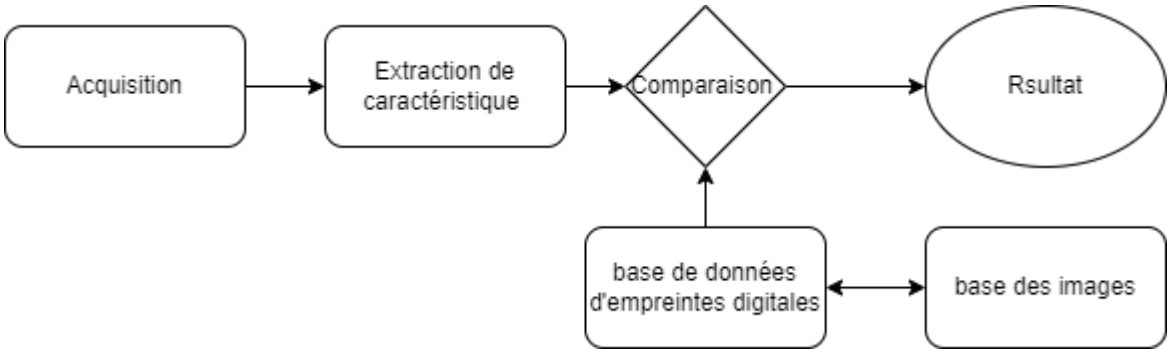


Figure I. 13 : Diagramme de système en haute niveau

Acquisition : Un système d'acquisition équipé d'un capteur est utilisé pour acquérir une caractéristique spécifique de l'utilisateur ;

Extraction : Ayant une image, une étape de segmentation permet d'extraire la caractéristique dont le processus d'authentification a besoin ;

Comparaison : Calculer la différence entre les caractéristiques extraites et la base de données et décider lesquelles est le plus semblable d'entrée.

I.9.4 Architecture de système d'empreinte digitale

Un système automatique de vérification (authentification) d'empreintes digitales est une chaîne de traitement qui se divise en deux étapes : enrôlement ou enregistrement et authentification comme l'illustre la **figure (I.14) :**

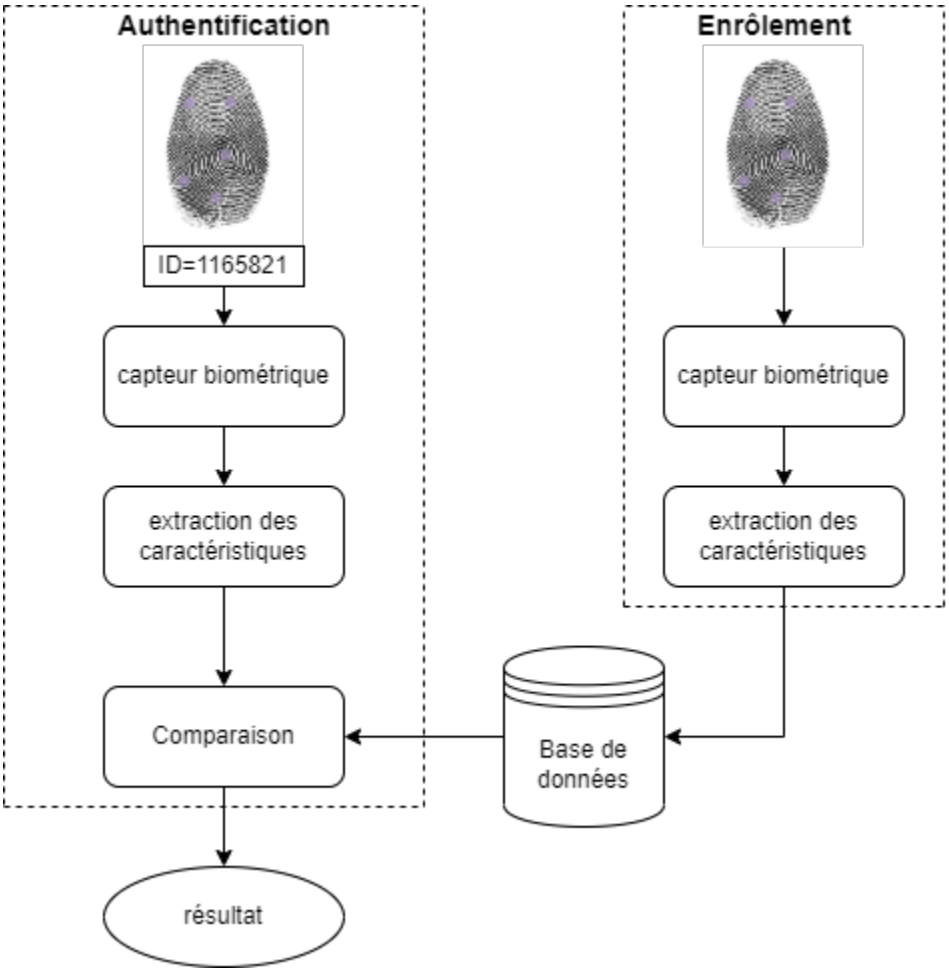


Figure I. 14 : Architecture d'un système d'authentification par empreinte digitale

Durant l'enrôlement, le trait biométrique de l'utilisateur est capturé (acquisition) et les caractéristiques sont extraites et sont sauvegardées dans une base de données comme modèle de référence. Durant l'authentification, le même trait biométrique de l'utilisateur est de nouveau capturé et les caractéristiques sont extraites et sont comparées avec celles dans la base de données pour calculer leur correspondance. L'enregistrement spécifique choisi pour la

comparaison est déterminé en fonction de l'identité annoncée par l'utilisateur (Berredjem Achref, 2019).

I.9.5 Capteur d'empreinte digitale

Le capteur d'empreintes digitales est un type de capteur utilisé dans les dispositifs de détection d'empreintes digitales. Ces appareils sont principalement intégrés à des modules de détection d'empreintes digitales pour la sécurité informatique. Les principales caractéristiques de l'appareil incluent principalement (la précision et la performance) [6].

I.9.5.1 Les capteurs d'empreintes digitales macroscopiques

La majorité des capteurs d'empreintes digitales optiques exploitent la modification de l'indice de réflexion de la surface d'un prisme lorsque les reliefs du doigt sont en contact à une des faces du prisme. Le principe de fonctionnement de ce type de capteur est représenté de manière simplifiée sur la **figure I.15** :

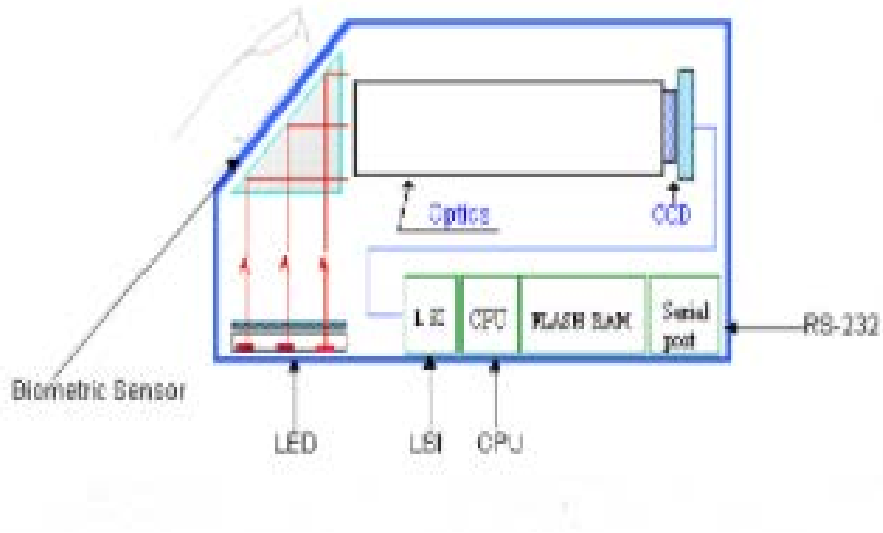


Figure I. 15 : Architecture d'un capteur macroscopique 29

L'image issue de ces capteurs possède généralement une bonne définition mais souffre de plusieurs défauts. En effet les images provenant de ces capteurs possèdent relativement peu de contraste et peuvent être facilement parasitées par les poussières et autres salissures ; notamment les traces résiduelles d'empreintes. De plus, l'écrasement du doigt à la surface du capteur induit une distorsion de l'image parfois importante qui peut soulever différents problèmes lors de la phase d'appariement de l'empreinte digitale. Malgré ces défauts, les

capteurs d'empreintes digitales optiques sont à l'heure actuelle les systèmes macroscopiques les plus utilisés et les plus aboutis (Fabien PARRAIN,2002/12/2).

I.9.5.2 Capteurs intégrés

Presque tous les capteurs d'empreintes digitales intégrés sur le marché aujourd'hui sont capacitifs ou thermiques. Les capteurs utilisant d'autres modes d'acquisition, comme les capteurs tactiles, sont encore marginaux, notamment à cause des problèmes posés par leurs boîtiers [7].

I.10 La reconnaissance faciale

Un système de reconnaissance faciale est un type d'application informatique biométrique qui peut identifier ou vérifier une personne à partir d'une image numérique en comparant et en analysant des modèles. Ces systèmes biométriques sont utilisés dans les systèmes de sécurité.

I.10.1 Le fonctionnement

Les systèmes de reconnaissance faciale fonctionnent en capturant des données à partir de nœuds sur une image numérique d'un visage, et les données résultantes peuvent être stockées sous forme d'empreinte faciale. Lorsque les conditions sont favorables, ces systèmes utilisent des empreintes faciales pour une identification précise. Actuellement, ces systèmes se concentrent sur les applications pour smartphones, y compris le marketing personnel, les médias sociaux et le marquage d'images. Les sites de réseaux sociaux comme Facebook utilisent un logiciel de reconnaissance faciale pour marquer les utilisateurs sur les photos. Le logiciel ajoute également une personnalisation marketing. Par exemple, les panneaux d'affichage sont conçus avec un logiciel intégré qui peut identifier la race, le sexe et l'âge estimé des téléspectateurs pour fournir un marketing ciblé [8].

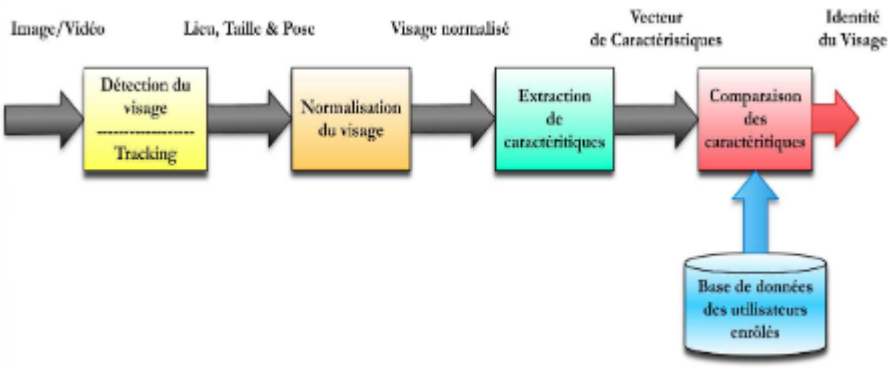


Figure I. 16 : Principe de fonctionnement de base d'un système de reconnaissance faciale

I.10.2 Les classes des techniques de reconnaissance de visages

Les systèmes de reconnaissance du visage reposent sur des algorithmes d'analyse de l'image, pouvant identifier les personnes qui y sont associées. Ces programmes créent une image du visage, en mesurant ses caractéristiques. Ils en produisent ensuite un fichier individuel, dénommé "Template ou signature". Les templates sont alors comparées avec toutes les images existantes au niveau de la base de données, en ressortant un score de similitude.

Les méthodes de la reconnaissance faciale

1) Méthode globale

Les méthodes globales sont basées sur des techniques d'analyse statistique bien connues. Il n'est pas nécessaire de repérer certains points caractéristiques du visage (comme les centres des yeux, les narines, le centre de la bouche, etc.) à part pour normaliser les images [9].

2) Méthode locale

Les méthodes locales, basées sur des modèles, utilisent des connaissances a priori que l'on possède sur la morphologie du visage et s'appuient en général sur des points caractéristiques de celui-ci [10].

3) Méthode hybride

En combinant la détection de caractéristiques géométriques (ou structurelles) avec l'extraction de caractéristiques d'apparence locales, il permet de combiner les avantages des

méthodes globales et locales. Ils peuvent améliorer la stabilité des performances de reconnaissance lors des changements de pose, d'éclairage et d'expression faciale [11].

Le schéma présenté par la **figure I.17** représente la classification des algorithmes principaux utilisés pour la reconnaissance faciale.

I.10.3 Systèmes biométriques basés sur la reconnaissance de visage

La **figure I.17** schématise les trois principales étapes de reconnaissance automatique de visage : détection de visages, extraction et normalisation des caractéristiques du visage, identification et/ou vérification.

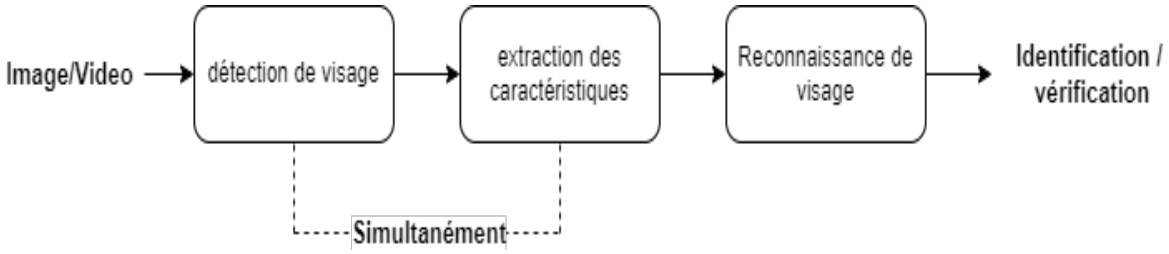


Figure I. 17 : Les étapes de la reconnaissance de visage.

Les étapes de la reconnaissance faciale sont détaillées dans ce qui suit :

- **Détection de visage**

L'efficacité des systèmes biométriques basés sur l'authentification de visage dépend essentiellement de la méthode utilisée pour localiser le visage dans l'image. Dans la littérature scientifique, le problème de localisation de visages est aussi désigné par la terminologie "détection de visages". Plusieurs travaux de recherches ont été effectués dans ce domaine. Ils ont donné lieu au développement d'une multitude de techniques allant de la simple détection du visage, à la localisation précise des régions caractéristiques du visage, tels que les yeux, le nez, les narines, les sourcils, la bouche, les lèvres, les oreilles, etc. [15].

- **Extraction de caractéristiques du visage**

L'extraction de caractéristiques telles que les yeux, le nez et la bouche est une étape de prétraitement nécessaire pour la reconnaissance faciale. On peut distinguer deux approches différentes : la première est basée sur l'extraction de toute la région du visage, qui utilise généralement une approche globale de reconnaissance des visages. La deuxième approche consiste à extraire des points spécifiques de différentes régions caractéristiques du visage, telles

que les coins des yeux, de la bouche et du nez. Il est utilisé avec des méthodes de reconnaissance locale et également pour l'estimation de la pose du visage [15].

➢ **La reconnaissance de visage**

Le module de reconnaissance exploite les caractéristiques du visage ainsi extraites pour créer une signature numérique qu'il stocke dans une base de données. Ainsi, à chaque visage de la base est associée une signature unique qui caractérise la personne correspondante. La reconnaissance d'un visage s'obtient par l'extraction de la signature requête correspondante et sa mise en correspondance avec la signature la plus proche dans la base de données (SOUHILA GUERFI ABABSA,2008).

I.10.4 Les difficultés de reconnaissance faciale

Dans cette section, on va donner quelques difficultés rencontrées lors d'une reconnaissance faciale :

I.10.4.1 Problème d'éclairage

L'apparence d'un visage dans une image varie énormément en fonction de l'illumination de la scène lors de la prise de vue comme montré dans la **figure I.18**. Les variations d'éclairage rendent la tâche de reconnaissance de visage très difficile [12].

Figure I. 18 : Exemple de variation d'éclairage

I.10.4.2 Problème de posture

Quand le visage est de profil dans le plan image (orientation < 30°), il peut être normalisé en détectant au moins deux traits faciaux (passant par les yeux). Cependant, lorsque

la rotation est supérieure à 30°, la normalisation géométrique n'est plus possible. La **figure I.19** illustre quatre variations de poses pour représenter le problème de posture.

Figure I. 19 : Exemples de variation de poses.

I.10.4.3 Problèmes d'expression

Les changements d'expression tels que la colère, le rire et la tristesse représentés dans **la figure I.20** reflètent la précision de la reconnaissance faciale, L'état de la technique ne traite pas assez bien ces aspects, qu'il s'agisse d'ouvrir la bouche ou de faire des expressions exagérées, L'information faciale se situant dans la partie supérieure du visage reste quasi invariable. Elle est généralement suffisante pour effectuer une identification. Toutefois, étant donné que l'expression faciale modifie l'aspect du visage, elle entraîne forcément une diminution du taux de reconnaissance [12].

Figure I.20 : Les diffèrent expression du visage face à la reconnaissance faciale

I.10.4.4 Changement d'âge

Le développement humain passe par différents stades d'âge (l'adolescence, la jeunesse, la vieillesse). Son apparence pourrait changer considérablement. Ce qui entraîne une diminution du taux de reconnaissance. Pour différents groupes d'âge, le taux de reconnaissance de l'algorithme de reconnaissance faciale est également différent [12]. La **figure I.21** représente le changement de l'apparence en conséquence du changement de l'âge.

Figure I.21 : Apparence avec l'âge

I.10.5 La multimodalité

Afin d'améliorer la performance des systèmes biométriques susmentionnés, (dits système unimodaux) la multimodalité est introduite. Cette dernière consiste à combiner plusieurs techniques biométriques en réduisant ainsi le risque d'impossibilité d'enrôlement, et obtenant un système robuste aux fraudes. [13]

Le système multimodal se réfère à la combinaison de deux ou plusieurs systèmes biométriques en acquérant les informations qui seront traitées par la suite. Ces deux procédures peuvent se faire simultanément (architecture parallèle) ou en série (architecture série). Cependant, l'architecture de système biométrique dépend essentiellement de la manière du traitement des données, car l'acquisition est souvent séquentielle. En fait, il n'existe pas des capteurs capables de recevoir simultanément des traits biométriques de différentes modalités, à l'exception de quelques capteurs d'empreintes multi-doigts ou palmaires. Et même l'architecture de traitement est liée à la décision. Il s'agit, donc, de prendre la décision après le traitement de toutes les modalités biométriques, on parle alors de la fusion en parallèle. Ou bien décider après avoir un score de similarité de chaque modalité ce qu'on appelle la fusion en série (Mme Nefissa KHIARI-HILI, 2016/05/24).

1.11 Conclusion

Dans ce chapitre nous avons présenté un aperçu général sur les systèmes biométriques, ainsi que les performances et les applications de la biométrie, afin d'avoir une vision sur les outils et les protocoles pouvant servir au développement de notre projet à partir des objectifs

tracés pour la réalisation de ce mémoire. Dans le chapitre suivant, nous parlerons de modules nécessaires ainsi que leurs configuration et brochage pour la construction de notre projet.

Bibliographies

(John D, 2003). John D. Woodward, Jr; Christopher Horn, Julius Gatune and Aryn Thomas, «Biometrics A look at Facial Recognition», documented briefing by RAND Public Safety and Justice for the Virginia State Crime Commission, 2003.

(Anouar Ben KHALIFA,2014). Anouar Ben KHALIFA, « Contribution aux techniques de fusion des modalités biométriques », THÈSE de Doctorat, Ecole Nationale d'Ingénieurs de Tunis, 2014.

(Fabien PARRAIN,2002/12/2). Fabien PARRAIN, « Capteur intégré tactile d'empreintes digitales à microstructures piezorésistives », THÈSE de Doctorat INSTITUT NATIONAL POLYTECHNIQUE DE GRENOBLE, et soutenue le 02 décembre 2002

(LAMRAOUI RAWIA,2016/06/7) LAMRAOUI RAWIA, BENHMIDCHA HANAN, « LA RECONNAISSANCE BIOMETRIQUE MULTIMODALE », Mémoire Master, 2016.

(M. Mohamad El Abed,2011) M. Mohamad El Abed, « Evaluation de systèmes biométriques », Thèse de Doctorat, UNIVERSITE de CAEN/BASSE-NORMANDIE, 2011.

(Nefissa KHIARI-HILI, 2016/05/24), « Biométrie multimodale basée sur l'iris et le visage », THÈSE de Doctorat L'UNIVERSITE DE TUNIS EL MANAR et de L'UNIVERSITE PARIS-SACLAY préparée à l'Université d'Evry Val d'Essonne, et Soutenue le 24 Mai 2016

(OUAMANE Hanane,2012). OUAMANE Hanane, Identification de reconnaissance faciale avec des expressions, Mémoire Master, Université Mohamed Khider Biskra, 2012.

(SOUHILA GUERFI ABABSA,2008/10/03). SOUHILA GUERFI ABABSA, « Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D », THÈSE de Doctorat UNIVERSITE D'EVRY VAL D'ESSONNE, 2008.

Webographie

[1]. Mémoire Online, « **Les techniques biométriques** », », [en ligne]. Disponible sur : https://www.memoireonline.com/03/15/8967/m_Conception-et-mise-en-place-dune-plateforme-de-securisation-par-synthese-et-reconnaissance-biom3.html consulte le : 2022/03/15

[2] [Biométrie-online, « principe de fonctionnement » [En ligne]. Disponible sur : https://www.biometrie-online.net/technologies/fonctionnement consulte le : 2022/04/02].

[3]. Solution intelligentes informatique, « Applications de la Biométrie en Algérie », [en ligne]. Disponible sur : https://www.solutionsinformatiques.dz/?Applications-de-la-Biometrie-en-Algerie consulte le : 2022/03/20

[4] TV5 MONDE, « Intelligence artificielle : l'UE va-t-elle autoriser la surveillance biométrique ? » [En ligne]. Disponible sur : https://information.tv5monde.com/info/intelligence-artificielle-l-ue-va-t-elle-autoriser-la-surveillance-biometrique-412805 consulte le : 2022/05/01

[5] Police scientifique, « Les types de dessins digitaux et leurs classifications » [En ligne]. Disponible sur :https://www.police-scientifique.com/empreintes-digitales/type-de-dessin-et-classification consulte le : 2022/04/04

(LE Duc Bao,2007/01/20) LE Duc Bao, « Authentification des empreintes digitales dans un système bioPki », travail d'intérêt personnel encadré, L'institut de la francophonie pour l'informatique, 20 janvier 2007 https://www.academia.edu/778964/Authentification_des_empreintes_digitales_dans_un_syst%C3%A8me_BioPKI

(Berredjem Achref,2019). Berredjem Achref, « La reconnaissance des individus par leur empreinte des articulations des doigts », Mémoire Master, juillet 2019.

https://dspace.univ-guelma.dz/jspui/bitstream/123456789/4037/1/La%20reconnaissance%20des%20individus%20par%20leur%20empreinte%20des%20articulations%20des%20doigts.pdf

[6] EL-PRO-CUS, « Fonctionnement et applications du capteur d'empreintes digitales», [En ligne]. Disponible sur : https://www.elprocus.com/fingerprint-sensor-working-and-applications/ consulte le : 2022/04/08

[7] 123dok, « Les capteurs intégrés d'empreintes digitales », [En ligne]. Disponible sur : https://123dok.net/article/les-capteurs-int%C3%A9gr%C3%A9s-d-empreintes-digitales.zkeexkez consulte le : 2022/04/08

[8] Electronique, « Capteurs biométriques - Types et fonctionnement », [En ligne]. Disponible sur : https://fr.jf-parede.pt/biometric-sensors-types consulte le : 2022/04/10

[9] KOMANDA BASEMA, Mémoire online, « Identification des personnes par reconnaissance de visage pour la sécurité d'une institution bancaire », [En ligne]. Disponible sur : https://www.memoireonline.com/01/14/8585/m_Identification-des-personnes-par-reconnaissance-de-visage-pour-la-securite-d-une-institution-banca15.html#:~:text=2.2.1%20M%C3%A9thodes%20globales,part%20pour%20normaliser%20les%20images. consulte le : 2022/04/15

[10] Chabane Djeraba, « Etude des expressions faciales en s'abstrayant du mouvement global de la tête », [En ligne]. Disponible sur : https://www.fil.univ-lille1.fr/~bilasco/PT/1617R/16MvtLocalVisage.html consulte le : 2022/05/02

[11] 123dok, « La place de la reconnaissance faciale parmi les autres techniques biométriques.15 », [En ligne]. Disponible sur : https://123dok.net/article/place-reconnaissance-faciale-techniques-biom%C3%A9triques.qo5ow5p7/ consulte le : 2022/05/05

[12] chowdera, « Difficultés de reconnaissance faciale », [En ligne]. Disponible sur : https://chowdera.com/2022/01/202201070257326570.html consulte le : 2022/05/12

[13] HAL, « La multimodalité », [En ligne]. Disponible sur : chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://hal.archives-ouvertes.fr/tel-01762973/document, consulte-le : 2022/05/18

Chapitre II

Matériels & logiciels utilisés

II.1 Introduction

Après avoir accompli une étude complète sur la biométrie, ses différents systèmes, ses performances, ses caractéristiques ainsi que ses applications. Dans ce chapitre, nous allons présenter la partie hardware et software du projet, en faisant une étude sur les composants, des cartes et des logiciels nécessaires pour la réalisation de notre projet.

II.2 Carte Arduino Uno

L'Arduino Uno est une carte électronique programmable open source basée sur du matériel et des logiciels faciles à utiliser. Qui permet, comme son nom l'indique, de contrôler des éléments mécaniques : systèmes, lumières, moteurs, etc. Cette carte électronique permet donc à son utilisateur de programmer facilement des choses et de créer des mécanismes automatisés, sans avoir de connaissances particulières en programmation. Il est un outil pensé et destiné aux inventeurs, artistes ou amateurs qui souhaitent créer leur propre système automatique en le codant de toute pièce.

Il existe plusieurs modèles de cartes Arduino mais le modèle Uno est le plus répandu et permet déjà un large éventail de possibilités.

L'un des avantages indéniables de ce microcontrôleur est sa facilité d'utilisation qui fait qu'il est accessible à tous, même les amateurs pourront s'en sortir aisément grâce aux explications claires distribuées un peu partout sur internet, la carte se connecte très facilement à un ordinateur via un câble USB fourni. [1]

II.2.1 Description

La carte Arduino Uno est basée sur un ATMega328 cadencé à 16 MHz. C'est la plus simple et la plus économique carte à microcontrôleur d'Arduino. Des connecteurs situés sur les

bords extérieurs du circuit imprimé permettent d'enficher une série de modules complémentaires. [2]

Cette carte peut se programmer avec le logiciel Arduino (**IDE**), un logiciel open source et extensible disponible gratuitement sur le site officiel de Arduino. [1]

La figure ci-dessous représente les différents compartiments de la carte Arduino :

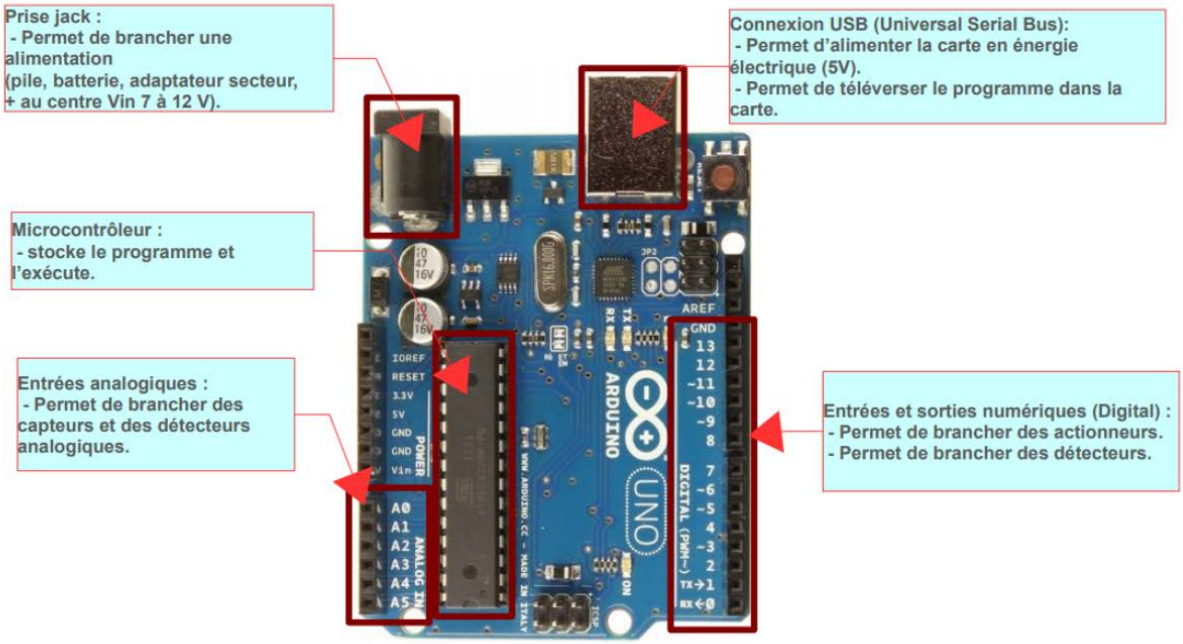


Figure II. 1: Les compartiments avec description de la carte Arduino Uno [3]

II.2.2 Caractéristiques

Le microcontrôleur ATMega328 contient un bootloader qui permet de modifier le programme sans passer par le programmeur. Cette carte est livrée avec un support en plastique mais pas de cordon USB et caractérisée par :

- Alimentation : via port USB ou 7 à 12 V sur connecteur alim 5,5 x 2,1 mm
- Microprocesseur : ATMega328
- Mémoire flash : 32 KB
- Mémoire SRAM : 2 KB

- Mémoire EEPROM : 1 KB
- Interfaces :
- 14 broches d'E/S dont 6 PWM
- 6 entrées analogiques 10 bits
- Bus série, I2C et SPI
- Intensité par E/S : 40 mA
- Cadencement : 16 MHz
- Gestion des interruptions
- Fiche USB B
- Version : Rev. 3
- Dimensions : 74 x 53 x 15 mm.[4]

II.2.3 La partie logicielle

Le logiciel de programmation de module Arduino est une application Java multiplateforme gratuite qui agit comme un éditeur de code et un compilateur, et peut également porter des micrologiciels et des programmes via une connexion série (RS232, Bluetooth ou USB, selon le module), Vous pouvez également l'exécuter sans l'interface Arduino et compiler le programme à partir de la ligne de commande. Le langage de programmation utilisé est le C++, compilé avec avrg++ et lié à la bibliothèque de développement Arduino. Cela permet d'utiliser la carte et ses entrées/sorties. Cette implémentation de langage standard permet à toute personne familiarisée avec C ou C++ de développer facilement des programmes sur la plate-forme Arduino. [5]

II.2.4 La partie matérielle

Un module Arduino est généralement construit autour du microcontrôleur Atmel AVR (ATmega328, ATmega32u4 ou ATmega2560 pour les versions récentes, ATmega168, ATmega1280 ou ATmega8 pour les plus anciennes), et de composants supplémentaires qui facilitent la programmation et la communication avec d'autres circuits. Chaque module possède au moins un régulateur linéaire de 5 V et un oscillateur à cristal de 16 MHz (ou un résonateur

en céramique dans certains modèles). Le microcontrôleur est préprogrammé avec un chargeur de démarrage, donc un programmeur dédié n'est pas nécessaire. Les modules sont programmés à l'aide d'une connexion série TTL, mais les connexions qui permettent cette programmation varient selon le modèle. Les Arduinos avaient d'abord un port série RS232, puis l'USB est apparu sur les modèles Diecimila, tandis que certains modules à usage portable comme Lillypad ou Promini se sont débarrassés de l'interface de programmation, passant à des modules USB-série dédiés (sous forme de cartes ou de câbles), cela permet également de réduire leur coût, les convertisseurs USB Serial TTL (FTDI232RL de FTDI) sont assez chers. L'Arduino utilise la plupart des entrées/sorties du microcontrôleur pour communiquer avec d'autres circuits. Par exemple, le modèle Diecimila possède quatorze entrées/sorties numériques, dont six peuvent générer des signaux PWM et six entrées analogiques. Les connexions sont établies via des connecteurs femelles HE14 situés sur le dessus de la carte, les modules d'extension s'empilant sur le dessus de l'Arduino. Plusieurs types d'extensions sont disponibles sur le marché. [5]

II.2.5 Schéma structurel

La figure 3.2 suivante représente le schéma structurel d'une carte Arduino UNO :

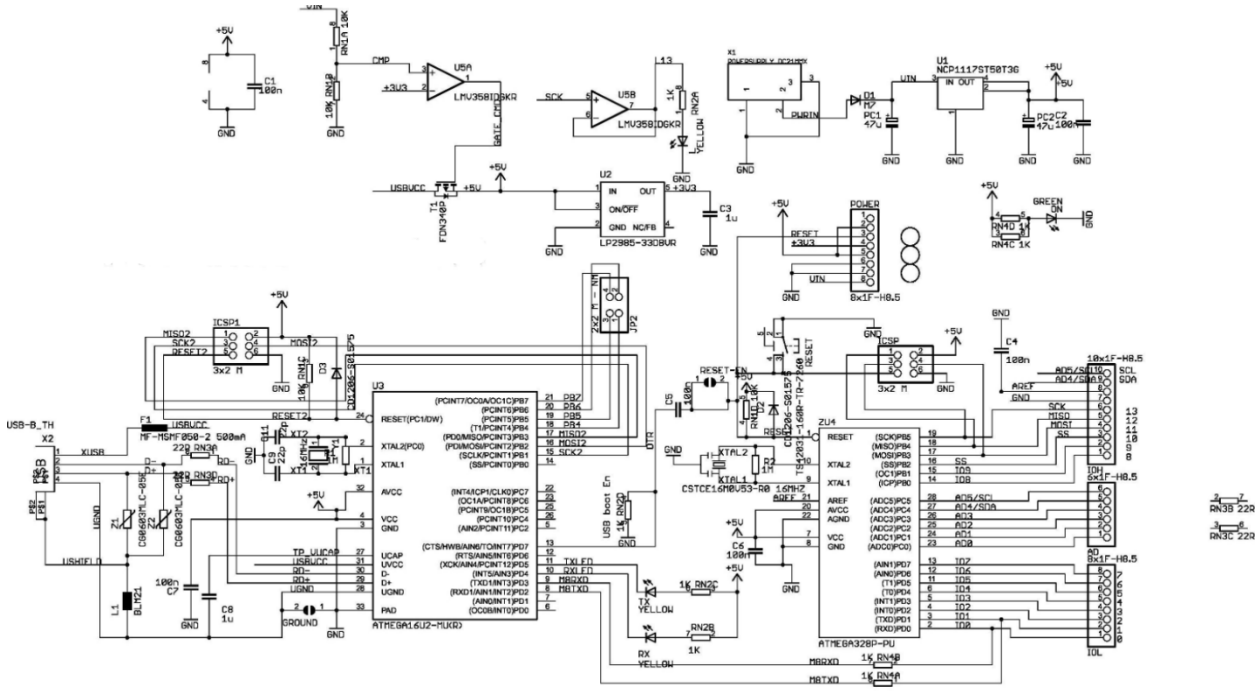


Figure II. 2: Schéma électronique structurel de l'Arduino Uno [6]

II.3 La carte ESP 32cam

Dans cette section, nous allons décrire la carte ESP32cam.

II.3.1 Description

Ce module AI Thinker IoT basé sur ESP32 cam fournit une interface WiFi et Bluetooth combinée à une caméra miniature. Ce kit est idéal pour créer des projets miniatures connectés qui nécessitent un enregistrement vidéo ou une photographie. La figure ci-dessous donne une image réelle d'une carte ESP32 cam [5].

Figure II. 3: Image réelle d'une ESP 32 cam.[7]

II.3.2 Caractéristiques de ESP 32 cam

Le module ESP32CAM a des spécifications très intéressantes que vous pouvez voir dans la fiche technique du fabricant. Nous résumons ici les plus importantes [7] :

-**Connectivité :** Wifi 802.11b / g / n + Bluetooth 4.2 avec BLE. Prend en charge le téléchargement d'images via Wifi.

- **Liens** : UART, SPI, I2Cet PWM. Il a 9 broches GPIO.

- **Fréquence d'horloge :** jusqu'à 160Mhz.

- **Puissance mémoire :** 520 Ko de SRAM + 4 Mo de PSRAM + fente pour carte SD de calcul du microcontrôleur : jusqu'à 600 DMIPS.

- **Liens utiles :** dispose de plusieurs modes de veille, d'un micrologiciel pouvant être mis à niveau par OTA et de voyants pour l'utilisation de la mémoire flash intégrée.

- **Appareil photo :** Prend en charge les caméras OV2640 qui peuvent être livrées dans le pack ou achetées indépendamment. Ces types de caméras ont :

- 2 MP sur votre capteur

- Taille de la matrice UXGA 1622 × 1200 px

- Format de sortie YUV422, YUV420, RGB565, RGB555 et compression de données 8 bits.

- Vous pouvez transférer une image entre 15 et 60 FPS.

II.3.3 Fonctionnement

Ce module se programme facilement via l'IDE Arduino® et permet d'accéder au flux vidéo de la caméra sur le réseau local. La caméra est livrée avec un microcontrôleur ESP32 branché sur le connecteur fourni. Il faut faire attention lors de la manipulation du câble de la caméra, il est très fragile. [8]

Pour programmer mon module ESP32CAM il est nécessaire d'utiliser un convertisseur qui fonctionne à un niveau logique de 3,3 V. [9]

II.3.4 Brochage de la carte ESP 32 cam

Il existe plusieurs manières et technique de brochage de la carte ESP 32 cam que nous allons citer et montre par la suite :

Brochage 1

Vous pouvez utiliser un adaptateur externe FTDI pour connecter ce module et vous faciliter le contrôle. Cela permet d'utiliser un port de type mini USB à la place du fil ESP32CAM. Pour utiliser un de ces modules, vous pouvez le connecter comme suit :

- Configurez le module FTDI pour qu'il fonctionne à 3.3v.
- Reliez la broche GPIO 0 et GND du module ESP32-CAM.
- La broche 3v3 du module doit être connectée à Vcc du FTDI.
- Le GPIO 3 (UOR) du module ira au TX du FTDI.
- GPIO 1 (U0T) du module va au RX du FTDI.
- L'autre GND de l'ESP32-CAM avec GND du module FTDI.

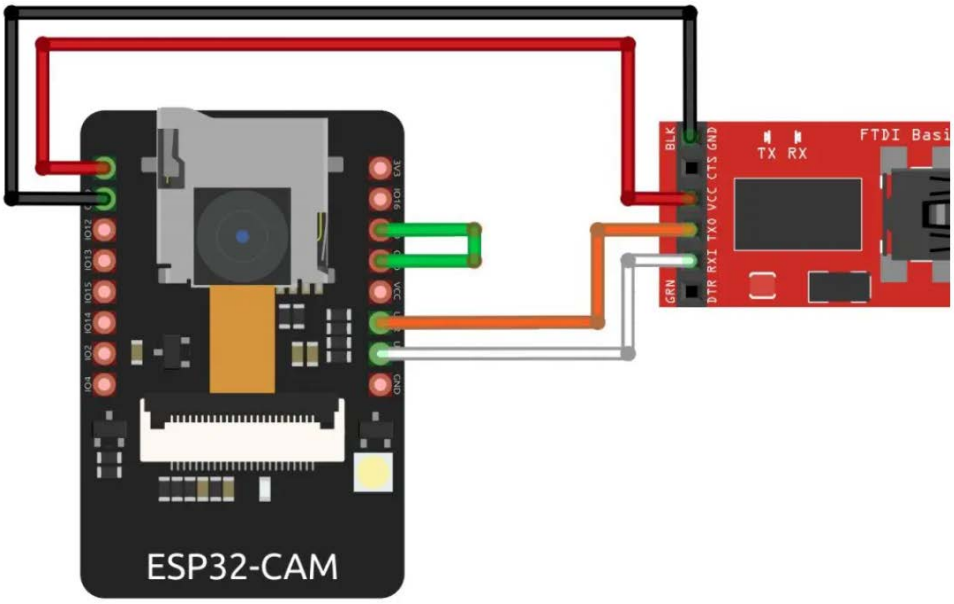


Figure II. 4: Brochage ESP 32 cam avec une FTDI

Brochage 2

Vous pouvez également utiliser un adaptateur à l'extérieur de la carte Arduino UNO pour connecter ce module et vous faciliter le contrôle. Cela permet d'utiliser un port de type mini USB à la place du fil ESP32CAM. Pour utiliser un de ces modules, vous pouvez le connecter comme suit [10] :

- Connecter Arduino 5 volts a ESP 32 cam 5 volts.
- Arduino GND a GND.
- Arduino RX a Cam board RX & TX to TX.
- Arduino reset pin a GND.
- ESP 32cam D0 a GND.

La figure suivante représente le schéma structurel du branchement de L'Arduino UNO et ESP 32 cam :

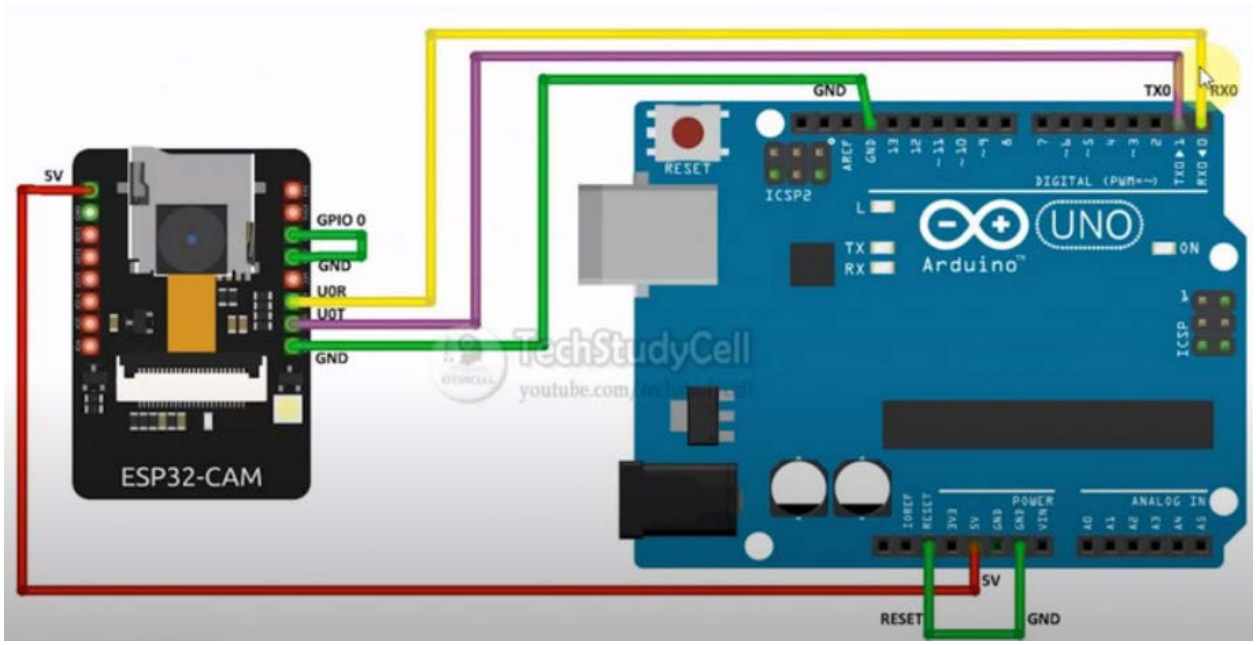


Figure II. 5: Branchement structurel Arduino UNO et ESP 32 cam.[11]

II.4 Module de capteur d'empreintes digitales avec Arduino (FPM10A)

Avec la sortie du module de capteur d'empreintes digitales FPM10A, la reconnaissance s'est améliorée, les empreintes digitales sont plus accessibles et faciles à ajouter à votre projet. Cela signifie que c'est très facile a utilisé pour la collecte3

, l'enregistrement, la comparaison et la recherche d'empreintes digitales, a une mémoire flash pour stocker les empreintes digitales fonctionnant avec des microcontrôleurs ou des systèmes avec des séries TTL. Ces modules ajoutés au système de sécurité, serrure de porte, système de présence, système de pointage…etc. [12]

Figure II. 6: Capteur d'empreinte FPM10A

II.4.1 Spécifications techniques

Les spécifications techniques d'un Capteur d'empreinte FPM10A sont résumés comme suit [13] :

-Tension d'alimentation : 3.3 V.

- Courant d'alimentation : courant de fonctionnement : <120mA.
- Courant de crête : <140 mA.
- Le temps d'entrée d'image d'empreinte digitale : < 1 seconde.
- La taille de la fenêtre : 14 x 18 mm.
- Profil : 256 octets.
- Fichier modèle : 512 octets.
- Capacité de stockage : 300.
- Taux de fausses acceptations (FAR) : < 0,001 % (niveau de sécurité 3).
- FRR (FRR) : < 1% (niveau de sécurité 3).
- Le temps de recherche : < 1 seconde (1 :500, moyenne).
- Interface informatique : UART (niveau logique TTL).
- Le débit en bauds de communication (UART) : (9600 x N) BPS où N=1 ~ 12 (la valeur par défaut de N=6, soit 57600 bps).
- Environnement de travail : température : -20°C à +50°C.
- Humidité relative : 40 % HR à 85 % HR (pas de traitement).
- Conditions de stockage : température : -40°C à +85°C.
- Humidité relative : < 85%H (pas de traitement).
- Dimensions (L * L * H) : 46,25 x 20,4 x 18,1 mm.

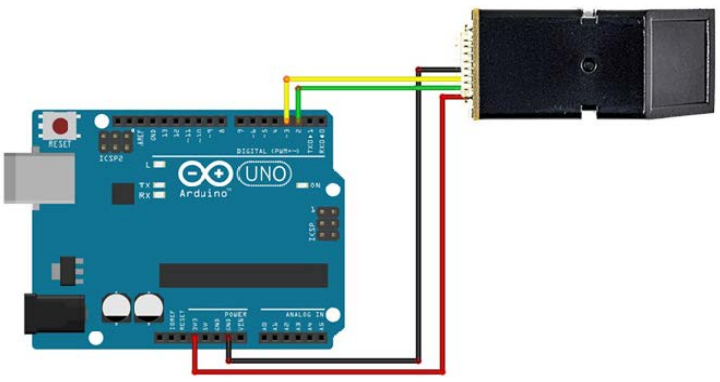


Figure II. 7: Brochage du FPM10A

II.4.2 Brochages

-VCC (alimentation 3,3 V)

-TXD (Sortie)

-RXD (Entrée)

-GND (terre d'alimentation et de signal)

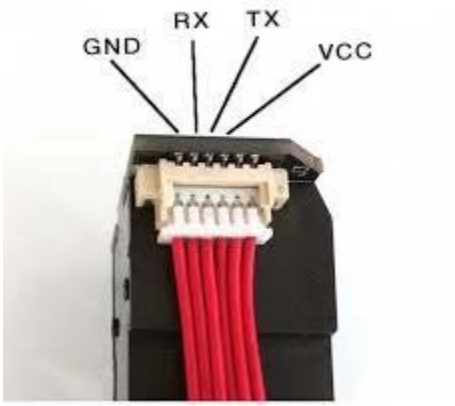


Figure II. 8: Brochage de capteur FPM10A

II.4.3 Principe d'opération

Le traitement des empreintes digitales comprend deux parties : l'enregistrement des empreintes digitales et la correspondance des empreintes digitales (la correspondance peut être 1 : 1 ou 1 : N). Lors de l'inscription, l'utilisateur doit saisir son doigt deux fois. Le système traitera les deux images, l'image génèrera un modèle du doigt en fonction des résultats du traitement et le stock en tant que modèle. Lors de la mise en correspondance, l'utilisateur entre le doigt par le biais du capteur optique et le système génère un modèle du doigt et le compare aux modèles existants dans la bibliothèque. Pour une correspondance 1 : 1, le système comparera le doigt vivant avec le modèle spécifique désigné dans le module ; pour une correspondance 1 : N, ou une recherche, le système recherchera le doigt correspondant dans toute la bibliothèque de doigts. Dans les deux cas, le système renvoie le résultat de la correspondance, succès ou échec [14].

II.4.4 Étape de comparaison d'empreintes digitales

Le système de vérification d'identité est basé sur la comparaison de deux ensembles de minuties (fichier "gabarit"), correspondants respectivement à deux doigts à comparer. Pour déterminer si deux ensembles de minuties extraits de deux images correspondent à des

empreintes du même doigt, il est nécessaire d'adopter un système de comparaison qui soit insensible à d'éventuelles translations, rotations et déformations qui affectent systématiquement les empreintes digitales [15]. A partir de deux ensembles de minuties extraites, le système est capable de donner un indice de similitude ou de correspondance qui vaut :

- 0 % si les empreintes sont totalement différentes.
- 100 % si les empreintes viennent de la même image.

Deux fichiers "gabarit" calculés à partir de la même empreinte ne donneront jamais 100% de ressemblance du fait des différences qui existent lors de l'acquisition de deux images (petites déformations ou déplacements), ils donneront cependant toujours un niveau élevé de similitude. La décision à partir de cet indice de similitude de savoir si deux empreintes sont issues du même doigt est une question purement statistique. Pour décider d'accepter la similitude entre deux "gabarits", il faut établir un seuil d'acceptation [16].

II.4.5 Installation de la bibliothèque de capteurs d'empreintes digitales Adafruit

Le moyen le plus simple de contrôler le module de capteur d'empreintes digitales avec l'Arduino consiste à utiliser la bibliothèque Adafruit pour ce capteur. Les étapes d'installation de la bibliothèque sont présentées dans ce qui suit :

1. La Bibliothèque utilisée a été télécharger par ce site Adafruit Fingerprint Sensor Library
2. Après le téléchargement il est nécessaire de décompresser le dossier .zip pour obtenir le dossier Adafruit-Fingerprint-Sensor-Library-master
3. Le dossier doit être déplacé vers le dossier des bibliothèques d'installation de votre IDE Arduino
4. Redémarrage d'Arduino IDE

II.4.6 Enregistrement d'une nouvelle empreinte digitale

Après avoir connecté le module de capteur d'empreintes digitales à l'Arduino, on doit suivre les étapes suivantes pour enregistrer une nouvelle empreinte digitale. Et s'assurer que nous avons bien la bibliothèque (Adafruit Fingerprint Sensor) précédemment,

1. Dans l'IDE Arduino, Fichier > Exemples > Bibliothèque de capteurs d'empreintes digitales Adafruit.
2. Téléchargement du code et ouverture du moniteur série à un débit en bauds de 9600.
3. On doit entrer un ID pour l'empreinte digitale. Comme il s'agit de notre première empreinte digitale, Ensuite, cliquer sur le bouton envoyer après avoir taper un numéro entre 1 et 127.

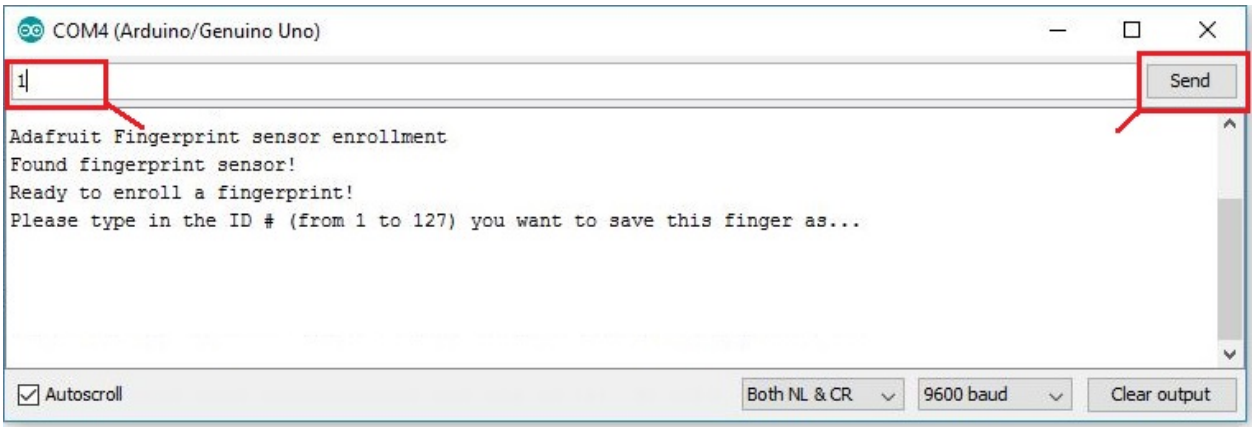


Figure II. 9: Le numéro ID du serial monitor

4. On place notre doigt sur le scanner et on suit les instructions sur le moniteur série.

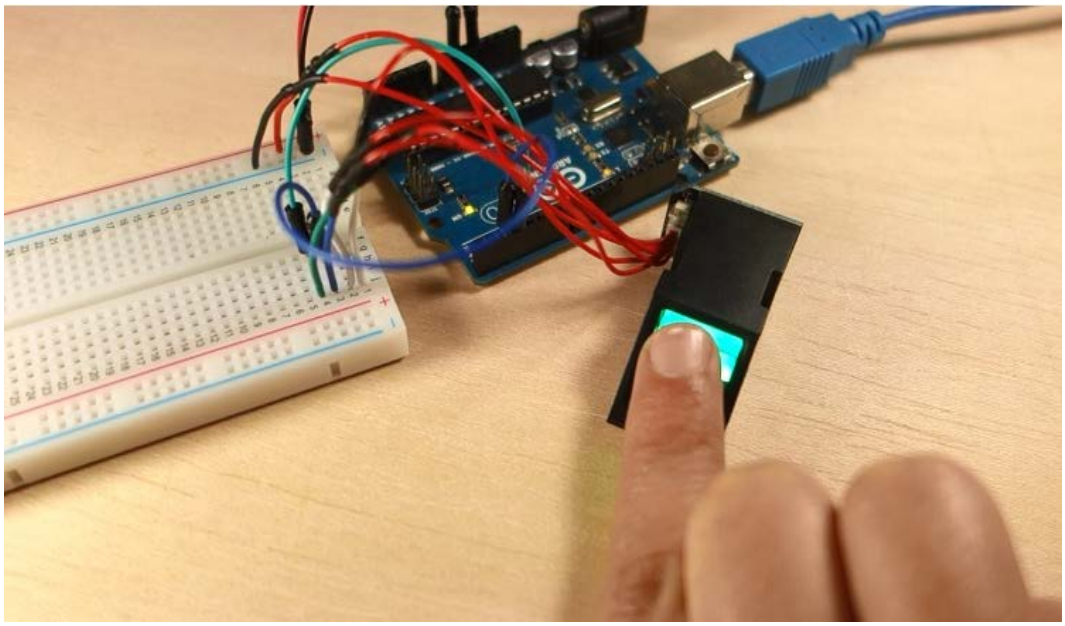


Figure II. 10: Emplacement du doigt sur le capteur

Il est obligatoire de placer deux fois le même doigt sur le scanner. Si on obtient le message " Impressions assorties ! ", comme indiqué ci-dessous, donc notre empreinte digitale a été enregistrée avec succès.

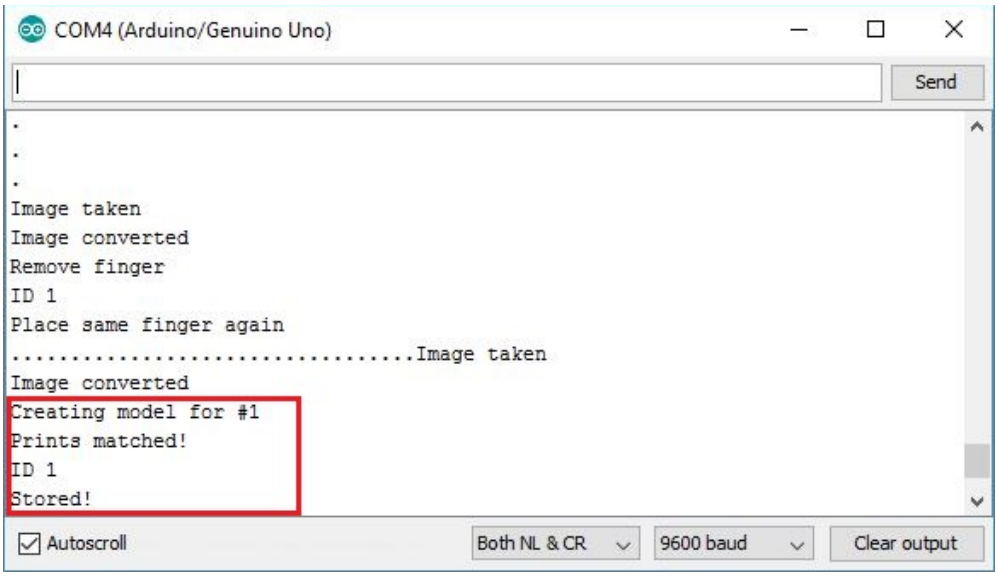


Figure II. 11: Empreinte enregistrée avec succès

II.4.6.1 La reconnaissance d'empreinte

On a déjà enregistré plusieurs empreintes digitales sur différents identifiants. Pour trouver une correspondance avec le capteur d'empreintes digitales, on suit les instructions suivantes :

1. Dans l'IDE Arduino, on accède au menu Fichier > Exemples > Bibliothèque de capteurs d'empreintes digitales Adafruit. Puis on va téléverser le code
2. On ouvre le moniteur série à un débit en bauds de 9600, et on va avoir ce message :

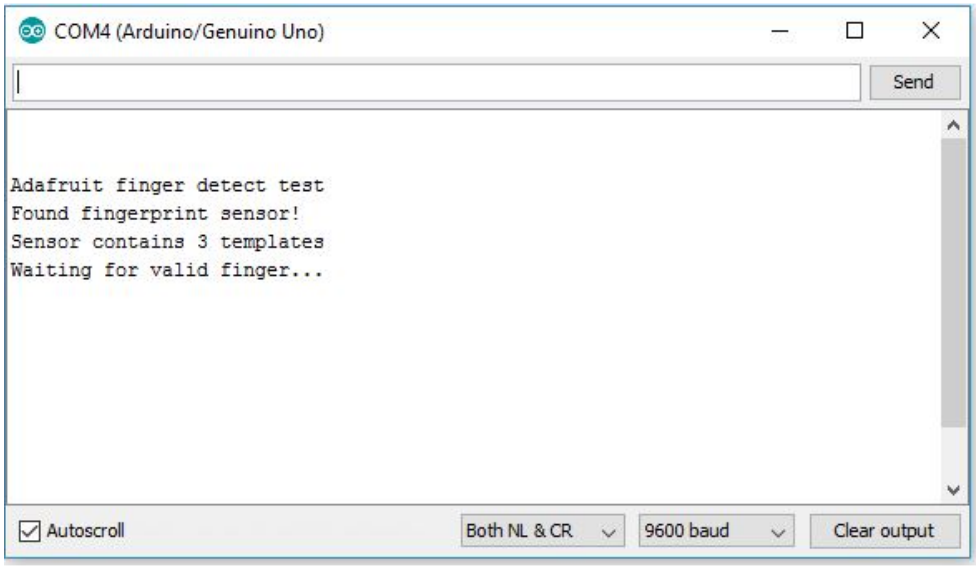


Figure II. 12: La reconnaissance d'empreinte

3. On place le doigt à identifier sur le scan.
4. Sur le moniteur série, on peut voir l'ID qui correspond à l'empreinte digitale.

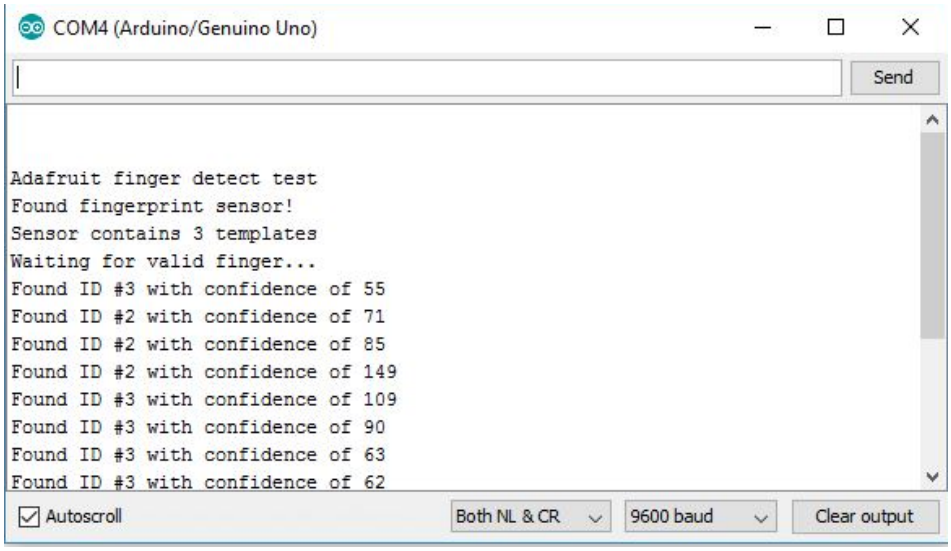


Figure II. 13: L'affichage de ID des empreintes autorisés

II.5 Unité de sortie et de communication (Afficheur LCD)

Un écran à cristaux liquides, est un module intelligent et compact qui nécessite peu de composants externes pour fonctionner correctement. Ils consomment une quantité relativement faible (1-5 mA), sont relativement bon marché et sont très faciles à utiliser.

Plusieurs présentoirs sont disponibles sur le marché et ne sont pas différents les uns des autres Non seulement les dimensions (1-4 lignes de 6-80 caractères), Caractéristiques techniques et leur tension de fonctionnement. Certains ont un rétro-éclairage publicité. Cette fonctionnalité utilise des LED montées derrière l'écran du module Cependant, cette lumière est gourmande en intensité (80-250 mA) [17].

Figure II. 14: Afficheur LCD et accroires associées

II.5.1 Brochage d'un afficheur LCD

Le brochage d'un écran LCD est "normalisé" avec 14 broches (ou 16 si l'écran est rétroéclairé) pour les "petits formats » [18].

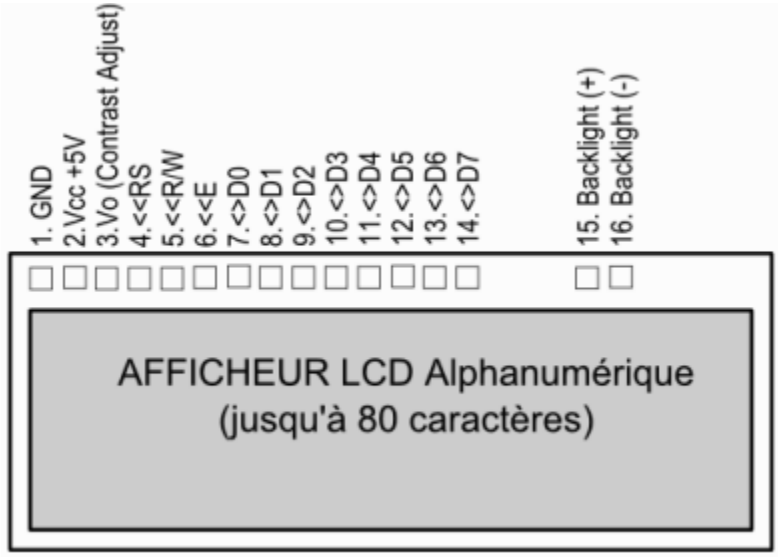


Figure II. 15: Brochage d'un écran LCD

Tableau II. 1 : Rôle et nom de chaque broche d'un afficheur LCD

Broche	Nom	Niveau	Fonction
1	GND	-	Masse
2	VCC	-	Alimentation positive (+5v).
3	V0	0-5V	Cette tension permet, en la faisant varier entre 0 et +5v, le réglage du contraste de l'afficheur.
4	RS	TTL	Sélection du registre grâce a cette broche, l'afficheur est capable de faire la différence entre une commande et une donnée. Un niveau bas indique une commande et un niveau haut indique une donnée.
5	RW	TTL	Lecture / écriture
6	E	TTL	Entrée de validation active sur front descendant. Le niveau haut doit être maintenue pendant au moins 450ns a l'état haut.
7	D0	TTL	Bus de données bidirectionnel 3 états (haute impédance lorsque E=0)
8	D1	TTL	
9	D2	TTL	
10	D3	TTL	
11	D4	TTL	
12	D5	TTL	

13	D6	TTL	
14	D7	TTL	
15	A	-	Anode rétro éclairage (+5v)
16	K	-	Cathode rétro éclairage (masse)

Tout projet qui nécessite tant de convivialité ou de contrôle pour l'utilisateur doit comporter un afficheur. En effet, celui-ci permet de manière très rapide de révéler n'importe quelle information qui pourrait être utile au programmeur ou à l'usager.

II.5.2 Principe de fonctionnement d'un écran LCD

L'afficheur LCD est constitué de deux polariseurs dont les directions de polarisation forment un angle de 90°, de chaque côté d'un sandwich formé de deux plaques de verre enserrant des cristaux liquides. À chacune des interfaces avec les cristaux liquides, une couche de polymère, généralement un polyamide, rainurée assure l'ancrage des molécules au repos [19].

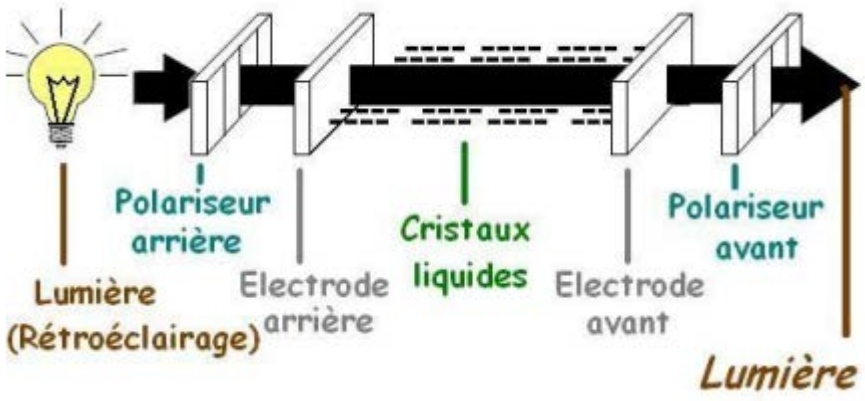


Figure II. 16: Principe de fonctionnement d'un écran LCD

II.6 PCF8574 (I2C)

C'est un Composants électroniques utilisé pour faciliter l'intégration avec la carte Arduino. Dans le cas où il s'agit d'un prolongateur des entrées et sorties pour le bus I2C, Le nom I2C vient de Circuit inter-intégré, Sa version 1.0 a été créée en 1992 par Philips. Puis un deuxième 2.1 viendrait en 2000 et aujourd'hui il est devenu un standard (à 100 kbit /s, bien qu'il autorise jusqu'à 3.4 Mbit / s maximum).

El I2C est un bus communication série bien connue. Il utilise un protocole de communication synchrone avec seulement 2 canaux (il y en a un troisième, mais il est couplé à une référence ou GND), en fait il est également connu sous le nom de TWI

- Un pour l'horloge (SCL).
- Autre pour les données (SDA) [20].

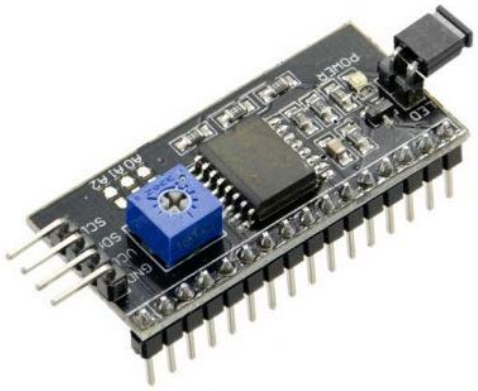


Figure II. 17: PCF8574 (I2C)

Cela implique que le **maître et esclave** ils envoient des données sur le même câble ou piste, qui est contrôlé par le premier qui est celui qui génère le signal d'horloge. Chacun des périphériques connectés au bus I2C aura une adresse unique attribuée, afin de diriger les transmissions. Mais il n'est pas nécessaire que l'enseignant soit toujours le même (multi-enseignant), c'est toujours lui qui initie le transfert [20].

II.7 Relais

Les relais électromécaniques sont des dispositifs de technologie électrique qui permettent de commuter des connexions électriques. Celui-ci permet d'envoyer des commandes de la partie commande vers la partie puissance de l'appareil électrique, et surtout, permet une isolation galvanique entre les deux parties [21].

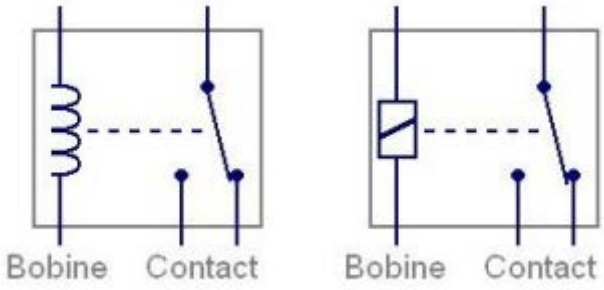


Figure II. 18: Symbole de relais

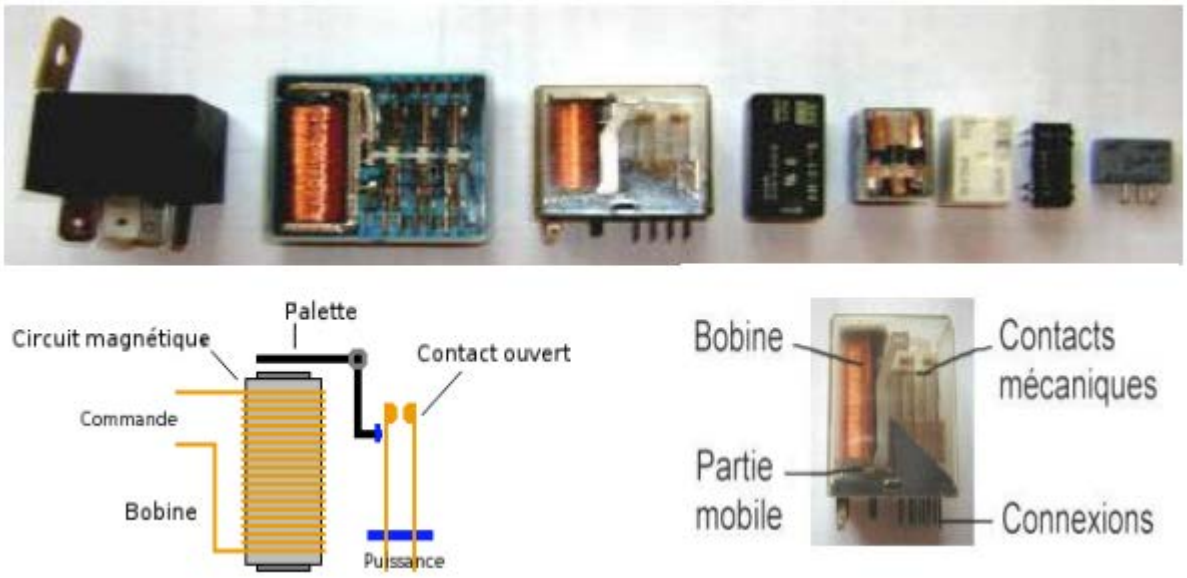


Figure II. 19: Schéma interne de relais

II.7.1 Avantages et inconvénients d'un Relais

Les avantages et les inconvénients d'un relais sont résumé comme suit :

1. **Avantage :**

- Capacité de commuter aussi bien des signaux continus qu'alternatifs sur une large gamme de fréquences.
- Fonctionnement avec une dynamique considérable du signal commuté.
- Aucun ajout de bruit ou de distorsion.
- Résistance de contact fermé très faible (il est moins facile de trouver des valeurs aussi faibles avec des composants électroniques)
- Résistance de contact ouvert très élevée (il est moins facile de trouver des valeurs aussi élevées avec des composants électroniques).

- Très grande isolation entre circuit de commande (bobine) et circuit commuté (contacts).
- Possibilité de résoudre des problèmes d'automatisme de façon parfois plus simple qu'avec un circuit électronique [22].

2. Inconvénient

- Elément de commande possédant une composante inductive non négligeable, provoquant une surtension importante lorsque le courant circulant dans la bobine est interrompu (loi de Lenz). Ce qui impose l'emploi d'au moins un composant de protection (une diode par exemple) pour protéger le circuit de commande si ce dernier est de type électronique.
- Présence de rebonds lors des commutations, le passage de l'état ON à l'état OFF (ou inversement) n'est pas "net". Le nombre de rebonds est en effet plus important quand ce courant de commande est bien inférieur ou bien supérieur à la valeur de courant nominal spécifiée par le fabricant.
- Compatibilité pas toujours assurée avec les circuits numériques, notamment pour les relais de forte puissance, qui peuvent nécessiter un circuit d'interface spécifique.
- Couplage capacitif entre les contacts pour les modèles multipolaires (à plusieurs pôles).
- Diminution de l'isolation à l'état ouvert à cause du couplage capacitif.
- Durée de vie faible si le nombre de commutation est important.
- Encombrement mécanique plus important pour les relais de moyenne et forte puissance, qu'il faut cependant comparer au transistors ou triacs munis de leur radiateur [22].

II.7.2 Principe de fonctionnement d’un Relais

Un courant de plusieurs dizaines de milliampères circule dans le circuit d'excitation Assez pour contrôler le relais. Lorsque le relais devient actif, les contacts qui étaient initialement en position de repos passeront en position. Tant que le courant circule dans le circuit d'excitation, il fonctionnera et restera dans cette position. Lorsque le circuit d'excitation est hors tension, les contacts reviennent en position de veille [23].

Figure II. 20: Principe de fonctionnement d'un Relais

II.8 Buzzer

Un Buzzer est un élément électromécanique ou électronique qui produit un son quand on lui applique une tension. Certains nécessitent une tension continue (Buzzers électromécaniques), d'autres nécessitent une tension alternative (transducteurs piézoélectrique) [24].

Figure II. 21: Buzzer 1. Électromécaniques, 2. piézo-électrique

Le son émis est simplement une vague de pression d'air variable. Ces ondes de pression provoquent une vibration de la membrane mince dans l'oreille et le cerveau interprète ces vibrations comme un son. Une échelle de décibels (dB) est utilisée pour décrire le niveau de pression acoustique [25].

II.9 La serrure électrique

La serrure électrique ne nécessite pas l'usage d'une clé, Elle rassemble l'ensemble des systèmes de verrouillage fonctionnant électriquement pour le verrouillage et le déverrouillage d'une porte. La serrure électrique est aujourd'hui fréquemment utilisée [26] :

- Sur des portes d'entrée d'immeuble,
- Sur des portes de chambre d'hôtel,
- Pour les voitures,
- Sur des portails et portillons.

II.9.1 Min serrure éélectromagnétique

Est une serrure électromagnétique de tiroir de porte de serrure nous permet d'ajouter un contrôle électrique de fermeture pour des projets Arduino, Raspberry ou tout simplement d'utiliser un interrupteur et une alimentation 12V pour contrôler la fermeture de petites portes ou couvercles, Le câble rouge est à raccorder au positif, le vert au négatif, Lors de la mise sous tension, le courant fera se rétracter la serrure et lorsqu'il n'y a plus de courant (0V), alors la serrure (ou plutôt son pêne) ressortira. L'application du courant permet donc l'ouverture [27].

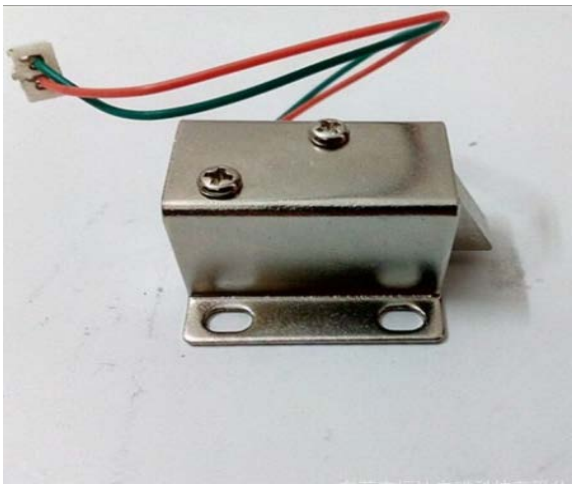


Figure II. 22: Serrure Électromagnétique

- **Spécifications :**
    1) Produit taille : 3.3x2.7x1.7 cm/1.3x1.06x0.67in
    2) Poids du produit : 35g
    3) Catégorie de produit : 6 V/12 V universel
- **Principe de fonctionnement**
    1) Puissance sure, la serrure rétracter, déverrouiller ;
    2) Hors tension, la serrure apparaît, ferme la serrure
- **Application principe**
    1) Déverrouiller : contrôle la tension ou hors tension
    2) Serrure : pousser la porte, serrure automatiquement verrouillée
- **Champ d'application**

Express armoires, casiers, boîtes à journaux, armoires de rangement, étagères de rangement, classeurs, classeurs, tiroirs, boîte de compteur, casier, intensive armoires et autres produits, et est largement utilisé dans les usines, mines, écoles, banques, troupes, les prisons, tribunaux, hôtels, fermes, centres de bain [28].

II.10 La diode électroluminescente LED

Le mot LED est l'acronyme de Light Emitting Diode (Diode Electroluminescente en français). Le symbole de la LED ressemble à celui de la diode mais on y a ajouté deux flèches sortantes pour représenter le rayonnement lumineux émis. [29]

Figure II. 23 Symbole de la LED.

II.11 Présentation de l'Espace de développement Intégré software (EDI) Arduino

Dans cette section, nous allons décrire l'espace de développement de l'Arduino.

II.11.1. Software de l'Arduino

Le logiciel Arduino (EDI) est facile à utiliser pour les débutants, mais suffisamment flexible pour que les utilisateurs avancés en profitent également. Pour les enseignants, il est basé sur l'environnement de programmation de traitement, de sorte que les étudiants qui apprennent à programmer dans cet environnement seront familiarisés avec le fonctionnement de l'IDE Arduino.

Le logiciel Arduino est publié sous forme d'outils open source, disponible pour extension par des programmeurs expérimentés. Le langage peut être étendu via les bibliothèques C++, et les personnes souhaitant comprendre les détails techniques peuvent passer d'Arduino au langage de programmation AVR C sur lequel il est basé. De même, nous pouvons ajouter du code AVR-C directement dans les programmes Arduino si en souhaite. [1]

L'interface EDI permet d'interagir et de se connecter avec la carte Arduino et ESP 32 cam

Le logiciel Arduino a pour fonctions principales (Mehdi DOUNAS,2021) :

- De pouvoir écrire et compiler des programmes pour la carte Arduino
- De se connecter avec la carte Arduino pour y transférer les programmes
- De communiquer avec la carte Arduino

Cet espace de développement intégré (EDI) est dédié au langage Arduino et à la programmation de la carte Arduino :

- Une BARRE DE MENUS comme pour tout logiciel une interface graphique (GUI),
- Une BARRE DE BOUTONS qui donne un accès direct aux fonctions essentielles du logiciel et fait toute sa simplicité d'utilisation,
- Un EDITEUR (à coloration syntaxique) pour écrire le code de vos programmes, avec onglets de navigation,
- Une ZONE DE MESSAGES qui affiche indique l'état des actions en cours,
- Une CONSOLE TEXTE qui affiche les messages concernant le résultat de la compilation du programme

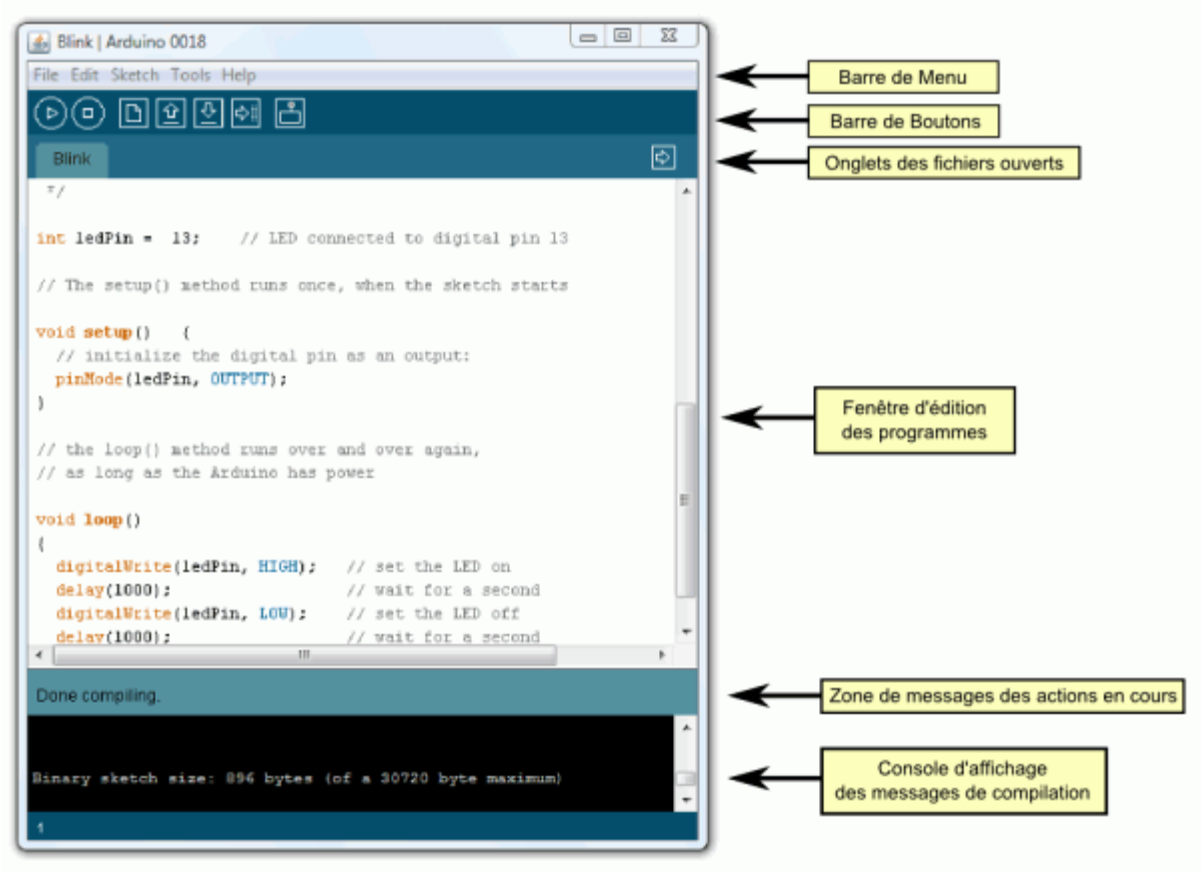


Figure II. 24: Présentation des éléments de l'ARDUINO software. (Jean- Noël ,2006)

Le logiciel Arduino intègre également :

• Un TERMINAL SERIAL (fenêtre privée) permet d'afficher les messages texte reçus de la carte Arduino et d'envoyer des caractères à la carte Arduino. Cette fonction facilite le débogage du programme, permettant l'affichage de l'état des variables, des résultats de calcul ou de conversion analogique-numérique sur l'ordinateur : un élément essentiel pour améliorer, tester et réparer le programme.

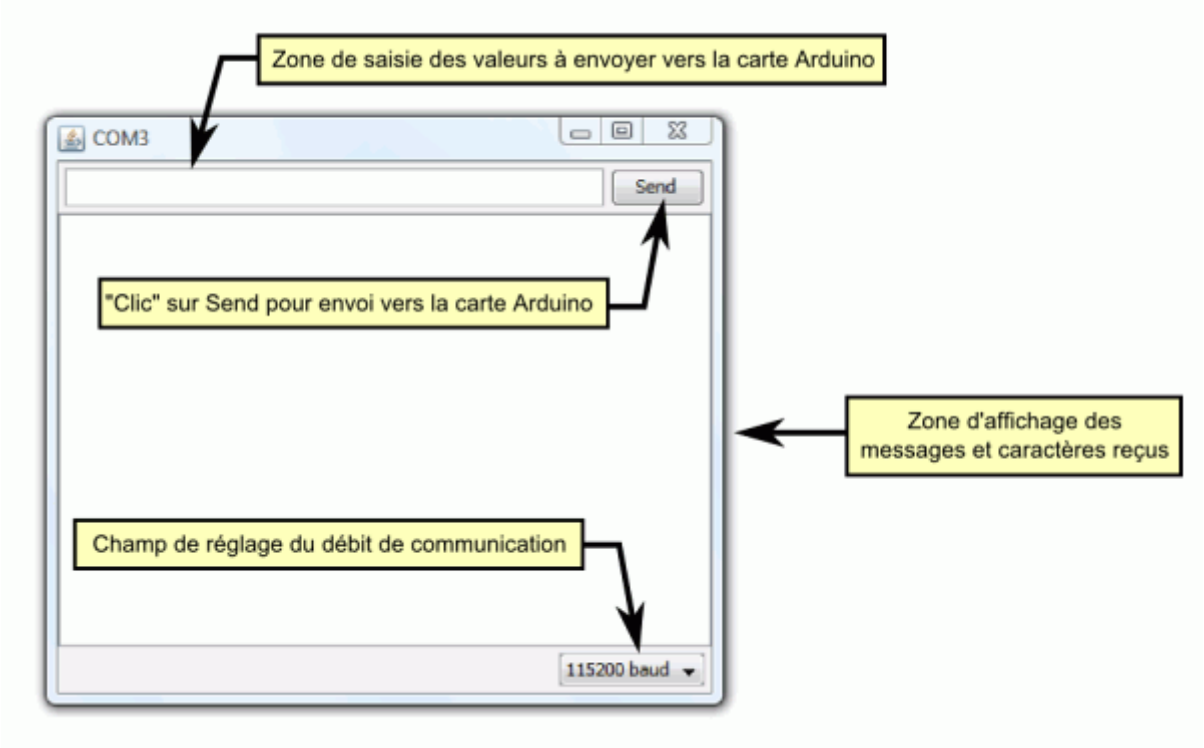


Figure II. 25: Module TERMINAL SERIE.[30]

II.11.2 Description de la structure d'un programme

Le programme utilisateur Arduino est une série d'instructions de base sous la forme de texte, lire ligne par ligne de haut en bas (TAKHA AIMEN,2020).

La structure minimale se compose de trois étapes consécutives :

- Définition des constantes et des variables :

Une déclaration (variable, constante, indicateur d'utilisation bibliothèque, etc.).

-Paramétrage des entrées et sorties :

A paramètre (initialisation) cette section n'est lue qu'une seule fois, elle comprend fonctions exécutées au démarrage (en utilisant des broches comme entrées ou sortie, démarrage, etc.)

-Interactions et comportements de programmation :

Une boucle : cette partie se lit en boucle ! C'est là que les fonctions menées

En plus de cette structure minimale, on peut ajouter :

Subprocess" ou "process" peut être appelé à tout moment dans la boucle, ce qui est utile pour créer des morceaux de code répétitifs.

Les rappels sont des fonctions qui sont automatiquement rappelées d'une bibliothèque.

Figure II. 26: Fenêtre graphique de l'EDI qui représente le programme de base.[30]

II.11.2.1 Description détaillée des parties

❖ **Définition des variables et constantes**

Dans cette section, nous déclarons les éléments qui sont utilisés tout au long du programme : constantes (statiques) et variables (dynamiques). Ce sont des emplacements de mémoire utilisés pour stocker des données (valeurs) qui peuvent être utilisées plus tard dans le programme. (C. Tavernier. 2019)

❖ **Variable** : une variable peut également représenter des données à lire ou à envoyer l'un des ports analogiques ou numériques, une étape de calcul pour lier ou traiter des données, plutôt

que le nombre "physique" de ces entrées ou sorties. Par conséquent, une "variable" n'est pas seulement un paramètre variable dans le programme.

- **Constante :** Une constante est une variable dont la valeur ne peut pas être exécuter un programme.
- **Différents types de données :** En programmation informatique, un type de données, ou simplement une entrée, définit les valeurs que peut prendre une donnée, ainsi que les opérateurs qui peuvent lui être appliqués.
- **Fonction principale :** void setup () Cette fonction n`est exécutée qu`une seule fois au début du programme. Elle donne la permission de configurée les entres et les sorties de la carte. Toutes les broches numériques de l'Arduino peuvent être configure en entrées ou en sortie.
- **Fonction de boucle** : void Loop () Cette fonction Loop () fait exactement ce que son nom suggère et se répète en continu, permettant à votre programme de s'exécuter. Dans cette boucle, nous définissons l'opération. La fonction Loop () est obligatoire, même vide, dans tous programme.

II.11.3 Téléversement du programme

Avant d'envoyer le fichier (.hex) dans la carte ESP 32 cam et l Arduino UNO, il est nécessaire de sélectionner le type de la carte (ESP 32) ainsi que le numéro de port USB attribué à la carte. (TAKHA AIMEN,2020)

II.11.3.1 Les étapes de téléversement du programme

Une simple opération de chaîne doit être suivie pour obtenir le code dans la carte de came Arduino UNO ou ESP 32 via le port USB(Abdelbasset,2015).

- Concevoir ou ouvrir un programme existant à l'aide du logiciel Arduino IDE
- Tester ce programme avec le logiciel Arduino (compile).
- Si une erreur est signalée, le programme devra être modifié.
- Le programme est chargé sur la carte.
- L'ensemble électronique est câblé.
- L'exécution du programme est automatique après quelques secondes.
- La carte est alimentée par port USB ou secteur libre.
- Vérification que le montage fonctionne.

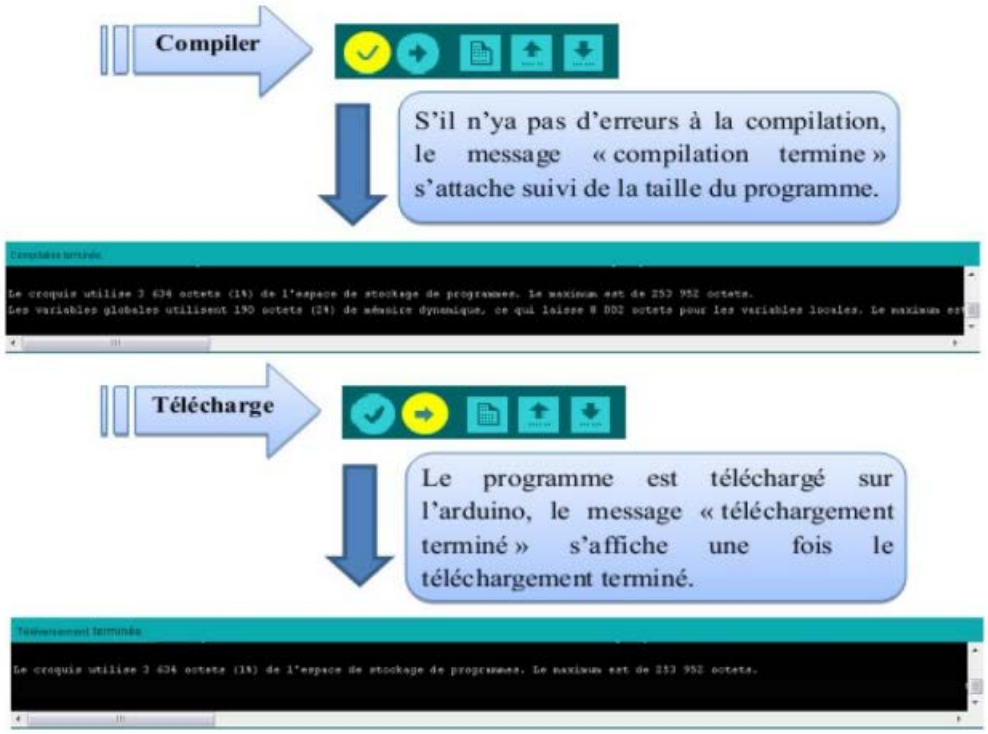


Figure II. 27: Les étapes de téléchargement du code. (TAKHA AIMEN,2020)

II.12 Bibliothèques utilisées

Les bibliothèques utilisées sont :

II.12.1 La bibliothèque ESP32

Avant d'ajouter la bibliothèque ESP32 il faut ajouter le lien de la bibliothèque pour pouvoir la télécharger comme le montre la figure ci-dessous : [31]

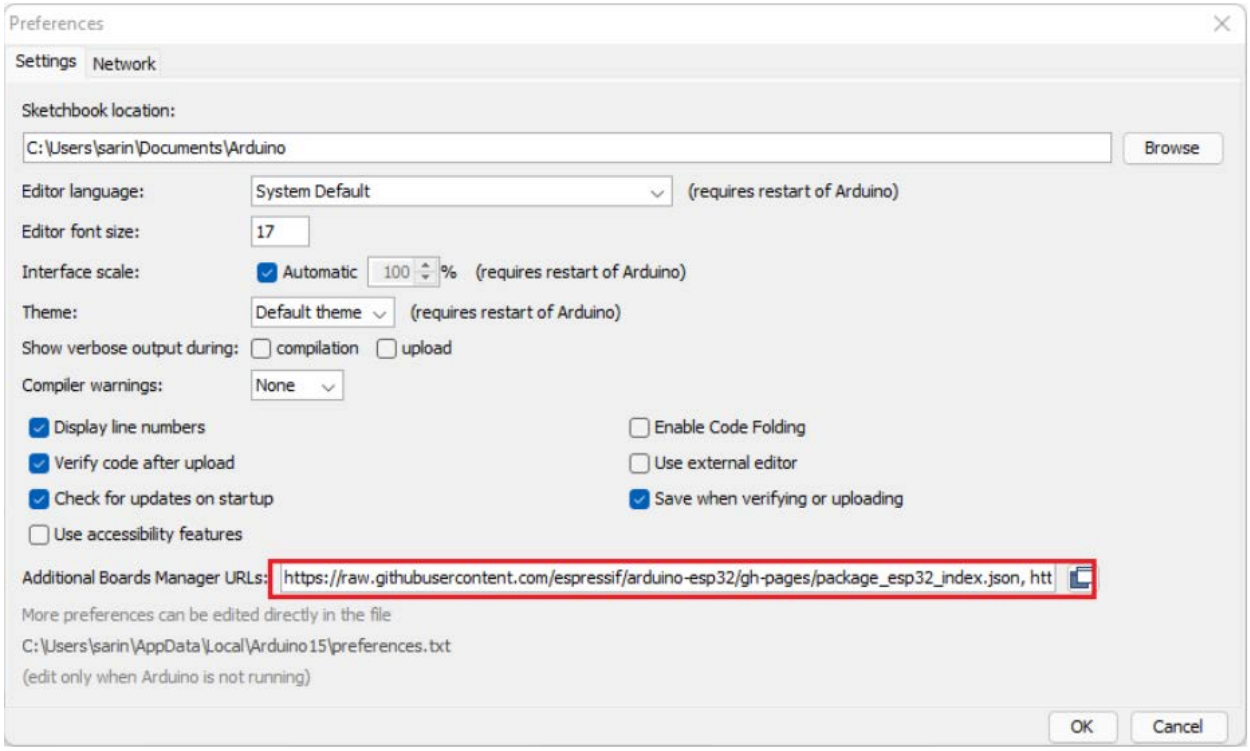


Figure II. 28: Les étapes pour ajouter le lien de la bibliothèque.[31]

Après avoir ajouté le lien de la bibliothèque il faut télécharger la version 1.0.4 comme le montre la figure suivante :

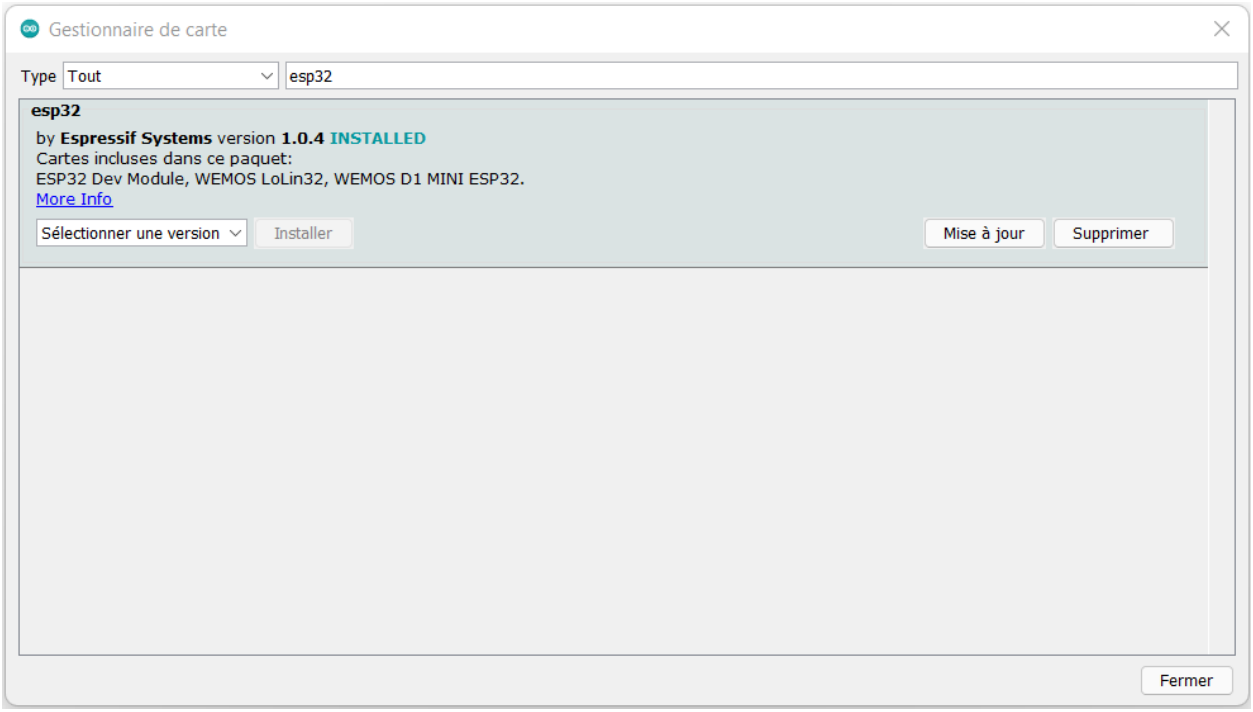


Figure II. 29: Installation de la bibliothèque ESP32

II.12.2 La bibliothèque Arduinowebsockets

Arduinowebsockets est une bibliothèque permettant d'utiliser des fonctionnalités comme :

- Cadre de texte
- Trame binaire
- Connexion fermer
- Ping
- Pong
- Cadre de continuation

Elle permet aussi la prise en charge de notre matériel puisque nous utilisant une carte ESP 32 cam et Arduino UNO, le matériel pris en charge est le suivant [32] :

- ESP 8266
- ESP 32 cam
- ESP 31B
- Particule avec STM32 ARM Cortex M3
- ATmega328 avec Ethernet Shield (succursale ATmega)
- ATmega328 avec enc28j60 (branche ATmega)
- ATmega2560 avec Ethernet Shield (succursale ATmega)
- ATmega2560 avec enc28j60 (branche ATmega).

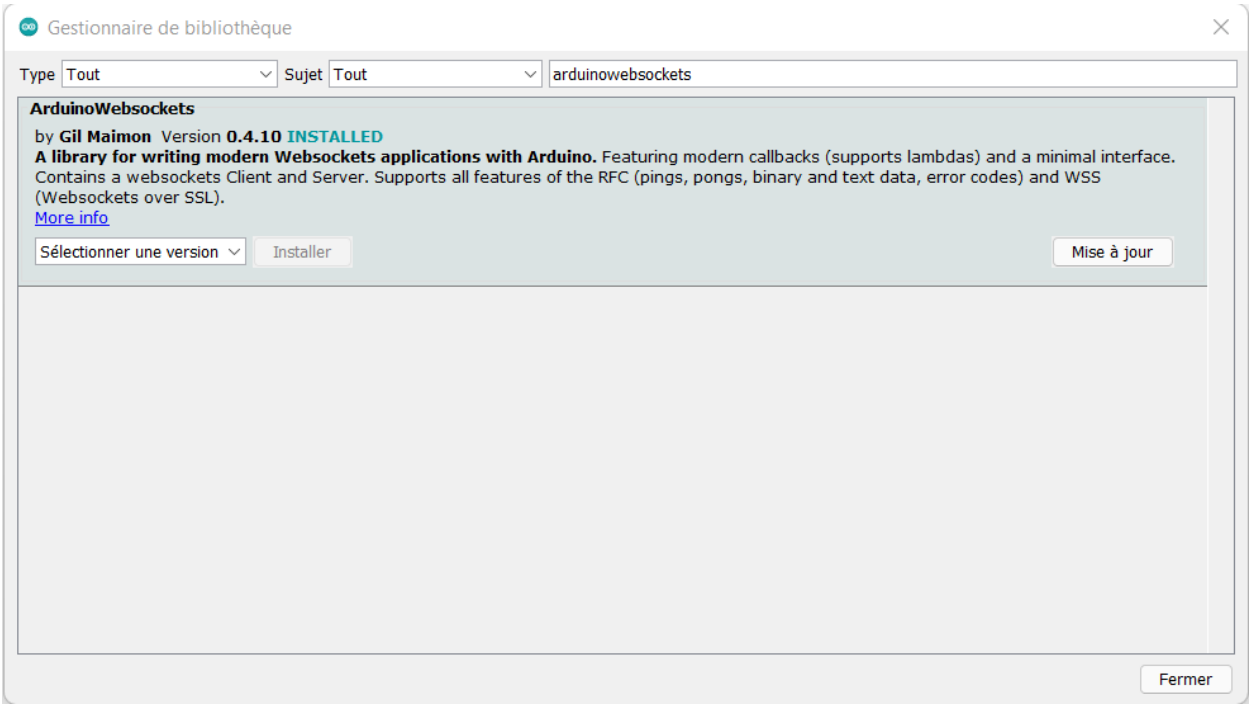


Figure II. 30: Bibliothèque Arduinowebsockets

II.12.3 EEPROM

Les microcontrôleurs de la carte basés sur Arduino et Genuino AVR disposent d'EEPROM : mémoire dont les valeurs sont stockées lorsque la carte est éteinte (comme petit disque dur). Cette bibliothèque vous permet de lire et d'écrire ces octets. Les microcontrôleurs pris en charge sur différentes cartes Arduino et Genuino ont nombre différent d'EEPROM : 1024 octets sur ATmega328P, 512 octets sur ATmega168 et ATmega8, 4 Ko (4096 octets) sur ATmega1280 et ATmega2560. Les cartes Arduino et Genuino 101 disposent d'un espace EEPROM émulé de 1024 octets, Pour utiliser cette bibliothèque de EEPROM : **Include <EEPROM.h>**

II.13 Les configuration de la carte ESP 32 cam

Il ya plusieurs configurations à faire avant de commencer la reconnaissance faciale pour cela faut suivre les étapes suivantes :

La première étape, il faut choisir le type de la carte utilisée (ESP32 Wrover) comme le montre la figure ci-dessous :

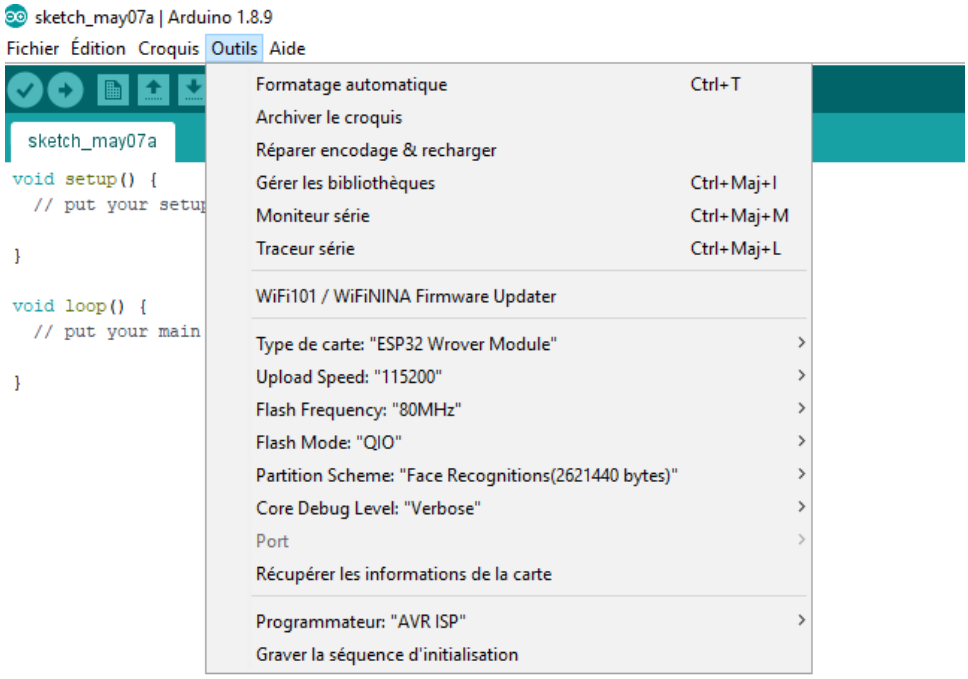


Figure II. 31: Le type de carte utiliser

II.14 HTML

HTML (HyperText Markup Langage) n'est pas un langage de programmation : c'est un langage de balisage utilisé pour indiquer au navigateur comment structurer les pages Web visitées. Cela peut être aussi complexe ou aussi simple que le souhaite le développeur Web. HTML se compose d'une série d'éléments que vous pouvez encadrer, envelopper ou marquer différentes parties de votre contenu pour les faire apparaître ou se comporter d'une certaine manière. L'habillage des balises peut transformer un petit élément de contenu en un lien vers une autre page sur le Web, mettre des mots en italique, etc. Prenons par exemple la phrase suivante : [33]

```
Mon chat est très grincheux
```

Figure II. 32: Exemple d'un texte avec le langage HTML.[33]

Si nous voulons que la ligne reste ainsi, nous pouvons dire que c'est un paragraphe en l'enveloppant avec un élément de paragraphe (<p>) :

```
<p>Mon chat est très grincheux</p>
```

Figure II. 33: représente comment rédiger un paragraphe dans un HTML

Ce langage permet aussi de crée une interface graphique sur une page web et d'interagir avec cette interface comme le montre la figure II.33 suivantes :

Figure II. 34: exemple d'une interface graphique sur un navigateur web.[33]

II.14.1 Interface graphique avec HTML

Un système de contrôle d'accès basé sur la reconnaissance faciale avec l'esp32cam et l'IDE Arduino, mais pour donner l'autorisation pour ouvrir la porte à l'individu il faut une interface qui aide à ajouter et supprimer les personnes qui sont autorisée ou pas à ouvrir la porte.

Cette interface est montrée sur la figure ci-dessous ; elle contient plusieurs options :

- **L'espace blanc** permet d'écrire le nom de la personne,
- Le bouton **caméra de flux** permet de passer en mode surveillance

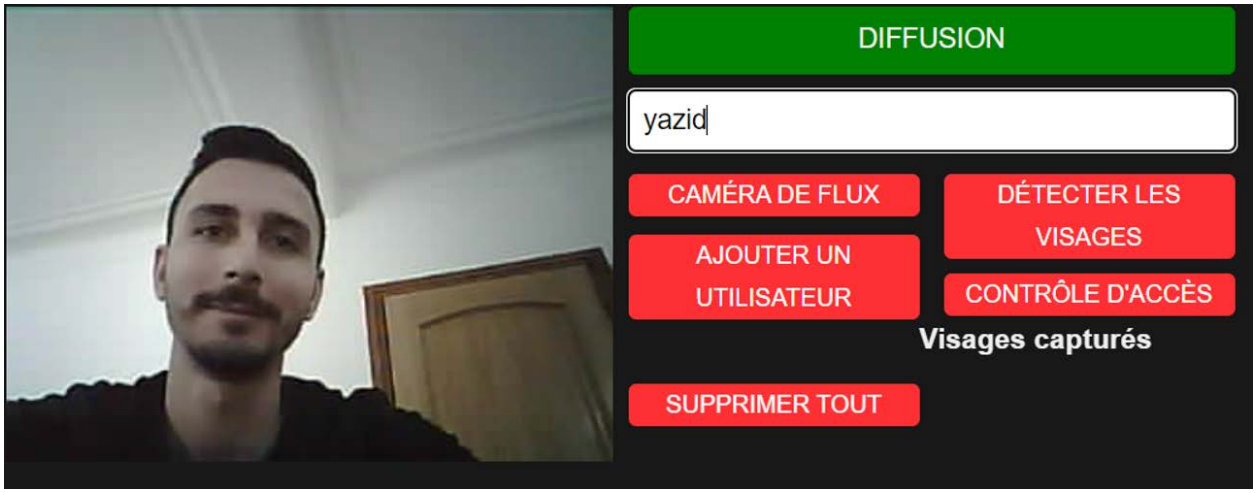


Figure II. 35: Mode de diffusion

Le deuxième mode permet de passer en mode détection des visages pour pouvoir ajouter un nouvel utilisateur ou contrôler l'accès comme le montre la **figure II.35** suivantes :

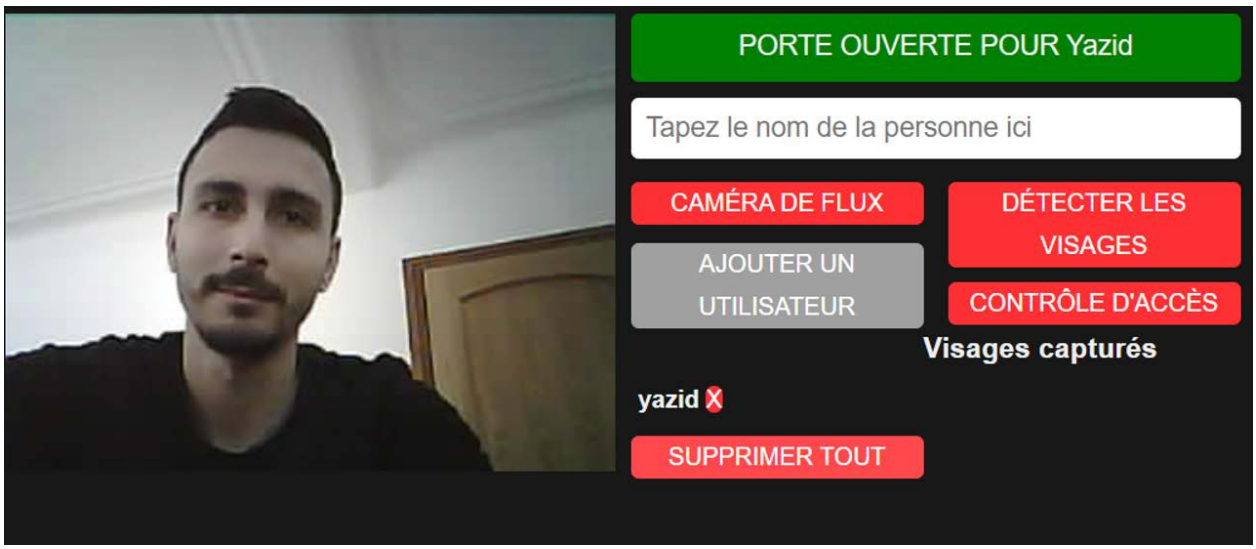


Figure II. 36: Mode détection des visages

II.15. Conclusion

Au cours de ce chapitre nous avons expliqué le contexte et présenté les logiciels et matériels nécessaires pour la réalisation du projet.

La conception, la présentation des organigrammes pour la réalisation du système ainsi que les résultats des différents tests effectués feront l'objet du prochain chapitre.

Bibliographie

(Abdelbasset, 2015) Krama Abdelbasset Gougui Abdelmoumen Etude et réalisation d'une carte de contrôle par Arduino via le système Android, Université Kasdi Merbah Ouargla 2015.

(Jean- Noël, 2006) Jean- Noël, « livret Arduino en français », Centre de ressources art sensitif en 2006.

(Mehdi DOUNAS, 2021) Mehdi DOUNAS, « Conception d'un système de pointage biométrique pour L'Institut Algérien du Pétrole IAP », Mémoire de Master, Université M'Hamed Bougera de Boumerdès, 2021.

(TAKHA AIMEN,2020) TAKHA AIMEN, « Traqueur de localisation en utilisant GSM SIM800 et Arduino », Mémoire de Master UNIVERSITE MOHAMED BOUDIAF-M'SILA, 2020.

(Tavernier, 2019) C. Tavernier. Arduino-2e éd. : Maitrisez sa programmation et ses cartes d'interface (Shields). Dunod, 2019.

Webographie

[1] « Arduino » [En ligne]. Disponible sur : https://www.arduino.cc/en/Guide/Introduction Consulté le 24/04/2022.

[2] « gotronic » [En ligne]. Disponible sur : https://www.gotronic.fr/art-carte-arduino-uno-12420.htm, Consulté le 24/04/2022.

[3] « Techmania » [Enligne]. Disponible sur : http://www.techmania.fr/arduino/Decouverte_arduino.pdf, Consulté le 24/04/2022.

[4] « gotronic » [Enligne]. Disponible sur : https://www.gotronic.fr/art-carte-arduino-uno-12420.htm#:~:text=Avis-,La%20carte%20Arduino%20Uno%20est%20bas%C3%A9e%20sur%20un%20ATMega328%20cadenc%C3%A9,une%20s%C3%A9rie%20de%20modules%20compl%C3%A9mentaires , Consulté le 24/04/2022.

[5] « Wikipédia » [En ligne]. Disponible sur : https://fr.wikipedia.org/wiki/Arduino Consulté le 06/05/2022.

[6] « pdfprof » [En ligne]. https://pdfprof.com/PDF_Doc_Telecharger_Gratuits.php?q=-16PDF81436-Arduino+UNO+Schematic, Consulté le 25/04/2022.

[7] « materielgratuit » [En ligne]. Disponible sur : https://www.hwlibre.com/fr/cam%C3%A9ra-esp32/ Consulté le 27/04/2022.

[8] « gotronic » [En ligne]. Disponible sur : https://www.gotronic.fr/blog/guides/utilisation-du-module-eps32-cam-avec-arduino/,Consulté le 24/04/2022.

[9] « électronique amateur » [En ligne]. Disponible sur : http://electroniqueamateur.blogspot.com/2020/01/esp32-cam-premiere-utilisation-avec.html,Consulté le 24/04/2022.

[10] « technore view » [En ligne]. Disponible sur : https://technoreview85.com/how-to-program-esp-32-cam-using-arduino-uno-board/ Consulté le 06/05/2022.

[11] « techno-tutos » [En ligne]. Disponible sur : https://www.e-techno-tutos.com/2021/01/01/esp32-cam/ Consulté le 06/05/2022.

[12], « ehub247, software consultant » [En ligne]. Disponible sur : https://ehub247.com.ng/guide-to-fingerprint-sensor-module-with-arduino-fpm10a/ Consulté le 11/05/2022.

[13] « Art of circuit » [En ligne]. Disponible sur : https://artofcircuits.com/product/fpm10a Consulté le 08/05/2022.

[14] « Fingerprint identification module » [En ligne]. Disponible sur : https://cdn-shop.adafruit.com/datasheets/ZFM+user+manualV15.pdf Consulté le 22/05/2022.

[15], « Biométrie en ligne » [En ligne]. Disponible sur : https ://www.biometrie-online.net/, Consulté le 19/05/2022.

[16], « Biométrie en ligne » [En ligne]. Disponible sur : https://www.biometrie-online.net/technologies/empreintes-digitales Consulté le 29/05/2022.

[17], « Les afficheurs à cristaux liquides » [En ligne]. Disponible sur : https://www.aurel32.net/elec/lcd.php Consulté le 1/05/2022.

[18], « Les dessoudures de l'extrême » [En ligne]. Disponible sur : https://dessoudeurs-ex.lebonforum.com/t17-initiation-pic-afficheur-lcd Consulté le 06/05/2022.

[19], « fr.scribd.com » [En ligne]. Disponible sur : https://fr.scribd.com/doc/35887890/Les-Afficheurs-LCD Consulté le 06/05/2022.

[20], « Matériel gratuit » [En ligne]. Disponible sur : https://www.hwlibre.com/fr/pcf8574/

[21], « electrosup » [En ligne]. Disponible sur : http://www.electrosup.com/relais_electromecanique.php Consulté le 30/04/2022.

[22], « sonelec-musique.com » [En ligne]. Disponible sur : https://www.sonelec-musique.com/electronique_theorie_relais.html Consulté le 02/05/2022.

[23], « Synthese_relais » [En ligne]. Disponible sur : http://gilles.berthome.free.fr/02-Syntheses/F_Transmision_info/Synthese_relais.pdf Consulté le 09/05/2022.

[24], « sonelec-musique.com » [En ligne]. Disponible sur : https://www.sonelec-musique.com/electronique_theorie_buzzers.html Consulté le 30/04/2022.

[25], « Piezoelectric sound components » [En ligne]. Disponible sur : http://www.aurelienr.com/electronique/piezo/applic.pdf Consulté le 06/05/2022.

[26], « Ooreka-MAISON » [En ligne]. Disponible sur : https://serrure.ooreka.fr/comprendre/serrure-electrique Consulté le 14/05/2022.

[27], « EUROMAKERS » [En ligne]. Disponible sur : https://euro-makers.com/fr/huisserie/1866-serrure-electrique-9v-12v-arduino-29mm-3701172908091.html Consulté le 18/05/2022.

[28], « POWERTECH » [En ligne]. Disponible sur : https://powertech-dz.net/products/single/min-serrure-electromagnetique-12v-035a-vente-composants-electronique-blida-algerie-644

[29] « positron libre » [En ligne]. Disponible sur : https://www.positronlibre.com/cours/electronique/diode/led/led.php Consulté le 05/05/2022.

[30] « mon-club-elec » [En ligne]. Disponible sur : http://www.mon-club-elec.fr/pmwiki_reference_arduino/pmwiki.php?n=Main.DebuterPresentationLogiciel Consulté le 06/05/2022.

[31] « randomnerdtutorials » » [En ligne]. Disponible sur : https://randomnerdtutorials.com/installing-the-esp32-board-in-arduino-ide-windows-instructions/ Consulté le 10/05/2022.

[32] « GitHub » [En ligne]. Disponible sur : https://github.com/Links2004/arduinoWebSockets/blob/master/README.md Consulté le 15/05/2022.

[33] « developer.mozilla » [En ligne]. Disponible sur : https://developer.mozilla.org/fr/docs/Learn/HTML/Introduction_to_HTML/Getting_started Consulté le 20/05/2022.

[34] robotzero1, « esp32cam-access-control », [En ligne]. Disponible sur : https://github.com/robotzero1/esp32cam-access-control consulte le : 2022/04/30

Chapitre III

Mise en œuvre du système de control d'accès

III.1 Introduction

Dans ce chapitre nous allons décrire l'aspect pratique de notre travail, pour la réalisation de notre projet destiné au contrôle d'accès par biométrie (empreinte et visage), nous nous concentrerons sur l'aspect pratique et la réalisation de notre maquette. Nous parlerons également sur l'environnement de développement et nous présenterons l'interface de notre projet.

III.2 Partie de la reconnaissance faciale

III.2.1 Logiciels et langages utilisés

Pour la conception de notre module de la reconnaissance faciale nous avons utilisé les logiciels et les langages suivants :

III.2.1.1 Arduino IDE

Il s'agit d'un espace de développement intégré pour l'écriture et le téléversement des programmes ou algorithmes sur la carte ESP32CAM.

III.2.1.2 Navigateur web utilisé

Dans notre cas nous avons utilisé le navigateur google chrome pour notre interface web, Le navigateur web google chrome est un navigateur développé par google en 2008, basé sur le projet open source Chromium qui fonctionne sur Mac, Windows, Android, Linux et IOS.

III.2.1.3 HTML

Pour l'affichage de l'interface sur le navigateur web nous avons utilisé le langage HTML qui permet de créer une interface ou un site web sur n'importe quelle navigateur web.

III.2.2 Montage de connexion de la carte ESP32CAM

La première étape consiste à tester la carte avec le programmateur ESP32-CAM-MB.

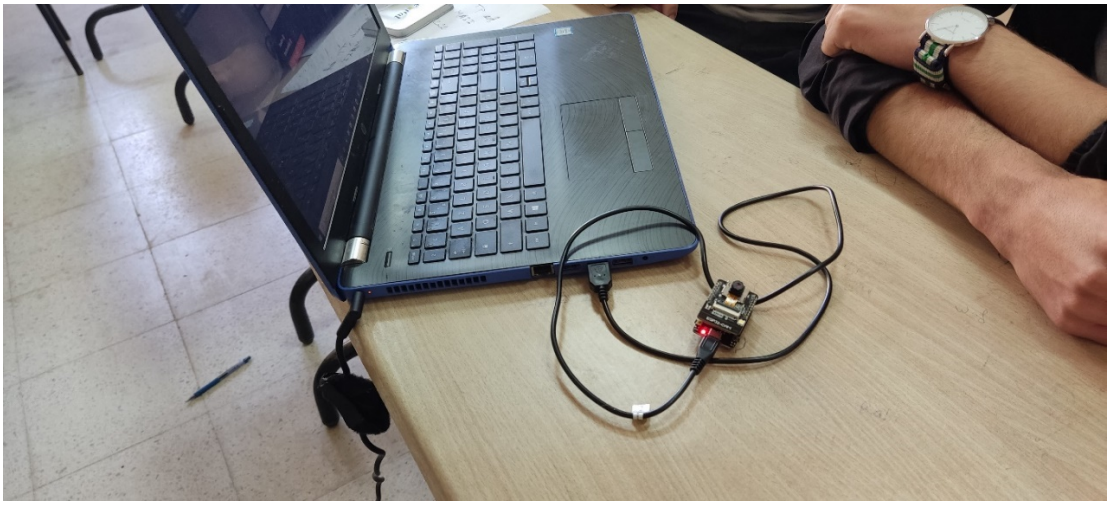


Figure III 1: Montage à base de esp32cam-MB

Après avoir vérifié le code Arduino, le programme est téléversé dans la carte ESP32CAM. Le programme Arduino à téléverser dans la carte est représenté dans le diagramme sur la **Figure III.2** ci-dessous :

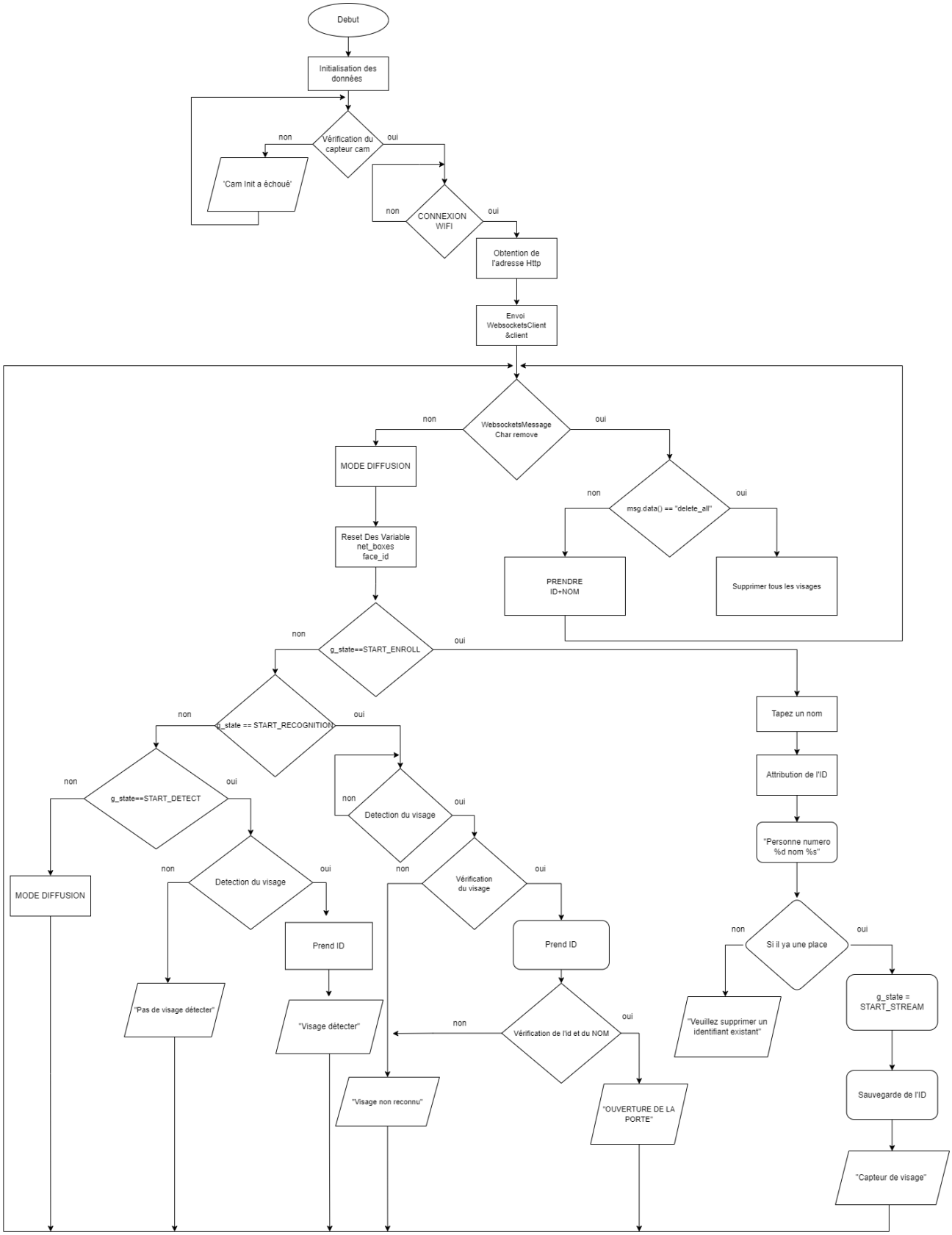


Figure III 2: Organigramme de la reconnaissance facial

1- Après le téléversement du code Arduino, la carte ESP32CAM se connecte au réseau wifi.

2- L'étape suivante consiste à ouvrir le serial monitor de l'Arduino IDE, puis il faut appuyer sur le bouton Reset de la carte ESP32CAM.

3- Ensuite la fenêtre suivante s'affiche pour montrer la connexion au réseau wifi et son adresse IP.

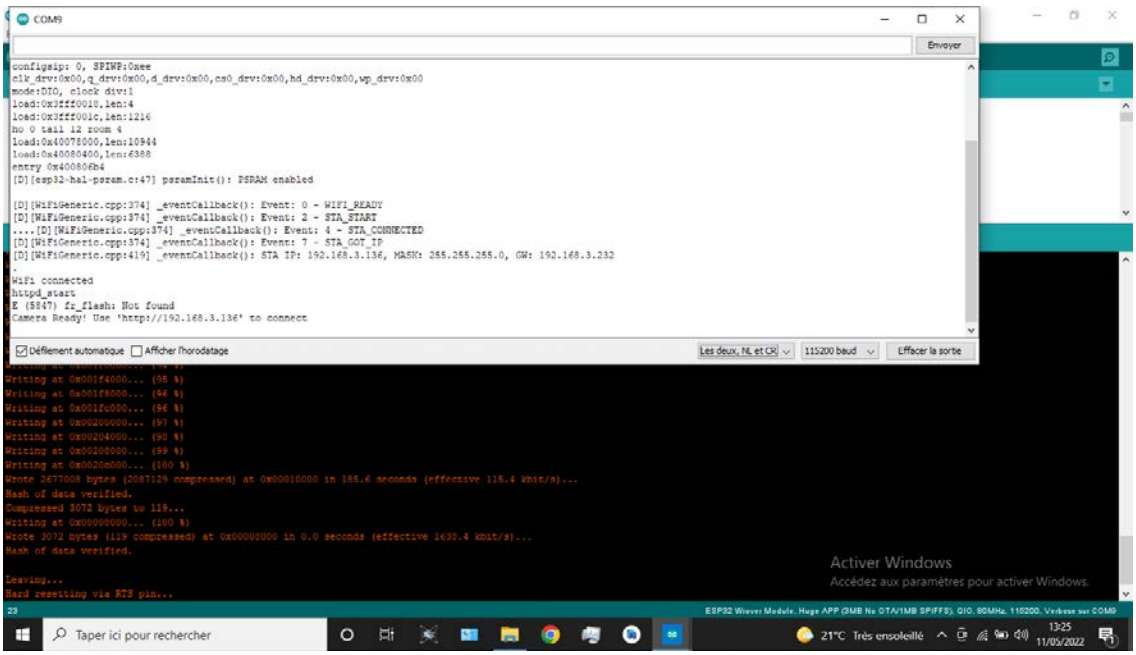


Figure III 3: Etablissement de la connexion wifi avec la carte ESP32cam

Ensuite, une copie de l'adresse IP donnée par ESP32CAM est faite dans le navigateur web. Après la validation, l'interface suivante s'affiche :

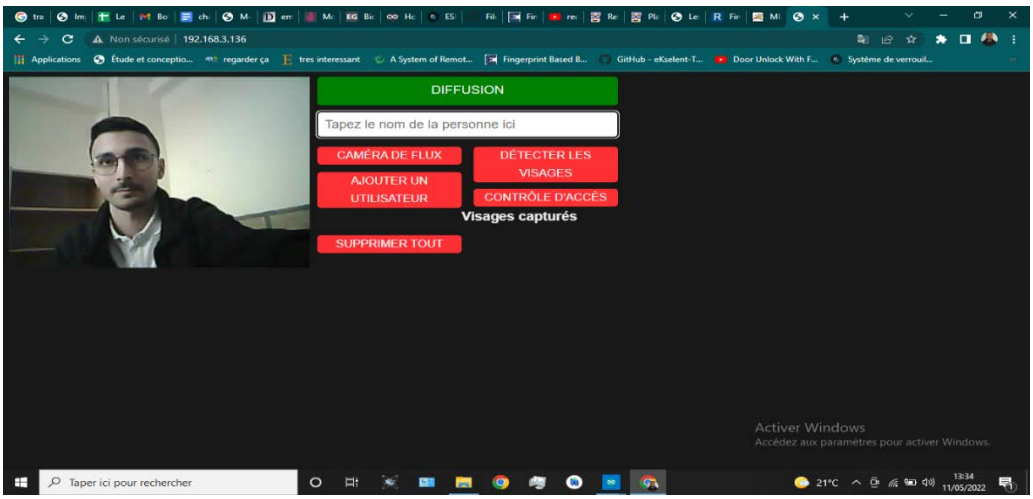


Figure III 4: Interface de la plateforme

III.2.3 Création de la liste des gens autorisés

La première étape consiste à ajouter les noms des gens autorisés à accéder. Pour cela on commence par l'écriture du nom de l'individu autorisé, et d'orienter son visage vers la caméra. Ensuite on clique sur le bouton « **détecter le visage »**, enfin on clique sur le bouton « **ajouter un utilisateur ».**

Dans notre cas la liste est constituée des deux noms : 'Badro' et 'Mohammed'. Les noms autorisés s'affichent comme le montre la **figure III.5** ci-dessous :

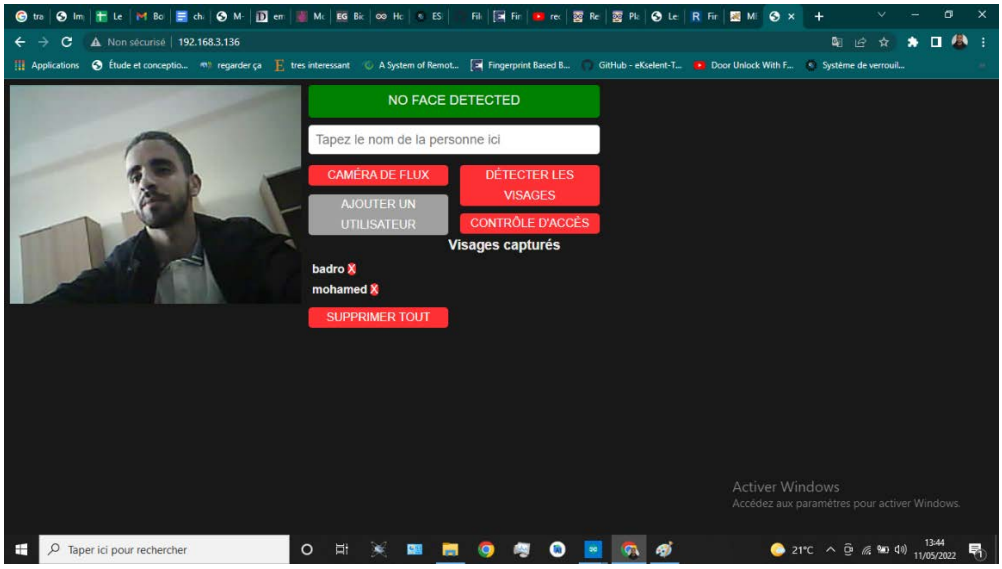


Figure III 5: Les noms enregistrés

III.2.5 Tests de la reconnaissance facial avec la carte ESP32CAM et Arduino

Dans cette partie, on connecte la carte ESP32CAM avec l'Arduino dans le but de commander la serrure (dans notre cas la serrure est remplacée par la LED). La **figure III.6** montre le montage réalisé sur la plaque d'essais :

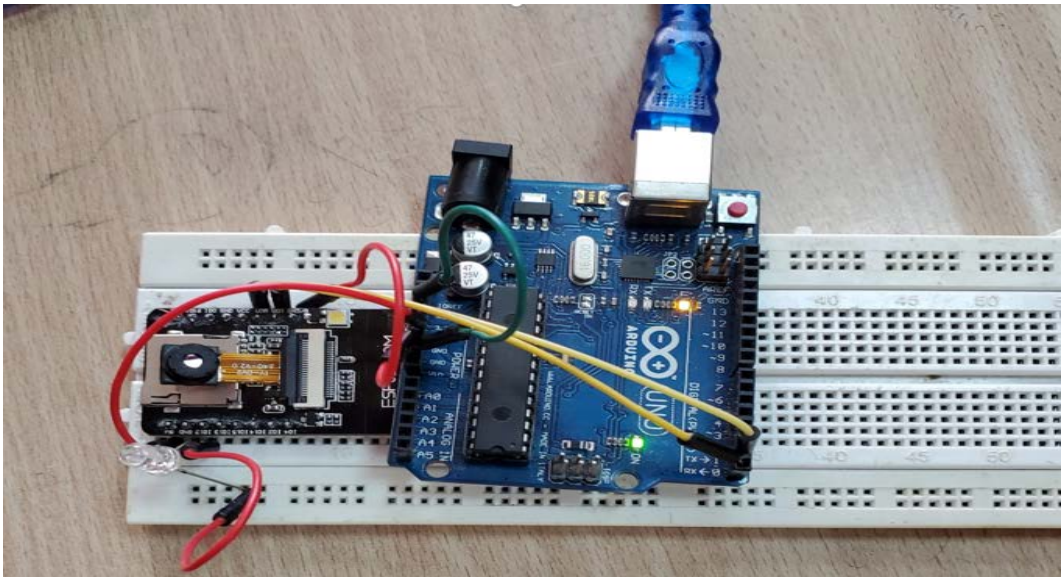


Figure III 6: Brochage de la carte esp32cam avec la carte Arduino

La LED est connectée au pin IO12 de la carte ESP32CAM, vient par la suite la saisie des noms et des visages des individus autorisés et le test des deux scénarios.

III 2.5.1 Test des cas possibles

Dans cette partie nous allons tester notre système de contrôle d'accès basé sur ESP32CAM pour les deux cas notés par : la personne est enregistrée dans la base de données, et lorsque la personne n'est pas enregistrée.

Cas 1 : la personne est enregistrée

Lorsque la personne **badro** est enregistré, son arrivée à la porte en face de la caméra de la carte ESP32CAM le message « **Porte ouverte pour badro** » s'affiche sur la plateforme comme le montre la **figure III.7**, et la LED s'allume comme le montre la **figure III.8**. Ce qui indique que la porte est ouverte.

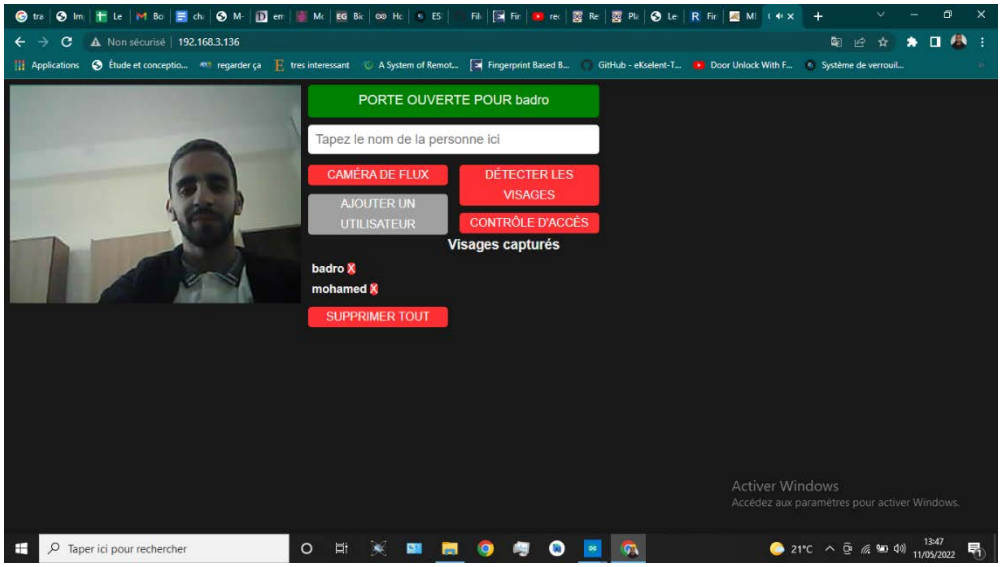


Figure III 7: Reconnaissance de la personne enregistrée

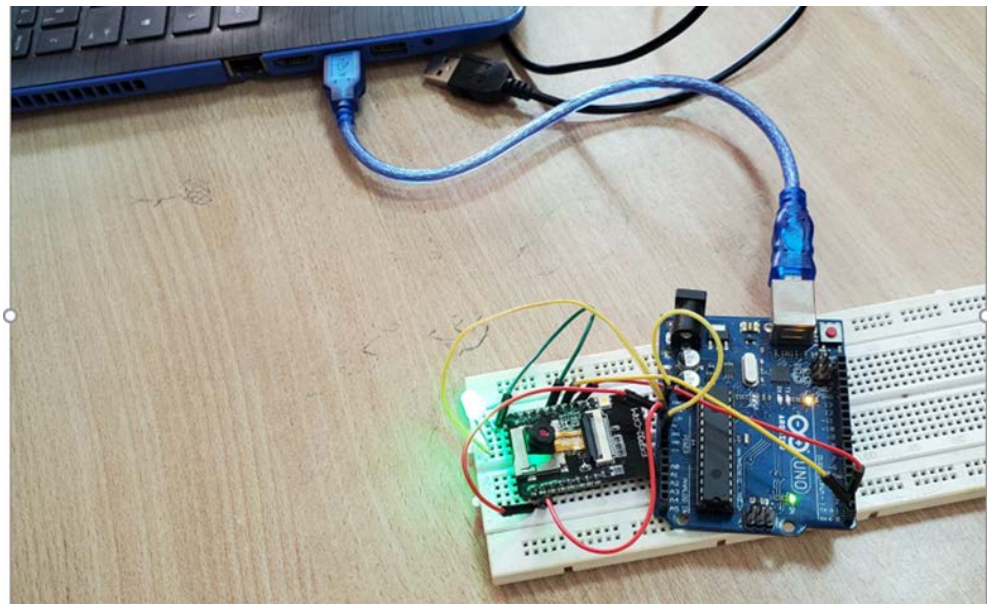


Figure III 8: LED allumée (serrure ouverte)

Cas 2 : La personne est non enregistrée

Dans le cas où la personne n'est pas enregistrée, le message « **Visage non reconnu** » s'affiche, comme le montre la figure III.9.

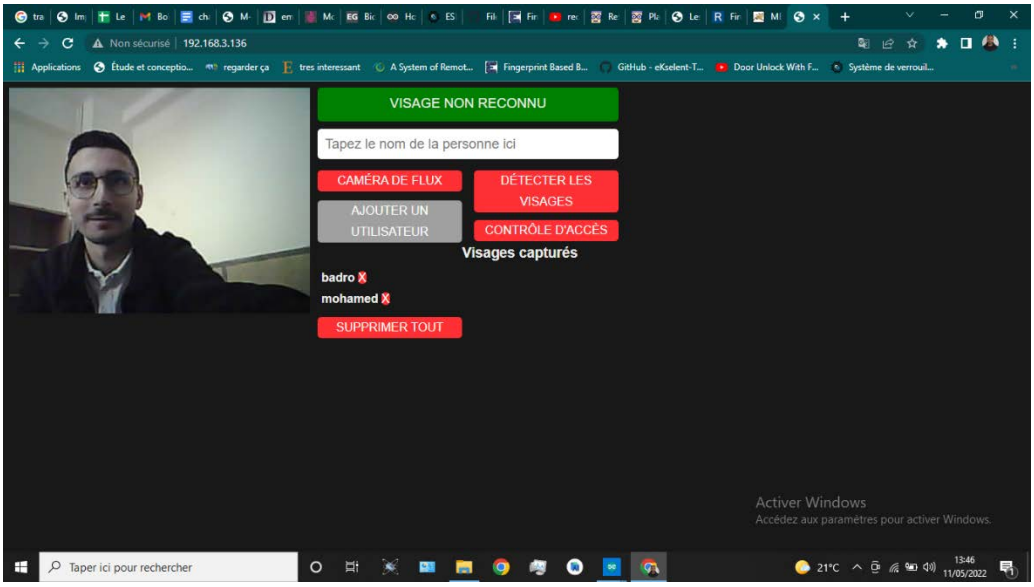


Figure III 9: Personne non enregistrée

Dans ce cas la LED ne s'allume pas. Ce qui signifie que la porte ne s'ouvre pas et la serrure reste fermée.

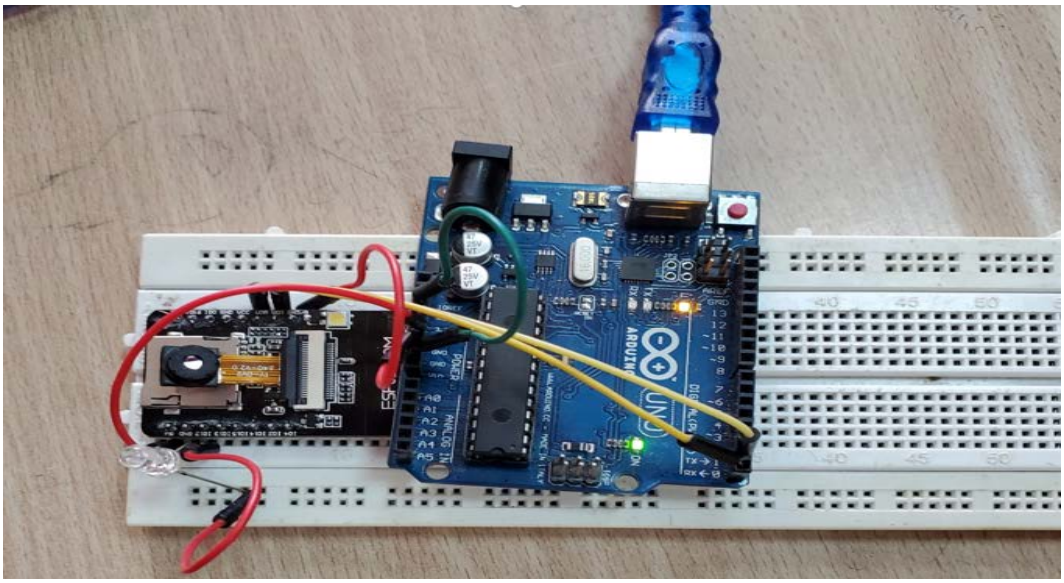


Figure III. 1 : LED éteinte (serrure fermée)

III.3 Partie d'empreinte digitale

Le lecteur d'empreintes digitales va faire appel à un capteur optique. Celui-ci va enregistrer l'empreinte qui sera par la suite traitée par un programme qui en fera l'analyse biométrique, c'est-à-dire une empreinte digitale réduite ou un indice de similitude. Ces derniers seront la base sur lesquelles le système s'appuiera pour comparer l'empreinte enregistrée à

celle scannée par le même capteur optique pour accéder à la pièce sécurisée par le lecteur d'empreintes digitales.

III.3.1 Principe de fonctionnement

Le principe du programme utilisé sur la carte Arduino pour l'utilisation de l'empreinte digitale a été résumé sur cet organigramme ci-dessous :

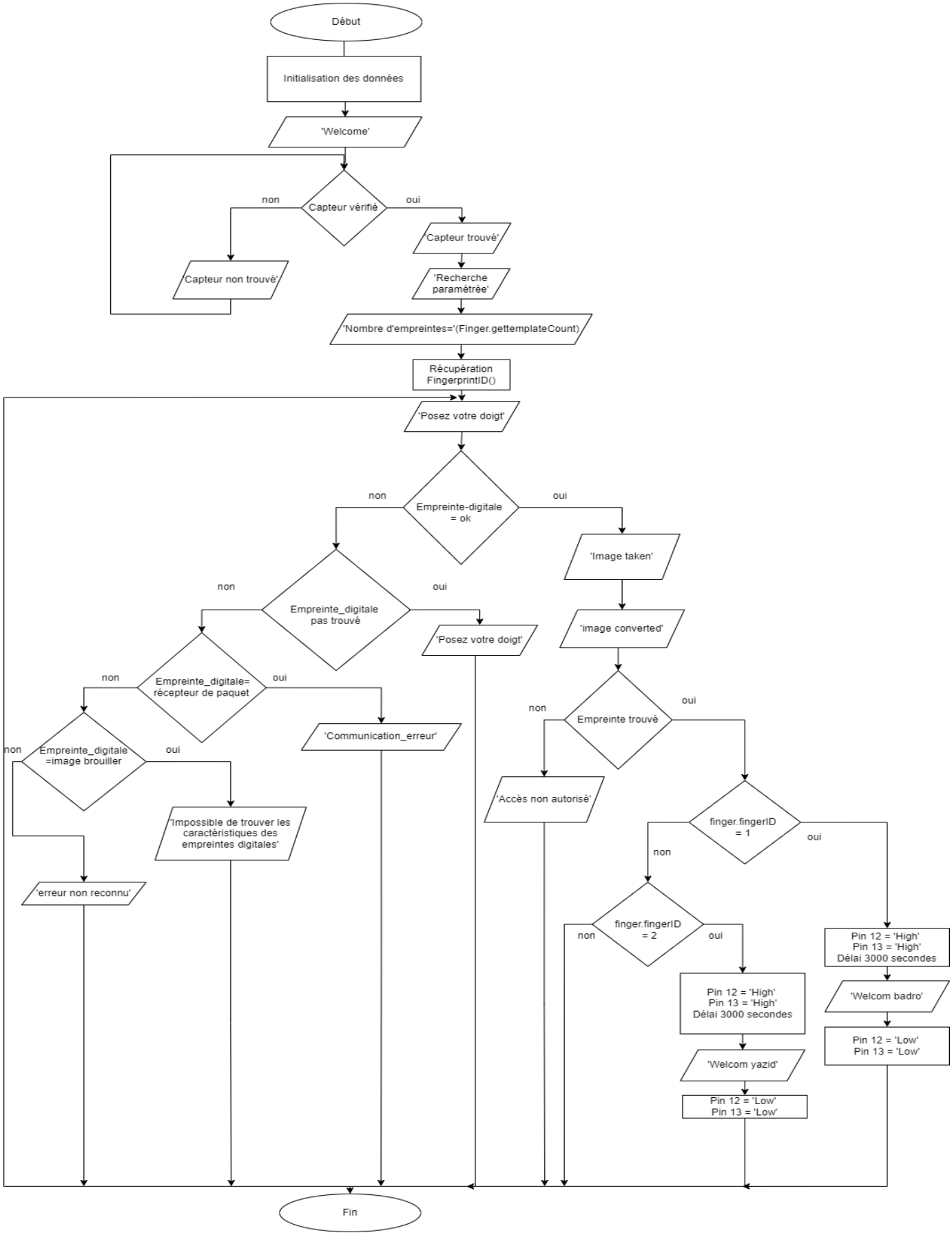


Figure III 10: L'organigramme de l'empreinte digitale avec la carte Arduino Uno

III.3.2 Schéma bloc

Le schéma bloc représenté sur la **figure III.11** détermine l'environnement de liaison de la carte Arduino. Cette dernière est liée avec la Base de données, Capteur d'empreinte, L'afficheur LCD et la serrure électrique.

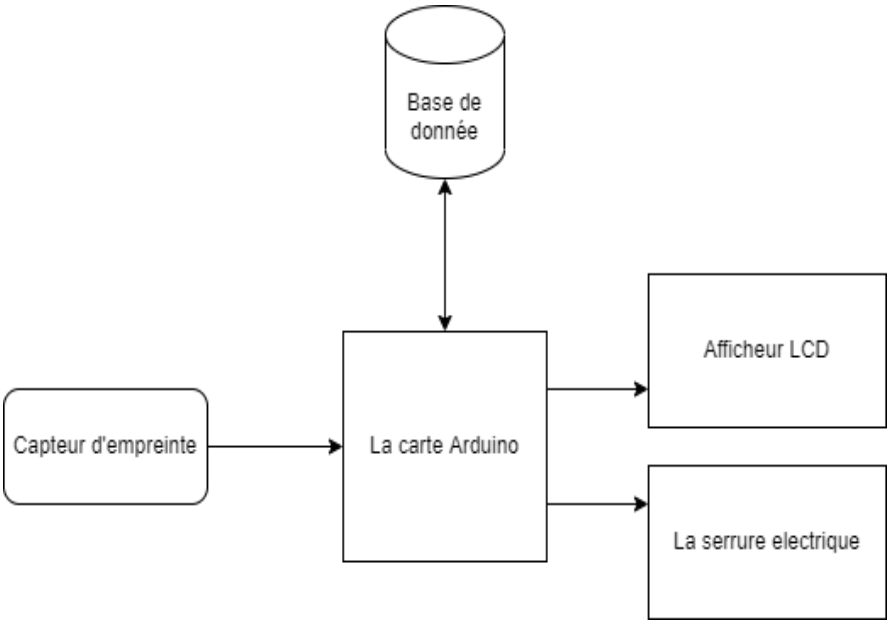


Figure III 11: Schéma bloc du capteur d'empreinte avec la carte Arduino

III 3.3 Test des cas possibles

Dans cette section on va résumer les cas possibles, pour tester notre système d'empreinte digitale à base de la carte arduino.

Cas 1 : La personne est enregistrée

Lorsqu'une personne enregistrée dans la base de données mis son doigt sur le capteur d'empreinte, la LED s'allume (dans notre cas la serrure est remplacée par la LED), comme le montre la **figure III.12.**

La LED est connectée au pin 8 de la carte Arduino, vient par la suite l'allumage de la Led.

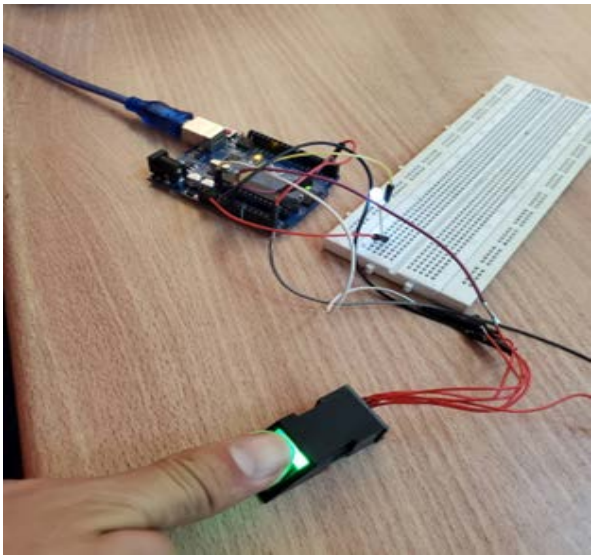


Figure III 12: LED allumée

Cas 2 : La personne est non enregistrée

Dans le cas où l'empreinte est non reconnue, la LED ne s'allume pas. Ce qui signifie la porte ne s'ouvre pas comme le montre la **figure III.13**.

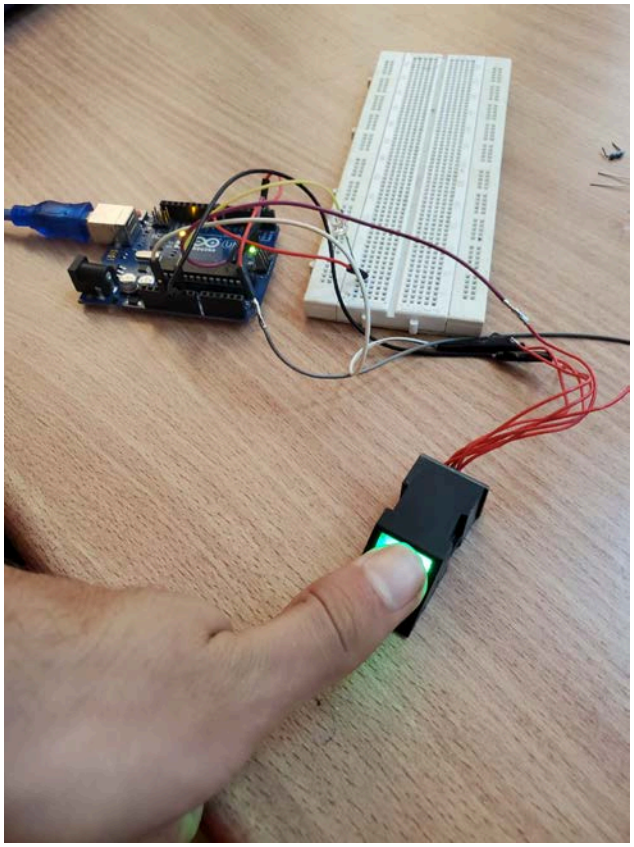


Figure III 13: Personne non enregistrée

III.4 La conception générale

Notre travail consiste à assurer une grande sécurité et fiabilité, pour cela le système effectué fait une double vérification de l'empreinte digitale et de la reconnaissance faciale simultanément. Si l'utilisateur réussit à s'authentifier avec l'empreinte digitale par exemple et n'arrive pas à s'identifier par reconnaissance faciale l'utilisateur n'auras pas l'accès.

III.4.1 Schéma bloc

La **figure III.16** schématise par bloc la liaison de ESP32CAM avec l'empreinte digitale par la carte Arduino dirigé par la base de données.

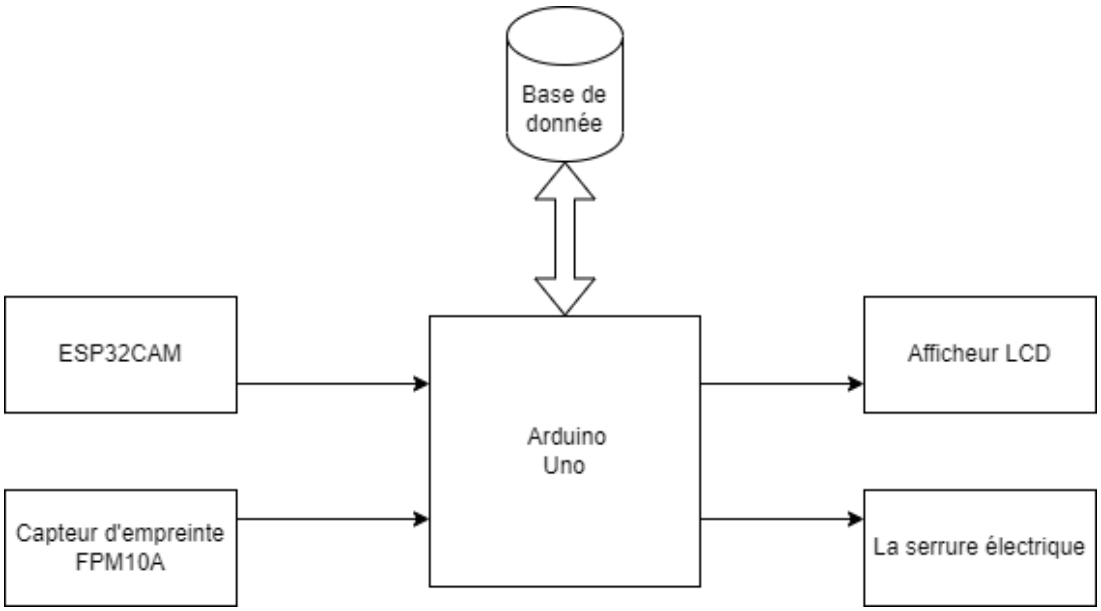


Figure III 14: Représente schéma bloc du circuit général

III.4.2 Organigramme général

L'organigramme général englobe les sous organigrammes de reconnaissance faciale et de l'empreinte digitale et toute la conception de notre système dans la **figure III.17** :

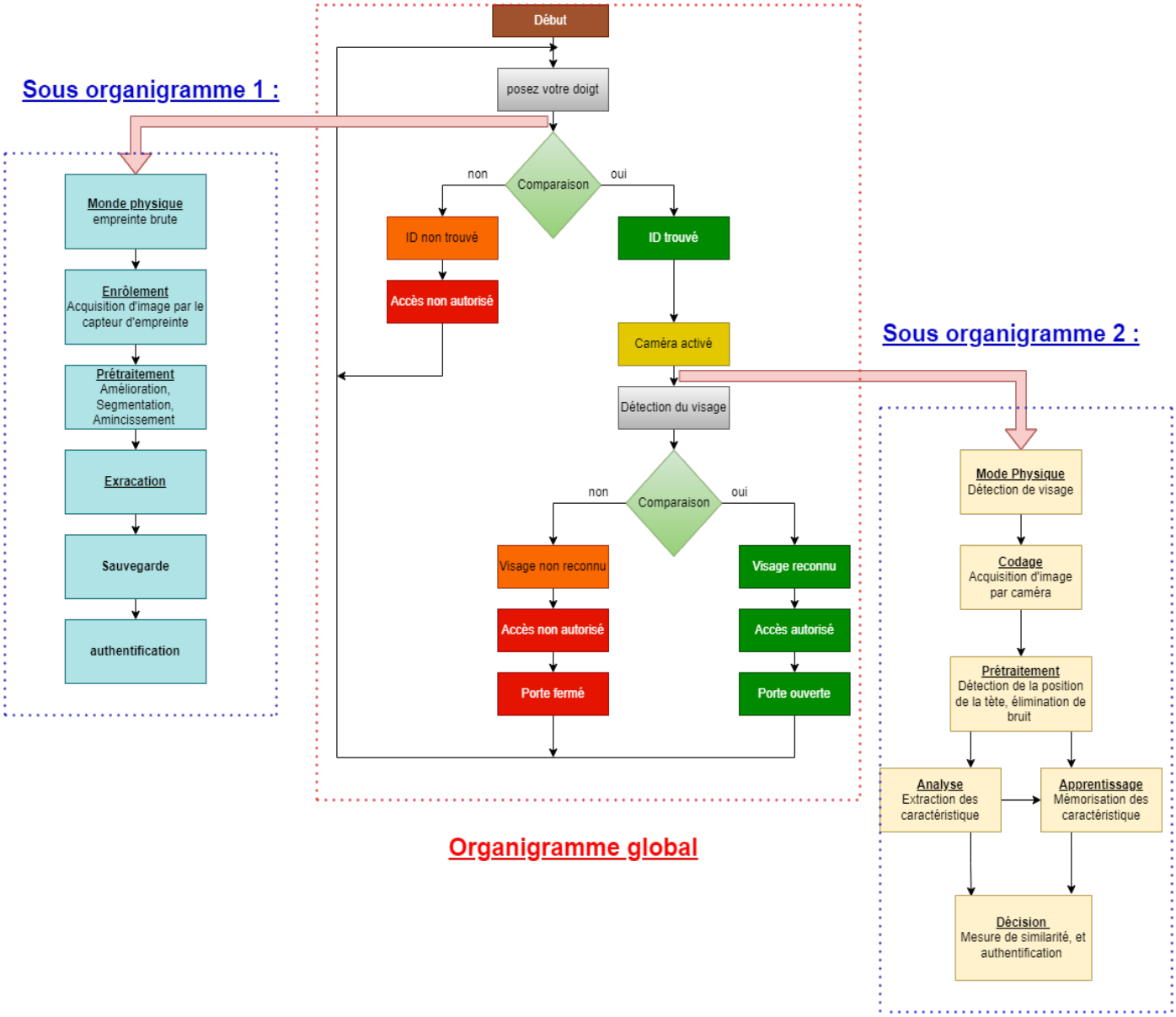


Figure III 15: Organigramme général

III.4.3 Comparaison

La correspondance s'effectue en temps réel et l'algorithme vérifie que la personne dispose des droits d'accès ou non. S'il y a une dissemblance entre le visage détecté et l'empreinte enrôlé, c'est-à-dire que la personne est non autorisée d'accéder au locale, mais il a pu accéder par le biais de l'autorisation d'un autre utilisateur. On déclenche donc une alarme permettant aux opérateurs de prendre les mesures appropriées.

III.5 Réalisation

Dans cette partie nous allons montrer notre maquette finale et ses différents compartiments et faire les tests finaux.

III.5.1 Montage sur la maquette

La réalisation de notre projet sur une maquette est montrée sur la **figure III.18** pour faciliter la compréhension du principe de notre système.

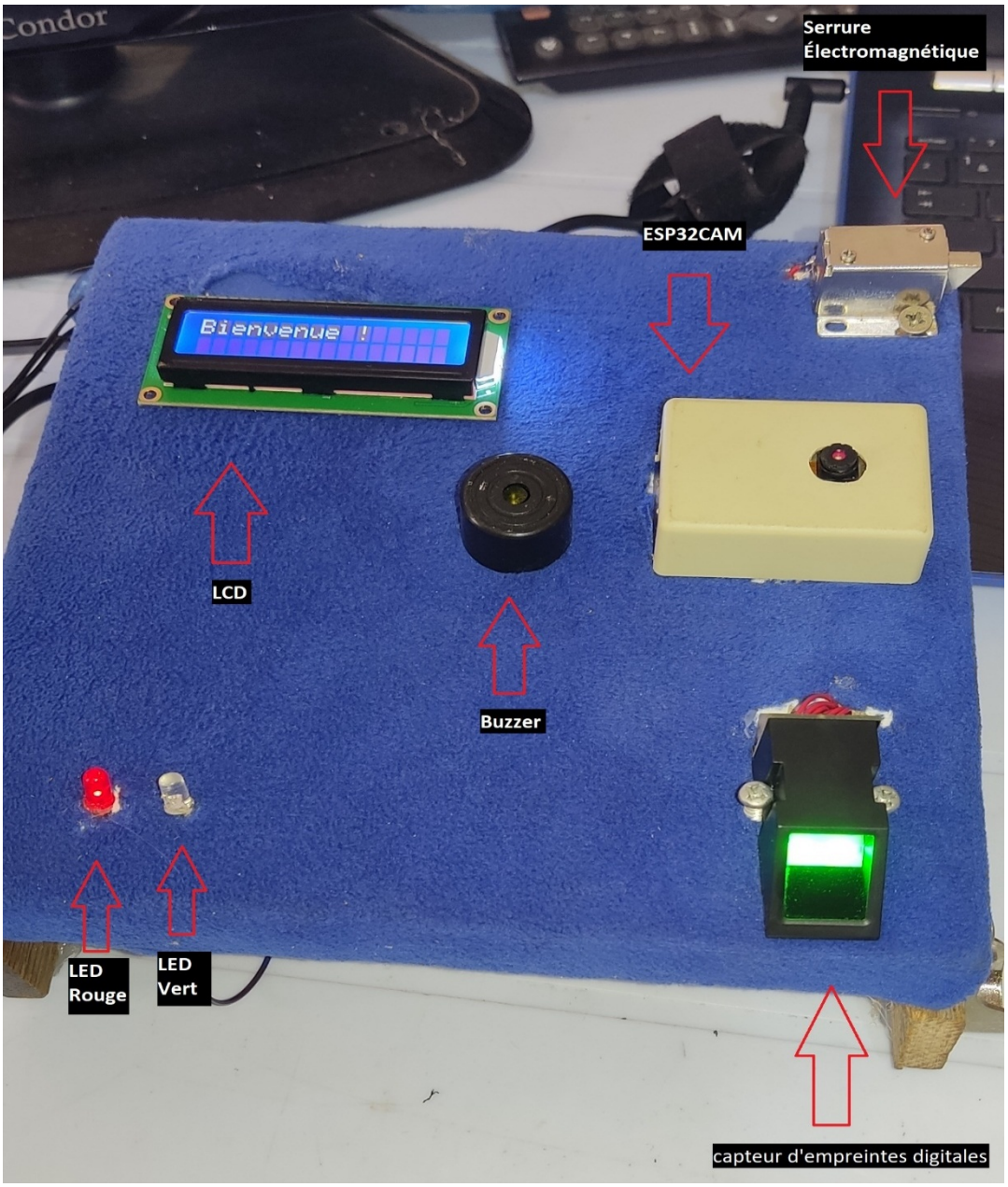


Figure III 16: Les différents composants de la maquette

III.5.2 Les étapes du fonctionnement de notre système

La première étape consiste à vérifier le bon branchement des capteurs (capteur d'empreinte et la carte ESP32-CAM), après il cherche les paramètres dans la base de données, puis il affiche le nombre d'empreintes enregistrés et le nombre de visages enregistrés sur la base de données. Si ces étapes sont bien configurées et confirmées donc le système est prêt et nous demande de « posez votre doigt » sur le capteur d'empreinte comme le montre la figure III.19 :

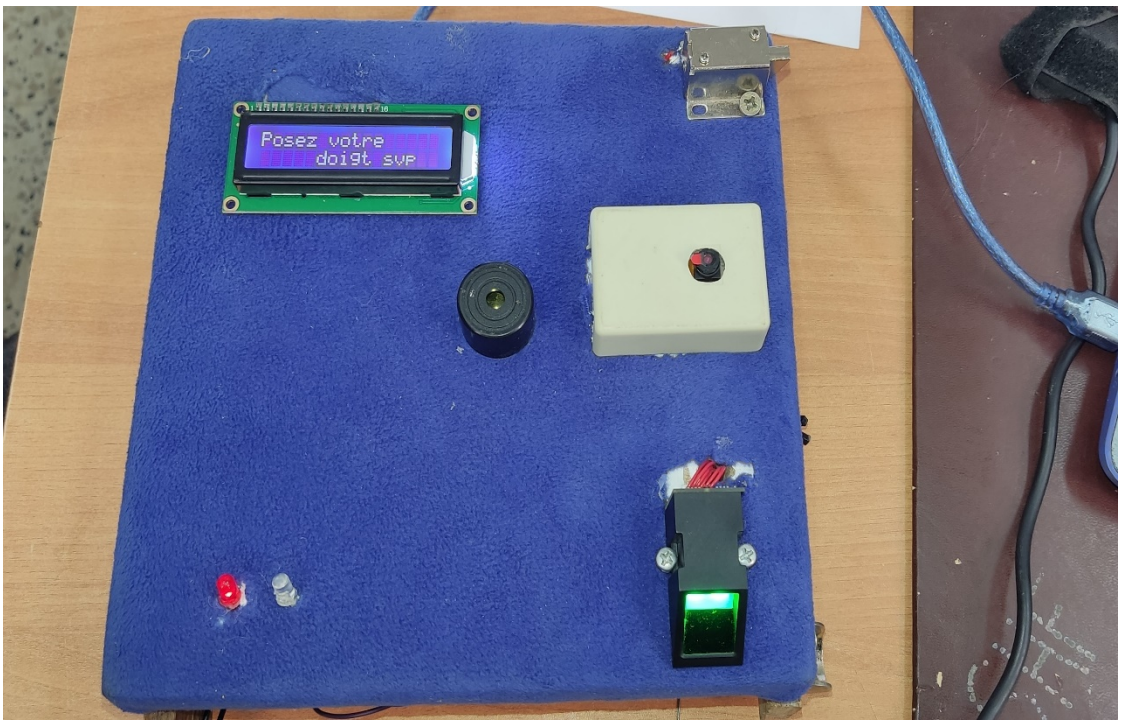


Figure III 17: Démarrage du système « posez votre doigt » lors du

Dans le cas où l'empreinte ne correspond pas à celle enregistrée le système s'arrête et affiche sur l'afficheur LCD « **Accès non-autorisé porte non-ouverte** », et la LED rouge s'allume et la serrure reste fermée comme le montre la **figure III.20** :

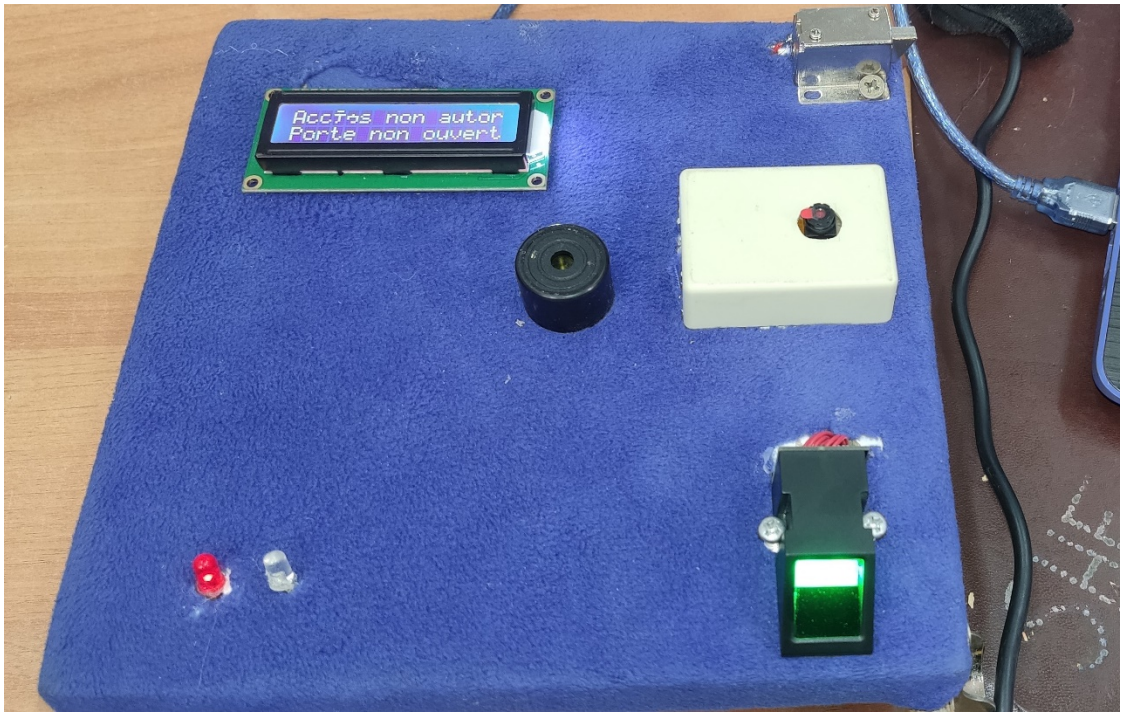


Figure III 18: Résultat de l'accès refusée

Dans le cas où l'empreinte est enregistrée dans la base de données donc empreinte autorisée. Le système nous demande de s'approcher de la caméra pour confirmer l'identification de la personne, et le message « **Approchez SVP** » s'affiche sur l'afficheur LCD. Il faut que la personne soit non mobile, et assez proche de la caméra pour pouvoir identifier correctement l'individu, le résultat est montré sur la **figure III.21**.

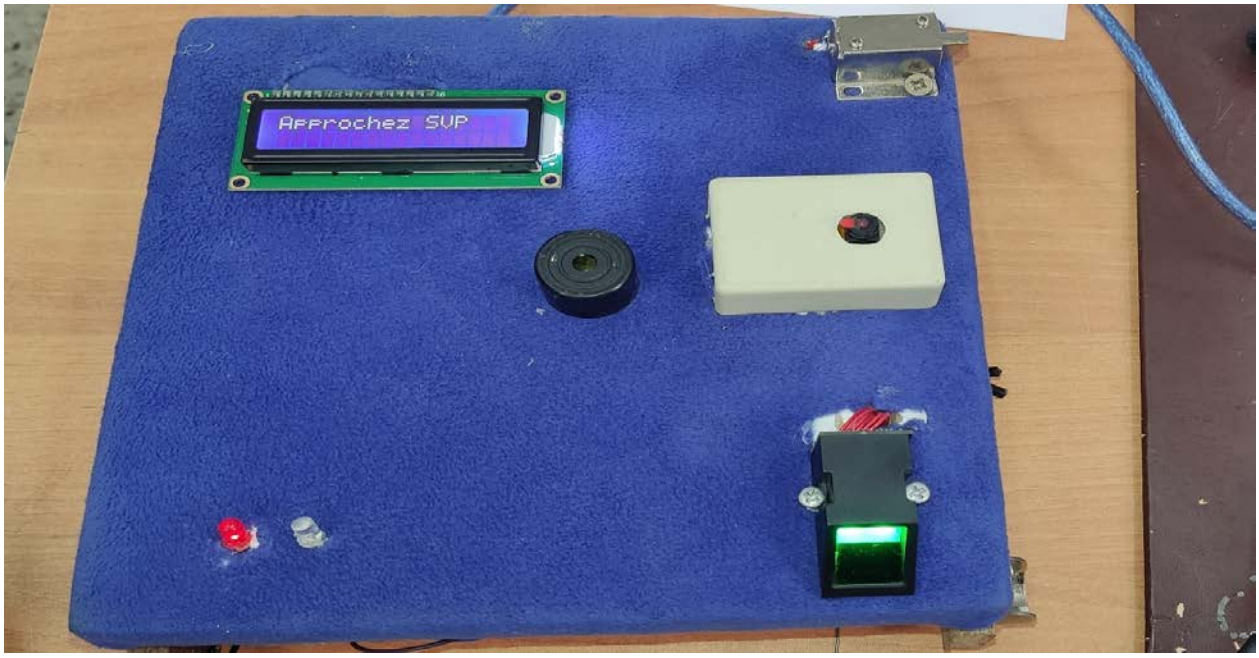


Figure III 19:Empreinte validée

Si la personne est bien identifiée ça veut dire l'empreinte et le visage reviennent à la même personne, ce qui fait, la serrure s'ouvre et la LED verte s'allume et le LCD affiche **« visage reconnu _ identification confirmée** ». Le résultat est montré sur la **figure III.22**.

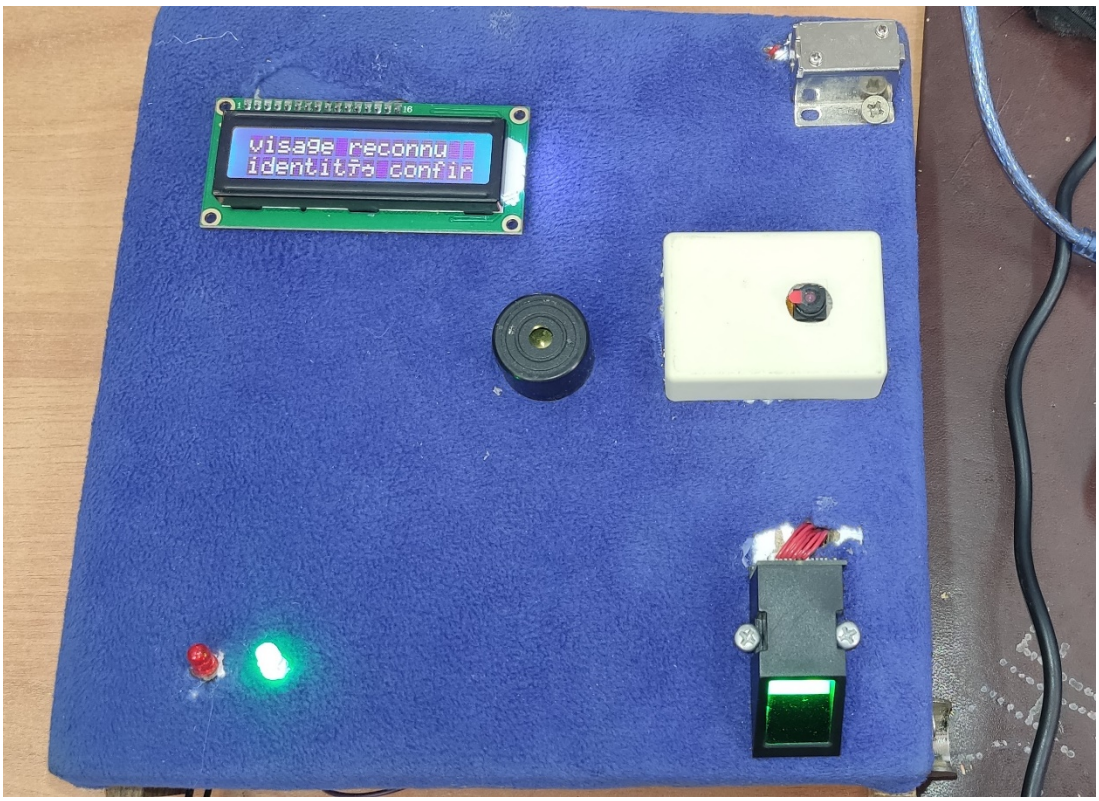


Figure III 20: Visage reconnu

Par la suite, le message "**Bienvenue et le nom de la Person identifiée**" s'affiche sur l'afficheur LCD, et la serrure s'ouvre comme le montre la **figure III.23**:

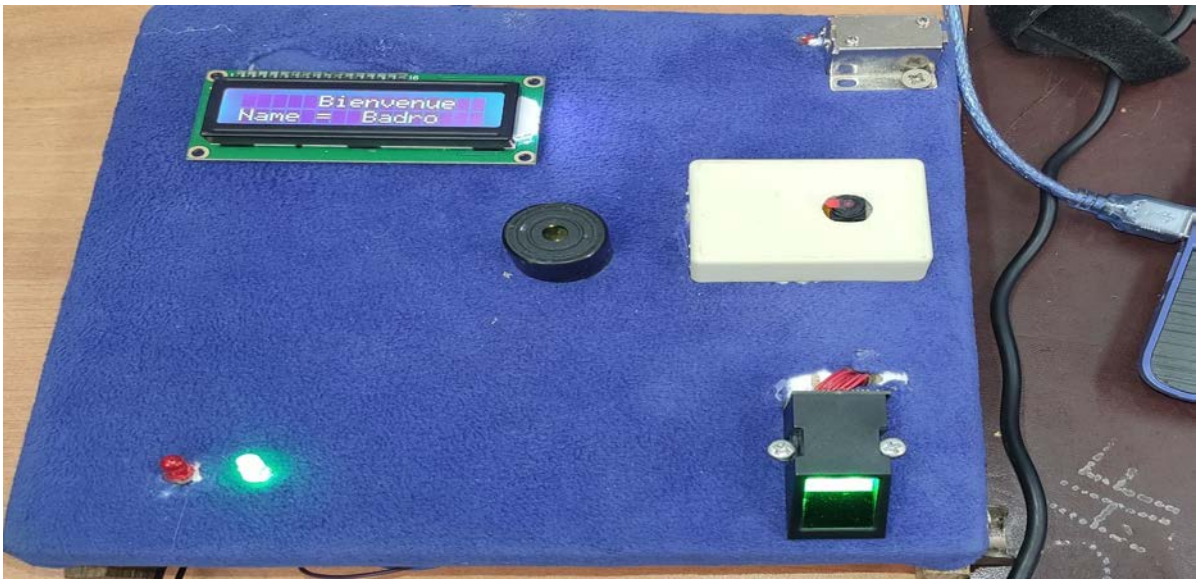


Figure III 21: Porte ouverte

Et dans le cas où l'empreinte est juste et la reconnaissance faciale est fausse la serrure reste fermée et le texte suivant s'affiche « Porte non ouverte_ Accès non autorisé » le résultat est montré sur la **figure III.24**.

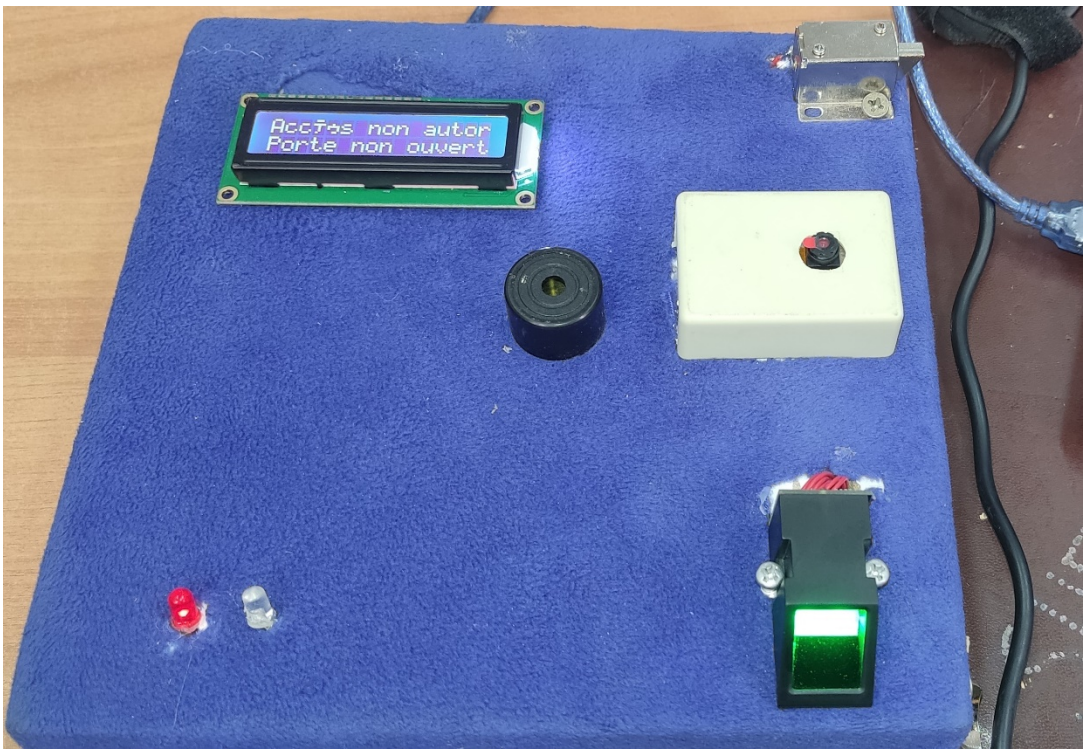


Figure III 22: Accès non autorisé, porte fermée

III.5.3 Test et résultats

Sur le tableau III.1 on résume nos tests, dont deux personne (Yazid et Badro) qui sont dans la base de données et une troisième personne (Inconnue) non enregistrée.

Tableau III. 1 : Rôle et nom de chaque broche d'un afficheur LCD

Empreinte (Badro)	X	X	X						
Empreinte (Yazid)				X	X	X			
Empreinte (Inconnue)							X	X	X
Visage (Badro)	X			X			.		
Visage (Yazid)		X			X			.	
Visage (Inconnue)			X			X			.
Accès :	Autorisé	Non-autorisé	Non-autorisé	Non-autorisé	Autorisé	Non-autorisé	Non-autorisé	Non-autorisé	Non-autorisé

Notre système de contrôle d'accès autorise l'accès à une personne lorsque son visage et son empreinte digitale soient les deux enregistrée.

III.5.4 Avantages et inconvénients de notre système de contrôle d'accès

Les avantages et les inconvénients de notre système sont résumés ci-dessous :

- **Avantages**
  - Bien accepté par le public
  - Aucune action de l'usager (peu intrusive)
  - Technique peu couteuse
- **Inconvénients :**
  - Technologie sensible à l'environnement (éclairages, position, expression du visage …etc)
  - Difficultés de différencier des vrais jumeaux
  - Sensible à la crasse poussier sur les capteurs

III.6. Conclusion

Dans ce chapitre, nous avons réalisé un système de contrôle d'accès sécurisé basé par technique biométrique. Ce dernier se réfère à la reconnaissance automatique des individus basée sur leurs caractéristiques physiologiques.

Notre système biométrique est basé sur l'empreinte digitale et la reconnaissance faciale ; Il s'agit de mettre en œuvre un système de contrôle d'accès dans un bureau d'entreprise composé d'une serrure biométrique à une particularité de pouvoir garder en mémoire un grand nombre d'empreintes, cette dernière est surveillée par une caméra permettant la reconnaissance faciale des individus.

Conclusion générale

Notre travail consiste à la conception et l'implémentation d'un système de la Biométrie multimodale : combinaison entre deux technique tel que l'empreinte digitale et la reconnaissance faciale, et chaque modalité a de différentes méthodes.

Notre travail consiste à la mise au point d'un algorithme robuste et solide destiné à reconnaître un individu à partir de son empreinte digitale et son visage. Dans chaque système on a utilisé une technique précise :

- Dans la reconnaissance d'empreinte digitale, la technique utilisée est l'extraction classique des minuties qui consiste à extraire les minuties à partir d'un squelette de l'image.

- Dans la reconnaissance faciale la méthode utilisée est LBP (local Binary Pattern), c'est une méthode mathématique dont son but consiste à caractériser la texture d'une image par le calcul du code LBP pour tous les pixels d'image,

- Le niveau de fusion choisit est la fusion de score dans ce niveau les scores individuels sont combinés de manière à former un unique score qui est ensuite utilisé pour prendre la décision finale.

Le système conçu peut être utilisé dans plusieurs endroits considérés comme très sensibles : les banques de sangs, laboratoires ou des zones militaires, qui réduisent considérablement le risque d'entrée non autorisée.

Nous pourrions appliquer certaines techniques avancées pour améliorer les performances de chaque type de technologie de vérification biométrique, cela pourrait signifier un avenir sans mots de passe ou une combinaison de divers systèmes d'identification pour assurer notre sécurité.

La partie pratique de ce projet a conclu que le contrôle d'accès en double authentification montre une fiabilité élevée mais vu que l'évolution des méthodes moderne de corruption (piratage, infiltration ...etc) pourra démineur le niveau de la crédibilité et la fiabilité de ce système. A ce propos, cette partie reste donc au futur chercheur d'investir des efforts

orientés vers une authentification plus sécurisée à base d'iris comme un troisième soutien du contrôle d'accès.

Résumé

Dans ce travail, nous avons conçu un système pour le contrôle d'accès par deux techniques biométriques : l'empreinte digitale et la reconnaissance faciale basés sur Arduino et Esp32cam successivement. Les différentes étapes du système proposé nous obligent à prendre en considération les inconvénients de chaque opération (la position des doigts/visage et leurs états, les différents capteurs utilisés pour la prise de l'image, la luminosité...etc.). Le système réalisé a répondu aux objectifs fixés dans le projet. Le système est sécurisé, fiable, simple et fonctionnel, d'après les tests effectués et les résultats obtenus nous pouvons dire que le but du projet est atteint.

***Mots clés* :** Biométrie, Empreinte digitale, Reconnaissance Faciale, Contrôle d'accès, ESP32cam, Arduino.

Abstract

In this work, we have designed a system for access control by two biometric techniques: fingerprint and facial recognition based on Arduino and Esp32cam. The different steps of the proposed system force us to take into consideration the drawbacks of each operation (the position of the fingers/face and their states, the different sensors used to take the image, the brightness...etc.). The realized system has met the objectives set in the project. The system is secure, reliable, simple and functional, from the tests carried out and the results obtained we can say that the goal of the project is achieved.

Key words: Biometrics, Finger print, facial recognition, access control, ESP32cam, Arduino.

ملخص

في هذا العمل قمنا بتصميم نظام للتحكم في الوصول من خلال تقنيتين من القياسات الحيوية؛ بصمة الإصبع والتعرف على الوجه على أساس ESP32CAM و Arduino . تلزمنا الخطوات المختلفة للنظام المقترح بمراعاة عيوب كل عملية (موضع الأصابع أو الوجه وحالاتهم، وأجهزة الاستشعار المختلفة المستخدمة في التقاط الصورة والسطوع ...). حقّق النظام المنتج الأهداف المحددة في المشروع، هذا النظام آمن وموثوق وبسيط وعملي، وحسب الاختبارات التي أجريت والنتائج التي تم الحصول عليها يمكننا القول إن الهدف من المشروع قد تحقق.

الكلمات المفتاحية: طباعة رقمية، القياسات الحيوية، Arduino، ESP32CAM، التعرف على الوجه، مراقبة وصول.