الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة غرداية
Université de Ghardaïa
كلية العلوم والتكنولوجيا
Faculté des Sciences et de la Technologie
قسم الآلية والكهروميكانيك
Département d'automatique et d'électromécanique

N° d'enregistrement

Mémoire de fin d'étude, en vue de l'obtention du diplôme

Master

Domaine : Sciences et Technologies
Filière : Automatique
Spécialité : Automatique et système

Thème

Conception et réalisation un système de pointage et de contrôle d'accès à base d'empreinte digitale

Présenté par :
REZZAG OMAR
BELABBASSI TAREK

Soutenue publiquement le 11/06/2022

Devant le jury composé de :

Prénom et nom	Grade	Université	Président
BEKKAR Belgacem	M.C.B	Université de Ghardaïa	Encadrant
MOSBAH Charaf Abdelkarim	M.C.B	Université de Ghardaïa	Examinateur
Arif Mohammed	M.A.A	Université de Ghardaïa	Examinateur

Année universitaire 2021/2022

Remerciements

Nous tenons à exprimer nos sincères remerciements à notre professeur M. Belgacem Bekkar pour nous avoir encadrés et guidés tout au long de notre projet et pour tous ces conseils judicieux qu'il nous a prodigués.

Aussi nous tenons à lui reconnaître ce temps précieux qu'il nous a consacré à nous aider.

Que les membres du jury trouvent ici nos très sincères remerciements pour avoir accepté d'examiner notre travail avec leur jugement, ainsi que pour le temps qu'ils consacrent pour nous donner leurs avis et corrections.

Enfin, merci à tous ceux qui contribué dans la réalisation de ce projet de près ou de loin: nos enseignants, nos chères familles et nous amis (es)

Dédicace

En signe de respect et de reconnaissance, je dédie ce travail :

- *Aux êtres les plus chers à mon coeur, mes parents pour leur soutien, Leur éducation ainsi que leur amour*
- *A mon cher grand frère Abbas qui m'a toujours soutenu*
- *A mes chères sœurs, en leurs souhaitant beaucoup de réussite*
- *A mes cousines et toute la famille de Belabbassi et Khedim*
- *A mes collègues de l'université de Ghardaïa et à*
- *Tous ceux qui m'ont enseigné au long de ma vie scolaire.*
- *A Tous ceux qui m'ont aidé pour accomplir ce mémoire*
- *A mon ami et collègue Omar que j'ai le plaisir de connaître et d'étudier avec lui depuis 12 ans.*

TAREK

I dedicate this modest work as a sign of respect and acknowledgment to:

- My parents, for their love, their encouragement, and their dedication to raise us as a loving family.
- My whole family, REZZAG and BENZAIT especially my brothers and sisters, all the love.
- My close friends whom I can't say all their names, I am privileged to say that the list is too long.
- my colleagues at the University of Ghardaia, and to all my teachers from primary school all the way to university, thank you.
- To my dear friend and colleague TAREK whom we've been friends for 12 years.

finally, to all who helped me complete this project.

OMAR

Résumé

Notre projet de fin d'étude but est de réaliser un système de pointage utilisent l'empreinte digitale à base de la carte ARDUINO de telle façon que l'empreinte digitale de chaque employé est prise par un capteur d'empreinte digitale et enregistrer l'arrivage et le départ de chaque employé, puis il enverra les données collectées à une base de données online.

MOTS CLES : Système de pointage, Empreinte digitale, Arduino, IoT.

Abstract

Our final year study project aim is to achieve a clocking system that uses the fingerprint based on the ARDUINO microcontroller, in such a way that the fingerprint of each employee is taken by a fingerprint sensor and record the arrival and departure of each employee, then it will send the collected data to an online database.

Keywords: Clocking system, Fingerprint scanner, Arduino, IoT.

ملخص

مشروع نهاية الدراسة الخاص بنا يهدف إلى إنشاء نظام تسجيل توقيت بقراءة البصمة المعتمد على المتحكم أردوينو، بحيث أن بصمة كل عامل تأخذ من طرف قارئ البصمة ويتم تسجيلها بالإضافة إلى تسجيل الحالة (دخول/خروج) ويتم إرسال البيانات إلى قاعدة بيانات على الأنترنت.

كلمات مفتاحية : نظام تأشير، قارئ البصمة الرقمي، أردوينو، إنترنت الأشياء.

Tableau de matière

Liste des figures

Liste des abréviations

CMOS: Complementary Metal-Oxide Semiconductor.

DPI: Dots Per Inch.

IDE: Integrated Development Environment.

IoT : Internet of Things.

LCD: Liquid Crystal Display.

RAM : Random-Access Memory.

RFID: Radio Frequency IDentification.

RTC: Real-Time Clock.

USB: Universal Serial Bus.

WI-FI : Wireless Fidelity.

Introduction générale

L’une des clés du succès des entreprises est la planification des employés, car les employés ont un impact financier à long terme énorme sur l’entreprise. L’organisation peut subir une perte de revenus inutile s'il n'y a pas de planification des employés de la bonne manière. Il faut donc être tout aussi prudent lors de la vérification de la présence d’employé. C’est la raison pour laquelle aujourd'hui de nombreuses organisations commerciales, quelle que soit la simplicité ou la complexité de leur main-d’œuvre, se tournent vers l’adoption d’un système de présence biométrique. Avec le système de pointage, les entreprises peuvent augmenter la sécurité et la précision du temps de leurs employés.

La raison principale d’utiliser ce système est ses données fiables, les données recueillies à partir d’un système de pointage sont en direct et honnêtes.

L’objectif principal de notre travail est de réaliser un système de pointage avec empreinte digitale ce qui contribue à déterminer avec précision les heures d’entrées et de sortie du lieu de travail de manière plus sécurisée. En utilise une carte Arduino avec capteur d’empreintes digitales et système WIFI pour envoyer le journal de présence vers une base de données sur Google scheet.

Pour réaliser ce système de pointage nous avons organisé notre travail en trois chapitres.

Chapitre 1 : (Biométrie et Les Empreintes Digitales) ce chapitre donne une idée générale sur les biométrie et leurs types et technologies, aussi les mécanismes de reconnaissance des empreintes digitales et comment fait l’acquisition de l’empreinte.

Chapitre 2: (Système de pointage) dans ce chapitre, nous avons mentionné les différents systèmes de pointage surtout les pointeuses biométriques et leur type qu’il existe.

Chapitre 3: (Conception et réalisation) ce chapitre est la partie pratique de notre mémoire qui présente le schéma synoptique du système, circuit de projet et la conception (matérielle et logicielle) les touts à base d’une carte Arduino et un capteur d’empreintes digitales.

Chapitre 1 : Biométrie et les empreintes digitales

1.1. Introduction

Les caractéristiques comportementales et physiologiques sont régulièrement utilisées pour vérifier ou déterminer manuellement l'identité – c'est quelque chose qui les humains font tous les jours lorsque nous saluons des amis ou vérifions une carte d'identité. Les technologies biométriques, en revanche, sont des ordinateurs automatisés ou des machines sont utilisées pour vérifier ou déterminer l'identité par le comportement ou les caractéristiques physiologique.

Parce que le processus est automatisé, l'authentification biométrique ne nécessite généralement que quelques secondes, et les systèmes biométriques sont capables de comparer des milliers d'enregistrements par seconde.

1.2. Qu'est-ce que la biométrie ?

Le terme biométrie vient du grec ancien **bios** = « vie » et **metron** = « mesure ». La biométrie fait référence à toute la classe de technologies et de techniques permettant d'identifier l'être humain de manière unique [1]. Bien que la technologie biométrique ait diverses utilisations, son objectif principal est de fournir une alternative plus sûre aux systèmes de contrôle d'accès traditionnels utilisés pour protéger les biens personnels ou d'entreprise.

1.3. Pourquoi la biométrie ?

Bon nombre des problèmes que la biométrie aide à résoudre sont les faiblesses des systèmes de contrôle d'accès actuels, par exemple :

- **Les faibles mots de passe :**

Les utilisateurs d'ordinateur en particulière tendre a utilisé des mots de passes facile à deviner, conséquemment résultant au piratage. Cela pourrait conduire à une faille de sécurité où des secrets personnels ou commerciaux sont volés par un étranger.

- **Le partage des identifiants :**

Dans les petites et les grandes organisations, nous entendons souvent parler de cas comme celui-ci : Un utilisateur d'ordinateur partage son mot de passe avec un collègue qui a besoin d'un accès — même si, dans la plupart des organisations et dans de nombreuses lois et réglementations liées à la sécurité, ceci est interdit par la politique.

- **Cartes-clés perdues**

De nombreuses organisations et entreprises utilisent des cartes-clés pour accorder l'accès à leurs employés et de nombreuses études montrent qu'au moins une fois dans leur vie, les employés ont tendance à perdre leurs cartes et ils peuvent également corriger le nom de l'organisation ou l'adresse de son emplacement, ce qui conduit à d'éventuelles effractions faciles. Il y a aussi un autre problème dans lequel les cartes-clés peuvent être clonées facilement en utilisant des moyens très bon marché de le faire.

La biométrie peut résoudre tous ces problèmes en exigeant un identifiant supplémentaire (quelque chose associé au propre corps de la personne) avant d'accorder l'accès à un bâtiment, une salle informatique ou un système informatique. Un système de contrôle d'accès qui utilise la biométrie comprendra un appareil électronique qui mesure un aspect spécifique du corps ou du comportement d'une personne qui identifie positivement cette personne. L'appareil peut être un lecteur d'empreintes digitales, un appareil photo numérique pour bien voir une iris ou une tablette de signature [1].

La technologie biométrique en tant que moyen de protection les atouts existe depuis un certain temps dans certains domaines. Les organisations militaires, de renseignement et d'application de la loi utilisent la biométrie pour améliorer les contrôles d'accès physiques et logiques depuis des décennies.

Mais au cours des dernières années, il y a eu une augmentation de l'utilisation de la biométrie pour protéger les atouts de grande valeur. Les centres de données Internet utilisent souvent la biométrie pour admettre du personnel à l'étage du centre de données. Les appareils biométriques d'empreintes digitales apparaissent partout - même intégrés dans les ordinateurs portables, les PDA et les clés USB. La reconnaissance faciale est disponible sur quelques modèles d'ordinateurs portables. Et pour protéger les entreprises et surveiller les employés, des ensembles de serrures biométriques à empreintes digitales sont disponibles.

1.4. Systèmes biométriques

Les systèmes biométriques peuvent être conçus en deux classes : physiologiques et comportementales.

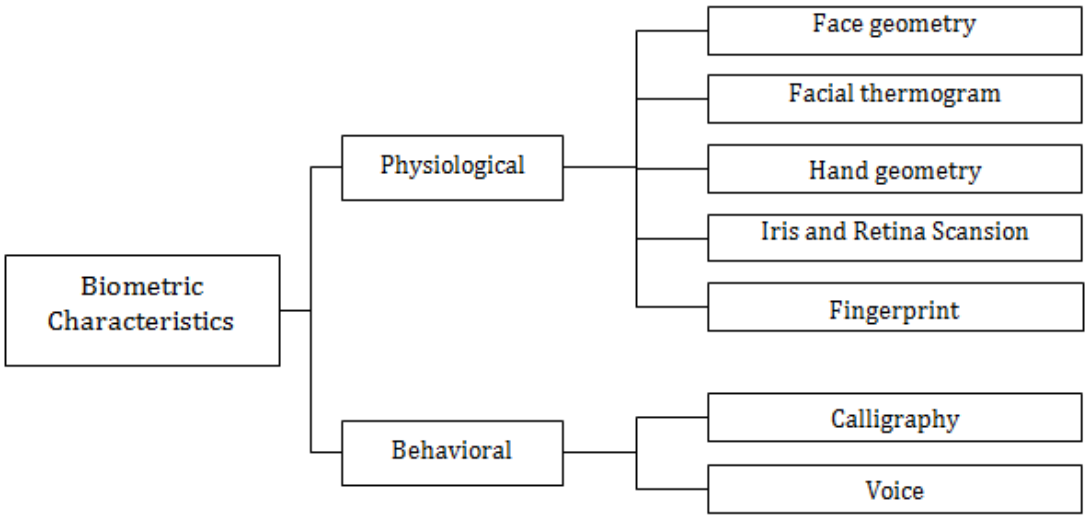


Figure 1-1 : les caractéristiques biométriques

1.4.1. Les systèmes biométriques physiologique :

La biométrie physiologique mesure une partie spécifique de la structure ou de la forme d'une partie du corps d'un sujet. Les types les plus courants de biométrie physiologique sont :

- **La forme de visage (Facial recognition) :**

La reconnaissance faciale est une catégorie de logiciels biométriques. Il s'agit d'une mode d'apprentissage automatique, fondée sur l'apprentissage de modèles de données. Ils cartographient mathématiquement les caractéristiques du visage d'un individu. Puis, ils stockent ces données, sous forme d'empreinte faciale. Un logiciel de reconnaissance faciale utilise des algorithmes de type l'apprentissage en profondeur (*deep Learning*).

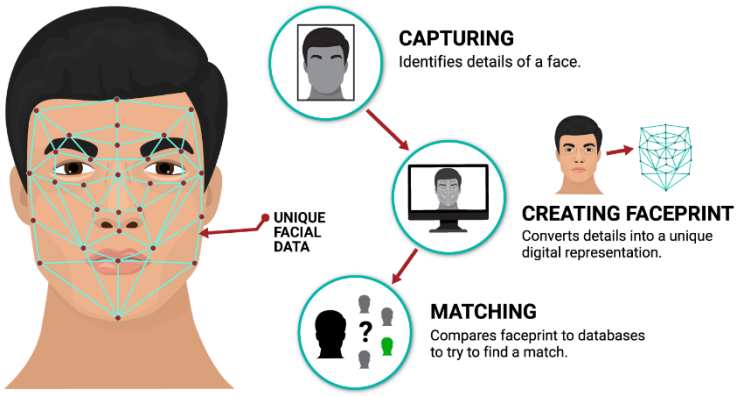


Figure 1-2 : reconnaissance faciale biométrique [2]

À cause de cet apprentissage profond, le logiciel est capable d'analyser une image, capturée en direct ou stockée numériquement, à celle de l'empreinte faciale enregistrée. Ainsi, il est capable de vérifier l'identité d'une personne. Les caméras de haute qualité des appareils mobiles ont fait de la reconnaissance faciale une option viable pour l'authentification des personnes [2].

- **Reconnaissance de l'iris (Iris recognition) :**

L'iris humain est un mince diaphragme circulaire qui se situe entre la cornée et le cristallin de l'œil humain. L'iris est perforée près de son centre par une ouverture circulaire appelée pupille. La fonction de l'iris est de contrôler la quantité de lumière entrant par la pupille, et cela est fait par le sphincter et les muscles dilatateurs, qui ajustent la taille de la pupille. Le diamètre moyen de l'iris est de 12 mm et la taille de la pupille peut varier de 10 à 80 % du diamètre de l'iris. L'iris se compose d'un certain nombre de couches, la plus basse de la couche épithéliale, qui contient des cellules pigmentées denses. La couche stromale se situe au-dessus de la couche épithéliale et contient des vaisseaux sanguins, des cellules pigmentaires et les deux muscles de l'iris. La densité de la segmentation stromale détermine la couleur de l'iris. La surface visible de l'extérieur de l'iris multicouche contient deux zones de couleurs différentes. Une zone externe est appelée la zone sclérotique et la zone interne est la zone pupillaire. Ces deux zones sont séparées par une iris constituée de la collerette, qui apparaît selon un motif aléatoire [2].

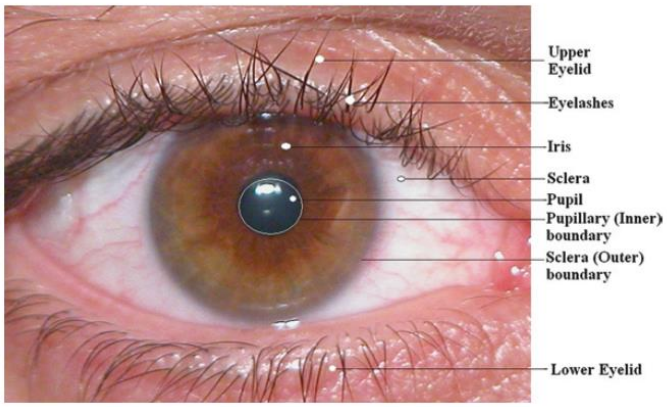


Figure 1-3 : caractéristiques de l'iris [3]

L'iris est l'anneau de tissus colorés entre la sclérotique blanche et la pupille sombre d'un œil. La lumière pénètre à l'intérieur de l'œil pour atteindre la rétine par la pupille. La taille de l'iris varie pour ajuster la quantité de lumière entrant dans la pupille. L'iris a généralement un riche motif de sillons, de crêtes et de taches pigmentaires. La couleur de l'iris peut changer à mesure que la quantité de pigment dans l'iris augmente pendant l'enfance. On pense que les moindres détails de la texture de l'iris sont aléatoires, uniques et très stables tout au long de la vie d'une personne.

- **Reconnaissance de la veine palmaire (Palm-Vein recognition)**

Le balayage des veines de la paume est une biométrie qui utilise la lumière infrarouge pour cartographier la structure veineuse unique de la paume, capturant plus de 5 millions de points de données. Le scanner de la veine de la paume convertit ensuite ces points de données en un code crypté unique qui devient identifiant biométrique.

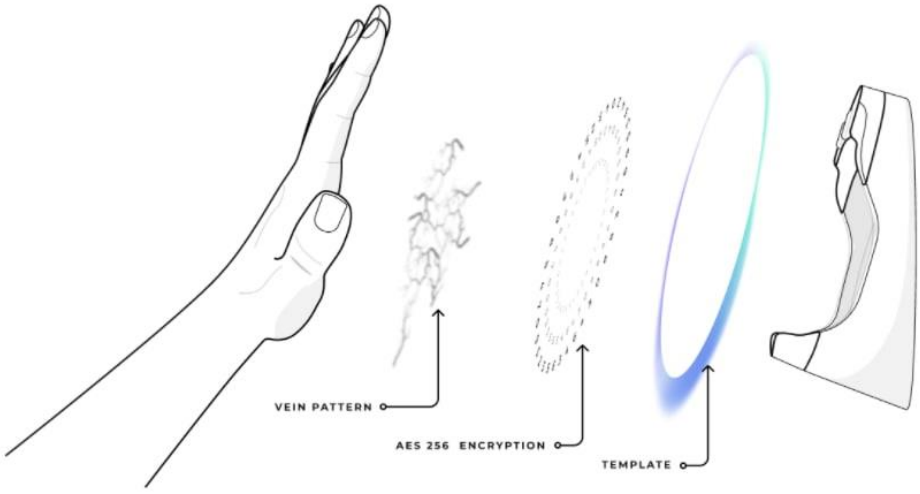


Figure 1-4 : Reconnaissance Palm-Vein [4]

Il existe une caractéristique clé qui distingue la reconnaissance des veines de la paume des autres données biométriques. Contrairement à l'empreinte digitale, à l'iris ou à la visage, le motif de la veine de la paume est interne [4].

Parce que le motif de veine de paume est caché à l'intérieur de la main, il n'est pas exposé comme les autres données biométriques. Cela lui confère plusieurs avantages uniques qui en font sans doute la biométrie la plus avancée du marché.

1.4.2. Systèmes biométriques comportementaux

La biométrie comportementale est le domaine d'étude lié à la mesure de modèles d'identification uniques et mesurables dans les activités humaines. Le terme contraste avec la biométrie physiologique, qui implique des caractéristiques humaines innées telles que les empreintes digitales ou les motifs de l'iris. Les exemples le plus courant sont :

- **La reconnaissance vocale (Voice recognition) :**

La biométrie vocale est un domaine scientifique et technologique lié à la reconnaissance vocale qui vise à développer des applications permettant de vérifier l'identité d'une personne uniquement par sa voix.

En fait, le son contrôle le grattage, et l'ensemble des caractéristiques vocales (timbre, hauteur, valence, etc.) propres à chaque être humain. Pour former une véritable empreinte vocale, ces caractéristiques sont sélectionnées pour être appariées à un modèle de référence, et ainsi servir d'identification [5].

Cependant, plusieurs éléments doivent être pris en compte, tout d'abord, le son possède une centaine de propriétés spécifiques qui, selon la qualité de la captation sonore et du traitement de l'information, font de ce médium un puissant moyen d'identification.

- **Analyse des signatures (Signature analysis) :**

L'analyse de signature est l'examen des signatures humaines afin de détecter les contrefaçons. L'analyse d'une signature humaine implique l'utilisation d'un logiciel spécialisé pour évaluer non seulement les contours mais les mouvements initialement effectués pour créer une signature. Les signatures falsifiées ont tendance à être produites plus lentement que les signatures authentiques. Même si l'auteur accélère le processus de falsification, il est impossible de dupliquer la fonction de mouvement en fonction du temps qui aurait lieu dans une signature authentique. Le logiciel peut également comparer plusieurs signatures. En raison des variations trouvées dans les multiples signatures d'une même personne, toute signature capturée électroniquement ne peut être utilisée

qu'une seule fois. Deux signatures identiques suggèrent qu'au moins l'une d'elles représente une tentative de fraude.

- **Reconnaissance de frappe (Keystroke recognition)**

La reconnaissance de frappe a été définie à la fois par l'industrie et les académiques comme le processus de mesure et d'évaluation d'un rythme de frappe sur des appareils numériques, y compris sur des claviers d'ordinateur, des téléphones portables et des écrans tactiles. Une mesure de frappe notée, la reconnaissance de frappe, souvent appelée « dynamique de frappe », fait référence aux informations de synchronisation détaillées qui décrivent exactement quand chaque touche a été enfoncée sur un appareil numérique et quand elle a été relâchée lorsqu'une personne tape.

La dynamique de frappe utilise un modèle biométrique unique pour identifier les individus en fonction du modèle de frappe, du rythme et de la vitesse. Les mesures brutes utilisées pour la dynamique de frappe sont appelées «*dwell time*» et «*flight time*». Le temps de pause est la durée pendant laquelle une touche est enfoncée, tandis que le temps de vol est la durée entre les frappes. La dynamique de frappe peut donc être décrite comme un algorithme logiciel qui mesure à la fois le temps de séjour et le temps de vol pour authentifier l'identité.

1.5. Empreintes digitales

1.5.1. Historique

Les empreintes digitales humaines ont été découvertes sur un grand nombre d'artefacts archéologiques et d'objets historiques. Bien que ces découvertes prouvent que les peuples anciens étaient conscients de l'individualité des empreintes digitales. Ce n'est qu'à la fin du XVIe siècle que la technique scientifique moderne des empreintes digitales a été lancée pour la première fois.

En 1864, le morphologue anglais des plantes, Nehemiah Grew, a publié le premier article scientifique rapportant son étude systématique sur la crête, le sillon et la structure des pores dans les empreintes.

Une avancée importante dans la reconnaissance des empreintes digitales a été réalisée en 1899 par Edward Henry, qui a établi le « système Henry » bien connu de classification des empreintes (Lee et Gaensslen, 2001). Au début du XXe siècle, la formation des empreintes digitales était bien comprise. Les principes biologiques des empreintes (Moenssens, 1971) sont résumés ci-dessous :

1. Les crêtes et les sillons épidermiques individuels ont des caractéristiques différentes pour différentes empreintes.

2. Les types de configuration sont variables individuellement, mais ils varient dans des limites qui permettent une classification systématique.
3. Les configurations et les moindres détails des crêtes et des sillons individuels sont permanents et immuables.

Au début du XXe siècle, la reconnaissance des empreintes a été officiellement acceptée comme méthode d'identification personnelle valide et est devenue une routine standard en médecine légale. Des agences d'identification des empreintes digitales ont été créées dans le monde entier et des bases de données criminelles sur les empreintes ont été créées. Diverses techniques de reconnaissance d'empreintes, y compris l'acquisition d'empreintes latentes, la classification d'empreintes et la comparaison d'empreintes ont été développées. Par exemple, la division d'identification des empreintes du FBI a été créée en 1924 avec une base de données de 810 000 cartes d'empreintes digitales [6].

La technologie de reconnaissance automatique des empreintes digitales s'est rapidement développée au-delà des applications médico-légales pour devenir des applications civiles et commerciales. En fait, les systèmes biométriques basés sur les empreintes digitales sont si populaires qu'ils sont presque devenus synonymes de systèmes biométriques.

1.5.2. Caractéristique de l'empreinte digitale

Une empreinte digitale est une marque laissée par les bords des doigts, des mains et des orteils.

Figure 1-5 : Caractéristique de l'empreinte [6]

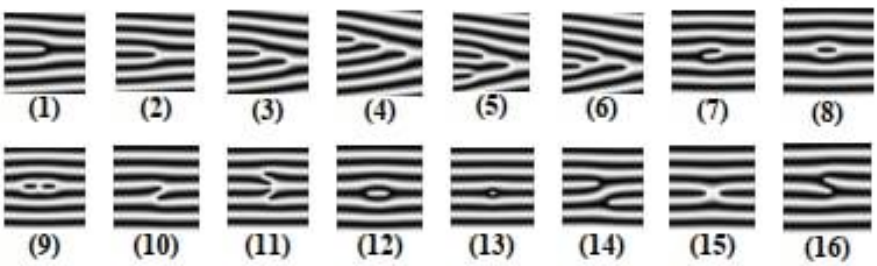
Les empreintes digitales sont regroupées en trois grandes catégories qui représentent à elles seules 95 % des doigts humains : arc, spirale et anneau. Au sein de chacune de ces catégories, il existe un très grand nombre d'empreintes digitales, qui sont les éléments qui nous distinguent les uns des autres. Aux cicatrices s'ajoutent des épines, des îlots et des indentations qui donnent un caractère unique aux empreintes latentes.

Figure 1-6 : Les trois grandes categories

- **Les boucles** constituent les motifs les plus vulgaris qui représentent 60% des doigts humains : dans ce type d'empreinte se replient sur elles même soit vers la droite, soit vers la gauche.
- **Les spires** qui correspondent à 30% des doigts humains : cette empreinte, comprend des lignes qui viennent s'enrouler autour d'un point, formant un genre de tourbillon.
- **Les arches** qui inclurent seulement 5% des doigts humains : cette empreinte contient des lignes disposées les unes au-dessus des autres.

Chaque empreinte possède un ensemble de points singuliers globaux (les centres et les deltas) et points singuliers Locaux (les minuties). Les centres correspondent à des lieux de convergences des stries tandis que les deltas correspondent à des lieux de divergence.

Il existe seize types de minuties différentes mais en général les algorithmes ne s'intéressent qu'aux bifurcations et terminaisons qui permettent d'obtenir les autres types par combinaison.



1.	terminaison	9.	boucle double
2.	bifurcation simple	10.	pont simple
3.	bifurcation double	11.	pont jumeau
4.	bifurcation triple I	12.	intervalle
5.	bifurcation triple II	13.	point isolé
6.	bifurcation triple III	14.	traversée
7.	crochet	15.	croisement
8.	boucle simple	16.	tête bêche

Figure 1-7 : Types des minuties [6]

1.5.3. Mécanisme de reconnaissance d'empreinte digitale

- **Principe générale :**

Un système de reconnaissance d'empreintes digitales entièrement automatique est une série d'opérations qui génèrent un résultat de sortie à partir de la saisie du doigt d'un utilisateur, permettant à l'utilisateur d'accéder ou non aux éléments nécessitant une sécurité. De nombreuses études ont été consacrées au développement d'un tel système, et de nombreuses approches de traitement différentes ont été présentées. Ces systèmes réagissent cependant toujours à la même structure.

La première phase permet l'acquisition d'une image de l'empreinte digitale de l'utilisateur (acquisition), qui sera ensuite prétraitée pour extraire les informations utiles de l'image (signature), éventuellement suivie d'un traitement complémentaire pour supprimer toute fausse information qui aurait pu se glisser dans la fissure dans la chaîne de traitement. Ensuite si l'utilisation du système consiste juste à créer une base de données (stockage) la signature est éventuellement compressée puis stockée dans la base de données au moyen d'une technique d'archivage (classification).

Pour un système d'identification, toutes les empreintes digitales de la base de données pouvant correspondre à celle de l'utilisateur (même modèle) sont désarchivées et comparées (appariement) une à une avec celle de l'utilisateur ; si une correspondance probable est trouvée, le système renvoie des informations personnelles sur l'utilisateur. Il n'y a qu'une seule comparaison dans un système de vérification, et un résultat binaire est renvoyé, permettant à l'utilisateur de l'accepter ou de le rejeter. [7].

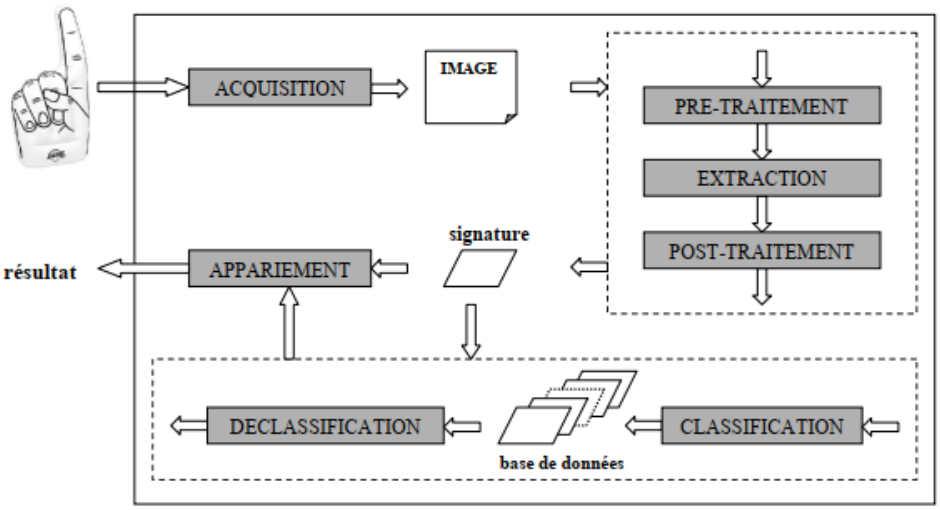


Figure 1-8 : Mécanisme de reconnaissance d'empreinte digitale

- **L'acquisition de l'empreinte**

L'acquisition des empreintes digitales se fait à l'aide de scanners d'empreintes digitales.

La structure générale d'un scanner d'empreintes digitales typique est la suivante : un capteur lit le motif de crête sur la surface du doigt et convertit la lecture analogique sous forme numérique via un convertisseur A/N (analogique à numérique) ; un module d'interface est chargé de communiquer (envoyer des images, recevoir des commandes, etc.) avec des périphériques externes (par exemple, un ordinateur personnel). Les différentes technologies sur lesquelles reposent les capteurs (par exemple, optique, à semi-conducteurs, à ultrasons, etc.). Souvent la sortie du capteur est déjà un signal numérique et donc aucune conversion A/N séparée n'est nécessaire ; certains scanners d'empreintes digitales peuvent ne pas avoir de convertisseur A/N intégré et une carte d'acquisition externe serait nécessaire pour transformer leur signal de sortie analogique. De plus, certains dispositifs intégrés System-on-a-Chip ont été et/ou correspondent aux données d'empreintes digitales. La conception de systèmes biométriques sécurisés basés sur les empreintes digitales nécessite la mise en œuvre de mécanismes de protection/cryptage dans les scanners biométriques [7].

Les scanners existants peuvent être classés dans l'une des catégories suivantes :

- Multi-doigts : plusieurs doigts peuvent être acquis simultanément. Habituellement, les quatre doigts d'une main (tous sauf le pouce) peuvent être acquis en même temps de sorte que trois coups ou placements de doigts suffisent pour acquérir les 10 doigts.
- Un seul doigt : un seul doigt à la fois peut être acquis ; ce type de scanner est le plus largement utilisé dans les applications commerciales et personnelles en raison de sa petite taille, de son faible coût et de sa simplicité d'utilisation.

- **Le traitement de l'image et l'extraction de la signature**

L'objectif est de développer un système capable de faire la distinction entre une image d'entrée et de nombreuses images stockées dans une base de données. Ceci nécessite l'emploi d'une méthode rapide et précise, c'est pourquoi nous abandonnerons la méthode de comparaison pixel par pixel car elle est peu efficace. La comparaison d'empreintes digitales est basée sur la détermination de la différence entre les détails de l'image d'entrée et ceux de la base de données.

La méthode généralement utilisée pour détecter les minuties consiste à mettre l’image de l’empreinte en noir et blanc, c’est la numérisation binaire de l’image, et à donner une même taille aux lignes de l’empreinte. Une fois que l’on dispose de l’image binaire, les minuties (singularités) sont mieux visibles, on procède alors à leur détection [7].

a) Prétraitement des images d'empreinte :

L'objectif initial est de binariser l'image de l'empreinte digitale, qui est le processus de conversion d'une image à plusieurs niveaux en une image en noir et blanc (seulement deux niveaux). La binarisation des empreintes digitales est une technique permettant de créer une image 1 bit avec des pics teintés en noir et des vallées ombrées en blanc.

Figure 1-9 : Binarisation de l'image

Pour arriver à une image binarisée correctement il faut bien choisie une méthode de binarisation qui nous donne la forme d'empreinte sans malformation.

Le principal paramètre caractérisant l'acquisition d'une image d''empreinte numérique est le nombre de points ou pixels par pouce (dpi), la diminution de la résolution entraîne une plus grande difficulté à résoudre.

Les crêtes des vallées et les points de minuties isolants. Une résolution de 250 à 300 dpi est probablement la résolution minimale qui permet aux algorithmes d'extraction d'empreintes digitales de localiser les détails dans les motifs d'empreintes digitales.

Enfin, les scanners 1 000 dpi ont commencé à remplacer les modèles 500 dpi dans les applications médico-légales où l'analyse de petits détails tels que les points, les crêtes naissantes, etc. est très importante pour faire correspondre de petites portions d'image d'empreinte digitale bruyante.

La figure suivante montre la même portion d'empreinte digitale acquise à 1 000 dpi et sous-échantillonnée à 500 dpi.

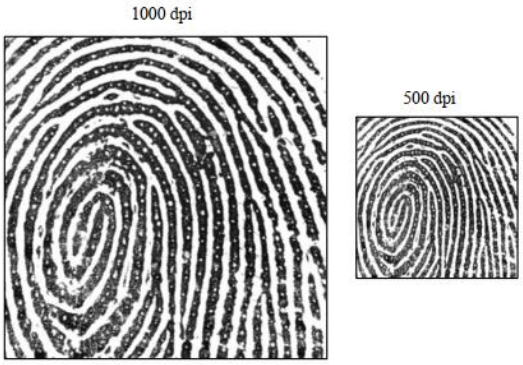


Figure 1-10 : Image acquise à 1000 dpi et sous-échantillonnée à 500 dpi.

- **Stockage de l'empreinte :**

Si la signature d'entrée doit être vérifiée avec toutes les signatures de la base de données, le processus d'identification peut prendre beaucoup de temps dans les systèmes avec de grandes bases de données. Afin de minimiser les temps de recherche, un processus de classification et de déclassification est nécessaire.

Lorsqu' une image est stockée, un groupe spécifique lui est attribué en fonction de ses caractéristiques. Lors de l'identification on désarchive l'ensemble des signatures de la base correspondant au groupe de l'empreinte nécessitant l'identification. Puis chacune des images désarchivées est comparée avec celle de l'utilisateur. Ceci permet de réduire sensiblement les temps de recherche en limitant le nombre d'images à comparer, à condition que les différentes catégories soient judicieusement choisies. Parmi les différentes techniques existantes on distingue principalement l'approche syntaxique (l'image est décrite au moyen de règles et de symboles et une analyse grammaticale permet de lui associer une classe), l'extraction des singularités de l'image (la position des centre et delta permet de déterminer la classe de l'empreinte) et l'utilisation des réseaux de neurones.

La phase d'appariement est l'étape critique du système, elle reçoit en entrée deux signatures issues de deux acquisitions différentes d'empreinte et renvoie en sortie un résultat binaire indiquant si oui ou non les deux signatures proviennent de la même empreinte. Bien entendues deux empreintes provenant de la même personne ne sera jamais identiques en raison de l'élasticité de la peau, de la présence de poussière, de l'orientation du doigt lors de l'acquisition Ceci est caractéristique des systèmes biométriques. La phase d'appariement va donc calculer le degré de similarité (taux d'appariement) entre les deux signatures et décider si elles peuvent être considérées identiques en fonction d'une valeur seuil. Bien que les deux empreintes puissent être comparées directement par corrélation la méthode qui a suscité le plus d'intérêt utilise les caractéristiques locales des minuties et consiste en l'appariement basé sur

L'alignement d'un motifs tel qu'il est aisé en théorie, efficace pour gérer les fausses données détectées dans les phases précédentes, et rapide par rapport aux différentes méthodes. Cet ensemble de règles est divisé en processus :

- ❖ L’alignement : on évalue la transformation géométrique (orientation, translation, homothétie) entre les deux ensembles à traiter et on les aligne suivant cette transformation.
- ❖ L’appariement : on évalue le nombre d’éléments caractéristiques qui sont alignés (moyennant une certaine marge d’erreurs car un alignement parfait est impossible) et le taux d’appariement est calculé en fonction des correspondances rencontrées [7].

1.5.4. Les capteurs d’empreintes digitales

La partie la plus importante d'un scanner d'empreintes digitales à balayage en direct est le capteur (ou élément de détection), qui est le composant où l'image de l'empreinte digitale est formée. La quasi-totalité des capteurs existants appartiennent à l'une des trois familles suivantes : optique, solide et ultrasonore.

- **Capteur d’empreinte optique :**

Réflexion interne totale frustrée (FTIR) : il s'agit de la technique d'acquisition en direct la plus ancienne et là plus couramment utilisée aujourd'hui (Hase et Shimisu (1984) ; Bahuguna et Corboline (1996)). Lorsque le doigt touche la face supérieure d'un prisme en verre/plastique, les arêtes sont en contact optique avec la surface du prisme, mais les vallées restent à une certaine distance. Le côté gauche du prisme est généralement éclairé par une lumière diffuse (un banc de diodes électroluminescentes [LED] ou un film de lumière plane). La lumière entrant dans le prisme est réfléchie au niveau des vallées et dispersée au hasard (absorbée) au niveau des crêtes. L'absence de réflexion permet aux crêtes (qui apparaissent sombres sur l'image) d'être discriminées des vallées (apparaissant claires). Les rayons lumineux sortent du côté droit du prisme et sont focalisés à travers une lentille sur un capteur d'image CCD ou CMOS. Étant donné que les dispositifs FTIR détectent une surface de doigt tridimensionnelle, ils ne peuvent pas être facilement trompés par la présentation d'une photographie ou d'une image imprimée d'une empreinte digitale [6].

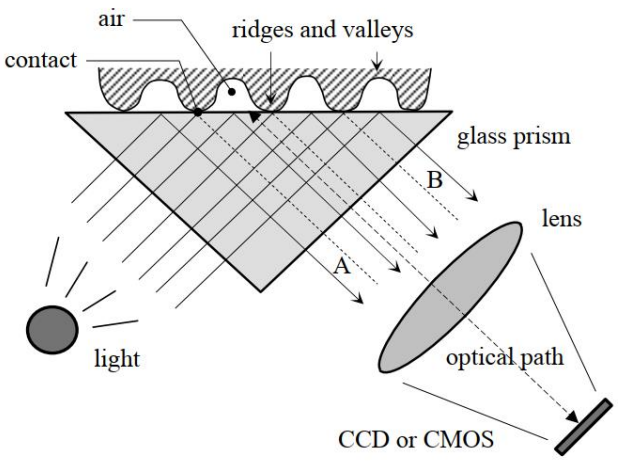


Figure 1-11 : Capteur d'empreinte optique

- **Capteur d'empreinte ultrasonore**

La détection par ultrasons peut être considérée comme une sorte d'échographie. Il est basé sur l'envoi de signaux acoustiques vers le bout du doigt et la capture du signal d'écho. Le signal d'écho est utilisé pour calculer l'image de distance de l'empreinte digitale et, par la suite, la structure de crête elle-même. Le capteur comporte deux composants principaux : l'émetteur, qui génère de courtes impulsions acoustiques, et le récepteur, qui détecte les réponses obtenues lorsque ces impulsions rebondissent sur la surface de l'empreinte digitale (Schneider et Wobschall (1991) et Bicz et al. (1999)). Cette méthode visualise la sous-surface de la peau des doigts (même à travers des gants fins) [6] ; La génération actuelle de scanners d'empreintes digitales à ultrasons est nettement plus petite qu'il y a dix ans et est même utilisée sur les smartphones ; cependant, la technologie est toujours verrouillée par les fabricants et ne doit être utilisée que par les produits propriétaire.

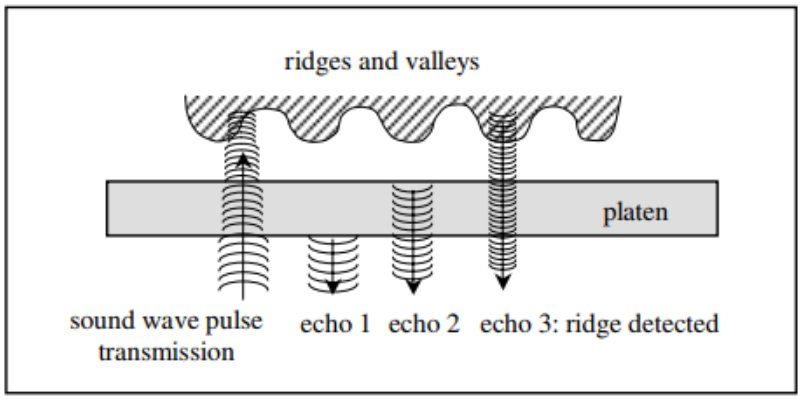


Figure 1-12 : Principe de fonctionnement de l'empreinte ultrasonore

- **Capteur Solide**

Les capteurs à semi-conducteurs (capteurs au silicium) ont été proposés dans la littérature des brevets depuis les années 1980, ce n'est qu'au milieu des années 1990 que ceux-ci sont devenus disponibles dans le commerce. Les capteurs à semi-conducteurs ont été conçus pour surmonter les problèmes de taille et de coût qui semblaient à l'époque être un obstacle au déploiement de systèmes de reconnaissance d'empreintes digitales dans diverses applications.

Tous les capteurs à base de silicium sont constitués d'un réseau de pixels, chaque pixel étant lui-même un petit capteur. Dans les capteurs à semi-conducteurs, il y a Quatre effets principaux ont été proposés pour convertir les informations physiques en signaux électriques : capacitif, thermique, champ électrique et piézoélectrique.

Capacitif : C'est la méthode la plus couramment utilisée aujourd'hui dans les capteurs à base de silicium : Un capteur capacitif est un réseau bidimensionnel de plaques de micro-condensateur intégré dans une puce. L'autre plaque de chaque micro-condensateur est la peau du doigt elle-même. De petites charges électriques sont créées entre la surface du doigt et chacune des plaques de silicium lorsqu'un doigt est posé sur la puce. L'amplitude de ces charges électriques dépend de la distance entre la surface de l'empreinte digitale et les plaques de capacité, Ainsi, les crêtes et les vallées des empreintes digitales entraînent des modèles de capacité différents sur les plaques [6].

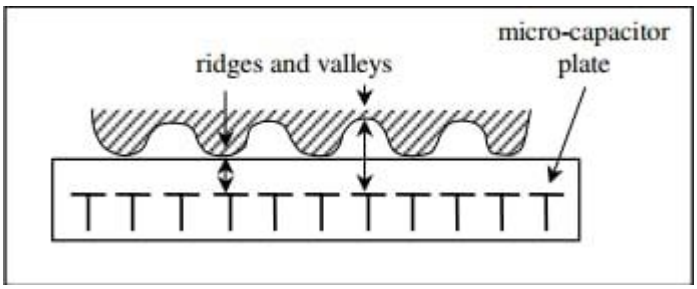


Figure 1-13 : Capteur Solide

1.6. Conclusion

Dans ce chapitre nous avons vu les méthodes de reconnaissance biométriques, Les caractéristiques des empreintes digitales ainsi que la structure globale d'un système de reconnaissance d'empreintes ont également été décrit.

L'étude des empreintes digitales appartient à beaucoup de domaines : l'histoire, la biologie, Les mathématiques. Elles intéressent aussi bien les scientifiques que la police.

Chapitre 2 : **Systèmes de pointage**

2.1. **Introduction**

Un système de pointage est un simple outil de mesure et de contrôle du temps de travail :

Elle doit répondre aux besoins de l'employeur en termes d'organisation du temps de travail dans son entreprise.

Le pointage est un dispositif qui permet de contrôler le temps de travail d'un salarié. A l'origine, les horaires et accès spécifiques à une zone étaient contrôlés par un salarié qui notait scrupuleusement chaque aller et venue d'un salarié.

Mais les premières pointeuses étaient malgré tout à vérifier manuellement, et certains salariés ont déploré une utilisation rébarbative et parfois sujette à litiges. Une arrivée à 13h58 était alors notée comme une arrivée à 14h, soit quelques minutes d'écart. Ces écarts ont fait bondir les organisations syndicales, convaincues qu'il s'agissait d'un travail dissimulé, car quelques minutes sur chaque salarié d'une grosse structure représentaient en réalité une productivité importante. Rapidement, dans les sociétés avec de nombreux salariés, ou prenant leur travail à des heures différentes, un système automatisé de contrôle des allers et venues des salariés a été mis en place pour simplifier ce contrôle.

Aussi, les fabricants ont modernisé les différents systèmes de pointage, qui sont régulièrement appelés « badgeuses ».

2.2. **Systèmes de pointage**

La productivité est le facteur clé de toute industrie fondée sur l'emploi. C'est pourquoi la gestion des heures des employés contribue à de nombreux facteurs du travail, tels que la gestion des salaires et la disponibilité des travailleurs. Dans le passé, il y avait un travail de gestion de ces tâches qui nécessitait un travailleur qui gérait les entrées et les sorties et calculait le temps et qui prenait du temps et de l'argent. Jusqu'à ce que les systèmes de pointage aient été inventés qui permettaient de gagner plus de temps et d'être rapides et rendaient le calcul des salaires moins chronophage.

2.3. Différents systèmes de pointage

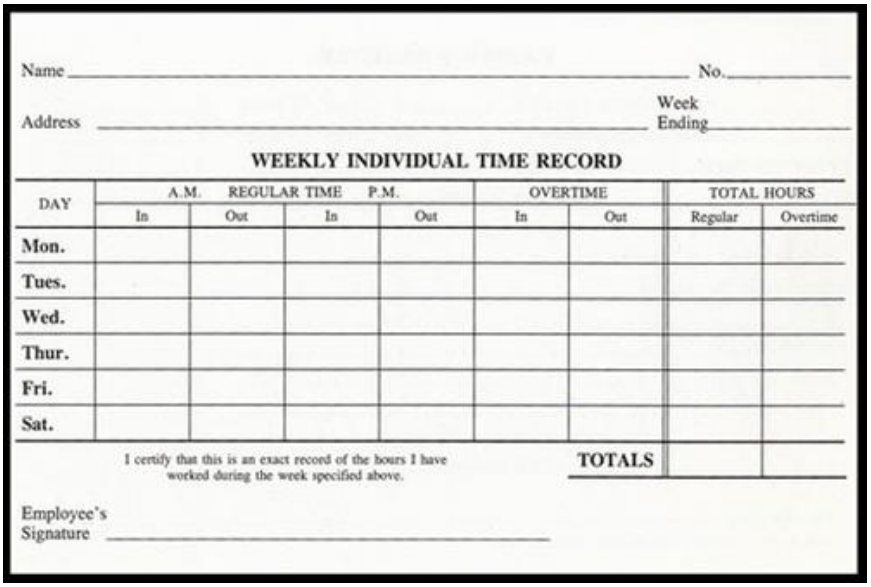
Il existe différents types du système de pointage :

- **Carte de pointage**

Les cartes de pointage ou les feuilles de temps sont toujours l'une des formes les plus populaires d'enregistrement des heures de travail. Les entreprises utilisent des feuilles de calcul en ligne ou parfois même des cartes papier pour suivre l'assiduité des employés.

Les employés écrivent l'heure de début et de fin de travail, les pauses déjeunées, les heures d'absence et les heures supplémentaires.

Parfois, si une entreprise ne dispose pas d'un système automatique de suivi du temps, les employés utilisent des applications personnelles de suivi du temps libre pour remplir avec précision les feuilles de temps. Bien que de plus en plus d'organisations décident d'utiliser une solution automatique.



Name _____ No. _____

Address _____ Week Ending _____

WEEKLY INDIVIDUAL TIME RECORD

DAY	A.M. REGULAR TIME		P.M.		OVERTIME		TOTAL HOURS	
	In	Out	In	Out	In	Out	Regular	Overtime
Mon.								
Tues.								
Wed.								
Thur.								
Fri.								
Sat.								

I certify that this is an exact record of the hours I have worked during the week specified above. **TOTALS**

Employee's Signature _____

Figure 2-1 : Carte de pointage

- **Horloge poinçon (pointage mécanique)**

C’est un système mécanique simple qui contient une horloge. En appuyant sur un bouton par l’employé, il imprime les heures d’arrivée, de départ et de pause sur une carte en plastique ou en papier.

De cette façon, l'entreprise peut surveiller les heures de travail de l'employé par un dispositif mécanique qui ne nécessite pas d'emploi supplémentaire pour le faire.

Figure 2-2 : Horloge poinçon

- **Pointage par Badge**

Il est considéré comme l'évolution de l'horloge à poinçons. En utilisant un badge physique unique pour chaque employé, il enregistre l'heure d'arrivée, de pause et de départ à l'aide de la technologie RFID. Il enregistre les entrées dans une base de données accessible uniquement par l'entreprise, soit par des moyens physiques tels que des clés USB et des cartes SD, soit via une base de donnée à distance à l'aide d'un service IoT. Il a été reconnu comme la prochaine génération de systèmes de pointage.

Figure 2-3 : Système de pointage par carte RFID

2.4. Pointage biométrique

Le pointage biométrique est considéré comme le système de pointage le plus rentable du secteur en raison de sa simplicité. À une certaine période, l'employeur enregistre une des données biométriques des salariés comme l'empreinte digitale ou l'iris.

Les données biométriques sont ensuite ajoutées à la base de données du lecteur biométrique afin qu'à chaque fois il lise les entrées et les ajoute à la base de données de l'entreprise. Le système de pointage biométrique ne nécessite aucun type d'authentification plutôt que les employés eux-mêmes et c'est un avantage de sécurité pour échapper à la fraude.

2.4.1. Avantage de pointage biométrique

Système de pointage utilisant la technologie de biométrique.

- Le lecteur identifie et enregistre le pointage d'une personne en moins d'une seconde.
- Evite la fraude.
- Sûr.
- Convivial (le scan de la biométrie se fait à l'aide d'un écran et d'un clavier)
- Économique (le coût de la machine est considéré comme bon marché car il remplace un employé salarié qui peut coûter plus cher à l'entreprise à long terme).

2.5. Différents types d'une pointeuse biométrique

La pointeuse biométrique réagit en déclenchant un décompte des horaires de travail quand un de ses capteurs (caméra, pad, etc.) reconnaît une caractéristique humaine comme :

- Un visage.
- Une iris
- Le contour d'une main
- Des empreintes digitales.

- **La pointeuse d'empreinte digitale**

Les empreintes digitales sont le dessin formé par les lignes de la peau des doigts, ils sont des signatures que nous laissons derrière nous à chaque fois que nous touchons un objet. Aussi Les motifs dessinés par les crêtes et plis de la peau sont différents pour chaque individu.

On distingue deux types d'empreintes : l'empreinte directe ou visible qui laisse une marque visible et l'empreinte latente ou invisible qui est composée de lipides, de sueur et de saletés déposés sur un objet touché.

L'employé peut pointer en utilisant son doigt seulement, sans carte ni badge. Cette solution de pointage facilite le travail des gestionnaires de ressources humaines en contrôlant toutes les entrées / sorties de façon très simple.

Figure 2-4 : Pointage par empreinte digitale

- **Pointeuse avec un contour d'une main**

La géométrie de la main est une technologie biométrique récente, elle consiste à analyser et à mesurer la forme de la main, c'est - à - dire mesurer la longueur, la largeur et la hauteur de la main d'un utilisateur et de créer une image 3-D. Des LEDs infrarouges sont utilisés pour acquérir les données de la main. Cette technologie offre un niveau raisonnable de précision et est relativement facile à Utiliser. Les utilisations les plus populaires de la géométrie de la main comprennent l'enregistrement de présence et le contrôle d'accès. Par contre, les systèmes de capture de la main sont relativement grands et lourds, ce qui limite leur utilisation dans d'autres applications comme : téléphones portables, voitures, ordinateurs portables.

Figure 2-5 : Pointeuse avec un contour d'une main

- **Pointeuse avec les contours de visage**

Les images faciales sont probablement la caractéristique biométrique la plus communément employée par l'homme pour effectuer une identification personnelle.

L'utilisation d'une caméra permet de capter la forme du visage d'un individu. Selon le système utilisé, l'individu doit être positionné devant l'appareil ou peut être en mouvement à une certaine distance. Les données biométriques qui sont obtenues sont par la suite comparées au fichier référence.

Figure 2-6 Pointeuse avec les contours de visage

- **Pointeuse d'iris**

L'iris est la région, sous forme d'anneau, située entre la pupille et le blanc de l'oeil, L'utilisation de l'iris comme caractéristique biométrique unique de l'homme a donné lieu à une technologie d'identification fiable et extrêmement précise.

L'iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu. Les algorithmes utilisés dans la reconnaissance de l'iris sont si précis que la planète toute entière pourrait être inscrite dans une base de données de l'iris avec peu d'erreurs d'identification.

L'image de l'iris est généralement capturée à l'aide d'une caméra standard mais il existe plusieurs contraintes liées à l'utilisation de cette technologie. Par exemple, il faut s'assurer que l'iris de l'individu est à une distance fixe et proche du dispositif de capture ce qui limite l'utilisation de cette technologie.

Figure 2-7 Pointeuse d'iris

2.6. **Conclusion**

L’aménagement du temps de travail avait été utilisé comme un outil de transformation des entreprises au service de projets : stratégie commerciale, politique d’offre économique, recherche de croissance, mobilisation des salariés, mutation de la gestion salariale, etc.

Un des nombreux outils pour ce faire (l’aménagement du temps de travail) c’est la pointeuse (Un système de pointage), en premier lieu, un appareil servant, comme son nom l’indique, à pointer les allées et venues des salariés et à les enregistrer. Mais avec les avancées technologiques, l’outil en soi n’est plus toujours obligatoire, il devient mobile et s’est transformé en une application qu’il suffit d’installer sur son smartphone ou sa tablette. Dans le premier comme dans le deuxième cas, le dispositif doit être relié à un logiciel de gestion, qui enregistrera et traitera les données

Chapitre 3 : Conception et réalisation un système de pointage à base d'empreinte digitale

3.1. Introduction

Ce chapitre présente les étapes de conception de notre projet ; le fonctionnement de cheque composants pour créer un système de pointage qui relais à l'empreinte pour la reconnaissance, clavier 4x4, LCD pour l'affichage et une carte ARDUINO MEGA2560 pour la gestion.

3.2. Schéma Synoptique

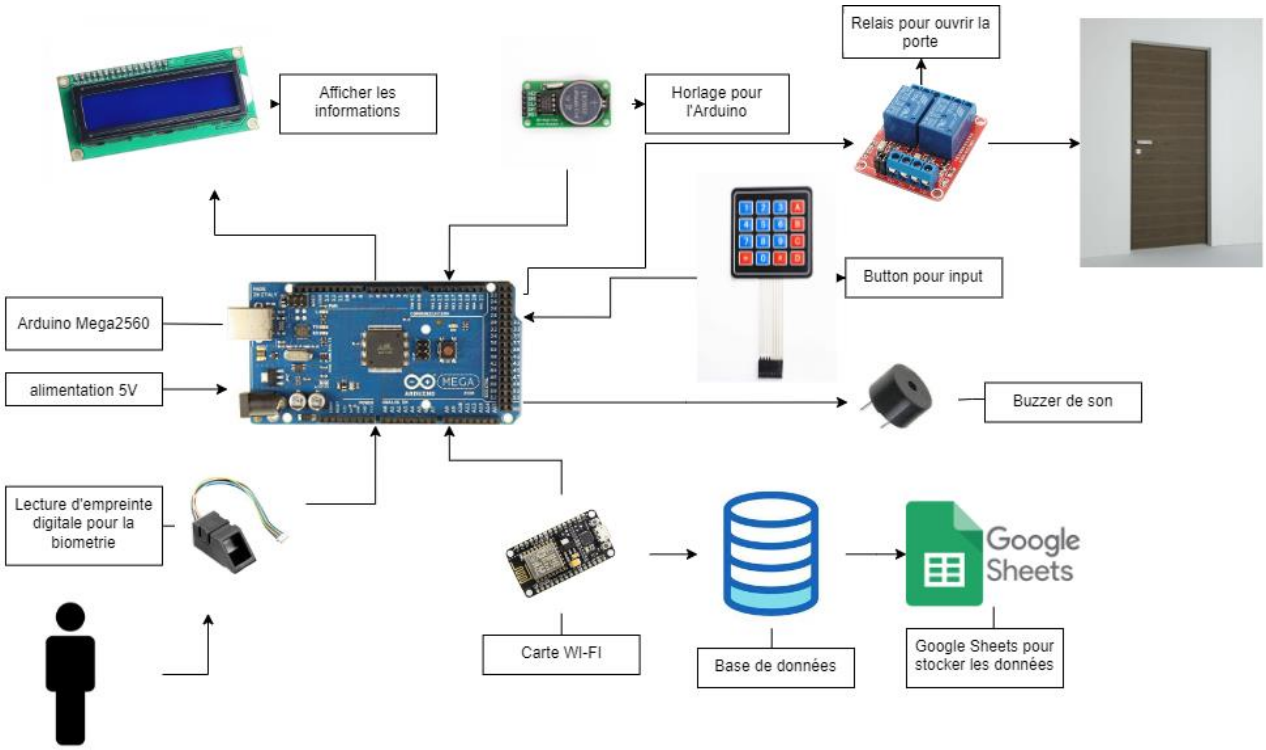


Figure 3-1 : Schéma Synoptique du Système

3.3. Conception Materielle

3.3.1. RTC DS1302

L'horloge temps réel (aussi connue sous l'acronyme RTC pour Real Time Clock) c'est une horloge numérique autonome qui donne l'heure quand on la lui demande. Ce type d'horloge est très utile dans des projets de mesure de grandeurs physiques avec horodatage par exemple [8].

Aussi équipée avec une pile pour rester à l'heure même lorsque le système est hors tension ou pendant qu'on peut reprogrammer notre microcontrôleur.

Le module que nous avons utilisé (DS1302) est un module bon marché avec une grande précision qui peut être utilisé dans différents projets. Ce module RTC est capable de gérer l'heure sur les secondes, les minutes, les heures, le jour, la date, le mois et l'année. Dans ce module, la date est définie automatiquement selon que le mois est de 29, 30 ou 31 jours et qu'il s'agit d'une année bissextile ou non. (Ce n'est valable que jusqu'à l'an 2100).

Figure 3-2 Brochage de RTC DS1302

- **Brochage du module RTC DS1302:**

Ce module a 5 broches :

VCC: Alimentation des modules – 5V

GND: la terre

CLK: Clock pin (Broche d'horloge)

DAT: Data pin(Broche de données).

RST: Reset.

Le circuit suivant montre comment on peut connecter Arduino au module DS1302.

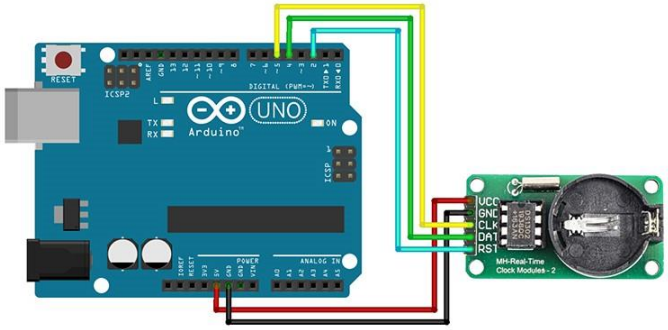


Figure 3-3 : Brochage de RTC avec Arduino UNO

On utilise le module DS1302 pour garder la date et l'horloge sur notre système même s'il y a coupure d'alimentation.

3.3.2. Clavier Matriciel 4x4

Les claviers sont fabriqués en différents types, mais les tailles les plus courantes sont 5x4 et 4x4. Ces chiffres indiquent le nombre de lignes et de colonnes des claviers. Par exemple, un clavier 3x4 à 4 lignes et 3 colonnes.

Comment fonctionne un clavier (Exemple de clavier 4*3)

Pour recevoir des données de 12 boutons, nous devons utiliser 12 broches numériques de notre microcontrôleur (Arduino), ce qui signifie gaspiller beaucoup de broches, mais en utilisant le clavier, nous n'avons besoin que de 7 broches numériques voir figure ci-dessous.

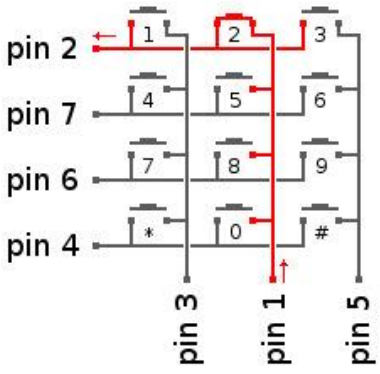


Figure 3-4 : Fonctionnement de clavier 4x3

En trouve plusieurs méthodes de brochage du clavier matriciel 4x4 avec la carte Arduino. Nous l'expliquons sous les formes suivantes :

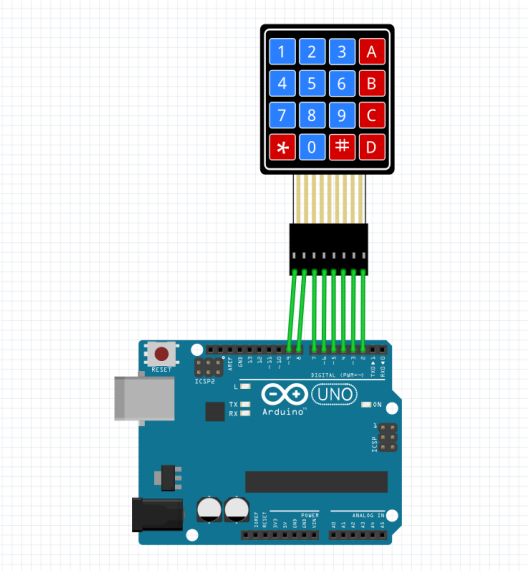


Figure 3-5 : Brochage de clavier 4x4 sur Arduino UNO

Nous utilisons le clavier pour faire la distinction entre les entrées si c'est arrivage ou départ et aussi pour obtenir des informations de contact en cas de panne.

3.3.3. Afficheur LCD 1602

Le module d'affichage de caractères est un module LCD avec 2 lignes et 16 colonnes, et a un rétroéclairage vert ou bleu et un caractère blanc. Ces écrans peuvent généralement être utilisés pour afficher du texte, des caractères et des chiffres. Le contraste peut être ajusté en connectant un potentiomètre à la broche 3. Les broches 15 et 16 sont pour le rétroéclairage. On peut utiliser 6 broches E, RS, D4, D5, D6, D7 pour interfacer l'écran avec Arduino. Nous brocherons un potentiomètre de 10KOhms.

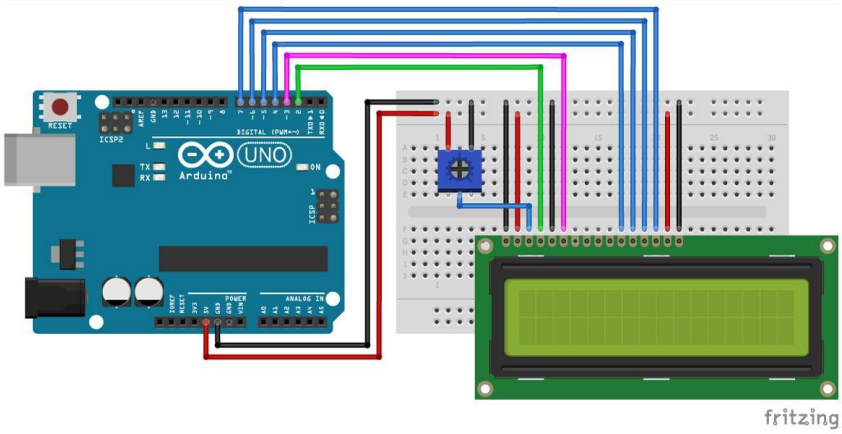


Figure 3-6 : Brochage de LCD1602 avec Arduino Uno

nous utilisons l'écran LCD pour afficher l'ID du personnel et le temps.

3.3.4. **Buzzer piezo :**

Buzzers et sirènes aussi connus sous le nom d'alarmes audio, d'indicateurs audio, de transducteurs audio, de buzzers piézo, de bips ou d'alarmes sonores, la variété de produits disponibles est vaste. Généralement, les buzzers sont utilisés à des fins d'alarme ou d'identification sur une large gamme d'applications.

L'un des nombreux types de buzzers est le Piezo Buzzer qui contient une plaque de vibration piézo-céramique ou un élément piézo dans un boîtier moulé. Fondamentalement, le son est généré lorsqu'une tension est appliquée et que l'élément piézo vibre à l'intérieur du boîtier. à la fin, les appareils piézo consomment moins de courant, ont une plage de fréquences plus large et génèrent une sortie sonore plus élevée.

Figure 3-7 : buzzer piezo

nous utilisons le buzzer pour émettre un son au cas où l'accès est accordé.

3.3.5. **Relais à deux canaux**

Le module (relais à deux canaux) contient deux relais isolés électriquement de l'entrée de commande. Les relais peuvent être utilisés pour commuter des charges de tension et de courant plus élevées qu'un microcontrôleur ne peut traditionnellement accomplir.

Figure 3-8 : Relais à deux canaux

Le relais à deux sorties normalement ouvertes et normalement fermées (NO et NF). Lorsque la broche IN1 ou IN2 est connectée à la terre, NO sera ouvert et NF sera fermé, et lorsque IN1 ou IN2 n'est pas connecté à la terre, l'inverse se produit [9].

- **Caractéristique de Relais à deux canaux:**

- Alimenté à partir de 5V.
- 2 canaux.
- Peut être utilisé comme Normalement Ouvert (NO) ou Normalement Fermé (NC).
- Entrées opto-isolées.

Nous utilisons le relais pour contrôler la serrure de la porte, lorsque l'accès est accordé pour le statut d'arrivée nous lui envoyons un signal afin d'ouvrir la porte.

3.3.6. Empreinte digitale FPM10A

Le capteur d'empreinte est un capteur qui détecte les empreintes digitales. L'identification et la vérification des empreintes digitales est donc très simple. Nous pouvons enregistrer jusqu'à 127 empreintes digitales. Ces empreintes seront stockées sous forme digitale dans la mémoire flash embarquée. Il y a une led vert dans la lentille qui s'allume durant la prise l'empreinte.

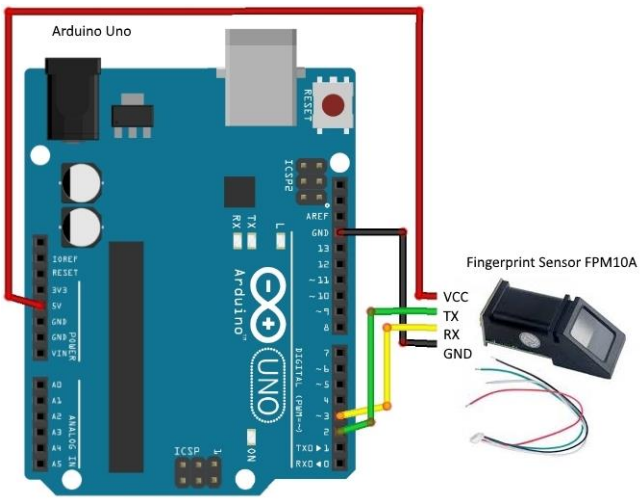


Figure 3-9 Brochage d'empreinte digitale avec Arduino Uno

3.3.7. NodeMcu

Aujourd'hui, les applications se multiplient, et connecter les objets prennent de plus en plus d'importance. Il existe plusieurs façons de connecter des objets tels que le protocole Wi-Fi. NodeMCU est une plate-forme open source basée sur ESP8266 qui peut connecter des objets et permettre le transfert de données en utilisant le protocole Wi-Fi. De plus, en fournissant certaines des fonctionnalités les plus importantes des microcontrôleurs telles que (GPIO, PWM, ADC) etc., il peut résoudre à lui seul de nombreux besoins du projet [10].

- **Les caractéristiques générales de cette carte sont :**
  - Facile à utiliser.
  - Programmable avec les langages Arduino IDE ou IUA.
  - Disponible en tant que point d'accès ou station.
  - Contient une antenne interne.

Les avantages de l'utilisation du module ESP8266 sont la connectivité Wi-Fi pour la connexion Internet et réseau, y compris un contrôleur puissant avec une RAM élevée et son prix abordable.

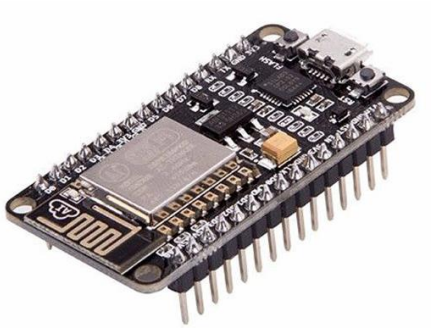


Figure 3-10 NodeMcu ESP8266 12-e

le nodemcu est utilisé pour recevoir les données de l'Arduino, se connecter à internet puis envoyer les données vers le cloud en utilisant le protocole HTTPS

3.4. Arduino Mega2560

L'Arduino Mega 2560 est une carte microcontrôleur basée sur l'ATmega2560. Il dispose de 54 broches d'entrée/sortie numériques (dont 15 peuvent être utilisées comme sorties PWM), 16 entrées analogiques, 4 UART (ports série matériels), un oscillateur à cristal 16 MHz, une connexion USB, une prise d'alimentation, un en-tête ICSP, et un bouton de réinitialisation, Le contrôleur ATMega2560 contient un bootloader qui permet de modifier le programme sans passer par un programmateur [11].

Un Arduino standard a un seul port série matériel tandis que l'Arduino Mega a quatre ports série matériels qui peuvent communiquer avec jusqu'à quatre périphériques série différents.

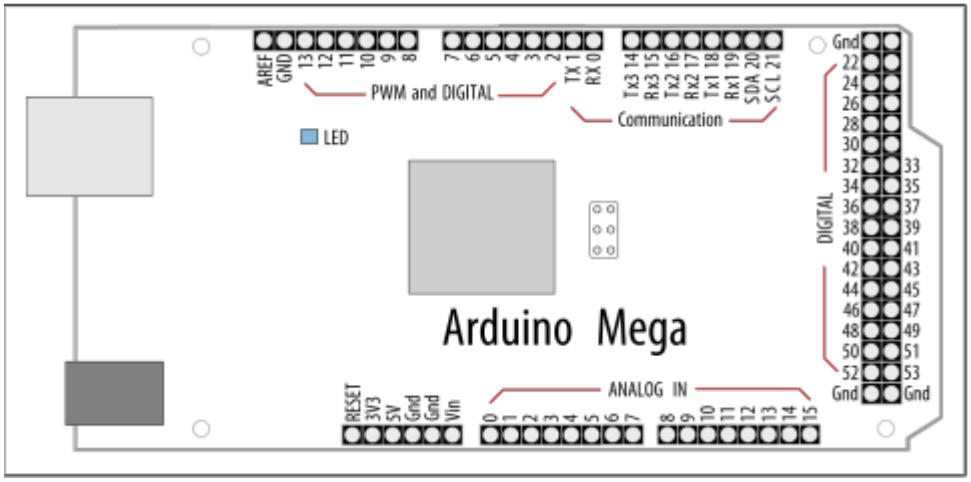


Figure 3-11 : Schéma d'Arduino Mega2560

Arduino a un nombre limité de broches pouvant être utilisées pour la sortie analogique. Sur une carte standard, on peut utiliser les broches 3, 5, 6, 9, 10 et 11. Sur la carte Arduino Mega, on peut utiliser les broches 2 à 13 pour la sortie analogique. La plupart des recettes qui suivent utilisent des broches qui peuvent être utilisées à la fois pour le numérique et l'analogique afin de minimiser le recâblage si nous souhaitons essayer différentes recettes.

3.4.1. Programme de Arduino Mega2560

Arduino Mega 2560 peut être programmé à l'aide du logiciel Arduino IDE qui est un logiciel Arduino officiel utilisé pour programmer toutes les cartes Arduino. Ce logiciel est utilisé pour écrire, compiler et télécharger le code dans la carte Arduino. Il est basé sur le langage de programmation C++.

Cet appareil est livré avec une interface USB afin qu'un câble USB puisse être utilisé pour connecter l'appareil à l'ordinateur à travers lequel on peut transférer le croquis (le programme Arduino est appelé un croquis) sur la carte. De plus, ce logiciel est open source, ce qui signifie qu'il est gratuit et que tout le monde peut utiliser ce logiciel pour permettre à la carte de fonctionner selon le nombre d'instructions qu'on peut envoyer de ce logiciel à la carte Arduino.

La carte comporte un chargeur de démarrage intégré, ce qui signifie qu'on n'a pas besoin d'un graveur externe pour graver le code dans l'appareil Arduino.

3.4.2. Applications

Cette carte peut fonctionner comme un projet autonome ou nous pouvons d'ajouter d'autres cartes Arduino, des boucliers Arduino et des cartes Raspberry Pi. Cette unité est recommandée pour les projets électroniques qui nécessitent plus d'espace mémoire et de broches GPIO

Voici quelques applications qu'on peut essayer avec la méga carte Arduino.

- Programmation parallèle et multitâche
- Peut contrôler plus d'un moteur
- Systèmes domotiques et de sécurité
- Systèmes embarqués
- Interfaçage de nombre de capteurs
- Détection et détection de la température
- Projets de détection de niveau d'eau
- Développer une imprimante 3D

3.4.3. Communication entre Arduino Mega2560, Empreinte digitale et NodeMcu

Pour la communication entre Arduino et l'ordinateur, nous avons utilisé la communication série via un port USB. Et pour communiquer avec le scanner d'empreintes digitales et NodeMcu que nous utilisons, nous avons utilisé la communication série avec des broches (Rx/Tx).

La communication série est utilisée pour la communication entre la carte Arduino et un ordinateur ou d'autres appareils. Toutes les cartes Arduino ont au moins un port série et Arduino Mega2560 a quatre ports série. Les broches 0 et 1 sont utilisées pour la communication avec l'ordinateur. La connexion de quoi que ce soit à ces broches peut interférer avec cette communication, notamment en provoquant des échecs de téléchargement vers la carte [11].

Pour communiquer avec le lecteur d'empreintes digitales, nous avons utilisé Serial2 (Rx2/Tx2) (broches 16 et 17), et pour communiquer avec le NodeMcu, nous avons utilisé Serial3 (Rx3/Tx3) (broches 14 et 15). Cette approche nous a assuré une communication matérielle qui ne repose pas sur un code d'un Arduino pour exécuter l'échange de données.

Quant au NodeMcu, il n'a qu'une seule communication série qui est celle connectée au port USB, et s'y connecter n'est pas recommandé car il interfère avec le signal USB. C'est pourquoi nous avons utilisé une bibliothèque sur l'IDE Arduino appelée <**SoftwareSerial.h**> qui nous a permis d'allouer différentes broches numériques pour agir en tant que communication série. Nous avons utilisé les broches D6 et D7 pour agir comme Tx et Rx pour notre communication série.

3.5. Schéma globale de projet

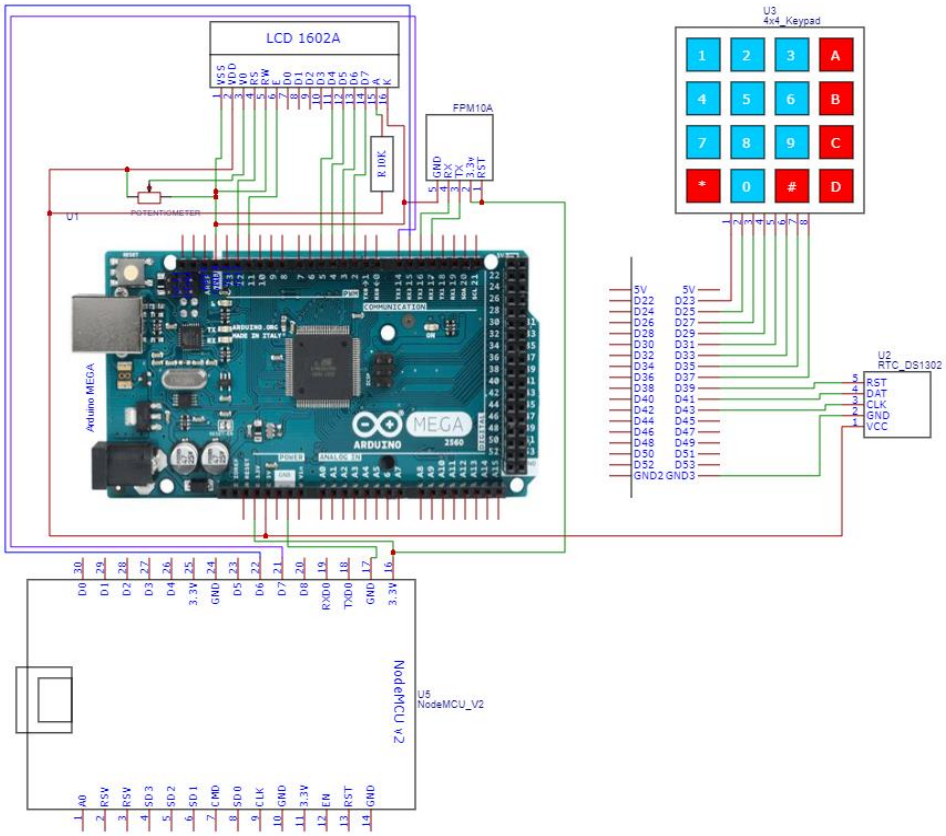


Figure 3-12 Schéma globale de projet

Pour désigne ce schéma en utilise Site Web EasyEDA , il base sur le câblage avec les files entre les composants et la carte Arduino. Ce schéma résume notre travail de manière très précise où il est facile d'expliquer notre travail de manière détaillée et très précise.

3.6. L'organigramme de système de pointage

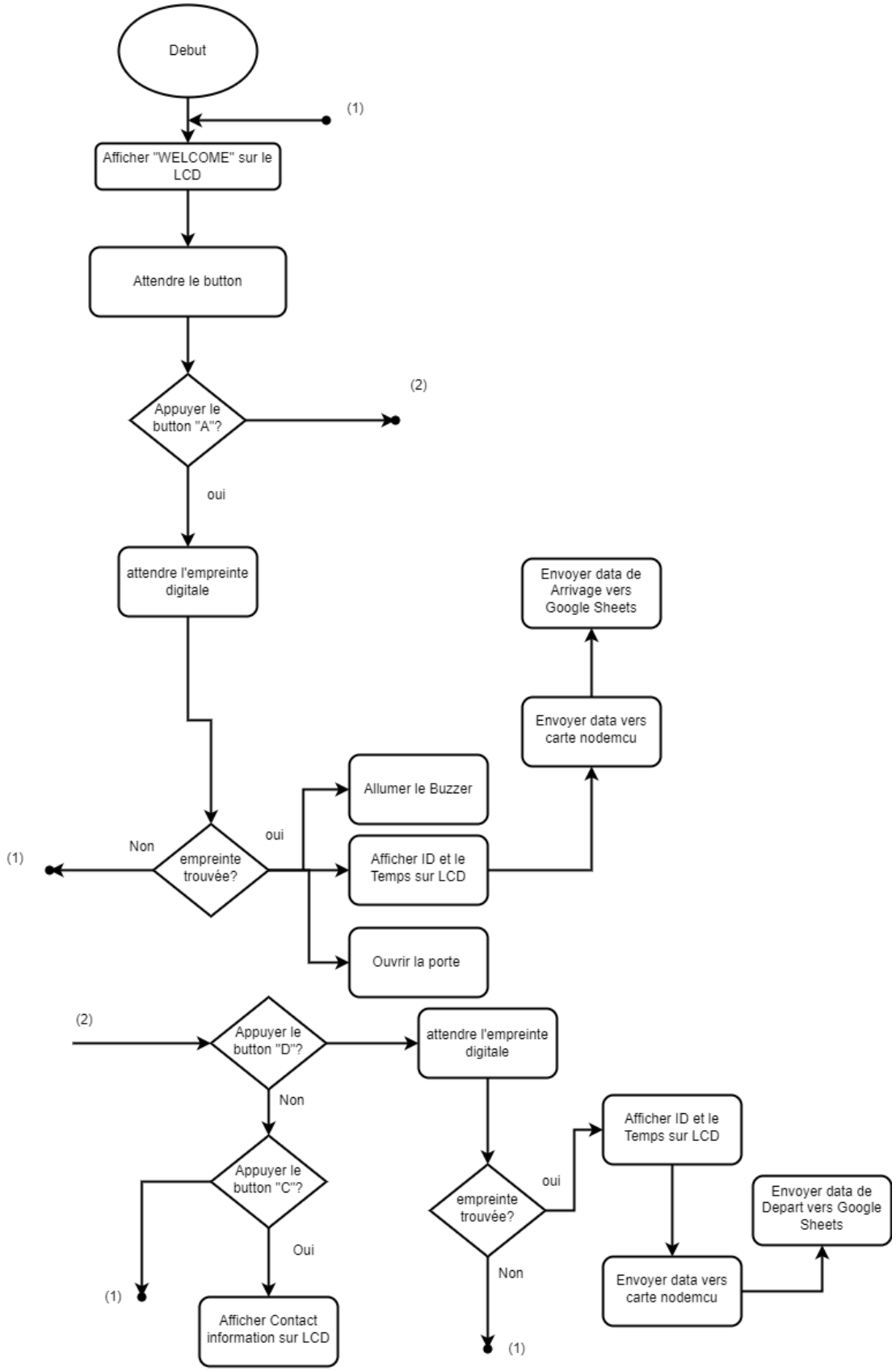


Figure 3-13 L'organigramme de système de pointage

3.7. Explication de l'organigramme

Le système commence par afficher «Bonjour» sur l'écran LCD, puis attend une pression sur une touche du clavier.

Si le personnel appuie sur «A», la phrase «APP EMPREINTE» s'affichera sur l'écran LCD et le système attendra l'empreinte digitale de l'utilisateur pendant 5 secondes, si l'empreinte digitale n'est pas détectée, le système reviendra au début. S'il est détecté, le système effectuera une recherche rapide en le comparant à la base de données du lecteur, s'il n'y a pas de correspondance, le système reviendra au début. S'il y a une correspondance, le système associera l'identifiant à la mémoire flash de l'Arduino pour extraire le nom d'utilisateur et mettre à jour l'heure sur le RTC.Ensuite, l'Arduino enverra le nom, l'ID, l'heure, la date et l'état (arrivée) au nodemcu et envoyer une impulsion au buzzer pour faire un son et un signal au relais pour ouvrir la porte puis revenir au début.

Après avoir reçu les données, le nodemcu se connectera à Internet en utilisant le WIFI, puis enverra les données aux feuilles de google.

Si le personnel appuie sur «B», le système effectuera les mêmes procédures sauf pour le statut (Départ) et n'ouvrira pas la porte.

Si le personnel appuie sur «C», le système affichera les informations de contact (numéro de téléphone et e-mail) sur l'écran LCD.

3.8. Google Sheets

Google Sheets est une application Web qui permet aux utilisateurs de créer, mettre à jour et modifier des feuilles de calcul et de partager les données en ligne en temps réel.

Le produit de Google offre des fonctionnalités de feuille de calcul typiques, telles que la possibilité d'ajouter, de supprimer et de trier des lignes et des colonnes. Mais contrairement à d'autres programmes de tableur, Google Sheets permet également à plusieurs utilisateurs géographiquement dispersés de collaborer sur une feuille de calcul en même temps et de discuter via un programme de messagerie instantanée intégré. Les utilisateurs peuvent télécharger des feuilles de calcul directement à partir de leurs ordinateurs ou appareils mobiles. L'application enregistre automatiquement chaque modification et les utilisateurs peuvent voir les modifications des autres utilisateurs au fur et à mesure qu'elles sont apportées.

3.8.1. À quoi sert Google Sheets ?

Google Sheets est généralement utilisé pour la collaboration de feuilles de calcul entre différents emplacements géographiques. Plusieurs utilisateurs peuvent modifier un document Google Sheets en temps réel, avec un suivi des modifications pour chaque utilisateur individuel.

L'application de feuille de calcul en ligne Google Sheets permet aux utilisateurs de créer, de modifier et de formater des feuilles de calcul en ligne pour organiser et analyser les informations. Google Sheets est souvent comparé à Microsoft Excel, car les deux applications sont utilisées à des fins similaires. Google Sheets est essentiellement la version cloud de Google des fonctionnalités de base de Microsoft Excel.

3.8.2. Fonctionnalités de Google Sheets

Google Sheets inclut les fonctionnalités principales suivantes :

- Édition et mise en forme de feuilles de calcul.
- Visualisation de données.
- Fonctionnalités basées sur l'apprentissage automatique.
- Fonctionnalités collaboratives.
- Sécurité.
- Gratuit.

3.9. Conclusion

Dans ce chapitre, nous expliquons les étapes par lesquelles nous avons créé un système de pointage basé sur le lecteur d'empreintes digitales et les procédures de sauvegarde des données d'entrée dans le *cloud* à l'aide de NodeMcu. Également les différents modes de fonctionnement pour l'enregistrement de l'état des entrées et l'ouverture de la serrure de la porte à l'aide du relais.

Conclusion générale

De ces jours, la biométrie existe de plus en plus dans notre vie, smartphones, ordinateurs... elle est considérée comme la nouvelle solution pour les entreprises afin qu'elles enregistrent et organisent les données d'entrée des employés de manière automatique et sécurisée qui ne nécessite pas d'informations supplémentaires ressources humaines et c'est économiquement mieux.

L'utilisation du système de pointage permet de mieux organiser les activités et de visualiser les heures d'entrée et de sortie, de notifier les absences et d'optimiser la productivité.

Le système de pointage est automatique et fournit un rapport détaillé sur l'activité des personnels.

Cette solution est également un avantage pour les employés car elle peut calculer un temps de travail exact afin d'aider le personnel à ne pas faire d'heures supplémentaires.

Enfin, nous espérons que ce projet nous aidera à acquérir des connaissances de base sur le travail avec les microcontrôleurs et sur le développement de la norme de l'industrie 4.0.

Références

[1] M. A. S. Peter Gregory, Biometrics For Dummies, For Dummies, 2008.

[2] Biometrics, Computer Security Systems and Artificial Intelligence Applications, Springer, 2006.

[3] J. Daugman, «How iris recognition works,» chez *The essential guide to image processing*, Elsevier, 2009.

[4] P. a. S. D. Wang, «A research on palm vein recognition,» *13th International Conference on Signal Processing (ICSP)*, 2016.

[5] V. A. a. D. R. a. C. S. Mann, «Development of voice recognition: Parallels with face recognition,» *Journal of experimental child psychology*, 1979.

[6] D. M. A. K. J. S. P. Davide Maltoni, Handbook of Fingerprint Recognition, New York: Springer, 2003.

[7] M. T. R. N. Samir Nanavati, Biometrics: Identity Verification in a Networked World, Wiley, 2002.

[8] H. a. O. W. Kopetz, «Clock Synchronization in Distributed Real-Time Systems,» *IEEE*, Vols. %1 sur %2C-36, 1987.

[9] V. Gurevich, Electric relays: principles and applications, CRC Press, 2018.

[10] Y. S. Parihar, «Internet of Things and Nodemcu,» *Journal of Emerging Technologies and Innovative Research*, 2018.

[11] «Arduino,» [En ligne]. Available: https://www.arduino.cc/.

[12] P. Reid, Biometrics for Network Security, Prentice Hall PTR, 2003.

[13] M. Margolis, Arduino Cookbook, 2nd Edition, O'Reilly Media, 2012.