الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

UNIVERSITÉ BADJI MOKHTAR - ANNABA
BADJI MOKHTAR – ANNABA UNIVERSITY

جامعة باجي مختار – عنابـــــــــة

Faculté : TECHNOLOGIE
Département : ELECTRONIQUE
Domaine : SCIENCES ET TECHNOLOGIES
Filière : ELECTRONIQUE
Spécialité : Electronique des systèmes embarqués / Instrumentation

Mémoire

Présenté en vue de l'obtention du Diplôme de Master

Thème :

Développement d'un système de reconnaissance faciale

Présenté par : *CHOUALA Fares / DELIMI Ismail*
Encadrante : *ZERMI Narima Grade M.C.A Université Badji Mokhtar-Annaba*

Jury de Soutenance :

BOUGHAZI Mouhamed	Professeur	Université Badji Mokhtar-Annaba	Président
ZERMI Narima	M.C. A	Université Badji Mokhtar-Annaba	Encadrante
MESSADEG Djemil	Professeur	Université Badji Mokhtar-Annaba	Examinateur

Année Universitaire : 2022/2023

Remerciements :

À Dieu, pour sa guidance précieuse,

Nous le remercions de tout cœur pour son soutien et sa présence tout au long de ce parcours. Sa lumière nous a éclairé et nous a donné la force de réaliser ce mémoire. Merci pour tout.

À notre encadreur Mme Narima ZERMI,

Nous tenons à exprimer notre gratitude pour votre accompagnement durant cette étude. Votre soutien et vos conseils ont été précieux. Nous vous sommes reconnaissants pour votre engagement et votre contribution à la réussite de ce travail.

Aux jurys présents,

Nous vous remercions d'avoir consacré du temps pour évaluer notre mémoire. Votre expertise a été un élément important dans la validation de notre travail. Nous vous sommes reconnaissants pour votre implication.

À nos familles, amis et tous ceux qui nous ont soutenu,

Nous vous adressons nos remerciements les plus sincères pour votre soutien, vos conseils et votre encouragement. Votre présence a été essentielle dans la réalisation de ce projet.

Merci à tous.

Dédicace

À ma famille, pilier inébranlable de ma vie, je tiens à exprimer ma gratitude infinie. Votre amour inconditionnel, vos encouragements constants et votre présence réconfortante ont été mes repères tout au long de ce parcours. Malgré les obstacles et les doutes, vous avez été mes piliers et mes épaules sur lesquelles m'appuyer. Chaque instant partagé avec vous a été une source de bonheur et de force. Vous avez su m'encourager à croire en moi-même et à poursuivre mes rêves, même lorsque le découragement menaçait de s'installer. Je vous remercie du fond du cœur pour votre amour incommensurable et pour avoir toujours été là, à mes côtés, me guidant sur le chemin de la réussite.

À ma mère, pilier solide de ma vie, je veux exprimer ma profonde gratitude. Ton amour inconditionnel, ta force et ton soutien sans faille ont été la clé de ma réussite. Tes prières et tes sacrifices ont ouvert les portes de l'accomplissement pour moi. Je te remercie du fond du cœur pour ton amour incommensurable et pour avoir été mon soutien dans les moments de doute.

À mon cher frère Said et mes chers sœurs, compagnons de vie et de rires, je vous suis reconnaissant pour notre lien indéfectible. Votre soutien, vos encouragements et votre présence ont rendu ce chemin plus agréable et significatif. Ensemble, nous avons partagé des moments de joie et de chagrin. Votre soutien inconditionnel m'a donné la force de poursuivre mes rêves. Je suis honoré d'avoir grandi à vos côtés et de pouvoir partager mes succès avec vous.

À la mémoire de mon frère bien-aimé Habib, qui a quitté ce monde trop tôt, je souhaite rendre hommage à sa présence éternelle dans mon cœur.

Et enfin, à la mémoire de mon père, au qui je souhaite accorder une importance particulière. Tu as été ma source d'inspiration et ma boussole tout au long de ma vie, je te dédie ce mémoire avec une gratitude infinie. Ta sagesse, ton amour et ta bienveillance continuent de guider chacune de mes décisions. Tu étais mon modèle de vie, mon exemple de détermination et de travail acharné. Ta disparition certes laisse un vide immense, mais ton héritage demeure vivant en moi. Chaque réussite, chaque accomplissement est un témoignage de l'héritage précieux que tu m'as laissé. Je garde précieusement en moi les valeurs que tu m'as transmises : l'intégrité, la persévérance et le désir incessant de viser l'excellence. Je sais que tu aurais été fier de moi aujourd'hui, que dieu t'accueille dans son vaste paradis.

À tous les membres de ma famille, à tous mes amis, que ces mots sincères atteignent chacun d'entre vous, portant avec eux la chaleur de ma reconnaissance et de mon amour. Votre impact sur ma vie restera gravé à jamais dans mon cœur. Aujourd'hui, je vous dédie ce mémoire avec humilité et gratitude infinie, sachant que sans vous, rien de tout cela n'aurait été possible.

Merci du fond du cœur.

Fares CHOUALA

Dédicace :

A ma mère Fadila, qui m'a entouré d'amour, d'affection et qui a faite tout pour ma réussite, que dieu la garde.

A mon père qui m'a aidé à devenir ce que je suis aujourd'hui, que dieu le garde et le protège.

A mon frère Labib, Chakib, Adel et mes sœurs Hana et Mouna qui ont toujours été à mes coté pour me soutenir et m'encourager.

A mes très chers amis symbole de tendresse et de fidélité.

Et finalement à Fares et Ikram qui ont fait tout leur possible pour m'aider dans mes années d'études.

Ismail Delimi.

Résumé

Dans ce projet, un système de verrouillage de porte est créé en combinant la reconnaissance faciale avec la caméra ESP32 pour une détection faciale plus précise. L'ESP32-CAM contrôle le système de verrouillage et de déverrouillage de la porte et restreint l'accès aux individus dans sa base de données. Deuxièmement, nous étions intéressés à développer un programme Python pour évaluer les fonctionnalités de reconnaissance faciale de la bibliothèque OpenCV.

Abstract

In this project, a door locking system is created by combining facial recognition with the ESP32 camera for more precise facial detection. The ESP32-CAM controls the door locking and unlocking system and restricts access to individuals in its database. Second, we were interested in developing a Python program to evaluate the OpenCV library's facial recognition features.

ملخص

في هذا المشروع، يتم إنشاء نظام قفل الباب عن طريق الجمع بين التعرف على الوجه وكاميرا ESP32 لاكتشاف الوجه بشكل أكثر دقة. يتحكم ESP32-CAM في نظام قفل الباب وفتحه ويقيد الوصول إلى الأفراد في قاعدة بياناته. ثانيًا، كنا مهتمين بتطوير برنامج Python لتقييم ميزات التعرف على الوجه في مكتبة OpenCV.

Sommaire

Liste des abréviations

API: Application Programming Interface

BLE: Bluetooth Low Energy

CLK: Clock

CMD: Command Microcontroller Data

COM: Common

CPU: Central Processing Unit

DC: Direct Current

FOTA: Firmware Over-the-Air

FTDI: Future Technology Devices International

GPIO: General Purpose Input/Output

Ghz: Gigahertz

GND: Ground

GO: General Office

IDE: Integrated Development Environment

IP: Internet Protocol

IOT: Internet of Things

I2C: Inter-Integrated Circuit

MP: Megapixel

NC: Normally Closed

NO: Normally Opened

NIP: Numéro d'Identification Personnel (Personal Identification Number)

OpenCV: Open-Source Computer Vision Library

PWM: Pulse Width Modulation

PSRAM: Pseudo Static Random Access Memory

QR: Quick Response

RAM: Random Access Memory

SAS: Secure Access System

SD: Secure Digital

SPI: Serial Peripheral Interface

TTL: Transistor-Transistor Logic

UART: Universal Asynchronous Receiver-Transmitter

USB: Universal Serial Bus

UXGA: Ultra Extended Graphics Array

V: Voltage

VCC: Voltage Common Collector.

Liste des figures

Liste des tableaux

Introduction Générale :

Dans diverses sphères de notre vie quotidienne, la sécurité est de la plus haute importance. Le contrôle d'accès, fondé principalement sur d'anciennes méthodes, n'est plus efficace du fait que les cartes et les clefs peuvent être falsifiées ou dupliquées, Les cartes d'identité peuvent être perdues, oubliées ou égarées. Le mot de passe peut être oublié ou compromis. Ces inconvénients rendent les formes classiques d'identification peu fiables et ne garantissent pas une haute sécurité en termes de contrôle d'accès.

Actuellement, beaucoup de méthodes biométriques sont menées afin de trouver des solutions de rechange aux méthodes d'identification précédentes. Comme les caractères biométriques sont universels, uniques et permanents, la méthode fondée sur la biométrie est plus efficace et fiable. Et parmi toutes les technologies biométriques qui existent, la reconnaissance faciale est l'une des technologies les plus utilisées et les plus adaptées puisqu'elle nous donne accès à une mine de données sur une personne.

Un système de reconnaissance faciale gère l'accès grâce à la vérification de l'identité. Mais avant de vérifier l'identité, il faut d'abord détecter le visage et en extraire les composantes faciales nécessaires à la procédure de reconnaissance.

Ce projet de fin d'études porte intérêt à cette technologie très utile et très en demande dans le domaine de la sécurité. Son continu propose de mettre en œuvre un système de sécurité utilisant la technologie de reconnaissance faciale à carte ESP32-CAM pour une identification plus précise.

L'objectif principal de la mise au point de ce système est de mettre à profit l'ESP32-CAM pour la détection et la reconnaissance faciale et ainsi contrôler le verrouillage/déverrouillage d'une serrure électrique limitant l'accès seulement aux personnes enregistrées dans la base de données de l'unité ESP32-CAM. En deuxième lieu tester les fonctions de la reconnaissance faciale de la bibliothèque Open cv en langage python.

Ce mémoire est organisé comme suivant :

- Le premier chapitre est consacré pour l'explication du principe de la biométrie et la reconnaissance faciale
- Le second chapitre présente la carte ESP32-CAM, ainsi que ses ressources et les bibliothèques associées.

- Le troisième chapitre est réservé pour la mise au point d'une simulation de la reconnaissance faciale ainsi que la réalisation pratique du projet proposé et les résultats obtenus.
- Ce mémoire se termine par une conclusion générale, les perspectives futures pour l'amélioration de ce travail, ainsi qu'une bibliographie indiquant quelques sources d'informations utilisées.

Chapitre I :

Biométrie et reconnaissance faciale

Introduction :

Comparativement aux méthodes d'authentification conventionnelles, les systèmes d'authentification biométrique offrent un degré de sécurité plus élevé parce qu'ils ne comptent pas sur des jetons, des clés, des épingles ou des mots de passe pour déterminer qui est autorisé ou non.

Les systèmes biométriques utilisent les traits distinctifs d'une personne pour les identifier et les vérifier. Ces traits distinctifs peuvent faire la distinction entre un utilisateur réel et un faux utilisateur au moyen de traits physiologiques (visage, empreinte digitale, iris, etc.) et comportementaux (voix, signature, démarche, etc.).

En raison de la vulnérabilité des méthodes traditionnelles d'authentification à la perte, au vol ou à l'oubli, les systèmes biométriques améliorent la sécurité et le confort dans le monde d'aujourd'hui. Ce chapitre est divisé en deux sections ; la première traite les systèmes biométriques en général et la seconde est consacrée aux spécificités de la détection et de la reconnaissance faciale.

Nous commencerons par des renseignements généraux sur la biométrie, y compris sa définition, son fonctionnement, les différents systèmes de biométrie, et en fin de compte ses applications. La deuxième partie de ce chapitre, consacrée à l'identification faciale, sa définition, ses avantages, les problèmes rencontrés, les techniques utilisée, ainsi qu'une conclusion générale pour ce chapitre.

I.1 Section 1 : La Biométrie

I.1.1 Définition :

Une définition concise de ***la biométrie*** est « la reconnaissance automatique d'une personne au moyen de traits distinctifs ». Une définition plus large de la biométrie est « toute caractéristique physique ou personnelle automatiquement mesurable, robuste et distinctive qui peut être utilisée pour identifier une personne ou vérifier son identité ». Cette définition doit être élaborée.

Mesurable signifie que la caractéristique ou le trait peut être facilement présenté à un capteur, localisé par lui, et converti en un format numérique quantifiable. Cette mesure permet d'effectuer l'appariement en quelques secondes et en fait un processus automatisé.

La robustesse de la biométrie désigne la mesure dans laquelle la caractéristique ou le trait est sujet à des changements importants au fil du temps. Ces changements peuvent découler de l'âge, d'une blessure, d'une maladie, d'une utilisation professionnelle ou d'une exposition à des produits chimiques. Une biométrie très robuste ne change pas beaucoup au fil du temps, tandis qu'une biométrie moins robuste changera. Par exemple, l'iris, qui change très peu au cours de la vie d'une personne, est plus robuste que sa voix.

Le caractère distinctif est une mesure des variations ou des différences dans le profil biométrique au sein de la population générale. Plus le degré de caractère distinctif est élevé, plus l'identificateur est individuel. Un faible degré de caractère distinctif indique un profil biométrique fréquemment observé dans la population générale. L'iris et la rétine ont des degrés de distinctivité plus élevés que la géométrie de la main ou du doigt.

La biométrie est utilisée pour la reconnaissance humaine, qui consiste à identifier et la vérification. Les termes diffèrent considérablement. Avec l'identification, le système biométrique demande et tente de répondre à la question « Qui est X ? ».

La vérification a lieu lorsque le système biométrique demande et tente de répondre la question « Est-ce X ? » après que l'utilisateur affirme être X. [1]

I.1.2 Modes de fonctionnement d'un système biométrique :

Les systèmes biométriques peuvent fournir trois modes de fonctionnement, à savoir, ***l'enrôlement, l'authentification*** (***ou vérification***) et ***l'identification***. Dans ce qui suit, les

figures illustreront l'exemple d'un système biométrique utilisant l'empreinte digitale comme modalité.

L'enrôlement (Figure. I.1) est la première phase de tout système biométrique, il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois et où une ou plusieurs modalités biométriques sont capturées et enregistrées dans une base de données. Cet enregistrement peut s'accompagner par l'ajout d'information biographique dans la base de données.

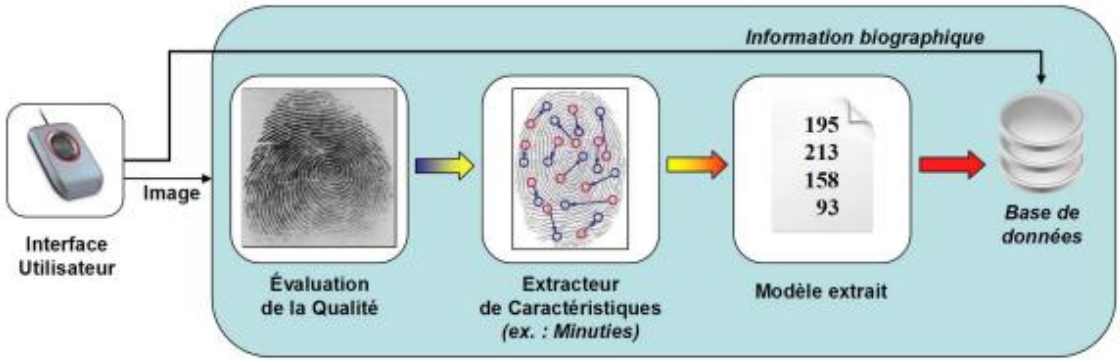


Figure I.1 – Enrôlement d'une personne dans un système biométrique.

Lorsqu'un système biométrique opère en **mode authentification** (Figure I.2), l'utilisateur affirme son identité et le système vérifie si cette affirmation est valide ou non.

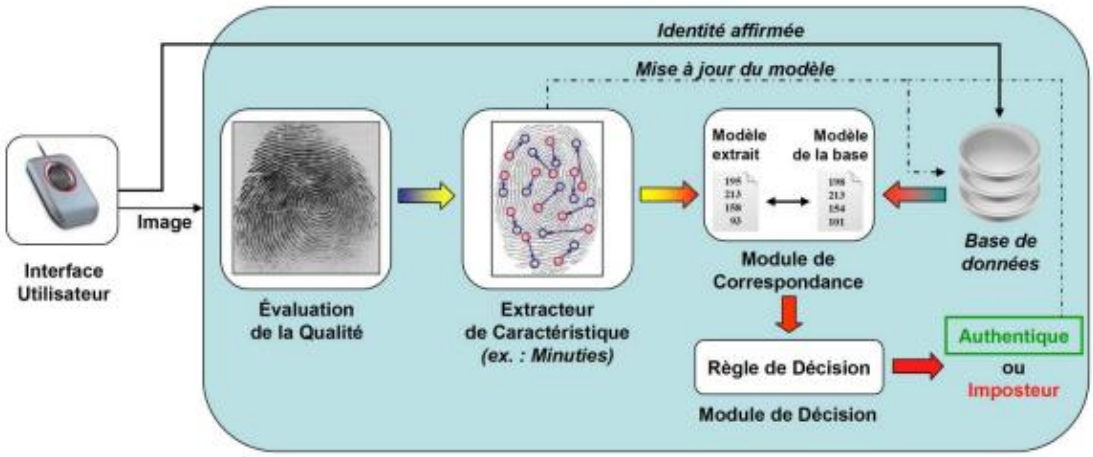


Figure I.2 – Authentification d'un individu dans un système biométrique.

Pour illustrer ce principe, prenons la situation où un utilisateur (M. X) souhaite retirer de l'argent à un distributeur de billets en entrant son code personnel d'identification (code PIN) et en présentant une modalité biométrique. Le système acquiert alors les données

biométriques et va les comparer uniquement avec le modèle enregistré correspondant à M. X. On parle alors de correspondance 1:1. Ainsi, si l'entrée biométrique de l'utilisateur et le modèle enregistré dans la base de données correspondant à l'identité affirmée possèdent un degré de similitude élevé, l'affirmation est validée et l'utilisateur est considéré comme étant un authentique. Dans le cas contraire, l'affirmation est rejetée et l'utilisateur est considéré comme étant un imposteur. En résumé, un système biométrique opérant en mode vérification répond à la question "Suis-je bien M. X ?".

Dans un système biométrique opérant en **mode identification** (Figure. I.3), l'utilisateur ne dévoile pas explicitement son identité. Cependant, l'affirmation implicite faite par l'utilisateur est qu'elle est une des personnes déjà enrôlées par le système. Ainsi, l'échantillon biométrique de l'individu est comparé avec les modèles de toutes les personnes de la base de données. On parle alors de correspondance 1:N. La sortie du système biométrique est constituée par l'identité de la personne dont le modèle possède le degré de similitude le plus élevé avec l'échantillon biométrique présenté en entrée. Typiquement, si la plus grande similarité entre l'échantillon et tous les modèles est inférieure à un seuil de sécurité minimum fixé, la personne est rejetée, ce qui implique que l'utilisateur n'était pas une des personnes enrôlées par le système. Dans le cas contraire, la personne est acceptée.

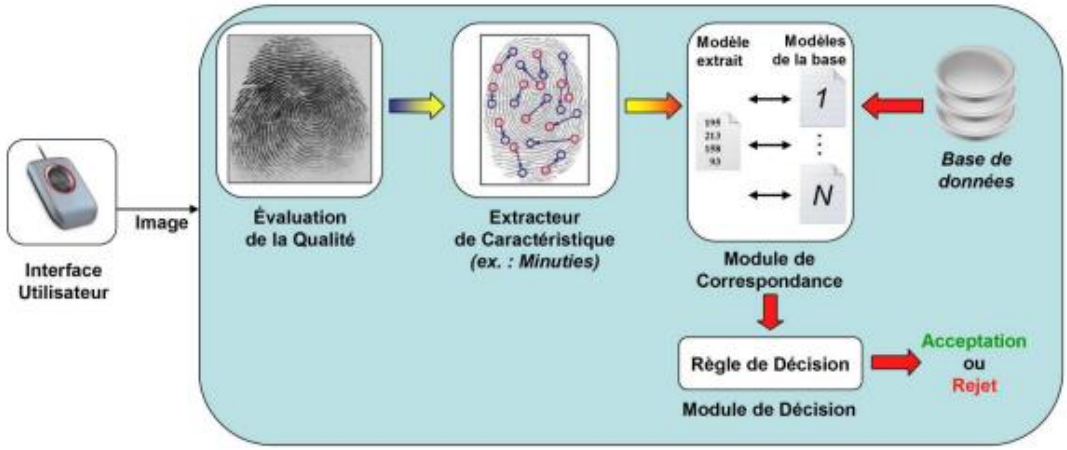


Figure I.3 – Identification d'un individu dans un système biométrique.

Un exemple de système opérant en mode identification serait l'accès à un bâtiment sécurisé : tous les utilisateurs qui sont autorisés à entrer dans le bâtiment sont enrôlés par le système ; lorsqu'un individu essaye de pénétrer dans le bâtiment, il doit d'abord présenter ses données biométriques au système et, selon la détermination de l'identité de l'utilisateur, le

système lui accorde le droit d'entrée ou non. En résumé, un système biométrique opérant en mode identification répond à la question "Suis-je bien connu du système ?".

I.1.3 Les différents systèmes biométriques :

Il existe de nombreux systèmes biométriques, mais il est possible de distinguer trois grandes familles (FIG I.4). :

- Celle relevant d'analyses biologiques (odeur, sang, salive, urine, ADN…),
- Celles relevant d'analyses comportementales,
- Enfin, celles relevant d'analyses morphologiques.

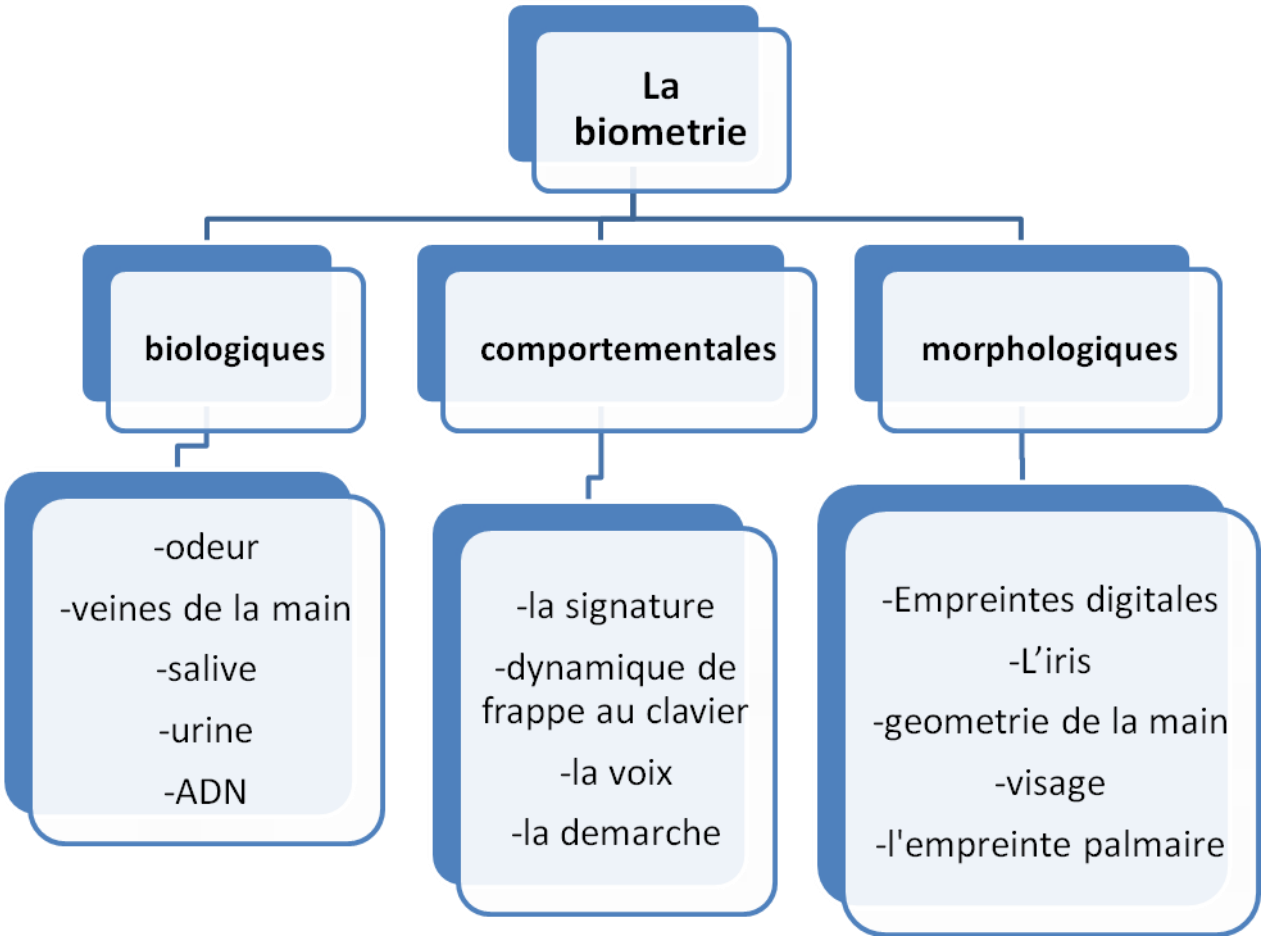


Figure I.4 : Schéma globale de la biométrie.

Les **biométries morphologiques** sont celles qui connaissent le plus grand déploiement dans les entreprises. L'identification à partir des empreintes digitales est la plus courante. L'empreinte est unique et immuable. Ses caractéristiques peuvent être numérisées. La reconnaissance de la personne se fait par le passage du doigt sur le lecteur, qui contrôle ensuite la validité de l'empreinte par la comparaison de points prédéfinis. Des limites existent néanmoins : empreinte modifiée par une brûlure, une coupure ou l'utilisation de produits corrosifs. Les lecteurs d'empreintes peuvent être combinés avec la carte à puce : l'empreinte est stockée dans le circuit intégré de cette dernière et la lecture s'effectue directement dans l'ordinateur. L'iris, du fait de ses caractéristiques propres, collerette, cryptes, tâches pigmentaires…, permettant de distinguer indéniablement un individu, constitue un autre support biométrique efficace. La fixation de l'objectif d'une caméra balayant l'iris permet la reconnaissance. La reconnaissance veineuse se fait, quant à elle, à partir de la lecture de la paume de la main. Contrairement aux empreintes qui peuvent se modifier, le réseau veineux de la main s'avère être le plus fiable. De plus, la lecture se fait sans contact, limitant le nombre de facteurs susceptibles de la fausser (notamment de possibles résidus résultant d'un précédent passage). Enfin, la biométrie s'est développée en matière de reconnaissance faciale ou de lecture du contour de la main.

Parallèlement, **les biométries comportementales** se développent. Elles se focalisent entre autres sur la dynamique de la frappe sur le clavier, la reconnaissance vocale, ou la signature. Ainsi, des facteurs, telles que la vitesse ou les accélérations, sont pris en compte pour identifier une personne. Mais leur fiabilité semble moins sûre que les biométries morphologiques. Elles sont donc moins utilisées par les entreprises.

Quant aux **analyses biologiques**, par leur coût, leur difficulté de mise en place, elles restent réservées aux sphères judiciaires et policières. Toutes les méthodes biométriques empruntent le même fonctionnement, c'est-à-dire la lecture de caractéristiques propres à l'individu, les paramètres traités générant une signature unique, enregistrée dans un dépôt de données. L'ensemble du processus porte le nom « enrôlement ». Lorsqu'une personne doit s'identifier, un terminal de lecture est utilisé : les caractéristiques saisies sont alors comparées aux signatures enregistrées dans le dépôt central des données. [3]

I.1.4 Applications des systèmes biométriques :

Les systèmes biométriques peuvent être utilisés dans un grand nombre d'applications. Pour des raisons de sécurité, la biométrie peut faciliter les transactions, et la vie quotidienne est à la fois plus sûre et plus pratique. Les domaines suivants utilisent des solutions biométriques pour répondre à leurs besoins respectifs :

Applications juridiques :

- Justice et application de la loi : La technologie biométrique et l'application de la loi ont une très longue histoire, et de nombreuses innovations très importantes dans la gestion de l'identité ont émergé de cette relation bénéfique. Aujourd'hui, la biométrie appliquée par la police est vraiment multimodale. La reconnaissance des empreintes digitales, du visage et de la voix joue un rôle unique dans l'amélioration de la sécurité publique et le suivi des personnes que nous recherchons.

Les applications gouvernementales :

- **Contrôle frontalier et aéroport :** un domaine d'application clé de la technologie biométrique est à la frontière. La technologie biométrique aide à automatiser le passage de la frontière. Des initiatives fiables et automatisées de contrôle des passagers et des SAS automatisés facilitent l'expérience des voyageurs internationaux tout en améliorant l'efficacité des organismes gouvernementaux et en maintenant les frontières plus sûres que jamais.
- **Santé :** Dans le domaine de la santé, la biométrie introduit un modèle amélioré. Les dossiers médicaux sont parmi les documents personnels les plus précieux ; les médecins doivent pouvoir y accéder rapidement et ils doivent être exacts. Un manque de sécurité et une bonne comptabilité peuvent faire la différence entre un diagnostic rapide et précis et la fraude en matière de santé.

Applications commerciales :

- **Sécurité :** Alors que la connectivité continue de se répandre dans le monde entier, il est clair que les anciennes méthodes de sécurité ne sont tout simplement pas assez solides pour protéger ce qui est le plus important. Heureusement, la technologie biométrique est plus accessible que jamais, prête à offrir plus de sécurité et de

commodité pour tout ce qui doit être protégé, de la porte d'une voiture au NIP du téléphone.

- **Finance :** Parmi les applications les plus populaires de la technologie biométrique, l'identification financière, la vérification et l'authentification dans le commerce aident à rendre les opérations bancaires, les achats et la gestion des comptes plus sûrs et plus pratiques et responsables. Dans le domaine financier, les solutions biométriques aident à s'assurer qu'un client est la personne qu'il prétend être lorsqu'il accède à des données financières sensibles en entrant ses caractéristiques biométriques uniques et en les comparant à un modèle stocké dans un appareil ou sur un serveur sécurisé. Les solutions bancaires et les technologies de paiement disponibles aujourd'hui utilisent un large éventail de modalités biométriques : empreintes digitales, iris, voix, visage, empreintes digitales, veines de paume, comportement et autres types de reconnaissance biométrique sont tous utilisés seuls ou combinés de manière multifactorielle comme un système, pour bloquer les comptes et lutter contre la fraude.
- **Mobile :** Les solutions biométriques mobiles vivent à l'intersection de la connectivité et de l'identité. Ils intègrent un ou plusieurs termes biométriques à des fins d'authentification ou d'identification et tirent parti des téléphones intelligents, des tablettes, d'autres types d'appareils portatifs, de la technologie portable et de l'Internet des objets pour des capacités de déploiement polyvalentes. Grâce à la polyvalence apportée par la technologie mobile moderne, ainsi qu'à la prolifération des paradigmes mobiles dans le monde du consommateur, public et privé, la biométrie mobile devient de plus en plus importante. [4]

I.2 Section 2 : La reconnaissance faciale :

I.2.1 Définition :

Un système de reconnaissance faciale est une technologie capable de faire correspondre un visage humain à partir d'une image numérique ou d'une trame vidéo à une base de données de visages, généralement utilisée pour authentifier les utilisateurs par le biais de services de vérification d'identité, en repérant et en mesurant les caractéristiques faciales d'une image donnée [5].

Ces caractéristiques faciales comprennent souvent la distance entre les yeux, la distance du front au menton, et d'autres "points de repère du visage" - créant ainsi votre "signature faciale". La technologie de reconnaissance faciale est utilisée par les agences gouvernementales, ainsi que par des sociétés privées. [6]

La reconnaissance faciale, en tant que type de méthodes biométriques, présente les caractéristiques suivantes : sans contact, sécurité et commodité. Elle est largement utilisée dans les domaines de l'interaction homme-machine, des transactions, de l'authentification, de la sécurité, etc.

Ces dernières années, avec le développement de l'Internet mobile et des ordinateurs embarqués, il devient possible d'exécuter la reconnaissance faciale sur un système embarqué. Ce type d'application a un énorme potentiel dans le paiement à distance et la sécurité des informations personnelles. La procédure de reconnaissance des visages comprend la détection, la normalisation et la reconnaissance des visages. [7]

I.2.2 Pourquoi la reconnaissance faciale ? :

La reconnaissance faciale semble offrir plusieurs avantages par rapport aux autres méthodes biométriques, dont quelques-uns sont présentés ici :

Presque toutes ces technologies nécessitent une action volontaire de la part de l'utilisateur, c'est-à-dire que celui-ci doit placer sa main sur un repose-main pour la prise d'empreintes digitales ou la détection de la géométrie de la main, ou bien se tenir dans une

position fixe devant une caméra pour l'identification de l'iris ou de la rétine. En revanche, la reconnaissance du visage peut être passive, sans action ou participation explicite de la part de l'utilisateur puisque les images du visage peuvent être acquises à distance par une caméra. Ceci est particulièrement bénéfique à des fins de sécurité et de surveillance. En outre, l'acquisition de données en général pose des problèmes pour les autres formes de biométrie : les techniques qui reposent sur les mains et les doigts peuvent être rendues inutilisables si le tissu de l'épiderme est endommagé d'une manière ou d'une autre (c'est-à-dire contusionné ou fissuré).

L'identification par l'iris et la rétine nécessitent des équipements coûteux et sont beaucoup trop sensibles à tout mouvement du corps. La reconnaissance vocale est sensible aux bruits de fond dans les lieux publics et aux fluctuations auditives d'une ligne téléphonique ou d'un enregistrement sur bande. Les signatures peuvent être modifiées ou falsifiées. Cependant, les images faciales peuvent être facilement obtenues avec quelques caméras fixes bon marché. De bons algorithmes de reconnaissance des visages et un prétraitement approprié des images peuvent compenser le bruit et les légères variations d'orientation, d'échelle et d'illumination.

Enfin, les technologies qui exigent que plusieurs individus utilisent le même équipement pour capturer leurs caractéristiques biologiques exposent potentiellement l'utilisateur à la transmission de germes et d'impuretés provenant d'autres utilisateurs. En revanche, la reconnaissance faciale est totalement non intrusive et ne comporte pas de tels risques pour la santé. [8]

I.2.3 technologie de la reconnaissance faciale :

I.2.3.1 Principe de fonctionnement de base d'un système de reconnaissance faciale :

Un système de reconnaissance faciale contient 3 principaux sous-systèmes : détection d'image, extraction des caractéristiques et pour finir la reconnaissance faciale (Figure I.5)

Figure I.5 : Principe de fonctionnement de base d'un système de reconnaissance faciale.

- **Détection faciale :**

Un système de détection faciale détermine la présence ou pas d'un visage dans une image et conçu pour répondre à la question : cette image contient-elle un visage ?

Le module de détection de visages permet de fournir en sortie une image du visage isolé du reste de la scène et prête à être traitée. L'efficacité des systèmes biométriques basés sur l'identification et/ ou authentification de visage dépend essentiellement de la méthode utilisée pour localiser le visage dans l'image(Figure I.6). [9]

Figure I.6 : Image de détection faciale.

- **Extraction des caractéristiques :**

Le rôle de cette étape est d'extraire les informations utiles qui reviennent à établir un modèle du visage (vecteur de caractéristiques). Ces informations nécessaires tel que les yeux, la bouche, la forme du nez, la distance entre les yeux, etc. Pour que le visage d'une personne ne ressemble pas à celui d'un autre, en même temps qu'il ressemble à lui-même dans d'autres conditions d'acquisition (Figure I.7). [9]

Figure I.7 : Image d'extraction des caractéristiques

- **Reconnaissance faciale :**

Il s'agit de l'étape de la vérification du système si les caractéristiques prise dans l'étape précédente correspondent aux caractéristiques de l'image ou d'une des images existantes dans la base de données. Et ainsi évaluer si ce visage est reconnu ou pas (dans le cas de ce projet, évaluer si le système de sécurité permet ou pas l'accès à cette personne) (FigureI.8).

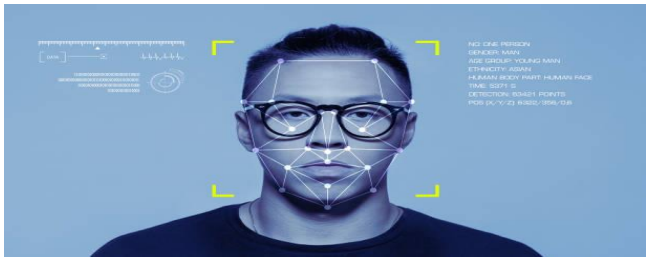
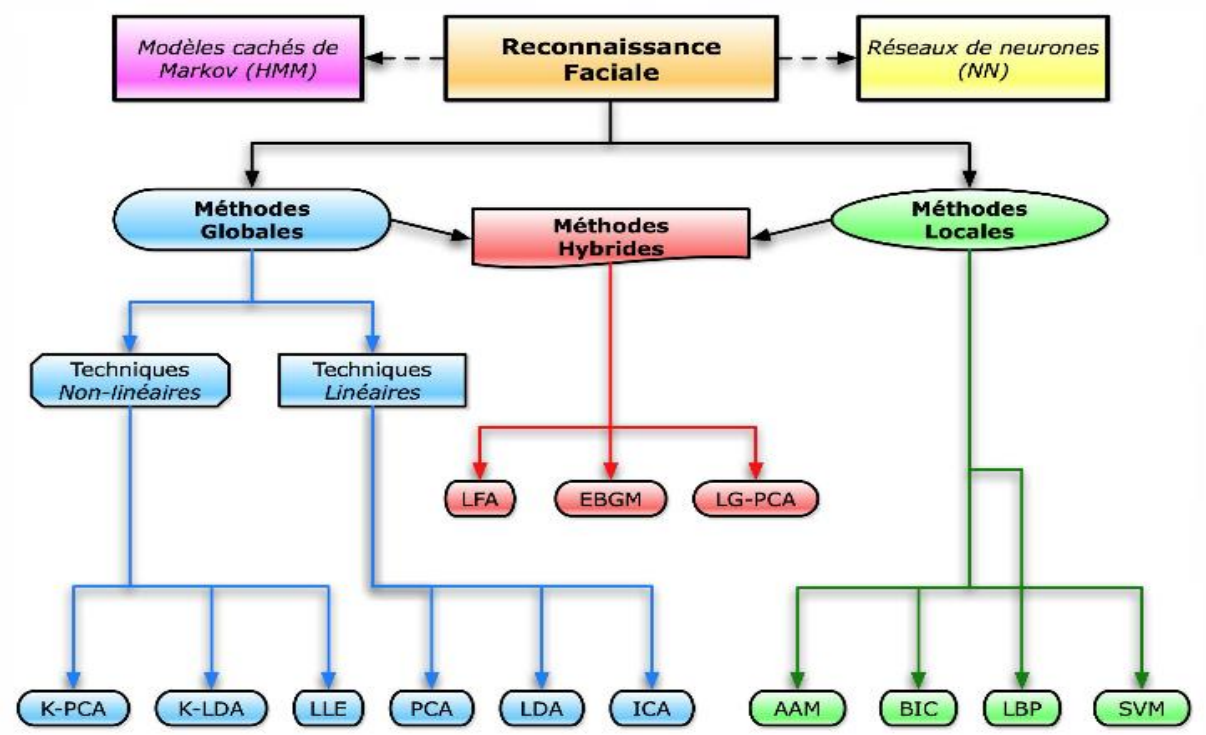


Figure I.8 : Image de reconnaissance faciale.

I.2.3.2 Méthodes de reconnaissance faciale :

Plusieurs méthodes de reconnaissance de visages ont été proposées durant les vingt dernières années. Elle est un axe de recherche ouvert attirant des chercheurs venants de disciplines différentes : psychologie, reconnaissance de formes, réseaux de neurone, vision artificielle et infographie. Les caractéristiques qui servent à la reconnaissance du visage sont les yeux, la bouche, la forme du visage (contour), etc. Les méthodes de reconnaissance faciales peuvent être séparées en trois grandes familles, les méthodes globales (ou holistiques), les méthodes locales, basées sur des modèles et les méthodes hybrides. Le diagramme suivant fournit une classification des méthodes principales de reconnaissance faciale (Figure I.9) : [2]



FigureI.9 : méthodes principales utilisées dans la reconnaissance de visage [2]

- **Méthodes globales :**

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, le centre de la bouche, etc.) à part pour normaliser les images. Dans ces méthodes, les images de visage (qui peuvent être vues comme des matrices de valeurs de pixels) sont traitées de manière globale et sont généralement transformées en vecteurs, plus faciles à manipuler. L'avantage principal des méthodes globales est qu'elles sont relativement rapides à mettre en œuvre et que les calculs de base sont d'une complexité moyenne. En revanche, elles sont très sensibles aux variations d'éclairement, de pose et d'expression faciale. Ceci se comprend aisément puisque la moindre variation des conditions de l'environnement entraîne des changements inéluctables dans les valeurs des pixels qui sont traités directement. [2]

Ces méthodes utilisent principalement une analyse de sous-espaces de visages. Nous pouvons distinguer deux types de techniques parmi les méthodes globales : les techniques linéaires et les techniques non linéaires. [2]

a. Les techniques linéaires :

Les techniques linéaires réalisent une projection linéaire des données d'un espace de grande dimension (par exemple, l'espace de l'image originale) sur un sous -espace de dimension inférieure. Cependant, ces techniques linéaires sont sensibles aux conditions de luminosité notamment, et plus généralement aux variations non convexes. Ainsi, l'utilisation de distances classiques dans l'espace projeté ne permet pas toujours de réaliser une bonne classification entre les classes « visages » et « non visages ».[10] Ce facteur crucial limite le pouvoir des techniques linéaires pour obtenir une détection et une reconnaissance du visage très précises. Parmi les méthodes globales les plus connues il y'a ACP (Analyse en Composante Principale) plus connue sous le nom de Eigen faces, ADL (Analyse Discriminante Linéaire) et ACI (Analyse en Composante Indépendantes) [9]

b. Les techniques non linéaires ;

Afin de pouvoir traiter le problème de la non-linéarité, des techniques globales non linéaires ont été développées, souvent à partir des techniques linéaires. Ainsi l'Analyse en Composantes principales à Noyaux (ou « Kernel –PCA ») et l'Analyse Discriminante linéaire à Noyaux (ou « Kernel–LDA ») utilisent la notion mathématique des noyaux en étendant les techniques linéaires l'ACP et la LDA.

D'autres techniques non linéaires ont également été utilisées dans le contexte de la reconnaissance faciale : [9]

– le Multidimensional Scaling (MDS)

– l'Isomap,

– les diffusions maps,

– le Local Linear Embedding (LLE)

– les Laplacian ei genmaps

– le Hessian LLE

– le Local Tangent Space Analysis (LTSA)

– les approches neuronales

L'utilisation de ces méthodes de projection de l'espace des images sur l'espace de caractéristiques est non linéaire et permet ainsi dans une certaine mesure de réduire la dimension des images de meilleure façon. Cependant, bien que ces méthodes permettent souvent l'amélioration des taux de reconnaissance sur des jeux de tests donnés, elles sont trop flexibles pour être robustes à de nouvelles données, contrairement aux méthodes linéaires. [9]

- **Méthodes locales :**

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.

Ces méthodes constituent une autre approche pour prendre en compte la non-linéarité en construisant un espace de caractéristiques local et en utilisant des filtres d'images appropriés, de manière à ce que les distributions des visages soient moins affectées par divers changements. Toutes ces méthodes ont l'avantage de pouvoir modéliser plus facilement les variations de pose, d'éclairage et d'expression par rapport aux méthodes globales. Toutefois, elles sont plus lourdes à utiliser puisqu'il faut souvent placer manuellement un assez grand nombre de points sur le visage alors que les méthodes globales ne nécessitent de connaître que la position des yeux afin de normaliser les images, ce qui peut être fait automatiquement et de manière assez fiable par un algorithme de détection [11].

Dans cette catégorie, on trouve plusieurs méthodes comme : HMM (Hidden Markov Models), RNA (réseaux de neurones) et SVM (Machines à Vecteur de Support). [9]

- **Méthodes hybrides :**

Les méthodes hybrides permettent d'associer les avantages des méthodes globales et locales en combinant la détection de caractéristiques géométriques (ou structurales) avec l'extraction de caractéristiques d'apparence locales. Elles permettent d'augmenter la stabilité de la performance de reconnaissance lors de changements de pose, d'éclairement et d'expressions faciales [12].

Parmi les algorithmes de reconnaissance de cette méthode nous citons l'EBGM. [9]

I.2.4 Les principales difficultés de la reconnaissance faciale :

Reconnaître les visages humains à partir d'images et de vidéos n'est pas une mince affaire. Il existe de nombreuses approches pour réaliser cette tâche mais aucune n'est capable de l'accomplir avec une avec une précision de 100% en raison des nombreux facteurs à prendre en compte. Ces facteurs sont divisés en 2 catégories, les facteurs intrinsèques et les facteurs extrinsèques. Les facteurs intrinsèques comprennent l'état physique du visage humain (vieillissement, expressions faciales, etc.) qui affectent le système, tandis que les facteurs extrinsèques sont les facteurs qui deviennent une raison pour changer l'apparence du visage, par exemple l'éclaircissement, la variation de la pose. [13]

I.2.4.1 Le vieillissement :

Le vieillissement est l'un des facteurs intrinsèques qui influencent les techniques de reconnaissance des visages car il s'avère être un désordre pour les algorithmes. La permanence est une qualité essentielle pour que toute mesure biologique soit considérée comme biométrique. Le visage est un mélange de tissus de la peau, de muscles faciaux et d'os. Lorsque les muscles se contractent, ils déforment les traits du visage. Cependant, le vieillissement entraîne des altérations significatives de l'apparence du visage d'un individu, par exemple la texture du visage (rides, etc.) et la forme du visage (Figure I.10). [14]

Figure I.10 : Vieillissement

I.2.4.2 Expressions faciale :

L'expression faciale est une approche de la communication non verbale car elle permet de transmettre des messages à l'aide d'expressions. Cependant, la variation des expressions crée un flou pour les systèmes de reconnaissance des visages. De nombreux systèmes de reconnaissance ont été développés qui fonctionnent bien pour les images dans un environnement contrôlé. Différentes expressions faciales montrent différentes humeurs, attitudes des gens, et modifient la géométrie des visages, s'il y a une variation mineure dans l'image, et ainsi la reconnaissance faciale devient difficile (Figure I.11). [15]

Figure I.11 : Expressions faciales

I.2.4.3 Variation de pose :

La variance de pose est encore un autre obstacle à la réussite d'un système de reconnaissance faciale. Les gens posent différemment à chaque fois qu'ils prennent une photo. Il n'existe pas de pose standard similaire. Ainsi, cela rend difficile de distinguer et de reconnaître les visages à partir des images avec des poses différentes. Les variations de pose dégradent la performance de l'exigence de visage. La plupart des systèmes fonctionnent dans des conditions d'imagerie rigides (Figure I.12). [15]

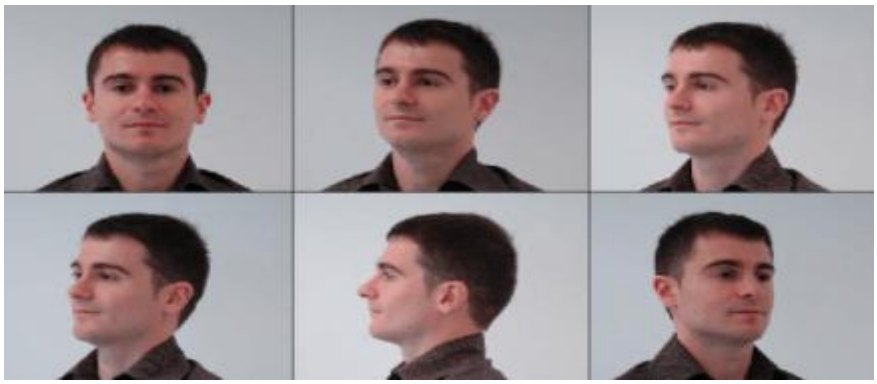


Figure I.12 : Variation de pose

I.2.4.4 Occlusion :

L'occlusion fait référence à des obstacles naturels ou artificiels dans une image. Les approches de la reconnaissance faciale avec une occlusion partielle sont classées en différentes catégories, notamment les méthodes basées sur les parties, les méthodes basées sur les caractéristiques et les méthodes basées sur les fractales. [16] De nombreux domaines du traitement de l'image ont été impactés par l'occlusion partielle, comme la reconnaissance par l'oreille est occultée à cause des boucles d'oreilles. L'occlusion affecte les performances d'un système lorsque des personnes le trompent soit par l'utilisation de lunettes de soleil, foulards, voiles ou en plaçant les téléphones portables ou les mains devant le visage, ou même le changement d'apparence (barbe, maquillage, etc.) Parfois, d'autres facteurs comme ombres dues à un éclairage extrême agissent également comme des facteurs d'occlusion. Les approches locales sont utilisées pour traiter le problème d'occlusion partielle, en divisant les visages en différentes parties (Figure I.13). [17]

Figure I.13 : Exemple d'occlusion du visage

I.2.4.5 Variation d'illumination :

La variation de l'illumination affecte beaucoup le système de reconnaissance des visages. Il devient difficile de reconnaître une ou plusieurs personnes à partir d'images fixes ou vidéo. Il est assez facile d'extraire l'information désirée d'images prises dans un environnement contrôlé où l'arrière-plan est uniforme, cependant, dans un environnement non contrôlé, le visage doit être reconnu à partir de divers arrière-plans. Cela inclut les variations dues aux ombres, la surexposition et la sous-exposition (Figure I.14). [15]

Figure I.14 : Variation d'illumination

Conclusion :

Les technologies biométriques se développent de plus en plus jour après jour, pénétrant de nombreux domaines de notre vie. De toutes les mesures biométriques, la reconnaissance faciale est la plus naturelle. Cela a un sens intuitif parce que nous nous connaissons nous-mêmes et les autres en regardant leurs visages plutôt que leurs empreintes et leurs iris. Dans le chapitre suivant nous présenterons la carte ESP32-CAM qui nous aidera à réaliser notre système de sécurité basé sur la reconnaissance faciale, ainsi que ses ressources et les bibliothèques associées.

Chapitre II :

ESP 32-CAM

Introduction :

L'ESP32-CAM est une petite carte de développement à faible coût basée sur l'ESP32 avec une caméra embarquée. C'est un excellent choix pour les applications IOT, les prototypes et les projets de bricolage.

Le but de ce chapitre est de décrire le module ESP32-CAM qu'on va utiliser dans ce projet pour la détection et la reconnaissance faciale, donner ses caractéristiques ainsi que ses différentes applications

II.1 Description du module ESP32-CAM :

L'ESP32-CAM est une carte de développement ESP-WROOM-32 du fabricant AI Thinker associé à une caméra couleur 2MP OV2640. Le module ESP32-CAM dispose également d'un lecteur de carte SD qui pourra servir à enregistrer des images lorsqu'un événement est détecté (détecteur de présence ou de mouvement par exemple).

La société E fournit une API complète qui permet d'accéder à toutes les fonctionnalités du module caméra. C'est vraiment une excellente base pour développer son propre système de vidéosurveillance IP sans avoir la crainte que le flux vidéo arrive sur des serveurs douteux.

L'ESP-32CAM peut être utilisé dans diverses applications IOT. Elle convient aux appareils intelligents domestiques, aux commandes sans fil industrielles, à la surveillance sans fil, à l'identification sans fil QR, aux signaux du système de positionnement sans fil et à d'autres applications IOT. C'est une solution idéale pour les applications IOT. [18]

Figure II.1 CARTE DE DÉVELOPPEMENT ESP32-CAM

II.2 CARACTERISTIQUES TECHNIQUES :

II.2.1 Spécifications ESP32-CAM :

L'ESP32-CAM est basé sur le module esp32-s, donc il partage les mêmes spécifications. Il a les caractéristiques suivantes :

- 802.11b/g/n Wi-Fi
- Bluetooth 4.2 avec BLE
- Interfaces UART, spi, i2c et PWM
- Vitesse d'horloge jusqu'à 160 MHZ
- Puissance de calcul jusqu'à 600 DMIPS
- 520 ko SRAM plus 4 mo PSRAM
- Prise en charge wifi image Upload
- Plusieurs modes de veille
- Mise à niveau possible du micro logiciel over the air (fota)
- 9 ports GPIO
- LED flash intégrée

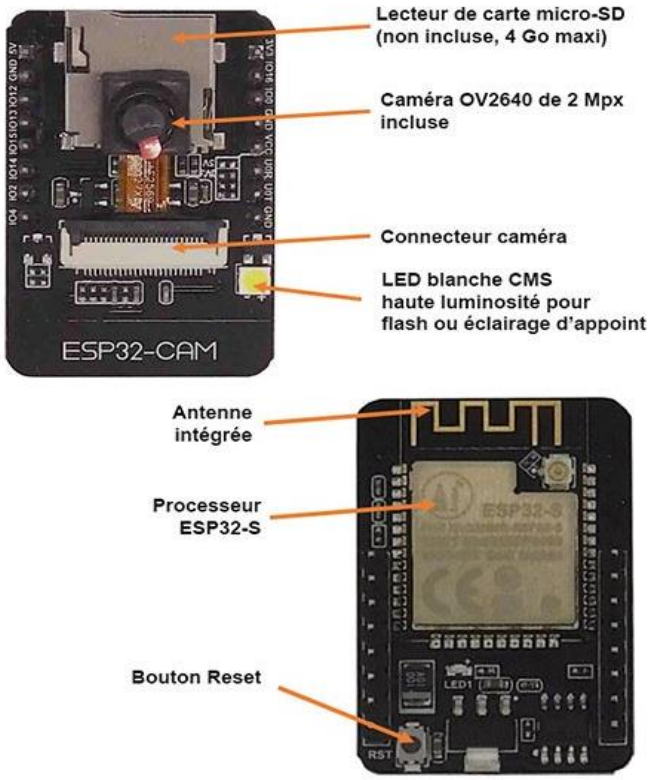


Figure II.2 Les composants de la carte ESP32-CAM

II.2.2 Spécifications de la caméra :

L'ESP32-CAM comprend un module de caméra OV2640. L'appareil prend également en charge les caméras OV7670. L'OV2640 a les caractéristiques suivantes :

- Capteur de 2 mégapixels
- Taille du réseau UXGA 1622 1200
- Les formats de sortie incluent les données compressées YUV422, YUV420, RGB565, RGB555 et 8 bits
- Taux de transfert d'image de 15 à 60 images/s. [19]

Figure II.3 Module de caméra ArduCAM OV2640

II.2.3 Broches GPIO ESP32 CAM

Il existe plusieurs broches GPIO qui prennent en charge comme UART, SPI, I2C, PWM, CAN et CNA. Il est possible d'obtenir une broche VCC 3,3 V ainsi qu'une broche 5 V à partir de ce module. Il existe également plusieurs broches GND.

Les broches suivantes sont connectées en interne au lecteur de carte micro SD :

GPIO 14 : CLK

GPIO 15 : CMD

GPIO 2 : Données 0

GPIO 4 : Données 1 (également connecté à la LED intégrée)

GPIO 12 : Données 2

GPIO 13 : Données 3

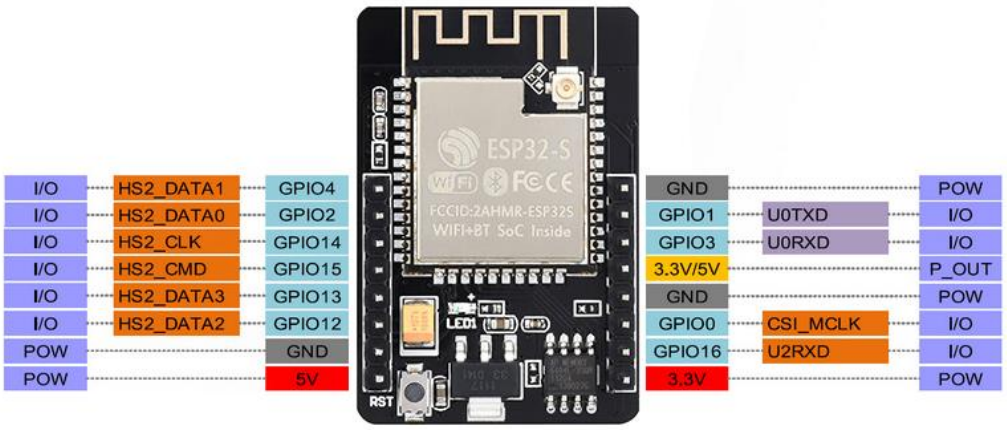


Figure II.4 différentes broches de l'ESP32-CAM

II.2.4 Connexion ESP32-CAM FTDI :

Pour programmer la carte, il faut utiliser un module de conversion USB vers TTL ou d'un module FTDI. Il y a tellement de modules FTDI disponibles basés sur la puce CP2102 ou CP2104 ou toute autre puce.

Pour commencer avec le module CAM ESP32, Il faut établir la connexion suivante entre le module FTDI et le module CAM ESP32.[20]

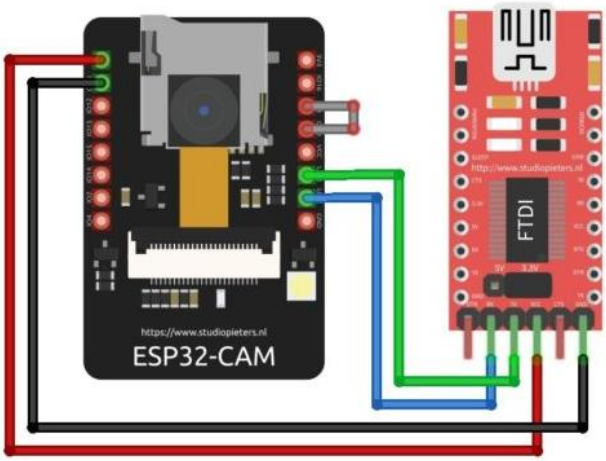


Figure II.5 Connexion ESP32-CAM FTDI

ESP32-CAM	PROGRAMMATEUR FTDI
GND	GND
5V	VCC (5v)
UOR	TX
UOT	RX
GPIO 0	GND

Tableau II.1 Connexion ESP32-CAM avec le module FTDI

II.3 APPLICATIONS :

• Appareils domestiques intelligents

• Surveillance sans fil

• Scanner OR intelligent

• Al - Reconnaissance faciale

• Ville intelligente

• Utiliser comme vidéosurveillance personnelle et webcam

• Diffusion en direct. [21]

CONCLUSION :

Dans ce chapitre, nous avons appris que l'ESP32 CAM est un module polyvalent et puissant qui offre un large éventail de caractéristiques et de spécifications. Son intégration transparente avec les langages et les cadres de programmation populaires en fait un rêve de développeurs. Grâce à sa capacité à capturer des images de haute qualité et à diffuser des vidéos, l'ESP32 CAM trouve ses applications dans les systèmes de sécurité, la surveillance à distance, les projets IOT, et bien plus encore.

Chapitre III :

Simulation et réalisation pratique

Introduction :

Ce chapitre contient deux parties qui aborderont la simulation de la reconnaissance faciale et la réalisation pratique d'un système de sécurité.

La première partie de ce chapitre couvre les bases d'OpenCV Python et la manière de l'utiliser pour la reconnaissance faciale. Nous décrivons le processus d'entraînement d'un modèle de reconnaissance de visages et la manière dont il peut être utilisé pour reconnaître des visages en temps réel. La deuxième partie du chapitre construit un système de verrouillage de porte à reconnaissance faciale à l'aide du module ESP32-CAM (un microcontrôleur bon marché équipé d'un module caméra). Le système est conçu de manière à ce que seules les personnes autorisées puissent y accéder.

Dans l'ensemble, ce chapitre fournit un guide complet pour la création d'un système de verrouillage de porte à reconnaissance faciale à l'aide de l'ESP32-CAM et une simulation de la reconnaissance faciale à l'aide de la bibliothèque OpenCV-Python. À la fin de ce chapitre, le lecteur aura une bonne compréhension des bases de la technologie de reconnaissance faciale et de la manière de l'appliquer pour construire un système de contrôle d'accès sécurisé.

III.1Simulation de la reconnaissance faciale :

Dans cette partie, nous montrerons l'installation des logiciels et bibliothèques nécessaire pour la réalisation d'un système de reconnaissance faciale à l'aide de la webcam du PC et la bibliothèque OpenCV-Python.

III.1.1 Outils de développement :

III.1.1.1 Le Hardware :

Nom de l'appareil : DESKTOP-9GNCOOA
Processeur : Intel(R) Core (TM) i7-5600U CPU @ 2.60 GHz
Mémoire RAM installée : 4.00GO (3.88GO utilisable)
Type du système : Système d'exploitation 64 bits, processeur x64
Camera : Webcam 0.9MP

III.1.1.2 Le Software :

Système d'exploitation : Windows 10 Professionnel version 21H2

Logiciel : Visual Studio Code

La bibliothèque : OpenCV 4.7.0.72

III.1.2 Les étapes d'implémentation :

III.1.2.1 Installation et configuration OpenCV-Python avec Visual studio Code :

Premièrement on doit télécharger Visual studio Code depuis son site officiel : https://code.visualstudio.com/download, le logiciel doit être compatible à notre système d'exploitation (Windows).

.

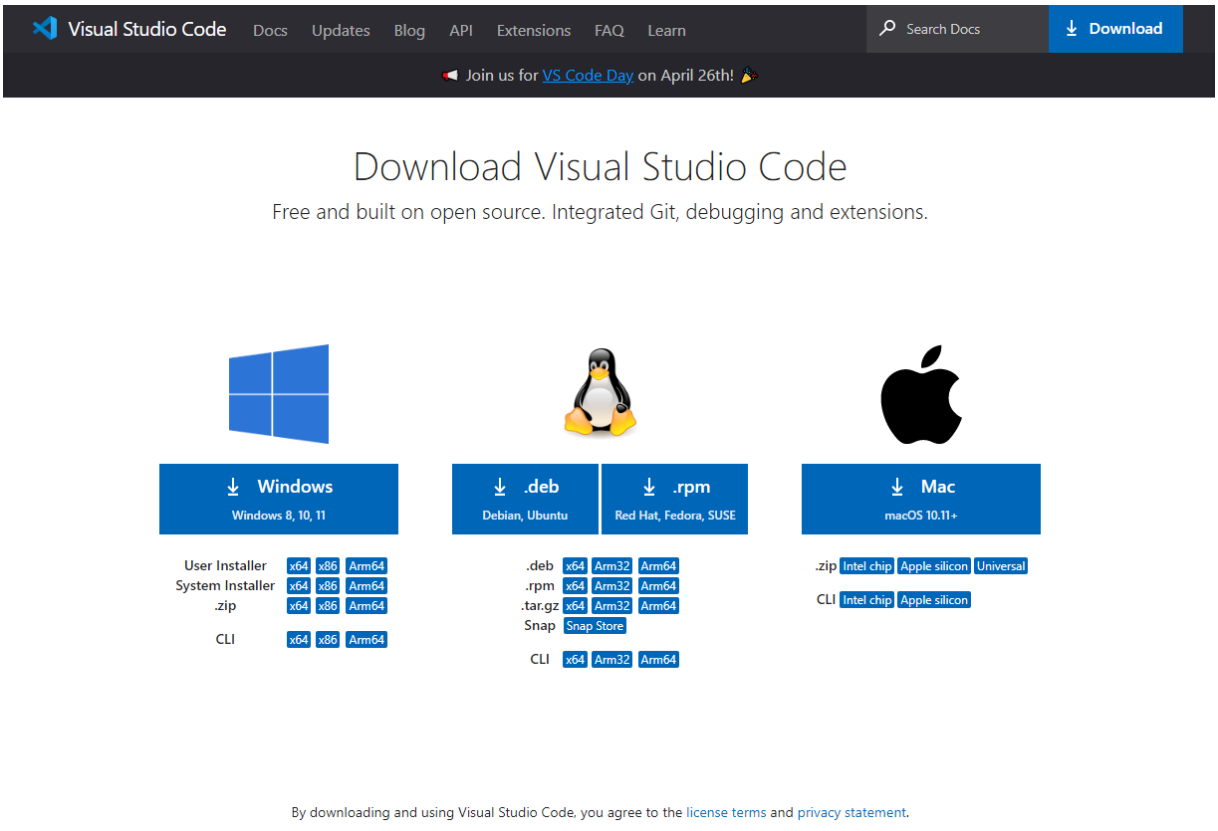


Figure III.1 Site officiel pour télécharger Visual studio Code

III.1.2.2 Téléchargement et installation Python :

Apres l'installation de Visual Studio Code nous devons installer Python, pour ce faire :

a) On clique sur l'onglet : EXTENSIONS

b) On cherche dans la boîte de recherche de mot : Python, Puis on appuie sur le premier résultat.

c) Puis on l'installe en appuyant sur : INSTALL.

d) Lorsque l'installation est terminée, Python est prêt pour l'utilisation.

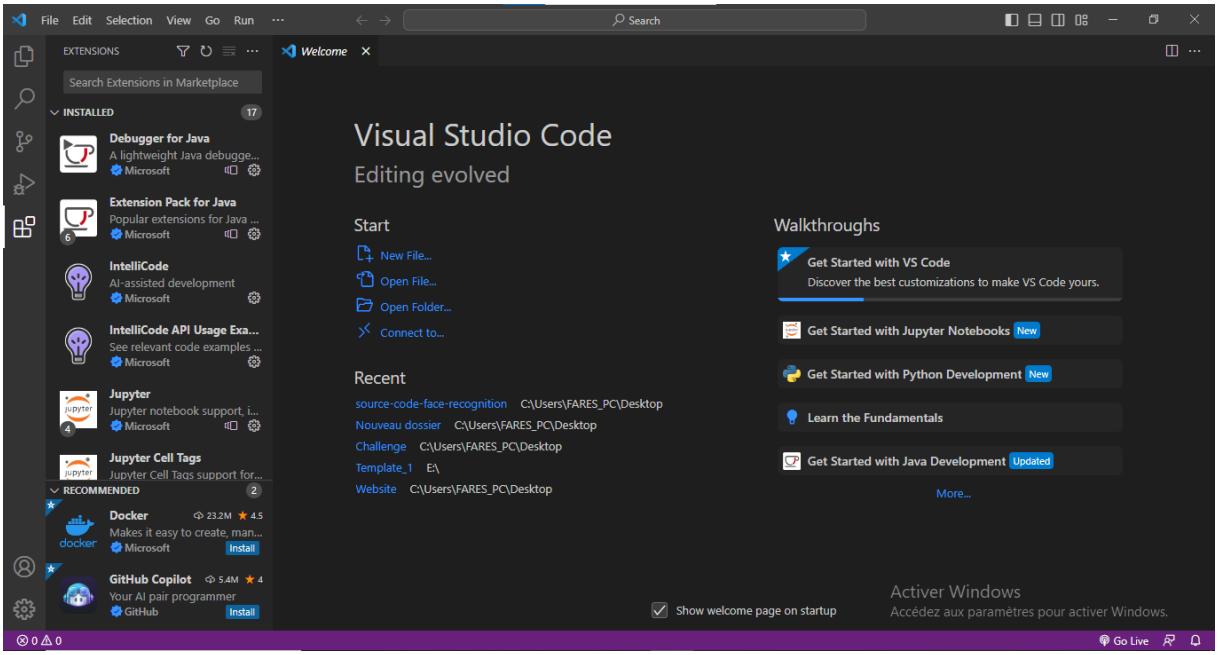


Figure III.2 Installation Python (1)

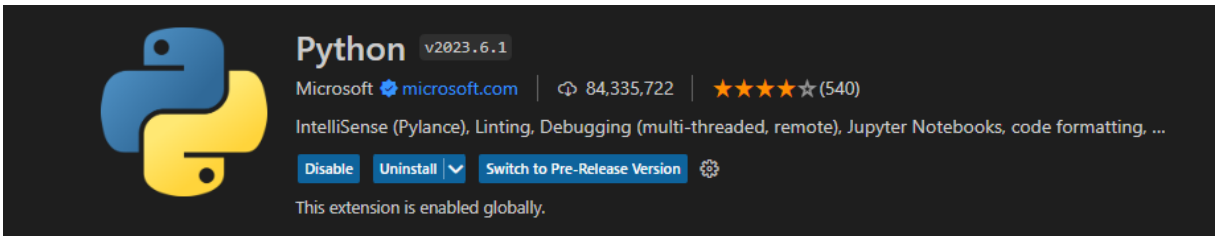


Figure III.3 Installation Python (2)

III.1.2.3 Téléchargement et installation des bibliothèques :

Pour entamer la reconnaissance faciale avec Python et OpenCV, nous devons d'abord installer les bibliothèques nécessaires. Nous pouvons utiliser pip, le gestionnaire de paquets pour Python, pour installer OpenCV :

pip install OpenCV-python

Ensuite, installer la bibliothèque de la reconnaissance faciale, qui s'installe en tapant la commande suivante :

pip install face_recognition

III.1.2.4 Reconnaissance faciale en temps réel sur une webcam :

- **Importation des bibliothèques :**

La première étape consiste toujours à rappeler les bibliothèques que nous avons installées (OpenCV et face_recognition) dans notre projet.

```
1   import cv2
2   from simple_facerec import SimpleFacerec
```

- **Prendre le flux de la webcam**

Avec une simple fonction OpenCV, nous prenons le flux de la webcam et le mettons en boucle

```
 8   # Load Camera
 9   cap = cv2.VideoCapture(0)
10
11
12   while True:
13       ret, frame = cap.read()
```

- **Localisation et reconnaissance faciale :**

Maintenant, nous identifions le visage passant le cadre de la webcam à cette fonction detect_known_faces (frame). Il nous donnera le nom de la personne et un tableau avec la position à chaque instant du

mouvement.

```
15    # Detect Faces
16    face_locations, face_names = sfr.detect_known_faces(frame)
17    for face_loc, name in zip(face_locations, face_names):
18        y1, x2, y2, x1 = face_loc[0], face_loc[1], face_loc[2], face_loc[3]
```

- **Afficher le nom et le rectangle**

Maintenant que nous avons tous les éléments, nous les montrons avec OpenCV.

```
20            cv2.putText(frame, name,(x1, y1 - 10), cv2.FONT_HERSHEY_DUPLEX, 1, (0, 0, 200), 2)
21            cv2.rectangle(frame, (x1, y1), (x2, y2), (0, 0, 200), 4)
22
23        cv2.imshow("Frame", frame)
24
25        key = cv2.waitKey(1)
26        if key == 27:
27            break
```

Et voici comment il montre la personne et le nom :

Figure III.4 Le résultat

III.1.2.5 Résultat après exécution du code :

Après avoir exécuté le code, le visage est précisément déterminé et le nom de la personne est indiqué, même à partir d'images du téléphone ou de la carte personnelle.

Figure III.5 Résultat final

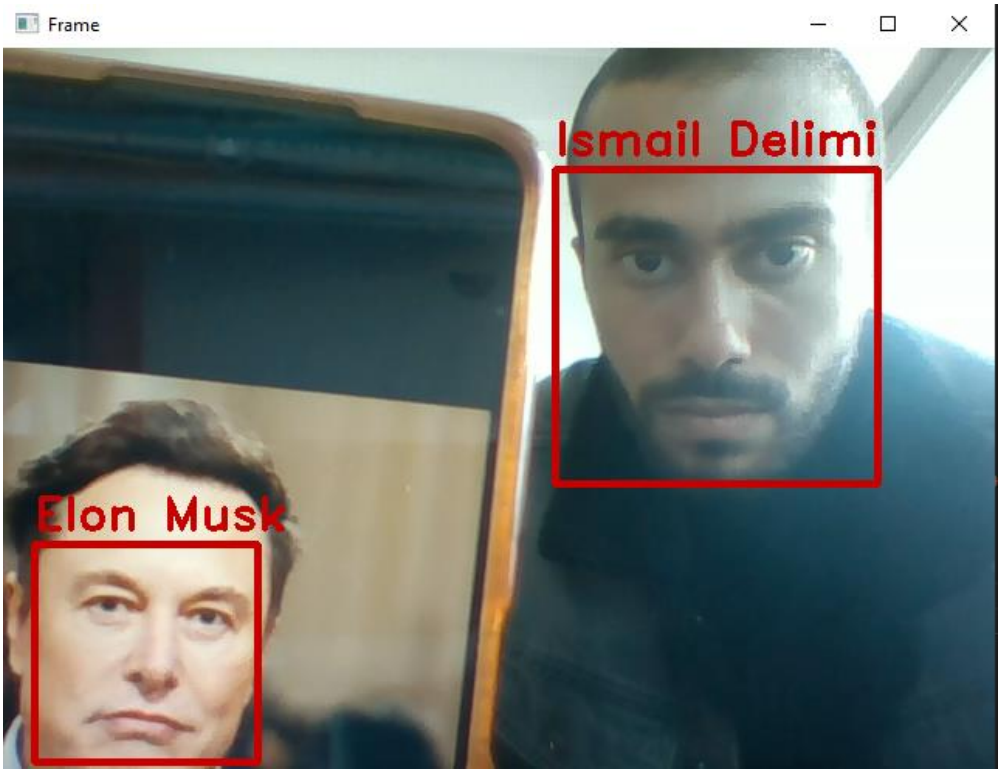


Figure III.6 Résultat finale à partir d'une image d'un téléphone

III.2 Réalisation pratique :

III.2.1 Description du projet :

Ce système utilise la carte ESP32-CAM pour la détection et la reconnaissance faciale en temps réel d'une personne se tenant devant la caméra OV2640. Les visages humains sont ensuite traités à l'aide d'algorithmes d'apprentissage automatique pour les identifier. La serrure de la porte se déverrouille automatiquement si l'utilisateur est reconnu comme un utilisateur autorisé et le message « Access Allowed » est affiché dans le vidéo-streaming avec une petite alerte d'un buzzer actif. Si la personne n'est pas reconnue, le système refuse l'accès en affichant le message « Access Denied ».

Le système compare les visages nouvellement détectés aux visages de la base de données pour déterminer si la personne est autorisée ou pas à accéder à la zone sécurisée. Cela est mieux expliqué dans le diagramme si dessous. (Figure III.18)

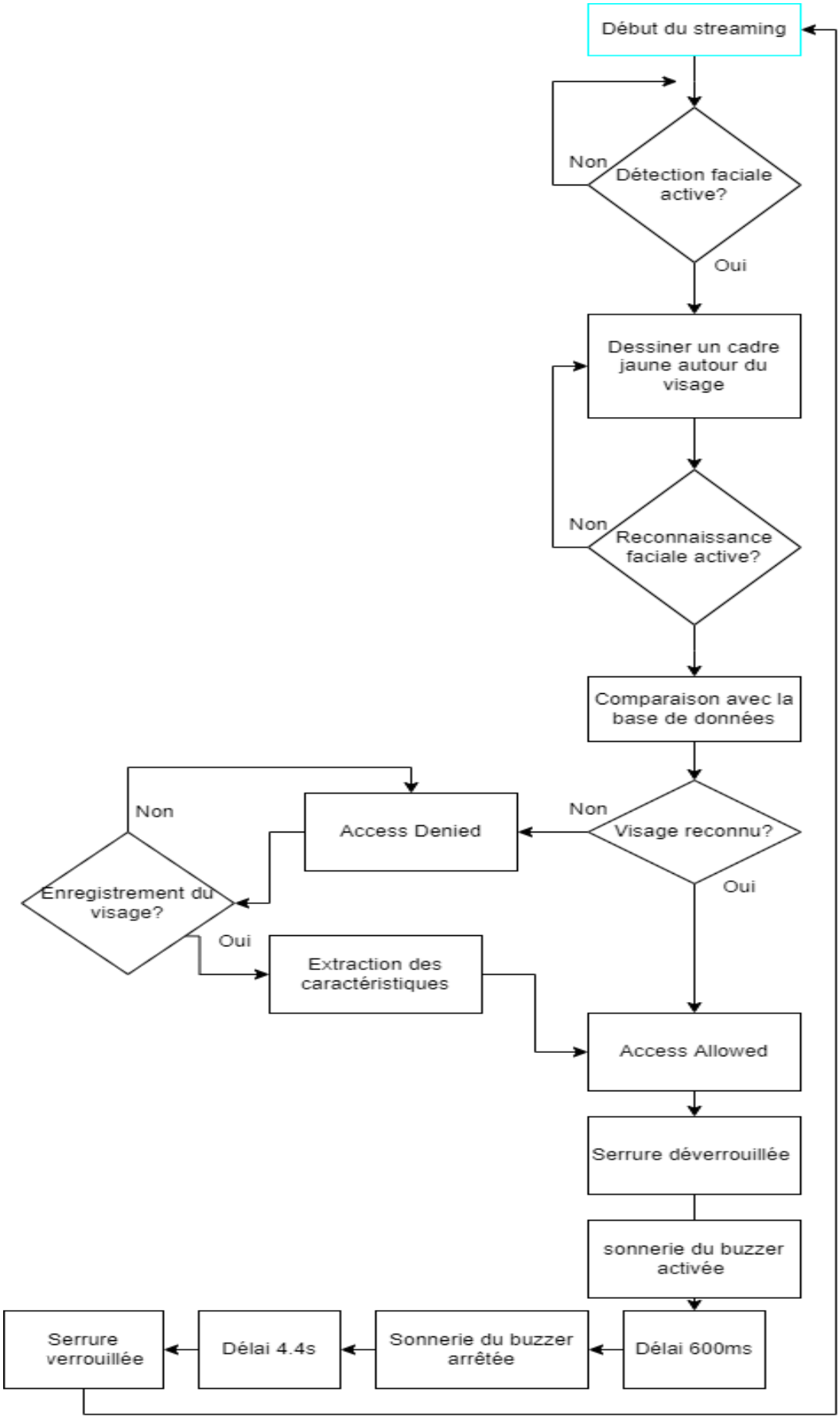


Figure III.7 Diagramme descriptif du système

III.2.2 Description Hardware :

1. ESP 32-CAM :

L'ESP32-CAM est une carte de développement ESP-WROOM-32 du fabricant AI Thinker associé à une caméra couleur 2MP OV2640. Le module ESP32-CAM dispose également d'un lecteur de carte SD qui pourra servir à enregistrer des images lorsqu'un événement est détecté (détecteur de présence ou de mouvement par exemple). [18]

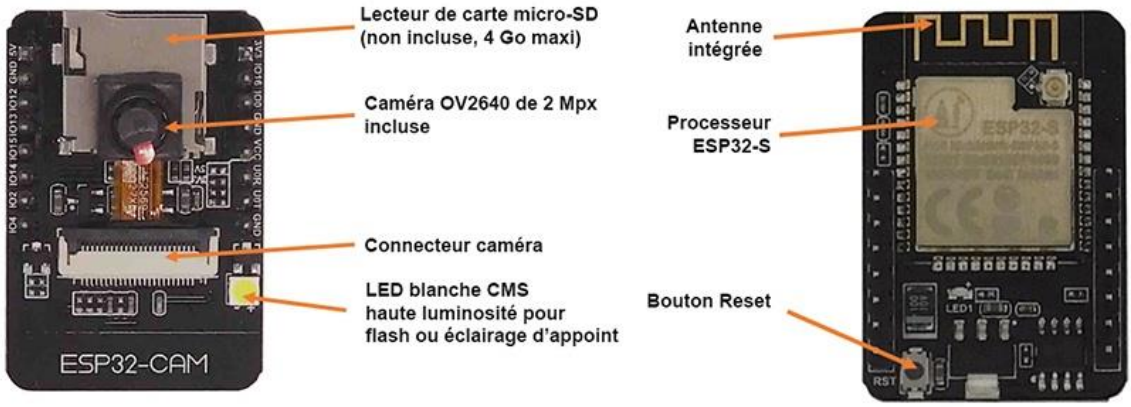


Figure III.8 Description de l'ESP32-CAM

2. Programmateur FTDI, USB à TTL :

Comme l'ESP32-CAM ne contient pas d'entrée USB, il n'est pas possible de le connecter directement à l'ordinateur. Donc on a besoin de faire appel au programmateur FTDI.

Les câbles FTDI sont une famille de câbles convertisseurs USB vers TTL série UART et ils sont incorporés avec le circuit intégré FT232R. La puce gère tout le protocole de conversion des données USB en données série UART. Les câbles offrent un moyen rapide et simple de connecter à l'USB des dispositifs dotés d'une interface série de niveau TTL. Ils ne nécessitent aucune installation logicielle supplémentaire ni aucun paramétrage avant d'être utilisés. Il s'agit donc de dispositifs simples, prêts à l'emploi. [22]

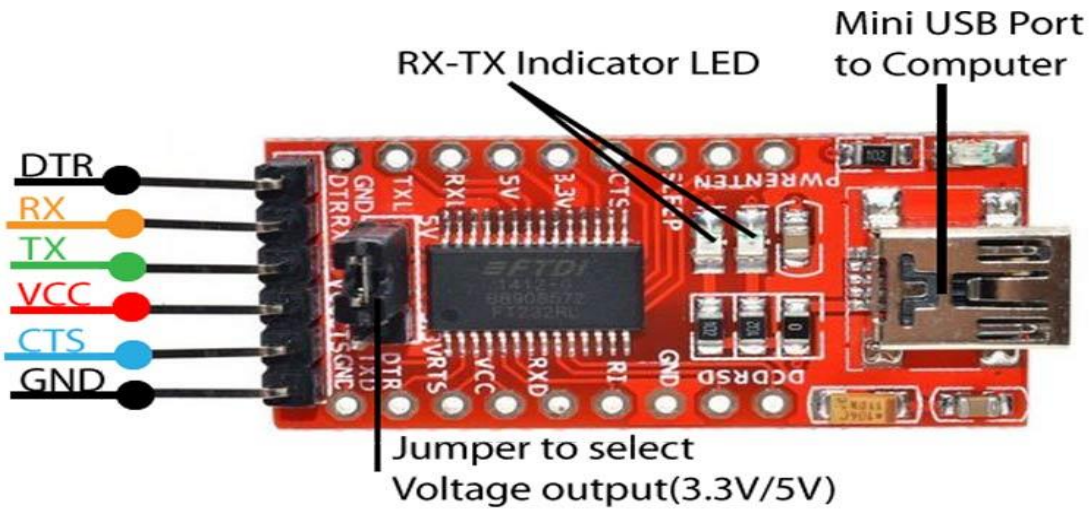


Figure III.9 Description du programmateur FTDI

3. Serrure électrique (solénoïde) 12V :

Les solénoïdes sont des électro-aimants : Ils sont composés d'une grosse bobine de cuivre avec une armature (un noyau en métal) en leur centre. Quand la bobine est alimentée, le noyau est attiré au centre de la bobine. Cela permet au solénoïde de se déplacer. [23]

La serrure à solénoïde 12V est dotée d'une patte avec une coupe inclinée et d'un bon support de montage. Il s'agit essentiellement d'une serrure électronique, conçue pour une armoire, un coffre-fort ou une porte de base. Lorsque l'on applique une tension de 12 V, l'ergot se replie pour ne pas dépasser et la porte peut être ouverte. [24]

Voici une explication simplifiée du fonctionnement d'une serrure à solénoïde :

-Lorsqu'un courant de 12 V CC est appliqué au solénoïde, il crée un champ magnétique.

-Ce champ magnétique attire un plongeur ou un pêne dans le solénoïde, ce qui déverrouille la serrure.

-Le plongeur ou le pêne reste dans cette position tant que le courant est appliqué.

-Lorsque le courant est coupé, le champ magnétique disparaît et le plongeur ou le pêne est libéré, verrouillant à nouveau la serrure.

Les serrures à solénoïde sont souvent utilisées dans des applications nécessitant un haut degré de sécurité, comme les serrures de porte, les coffres forts et les distributeurs automatiques. Elles sont également couramment utilisées dans l'automatisation industrielle et la robotique.

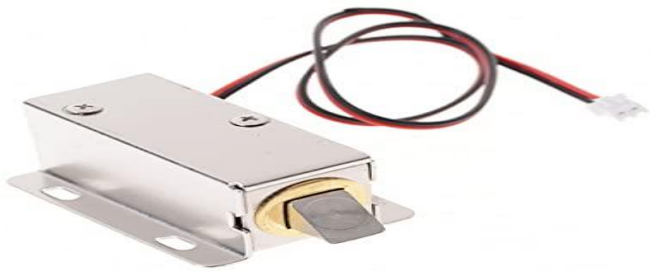


Figure III.10 Serrure électrique

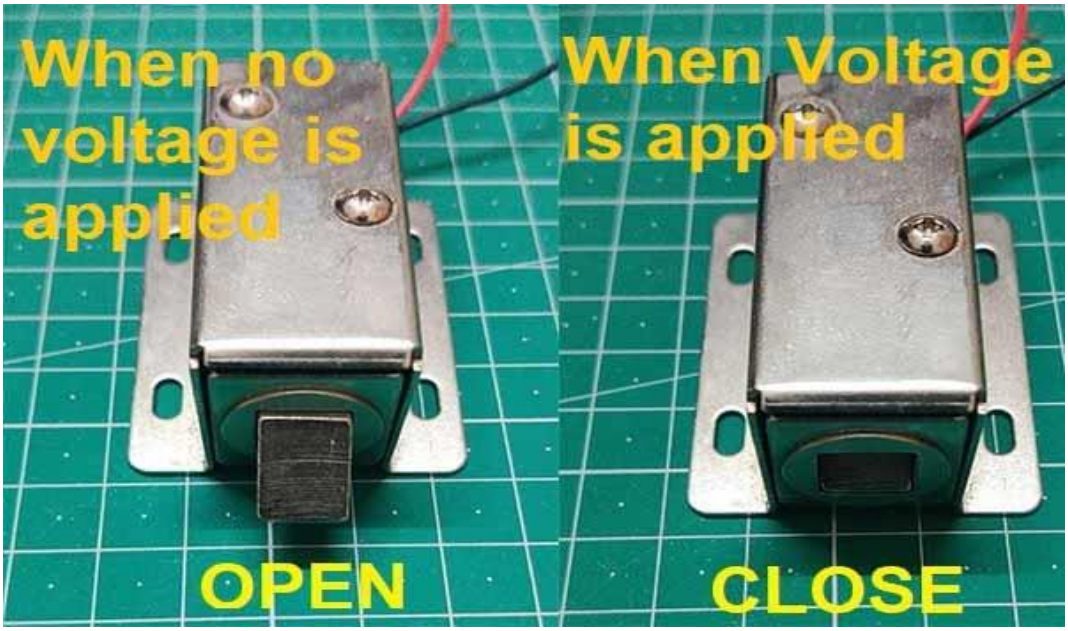


Figure III.11 Verrouillage/ Déverrouillage de la serrure

4. 3 Batteries Li-ion 18650 3.7v + support 18650x3 :

Une batterie 18650 est une batterie lithium-ion. Son nom provient de ses dimensions spécifiques : 18 mm x 65 mm À titre indicatif, c'est plus grand qu'une pile AA. La batterie 18650 a une tension d'environ 3,6v-3.7v. Ces batteries sont utilisées dans les lampes de poche, les ordinateurs portables, les appareils électroniques et même certaines voitures électriques en raison de leur fiabilité, de leur longue durée de vie et de leur capacité à être rechargées des centaines de fois. [25]

Le support 18650x3 est en support en plastique pour porter trois piles 18650 en série (3.7 * 4= 11.1 ≈ 12v) pour donner la tension suffisante dans le cas de notre projet à la serrure électrique pour se déverrouiller. Il est généralement utilisé dans les ordinateurs portables et les POWER-Banks.

Figure III.12 Pile 18650 3.7v

Figure III.13 Support 18650x3

5. Buzzer active :

Le buzzer utilisé est un buzzer actif, ce qui signifie qu'il émettra une sonnerie à une fréquence prédéfinie (2300 ±300 Hz), même en appliquant seulement qu'une alimentation continue.

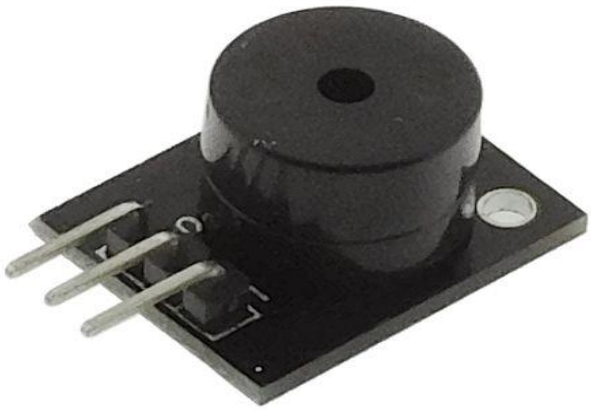


Figure III.14 Buzzer active

6. Module relai 5v :

La serrure électrique ne peut pas être alimentée directement à partir de la carte ESP32-CAM, car la dernière ne donne qu'une tension de 5V qui est insuffisante pour déverrouiller la serrure en cas de besoin. C'est là où il faut faire appel au relai 5V qui est liée à l'ESP32-CAM et quand il est excité, les contacts NO (Normally Opened) et le COM (Commun) ne sont plus en liaison. C'est pour cela qu'on va devoir configurer dans notre programme la broche de commande du relai par défaut HIGH. Dans le cas de présence d'une personne autorisée devant la caméra, la broche du relai devient en LOW pour que le GND de la batterie 12V branché dans le contact NO et le GND de la serrure branchée au contact COM sont lié. Ceci est expliqué dans le circuit de la Figure III.27

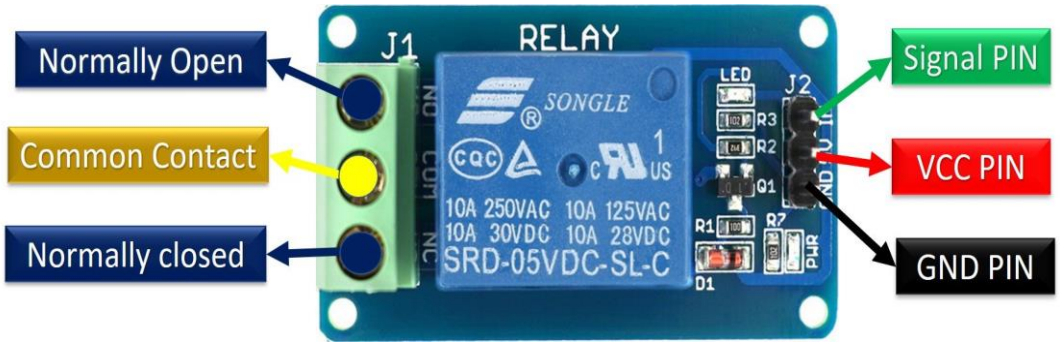


Figure III.15 Description du module relai 5V

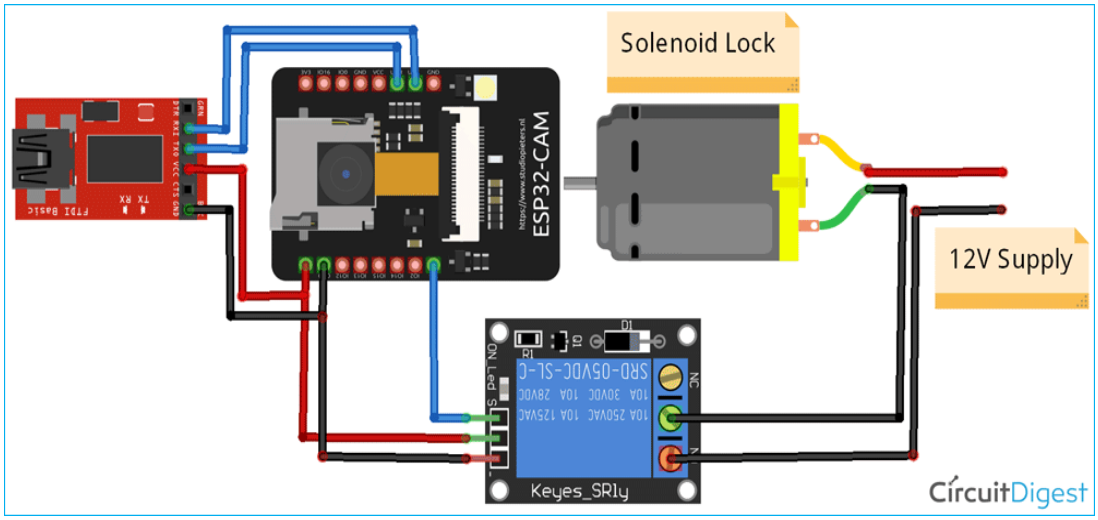


Figure III.16Circuit de liaison ESP32-CAM, Relai et serrure électrique

7. PC (Ordinateur) :

Pour alimenter la carte ESP32-CAM, lancer le streaming et activer la détection et/ou la reconnaissance faciale

8. Point d'accès mobile (Téléphone portable):

Pour effectuer le partage de connexion nécessaire pour le système qui demande de la connexion WI-FI

Le circuit du système :

La mise au point du système de reconnaissance faciale se fera suivant le circuit suivant :

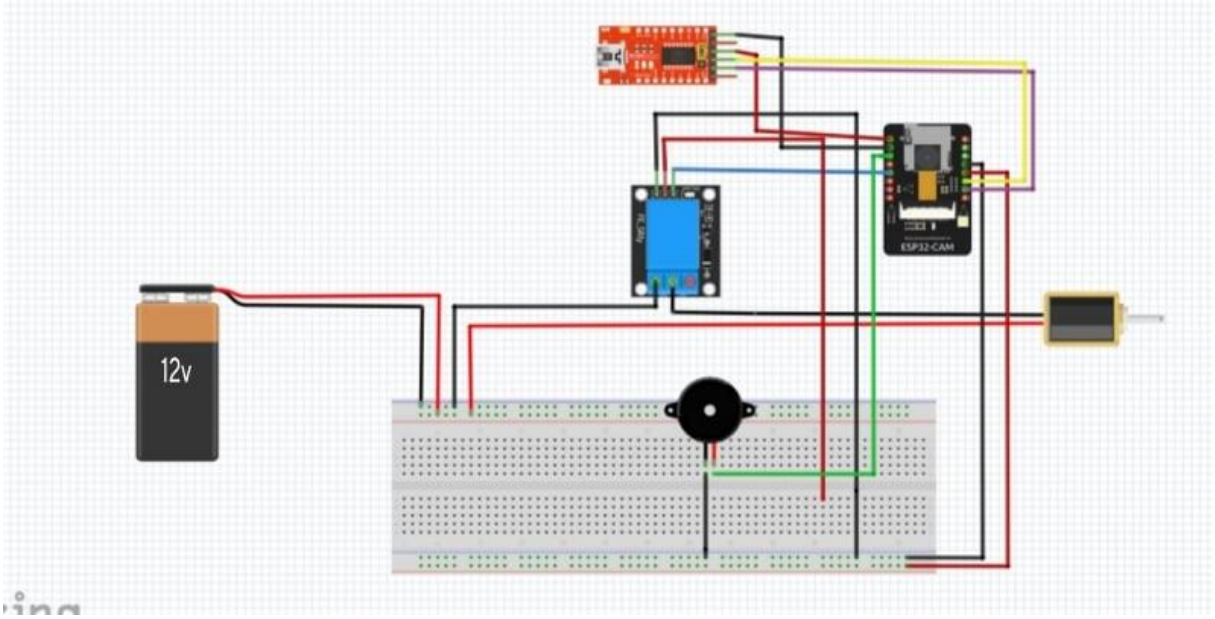


Figure III.17 Système de sécurité basé sur la reconnaissance faciale et la carte ESP32-CAM

III.2.3 Description software :

3. Arduino IDE 1.8.10:

Pour la programmation du système de sécurité.

4. Google Chrome :

Pour afficher le streaming en ligne.

III.2.4 Implémentation du code :

3. Installation et configuration ESP32 avec Arduino IDE :

Le logiciel Arduino IDE n'ayant pas le package ESP32 par défaut, il faut tout d'abord installer la bibliothèque ESP32. Pour se faire il faut tout simplement sélectionner Fichier> Préférences puis coller le lien suivant : https://dl.espressif.com/dl/package_esp32_index.json

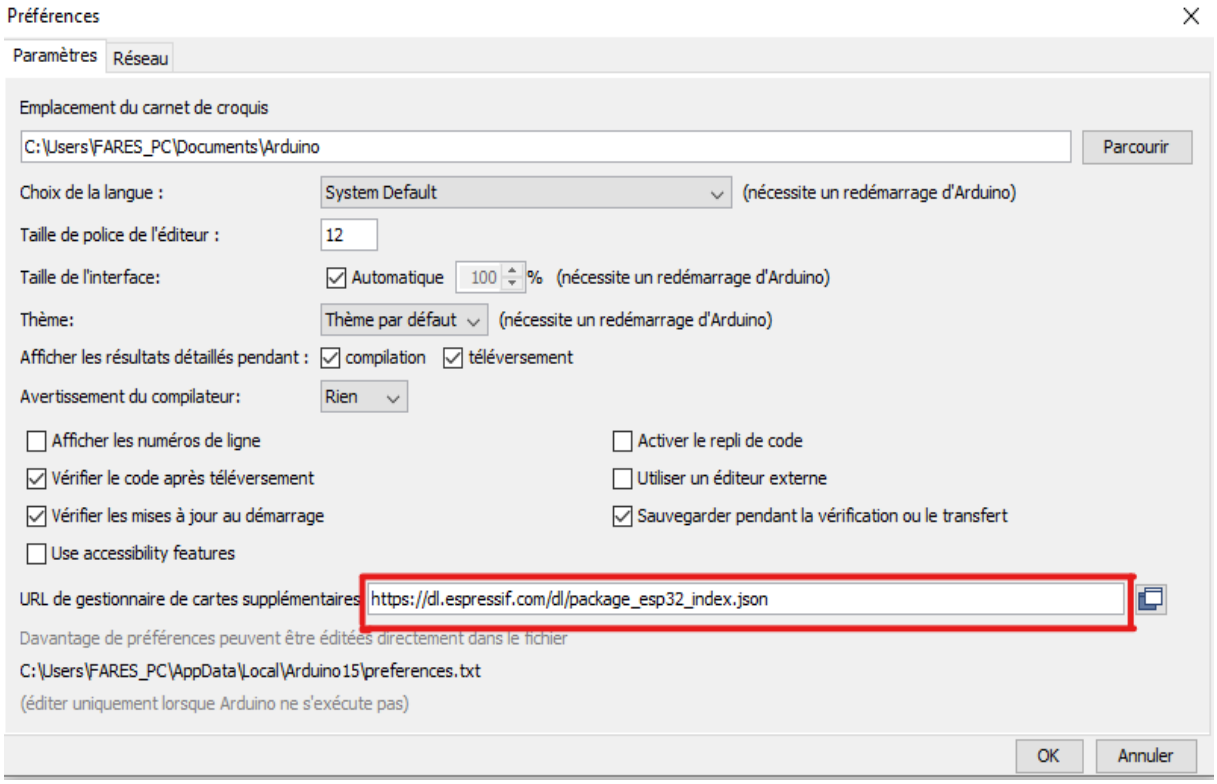


Figure III.18 Installation ESP32 (1)

Ensuite il faudra installer la bibliothèque ESP32, pour se faire il faut sélectionner Outils>Type de carte > Gestionnaire de carte, puis taper dans la barre de recherche ESP32

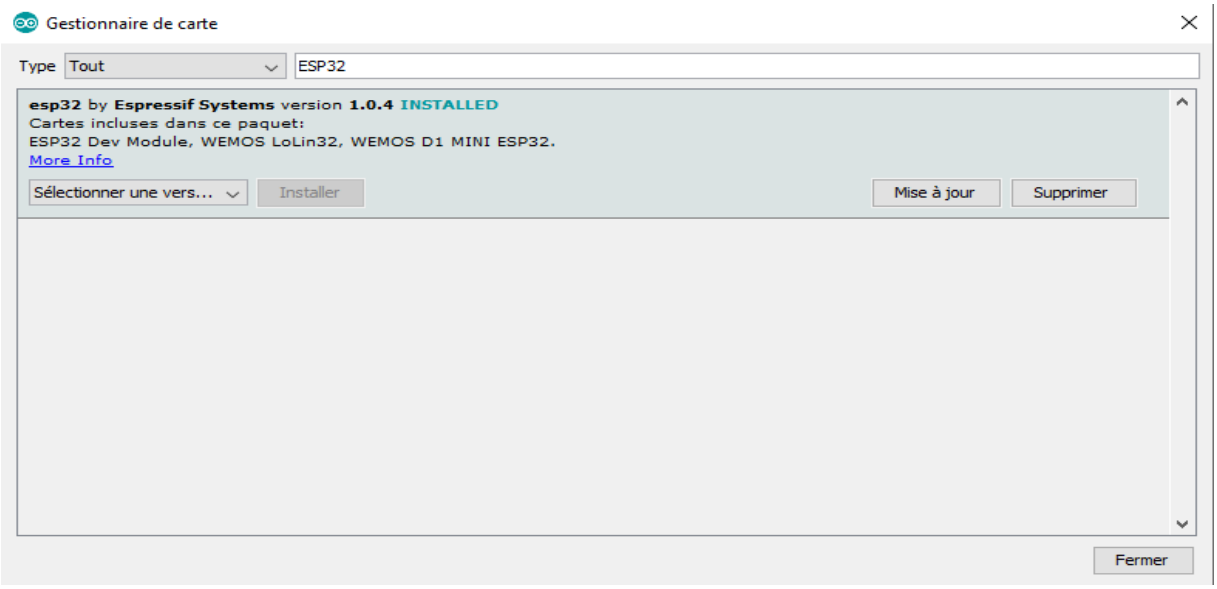


Figure III.19 Installation ESP32 (2)

4. Conception du code :

Une fois la bibliothèque ESP32 installée, il faut ouvrir l'exemple de reconnaissance faciale dans l'Arduino IDE. Pour se faire on doit sélectionner Fichier > Exemple > ESP32 > Camera > Camera Web Server

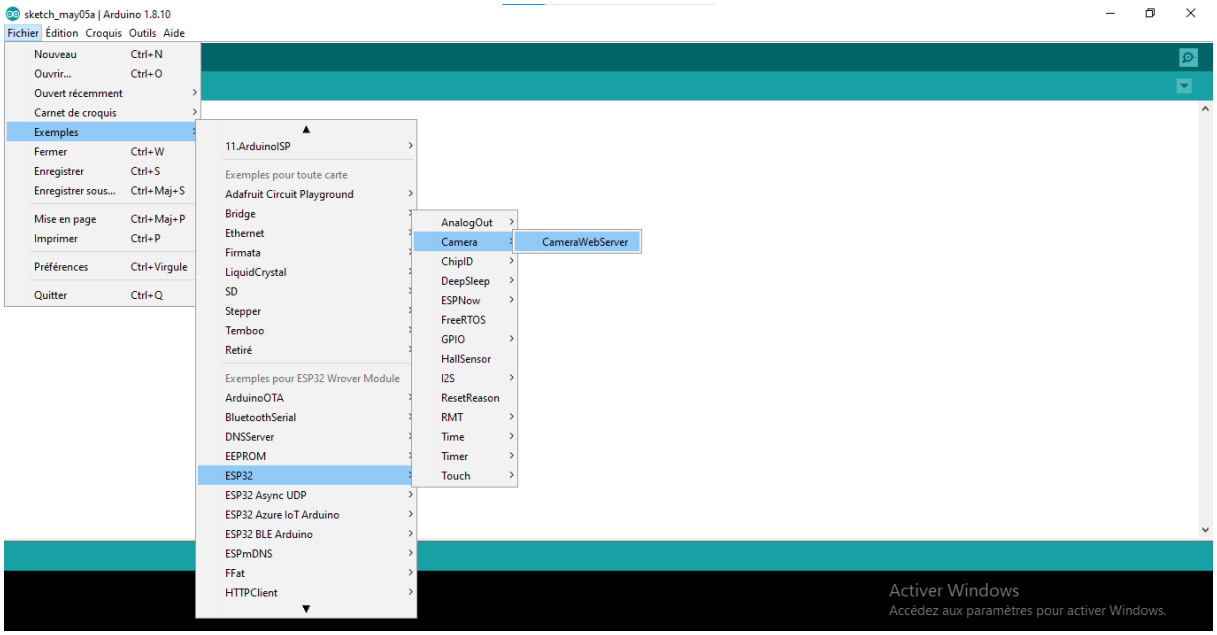


Figure III.20 Exemple ESP32 Camera Web Server

Une fois l'exemple ouvert, il faut modifier le programme comme suivant :

- Tout d'abord, sélectionner le modèle de camera utilisé en décommentant le modèle en question qui est dans notre cas le module AI THINKER :

```
// Select camera model
//#define CAMERA_MODEL_WROVER_KIT
//#define CAMERA_MODEL_ESP_EYE
//#define CAMERA_MODEL_M5STACK_PSRAM
//#define CAMERA_MODEL_M5STACK_WIDE
#define CAMERA_MODEL_AI_THINKER
```

-Ensuite, inclure les informations d'identification du réseau WI-FI :

```
const char* ssid = "Entrer le nom de l'adresse WI-FI ICI";
const char* password = "Entrer le mot de passe WI-FI ICI";
```

Important ! : L'exemple Camera Web Server comprend seulement la reconnaissance faciale et non le système de sécurité qu'on a besoin de mettre au point. Donc il faut ajouter des conditions au programme. Pour se faire, on a suivi les étapes suivantes :

-Premièrement, on a choisi de Configurer les pins 12 et 15 en sortie pour contrôler le buzzer et le relai 5v, et initialiser la pin 12 LOW tandis que la pin 15 doit être initialisée HIGH car les contacts NO et COM ne doivent pas encore être liés.

```
void setup() {
  pinMode(12, OUTPUT);
  pinMode(15, OUTPUT);
  digitalWrite(12,LOW); //buzzer
  digitalWrite(15,HIGH); //relai
```

-En cas de visage reconnu, le buzzer sonne, la bobine du relai n'est plus excitée donc les contacts NO et COM sont à nouveau liés et ainsi la serrure est déverrouillée et le message « Access Allowed » s'affiche en vert.

```
    if (matched_id >= 0) {
        Serial.printf("Match Face ID: %u\n", matched_id);
        rgb_printf(image_matrix, FACE_COLOR_GREEN, "Access allowed", matched_id);
        digitalWrite(15,LOW); //relai
        digitalWrite(12,HIGH); //buzzer
       delay(600);
       digitalWrite(12,LOW);
       delay(4400);
       digitalWrite(15,HIGH);
```

-En cas de visage non-reconnu, la serrure est verrouillée et le message « Access Denied » s'affiche en rouge.

```
    } else {
        Serial.println("No Match Found");
        rgb_print(image_matrix, FACE_COLOR_RED, "Access denied");
        matched_id = -1;
        digitalWrite(15,HIGH); //relai
    }
```

Une fois ses modifications apportées, on vérifie si l'ESP32-CAM est configuré selon les paramètres ci-dessous puis vérifier si les pins GPIO 0 et GND sont connectées ensuite on clique sur le bouton téléverser.

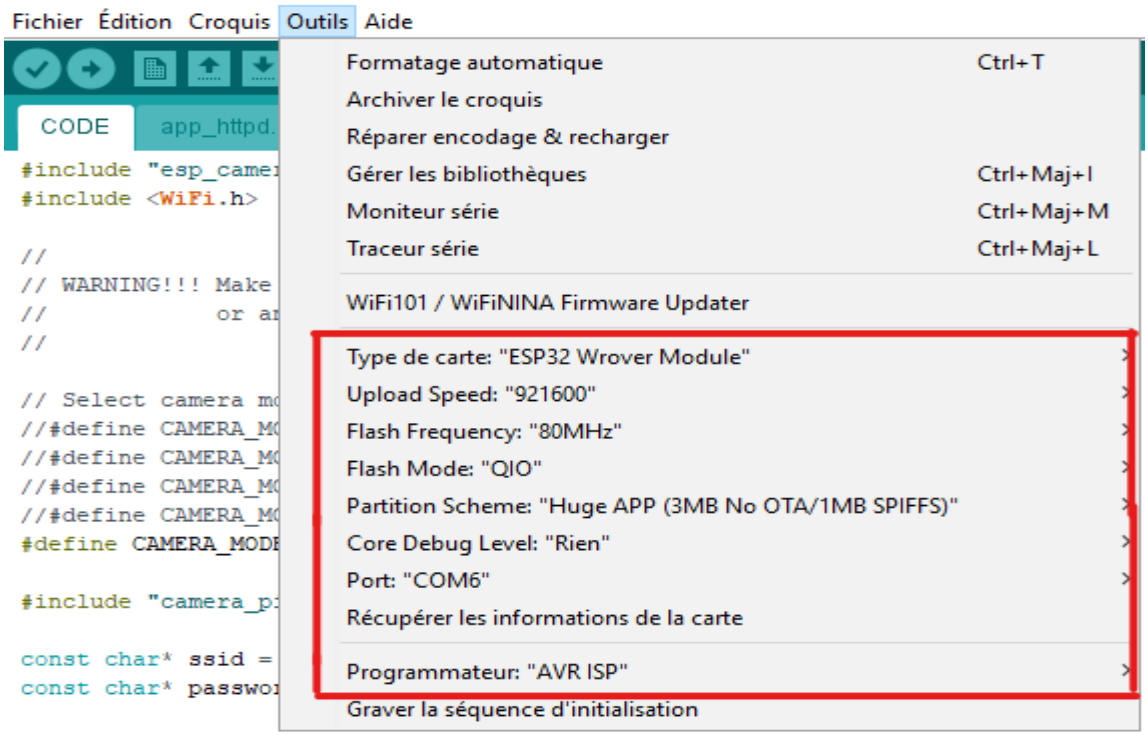


Figure III.21 Configuration ESP32-CAM

Une fois que le code téléversé on obtient le résultat suivant :

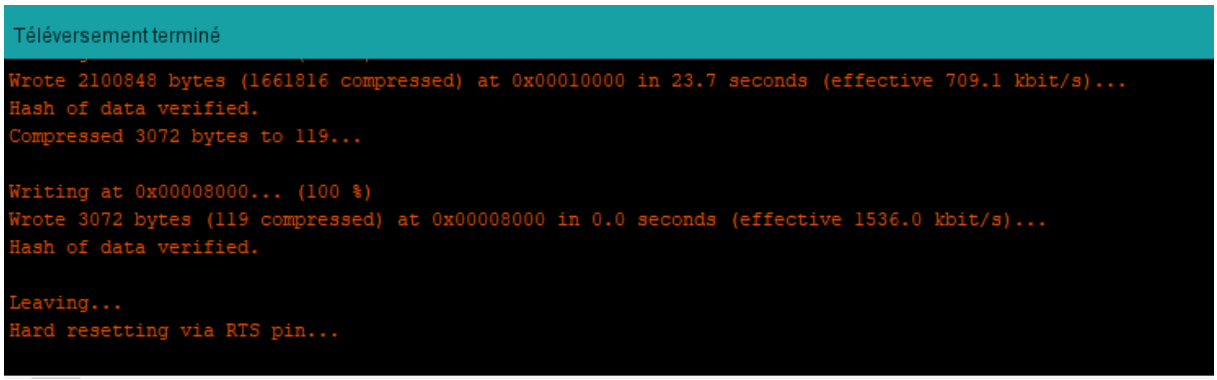


Figure III.22 Téléversement terminé

On ouvre le moniteur série, en nous assurant qu'il est réglé sur un débit de 115200 Baud. Puis on appui sur le bouton de réinitialisation (RESET) sur le module ESP32-CAM. On s'attend à voir quelques informations d'initialisation, suivies d'une déclaration disant que l'appareil s'est connecté au réseau et a obtenu une adresse IP sous forme de lien URL.

Figure III.23 Adresse obtenue

Une fois l'adresse copiée et collée sur le navigateur GOOGLE CHROME, une interface est affichée :

: :

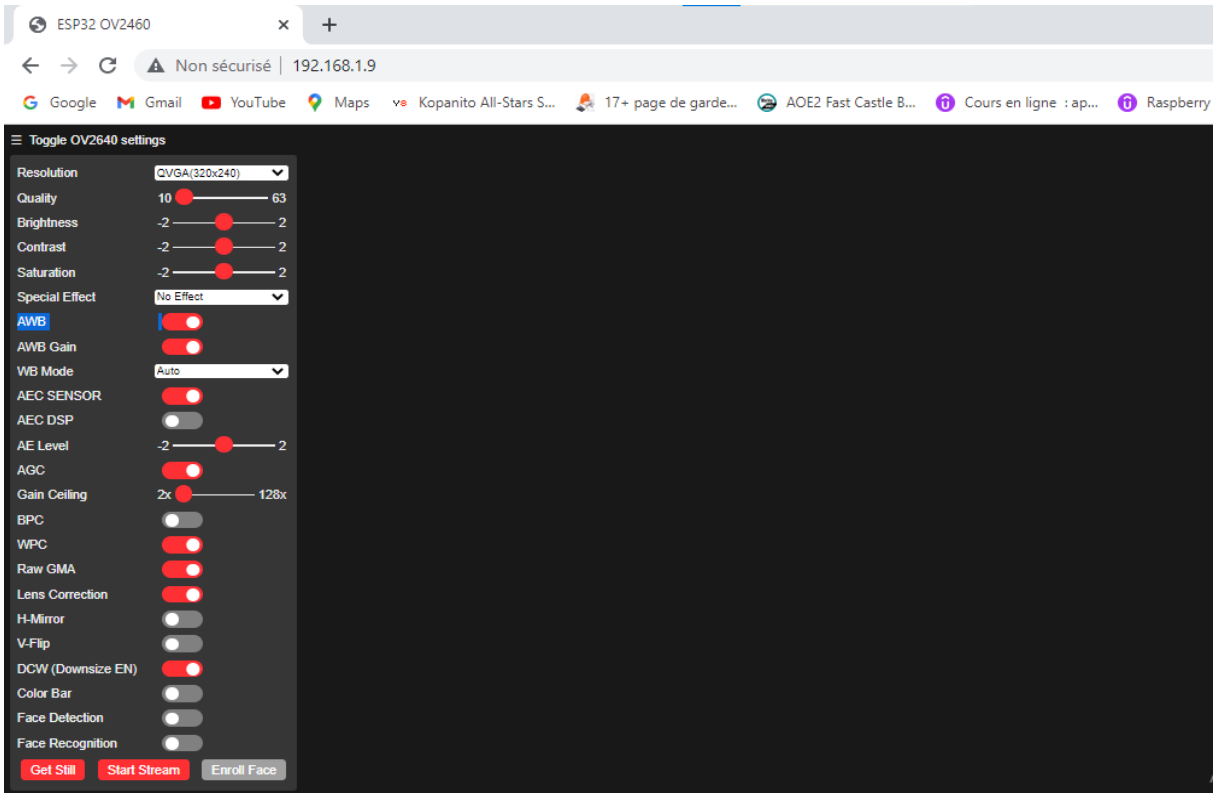


Figure III.24 Interface du streaming

L'étape d'implémentation du code est terminée, et maintenant on peut passer à l'étape suivante.

III.2.5 Résultats obtenus :

-On lance le Stream puis on active la détection faciale en cliquant sur le bouton « Face Detection », un cadre jaune s'affiche autour du visage détecté.

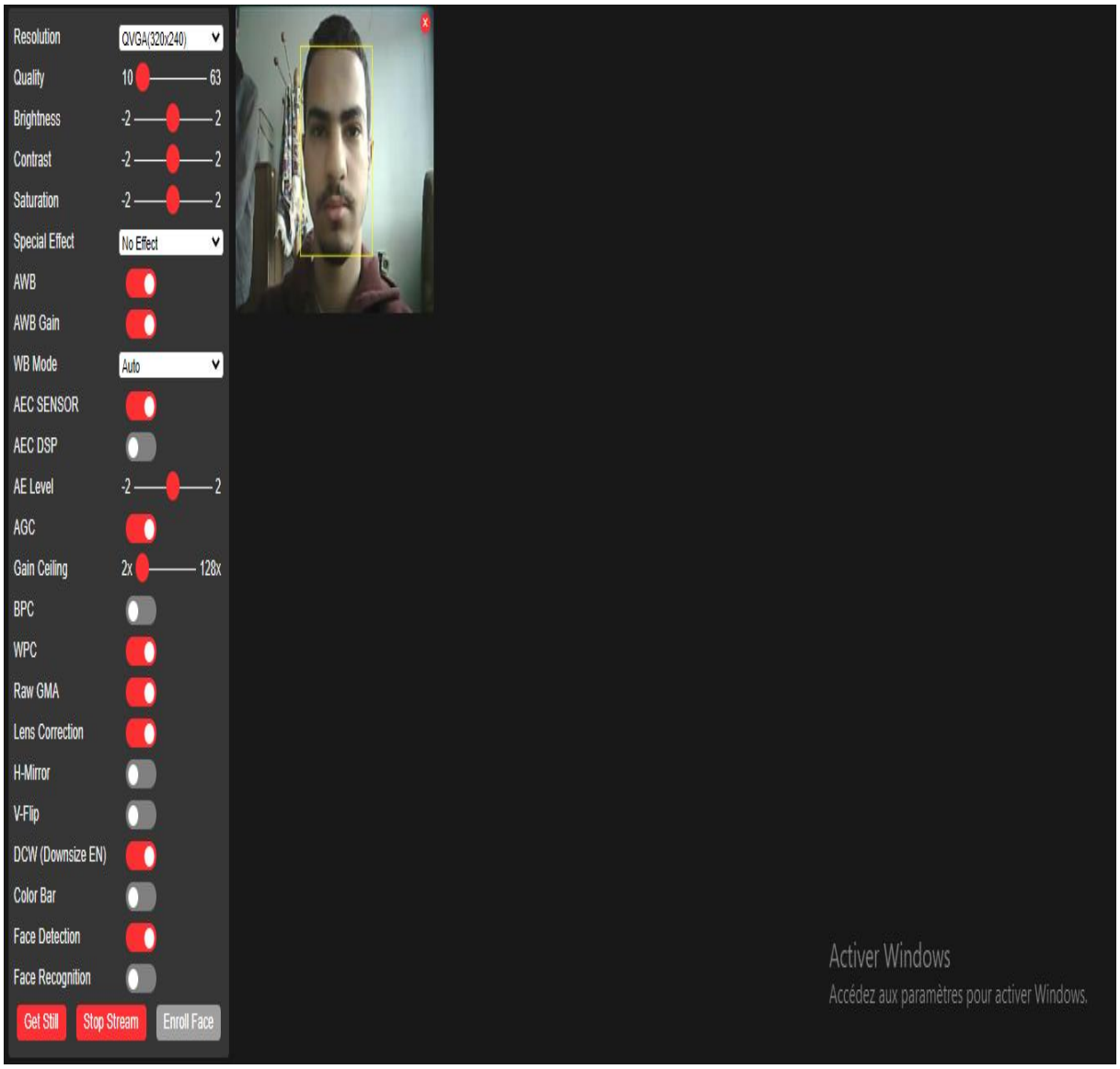


Figure III.25Détection faciale

-Ensuite, on active la reconnaissance faciale en cliquant sur le bouton « Face Recognition ». On remarque que la personne n'est pas encore enregistrée c'est-à-dire que l'accès est interdit pour le moment.

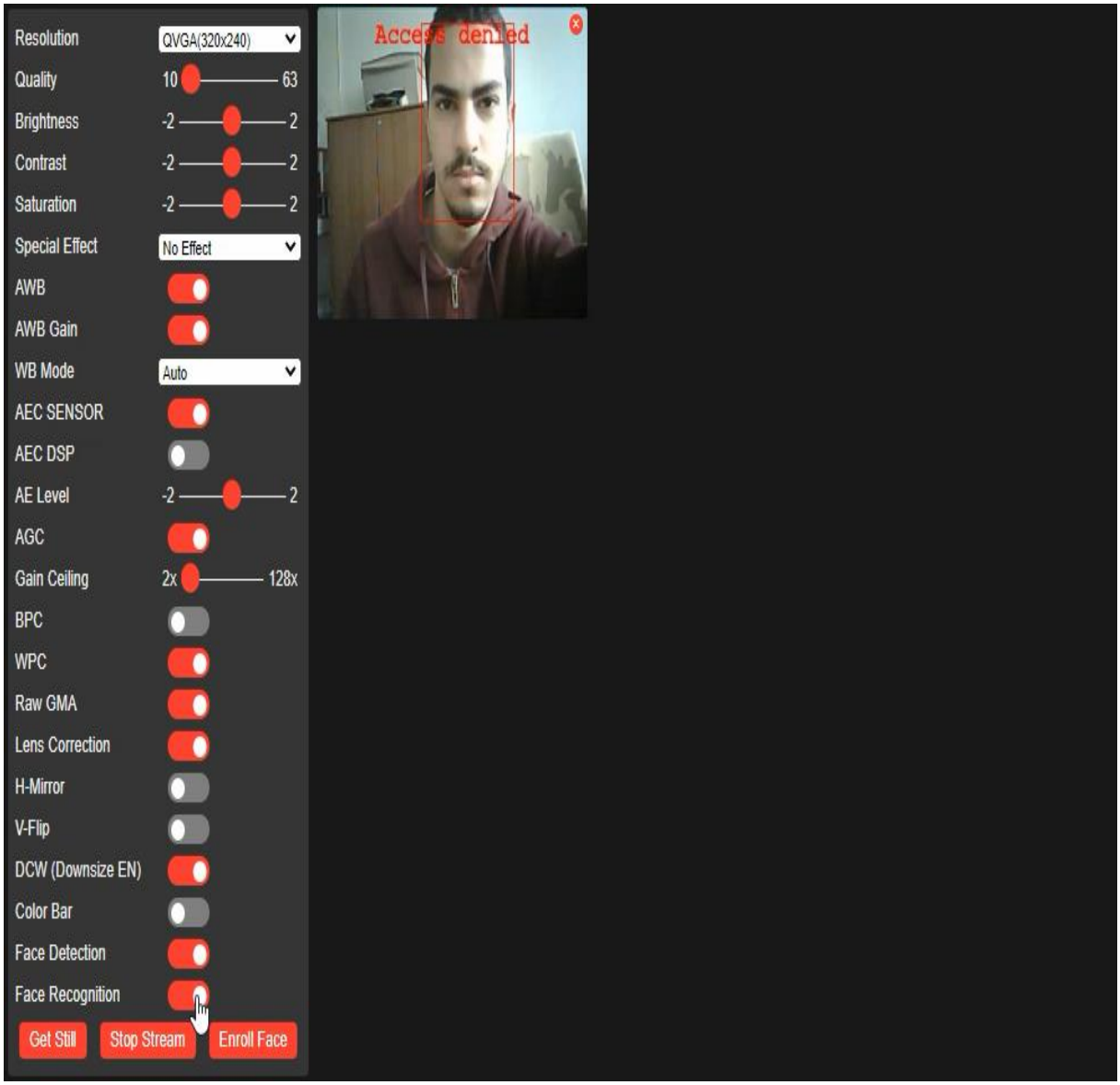


Figure III.26 Reconnaissance faciale (Accès interdit)

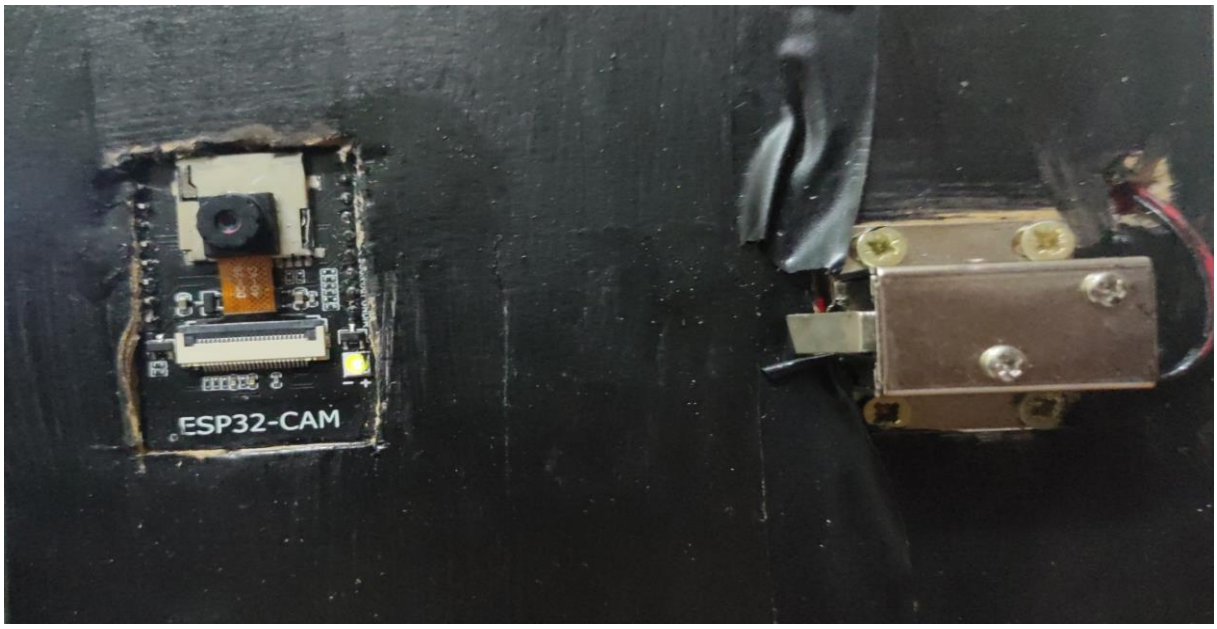


Figure III.27 Serrure verrouillée

-Pour enregistrer la personne, il faut simplement cliquer sur le bouton « Enroll Face ». Une fois le visage reconnu, le message « Access Allowed » est affiché en vert.

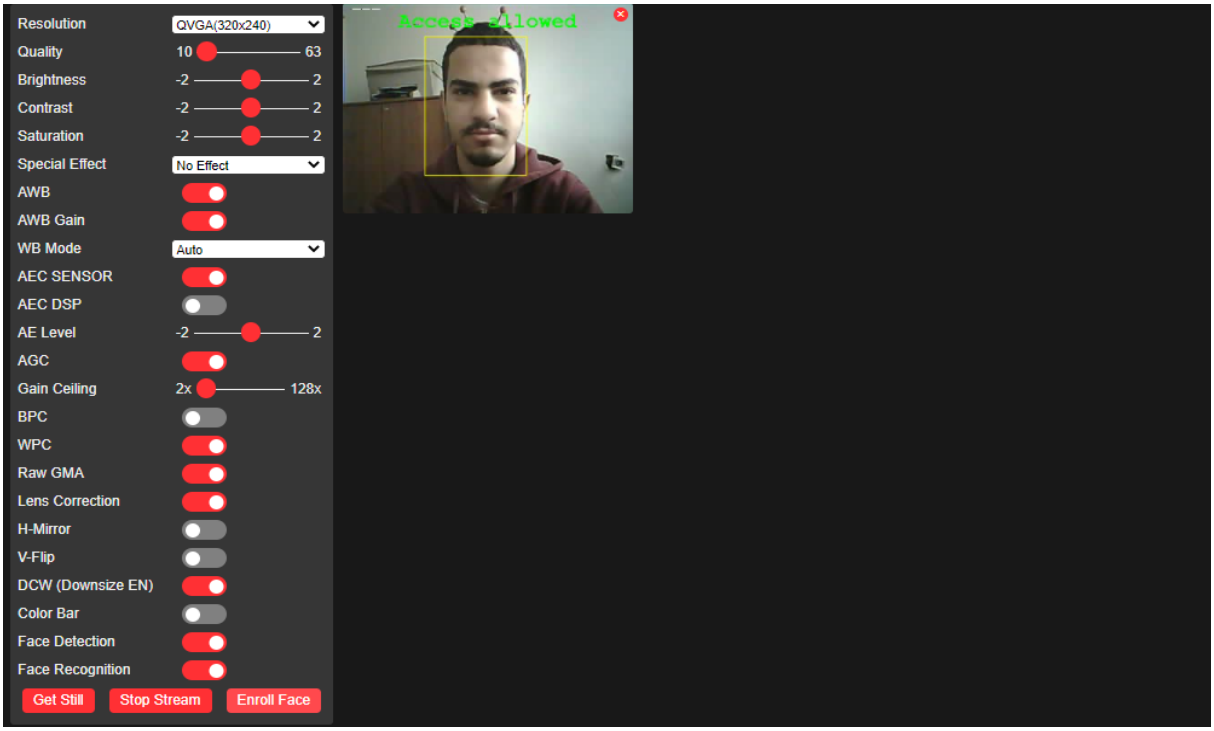


Figure III.28 Reconnaissance faciale (Accès autorisé)

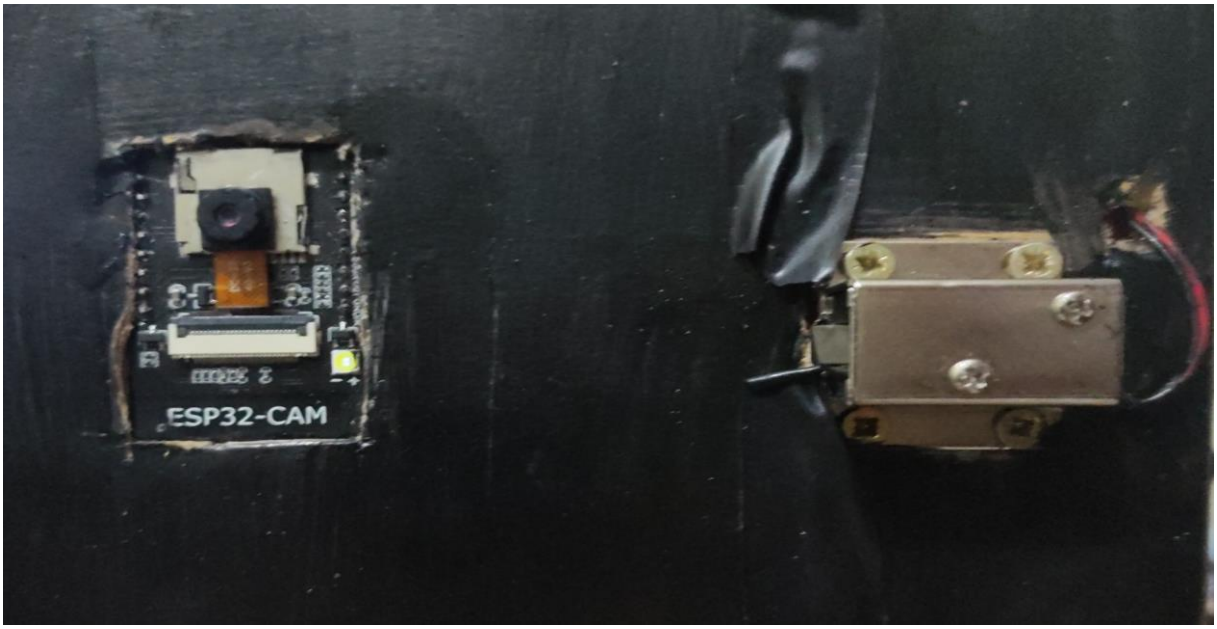


Figure III.29 Serrure déverrouillée

-On teste avec une autre personne non reconnue, et l'accès n'est pas autorisé.

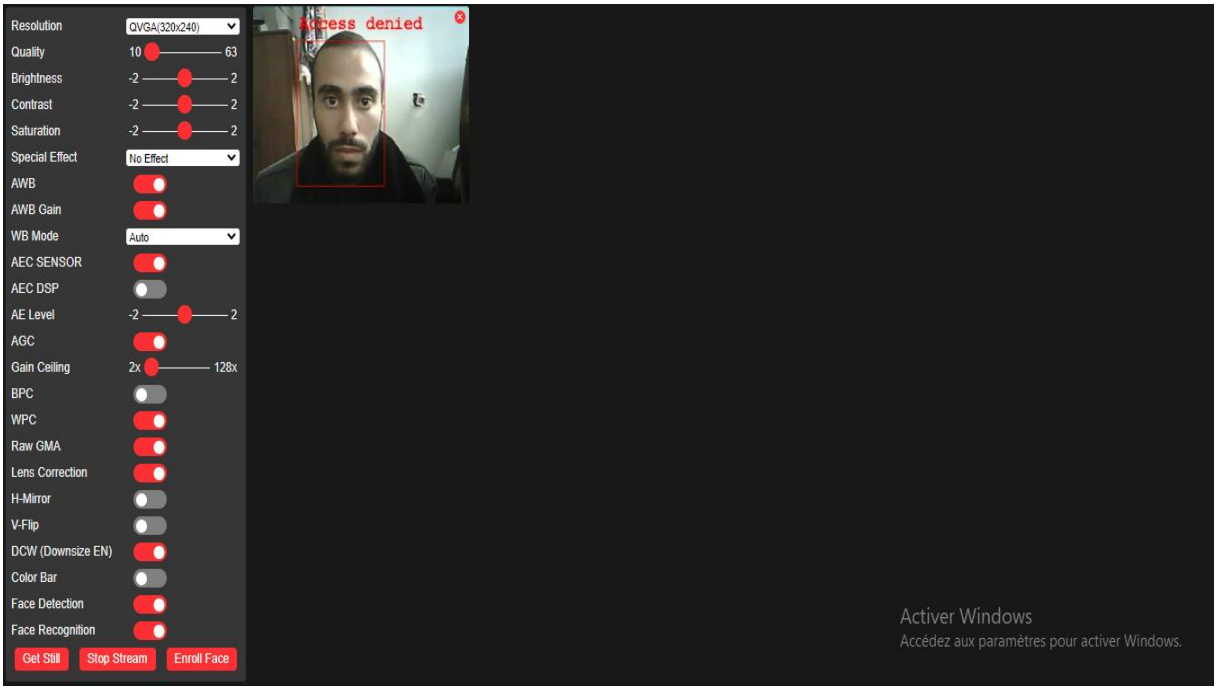


Figure III.30 Reconnaissance faciale (Accès refusé) personne 2

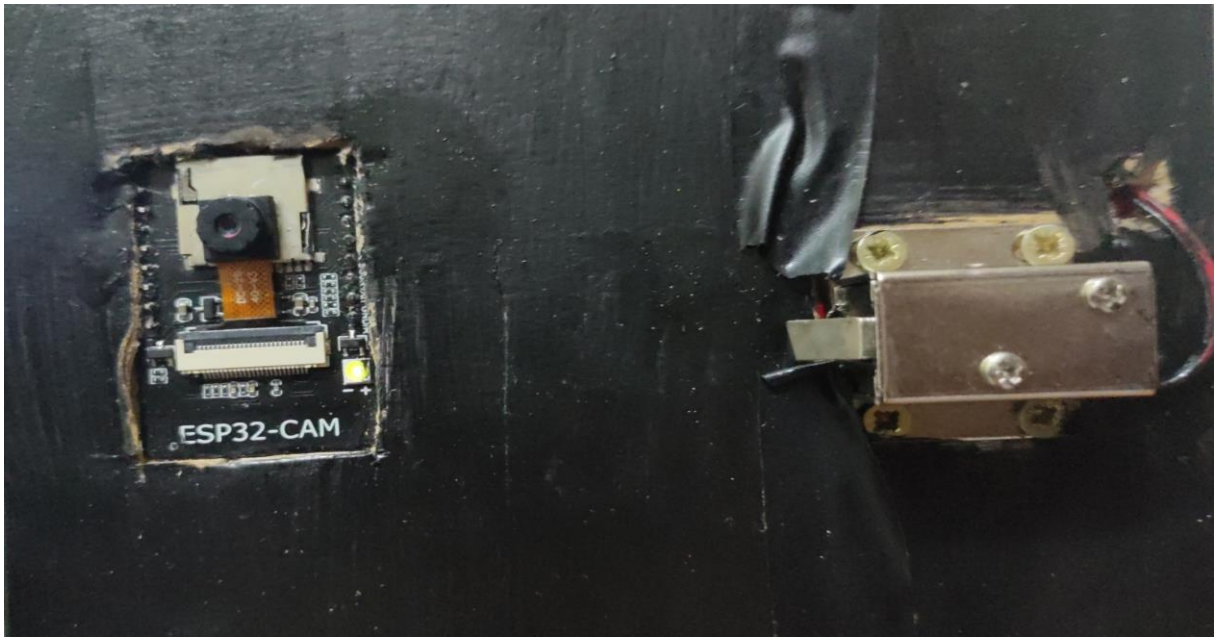


Figure III.31 Serrure verrouillée (2)

Conclusion :

Nous avons terminé notre mise en œuvre pratique dans ce chapitre. Nous avons tenté de décrire les procédures et les étapes que nous avons suivies pour atteindre notre objectif.

Nous avons commencé ce chapitre par une description générale du projet, en enregistrant les étapes de la simulation ainsi que les résultats obtenus puis expliqué la réalisation pratique de la reconnaissance faciale et démontré les résultats afin que les outils et logiciels soient clairs pour chaque méthode.

Malgré les capacités de la caméra, l'utilisation de la carte esp32cam s'est avérée très utile dans l'avancement du système de reconnaissance faciale, prédisant un avenir prometteur pour la carte dans le domaine de la reconnaissance faciale.

Conclusion générale :

En conclusion, ce mémoire a exploré le sujet fascinant de la technologie de la reconnaissance faciale et de ses applications pratiques. Le premier chapitre a abordé les bases de la reconnaissance faciale et les différentes méthodes utilisées pour identifier et vérifier les individus. Le deuxième chapitre s'est concentré sur l'ESP32-CAM, une carte microcontrôleur polyvalente qui peut être utilisée pour une variété de projets, y compris la reconnaissance faciale. Enfin, le troisième chapitre présente deux exemples pratiques de systèmes de reconnaissance faciale. Le premier exemple présentait un système de reconnaissance faciale utilisant la bibliothèque OpenCV-python, tandis que le second exemple présentait un système de reconnaissance faciale de serrure de porte utilisant l'ESP32-CAM et l'IDE Arduino. Malgré ses nombreux avantages, le système de serrure à reconnaissance faciale ESP32-CAM présente également certains défis, tels que la nécessité de disposer des caméras et d'algorithmes de traitement d'images de haute qualité, ainsi qu'une connexion internet plus performante. Toutefois, grâce aux progrès technologiques, ces difficultés peuvent être surmontées, ce qui fait de ce système un choix de plus en plus populaire pour la sécurité et le contrôle d'accès.

Dans l'ensemble, ce mémoire a mis en évidence le potentiel de la technologie de reconnaissance faciale et sa capacité à améliorer la sécurité et la commodité dans divers contextes. Qu'il s'agisse d'un usage personnel ou d'applications commerciales, la technologie de reconnaissance faciale a le potentiel de révolutionner notre mode de vie et de travail. Grâce aux progrès constants du matériel et des logiciels, nous pouvons nous attendre à voir des utilisations encore plus innovantes de cette technologie dans un avenir proche.

Références bibliographiques :

[1]: WOODWARD JR, John D., HORN, Christopher, GATUNE, Julius, et al. Biometrics: A look at facial recognition. RAND CORP SANTA MONICA CA, 2003.

[2] : MORIZET, Nicolas. Reconnaissance biométrique par fusion multimodale du visage et de l'iris. 2009. Thèse de doctorat. Télécom ParisTech.

[3] : https://www.preventica.com/dossier-surete-biometrie-caracteristiques.php.

[4] : GUENNOUNI, Souhail, MANSOURI, Anass, et AHAITOUF, Ali. Biometric systems and their applications. In: Visual impairment and blindness-what we know and what we have to know. IntechOpen, 2019.

[5]: L. Mohamed Takieddine, D. Naoufel <<Security system based on face recognition>> UNIVERSITÉ BADJI MOKHTAR - ANNABA-2022, mémoire Master2

[6] : MCCLELLAN, Elizabeth. Facial Recognition Technology: Balancing the Benefits and Concerns. J. Bus. & Tech. L., 2019, vol. 15, p. 363.

[7] : GAO, Weihao. Face Recognition Application Based on Embedded System. 2013. Thèse de doctorat. Case Western Reserve University.

[8] : JAFRI, Rabia ET ARABNIA, Hamid R. A survey of face recognition techniques. Journal of information processing systems, 2009, vol. 5, no 2, p. 41-68.

[9] : HAYET, Goumeziane et DJAMILA, Laribi. Développement d'un system biométrique pour la reconnaissance de visage, basé sur l'opérateur binaire local (LBP) et ses variantes. 2018. Mémoire de Fin d'Etudes De MASTER ACADEMIQUE. Université Mouloud Mammeri.

[10] : BUYSSENS, Pierre. Fusion de différents modes de capture pour la reconnaissance du visage appliquée aux e_transactions. 2011. Thèse de doctorat. Université de Caen.

[11] : ARCA, Stefano, CAMPADELLI, Paola, et LANZAROTTI, Raffaella. A face recognition system based on automatically determined facial fiducial points. Pattern recognition, 2006, vol. 39, no 3, p. 432-443.

[12] : ABDESSETTAR, BETTAHAR et FATHI, SABER. Extraction des caractéristiques pour l'analyse biométrique d'un visage. 2014. Thèse de Master.

[13] : GONG, Shaogang, MCKENNA, Stephen J., et PSARROU, Alexandra. Dynamic vision : from images to face recognition. World Scientific, 2000.

[14]: Park, Unsang, Yiying Tong, and Anil K. Jain. "Age-invariant face recognition." Pattern Analysis and Machine Intelligence, IEEE Transactions on 32.5 (2010) : 947-954.

[15] : SHARIF, Muhammad, NAZ, Farah, YASMIN, Mussarat, et al. Face Recognition : A Survey. Journal of Engineering Science & Technology Review, 2017, vol. 10, no 2.

[16] : AZEEM, Aisha, SHARIF, Muhammad, RAZA, Mudassar, et al. A survey : Face recognition techniques under partial occlusion. Int. Arab J. Inf. Technol., 2014, vol. 11, no 1, p. 1-10.

[17] : TARRÉS, Francesc, RAMA, Antonio, ET TORRES, L. A novel method for face recognition under partial occlusion or facial expression variations. In : Proc. 47th Int'l Symp. ELMAR. 2005. p. 163-166.

[18] : https://letmeknow.fr/fr/cartes-compatibles/1788-carte-de-developpement-ESP32-CAM-camera-bluetooth-wifi-ov2640-7426925369115.html

[19] : https://dronebotworkshop.com/ESP32-CAM-intro/

[20] : https://how2electronics.com/getting-started-with-ESP32-CAM-board-video-streaming-over-wifi/

[21] : https://robocraze.com/blogs/post/all-about-ESP32-CAMera-module

[22] : https://components101.com/cables/ftdi-cable-usb-to-rs232-converter

[23] : https://megma.ma/serrure-electrique-12vdc-solenoid-lock/

[24] : https://www.rhydolabz.com/miscellaneous-miscellaneous-c-205_82/12v-solenoid-lockp2327.html#:~:text=12V%20Solenoid%20lock%20has%20a,any%20power%20in%20this%20state.

[25] : https://www.fenixlighting.com/blogs/news/the-ultimate-guide-to-the-18650-battery#:~:text=What%20is%20an%2018650%20Battery,mili%2Damp%2Dhours).