République Algérienne Démocratique et Populaire

MinistèredelEnseignementSupérieuretdelaRechercheScientifique

Université de Bouira, Faculté des Sciences et des Sciences Appliquées

Département de Génie électrique

Bouira le :22/06/2024

Autorisation de soutenanced'un mémoire de Master

Je soussigné(e), l'enseignant :MoudacheSaid

Encadreur des étudiants (:

1- Saoudi Hocine

Spécialité : ESE

Les autorise à soutenir leur **mémoire** de Master.

Signature du rapporteur

Mémoire de Master

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Akli Mohand Oulhadj - Bouira -
Tasdawit Akli Muḥend Ulḥağ - Tubirett -

وزارة التعليم العالي والبحث العلمي
جامعة أكلي محند أولحاج
- البويرة -

Faculté des Sciences et des Sciences Appliquées

كلية العلوم والعلوم التطبيقية

Présenté au

Département: Génie Électrique
Domaine: Sciences et Technologies
Filière: Electronique.
Spécialité: Electronique des systèmes embarqués .

Réalisé par :

SAOUDI Hocine

Thème

Réalisation d'un projet de contrôle d'accès basé sur les empreintes digitales

---

Soutenu le: **03/07/2024**

Devant le Jury composé de :

Mme : MADI SAIDA	Univ. Bouira	Président
Mr : MOUDACHE SAID	Univ. Bouira	Rapporteur
Mr : BENAOUICHA KARIM	Univ. Bouira	Examinateur

Année Universitaire: 2023-2024

Dédicaces

À mes parents, qui ont été ma source d'inspiration et de motivation. Merci pour vos sacrifices, votre sagesse et vos conseils qui ont guidé mes pas dans cette aventure académique.

Je dédie ce mémoire à mes frères et sœurs, dont l'amour, le soutien et la patience ont été des piliers essentiels tout au long de mes études. Vous avez toujours cru en moi et m'avez encouragé à surmonter chaque obstacle.

À mes amis, qui ont partagé avec moi des moments de joie, de doutes et de réussites. Votre amitié et votre soutien ont rendu ce parcours plus agréable et enrichissant.

Enfin, à tous ceux qui, de près ou de loin, ont contribué à l'aboutissement de ce travail. Merci pour votre aide, vos encouragements et votre présence qui ont illuminé mon chemin.

Avec toute ma gratitude et mon affection.

Remerciements

Nous tenons à remercier tout d'abord notre Dieu, le tout puissant, de nous avoir donné la santé et la volonté pour compléter ce modeste travail.

Nous tenons à remercier vivement notre promoteur monsieur Mr. MOUDACHE. Je suis profondément reconnaissant pour son soutien inestimable, ses conseils avisés et sa patience tout au long de ce projet. Sa rigueur scientifique et ses encouragements constants ont été déterminants pour la réussite de ce travail. Ses précieuses orientations et ses remarques pertinentes m'ont permis de surmonter les défis rencontrés et de mener à bien cette recherche.

Nous remercions vivement tous les membres du jury d'avoir accepté d'examiner et d'évaluer ce modeste travail.

Nous remercions aussi tous nos amis, et toutes les personnes qui de près ou de loin ont contribué à l'élaboration de ce mémoire.

Enfin, nous tenons à remercier tous les membres de notre famille profondément, pour leurs encouragements et leurs soutiens sans lesquels nous n'aurions pas pu terminer ce travail.

Résumé

Dans ce mémoire, nous exposons la création et la mise en place d'un système de contrôle d'accès qui repose sur la reconnaissance des empreintes digitales, intégré à une connectivité WiFi afin de centraliser la gestion des données. Pour concevoir un système sécurisé, efficace et convivial, le projet utilise un microcontrôleur ESP32, un capteur d'empreintes digitales et un écran OLED. Grâce à la connexion WiFi, il est possible de communiquer en temps réel avec une base de données lointaine, ce qui facilite l'enregistrement, la vérification et la gestion des accès. Les résultats obtenus mettent en évidence une nette amélioration par rapport aux techniques classiques de contrôle d'accès, en proposant une solution contemporaine et fiable. Ce document examine aussi les possibilités d'amélioration à venir, comme l'intégration de l'intelligence artificielle et la collaboration avec d'autres systèmes de sécurité.

Sommaire

Table des matières

Chapitre 2 : Méthodes et des algorithmes de reconnaissance des empreintes digitales

Chapitre3 : Résultats et discussions

Liste des Figures

Liste des Tableaux

Liste des Acronymes

ADN : Acide Désoxyribonucléique (DNA en anglais).

API : Application Programming Interface (Interface de Programmation d'Applications).

CN : Nombre de Croisements (Crossing Number).

ESP32 : Microcontrôleur ESP32.

FKP : Finger-Knuckle Print (Empreinte des Articulations des Doigts).

HTTP : HyperText Transfer Protocol (Protocole de Transfert Hypertexte).

I2C : Inter-Integrated Circuit (Circuit Inter-Intégré).

IDE : Integrated Development Environment (Environnement de Développement Intégré).

OLED : Organic Light-Emitting Diode (Diode Électroluminescente Organique).

PIN : Personal Identification Number (Numéro d'Identification Personnel).

RFID : Radio Frequency Identification.

SVM : Support Vector Machine (Machine à Vecteurs de Support).

USB : Universal Serial Bus.

UTL : Universal Time Coordinated (Temps Universel Coordonné).

Wi-Fi : Wireless Fidelity.

Introduction Générale

Introduction Générale

Dans un monde de plus en plus numérique et interdépendant, la sécurité des espaces physiques et numériques est cruciale. La gestion des accès, qu'il s'agisse de l'accès aux bâtiments sensibles, aux données confidentielles ou aux systèmes d'information, est devenue une priorité pour les entreprises, les institutions et les particuliers. Les méthodes traditionnelles de contrôle d'accès, telles que les clés mécaniques, les cartes d'entrée ou les mots de passe, montrent leurs limites en termes de sécurité et de commodité.

Les développements technologiques ont permis le développement de solutions biométriques, notamment l'identification des empreintes digitales avec fiabilité, facilité d'utilisation et efficacité. L'adoption croissante de cette technologie est motivée par la recherche d'un compromis idéal entre une sécurité renforcée et une expérience utilisateur fluide.

Ce mémoire propose de développer un système de contrôle d'accès basé sur les empreintes digitales, intégrant la connectivité WiFi pour la gestion et la supervision centrales. L'objectif principal de ce projet est de concevoir un système non seulement sûr, mais aussi facile à déployer et à utiliser au quotidien.

Dans ce mémoire, nous visons à présenter les bases de la biométrie et les spécificités de la reconnaissance d'empreintes digitales. Nous allons concevoir et mettre en œuvre un système de contrôle d'accès en développant un prototype utilisant un capteur d'empreintes digitales et un module ESP32 pour connecter le WiFi, permettant une connectivité sécurisée à une base de données centrale.

Pour atteindre ces objectifs, nous avons divisé ce mémoire en trois chapitres :

Chapitre 1 : Les Systèmes de Contrôle d'Accès : Concepts et Technologies de Base

Ce chapitre introduit les concepts fondamentaux des systèmes de contrôle d'accès, expliquant leur importance pour la sécurité des bâtiments, des installations et des ressources sensibles. Il explore les différentes technologies utilisées dans ces systèmes, y compris les cartes à puce, les codes PIN, les systèmes biométriques et les combinaisons de ces méthodes. Le chapitre aborde également les composants principaux des systèmes de contrôle d'accès, comme les dispositifs de lecture, les contrôleurs et les logiciels de gestion. Enfin, il examine les critères de sélection et les défis associés

à la mise en œuvre de ces systèmes, tels que la sécurité, la fiabilité, l'évolutivité et la facilité d'utilisation.

Chapitre 2 : Méthodes et Algorithmes de Reconnaissance des Empreintes numérique

Ce chapitre se concentre sur les méthodes et les algorithmes utilisés pour la reconnaissance des empreintes digitales, un élément clé des systèmes biométriques de contrôle d'accès. Il décrit les étapes principales du processus de reconnaissance, y compris la capture de l'empreinte digitale, le prétraitement des images, l'extraction des caractéristiques et la comparaison des empreintes. Les algorithmes couramment utilisés, tels que les minutie-based matching, les algorithmes basés sur les caractéristiques globales et les techniques de deep learning, sont discutés en détail. Le chapitre examine également les défis techniques, comme la qualité des images, les variations des empreintes digitales et les méthodes pour améliorer la précision et la vitesse de reconnaissance.

Chapitre 3 : Résultats et Discussions

Ce chapitre présente les résultats obtenus lors de la mise en œuvre du système de contrôle d’accès basé sur les empreintes digitales. Il analyse les performances du système en termes de précision, de rapidité et de fiabilité de la reconnaissance des empreintes. Les tests effectués dans différents scénarios et environnements sont décrits, et les résultats sont comparés aux objectifs initiaux du projet. Le chapitre discute des réussites et des défis rencontrés, ainsi que des solutions apportées pour surmonter ces obstacles. Enfin, il aborde les perspectives d'amélioration et d'extension du système, en suggérant des directions pour les travaux futurs et des applications potentielles.

Chapitre1:

Les Systèmes de Contrôle d’Accès : Concepts et Technologies de Base

Chapitre1 : Les Systèmes de Contrôle d'accès : Concepts et Technologies de Base

1. Introduction :

De nos jours, les méthodes de sécurité traditionnelles ou classiques des systèmes d'information ne sont plus acceptables lorsqu'elles sont utilisées par des individus. Il existe deux approches pour cette sécurité : la première dépend du savoir de la personne, tel qu'un mot de passe ou un code PIN, et la deuxième dépend de ce que la personne possède, tel qu'un badge ou une carte à puce.

Dans la première situation, l'utilisateur peut oublier son mot de passe ou celui-ci peut être deviné par une autre personne. Le badge (ou la pièce d'identité ou la clé) peut être perdu ou volé dans le deuxième cas. Afin de surmonter cette contrainte ou cette lacune, un autre moyen de sécurité a été mis au point, permettant d'utiliser non pas les informations qu'un individu possède ou connaît, mais une information qui lui est propre. La biométrie est une nouvelle méthode d'identification des individus. [3].

1. Système de contrôle d'accès :

Le terme "système de contrôle d'accès" est souvent utilisé pour désigner un système de sécurité électronique. Ainsi, ils permettent de créer, de gérer et de surveiller des droits d'accès. Ils gèrent l'identification des autorisations, l'authentification, l'approbation des accès et la responsabilité des entités grâce à des identifiants, notamment des mots de passe, des codes PIN, des analyses biométriques et des clés physiques ou électroniques. Et, comme ils sont capables d'enregistrer qui est entré où et quand, ils peuvent fournir par la suite des données précieuses pour le suivi et l'utilisation du local ou du bâtiment[2].

2. Types de contrôle d'accès :

Il existe plusieurs types de contrôle d'accès, chacun adapté à des besoins spécifiques en termes de sécurité et de gestion. Voici quelques-uns des types courants de contrôle d'accès :

2.1. Contrôle d'accès physique :

- **Badges ou cartes magnétiques :** Les utilisateurs portent des badges ou des cartes magnétiques qui sont scannés par des lecteurs pour autoriser l'accès.
- **Codes PIN :** Les utilisateurs entrent un code personnel pour accéder à une zone restreinte.
- **Biométrie :** L'utilisation d'empreintes digitales, de scans de la rétine, de reconnaissance faciale ou d'autres caractéristiques biométriques pour identifier et autoriser l'accès.

2.2. Contrôle d'accès logique :

Identifiants et mots de passe : Les utilisateurs doivent fournir un nom d'utilisateur et un mot de passe pour accéder à des systèmes informatiques ou des réseaux.

Cartes à puce : Des cartes à puce sont souvent utilisées pour l'authentification dans le contexte des systèmes informatiques.

Il est également possible de combiner ces types. Chaque méthode d'identification présente des avantages et des inconvénients, et le choix de la méthode dépend donc de la situation. La combinaison de ces normes augmente le niveau de sécurité. C'est ce qu'on appelle la vérification en deux étapes : par exemple, une personne peut présenter son badge pour s'identifier, puis un code PIN ou une empreinte digitale sera requis pour la vérification.

Fig .1.1 montre quelques-uns des types courants de contrôle d'accès. Et Tableau 1.1 représente les différentes méthodes de contrôle d'accès et les évalue selon leur capacité à empêcher la copie, le vol, l'oubli et la perte :

METHODES	COPIER	VOLER	OUBLIER	PERDRE
CLE	C	C	C	C
BADGE	--	C	C	C
CODE	C	--	C	--
BIOMETRIE	--	--	--	--

Tableau I.1 :Les différentes méthodes des systèmes des contrôle d'accès

Fig. 1.1. Types de dispositifs de contrôle d'accès[22].

3. Fonctions d'un système de contrôle d'accès :

Ces fonctions sont assurées à chaque point auquel l'on accède aux trois fonctions principales du système de contrôle d'accès physique, qui sont les suivantes :

- L'identification et l'authentification .
- Le traitement des données .
- Le déverrouillage.

Ces rôles sont remplis à chaque endroit où l'accès est surveillé. Le schéma fonctionnel d'un système de contrôle d'accès physique est illustré dans l'image suivante. Fig.1.2 représente le schéma fonctionnel d'un système de contrôle d'accès physique.

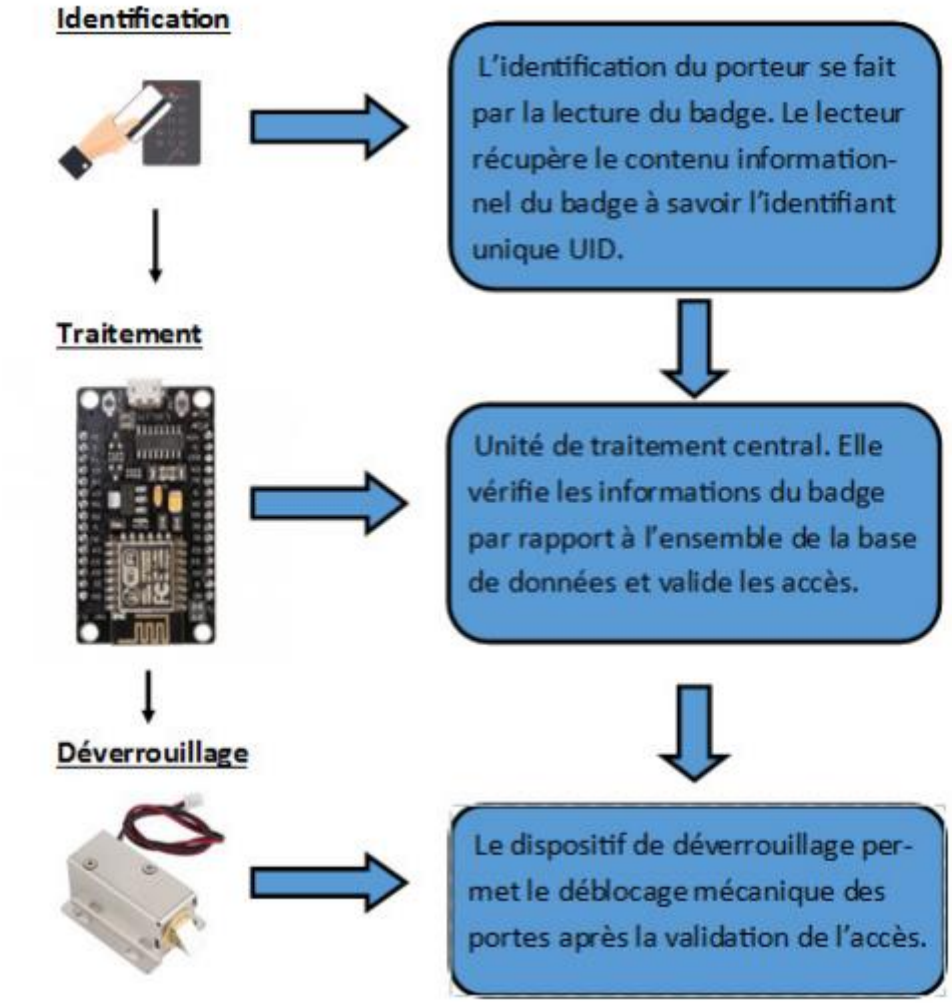


Fig 1.2. Fonctionnement d'un système de contrôle d'accès.

3.1.Phase d'identification et d'authentification :

Pour débuter, il est crucial de clarifier les termes employés dans le processus d'identification et d'authentification. L'acte de s'identifier implique la communication de son identité, tandis que l'authentification requiert la présentation de preuves confirmant cette identité. Il convient de rappeler que l'identité d'un individu englobe l'ensemble des données de fait et de droit permettant de le distinguer. Ainsi :

- La vérification de l'identité conduit à l'identification.
- La démonstration de l'identité mène à l'authentification.

Dans le cadre des systèmes de contrôle d'accès physique, notamment avec les technologies sans contact, la phase d'identification/authentification peut se limiter à la reconnaissance du badge ou à la combinaison de l'identification et de l'authentification du badge uniquement.

A. Identification :

Dans un système basé sur une technologie sans contact, l'identification se manifeste par la présentation d'un badge à un lecteur.

B. Authentification du badge :

L'authentification vise à confirmer la validité du badge. Pour un système de contrôle d'accès reposant sur des cartes sans contact, l'authentification du badge s'effectue généralement par un échange cryptographique, permettant au badge de prouver sa légitimité sans divulguer ses éléments confidentiels.

C. Authentification du porteur :

Une fois le badge authentifié au préalable, le porteur doit prouver qu'il est le détenteur légitime. L'authentification du porteur s'opère par l'utilisation d'un second élément choisi parmi "ce que l'on est et ce que l'on sait". Cela peut se concrétiser, par exemple, par la saisie d'un mot de passe ou par l'exploitation de la biométrie.

3.2. Traitement des données :

Le traitement des données repose principalement sur l'unité de traitement et de contrôle local (UTL). Cette entité assume la responsabilité de la gestion de toutes les demandes d'accès, en comparant ces requêtes avec un ensemble de droits d'accès stockés dans sa base de données. En conséquence, elle émet les instructions nécessaires pour libérer les verrouillages.

3.3.Verrouillage et déverrouillage :

Le mécanisme de verrouillage garantit le blocage physique du point d'accès afin d'entraver le passage des individus non autorisés. Le système de contrôle d'accès, quant à lui, autorise le déverrouillage correspondant[4].

4. La biométrie :

La biométrie est la mesure et l'analyse statistique des caractéristiques physiques et comportementales des individus. Cette technologie est principalement utilisée à des fins d'identification et de contrôle des accès. Elle permet aussi de tracer des individus sous surveillance.

Selon le principe de base de l'authentification biométrique, chaque individu est unique et peut être identifié par ses caractères physiques et ses traits de comportement intrinsèques. Le terme « biométrie » signifie la « mesure du vivant ».) [5].

Il existe deux principales classes d'identificateurs biométriques :

- **Les caractéristiques morphologiques** : forme ou composition du corps.
- **Les caractéristiques comportementales** : la façon dont se comporte une personne.

4.1. Un bref historique de la biométrie :

L'histoire de la biométrie remonte à l'ancienne Chine, où les marchands utilisaient les empreintes digitales des enfants pour les distinguer les uns des autres lors de la signature de documents. Cette méthode, l'une des plus anciennes pratiques biométriques, était également employée dans les échanges commerciaux de Babylone il y a 3000 ans avant J.-C. De même, dans l'Amérique précolombienne, des architectes laissaient des traces de leurs mains colorées sur les parois de grottes aménagées.

Cependant, ce n'est qu'au début du XVIIIe siècle que le Dr Henri Faulds a développé l'utilisation des empreintes digitales pour l'identification des personnes. Francis Galton a également contribué à cette époque en créant la méthode "Fingerprints", établissant l'unicité et la permanence des empreintes cutanées. Au XIXe siècle, la police criminelle a commencé à utiliser les empreintes digitales après l'échec du bertillonnage, une méthode basée sur les mensurations des criminels.

Au cours des trois dernières décennies, la biométrie a connu une évolution significative, passant d'une seule méthode, les empreintes digitales, à plus de dix méthodes distinctes. Malgré les préoccupations liées aux libertés et à la vie privée, des progrès continus sont réalisés, avec des centaines de nouvelles méthodes développées par les sociétés de biométrie. Aujourd'hui, la biométrie est une technologie établie utilisant des critères permanents et uniques pour garantir la sécurité dans les environnements physiques et numériques, marquant une révolution dans les domaines du e-business et du l'e-commerce[6].

5. Modalités biométriques

Aucune biométrie unique ne pouvant répondre efficacement aux besoins de toutes les applications d'identification. Un certain nombre de techniques biométriques ont été proposées, analysées, et évaluées. Chaque biométrie a ses forces et ses limites et ses conséquences, chaque biométrie est utilisée dans une application particulière. La biométrie biologique se base sur l'analyse des données biologiques liées à l'individu (salive, ADN, etc.). La biométrie comportementale se base sur l'analyse des comportements d'un individu (manière de marcher, dynamique de frappe au clavier, etc.). La biométrie morphologique se

base sur les traits physiques particuliers qui, pour toutes les personne, sont permanents et uniques (empreinte digitale, visage, etc.) [3].

5.1.Biométries physiques (Morphologiques)

Les modalités biométriques morphologiques reposent sur l'identification de caractéristiques morphologiques spécifiques obtenues à partir de diverses parties du corps humain. Ces parties incluent notamment l'œil (pour l'iris et la rétine), la main (pour les empreintes digitales, palmaires, les articulations du doigt et la géométrie de la main), ainsi que le visage. Il est également possible d'ajouter à cette liste d'autres modalités comme la forme de l'oreille, les vaisseaux sanguins de la main, et d'autres encore.

5.1.1. Les empreintes digitales :

Les empreintes digitales sont les minuscules crêtes, les verticilles et les motifs de vallée sur le bout de chaque doigt. Ils se forment à partir de la pression exercée sur les petits doigts en développement d'un bébé dans l'utérus. On n'a pas trouvé deux personnes ayant les mêmes empreintes digitales -- elles sont totalement uniques. Il y a une chance sur 64 milliards que vos empreintes correspondent exactement à celles de quelqu'un d'autre[7].

Les empreintes digitales sont encore plus uniques que l'ADN, le matériel génétique de chacune de nos cellules. Bien que les jumeaux identiques puissent partager le même ADN -- ou au moins la plupart -- ils ne peuvent pas avoir les mêmes empreintes digitales.

Les empreintes digitales sont une forme de biométrie, une science qui utilise les caractéristiques physiques des gens pour les identifier. Les empreintes digitales sont idéales à cette fin car elles sont peu coûteuses à collecter et à analyser, et elles ne changent jamais, même en vieillissant.

Bien que les mains et les pieds aient de nombreuses zones striées qui pourraient être utilisées pour l'identification, les empreintes digitales sont devenues une forme populaire de biométrie parce qu'elles sont faciles à classer et à trier. Ils sont également accessibles.

Les empreintes digitales sont faites d'un arrangement de crêtes, appelées crêtes de frottement. Chaque crête contient des pores, qui sont attachés aux glandes sudoripares sous la peau. Vous laissez des empreintes sur les verres, les tables et à peu près tout ce que vous touchez à cause de cette sueur.

Fig.1.3 représente un système de contrôle d'accès par l'empreinte digitale

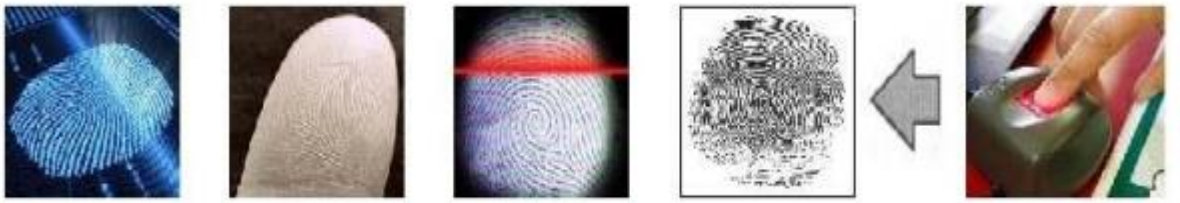


Fig 1.3. Contrôle d'accès par empreinte digitale.

5.1.2. Modalité de la main :

La reconnaissance de la main est l'une des modalités biométriques les plus anciennes. Elle a été utilisée dans les systèmes biométriques commerciaux. Ce n'est pas la première modalité apparue mais elle a été la première à être pratiquement utilisée. Le premier système commercialisé a fait son apparition en 1974. Il a été conçu pour le contrôle d'accès à certains lieux, pour identifier les personnes et le temps de travail des employés. Les premiers succès de la reconnaissance palmaire étaient vers 1985 grâce au travail de David Sidlauskas sur cette technologie[8].

La modalité de la main repose principalement sur trois notions qui permettent de qualifier numériquement la main : la géométrie de la main, les traits de la paume et les veines de la main.

- La géométrie de la main grâce à son principe trivial, la géométrie de la main est la première technique à avoir été utilisée dans la modalité de la main. Elle est basée sur des mesures géométriques de la main telles que la taille, les dimensions des doigts et la surface de la paume pour faire le codage des données .
- Les empreintes palmaires Une simple capture de la paume de la main montre qu'elle comporte deux types de lignes : Lignes principales et lignes secondaires. La reconnaissance palmaire est basée sur les descripteurs suivants :
    - Les lignes principales : Ce sont les trois lignes foncées tracées sur la surface de la paume.
    - Les rides : Ce sont les courtes lignes, dites lignes secondaires, dispersées irrégulièrement sur la surface de la paume.
    - Points de référence : Ce sont les deux points d'extrémité de la paume.
    - Les minuties : Ce sont les points de discontinuité des épuisements de l'épiderme se situant sur la face intérieure de la main.

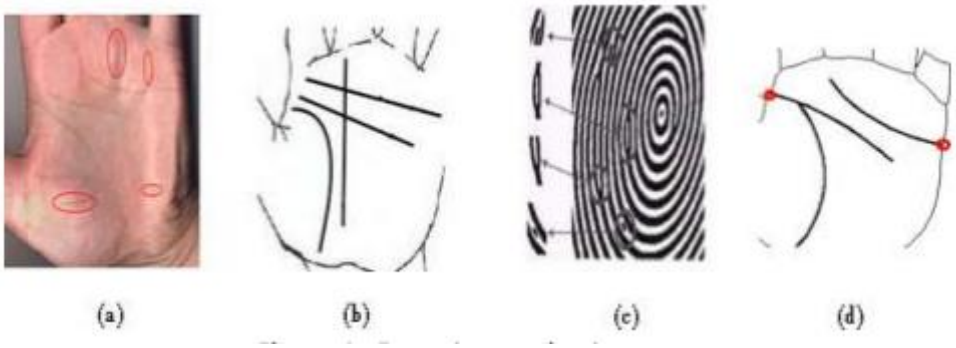


Fig 1.4. Empreintes palmaires : (a) les rides, (b) les lignes principales, (c) les minuties et (d) les points de référence.

5.1.3. Le visage :

Nos visages sont des objets complexes avec des traits qui peuvent varier dans le temps. Cependant, les humains ont une capacité naturelle à reconnaitre les visages et à identifier les personnes dans un coup d'œil. Bien sûr, notre capacité de reconnaissance naturelle d'un être humain ne s'étend pas au-delà de la reconnaissance du visage, où nous sommes également en mesure de repérer rapidement des objets, des sons ou des odeurs. Malheureusement, cette aptitude naturelle n'existe pas dans les ordinateurs. C'est ainsi qu'est né le besoin de simuler artificiellement la reconnaissance afin de créer des systèmes intelligents autonomes simulant notre capacité naturellement. La reconnaissance des visages dans les machines est une tâche difficile, mais pas impossible. Tout au long de notre vie, de nombreux visages sont vus et conservés facilement dans nos mémoires, formant une sorte de base de données. La reconnaissance du visage est utilisée comme un système de surveillance ou d'identification par les autorités ou les corps policiers, principalement dans les lieux publics. Elle est parmi les techniques les plus acceptables, mais elle nécessite un arrière-plan simple et fixe pour que le résultat soit précis.

Fig 1.5. Scanner le visage de l'identité.

5.1.4. L’iris :

L’iris est la région, sous forme d’anneau, située entre la pupille et le blanc de l’œil. C’est unique. L’iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu. La reconnaissance de l’iris est développée dans les années 80,c’est pour cela qu’elle est une technologie plus récente. L’image de l’iris est capturée par un appareil qui contient une caméra infrarouge, lorsque la personne se place à une courte distance de l’appareil [9].

Fig.1.6 représente un système de contrôle d’accès par reconnaissance de l’iris

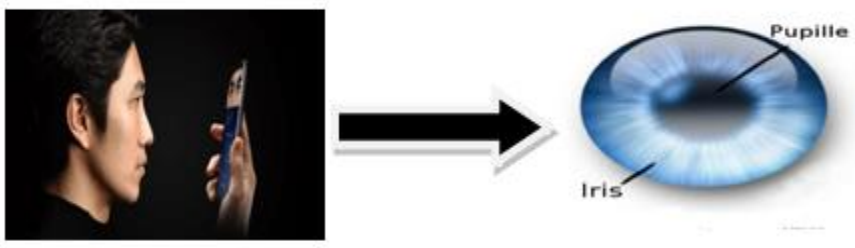


Fig 1.6. Reconnaissance de l’iris .

5.1.5. La rétine :

La rétine, localisée au fond de l'œil, représente la couche sensorielle essentielle. Elle constitue la paroi interne opposée de l'œil, sur laquelle les images que nous percevons sont projetées. Cette couche est parcourue par un réseau complexe de vaisseaux sanguins, dont la configuration reste constante au fil du temps et varie d'un individu à l'autre, même en cas de jumeaux. De plus, l'empreinte rétinienne est relativement à l'abri des blessures, et la disposition des vaisseaux demeure inchangée tout au long de la vie, sauf en cas de certaines maladies. Ces caractéristiques la rendent résistante aux altérations, renforçant ainsi la rétine comme l'une des méthodes biométriques les plus fiables actuellement disponibles[20].

Lors de la reconnaissance rétinienne, l'utilisateur doit positionner son œil à quelques centimètres d'une ouverture de capture située sur le lecteur de rétine. Il est crucial de maintenir une immobilité totale tout en fixant un point vert lumineux en rotation. À ce moment précis, un faisceau lumineux traverse l'œil jusqu'aux vaisseaux sanguins capillaires de la rétine.

Fig.1.7 représente un système de contrôle d’accès par reconnaissance de la rétine

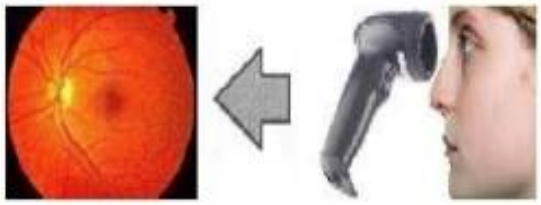


Fig 1.7. Reconnaissance de La rétine.

5.2.Biométries comportementales :

Les caractéristiques biométriques comportementales se réfèrent à des traits distinctifs basés sur les comportements individuels d'une personne. Contrairement aux caractéristiques physiques telles que les empreintes digitales ou la rétine, les biométriques comportementales se concentrent sur des aspects liés aux habitudes et aux actions de l'individu. Ces caractéristiques peuvent inclure des modèles de frappe au clavier, la manière de marcher, la voix, les expressions faciales, les schémas de mouvement des yeux, ou d'autres comportements spécifiques.

5.2.1. La voix :

Chaque individu possède une voix unique, formée par des composantes physiologiques et comportementales. La reconnaissance vocale a pour objectif d'identifier les caractéristiques distinctives de la voix de chaque personne. Ce processus s'appuie sur des éléments tels que la tonalité de la voix de la personne examinée, la fréquence vocale, et la distance entre la formation des lettres lors de la parole.

La voix permet de différencier les hommes des femmes, bien que cette distinction soit fortement influencée par la qualité de l'enregistrement et le type de message. Diverses caractéristiques de la voix sont extraites, telles que le débit, la force, la dynamique et la forme des ondes générées. Il est important de noter que la manière dont un individu s'exprime peut varier en fonction de l'âge et être temporairement influencée par l'état de santé ou émotionnel du locuteur. Afin de surmonter ces variations, une méthodologie appropriée doit être appliquée[10].

Cette forme de biométrie est généralement bien acceptée, car la voix est un signal naturel à produire, offrant ainsi une méthode de reconnaissance pratique et accessible.

Fig.1.8 représente un forme de signal de voix

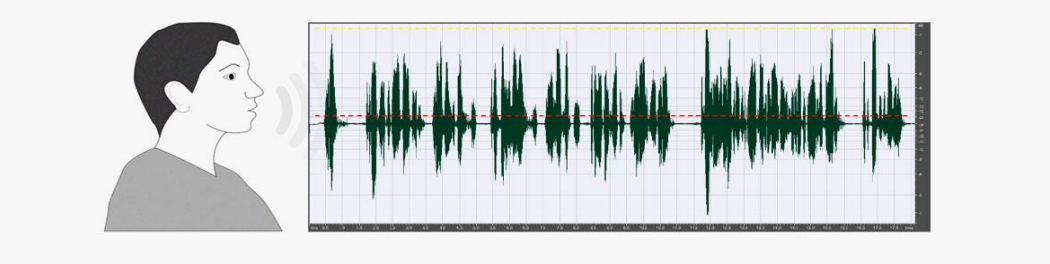


Fig 1.8. Signal de voix.

5.2.2. Dynamique de frappe au clavier :

La vérification d'identité par la dynamique de frappe au clavier repose sur l'analyse du rythme de frappe d'un individu. Chaque personne a une méthode unique de taper, caractérisée par la pression exercée sur les touches, les erreurs fréquentes, et la vitesse de frappe.

Plusieurs méthodes permettent de détecter des erreurs, comme prendre en considération les variations de la durée de pression sur une touche ou le laps de temps entre la fin de la saisie d'un mot et l'appui sur la barre d'espace. Ces erreurs deviennent des marqueurs distinctifs permettant de différencier les individus et d'effectuer une identification précise.

Bien que l'analyse de la dynamique de frappe au clavier ne prenne pas encore en compte certains éléments extérieurs tels que la fatigue, l'humeur ou une blessure, les habitudes de frappe sont enregistrées au fil du temps. Cette fonctionnalité confère au système une flexibilité lui permettant de vous reconnaître même en cas de stress ou de fatigue occasionnels.

5.2.3. Signature dynamique :

La signature dynamique est une méthode de biométrie comportementale qui vise à authentifier et à identifier une personne en analysant la manière dont elle signe de manière électronique. Contrairement à la signature statique traditionnelle, qui se concentre sur l'apparence de la signature sur un document papier, la signature dynamique capture des aspects dynamiques et temporels de l'acte de signer[7].

Fig.1.9 représente certains types de signature manuscrite

Fig 1.9. Signature manuscrite.

5.3.Biométrie biologique :

Une autre catégorie qui est l'étude des traces biologiques. Elle regroupe des caractéristiques telles que l'odeur, le sang, la salive, le cheveu, l'ADN, la thermographie faciale et la forme des veines de la main, etc.

5.3.1. Les veines de la main :

La biométrie basée sur les veines de la main, également connue sous le nom de reconnaissance des veines palmaires, est une méthode d'identification qui utilise les caractéristiques uniques des veines visibles sous la peau de la main. Cette technologie repose sur le principe que la disposition des veines dans la paume de la main est unique pour chaque individu.

Les avantages de la biométrie des veines de la main comprennent la difficulté de falsification, car les veines sont sous la surface de la peau et ne sont généralement pas visibles à l'œil nu. De plus, cette méthode est peu invasive puisqu'elle ne nécessite pas de contact direct avec le capteur, contrairement à certaines autres formes de biométrie.

5.3.2. Analyse de l'ADN :

L'ADN (Acide Désoxyribonucléique) représente le code ultime et unique de l'individualité d'une personne, à l'exception du fait que les jumeaux identiques ont un motif d'ADN identique. L'ADN est la partie d'une cellule qui contient des informations génétiques (structure chimique) propres à chaque personne, utilisée dans le cadre d'une forme d'identification. L'ADN d'une personne peut être trouvé dans tout son corps. L'ADN est présent dans divers matériaux corporels tels que le sang, la salive, les cheveux, les dents, le mucus et le sperme.

L'utilisation de l'ADN dans les enquêtes criminelles a considérablement augmenté ces dernières années. Cela a grandement aidé les forces de l'ordre à identifier les criminels et à résoudre des crimes difficiles.

Fig.1.10 représente un système de contrôle d'accès par reconnaissance d'ADN

Fig 1.10. Reconnaissance d'ADN.

6. Architecture d'un système biométrique :

Un système biométrique est un système qui possède en entrée l'acquisition des données biométriques à partir d'un appareil de mesure (cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité,…etc.). Il extrait l'ensemble des caractéristiques à partir des données acquises et les compare avec celles enregistrées dans la base de données.

Selon le contexte d'application, on distingue deux modes d'utilisation distincts d'un système biométrique : Le mode d'identification et le mode de vérification**.**

6.1.Mode d'identification :

Ce mode implique l'identification d'une personne parmi un ensemble composé de N individus. A l'aide de la base de données disposée dans le système biométrique, on compare les données fournies par l'utilisateur avec celles contenues dans la base afin de trouver la personne correspondante.

Fig.1.11 représente l'identification d'une personne dans un système biométrique.

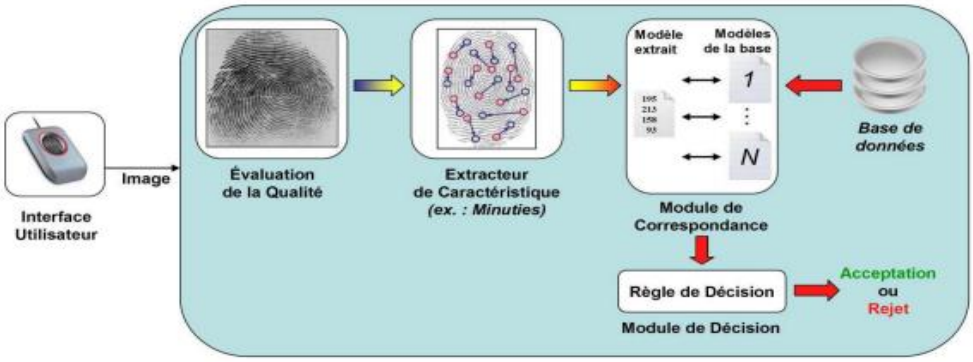


Fig 1.11. Identification d'une personne dans un système biométrique [21].

6.2.Mode de vérification (authentification):

Ce procédé est plus simple. L'utilisateur doit fournir une donnée et un identifiant. Le système valide l'identité d'une personne en comparant la donnée contenue dans la base de données biométriques correspondante à l'identifiant avec celle de l'utilisateur. Un tel système devra simplement prendre une décision d'acceptation ou de rejet.

Fig.1.12 montre l'authentification d'une personne dans un système biométrique.

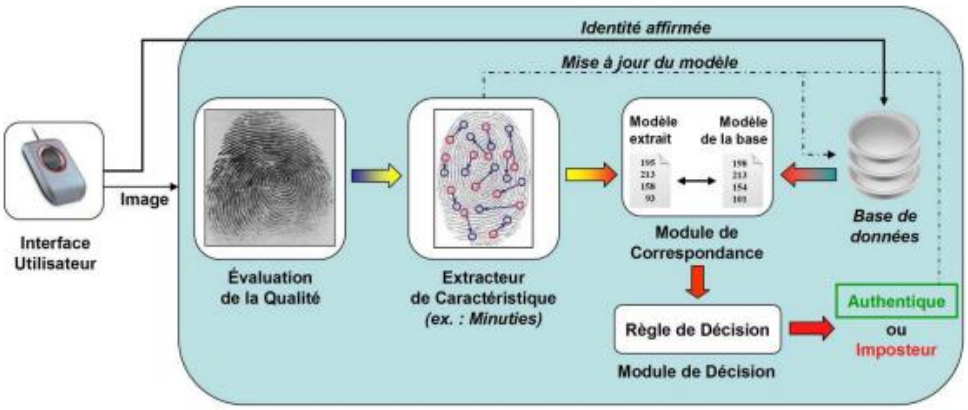


Fig 1.12. Authentification d'une personne dans un système biométrique [21].

Un système biométrique comporte deux phases essentielles: le module d'apprentissage et celui de reconnaissance et une phase facultative qui est le module d'adaptation.

Fig.1.13 représente l'architecture d'un système de reconnaissance biométrique.

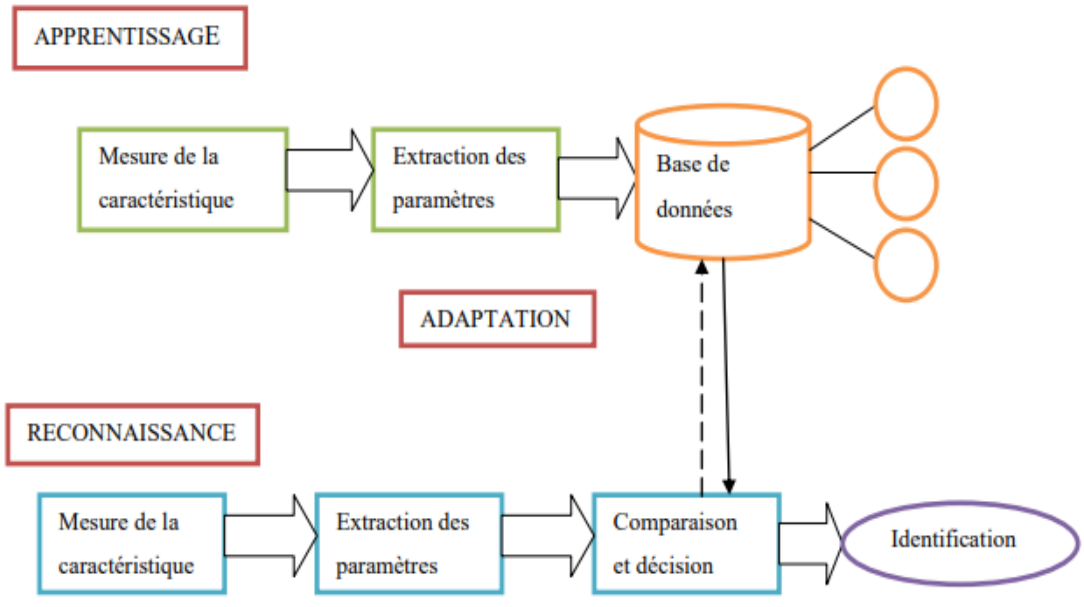


Fig 1.13. Architecture d'un système de reconnaissance biométrique.

- **Le module d'apprentissage :**

Lors de la phase d'apprentissage, l'acquisition des caractéristiques se fait grâce au module de capture. En général, cette capture est enregistrée après un ensemble de transformations qu'on lui applique dans le module d'extraction de caractéristiques. Donc, on extrait seulement l'information pertinente afin de former une nouvelle présentation compacte dans le but de faciliter la reconnaissance et de diminuer aussi la quantité de stockage.

Enfin, le rôle principal de ce module est de constituer une base de données où chaque modèle est obtenu à partir d'un ou de plusieurs enregistrements de la modalité considérée. Chaque personne a un modèle spécifique et unique dans la base de données biométriques. La plupart des modèles rencontrés sont des modèles statistiques qui permettent de prendre en compte une certaine variabilité dans les données individuelles.

- **Le module de reconnaissance :**

Au cours de ce module, l'ensemble des caractéristiques extraites sera comparé avec le modèle enregistré dans la base de données du système. L'étape de décision permet soit de vérifier l'identité affirmée par un utilisateur ou de déterminer l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et les modèles stockés.

Alors, ce module permet de prendre une décision. Si l'on est en mode identification, le système compare le signal mesuré avec les différents modèles contenus dans la base de données et sélectionne le plus proche. En mode vérification, le système compare le signal mesuré avec un seul des modèles de la base de données et autorise ainsi la personne ou la rejette.

- **Le module d'adaptation :**

Pendant la phase d'apprentissage, le système biométrique ne capture souvent que quelques instances d'un même attribut afin de limiter la gêne pour l'utilisateur. Il est donc difficile de construire un modèle assez général capable de décrire toutes les variations possibles de cet attribut. De plus, les caractéristiques de cette biométrie ainsi que ses conditions d'acquisition peuvent varier. L'adaptation est donc nécessaire pour maintenir ou améliorer la performance d'un système utilisation après utilisation[11].

Conclusion :

Les systèmes de contrôle d'accès biométriques émergent comme une alternative prometteuse aux méthodes traditionnelles basées sur des mots de passe ou des badges, en offrant une sécurité accrue grâce à l'utilisation de caractéristiques physiques ou comportementales uniques à chaque individu.

Les avantages de la biométrie pour le contrôle d'accès sont nombreux. Tout d'abord, elle garantit une sécurité renforcée, ce qui offre une protection accrue contre les accès non autorisés. De plus, elle présente une commodité pour l'utilisateur, éliminant le besoin de se souvenir de codes ou de transporter des badges, l'authentification étant simple et rapide

Cependant, des défis subsistent. Les coûts associés aux technologies biométriques peuvent être plus élevés que les méthodes traditionnelles. De plus, la collecte et le stockage sécurisés des données biométriques sensibles soulèvent des préoccupations en matière de confidentialité. La précision des technologies biométriques peut parfois être imprécise, générant des erreurs de rejet ou d'acceptation, et leur fiabilité peut être impactée par des facteurs environnementaux ou des variations physiologiques.

Bien que la biométrie offre des avantages significatifs en matière de sécurité et de commodité pour le contrôle d'accès, le choix judicieux de la technologie adaptée à l'application est crucial. Il est essentiel de prendre en compte les défis liés à la confidentialité, à la précision et à la fiabilité. Des recherches et des développements continus sont nécessaires pour améliorer les performances des technologies biométriques et réduire les coûts. L'avenir de la biométrie dans le contrôle d'accès s'annonce prometteur, avec son rôle croissant dans la sécurisation des accès et la protection des données sensibles, grâce à l'évolution des technologies et la prise en compte des défis existants.

Chapitre 2:

Méthodes et des algorithmes de reconnaissance des empreintes digitales

Chapitre 2: Méthodes et des algorithmes de reconnaissance des empreintes digitales

1. Introduction :

Ce chapitre offre une revue exhaustive des méthodes et des algorithmes de reconnaissance des empreintes digitales, en présentant les principes de base sur lesquels reposent ces technologies, ainsi qu'une analyse des principaux algorithmes utilisés dans ce domaine. Nous discuterons d'abord des étapes générales du processus de reconnaissance des empreintes digitales, qui incluent la collecte de données, l'amélioration de la qualité des images, l'extraction des caractéristiques et la correspondance des empreintes digitales. Ensuite, nous aborderons les algorithmes de base tels que l'algorithme basé sur les minuties (Minutie-based Algorithm).

De plus, nous mettrons en lumière les défis rencontrés dans le processus de reconnaissance des empreintes digitales, telles que la variabilité de la qualité des images, l'influence des facteurs environnementaux et le besoin de développer des algorithmes plus efficaces et précis. Enfin, nous examinerons les diverses applications de ces technologies dans différents domaines et comment elles bénéficient des progrès continus dans ce domaine.

À travers ce chapitre, nous visons à fournir une compréhension approfondie des mécanismes de reconnaissance des empreintes digitales et à expliquer comment appliquer ces technologies de manière pratique dans les systèmes de reconnaissance et de vérification d'identité.

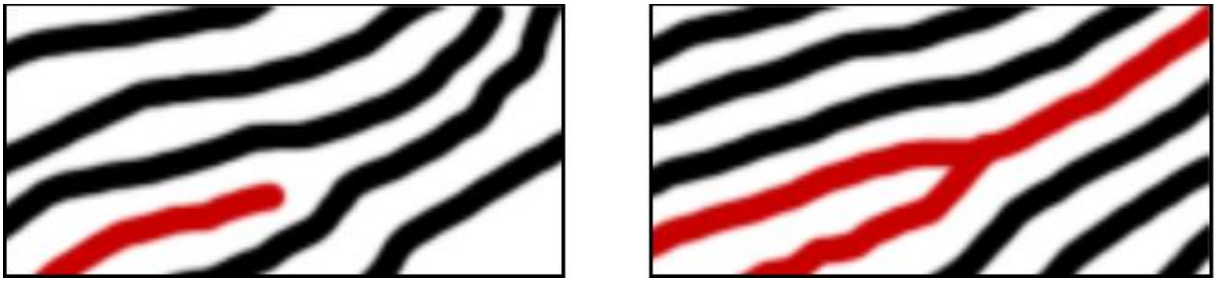
2. Introduction aux minuties

De nombreuses méthodes d'identification par empreintes digitales ont été proposées dans la littérature au fil des ans. L'approche de correspondance la plus populaire pour l'identification par empreintes digitales est généralement basée sur des caractéristiques de bas niveau déterminées par des singularités dans les motifs de crêtes digitales appelées minuties. En général, les deux caractéristiques les plus utilisées sont les extrémités de crêtes et les bifurcations de crêtes. Des caractéristiques d'empreintes digitales plus complexes peuvent être exprimées comme une combinaison de ces deux caractéristiques de base[12].

Fig.2.1 représente un exemple de minuties.

L'extraction de minuties consiste à détecter et à décrire ces points caractéristiques dans une empreinte digitale. Pour chaque minutie détectée, quatre paramètres sont généralement utilisés pour la décrire suivant l'équation suivante :

$$mi\ (xi, yi, \theta i, ti) \qquad (1)$$



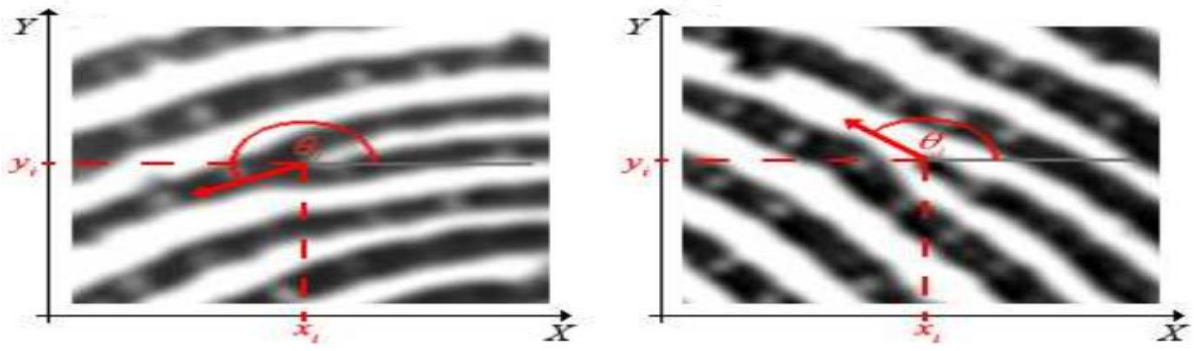
a. fin de crête b. bifurcation.

Fig.2.1. Exemple de minuties

Où, (x) et (y) sont les coordonnées du point dans l'image où la minutie est détectée. Elles indiquent où se trouve la minutie dans l'empreinte digitale. (θ) est la direction de la minutie par rapport à l'axe horizontal. Cette direction est souvent déterminée à partir de l'orientation locale des crêtes dans la région entourant la minutie. Le type (t) s'agit du type de la minutie, c'est-à-dire s'il s'agit d'une extrémité de crête ou d'une bifurcation de crête.

Dans le cadre de la description mathématique, chaque minutie (mi) est donc représentée par un ensemble de ces quatre paramètres. La position de la minutie correspond à ses coordonnées dans l'image, tandis que sa direction et son type fournissent des informations sur la structure locale de l'empreinte digitale à cet endroit précis.

Fig.2.2 représente un exemple détaillé de minuties.



a) b)

Fig.2.2. Paramètres des détails a) bifurcation et b) type de fin de crête

3. L'algorithme de la reconnaissance d'empreintes digitales :

L'objectif principal consiste donc à avoir un système qui distingue une image en entrée de plusieurs images présentes dans une base de données. Afin d'y parvenir, il est nécessaire d'adopter une méthode rapide et précise. C'est pourquoi nous allons supprimer l'approche de comparaison des images pixel par pixel car elle est assez lente. La comparaison des empreintes repose sur l'analyse de la distinction entre les minuties d'image d'entrée et les autres dans la base de données.

La technique la plus courante pour repérer les anomalies est de représenter l'empreinte en noir et blanc, ce qui est appelé binarisation de l'image, et de donner une même taille aux lignes de l'empreinte, ce qui est appelé squelettisation. Après avoir obtenu l'image binaire squellettisée, on peut mieux observer les minuties (singularités), ce qui permet de les détecter.

3.1. Prétraitement des images d'empreinte:

Basé sur la nature des bases de données qui contient les différentes empreintes on observe que tous les images nécessitent un traitement.

Fig.2.3 représente un exemple d'empreintes digitales extraites de bases de données.

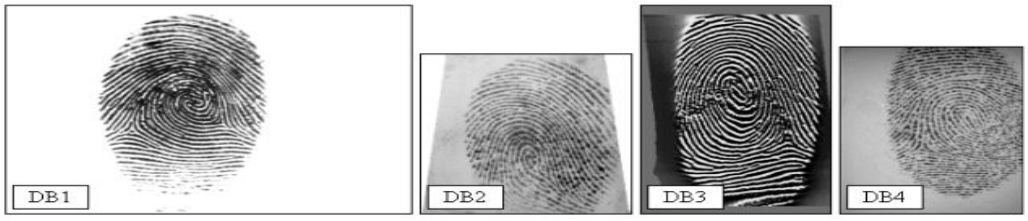


Fig.2.3. Exemple d'empreintes digitales extraites de bases de données.

L'objectif principal est de rendre l'image d'empreinte binaire, ce qui implique de convertir une image à plusieurs niveaux en une image en noir et blanc (seulement deux niveaux).

La technique de binarisation des empreintes digitales consiste à créer une image de type 1-bit, avec 0 pour les crêtes teintées de noir et 1 pour les vallées teintées de blanc[13].

Afin d'obtenir une image binarisée de manière adéquate, il est essentiel de sélectionner une méthode de binarisation qui nous donne une forme d'empreinte sans anomalies. Dans cette étude, nous avons testé différents algorithmes de binarisation.

Fig.2.4 représente un exemple d'opération de la binarisation.

Fig.2.4 : Example d' operation de la binarisation.

La deuxième étape, appelée squelettisation, vise à réduire la quantité d'informations redondantes présentes dans une image, ce qui réduit la quantité de données à analyser. La technique consiste à séparer les lignes principales de l'image en les amincissant progressivement jusqu'à ce que l'image finale ne contienne que des lignes d'une épaisseur de 1 pixel.

Un algorithme d'amincissement (ou shrinking algorithm) implique la suppression de points simples jusqu'à ce qu'ils soient stabilisés, ce qui donne lieu à un noyau homotypique. Si la suppression est effectuée de manière séquentielle, cela permet de préserver la topologie en définissant un point simple. Lorsqu'on modifie le processus de manière que certains points simples soient conservés pendant la suppression, on peut alors conserver des caractéristiques géométriques. Un algorithme de squelettisation (ou thinning algorithm) est utilisé pour désigner ce processus, et le résultat est connu sous le nom de squelette. On appelle points terminaux ou points extrémités les points à conserver [14].

3.2. Extraction des minuties :

L'extraction des minuties est une étape cruciale dans la reconnaissance des empreintes digitales. Elle consiste à identifier et à décrire les points singuliers dans le motif des crêtes des empreintes. Ces points singuliers, appelés minuties, sont utilisés pour créer une représentation unique et distinctive de l'empreinte digitale.

L'extraction des minuties est cruciale car ces caractéristiques sont uniques à chaque empreinte digitale, même entre des empreintes de doigts différents du même individu. Elles permettent de créer une représentation unique de l'empreinte qui peut être utilisée pour la comparaison et la reconnaissance dans les systèmes biométriques.

4. Algorithme d'Extraction des Minuties :

L'extraction des minuties est une étape clé dans le processus de reconnaissance d'empreintes digitales. Elle consiste à identifier les points caractéristiques, ou minuties, sur une empreinte digitale, qui sont utilisés pour la comparaison et l'identification. Pour assurer une extraction précise et fiable, il est crucial de suivre plusieurs étapes méthodologiques, incluant le prétraitement de l'image, la binarisation et la squelettisation. Ces étapes permettent de préparer l'image de l'empreinte digitale pour une analyse détaillée et l'extraction des minuties.

4.1. Prétraitement d'image d'empreinte :

Afin de faciliter la squelettisation, il est nécessaire de convertir l'image en 256 niveaux de gris à ce stade en une image binaire, où les pixels noirs représentent les stries et les pixels blancs les vallées.

4.1.1. Binarisation d'images :

La binarisation d'images est une étape critique dans le traitement des empreintes digitales. Elle consiste à convertir une image en niveaux de gris en une image binaire, où les pixels sont soit noirs, soit blancs. Cette conversion permet de simplifier l'image et de mettre en évidence les structures importantes pour les étapes ultérieures de traitement, comme la squelettisation et l'extraction des minuties. Une binarisation efficace est essentielle pour obtenir des résultats précis et fiables.

A) Binarisation d'images par la méthode d'Otsu :

La sélection du seuil Otsu est l'une des méthodes les plus cruciales pour déterminer le seuil global. Lorsque nous établissons un seuil général, nous optons pour une valeur de seuil unique pour toutes les images.

Après la mise en œuvre, il est évident que lorsque la qualité d'une image d'empreinte est très faible, la méthode de seuil général ne peut pas assurer des résultats satisfaisants. Est-ce qu'il faut trouver un seuil spécifique qui ait un effet adéquat pour déduire une image résultante acceptable et utilisable lors de la prochaine étape de la squelettisation?

Fig.2.5 représente un exemple de binarisation avec la méthode D'OTSU.

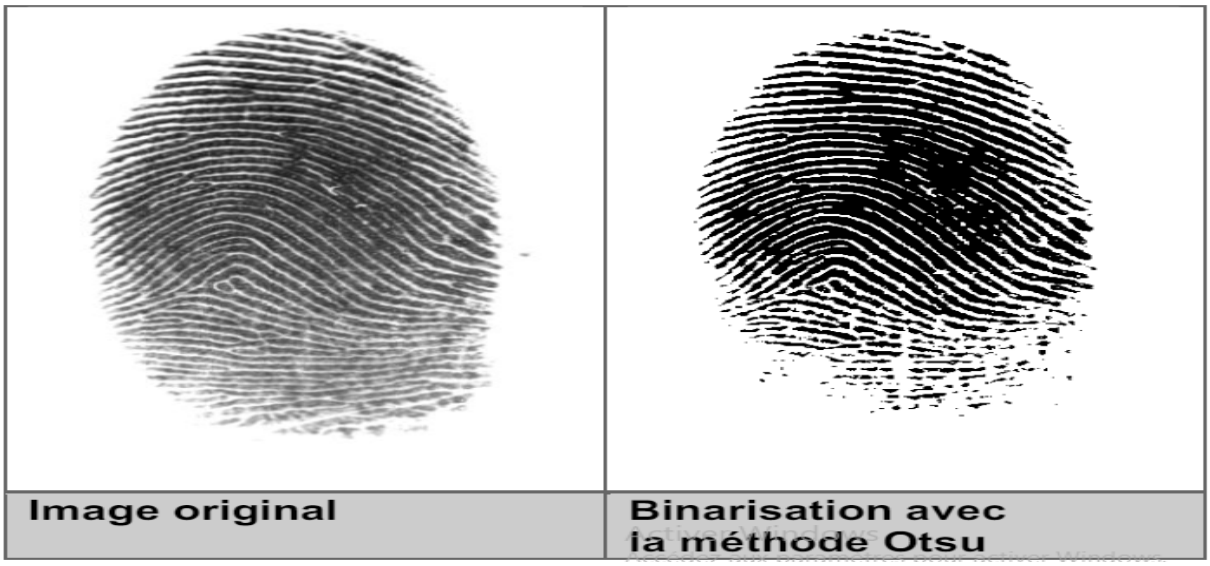


Fig.2.5. Binarisation avec la méthode D'OTSU.

La solution:

Nous allons opter pour des méthodes de binarisation locale qui appliqueront le seuil de manière distincte dans chaque canal. Il y a d'autres algorithmes similaires qui se spécialisent dans la résolution du problème de la binarisation locale tels que :

• Threshold Local de Bradley.

• Threshold local de Bernsen.

• Threshold maximum d'entropie.

Il s'agit de méthodes de seuillage employées lorsqu'un fond est homogène ou que les différentes parties d'un document ont des origines différentes.

Nous allons sélectionner l'une des trois approches pour l'intégrer dans notre système.

B) Bernsen local Threshold:

Des techniques de seuillage local sont employées.Le terme "local" fait référence au calcul du seuil pour chaque pixel en fonction des caractéristiques de l'image à l'intérieur d'une fenêtre de rayon R autour d'elle.

Le seuillage local du Bernsen permet de déterminer le minimum et le maximum pour un voisinage autour de chaque pixel du processus.

Un seuil de contraste est fourni par l'utilisateur pour le procédé. En cas d'augmentation ou d'égalité du contraste local (max-min), le seuil est établi à la valeur de moyenne gris locale (la moyenne du minimum et du maximum des valeurs de gris dans la fenêtre locale).

4.1.2. Squelettisation d'image

Pour faciliter l'extraction des minuties, l'image doit être squelettique.

Les deux méthodes de squelettisation Zhang et Shapiro qu'on a nous allons les expérimenter sur des images binaires, l'objectif étant d'extraire les minuties.

Supposant qu'on a une image 3*3 démontré comme suit :

a) L'algorithme d'amincissement de Zhang-Suen

A(P1) : Nombre de pixel 1 ou 0 qui dans l'entourage de P1, dans notre cas P2, P3, P4, P5, P6, P7, P8, P9, P8.

B(P1) : Nombre des pixels noire ou 1 qui dans l'entourage de P1.

On ajoute la 1ère condition pour sélectionner les pixels noire pour supprimer

Condition 1: $2 \leq B(P1) \leq 6$

Condition 2: A(P1)=1.

Condition 3: P2. P4. P6 = 0

Condition 4: P4.P6.P8=0

Cette itération est répétée jusqu'à stabilité, i.e. jusqu'à ce qu'il n'y ait plus de point simple[15].

b)L'algorithme d'amincissement de Hilditch :

B (p1) = Nombre de voisins non nuls de p1

Et

A (p1) =Nombre de motifs 0,1 dans la séquence p2, p3, p4, p5, p6, p7, p8, p9, p2

Il existe deux versions pour l'algorithme de Hilditch, une en utilisant une fenêtre de 4x4 et l'autre à l'aide d'une fenêtre de 3x3.

L'algorithme de Hilditch consiste à effectuer plusieurs passes sur le modèle et à chaque passage, l'algorithme vérifie tous les pixels et décide de changer un pixel du noir au blanc si elle satisfait les quatre conditions suivantes [16]:

Condition 1: 2 <= B(p1) <= 6

- B(p1) est le nombre de pixels noirs parmi les huit voisins de p1 .
- Cette condition assure que le pixel \(p1 \) n'est ni un point isolé ni un point trop connecté.

Condition 2 : A(p1) = 1

- A(p1) est le nombre de transitions de 0 à 1 parmi les huit voisins de p1 en parcourant dans le sens horaire.
- Cela signifie que p1 a exactement une composante connectée noire parmi ses voisins.

Condition 3 : p2 * p4 * p8 = 0 ou A(p2) diffèrent a 1

- p2 , p4 , et p8 sont les pixels voisins de p1 en haut, à gauche, et en bas à gauche, respectivement.
- Cette condition vérifie que la suppression de p1 ne déconnecte pas le squelette.

Condition 4 : p2 * p4 * p6 = 0 ou A(p4) diffèrent a 1

- p2 , p4 , et p6 sont les pixels voisins de p1 en haut, à gauche, et à droite, respectivement.

Fig.2.6 montre l'opération du prétraitement

Fig.2.6. Opération du prétraitement.

4.2. Extraction des minuties:

L'extraction des minuties est une étape fondamentale dans le processus de reconnaissance des empreintes digitales. Elle consiste à détecter et isoler les points singuliers, comme les terminaisons de crêtes et les bifurcations, qui sont uniques à chaque empreinte. Cette étape requiert une série de traitements et de transformations de l'image pour assurer que les minuties extraites soient précises et utiles pour l'identification.

4.2.1. Méthode d'amincissement des crêtes :

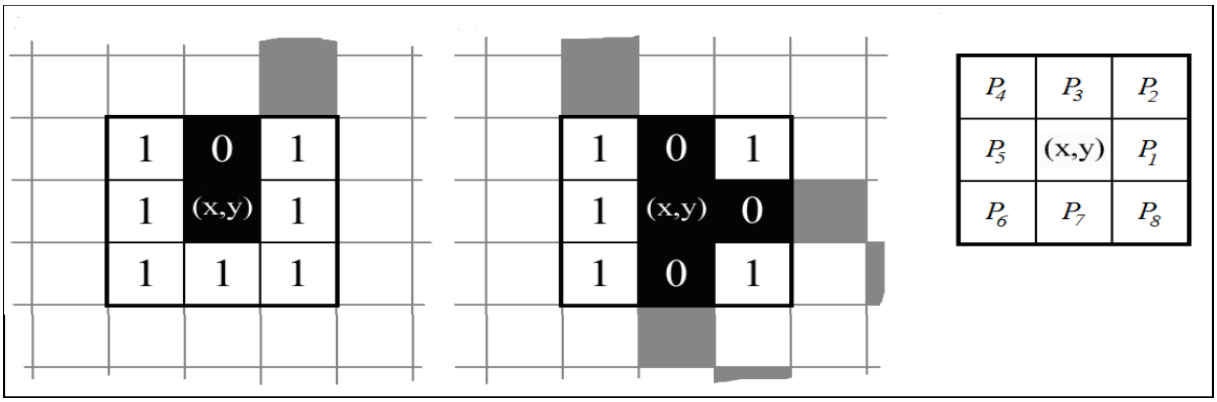
La méthode la plus couramment utilisée pour l'extraction des minuties est le concept de Nombre de Croisements (CN) [2, 3, 4]. L'image de crête binaire nécessite un traitement supplémentaire avant que les caractéristiques de minutie puissent être extraites. La première étape consiste à binariser et ensuite à amincir les crêtes, de manière à ce qu'elles ne fassent qu'un seul pixel de largeur Fig2.7. Un grand nombre de méthodes de squelettisation sont disponibles dans la littérature, en raison de leur rôle important dans de nombreux systèmes de reconnaissance[17].

a) b)

Fig.2.7. Image d'empreinte digitale a) binarisation. et b) squelettisation.

Les points de minutie sont déterminés en balayant le voisinage local de chaque pixel dans l'image des crêtes amincies, en utilisant une fenêtre 3×3.

Fig.2.8 représente un matrice d'un pixel.



a) b) c)

Fig.2.8. Matrice d'un pixel a) Fin de crête et b) bifurcation et c) fenêtre 3×3.

La valeur du CN est alors calculée, définie comme la moitié de la somme des différences entre les paires de pixels voisins ip et ip+1 , comme le montre l'équation (2)

$$CN_{(x,y)} = \frac{1}{2}\sum_{i=1}^{8}\left|p_i - p_{i+1}\right|, \quad p_1 = p_9 \qquad (2)$$

En utilisant les propriétés du CN comme indiqué dans le tableau , le pixel de crête peut alors être classé comme une extrémité de crête, une bifurcation ou un point non-minutie.

Propriété du CN :

- 0 : Point isolé
- 1 : Extrémité de crête
- 2 : Crête continue
- 3 : Bifurcation
- 4 : Croisement

4.3. Comparaison des minuties:

La précision et la rapidité sont les premiers objectifs que nous souhaitons atteindre lors de la conception d'un système de reconnaissance des empreintes digitales. Si nous optons pour une méthode basée sur la comparaison des images pixel par pixel, cela peut être assez lent. C'est pourquoi nous avons opté pour une méthode qui prend en compte les coordonnées des minuties stockées sous format texte dans une table de bases de données. Ainsi, la partie d'authentification ou de comparaison des empreintes se réduit à une simple comparaison de minuties. Il est important de noter que nous avons établi une table comprenant le nom, prénom, id et les coordonnées des utilisateurs.

Dans la section d'authentification, il est utilisé un moteur de recherche pour rechercher une empreinte parmi les empreintes de la base de données.

L'API r2xml a été utilisée pour effectuer la recherche.

Résume :

Ainsi, nous avons apporté notre contribution dans le domaine de la biométrie en créant un système qui permet de rechercher une empreinte à partir des coordonnées des minuties extraites.

L'application que nous proposons est composée de trois grandes parties principales ainsi que d'autres fonctionnalités additionnelles :

1- L'analyse de l'empreinte consiste à procéder au traitement (binarisation, squelettisation) et à extraire les minuties de manière manuelle. Cela nous permet d'examiner attentivement la nature des bifurcations et des terminaisons.

2- Authentification automatique : Facilite le prétraitement et l'extraction des informations. Lorsque l'utilisateur ajoute une nouvelle image d'empreinte, la fenêtre d'application affichera automatiquement l'image squelettisée avec les informations sélectionnées à gauche et à droite, ainsi que l'image originale de l'empreinte, et les coordonnées des minuties seront affichées dans une TextArea.

3- Comparer les empreintes: Cette partie permet de faire la comparaison entre deux empreintes digitales.

Cette partie présente un mini moteur de recherche qui permet de rechercher le nom d'un utilisateur dans notre base de données.

Fig.2.9 montre les processus utilisés dans le système de reconnaissance des empreintes digitales

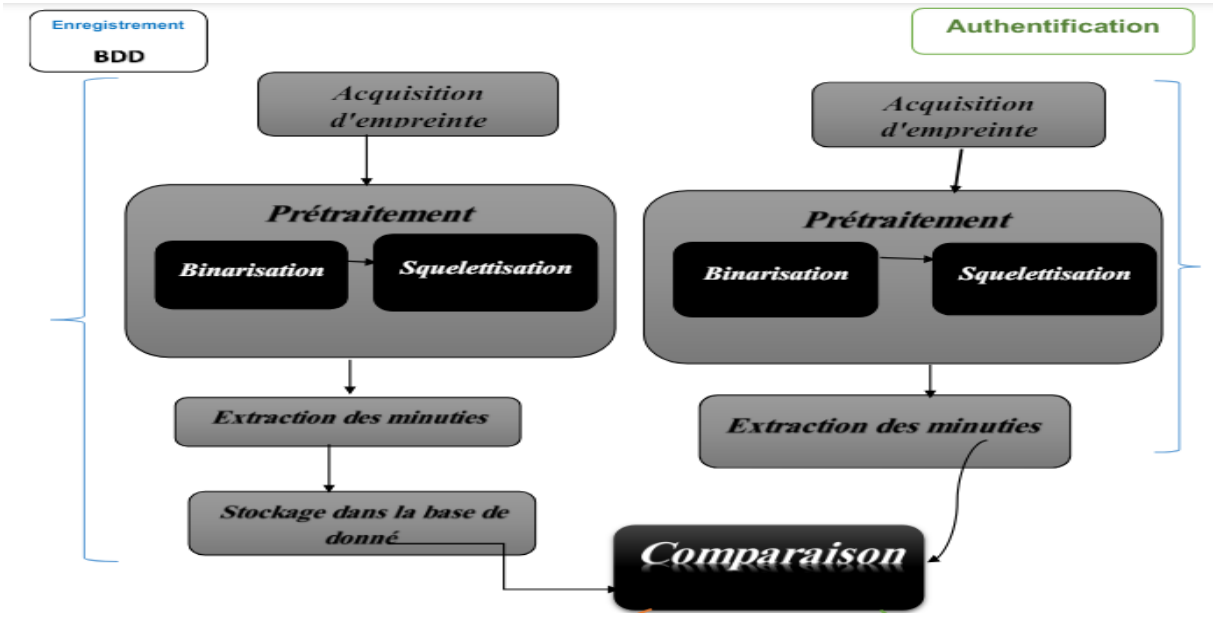


Fig.2.9. Processus suivis dans un system de la reconnaissance des empreintes.

5. Conclusion

Dans ce chapitre, nous avons examiné les différentes méthodes et algorithmes utilisés pour la reconnaissance des empreintes digitales, en commençant par les principes de base jusqu'à l'analyse détaillée des principaux algorithmes. Nous avons abordé les étapes du processus de reconnaissance des empreintes digitales, y compris la collecte de données, l'amélioration de la qualité des images, l'extraction des caractéristiques et la correspondance des empreintes digitales. Nous avons également mis en lumière les principaux défis de ce processus, tels que la variabilité de la qualité des images et les influences environnementales, ainsi que le besoin urgent de développer des algorithmes plus efficaces et précis.

L'analyse a montré que les algorithmes de reconnaissance des empreintes digitales ont réalisé des progrès significatifs grâce aux avancées dans les domaines de l'informatique et des technologies de l'information. Cependant, il reste des défis qui nécessitent davantage de recherche et de développement pour garantir la précision et l'efficacité de ces technologies dans diverses conditions et applications.

Chapitre 3:

Résultats et discussion

Chapitre 3:
Résultats et discussion

1. Introduction :

Grâce aux avancées technologiques, les méthodes de reconnaissance d'empreintes digitales ont gagné en popularité et en utilisation en raison de leurs multiples bénéfices. Ils garantissent une grande sécurité car ils sont authentiques, ce qui les rend difficiles à falsifier ou à dérober. De plus, ils sont pratiques et rapides, ce qui en fait une alternative privilégiée pour vérifier l'identité par rapport aux méthodes classiques comme les cartes d'entrée ou les mots de passe.

L'objectif de ce chapitre est de présenter un projet de création d'un système de contrôle d'accès par empreintes digitales, en intégrant la connectivité WiFi afin d'améliorer la souplesse et l'efficacité. Nous étudierons les différents aspects techniques du projet, allant des appareils utilisés et des connexions électriques à la programmation et à la connectivité, en passant par un site Web et une base de données pour suivre et gérer les empreintes digitales. Ce chapitre présentera une vue d'ensemble de la mise en place de ce système, en mettant l'accent sur la sécurité et les bénéfices opérationnels qu'il offre.

2. Synoptique du Projet :

La reconnaissance et la gestion d'accès par empreinte digitale représentent une avancée majeure dans le domaine de la sécurité et de l'identification. Ce projet vise à développer un système complet qui intègre plusieurs composants technologiques pour assurer une vérification et une authentification efficaces. En combinant des technologies matérielles et logicielles, ce système offre une solution robuste et sécurisée pour le contrôle d'accès.

2.1. Composants Principaux:

Dans la conception d'un système de reconnaissance et de gestion d'accès par empreinte digitale, plusieurs composants clés jouent un rôle crucial. Ces composants travaillent en synergie pour garantir que l'ensemble du système fonctionne de manière fluide et efficace. L'intégration de ces éléments, de l'émission des tokens à la communication entre le dispositif émetteur et le site web, est essentielle pour assurer une vérification et une authentification sécurisées.

Dans notre projet, nous avons utilisé les composants suivants :

Dispositif Émetteur: Utilisation d'une ESP32.

Module de Scanner: Utilisation d'un module d'empreinte digitale.

Site Web:Génération et gestion des tokens.Communication avec le dispositif émetteur.

2.2. Fonctionnement :

Génération du token:

Le site web génère un token unique.

Ce token est ensuite intégré dans le code du dispositif émetteur.

Fonctionnement du Dispositif Émetteur:

Lorsque le dispositif est allumé, il envoie une requête HTTP GET au site web pour déterminer son mode de fonctionnement.

Vérification par le site web:

Le site web vérifie l'existence du token dans la base de données.Selon le résultat de la vérification, le site envoie une réponse au dispositif émetteur en indiquant le mode .

Résumé des Étapes:

Génération du Token: Génération et intégration du token dans le code du dispositif émetteur.

Requête du dispositif émetteur: Envoi de la requête HTTP GET au site web.

Vérification du site web: Vérification du token et détermination du mode de fonctionnement.

Ce schéma synoptique décrit de manière claire et concise le fonctionnement du système de contrôle d'accès basé sur les empreintes digitales, assurant une communication fluide entre le dispositif émetteur, le site web et le module d'empreinte digitale.

Fig.3.1 représente Schéma Fonctionnel de notre projet.

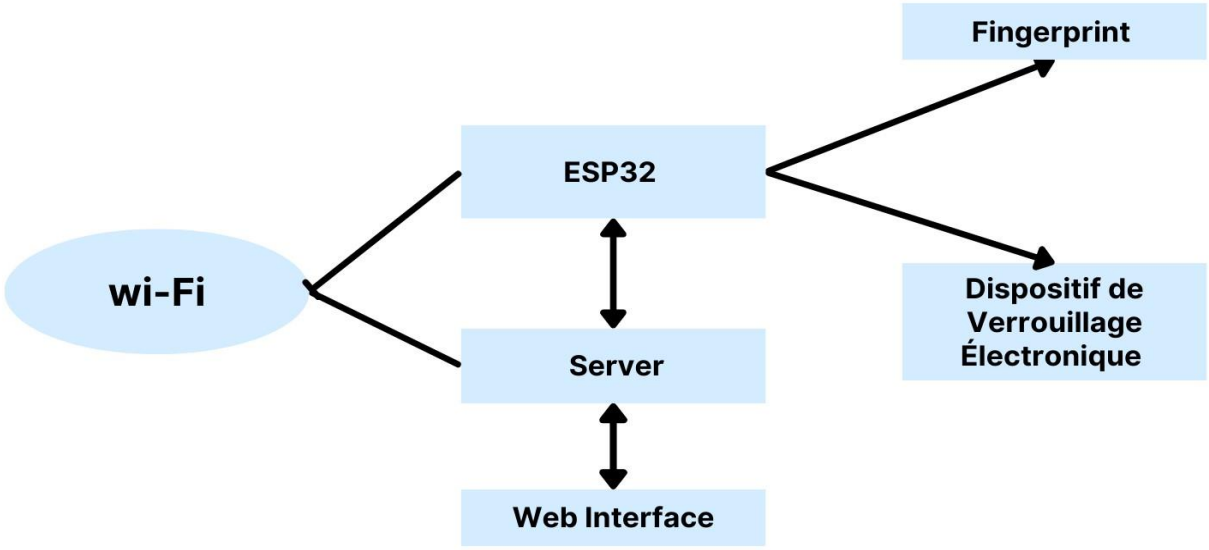


Fig.3.1. Schéma Fonctionnel de notre projet

3. Materiels utilisés :

Dans le développement de notre système de reconnaissance et de gestion d'accès par empreinte digitale, nous avons utilisé divers matériels technologiques pour garantir la performance et la fiabilité du système. Chaque composant matériel a été soigneusement sélectionné pour répondre aux exigences spécifiques du projet, offrant une intégration harmonieuse et une facilité d'utilisation.

3.1. Tableau de bord (ESP32) :

L'ESP32 est une petite carte électronique, appelée microcontrôleur, facile à prendre en main grâce à ses ressemblances avec la carte Arduino qui est bien plus répandue. . L'ESP32 peut avoir différentes tailles et la plus courante est montrée dans la Fig.3.2 :

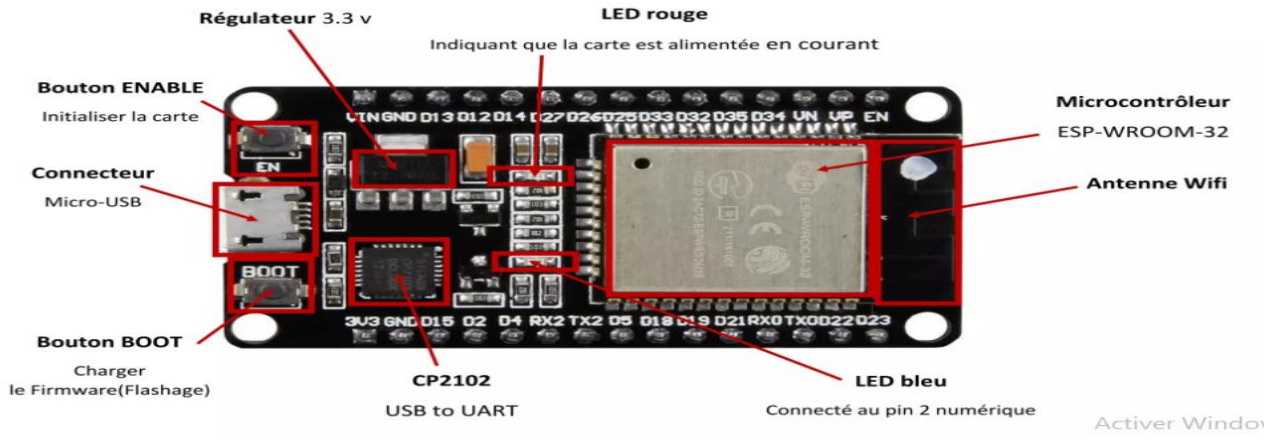


Fig.3.2. Microcontrôleur ESP32.

Comme mentionné précédemment, l'ESP32 est une carte électronique permettant de réaliser des projets «IoT» assez facilement. Elle possède en effet une connectivité assez complète, que nous détaillerons dans la partie suivante. L'ESP32 est assez simple à prendre en main car elle est cousine de la carte Arduino. Il est donc possible de l'utiliser comme la carte microcontrôleur italienne, en utilisant le même langage de programmation, les mêmes modules complémentaires et surtout le même logiciel de compilation (Arduino IDE). Pas de changement fondamental d'interface pour l'utilisateur, ce qui la rend d'autant plus simple à utiliser. Par ailleurs, on peut relever que sa taille miniature lui est un avantage considérable : elle mesure en effet moins de 3 cm par 5 cm, malgré les technologies qu'elle embarque! L'ESP32 est sans doute la carte microcontrôleur qui possède le meilleur compromis taille / connectivité / entrées sorties. Cela en fait un outil redoutable pour la miniaturisation des projets connectés Pour finir elle est aussi tout à fait adaptée à la réalisation de prototypes et non uniquement à la réalisation de projets «finis et définitifs». Elle est une référence dans l'univers maker pour ces nombreuses[19].

3.2. Le capteur d'empreintes digitales FPM10A

Le capteur d'empreintes digitales optique FPM10A simplifie la détection et la vérification des empreintes digitales. Équipé d'une puce DSP de nouvelle génération, il effectue rapidement des tâches complexes telles que le rendu d'image, la reconnaissance de formes et la compression d'image. Le capteur dispose d'une mémoire flash interne capable de stocker jusqu'à 300 empreintes digitales. Une LED rouge dans l'objectif s'allume pendant la détection des empreintes digitales, indiquant le fonctionnement[18].

Fig.3.3 représente le capteur d'empreintes digitales FPM10A

Fig.3.3. Le capteur d'empreintes digitales FPM10A.

Caractéristiques :

Le capteur d'empreintes digitales optique FPM10A a les spécifications suivantes :

Alimentation et Courant :

Tension d'alimentation : DC 3.6 ~ 6.0V / 3.3V

Courant de fonctionnement **:** <120mA

Courant de crête : <140mA

Performances :

Temps de capture d'image **:** <1,0 seconde

Taille de la fenêtre **:** 14 x 18 mm

Mode de correspondance **:** 1:1 (mode de correspondance)

Mode de recherche **:** 1: N (mode de recherche)

Taille du fichier de signature **:** 256 octets

Taille des fichiers de modèles **:** 512 octets

Capacité de stockage **:** 300 empreintes digitales

Niveaux de sécurité : Cinq niveaux (de faible à élevé : 1, 2, 3, 4, 5)

Taux de fausse acceptation (FAR) **:** <0,001 % (au niveau de sécurité 3)

Taux de faux rejet (FRR) **:** <1,0 % (au niveau de sécurité 3)

Temps de recherche **:** <1,0 seconde (pour 1:500, en moyenne)

Communication :

Interface PC **:** UART (niveau logique TTL) ou USB2.0 / USB1.1

Débit de communication (UART) **:** (9600 x N) bps où N = 1 ~ 12 (valeur par défaut N = 6, soit 57600bps)

Conditions Environnementales :

Environnement de travail :

Température : -20°C à +50°C

Humidité relative : 40% RH à 85% RH (sans condensation)

Environnement de stockage :

Température : -40°C à +85°C

Humidité relative : <85% RH (sans condensation)

Dimensions Physiques :

Dimensions du capteur d'empreintes digitales **:** 56 mm (L) x 20 mm (l) x 21,5 mm (H)

Ce capteur est robuste, efficace et polyvalent pour diverses applications de reconnaissance d'empreintes digitales, offrant des temps de traitement rapides et des performances fiables.

3.3. Min Serrure électromagnétique :

La serrure électromagnétique est un dispositif crucial dans notre système de gestion d'accès. Elle fonctionne grâce à un électroaimant qui contrôle l'ouverture et la fermeture de la porte. Lorsque l'ESP32 envoie un signal de validation après la reconnaissance de l'empreinte digitale, la serrure électromagnétique se déverrouille, permettant ainsi l'accès. Cette serrure offre une sécurité renforcée et une réponse rapide aux commandes, assurant une gestion efficace des accès.

Fig.3.4 représente un module de serrure électromagnétique

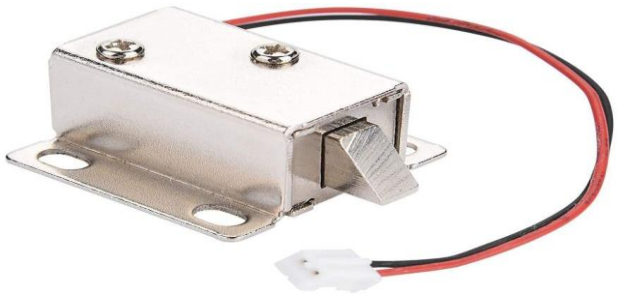


Fig.3.4. Serrure électromagnétique.

spécifications:

Alimentation et courant : 12V , 0,35A pour porte 6 V/12 V pour des projet arduino.

Produit taille: 3.3x2.7x1.7 cm/1.3x1.06x0.67in.

Poids du produit: 35g.

Catégorie de produit: 6 V/12 V universel.

Principe de fonctionnement

Puissance sur, la serrure rétracter, déverrouiller;

Hors tension, la serrure apparaît, ferme la serrure

Application principe

Déverrouiller: contrôle la tension ou hors tension

Serrure: pousser la porte, serrure automatiquement verrouillé.

3.4. Modules relais

Les relais se composent de trois broches normalement ouvertes, d'une broche normalement fermée, d'une broche commune et d'une bobine. Lorsque l'antenne**.** Le champ magnétique est généré par les contacts connectés les uns aux autres.

Fig.3.5 représente le fonctionnement du relais

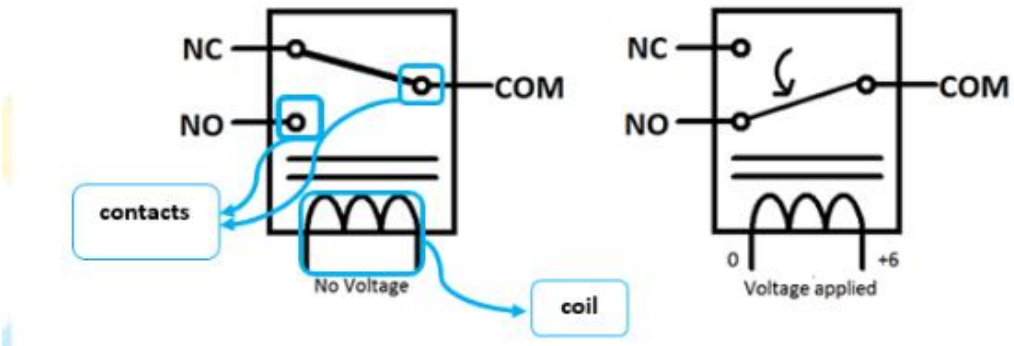


Fig.3.5. Fonctionnement du relais.

Caractéristiques des modules relais :

- Courant de contact 10A et 250V CA ou 30V CC.
- Chaque canal est équipé d'une LED d'indication.
- Tension de bobine 12 V par canal.
- Tension de fonctionnement du kit 5-12 V
- Signal d'entrée 3-5 V pour chaque canal.
- Trois broches normalement ouvertes et fermées pour chaque canal.

Fig.3.6 représente le module de relais 5v

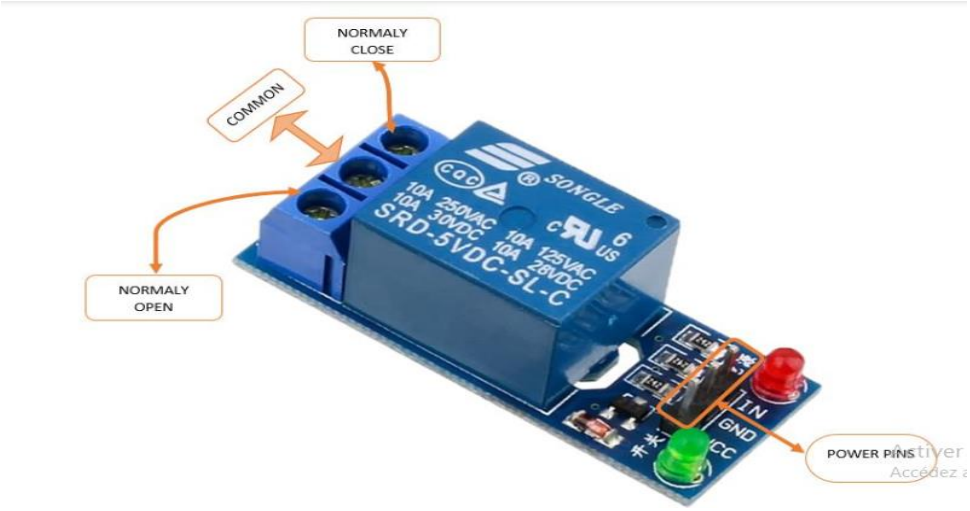


Fig.3.6. relais 5v.

4. Aperçu du système :

Un système de gestion d'accès par empreinte digitale repose sur une série d'étapes bien définies pour assurer la sécurité et l'efficacité du processus. Comprendre le flux de travail de ce système permet de mieux appréhender son fonctionnement global, depuis la création des jetons jusqu'à la vérification et la communication entre les différents composants.

4.1. Flux de travail :

Le flux de travail de notre système de reconnaissance et de gestion d'accès par empreinte digitale est conçu pour être simple et efficace. Chaque étape est orchestrée pour garantir une interaction fluide entre les composants matériels et logiciels, assurant ainsi une authentification sécurisée et rapide des utilisateurs.

4.1.1. Créer un code de site Web

Le site Web génère un token pour une utilisation ultérieure dans le code. Copiez ce token dans le token de l'émetteur.

4.1.2. Processus de transmission :

Lorsque l'émetteur est allumé, il envoie la demande HTTP GET au site Web pour examiner son état.

4.1.3. Vérification du site :

Le site Web vérifie l'existence du jeton dans la base de données.

Basé sur la vérification, le site Web envoie une réponse à l'expéditeur avec le mode (par exemple, le mode d'enregistrement).

4.2. Nouvel enregistrement des empreintes digitales :

Identification des empreintes digitales et renseignements sur l'appareil :

Emballez un 1 à 127 ID d'empreinte digitale avec l'appareil qui devrait stocker l'empreinte digitale.

Ces données seront envoyées à la base de données avec "Ajouter un doigt" activé.

Émetteur-récepteur en mode enregistrement :

L'émetteur, en mode d'enregistrement, enverra la demande HTTP GET pour l'ID qui doit être ajouté.

Le site web répond à l'ID associé à cet appareil.

Numérisation et stockage des empreintes digitales :

Le dispositif affiche un message de balayage et le module de scanner sera prêt à balayer le doigt.

Après avoir stocké l'empreinte digitale, l'appareil envoie une demande de confirmation au site.

Le site web explique que le nouvel ID a été ajouté avec succès.

5. Développement logiciel pour le système :

Le développement logiciel est une composante essentielle de notre système de reconnaissance et de gestion d'accès par empreinte digitale. Il englobe la programmation du microcontrôleur, la

gestion des communications réseau, ainsi que le traitement et la vérification des données biométriques. Le choix des langages de programmation et des environnements de développement, ainsi que l'utilisation de bibliothèques logicielles spécialisées, sont cruciaux pour assurer le bon fonctionnement et la sécurité du système.

5.1. Langage de programmation et environnement de développement :

Le logiciel pour ce système utilise le langage C++ dans l'environnement de développement Arduino IDE. Cet environnement est largement utilisé pour le développement de logiciels pour microcontrôleurs tels que l'ESP32, offrant des bibliothèques et des outils facilitant le processus de programmation et de développement.

5.2. Bibliothèques logicielles principales utilisées :

Pour développer un système de gestion d'accès par empreinte digitale efficace et fiable, il est nécessaire d'utiliser diverses bibliothèques logicielles. Ces bibliothèques fournissent les fonctionnalités essentielles pour la communication, la gestion des connexions et le traitement des données. La sélection des bibliothèques appropriées est cruciale pour assurer la performance et la sécurité du système.

5.2.1. Bibliothèque WiFi :

La bibliothèque **WiFi.h** est utilisée pour la connexion WiFi. Elle est essentielle pour connecter la carte de contrôle ESP32 au réseau local, puis à Internet. Cette bibliothèque fournit des fonctions pour configurer la connexion au réseau, vérifier l'état de la connexion et gérer la connexion en général.

```
#include <WiFi.h>

const char* ssid = "your_SSID";
const char* password = "your_PASSWORD";

void setup() {
Serial.begin(115200);
WiFi.begin(ssid, password);

while (WiFi.status() != WL_CONNECTED) {
delay(1000);
Serial.println("Connecting to WiFi...");
}
Serial.println("Connected to WiFi");
}
```

5.2.2. Bibliothèque Fingerprint :

La bibliothèque **Adafruit_Fingerprint.h** est utilisée pour interagir avec le capteur d'empreintes digitales. Cette bibliothèque fournit des fonctions pour capturer les empreintes, les analyser et les comparer avec les empreintes enregistrées dans le système.

```
#include <Adafruit_Fingerprint.h>

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

void setup() {
   Serial.begin(9600);
   finger.begin(57600);
   if (finger.verifyPassword()) {
      Serial.println("Found fingerprint sensor!");
   } else {
      Serial.println("Did not find fingerprint sensor :(");
   }
}
```

5.2.3. Bibliothèque OLED :

La bibliothèque **Adafruit_SSD1306.h** est utilisée pour contrôler l'écran OLED et afficher des informations telles que l'état du système, les messages d'erreur et l'état de la connexion WiFi. Cette bibliothèque fournit des fonctions pour dessiner du texte, des formes et des images sur l'écran OLED.

```
#include <Wire.h>
#include <Adafruit_GFX.h>
#include <Adafruit_SSD1306.h>

#define SCREEN_WIDTH 128
#define SCREEN_HEIGHT 64
Adafruit_SSD1306 display(SCREEN_WIDTH, SCREEN_HEIGHT, &Wire, -1);

void setup() {
  if (!display.begin(SSD1306_I2C_ADDRESS, OLED_RESET)) {
     Serial.println(F("SSD1306 allocation failed"));
     for (;;);
  }
  display.display();
  delay(2000);
  display.clearDisplay();
  display.setTextSize(1);
  display.setTextColor(SSD1306_WHITE);
  display.setCursor(0, 0);
```

```
    display.print("Hello, OLED!");
    display.display();
}
```

5.2.4. Bibliothèque http :

La bibliothèque **HTTPClient.h** est utilisée pour transférer des données via WiFi. Cette bibliothèque est utilisée pour envoyer des données à un serveur web et recevoir des réponses de celui-ci. Ceci est utile pour enregistrer les entrées et vérifier la validité des empreintes digitales en ligne.

```
#include <WiFi.h>
#include <HTTPClient.h>

void setup() {
  Serial.begin(115200);
  WiFi.begin(ssid, password);

  while (WiFi.status() != WL_CONNECTED) {
    delay(1000);
    Serial.println("Connecting to WiFi...");
  }
  Serial.println("Connected to WiFi");

  if (WiFi.status() == WL_CONNECTED) {
    HTTPClient http;
    http.begin("http://your_server/api/endpoint");
    int httpResponseCode = http.GET();

    if (httpResponseCode > 0) {
      String payload = http.getString();
      Serial.println(payload);
    } else {
      Serial.print("Error on HTTP request: ");
      Serial.println(httpResponseCode);
    }

    http.end();
  }
}
```

5.3. Intégration des composants logiciels :

Les bibliothèques sont intégrées dans le programme principal pour faire fonctionner le système de contrôle d'accès. Le code principal inclut les étapes suivantes :

Initialisation des composants : initialisation du WiFi, du capteur d'empreintes digitales et de l'écran.

Reconnaissance des empreintes : lecture de l'empreinte digitale depuis le capteur et vérification de sa validité.

Connexion au serveur : envoi des données d'empreinte digitale pour vérification en ligne.

Affichage des résultats : affichage de l'état de la vérification sur l'écran OLED et émission d'alertes sonores ou visuelles en fonction de l'état.

Toutes ces parties du code peuvent être intégrées dans un fichier unique dans l'IDE Arduino pour assurer le fonctionnement cohérent et fluide du système.

6. Description Détaillée du Code :

6.1. Définition des Broches et des Composants :

```
#define Finger_Rx 16 //Rx2
#define Finger_Tx 17 //Tx2
#define BUZZZER_PIN 27
#define MOTOR_PIN 26
#define RELAY_PIN 25
#define SCREEN_WIDTH 128
#define SCREEN_HEIGHT 64
#define OLED_RESET 0

Adafruit_SSD1306 display(SCREEN_WIDTH, SCREEN_HEIGHT, &Wire, OLED_RESET);
HardwareSerial mySerial(2);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
```

Les broches utilisées dans le projet sont définies, ainsi que l'écran OLED, et la bibliothèque d'empreintes digitales est initialisée pour gérer le scanner.

6.2. Configuration du WiFi :

```
const char *ssid = "realme C55";
const char *password = "b5gh6nah";
const char *device_token = "c8b98294";

void connectToWiFi() {
  WiFi.mode(WIFI_OFF);
  delay(1000);
  WiFi.mode(WIFI_STA);
  Serial.print("Connecting to ");
  Serial.println(ssid);
  WiFi.begin(ssid, password);
  ...
  if (WiFi.isConnected()) {
    Serial.println("Connected");
    display.clearDisplay();
    display.setTextSize(2);
    display.setTextColor(WHITE);
    display.setCursor(8, 0);
    display.print(F("Connected \n"));
    display.display();
  } else {
    Serial.println("Not Connected");
    WiFi.mode(WIFI_OFF);
```

```
      delay(1000);
    }
    delay(1000);
  }
```

Cette fonction tente de se connecter au réseau WiFi en utilisant les paramètres définis. Si la connexion est réussie, un message est affiché sur l'écran OLED.

6.2.1. Vérification de l'Empreinte Digitale :

```
void CheckFingerprint() {
  FingerID = getFingerprintID();
  DisplayFingerprintID();
}

int getFingerprintID() {
  uint8_t p = finger.getImage();
  if (p != FINGERPRINT_OK) return -1;
  p = finger.image2Tz();
  if (p != FINGERPRINT_OK) return -1;
  p = finger.fingerFastSearch();
  if (p == FINGERPRINT_OK) return finger.fingerID;
  return -1;
}

void DisplayFingerprintID() {
  if (FingerID > 0) {
    display.clearDisplay();
    display.drawBitmap(34, 0, FinPr_valid_bits, FinPr_valid_width, FinPr_valid_height,
WHITE);
    display.display();
    SendFingerprintID(FingerID);
  } else {
    display.clearDisplay();
    display.drawBitmap(32, 0, FinPr_invalid_bits, FinPr_invalid_width, FinPr_invalid_height,
WHITE);
    display.display();
  }
}
```

Ces fonctions sont responsables de la lecture et de la vérification de l'empreinte digitale, et d'afficher les résultats sur l'écran OLED. Si la vérification est réussie, l'ID de l'empreinte est envoyé au site web.

6.2.2. Envoi de l'ID de l'Empreinte Digitale au Site Web :

```
void SendFingerprintID(int finger) {
  if (WiFi.isConnected()) {
    HTTPClient http;
```

```
        String getData = "?FingerID=" + String(finger) + "&device_token=" + device_token;
        String Link = URL + getData;
        http.begin(Link);
        int httpCode = http.GET();
        String payload = http.getString();
        if (payload.substring(0, 5) == "login") {
          String user_name = payload.substring(5);
          display.clearDisplay();
          display.setTextSize(2);
          display.setTextColor(WHITE);
          display.setCursor(15, 0);
          display.print(F("Welcome"));
          display.setCursor(0, 20);
          display.print(user_name);
          digitalWrite(BUZZZER_PIN, HIGH);
          digitalWrite(RELAY_PIN, HIGH);
          delay(2000);
          digitalWrite(BUZZZER_PIN, LOW);
          digitalWrite(RELAY_PIN, LOW);
          display.display();
        } else if (payload.substring(0, 6) == "logout") {
          String user_name = payload.substring(6);
          display.clearDisplay();
          display.setTextSize(2);
          display.setTextColor(WHITE);
          display.setCursor(10, 0);
          display.print(F("Good Bye"));
          display.setCursor(0, 20);
          display.print(user_name);
          display.display();
        }
        delay(10);
        http.end();
      }
    }
```

Cette fonction envoie l'ID de l'empreinte digitale au site web et vérifie la réponse pour déterminer si le login ou le logout a été réussi.

6.3. Gestion des Empreintes via le Site Web :

6.3.1. Ajout d'une Nouvelle Empreinte :

```
void ChecktoAddID() {
  if (WiFi.isConnected()) {
    HTTPClient http;
    String getData = "?Get_Fingerid=get_id&device_token=" + String(device_token);
    String Link = URL + getData;
    http.begin(Link);
    int httpCode = http.GET();
    String payload = http.getString();
    if (payload.substring(0, 6) == "add-id") {
      id = payload.substring(6).toInt();
      http.end();
      getFingerprintEnroll();
```

```
        }
        http.end();
    }
}
```

Cette fonction vérifie s'il y a une nouvelle empreinte à ajouter via le site web, et si c'est le cas, appelle la fonction de l'inscription de l'empreinte.

6.3.2. Inscription d'une Nouvelle Empreinte :

```
uint8_t getFingerprintEnroll() {
    int p = -1;
    display.clearDisplay();
    display.drawBitmap(34, 0, FinPr_scan_bits, FinPr_scan_width, FinPr_scan_height, WHITE);
    display.display();
    while (p != FINGERPRINT_OK) {
        p = finger.getImage();
        ...
    }
    p = finger.image2Tz(1);
    if (p != FINGERPRINT_OK) return p;
    display.clearDisplay();
    display.setTextSize(2);
    display.setTextColor(WHITE);
    display.setCursor(0, 0);
    display.print(F("Remove"));
    display.setCursor(0, 20);
    display.print(F("finger"));
    display.display();
    delay(2000);
    p = 0;
    while (p != FINGERPRINT_NOFINGER) {
        p = finger.getImage();
    }
    p = -1;
    display.clearDisplay();
    display.drawBitmap(34, 0, FinPr_scan_bits, FinPr_scan_width, FinPr_scan_height, WHITE);
    display.display();
    while (p != FINGERPRINT_OK) {
        p = finger.getImage();
        ...
    }
    p = finger.image2Tz(2);
    if (p != FINGERPRINT_OK) return p;
    p = finger.createModel();
    if (p != FINGERPRINT_OK) return p;
    p = finger.storeModel(id);
    if (p == FINGERPRINT_OK) {
        confirmAdding(id);
    }
    return p;
}
```

Cette fonction gère l'inscription d'une nouvelle empreinte dans l'appareil, vérifie sa validité et la stocke sur le site web.

7. Conclusion :

En conclusion, ce chapitre détaille l'élaboration et la mise en œuvre d'un système de gestion des présences moderne et sécuritaire utilisant la technologie des empreintes digitales et la connectivité WiFi. Ce système représente une avancée significative par rapport aux méthodes traditionnelles, offrant une solution fiable, précise et conviviale pour les entreprises de toutes tailles. Les technologies et les processus décrits ici jettent les bases d'améliorations futures et d'une intégration plus complexe, ouvrant la voie à une gestion de présence plus sophistiquée et efficace.

Ce projet fournit une solution efficace pour gérer la présence à l'aide d'un scanner d'empreintes digitales, avec la possibilité de se connecter au WiFi pour transmettre et gérer à distance les données via un site Web et une base de données. Le système offre plusieurs fonctionnalités telles que l'enregistrement de nouvelles empreintes digitales et la suppression et la vérification des empreintes digitales, avec un rendu instantané des résultats sur l'écran OLED.

En outre, l'intégration de divers composants tels que l'écran OLED, la cloche et le moteur fournit une interaction intégrée et conviviale pour les utilisateurs. Exploiter de puissantes bibliothèques de programmation telles que Adafruit_Fingerprint, WiFi. h et HTTPClient. h garantit que le système est non seulement précis et fiable, mais aussi évolutif et l'optimisation future.

Conclusion Générale

Conclusion Générale

La conclusion de ce mémoire sur le contrôle d'accès basé sur les empreintes digitales et la connectivité WiFi récapitule les points clés abordés tout au long du projet et met en lumière l'importance et l'impact de la solution développée. Nous avons commencé ce mémoire par une exploration approfondie des technologies de contrôle d'accès et de la biométrie, en mettant l'accent sur la reconnaissance des empreintes digitales. Cette technologie, choisie pour sa précision et sa fiabilité, a été intégrée dans un système utilisant un microcontrôleur ESP32 pour bénéficier de la connectivité WiFi, permettant une gestion centralisée et à distance des accès.

Un prototype fonctionnel a été conçu, intégrant un capteur d'empreintes digitales, une interface utilisateur via un écran OLED, et des capacités de communication via WiFi. Ce système permet l'enregistrement, la vérification et la gestion des empreintes digitales de manière sécurisée et efficace. Le système a été testé dans divers scénarios pour vérifier sa robustesse, sa fiabilité et sa convivialité. Les résultats ont démontré une amélioration significative par rapport aux méthodes de contrôle d'accès traditionnelles, offrant une sécurité accrue et une facilité d'utilisation. Grâce à la connectivité WiFi, les données de contrôle d'accès peuvent être gérées à distance via un site web et une base de données centralisée. Cela permet une supervision en temps réel, une mise à jour facile des autorisations d'accès et une analyse des données de présence.

L’intégration de la biométrie dans les systèmes de contrôle d’accès est une avancée majeure pour la sécurité des environnements physiques et numériques. Le système développé dans cette mémoire offre une solution moderne, sûre et évolutive, adaptée aux besoins actuels des entreprises et des institutions. Les perspectives évolutives comprennent une interface utilisateur améliorée, des performances améliorées des capteurs d’empreintes digitales et l’intégration à d’autres systèmes de sécurité tels que la vidéosurveillance et les alarmes. Le système devrait voir des améliorations futures grâce à l’intégration de l’intelligence artificielle et des techniques d’apprentissage automatique, qui permettront de prédire les absences et d’analyser les modèles de comportement. En outre, l’amélioration de la sécurité des données et l’ajout de fonctionnalités de sauvegarde et de récupération amélioreront la fiabilité du système.

Ce mémoire a montré que l’utilisation des empreintes digitales pour contrôler l’accès, avec la connexion WiFi, est une solution efficace et moderne. Les contributions ont jeté les bases des développements futurs en matière de sécurité biométrique, offrant des opportunités d’innovation durable pour relever les défis croissants de sécurité d’un monde de plus en plus interdépendant.

Références bibliographiques

[1] https://science.howstuffworks.com/fingerprinting1.htm (accès le 03 01, 2024).

[2] https://www.nedapfrance.fr/post/qu-est-ce-que-le-contr%C3%B4le-d-acc%C3%A8s-est-pourquoi-est-ce-vital. Consulté le:23/05/2024

[3] BENAGGA Abderahmane, TELIB Lina. Reconnaissance des personnes basée sur l'empreinte de l'articulation de doigt. Mémoire Master Académique en electronique des systèmes embarqués. Université KasdiMerbah.Ouargla. Algérie. 01/06/2016.

[4] ELBOU, DIARRA Pierre Dit Prince Mohamed Ghaly Ould. Gestion intelligente et contrôle de l'accès aux salles de cours. Mémoire de master en électronique des systèmes embarqués. Université Abdelhamid Ibn Badis de Mostaganem., 2020.

[5] Achref, Berredjem. La reconnaissance des individus par leur empreinte des articulations des doigts. Mémoire de master en instrumentation .Université 8Mai 1945 – Guelma, Juillet 2019.

[6] Benchennane, Ibtissam. Étude et mise au point d'un procédé biométrique multimodal pour la reconnaissance des individus. Thèse de doctorat en électronique, option : communication, Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf, Alger, 2016.

[7] E. Boutellaa, M. Bengherabi, S. Ait-Aoudia, F. Harizi, "Système de vérification de signatures manuscrites en ligne à base des paramètres DCT". 10ème Colloque International sur le Traitement d'Images et la Vision Artificielle (CIPA 2007), pp. 215-220, 2007.

[8] OULED KADDOUR, Mohamed**.** La discrimination du genre à base de classifieurs SVM. Mémoire de Magister en informatique, Département de Post-Graduation, Ecole Nationale Supérieure d'Informatique, Alger, Algérie, 2015.

[9] Lajevardi, S. M., Arakala, A., Davis, S. A., & Horadam, K. J. (2013). Retina verification system based on biometric graph matching. *IEEE Transactions on Image Processing*, *22*(9), 3625-3635.

[10] [10] Suman Senapati, Goutam Saha. Speaker Identification by Joint Statistical Characterization in the Log-Gabor Wavelet Domain. International Journal of Intelligent Systems and Technologies., , Vol. 64, No. 2, pp. 173–189,2007.

[11] N. Bettayeb, & R. Bouzar. Conception d'un système biométrique FKP. Mémoire de fin d'études en vue de l'obtention du diplôme d'Ingénieur d'Etat en Electronique, École Nationale Polytechnique Algérie, Juin 2013.

[12] BEBIS G., DEACONU T., GEORGIOPOULOS M. "Fingerprint Identification Using Delaunay Triangulation." Proc. of Int. Conf. on Information Intelligence and Systems, pp. 452-459, Washington, DC, USA, 1999.

[13] Tisse, C.-L., Martin, L., Torres, L., & Robert, M. .Système automatique de reconnaissance d'empreintes digitales. Sécurisation de l'authentification sur carte à puce. https://core.ac.uk/download/pdf/15494538.pdf

[14] LOHOU, Christophe. "Contribution à l'analyse topologique des images : étude d'algorithmes de squelettisation pour images 2D et 3D, selon une approche topologie digitale ou topologie discrète." Informatique Fondamentale et Applications, 20 décembre 2001.

[15] Zhang-Suen, T.C. (1984). "Character Recognition Systems: A Guide for Students and Practitioners". Pattern Recognition and Image Processing Series.

[16] Danielle Azar, Pattern Recognition course: Hilditch's Algorithm for SkeletonizationmProf. Godfried Toussaint.1997

[17] Łukasz WIĘCŁAW . minutiae points, matching score, fingerprint matching Journal of medical informatics & technologies. Journal of medical informatics & technologies Vol. 13/2009, ISSN 1642-6037.

[18] **FPM10A**. (2024). https://alitools.io/fr/showcase/fpm10a-lecteur-d-empreintes-digitales-capteur-module-optique-d-empreintes-digitales-d-empreintes-digitales-module-pour-arduino-serrures-interface-de-communication-serie-32834946780.

[19] https://esp32.com/ Consulté le:2024/04/21.

[20] Jlassi, H., & Hamrouni, K. (2005, March 27-31). Caractérisation de la rétine en vue de l'élaboration d'une méthode biométrique d'identification de personnes. In *3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications* (SETIT), Tunis, Tunisia. École Nationale d'Ingénieurs

[21]K. Hrechak and J. A. McHugh, "Automated fingerprint recognition using structural matching,"PatternRecognit.,vol.23,pp.893–904,1990.

[22]http://sti.sn/-Controle-d-acces-Biometrique-12-Consultéle :22/05/2024

ملخص

في هذه الأطروحة، نقدم إنشاء وتنفيذ نظام التحكم في الوصول بناءً على التعرف على بصمات الأصابع، مدمج مع اتصال WiFi لمركزية إدارة البيانات. لتصميم نظام آمن وفعال وسهل الاستخدام، يستخدم المشروع جهاز تحكم دقيق ESP32 ومستشعر بصمات الأصابع وشاشة OLED. بفضل اتصال WiFi، من الممكن الاتصال في الوقت الفعلي بقاعدة بيانات عن بعد، مما يسهل التسجيل والتحقق وإدارة الوصول. تظهر النتائج تحسنًا واضحًا مقارنة بتقنيات التحكم في الوصول التقليدية، مما يوفر حلاً معاصرًا وموثوقًا به. تبحث هذه الورقة أيضًا في الفرص المستقبلية للتحسين، مثل تكامل الذكاء الاصطناعي والتعاون مع أنظمة الأمان الأخرى.

الكلمات المفتاحية: التحكم في الوصول، بصمات الأصابع، الأمن البيومتري، نظام الأمان، قاعدة البيانات، واجهة المستخدم.

Résumé

Dans ce mémoire, nous exposons la création et la mise en place d'un système de contrôle d'accès qui repose sur la reconnaissance des empreintes digitales, intégré à une connectivité WiFi afin de centraliser la gestion des données. Pour concevoir un système sécurisé, efficace et convivial, le projet utilise un microcontrôleur ESP32, un capteur d'empreintes digitales et un écran OLED. Grâce à la connexion WiFi, il est possible de communiquer en temps réel avec une base de données lointaine, ce qui facilite l'enregistrement, la vérification et la gestion des accès. Les résultats obtenus mettent en évidence une nette amélioration par rapport aux techniques classiques de contrôle d'accès, en proposant une solution contemporaine et fiable. Ce document examine aussi les possibilités d'amélioration à venir, comme l'intégration de l'intelligence artificielle et la collaboration avec d'autres systèmes de sécurité.

Mots clés : Contrôle d'accès, Empreintes digitales, Sécurité biométrique, Système de sécurité, Base de données, Interface utilisateur

Abstract

In this thesis, we present the creation and implementation of an access control system based on fingerprint recognition, integrated with WiFi connectivity to centralize data management. To design a secure, efficient and user-friendly system, the project uses an ESP32 microcontroller, a fingerprint sensor and an OLED screen. Thanks to the WiFi connection, it is possible to communicate in real time with a remote database, which facilitates registration, verification and access management. The results show a clear improvement compared to conventional access control techniques, offering a contemporary and reliable solution. This paper also looks at future opportunities for improvement, such as the integration of artificial intelligence and collaboration with other security systems.

Keywords: Access Control, Fingerprint, Biometric Security, Security System, Database, User Interface.