

الجمهورية الجزائرية الديمقراطية الشعبية

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université Dr Tahar Moulay de Saida

Faculté de Technologie

Département d'électronique



Mémoire De fin d'étude pour obtention du diplôme

Master en électronique

***Présenté par: KHEDIR IKHRAM
RAMLI BADIAA***

Option : électronique d'instrumentation

***Conception et Réalisation un Système De
Pointage à Base D'empreinte Digitale***

**Soutenu le: 20 Septembre 2023, devant l'honorable jury
composé de :**

Président: M. BOUDKHIL Abdelhakim

Examineur : M. DAMOU Mehdi

Encadreur : M. BERBER Redouane

Année universitaire 2022 – 2023

Dédicaces

Nous dédions ce mémoire à :

- ❖ **Nos chers parents** qui ont consacré leur vie à nous soutenir et à nous encourager pour réaliser nos rêves, et ce mémoire est une étape simple sur le chemin pour leur rendre la pareille et les satisfaire et les remercier pour tout l'amour, le soutien et les sacrifices qu'ils ont faits.
- ❖ **À nos proches** qui nous ont soutenus à chaque fois d'avoir besoin d'eux et nous ont encouragés à chaque fois que nous sommes succombé dans notre parcours académique
- ❖ À toute la famille **RAMLI ET KHADIR.**
- ❖ Nos collègues de l'université de **MOLAY TAHAR** et à tous ce qui nous ont enseignés au long de notre vie scolaire.
- ❖ Tous ceux qui nous ont aidés pour accomplir ce mémoire.

Ikram

Badiaa

Remerciements

Tout d'abord, je remercie le dieu, notre créateur de nous avoir donné la force, la volonté et courage afin d'accomplir ce modeste travail.

Les remerciements vont tout d'abord au corps professoral et administratif de département d'électronique, pour la richesse et la qualité de leur enseignements et qui déploient de grands efforts pour assurer à leurs étudiants une formation actualisée. Et nous remercions aussi les membres des jurys d'avoir accepté d'évaluer notre travail.

Nous remercions notre encadreur Mr. BERBER Redouane, pour sa gentillesse, pour ses précieux conseils et pour sa patience avec nous, et pour le temps qu'il a consacré à nous apporter les outils méthodologiques indispensables à la conduite de ce projet. Sans oublier tous ceux qui nous ont aidés et soutenus dans notre projet.

Finalement, nous tenons à exprimer notre profonde gratitude à nos familles « chers parents, frères et sœurs » qui ont contribué à la réalisation de ce mémoire.

Ikram

Badiaa

Résumé

Ce projet est un enregistreur biométrique de présence et d'absence pour les étudiants. Ce système repose sur le système d'empreintes digitales. Il fonctionne en prenant l'empreinte digitale via le capteur optique. Il est réalisé avec le microcontrôleur dans l'environnement Arduino ID pour stocker les empreintes digitales dans une base de données avec les informations sur l'étudiant.

Le système fonctionne dans les deux cas d'inscription et de présence, où il enregistre l'empreinte digitale puis la reconnaît en cas de présence.

En fin de compte, on peut dire que cet appareil est utile pour le professeur et l'étudiant car il raccourcit le temps et élimine les problèmes de la carte d'étudiant tels que la perte et l'oubli, et l'empreinte digitale est une solution idéale pour certains cas de truchage aux examens.

Il peut également être utilisé dans les entreprises et les usines pour surveiller les travailleurs, car il peut nous fournir un rapport détaillé des entrées et sorties hebdomadaires ou mensuelles.

ملخص

هذا المشروع عبارة عن مسجل بيومتري لحضور وغياب الطلاب. يعتمد هذا النظام على نظام البصمة حيث يعمل عن طريق أخذ بصمة الإصبع بواسطة المستشعر البصري و باستخدام وحدة التحكم الدقيقة المعرفة بـ: Arduino لتخزين بصمات الأصابع في قاعدة بيانات تحتوي على معلومات الطالب و من ثم التعرف عليها في حالة الحضور.

وفي النهاية يمكن القول أن هذا الجهاز مفيد لكل من الاستاذ والطالب لأنه يختصر الوقت لمعاينة الحضور ويقضي على مشاكل بطاقة الطالب مثل الضياع والنسيان، وتعتبر بصمة الإصبع حلاً مثالياً لبعض التجاوزات في الامتحان. كما يمكن استخدامه في الشركات والمصانع لمراقبة العمال، حيث يمكن أن يزودنا بتقرير مفصل عن الدخول والخروج اليومي أو الأسبوعي و حتى الشهري.

Sommaire

INTRODUCTION GENERALE	1
-----------------------------	---

CHAPITRE I :

SYSTEME DE POINTAGE

I.1 INTRODUCTION.....	1
I.2 DIFFERENTS SYSTEMES DE POINTAGE.....	1
I.2.1 CARTE DE POINTAGE	1
I.2.3 POINTAGE PAR BADGE.....	3
I.2.4 POINTAGE BIOMETRIQUE.....	3
I.3 AVANTAGE DE POINTAGE BIOMETRIQUE.....	3
I.4 DIFFERENTS TYPES D'UNE POINTEUSE BIOMETRIQUE	4
I.4.1 LA POINTEUSE D'EMPREINTE DIGITALE	4
I.4.2 POINTEUSE AVEC UN CONTOUR D'UNE MAIN	5
I.4.3 POINTEUSE AVEC LES CONTOURS DE VISAGE	5
I.4.4 POINTEUSE D'IRIS	6
I.5 CONCLUSION	7

CHAPITRE II

LA BIOMETRIE ET L'EMPREINTE DIGITALE

II.1 INTRODUCTION.....	9
II .2 QU'EST-CE QUE LA BIOMETRIE ?	9
II .3 POURQUOI LA BIOMETRIE ?.....	9
II.3.1 LES FAIBLES MOTS DE PASSE :	9
II.3.2 LE PARTAGE DES IDENTIFIANTS :	9
II.3.3 CARTES-CLES PERDUES.....	10
II .4 SYSTEMES BIOMETRIQUES.....	10
II.4.1 LES SYSTEMES BIOMETRIQUES PHYSIOLOGIQUE :	11
II.4.1.1 LA FORME DE VISAGE (FACIAL RECOGNITION) :	11
II.4.1.2 RECONNAISSANCE DE L'IRIS (IRIS RECOGNITION) :	12
II.4.1.3 RECONNAISSANCE DE LA VEINE PALMAIRE (PALM-VEIN RECOGNITION).....	13
II.4.2. SYSTEMES BIOMETRIQUES COMPORTEMENTAUX.....	13
II.4.2.1. LA RECONNAISSANCE VOCALE (VOICE RECOGNITION) :	13
II.4.2.2. ANALYSE DES SIGNATURES (SIGNATURE ANALYSIS) :	14
II .5. LES PROBLEMES POSES PAR L'UTILISATION DE LA BIOMETRIE	15
II.6. EMPREINTES DIGITALES	15
II .6.1 HISTORIQUE.....	15
II.6.2 DEFINITION DE L'EMPREINTE DIGITALE.....	16

II .6.3. LES POINTS CARACTERISTIQUES DE L'EMPREINTE DIGITALE	17
II.6.3.1. LES POINTS SINGULIERS GLOBAUX	17
II.8.2 LES POINTS SINGULIERS LOCAUX (MINUTIERS).....	18
II .6.3.2. LES CLASSES DE L'EMPREINTE DIGITALE.....	18
II .7. AMELIORATION DE L'EMPREINTE DIGITALE	19
II.8. RECONNAISSANCE D'EMPREINTES.....	20
II.8.1. LES MINUTIES.....	20
II .9. LES CAPTEURS D'EMPREINTES DIGITALES	22
II .9.1. LES CAPTEURS D'EMPREINTES DIGITALES MACROSCOPIQUES.....	23
II .9.2. CAPTEURS D'EMPREINTES DIGITALES OPTIQUES.....	23
II .9.3. CAPTEURS D'EMPREINTES DIGITALES ULTRASONIQUES.....	24
II .10. LES CAPTEURS INTEGRES D'EMPREINTES DIGITALES.....	25
II .10.1. CAPTEURS INTEGRES CAPACITIF.....	26
II .10.2. CAPTEURS INTEGRES THERMIQUES.....	27
II .10.3. CAPTEURS INTEGRES TACTILES	28
II .11. TRAITEMENT INFORMATIQUE D'UNE EMPREINTE DIGITALE	29

CHAPITRE III

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

III .1 INTRODUCTION.....	33
III.2 SCHEMA SYNOPTIQUE.....	33
III.3 CONCEPTION MATERIELLE	33
III.3.1 HOROLOGE RTC (REAL TIME CLOCK).....	33
III.3.2 KEYPAD :	34
III.3.3 AFFICHEUR LCD :	35
III.3.4 SERVO MOTEUR :	36
III.3.4.1. COMMANDE DU SERVO MOTEUR :	36
III.3.5. LES LEDS	37
III.3.3.6 LES RESISTANCES :	37
III.3.3.7. CAPTEUR D'EMPREINTE DIGITALE	38
III.4 BRANCHEMENTS	39
III.5 CONNEXION MATERIELLE.....	40
III.5.1 ARDUINO UNO :	40
III.5.1.1. CARACTERISTIQUES TECHNIQUES DE LA CARTE ARDUINO UNO :	41
III.5.1.2. SCHEMA SIMPLIFIE DE LA CARTE ARDUINO UNO :	42
III.6. L'ENVIRONNEMENT IDE ARDUINO :	42
III .7. L'INTERFACE :	42
III.8. METHODE D'IDENTIFICATION :	44
III .9. LE SCHEMA COMPLETE DU SYSTEME A L'AIDE DE PROGRAMME PROTUS :	45
III.10. PROGRAMME FRITZING :	45

III.11.ORGANIGRAMME DEFONCTIONNEMENT:	46
III.12. CARTE SD	47
III .12.1 EXERCICE PREALABLE	47
III .12.2 INSTALLATION DE WINIMAGE.....	48
II.12.3. CREATION DU FICHIER IMAGE WINIMAGE	50
III .13. SIMULATION.....	ERROR! BOOKMARK NOT DEFINED.
III .14.RESULTATSPRATIQUES:	55
III .19. LE MONTAGE GLOBAL :	56
CONCLUSION	57
CONCLUSION GENERALE	59
REFERENCES BIBLIOGRAPHIQUES	67

Table des Figures

FIGURE 1 : CARTE DE POINTAGE.....	2
FIGURE 2 : HORLOGE POINÇON.....	2
FIGURE 3 : SYSTEME DE POINTAGE PAR CARTE RFID.....	3
FIGURE 4 : POINTAGE PAR EMPREINTE DIGITALE.....	5
FIGURE 5 : POINTEUSE AVEC UN CONTOUR D'UNE MAIN	5
FIGURE 6 POINTEUSE AVEC LES CONTOURS DE VISAGE	6
FIGURE 7 POINTEUSE D'IRIS	7
FIGURE 8 : SYSTEMES BIOMETRIQUES.....	11
FIGURE 9 : RECONNAISSANCE FACIALE BIOMETRIQUE.....	11
FIGURE 10 : CARACTERISTIQUES DE L'IRIS	12
FIGURE 11 : RECONNAISSANCE PALM-VEIN.....	13
FIG. 12: ETUDE DU DESSIN DIGITAL	17
FIGURE 13 : DIFFERENT POSITION DE DELTA.....	17
FIGURE.14 : LES COUPURES.....	18
FIGURE. 15: LES DIVISIONS.....	18
FIGURE.16: LES ANNEAUX.....	18
FIGURE.17: LES ILOTS.....	18
FIGURE.18: LES FORMES DES CRETES A LA ZONE CENTRALE DE L'EMPREINTE.	19
FIGURE.19 : TROIS TYPES DE DESSINS GENERAUX.....	20
FIGURE.20 : DIVERSES MINUTIES DE CRETE PAPILLAIRE.	21
FIGURE 21 : COMPARAISON DE L'IDENTIFICATION.....	22
FIGURE.22: PRINCIPE DE FONCTIONNEMENT D'UN CAPTEUR D'EMPREINTES DIGITALES OPTIQUE.	24
FIGURE.23: PRINCIPE DEFONCTIONNEMENT D'UN CAPTEUR D'EMPREINTES DIGITALES ULTRASONIQUE AEMETTEUR/RECEPTEUR EN ROTATION.....	25
FIGURE.24: CAPTEUR CAPACITIF UTILISANT DES PIXELS A DOUBLE ELECTRODE	26
FIGURE 25 : CAPTEUR THERMIQUE UTILISANT UNE COUCHE DE MATERIAU PYROELECTRIQUE	27
FIGURE 26 : CAPTEUR THERMIQUE A ELEMENTS CHAUFFANTS.....	28
FIGURE.28: LES PRINCIPALES ETAPES EN IMAGES	30
FIGURE.29: DETERMINATION DE LA DIRECTION DES MINUTIES	31
FIGURE. 30: BROCHAGE (FRITZING) D'ARDUINO YUN AVEC DS1703.....	34
FIGURE 32 : CABLAGE DE LCD I2C AVEC LA CARTE ARDUINO.....	36
FIGURE 34 SIGNAL DE COMMANDE DE MOTEUR SERVO.....	37
FIGURE 35: LED	37
FIGURE 36 : LES RESISTANCES	38
FIGURE. 37: CAPTEUR OPTIQUE D'EMPREINTE DIGITALE POUR ARDUINO.....	38
FIGURE. 38: LES BROCHES D'UN CAPTEUR D'EMPREINTE DIGITALE.....	39

FIGURE 39 : LES PINS E/S D'UNE CARTE ARDUINO UNO.	41
FIGURE 40 : SCHEMA SIMPLIFIE DE LA CARTE ARDUINO UNO.	42
FIGURE 41: LA FENETRE DE L'ATELIER ARDUINO SOUS WINDOWS.	44
FIGURE 42 : LE SCHEMA COMPLETE DU SYSTEME SOUS PROTUS.	45
FIGURE 43 : LE SCHEMA COMPLET DU SYSTEME A L'AIDE DE PROGRAMME DE SIMULATION FRITZING	46
FIGURE44:ORGANIGRAMMEDESISTEME DE POINTAGE.....	46

Introduction Générale

Introduction générale

INTRODUCTION GENERALE

Les progrès technologiques en biométrie d'empreintes digitales ouvrent de nouvelles opportunités dans les différents environnements dans lesquels elle s'applique, en s'adaptant aux besoins de chaque moment et chaque personne. Un point commun pour les différentes options de sécurité c'est qu'il doit être facile à utiliser et facile à installer.

Les progrès réalisés dans la technologie biométrique d'empreintes digitales nous montrent la grande variété d'applications et des systèmes que la biométrie d'empreintes digitales offre, en particulier pour l'accès logiques physique aux bureaux et aux lieux de travail.

Parmi ces système le système de pointage avec l'empreinte digitale ce qui contribue à déterminer avec précision les heures d'entrées et de sortie du lieu de travail de manière plus sécurisé.

Le système de pointage détermine le temps d'entrée et de sortie du lieu de travail de chaque travailleur soit par le mot de passe personnel au soit via l'empreinte digitale (capteur d'empreinte digital).

Pour réaliser ce système de pointage nous avons besoin d'un capteur d'empreinte digitale et une carte « ARDUINO UNO » qui donne la possibilité d'assembler les performances de programmation et d'électronique.

Le mémoire est divisé en trois chapitres :

- Le premier chapitre représente les systèmes pointage.
- Le deuxième chapitre est une étude sur la biométrie et d'empreinte digitale
- Le dernier chapitre présente la méthode de la conception et la réalisation de ce projet.

Chapitre I :

Systèmes dePointage

I.1 Introduction

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

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

I.2 Différents systèmes de pointage

Il existe différents types du système de pointage :

I.2.1 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 1 : Carte de pointage

I .2.2 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 : Horloge poinçon

I.2.3 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 3 : Système de pointage par carte RFID

I.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.

I.3 Avantage de pointage biométrique

Système de pointage utilisant la technologie de biométrie.

- ✓ 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).

I.4 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.

I.4.1 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 4 : Pointage par empreinte digitale

I.4.2 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 5 : Pointeuse avec un contour d'une main

I.4.3 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 6 Pointeuse avec les contours de visage

I.4.4 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 7 Pointeuse d'iris

I .5 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 cas comme dans le deuxième cas, le dispositif doit être relié à un logiciel de gestion, qui enregistrera et traitera les données

Chapitre II : la biométrie et l`empreinte digitale

II.1 Introduction

Les caractéristiques comportementales et physiologiques sont régulièrement utilisées pour vérifier ou déterminer manuellement l'identité – c'est quelque chose que 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.

II .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.

II .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 :

II .3.1 Les faibles mots de passe :

Les utilisateurs d'ordinateur en particulier tendent à utiliser des mots de passes faciles 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.

II .3.2 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.

II .3.3 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.

II .4 Systèmes biométriques

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

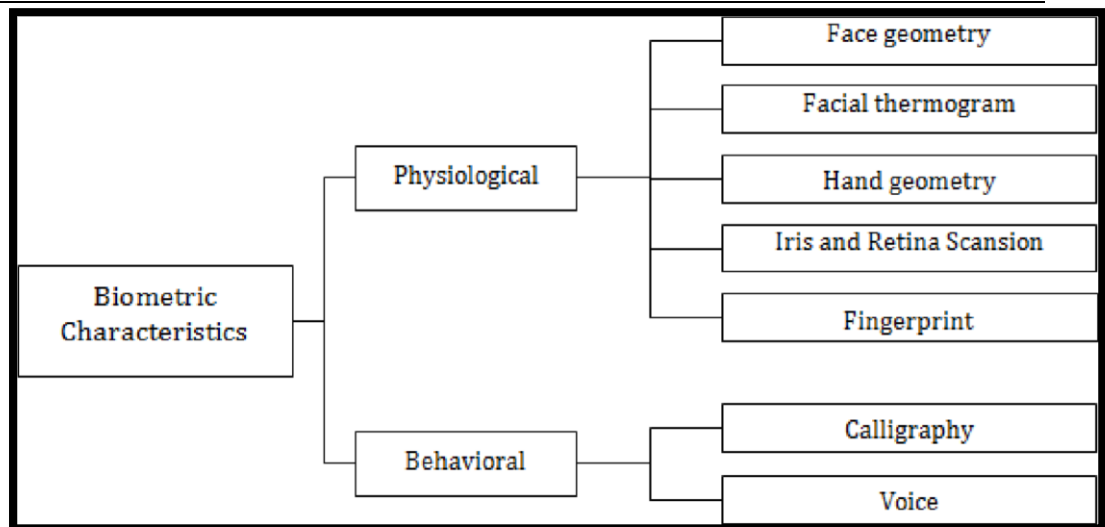


Figure 8 : Systèmes biométriques

II.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 :

II.4.1.1 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*).

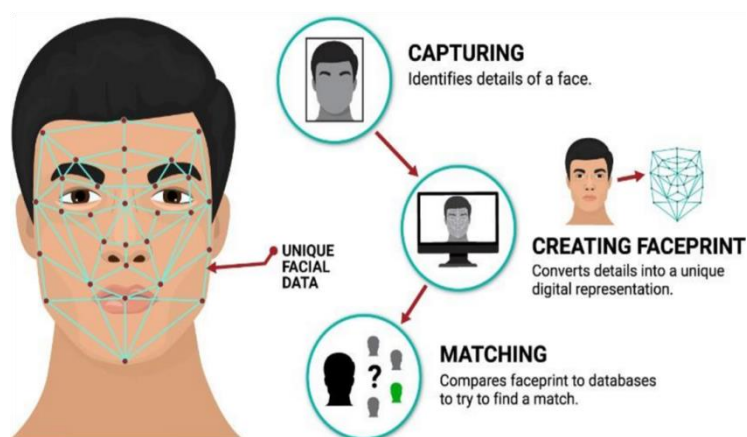


Figure 9 : reconnaissance faciale biométrique

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

II .4.1.2 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

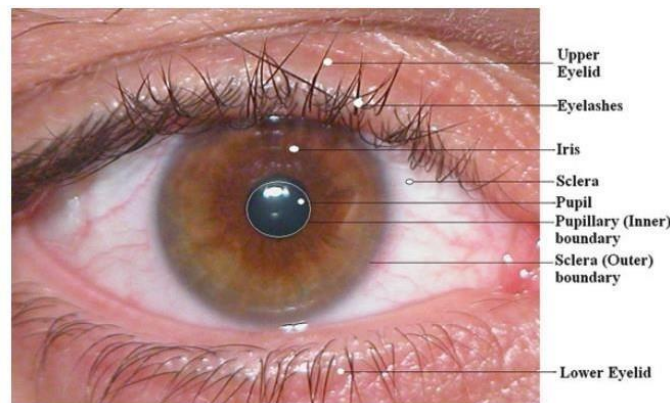


Figure 10 : caractéristiques de l'iris

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.

II.4.1.3 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.

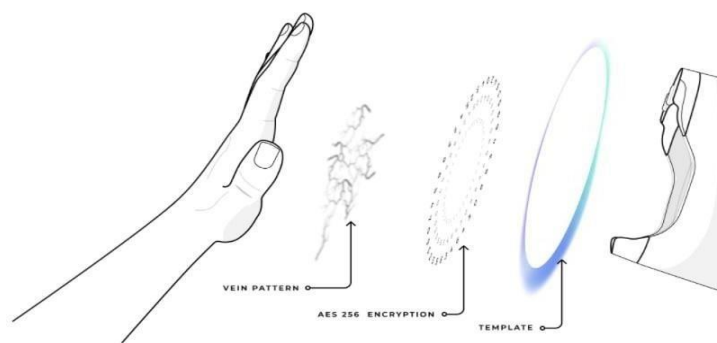


Figure 11 : Reconnaissance Palm-Vein

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 au visage, le motif de la veine de la paume est interne.

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.

II.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 les plus courants sont :

II.4.2.1. 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.

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.

II.4.2.2. 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.

II .4.2.3 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.

II .5. Les problèmes posés par l’utilisation de la biométrie

Dans les systèmes biométriques la phase finale d’appariement estime le degré de similitude (taux d’appariement) entre deux fichiers signatures et le compare à un seuil fixé à l’avance, ainsi le résultat n’est jamais fiable à 100% mais en approche selon le réglage du seuil.

Les systèmes biométriques posent aussi des problèmes de sécurité car il n’est jamais vérifié que les données biométriques en entrée proviennent de leur réel possesseur. En effet les moyens de flouer un tel système existent, et de plus les caractères biométriques ne sont pas secrets. Il est relativement facile de se procurer une photo du visage, une empreinte digitale ou un enregistrement audio d'une personne.

II.6. Empreintes digitales

II .6.1 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 XVI^e 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 XX^e 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.

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.

II.6.2 Définition de l’empreinte digitale

L’empreinte digitale scientifiquement est composée des crêtes qui contiennent des pores et des sillons, et les pores permettent de sortir 80% d’eau et 20% de matières organiques, ces matières laissent des marques sous forme de lignes.

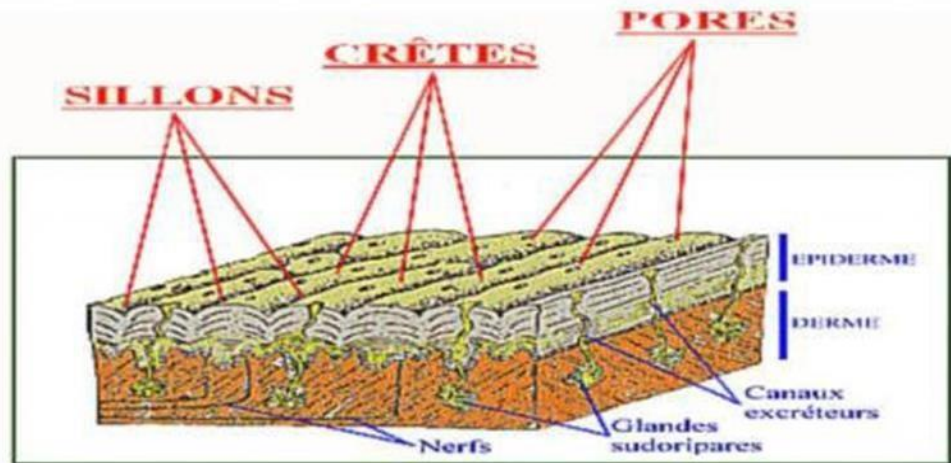


Fig. 12: Etude du dessin digital .

II .6.3. Les points caractéristiques de l'empreinte digitale

Les points caractéristiques ou les crêtes sont utilisées pour différencier deux empreintes digitales et aussi faire une classification selon les points singuliers globaux et les points singuliers locaux.

II.6.3.1. Les points singuliers globaux

On distingue les points caractéristiques globaux par le Core et le Delta.

- **Le Core** : centre ou le noyau contient de courbure maximale des lignes del'emprei
- **Le Delta** : est proche du lieu où se deux lignes, aussi est le lieu de divergence des lignes les plus internes.

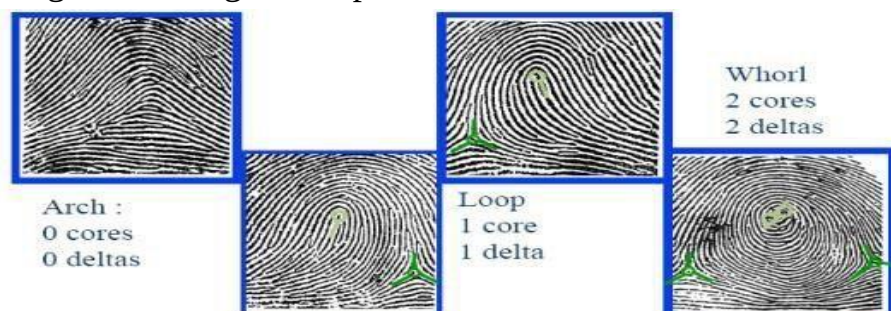


Figure 13 : different position de delta

II.8.2 Les points singuliers locaux (minutiers)

En chaque empreinte il y a des minuties spécifiques permettent de différencier et classer les empreintes, et il ya plusieurs formes des minutiers généralement on a quatre types :

Les coupures : terminaison à droite ou à gauche, minuties située en fin de.

- **Les divisions :** Bifurcation à droite ou à gauche, intersection de deux stries.

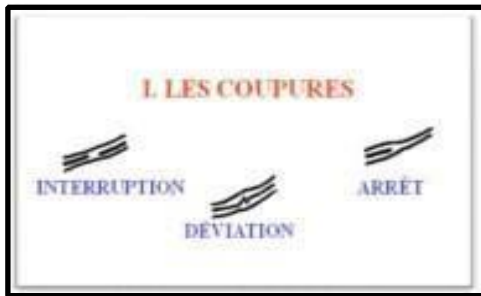


Figure.14 : Les Coupures...

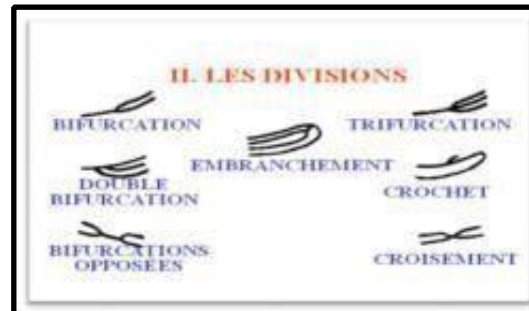


Figure. 15:Les Divisions

- **Les anneaux :** Lac, assimilée à deux bifurcations.
- **Les îlots:** assimilés à deux terminaisons.

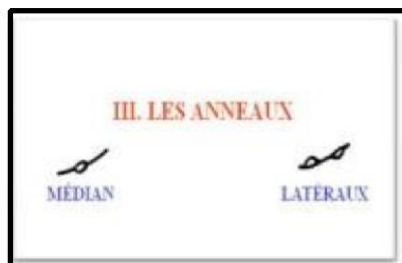


Figure.16:Les Anneaux

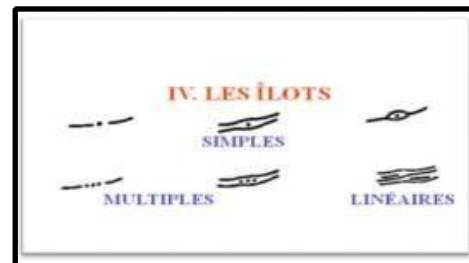


Figure.17:Les îlots

II .6.3.2. Les classes de l'empreinte digitale

Français Galton (1822-1916) ont été faites les premières études scientifiques sur les classifications des empreintes digitales, ces études ont affiné par Edward Henry (1850-1931), il est classé les empreintes en cinq classes : arc, arc tendu, boucle à gauche, boucle à droite, et spire.

- **Classe 1:** il contient en maximum un Delta et au moins une crête montre une courbure élevée, est une classe poubelle.
- **Classe 2:** il contient un Delta à droite et des boucles situés en côté à gauche de l'empreinte.

- **Classe 3:**il contient un Delta à gauche et des boucles situé en côté à droite del'empreinte.
- **Classe 4:**il contient un Delta à gauche et d'autre à droite avec un centre spirale.
- **Classe 5:**il contient trois Delta autour de forme besace.
- **Classe 6 :**il contient des empreintes invisibles.

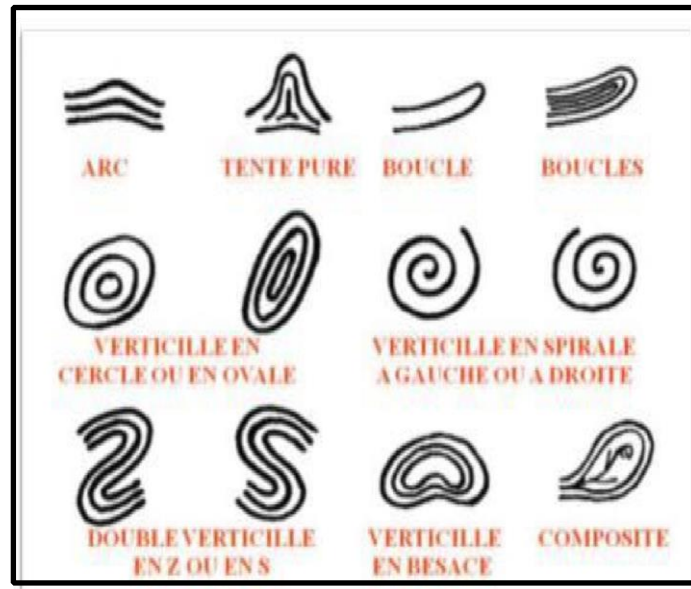


Figure.18: Les formes des crêtes à la zone centrale de l'empreinte.

II .7. Amélioration de l'empreinte digitale

Pour améliorer la reconnaissance des empreintes digitales il faut d'abord faire un traitement l'empreinte, ce traitement prendre l'empreinte digitale comme une image numérique. Dans un côté informatique c'est quoi une image numérique ?

On peut représenter l'image numérique comme une interface divisé dans ensembles des cellules appelée pixels de tailles fixes et chaque pixel a une couleur correspond à l'image réel. Et on générale l'image numérique définie par un ensemble de pixels situé dans un espace limité par une hauteur et largeur. Le dynamique de l'image chaque pixels pendre teintes de gris ou des couleurs.

II.8. Reconnaissance d'empreintes

II.8.1. les minuties

La surface de la peau des doigts est pourvue d’une texture particulière, continuellement striée par des crêtes, qui permettent d’accroître le pouvoir agrippant des mains. Les crêtes sont parsemées de petits orifices, les pores, par lesquels s’écoule la sueur. Celle-ci, mélangée à des sécrétions grasses, laisse des traces lorsque les doigts sont appliqués sur une surface propre. Ces traces, appelées empreintes, sont uniques et caractéristiques de chaque individu. Même les vrais jumeaux présentent des empreintes digitales différentes. Elles peuvent donc être utilisées pour identifier une personne.

L’étude d’une empreinte digitale commence par l’observation de sa forme générale. Le but est de classer l’empreinte étudiée en trois grandes familles

- **empreinte en boucle** : les lignes se replient sur elles-mêmes, soit vers la droite, soit vers la gauche (motif courant).
- **empreinte en verticille** : présence de lignes qui s’enroulent autour d’un point enformant une sorte de tourbillon.
- **empreinte en arc** : les lignes sont disposées les unes au-dessus des

Une fois la forme générale de l’empreinte déterminée, on peut alors passer à une étude plus précise qui consiste à prendre en compte les détails, appelés minuties, visibles sur l’empreinte. La figure ci-dessous présente quelques-unes des minuties repérables.



Figure.19 : Trois types de dessins généraux

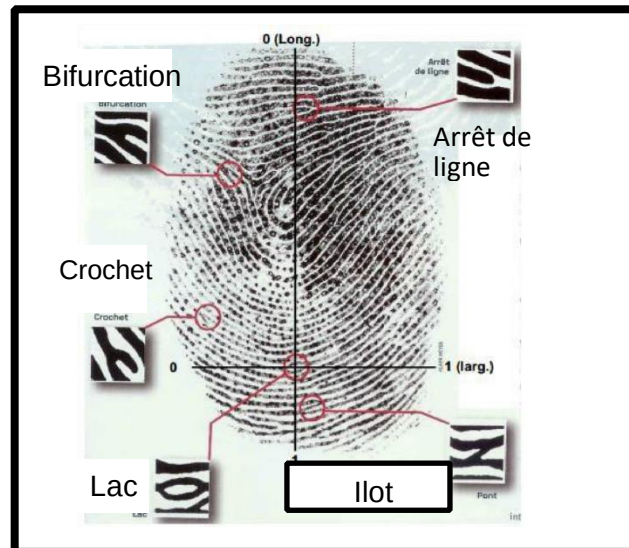


Figure.20 : Diverses minuties de crête papillaire.

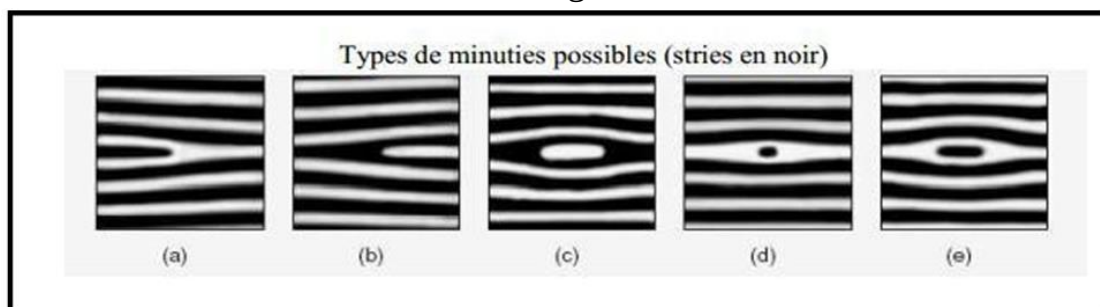
L'association des minuties ainsi que leur localisation rend l'empreinte unique : c'est ce qui permet d'attribuer une empreinte digitale à un individu.

On peut relever jusqu'à seize types de minuties mais dans les algorithmes on n'en retient généralement que quatre types:

- Terminaison à droite ou à gauche (minutie située en fin de strie):figure a.
- Bifurcation à droite ou à gauche (intersection de deux stries) : figure b.

On peut citer également :

- Île : assimilée à deux terminaisons : figure d et e.
- Lac : assimilée à deux bifurcations : figure c.



Pour pouvoir obtenir des images numériques de ces empreintes, nous avons besoin d'un capteur d'empreintes digitales. Le principe de l'application est assez simple. L'individu pose son doigt sur le capteur, scanne et capture l'image de l'empreinte. L'image capturée représente toutes les lignes de crêtes du doigt en contact direct sur le capteur.

C’est à partir de l’image capturée que les minuties sont extraites, donc la qualité de l’image est un point aussi déterminant que les éléments à extraire.

Différents facteurs jouent sur la qualité de l’image, la pression que l’on exerce sur le capteur, la lumière ambiante lors du scan du doigt, les doigts abîmés ou sales.

L’image capturée subira divers traitements (contraste, filtrage, érosion, dilatation, binarisation, squelettisation) permettant ainsi de pouvoir mieux définir et extraire les minuties.

L’extraction des minuties est le processus final qui complète l’obtention de la "signature" de l’empreinte appelée gabarit. Le "gabarit" retenu pour caractériser l’empreinte est basé sur un ensemble suffisant et fiable de minuties, qui sera comparé et permettra l’identification.

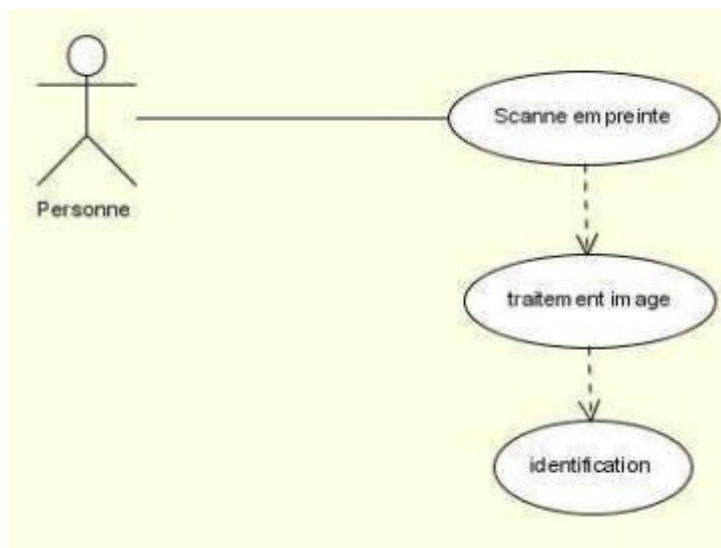


Figure 21 : comparaison de l’identification

II .9. Les capteurs d’empreintes digitales

Les capteurs d’empreintes digitales sont à l’heure actuelle les capteurs biométriques les plus employés. En effet la saisie de l’empreinte digitale est relativement simple et rapide pour l’utilisateur qui n’a, le plus souvent, qu’à poser ou passer son index (ou plus rarement son pouce) sur la surface active du système de capture. De plus la saisie de l’empreinte digitale se heurte à très peu de freins psychologiques, cette pratique d’identification étant utilisée par les services de police depuis longtemps. En outre les travaux concernant

le traitement et la Reconnaissance de l’empreinte sont nombreux et les algorithmes éprouvés.

Les capteurs d’empreintes sont certainement les seuls capteurs biométriques pouvant être intégrés au sein d’un système monolithique réalisé sur un unique substrat semiconducteur. Cette particularité fait que ce genre de capteur peut être produit de manière collective en très grand nombre et à très bas prix en utilisant les technologies microélectroniques et microsystèmes actuelles. Ces capteurs réalisés selon cette voie sont normalement dénommés sous le terme de capteurs intégrés à contrario des capteurs dits macroscopiques incorporant des éléments optiques ou mécaniques.

II .9.1. Les capteurs d'empreintes digitales macroscopiques

On rencontre principalement deux types de capteurs d'empreintes digitales macroscopiques qui sont soit de type optique, soit de type ultrasonique. Quel que ce soit leur mode de fonctionnement, ces systèmes procèdent tous à l’acquisition de l’image de l’empreinte sans que l’utilisateur ait besoin d’opérer avec son doigt un mouvement de translation à la surface du capteur.

II .9.2. Capteurs d'empreintes digitales optiques

La majorité des capteurs d'empreintes digitales optiques exploitent la modification de l'indice de réflexion de la surface d'un prisme lorsque les reliefs du doigt sont en contact avec cette dernière.

De nombreux systèmes de ce type sont actuellement commercialisés par des sociétés comme Identix Du fait de l'utilisation de lentilles et de capteurs optiques intégrés (capteurs matriciels de type CCD ou APS), ces capteurs sont relativement encombrants et d'un coût généralement élevé (de l'ordre de 100 € à 1000 € environ). De plus ils sont relativement fragiles et d'un assemblage mécanique peu commode rendant difficile leur intégration au sein d'un système portable.

L'image issue de ces capteurs possède généralement une définition de l'ordre de 500 dpi (dpi : dot per inch) et souffre de plusieurs défauts. En effet l'image, qui possède peu de contraste, peut être facilement parasitée par les poussières et autres salissures (notamment les traces résiduelles d'empreintes) qui peuvent être en contact avec la face du prisme devant accueillir le doigt de

l'utilisateur. De plus l'écrasement du doigt à la surface du capteur induit une distorsion de l'image parfois importante qui peut soulever différents problèmes lors de la phase d'appariement de l'empreinte digitale.

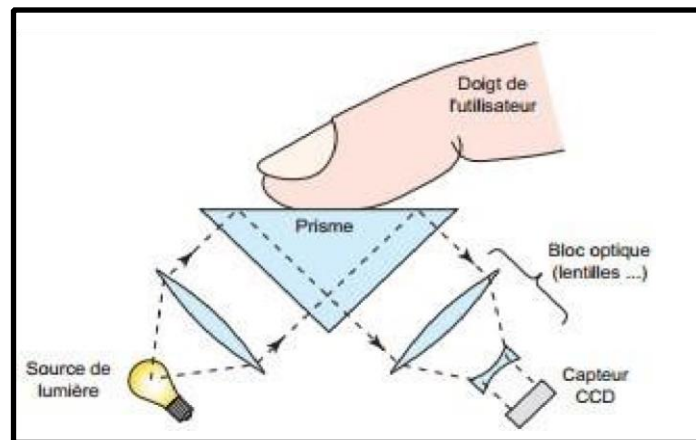


Figure.22: Principe de fonctionnement d'un capteur d'empreintes digitales optiques.

Malgré ces défauts, les capteurs d'empreintes digitales optiques sont à l'heure actuelle les systèmes macroscopiques les plus utilisés et les plus aboutis.

II.9.3. Capteurs d'empreintes digitales ultrasoniques

En 1986, une méthode basée sur l'échographie ultrasonore de la surface du doigt a été proposée afin de pratiquer l'acquisition de l'empreinte digitale. Ce système se base sur le principe qu'une onde ultrasonore est en partie réfléchi lors du passage d'un milieu physique à un autre. Ici, les deux milieux physiques mis en jeu sont la surface du capteur et la surface du doigt de l'utilisateur.

Afin de déterminer l'image de l'interface entre ces deux milieux et donc l'image de l'empreinte, le système utilise un émetteur/récepteur d'ultrasons en rotation qui permet d'obtenir la signature de l'écho sous différents angles (généralement 256 positions fixes). A partir de ces données, l'image de l'empreinte digitale peut alors être recomposée grâce à un traitement informatique approprié. Le principe de fonctionnement est illustré sur la Figure 9. Notons que l'émetteur/récepteur en rotation peut être avantageusement remplacé par différents émetteurs/récepteurs fixes convenablement disposés. [16]

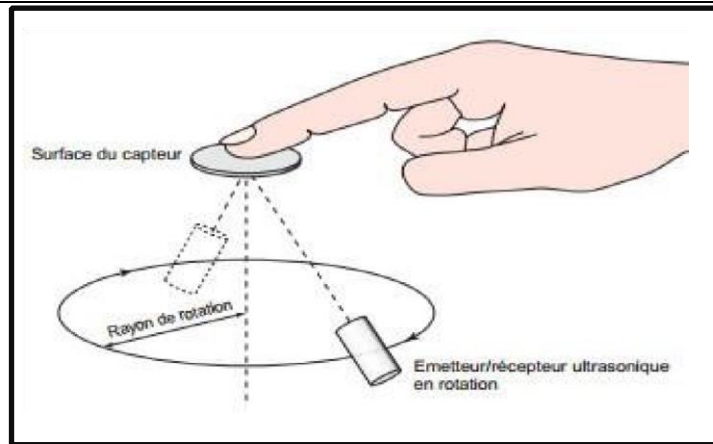


Figure.23: Principe de fonctionnement d'un capteur d'empreintes digitales ultrasonique à émetteur/récepteur en rotation

Ce genre de capteur possède de nombreux avantages comme une très grande immunité vis-à-vis des salissures présentes à la surface du capteur ainsi qu'une très grande définition qui, dans le cas de certains systèmes commercialisés, atteint 1000 dpi. La haute définition de l'image scannée peut permettre l'identification de personnes dont l'empreinte se compose de sillons extrêmement fins comme c'est le cas chez les enfants par exemple. On a montré qu'il était possible avec ces capteurs d'identifier des enfants de moins de cinq ans, ce qui a motivé les autorités Sud-Africaines afin d'adopter ce système pour des applications de Sécurité Sociale.

II .10. Les capteurs intégrés d'empreintes digitales

La quasi-totalité des capteurs d'empreintes digitales intégrés commercialisés à l'heure actuelle sont, soit de type capacitif, soit de type thermique. Les capteurs utilisant d'autres modes d'acquisition tels que les capteurs tactiles (cas des capteurs réalisés dans le cadre de ce travail de thèse) sont encore marginaux notamment à cause des problèmes soulevés par leur mise en boîtier.

Les capteurs intégrés, au contraire des capteurs macroscopiques, peuvent être d'une part classés suivant le principe physique utilisé pour effectuer la saisie de l'empreinte digitale mais également suivant leur géométrie. En effet, la surface active du capteur est susceptible de prendre trois configurations différentes suivant que les pixels sont disposés en ligne (en fait une ou plusieurs) ou en matrice qui peut alors être soit totale, soit partielle.

Les capteurs intégrés, au contraire des capteurs macroscopiques, peuvent être d'une part classés suivant le principe physique utilisé pour effectuer la saisie de l'empreinte digitale mais également suivant leur géométrie. En effet, la surface active du capteur est susceptible de prendre trois configurations différentes suivant que les pixels sont disposés en ligne (en fait une ou plusieurs) ou en matrice qui peut alors être soit totale, soit partielle.

II .10.1. Capteurs intégrés capacitif

Les capteurs intégrés capacitifs sont à l'heure actuelle les systèmes les plus aboutis et les plus économiquement viables car pouvant être facilement réalisés sur la base de technologies microélectroniques standards. Comme nous allons le voir dans la suite, il existe plusieurs types de capteurs capacitifs qui utilisent soit une, soit deux électrodes de mesure par pixel. Ces capteurs procèdent à l'acquisition de l'empreinte en mesurant soit les perturbations locales du champ électrique (pixel à double électrode), soit la variation de capacité entre l'électrode de mesure (électrode unique) et la peau suivant que cette dernière est en contact ou non avec la surface du système.

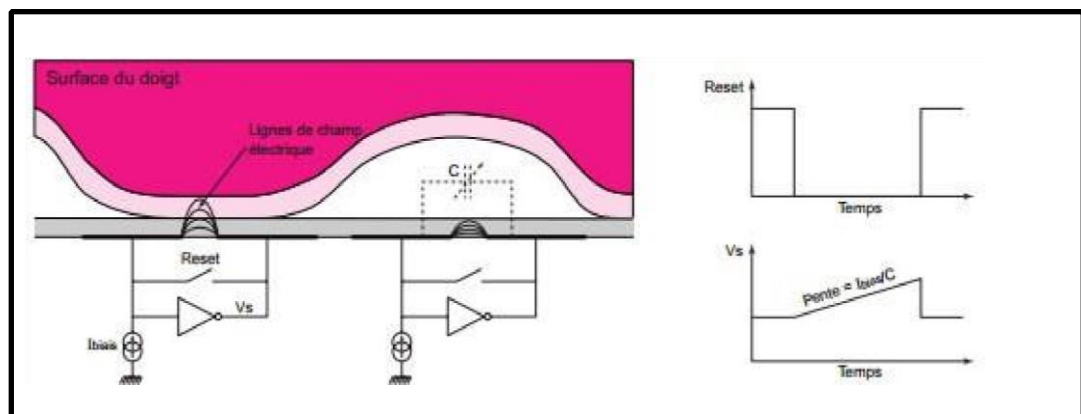


Figure.24: Capteur capacitif utilisant des pixels à double électrode

Afin de mesurer les variations de capacité électrique entre les deux électrodes, le condensateur ainsi formé est, dans le cas présenté ici, utilisé comme boucle de contre-réaction au sein d'un circuit intégrateur. Lors de la mesure, le commutateur *reset* est ouvert de telle sorte que la capacité formée par les deux électrodes se charge à courant constant. Suivant la pente de la tension disponible en sortie de l'inverseur, il est ainsi possible de déterminer la valeur de la capacité électrique existante entre les deux électrodes et par conséquent de conclure sur la présence ou non du relief du doigt en contact avec la surface du capteur. Notons qu'il existe de nombreuses autres architectures de circuits pouvant être utilisées afin de mesurer la variation de

capacité électrique. [16] L’un des avantages de ce type de capteur est qu’il n’y a pas de contact électrique entre le capteur et le doigt puisque il n’est en aucun cas nécessaire de polariser ce dernier, facilitant ainsi grandement la mise en boîtier du système. Malheureusement, la qualité des images issues de ces capteurs laisse quelques fois à désirer. En effet, afin d’extraire l’image de l’empreinte, ces systèmes mesurent les perturbations du champ électrique provoquées essentiellement par la partie la plus externe de l’épiderme qui est souvent fortement altérée par des microcoupures. De plus, ces capteurs sont fortement sujets au phénomène de *cross-talk* entre pixels adjacents, réduisant ainsi la définition effective de l’image obtenue.

Le deuxième type de capteurs intégrés capacitifs pallie à ce défaut en exploitant les couches les plus internes de la peau afin de procéder à l’acquisition de l’empreinte digitale. Ce type de capteurs utilise une seule et unique électrode de mesure par pixel, la deuxième électrode nécessaire à la formation.

II .10.2. Capteurs intégrés thermiques

La société Atmel commercialise depuis quelques années un capteur intégré d’empreintes digitales thermique. Le principe de fonctionnement de ce capteur repose sur le fait que les zones de l’empreinte digitale en contact avec la surface du système (les stries) réchauffent localement cette dernière. Afin de déterminer l’élévation de température, ce capteur utilise une couche de matériau pyroélectrique déposée entre une électrode de référence et une électrode de mesure (une par pixel). Lorsque le matériau pyroélectrique subit une élévation de température imputable à la présence du doigt, une différence de potentiel électrique apparaît entre les deux électrodes permettant ainsi la mesure.

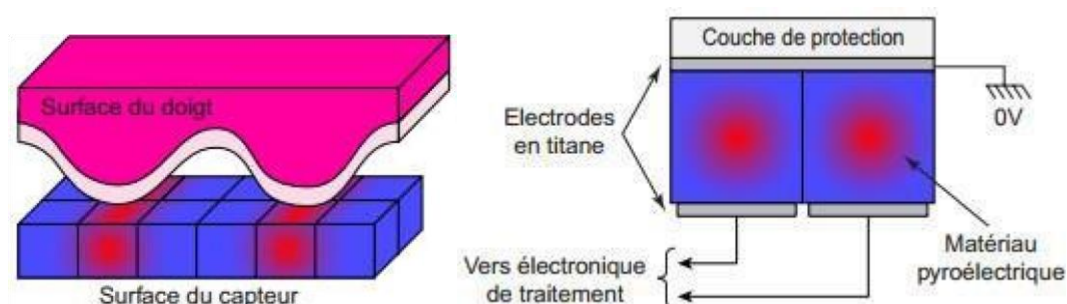


Figure 25 : Capteur thermique utilisant une couche de matériau pyroélectrique

Outre le fait que ces capteurs nécessitent l’emploi de technologies non standard et donc chères, ces derniers souffrent de différents désavantages nuisant à la qualité de l’image obtenue. Ainsi, l’acquisition de l’image doit se dérouler durant un laps de temps relativement court (inférieur à la seconde) afin que l’équilibre thermique au niveau de la surface active du capteur ne soit pas atteint (homogénéisation de la température et donc du signal). De plus, ces capteurs nécessitent d’être réchauffés si la température du milieu dans lequel ils se trouvent, descend en dessous d’un certain seuil. Cette nécessité rend ce type de capteur totalement inutilisable dans le cadre de système basse consommation comme c’est le cas avec les applications portables.

Des travaux ont montré qu’il était possible de réaliser des capteurs d’empreintes digitales thermiques en utilisant une matrice d’éléments chauffants. Ces capteurs utilisent le fait que la déperdition de chaleur est plus importante au niveau des pixels en contact avec la surface du doigt (la température de ces derniers est donc moins importante). La Figure 18 illustre le principe de fonctionnement de ce capteur. Dans le cas présenté ici, les éléments chauffants sont des résistances électriques réalisées en silicium monocristallin qui sont suspendues au-dessus du substrat afin de limiter les déperditions de chaleur parasites par l’intermédiaire du substrat. Aucun capteur utilisant ce principe n’est à l’heure actuelle commercialisé.

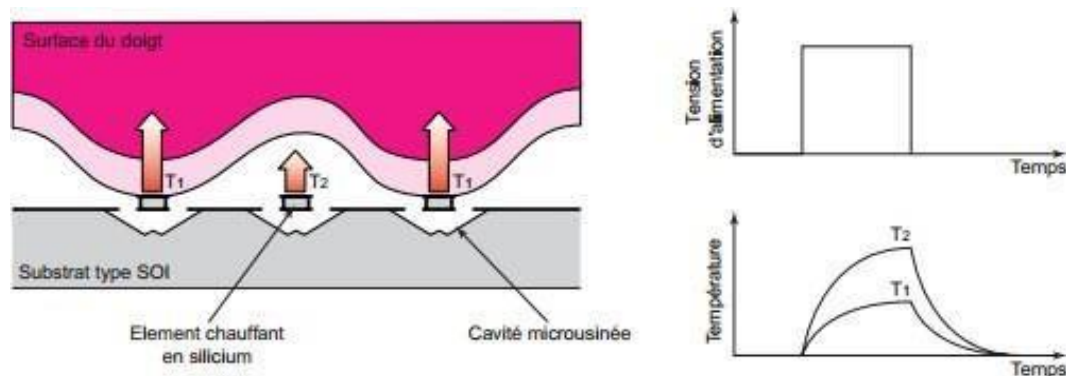


Figure 26 : Capteur thermique à éléments chauffants

II .10.3. Capteurs intégrés tactiles

Historiquement, les capteurs tactiles d’empreintes digitales ont été les premiers à donner lieu à des prototypes mais aucun d’entre eux n’a encore été commercialisé du fait de leur relative fragilité et des problèmes liés à leur mise en boîtier. [16]

La Figure 27 illustre le cas d'un capteur tactile à détection capacitive. Le capteur présenté ici se compose d'une matrice de plaques de silicium monocristallin (une par pixel) maintenues au-dessus du substrat par deux bras de suspension de type *crab-leg*. Les plaques ainsi suspendues forment l'électrode supérieure d'une structure capacitive pouvant se déformer sous l'action mécanique du doigt posé à la surface du capteur. L'électrode inférieure est ici réalisée par le biais d'un dépôt métallique suivi d'une étape de lithographie. L'adressage du pixel actif est réalisé suivant un mode x-y, les électrodes inférieures et supérieures étant connectées en ligne. Notons que ce prototype n'intègre pas d'éléments électroniques permettant le conditionnement du signal, les différentes étapes technologiques nécessaires étant irréalisables sur la base d'un circuit de type VLSI.

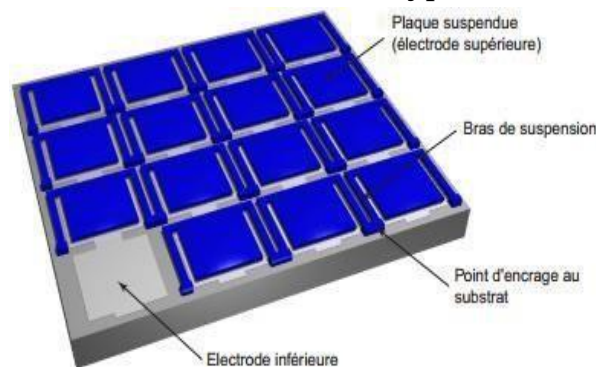


Figure.27:Exemple de capteur d'empreintes digitales tactile

D'autres travaux ont montré qu'il était possible d'obtenir des microstructures capacitives réalisées par le biais d'étapes basse température (300°C maximum) permettant ainsi de réaliser le capteur sur la base d'un circuit CMOS. Les pixels ainsi réalisés possèdent un pas inférieur à 50 μm (résolution supérieure à 500 dpi) et sont constitués d'une membrane déformable de nitrure de silicium (Si_3N_4).

II .11. Traitement informatique d’une empreinte digitale

Différents procédés que nous ne développerons pas ici permettent l'acquisition c'est à dire la capture de l'empreinte.

L'image d'origine est binarisée (noir et blanc) puis squelettisée (les stries ont toutes la même épaisseur de 1 pixel).

On peut ensuite grâce à différents algorithmes extraire les minuties et éjecter les « fausses ». On récupère ainsi en moyenne une centaine de minuties par empreinte. On obtient alors la signature de l’empreinte.

D’une manière générale on distingue deux catégories d’algorithmes de reconnaissance d’empreintes digitales : la première catégorie concerne les algorithmes plutôt « conventionnels » qui s’appuient sur la position relative des minuties entre elles, alors que la seconde regroupe les algorithmes visant à extraire d’autres particularités de l’empreinte digitale telles que la direction locale des sillons, ou encore les composantes fréquentielles locales de la texture au cœur de l’image.

L’approche retenue, appartenant à la première catégorie, est celle proposée par A.K Jain qui est vraisemblablement la plus connue. On réalise successivement le filtrage directionnel et la binarisation de l’image, la squelettisation des sillons (voir figure ci-dessous), puis on détermine la position des minuties au sein de l’image pour quantifier les caractéristiques de ressemblance entre deux gabarits par « point pattern matching ».



Figure.28: Les principales étapes en images .

Le premier algorithme de traitement des images d’empreintes permet de s’affranchir du bruit lié à la mesure, perturbations désignées sous le terme de bruit image (provenant essentiellement de l’imperfection de la peau et des poussières entre le doigt et le capteur), mais aussi de mettre en évidence l’information relative aux sillons en les synthétisant sous forme filaire par leur squelette. La méthodologie globale retenue pour ce prétraitement est tout à fait classique. Chaque minutie est repérée et répertoriée comme suit :

- Le type de minutie : bifurcation ou terminaison.
- La position de la minutie dans l'image : coordonnées (x; y).
- La direction du bloc local associé à la strie : θ .

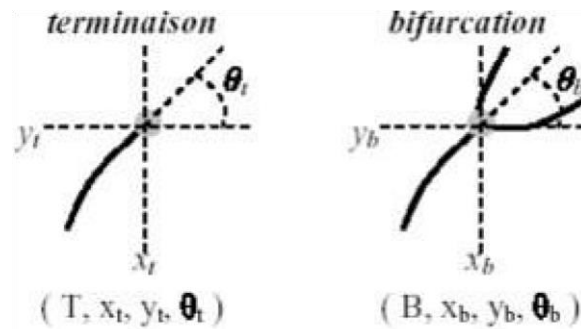


Figure.29: détermination de la direction des minuties.

Cette étape permet alors **le stockage** de la signature intégrée ensuite dans une base de données au moyen d'une technique d'archivage c'est **la classification**. Ce fichier a une taille inférieure à 0,5 Ko ce qui est un gain de mémoire non négligeable par rapport au stockage d'images consommatrices de Ko.

Conclusion :

La biométrie aide à résoudre un bon nombre des problèmes des systèmes de contrôle d'accès actuels tel que : Faiblesse des mots de passe, piratage des identifiants, perte des clés ou des cartes personnel.

Les systèmes biométriques peuvent être conçus en deux classes : physiologiques (reconnaissance faciale, l'Iris de l'œil humaine, la veine palmaire, ...) et comportementales (reconnaissance : vocale et de frappe,..)

Une définition et une classification de l'empreinte digitale est présentées dans ce chapitre, ainsi un aperçu sur les techniques de reconnaissance, le traitement informatique et les différents capteurs utiles pour la détection digitale de l'empreinte biométrique.

Chapitre III :

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

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

III .1 Introduction

Ce chapitre présente les étapes de conception de notre projet ; le fonctionnement de chaque composant nécessaire à notre système de pointage qui a base d'un capteur d'empreinte et une carte ARDUINO UNO, une carte SD, un clavier et un afficheur LCD sont connecte pour la bonne gestion du système.

III.2 Schéma Synoptique :

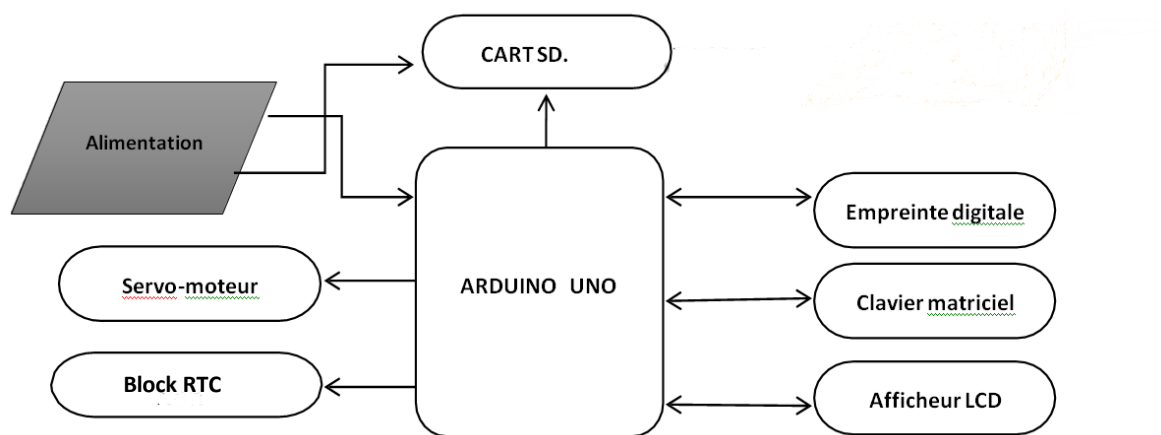


Schéma synoptique de notre système de pointage

III.3 Conception Matérielle :

III.3.1 Horloge RTC (REAL TIME CLOCK)

L'horloge temps réel (aussi connue sous l'acronyme RTC pour Real Time Clock) équipée d'une pile pour rester à l'heure même lorsque votre projet est hors tension ou pendant que vous reprogrammez votre microcontrôleur. C'est une horloge numérique autonome qui donne l'heure quand on la lui demande. Ce genre d'horloge est très utile dans des projets de mesure de grandeurs physiques avec horodatage par exemple

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

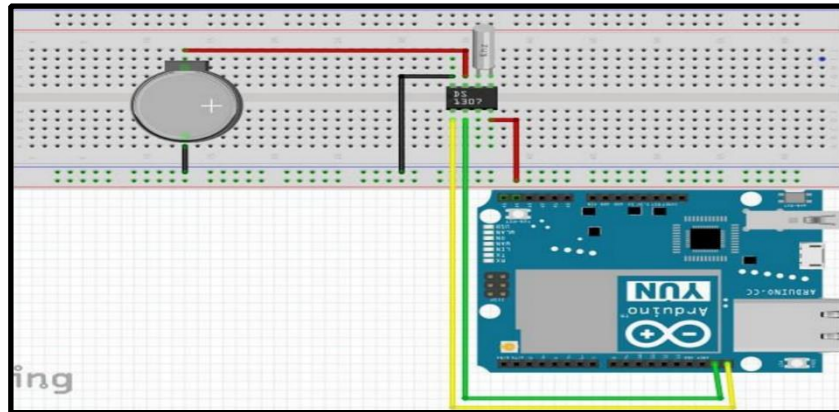


Figure. 30: Brochage d'Arduino YUN avec DS1703(avec fritzing)

Ce module RTC est capable de gérer l'heure (heures, minutes, secondes) et la date (jours, mois, année) tout en s'occupant des mois de 30 ou 31 jours, des années bissextiles, etc. Le calendrier intégré dans le module DS1307 est valable de l'an 2000 à l'an 2100, ce qui devrait être suffisant pour la plupart des projets.

Le module dérive de quelques secondes par jours en moyenne. Cela dépend de la température ambiante et de la qualité du quartz d'horloge. La communication avec le microcontrôleur maître se fait via un bus I²C. Le module dispose de tout le nécessaire pour garder en mémoire l'heure en cas de coupure d'alimentation grâce à une simple pile externe.

Le module DS1307 ne dispose pas de fonctionnalité "alarme" contrairement à d'autres modules RTC plus haut de gamme. Le module DS1307 dispose cependant d'une sortie "base de temps" permettant d'avoir un signal logique à une fréquence fixe (1 Hertz par exemple) pour faire fonctionner un circuit ou un compteur externe. Cela peut être utile dans certaines applications.

III.3.2 Keypad :

Le clavier est l'unité de saisie du code secret pour ouvrir la porte, de clavier à utiliser est un clavier 8 broches 4x4 (4 rangées 4 points) Il est connecté à l'Arduino comme suit :

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

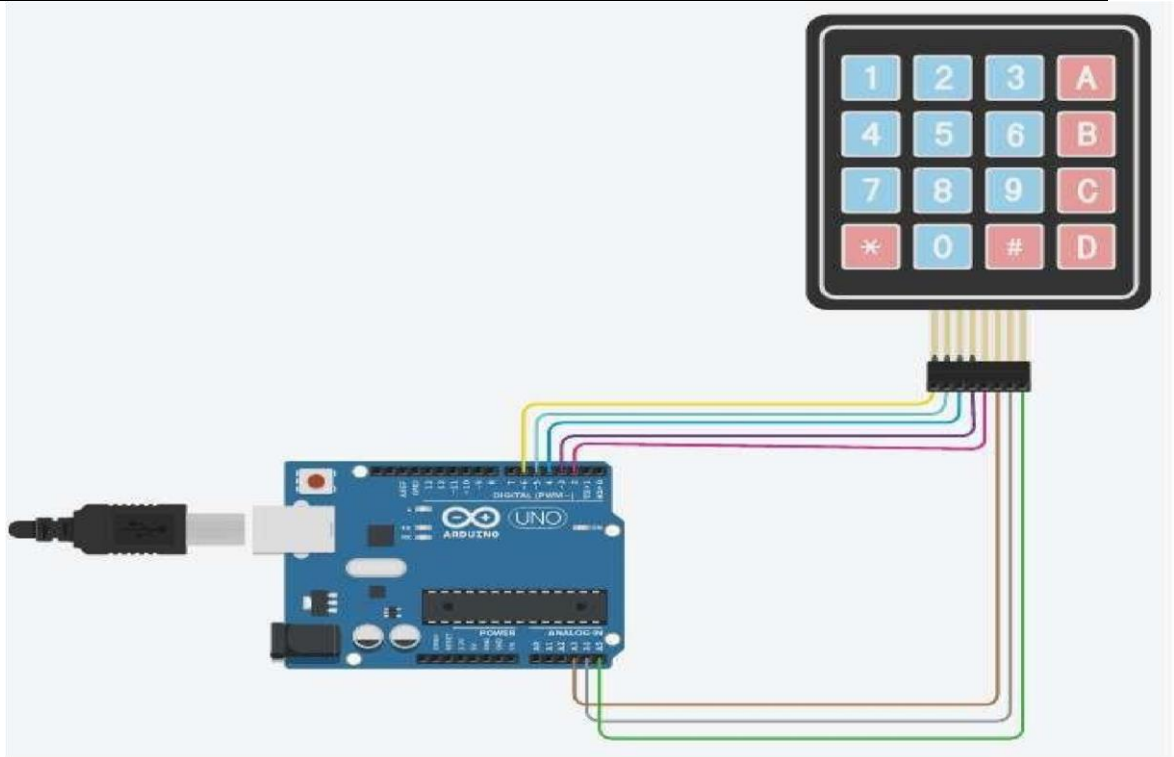


Figure 31 : câblage du keypad 4*4 avec la carte Arduino.

III.3.3 Afficheur LCD :

L'écran LCD est l'élément de visualisation de l'information entre l'utilisateur et le microcontrôleur, ça permet aussi d'afficher des messages en cas de fausse opération comme : "entrer le code", <Erreur> si c'est faux et < Bonjour> si c'est correct. Et permet aussi d'afficher les messages des commandes administrative comme l'enregistrement ou la lecture d'une empreinte, voir l'état de capteur et la lecture de journal des événements

Nous avons choisi le LCD 16x2 qui contient 2 lignes et 16 colonnes, utilisons le module I2C pour ne pas charger la carte Arduino (réduire le nombre de pins utilisé).

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

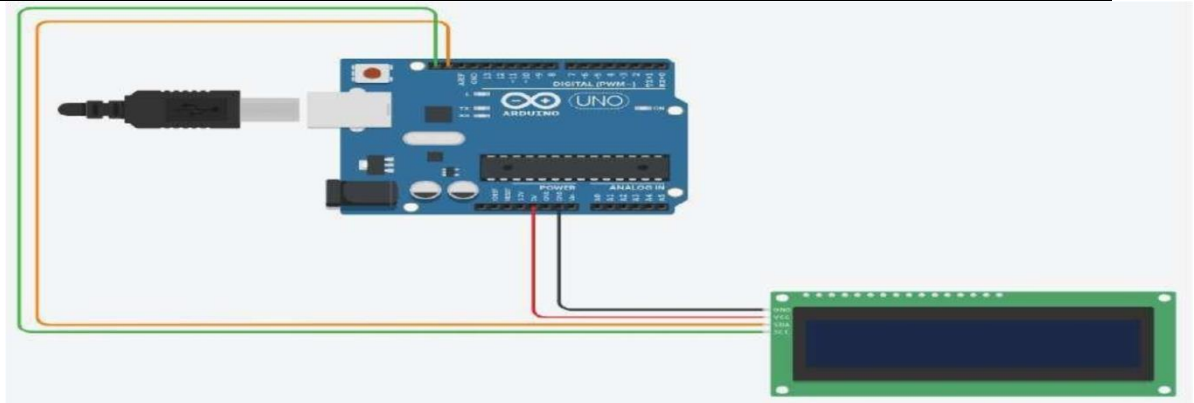


Figure 32 : câblage de LCD I2C avec la carte Arduino.

III.3.4 Servo moteur :

Le servo-moteur contient 3 fils (alimentation 5V, GND, et le dernier fil sert à contrôler la position de rotation du moteur), ce dernier fil est connecté à Arduino via le pin 13, qui sera commandé par une instruction dans le programme de base en fonction de besoin du système.

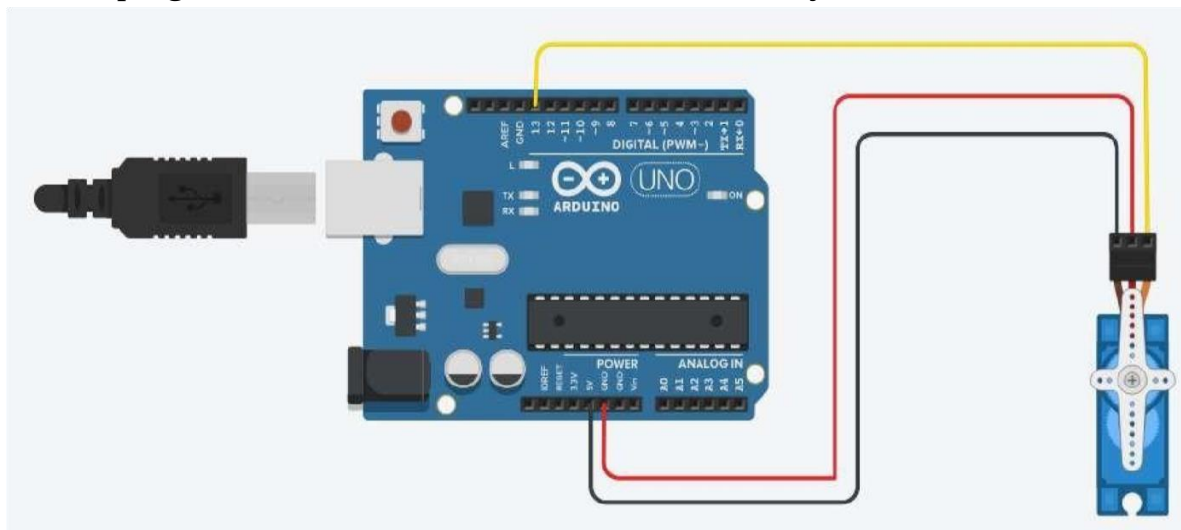


Figure 33 : Connexion servomoteur Arduino.

III.3.4.1. Commande du servo moteur :

Les servomoteurs sont des moteurs relativement précis dans l'angle de rotation pouvant tourner jusqu'à 180°, le servomoteur peut être contrôlé en envoyant une série d'impulsions sur la ligne de signal. La longueur de l'impulsion détermine la position de l'actionneur.

Le schéma représentant la connexion de la carte Arduino au servo moteur :

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

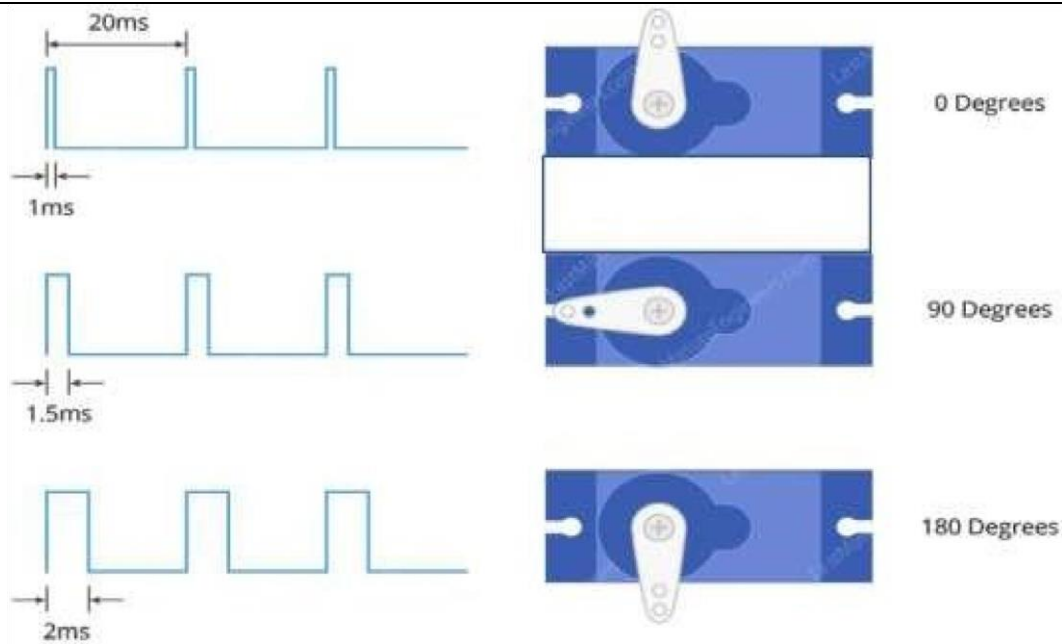


Figure 34 Signal de commande de moteur servo.

III.3.5. Les LEDS

LED (Diode électro-luminescente) : lorsque vous observez une LED, vous notez que l'un des connecteurs est plus long que l'autre. Le plus long (anode) sera connecté à la borne positive du circuit, alors que le plus court (cathode) sera connecté à la borne négative aussi appelée "ground" (GND) ou "masse". Elle sert principalement pour la signalisation [11].



Figure 35: LED .

III.3.3.6 Les résistances :

Une résistance est l'un des composants primordiaux dans le domaine de l'électricité dont la principale caractéristique est l'aptitude d'un matériau conducteur à s'opposer au passage d'un courant électrique sous une tension électrique donnée. Relié en série avec les LED pour une protection via limitation de courant d'alimentation

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale



Figure 36 : Les résistances

III.3.3.7. Capteur d'empreinte digitale

L'identification et la vérification des empreintes digitales est donc devenu très simple par l'évolution technologique de ses capteurs biométriques. Ils peuvent enregistrer jusqu'à 162 (voir 1000) empreinte en fonction du model et du type de capteurs choisi. Les empreintes seront stockées sous format digitale dans la mémoire flash embarquée dans le capteur.

Dans le capteur optique choisi, il y a une LED verte dans la lentille qui s'allume durant la prise l'empreinte. Il est certainement le meilleur capteur d'empreintes digitales rapport qualité prix trouvé sur le marché, et son utilisation est très simple. Ce capteur optique d'empreinte permet la sauvegarde et la détection des empreintes digitales.

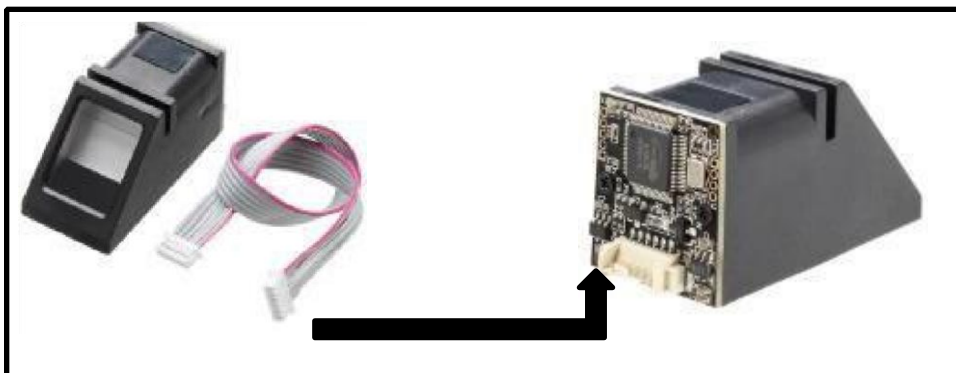


Figure. 37: Capteur optique d'empreinte digitale pour Arduino

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

En trouve dans le capteur d'empreinte digitale 6 broches : deux pour la communication avec ARDUINO (Tx,Rx) et deux pour l'alimentation (VCC et GND), les deux autres broches pour d'autre fonctionnalité non utiliser dans notre système.



Figure. 38: Les broches d'un capteur d'empreinte digitale

III.4 Branchements du capteur optique :

Le capteur travail avec la tenions de 3,3Volt. Il sera donc alimenté par +3.3V de la carte arduinouno. Tandis pour la communication, le capteur travail entre (0 et +3.3V) alors que la carte Arduino communique en (0 et +5V) pour cela il faut :

- dans le sens capteur TX -> Arduino RX, pas besoin d'adapter la tension car la carte Arduino peut lire 3,3V comme un niveau logique haut.
- dans le sens Arduino TX -> Capteur RX, on passera par un pont diviseur de tension qui permet d'abaisser le 5V en sortie de la carte Arduino à 3,3V.

N broche	Nom	Type	Fonction et Description
1	Vtouch	in	Touche d'entrée d'alimentation par induction (couleur du câble: bleu)
2	Sout	out	Signal de sortie (couleur du câble:

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

			jaune)
3	Vin	in	Entrée d'alimentation (couleur du câble: rouge)
4	TD	out	Sortie de données. Niveau logique TTL (couleur du câble: vert
5	RD	in	Entrée de données. Niveau logique TTL (couleur du câble: blanc)
6	GND		Masse de signal. Connecté à la terre (couleur du câble: noir

III.5 Connexion matérielle

Le module via l'interface de communication série, peut être utilisé directement avec le microcontrôleur 3.3V ou 5V pour communiquer: broche de transmission de données de module (TX à 4 broches) connectée au récepteur de données d'ordinateur hôte (RXD), broche de réception de données de module (5 pieds RX)) connectez-vous au terminal de transmission des données de la machine de position (TXD).

III.5.1 Arduino UNO :

La carte ArduinoUno est une carte électronique programmable basée sur un microcontrôleur (ATMega328), cadencé à 16 MHz. C'est la plus simple et la plus économique carte à microcontrôleur d'Arduino. Des connecteurs situés sur les bords extérieurs du circuit imprimé permettent d'enficher une série de modules complémentaires.

Cette carte peut se programmer avec le logiciel IDE Arduino basé sur le langage C et disponible gratuitement en téléchargement. Le microcontrôleur ATMega328 contient un bootloader qui permet de modifier le programme sans passer par un programmeur,

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

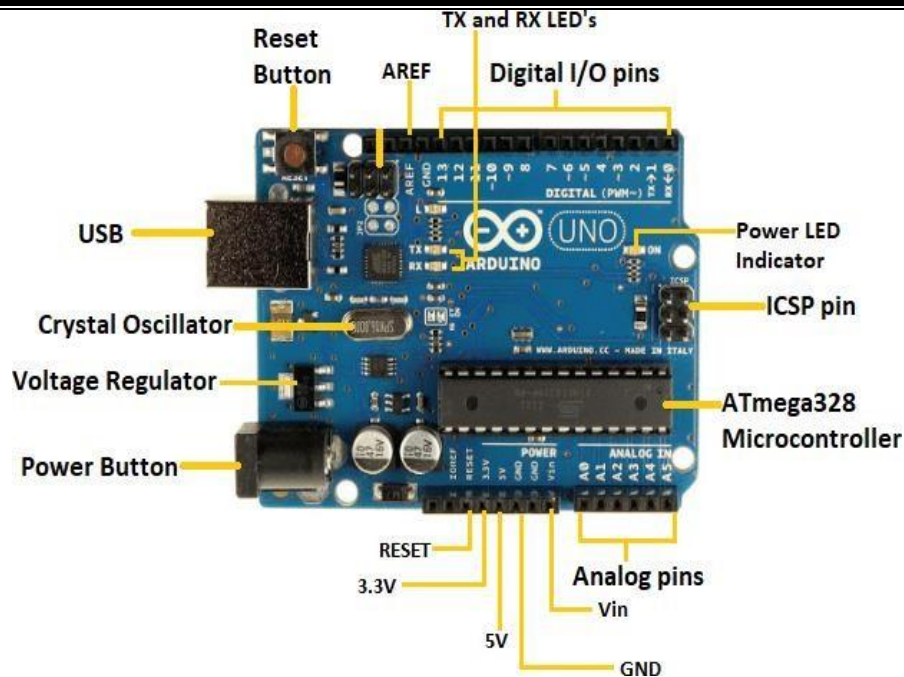


Figure 39 : Les pins E/S d'une carte Arduino UNO.

III.5.1.1. Caractéristiques techniques de la carte Arduino UNO :

- Microcontrôleur : ATmega328p.
 - Tension de fonctionnement nominale : 5V.
- Tension d'alimentation (recommandé) : 7-12V.
- Tension d'alimentation (limites) : 6-20V.
- Entrées/sorties numériques : 14 (dont 6 pouvant être utilisées comme sorties PWM).
- Entrées analogiques : 6.
- Courant DC pour I/O : 40 mA.
- Courant DC pour 3.3V : 50 mA.
- Mémoire Flash : 32 KB (ATmega328) dont 0.5 KB utilisé par le bootloader.
- SRAM: 2 KB (ATmega328).
- EEPROM: 1 KB (ATmega328).
- Fréquence d'horloge : 16 MHz .

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

III.5.1.2. Schéma simplifié de la carte Arduino UNO :

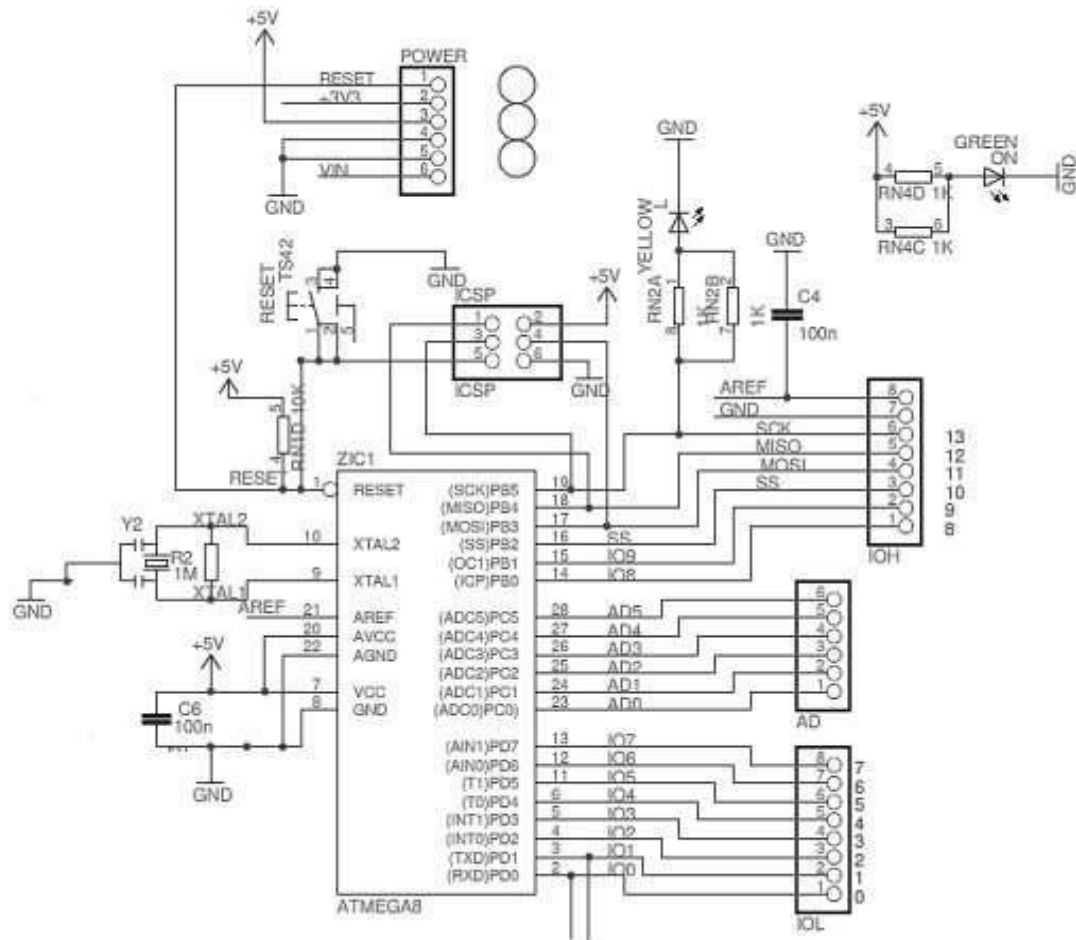


Figure 40 : Schéma simplifié de la carte Arduino UNO.

III.6. L'environnement IDE Arduino :

Les programmes écrits pour Arduino s'appellent des *croquis*. C'est une convention de nommage héritée de Processing, qui permettait aux utilisateurs de créer des programmes rapidement, de la même manière que vous pouvez croquer une idée dans un carnet de croquis.

III.7. L'interface :

La barre de menus est semblable à la barre de menus d'autres programmes qui vous sont familiers, la barre de menus Arduino contient des menus déroulants pour tous les outils, paramètres et informations du programme elle est composée de :

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

- A : Bouton Vérifier : Ceci compilera le programme qui est actuellement dans l'éditeur. Il ne se contente pas de vérifier la syntaxe du programme. Il le tourne aussi dans une représentation adaptée à la carte Arduino.
- B : Bouton Upload : Ceci compilera et téléchargera le programme actuel vers la carte Arduino connectée.
- C : Bouton Nouveau : crée un nouveau programme en ouvrant un nouvel éditeur la fenêtre.
- D : Bouton Ouvrir : Avec ce bouton, vous pouvez ouvrir un programme existant depuis le système de fichiers.
- E : Bouton Enregistrer : pour enregistrer le programme actuel.
- F : moniteur série : Arduino peut communiquer avec un ordinateur via un lien. Cliquer sur le bouton Serial Monitor ouvre une fenêtre de moniteur série qui vous permet de regarder les données envoyées par Arduino et également de renvoyer des données. Vous en apprendrez plus à ce sujet dans la section Utilisation de la communication série.
- G : Fenêtre de l'éditeur : C'est ici que vous écrirez le code.
- H : console d'erreur : c'est ici que vous verrez tous les messages d'erreur de votre code.
- I : Barre d'état : elle affiche le nom de la carte Arduino connectée ainsi que le numéro de portCOM.

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

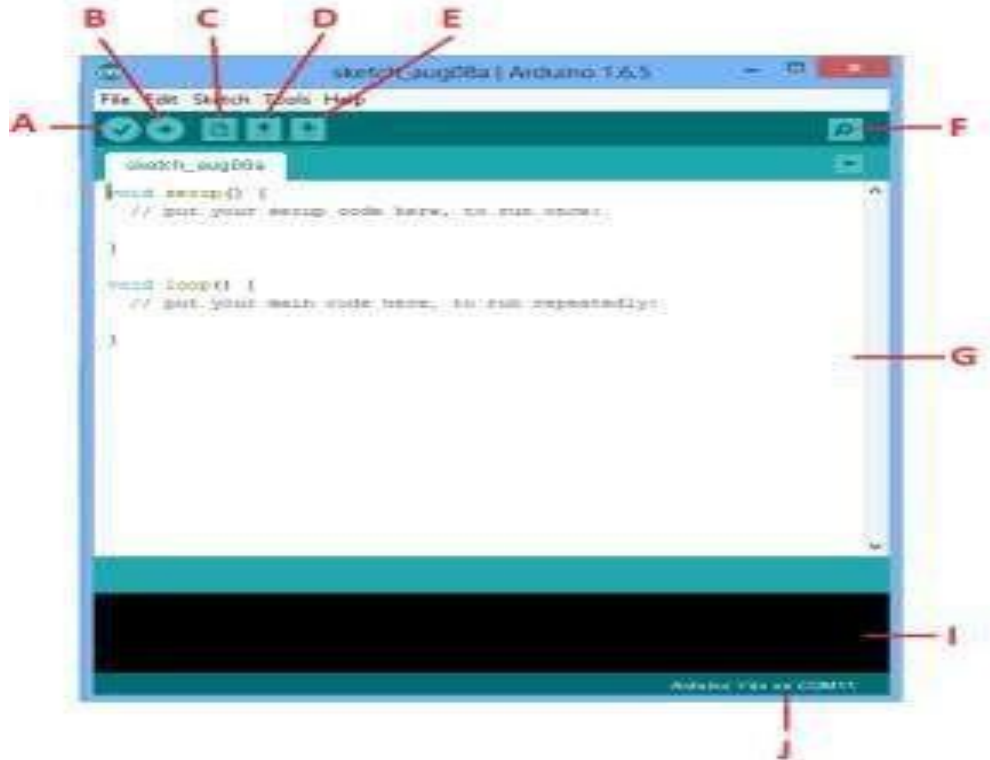


Figure 41: La fenêtre de l'atelier Arduino sous Windows.

III.8. Méthode d'identification utilisée par notre système:

La technique d'identification consiste à accorder l'accès après avoir passé les étapes d'identification et de vérification d'identité qui sont :

- Lecture d'empreinte via le capteur et confirmation de l'identité en comparant l'empreinte de la personne qui demande accès avec celles pré-identifiées, en cas de confirmation la serrure sera ouverte (servo moteur activé), sinon le système d'alerte est enclenché (affichage de message d'erreur et signalisation par la LED Rouge).
- Si jamais un problème est rencontré avec l'empreinte digitale, activer la saisie du mot de passe composé de plusieurs caractères par le keypad, on offre à l'utilisateur trois tentatives pour introduire correctement le mot de passe, si les trois tentatives sont erronées, le système signalant une tentative d'accès illicite.
- Enregistrement du journal d'événement (utilisateur «code identifiant», l'opération faite durant la tentative, la date et le temps d'accès) dans un fichier sur la carte SD

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

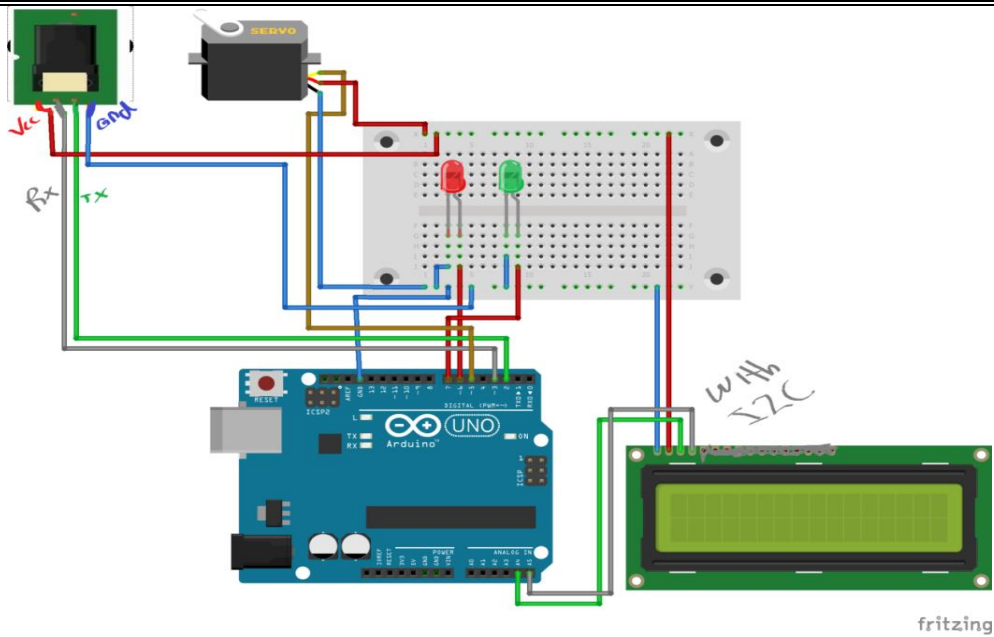


Figure 43 : Le schéma complet du système à l'aide de logiciel Fritzing

III.11.Organigramme :

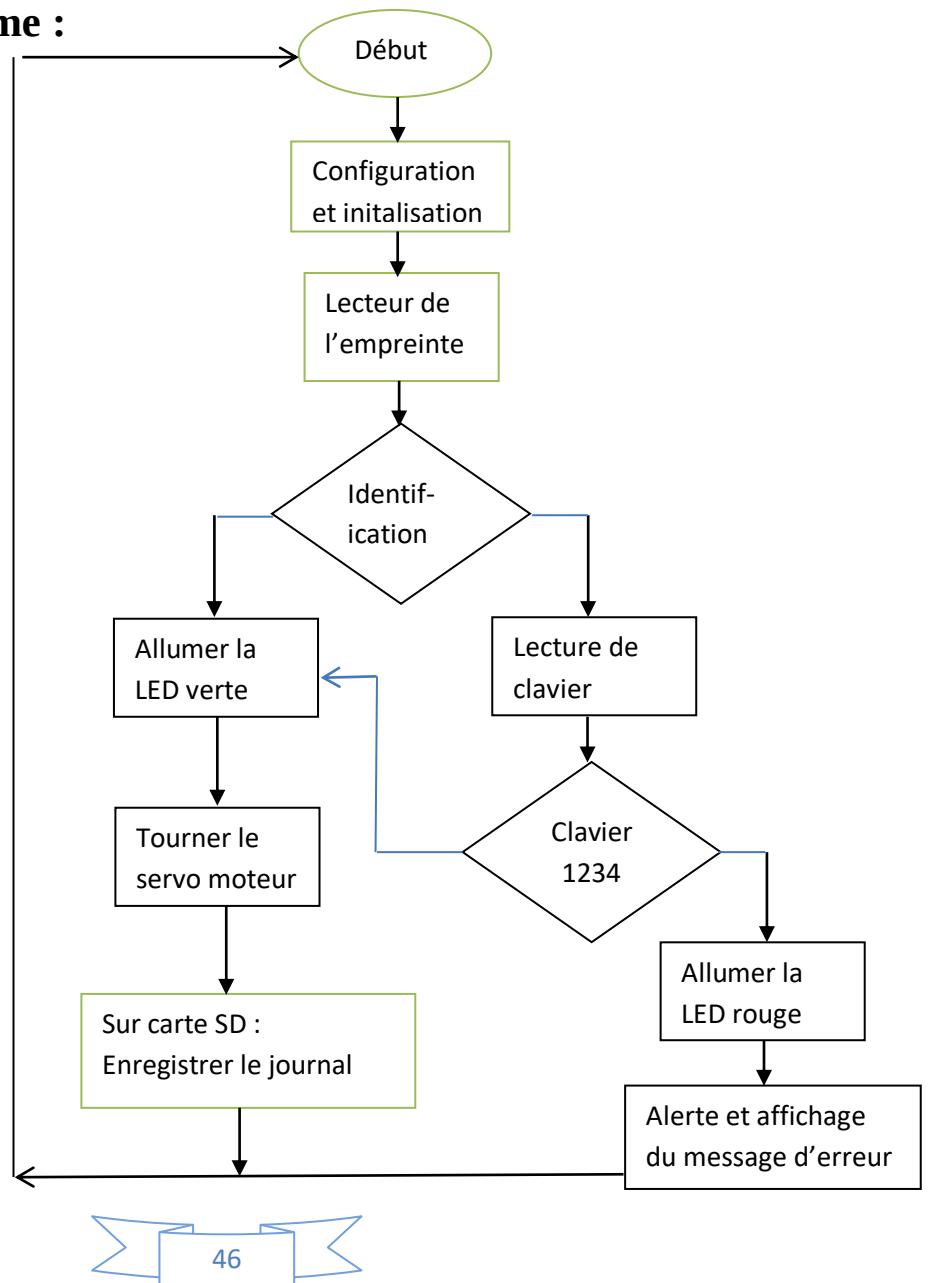


Figure44:Organigramme de système de pointage

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

III.12. Carte SD

On vous explique comment lire les informations sur une carte SD virtuel pour vous familiariser avec le concept de simulation de notre système.

Exemple : Dans cet exemple, nous allons apprendre à créer un fichier image à l'aide du **logiciel Win image** et à sélectionner certains paramètres tels que le type de volume, l'espace libre et d'autres informations à l'aide de Win image et de la bibliothèque SD, et à l'envoyer via le port série. Ensuite, nous imiterons l'exemple dans proteus pour arriver aux meilleurs résultats requis qui ressemblent à l'expérience pratique.

Sachant que la bibliothèque de cartes SD pour Ardin est assez excellente et facilite l'interaction avec les cartes SD. La lecture et l'écriture sur des cartes SD sont possibles avec la bibliothèque SD Ardin. Il est basé sur la sdfatlib de William Greimas. Sur les cartes SD et SDHC ordinaires, la bibliothèque prend en charge les systèmes de fichiers FAT16 et FAT32. Pour les noms de fichiers, il utilise des noms courts 8.3.

Le SPI est utilisé pour communiquer entre le microcontrôleur et la carte SD, et il est situé sur les broches numériques 11, 12 et 13 (sur la plupart des cartes Arduino) ou 50, 51 et 52 (sur certaines cartes Arduino) (ArduinoMega). Un deuxième pin est également nécessaire pour choisir la carte SD. La broche matérielle SS - broche 10 sur la plupart des cartes Arduino ou broche 53 sur le Mega - ou une autre broche spécifiée dans l'appel SD.begin() peut être utilisée.

Et pour se faire cet exemple, les composants requièrent :

Carte Arduino, Carte SD avec système de fichiers FAT16 ou FAT32

LM35 Terminal virtuel (en tant que moniteur série), Module d'interface LCD I2C PCF8574, Affichage LM016L (LCD), R1 et R2 = 10 000 ohms

Logiciel Protée EDI Arduino, Winimage

III .12.1Prérequis pour notre exemple

Avant de procéder à la simulation de pièce proprement dite, nous allons d'abord nous échauffer avec un simple exercice de téléchargement,

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

d'installation et de configuration de bibliothèques pour Arduino IDE & Proteus.

III .12.2 Installation de Winimage

Notre première étape consiste à télécharger le winimage à partir d'Internet et à définir le chemin de téléchargement pour qu'il soit facilement accessible pour les parties ultérieures. Sélectionnez le dernier fichier .exe approprié sur le site officiel selon la configuration système requise indiquée dans l'image ci-dessous.

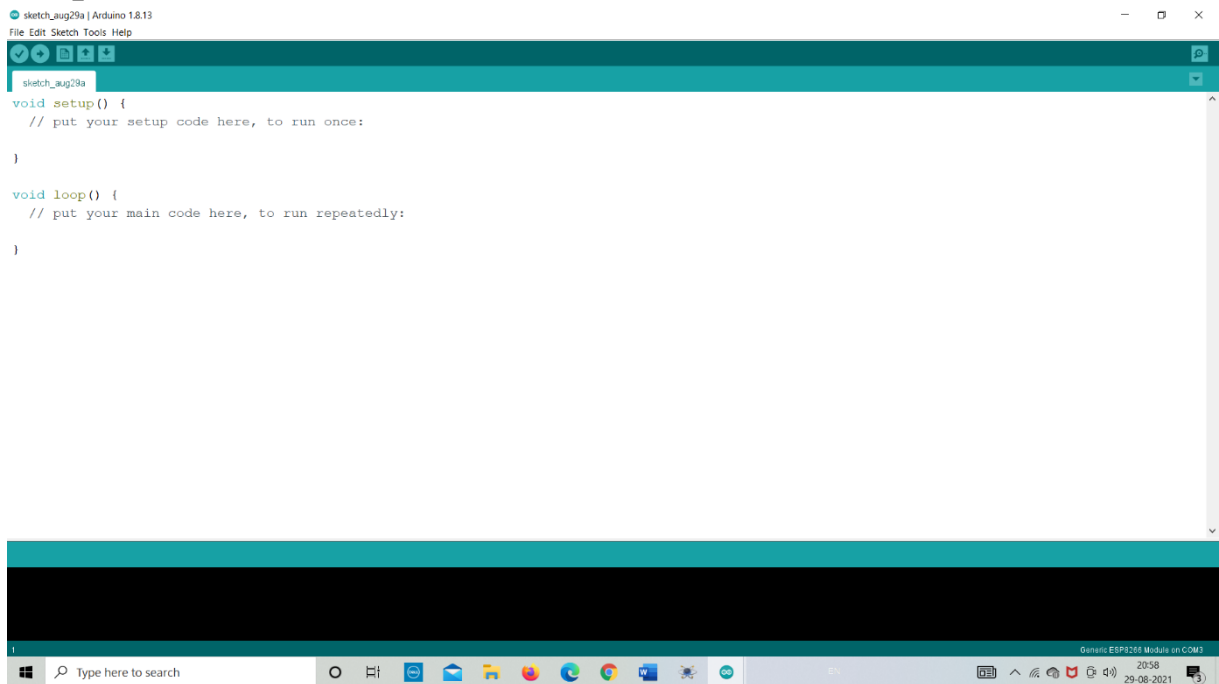


Ajout de la bibliothèque de cartes SD dans l'IDE

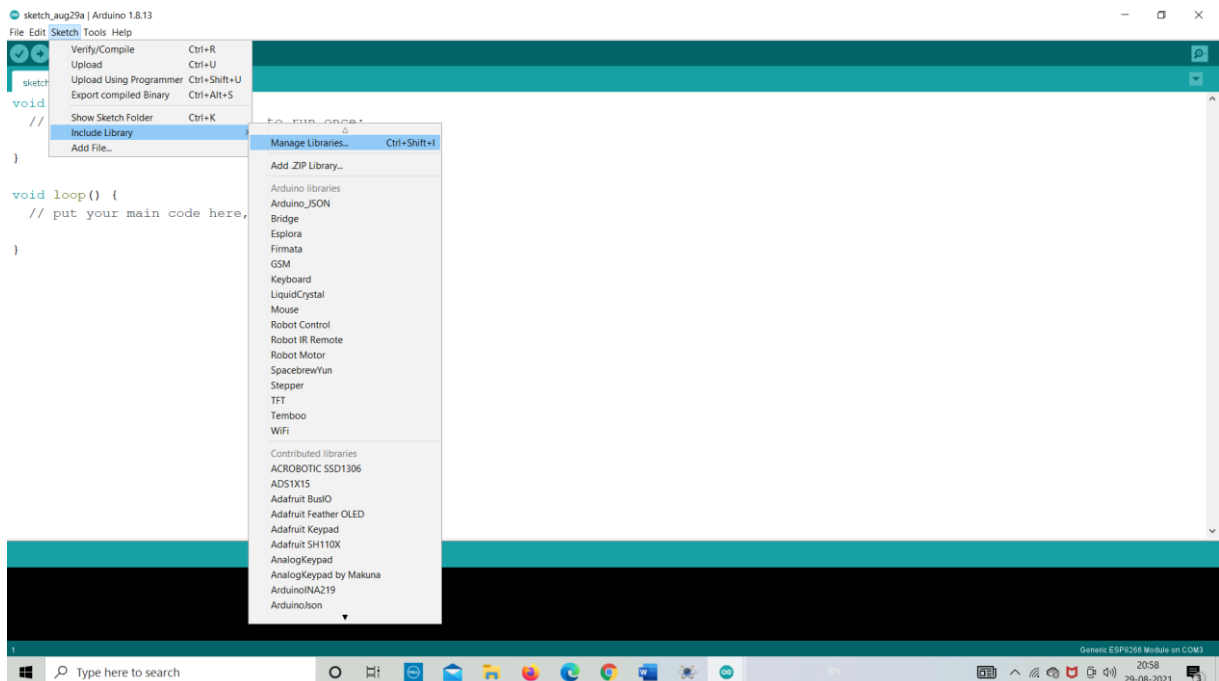
Nous allons maintenant télécharger la bibliothèque SD depuis IDE. Suivez les étapes indiquées dans l'image ci-dessous pour en savoir plus sur le téléchargement de la bibliothèque SD pour Arduino IDE. Cette bibliothèque nous servira à programmer l'Arduino pour le module de carte SD pour stocker et récupérer des données.

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

Étape 1 : Ouvrez l'IDE Arduino

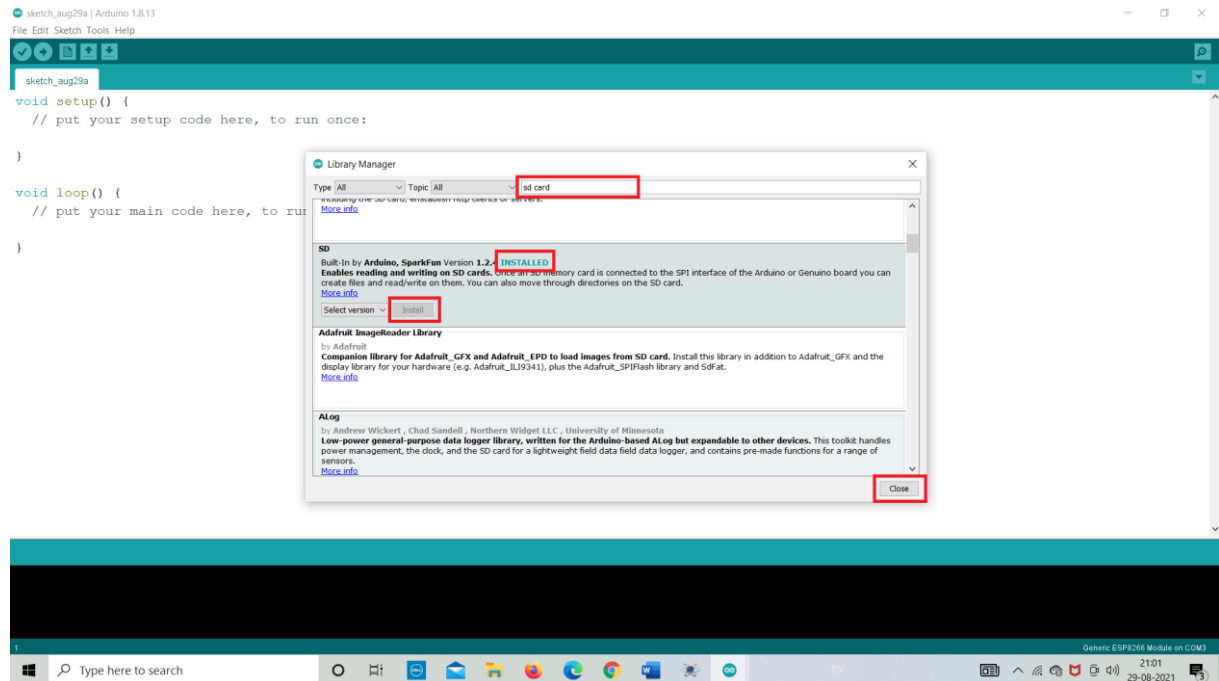


Étape 2 : Allez dans "Sketch" >> "Inclure la bibliothèque">> "Gérer les bibliothèques"



Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

Étape 3 : Recherchez "SD" dans la barre de recherche et "Installez-le" à partir de là



II.12.3. Création du fichier image Winimage

L'étape suivante consiste à créer un fichier image à l'aide du logiciel winimage.exe. Ici, nous l'ouvrons à partir du dossier téléchargé et créons le fichier de 2 Mo. Ce fichier sera utilisé pour stocker les données du module de carte SD au format.

Avec WinImage en place, vous pouvez recréer l'image disque sur le disque dur ou un autre support, afficher son contenu, extraire des fichiers basés sur l'image, ajouter de nouveaux fichiers et répertoires, modifier le format et défragmenter l'image.

Suivez les images ci-dessous pour savoir comment créer le fichier image.

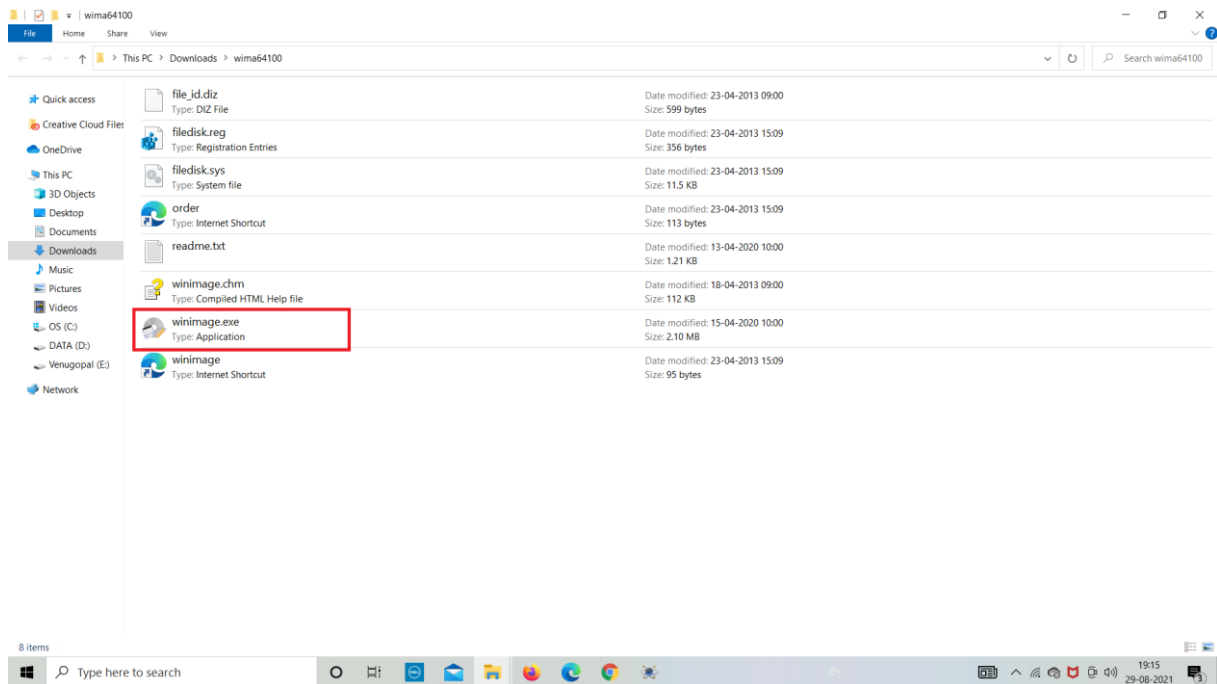
Gardez le FAT 12/16 et les autres paramètres sans incidence, à l'exception de la taille de l'image.

Rappelons notre exemple, nous utiliserons un fichier image de 2 Mo et donc le même est créé ci-dessous dans les images. Nous avons donné le nom à notre fichier image « carteSD.IMG ».

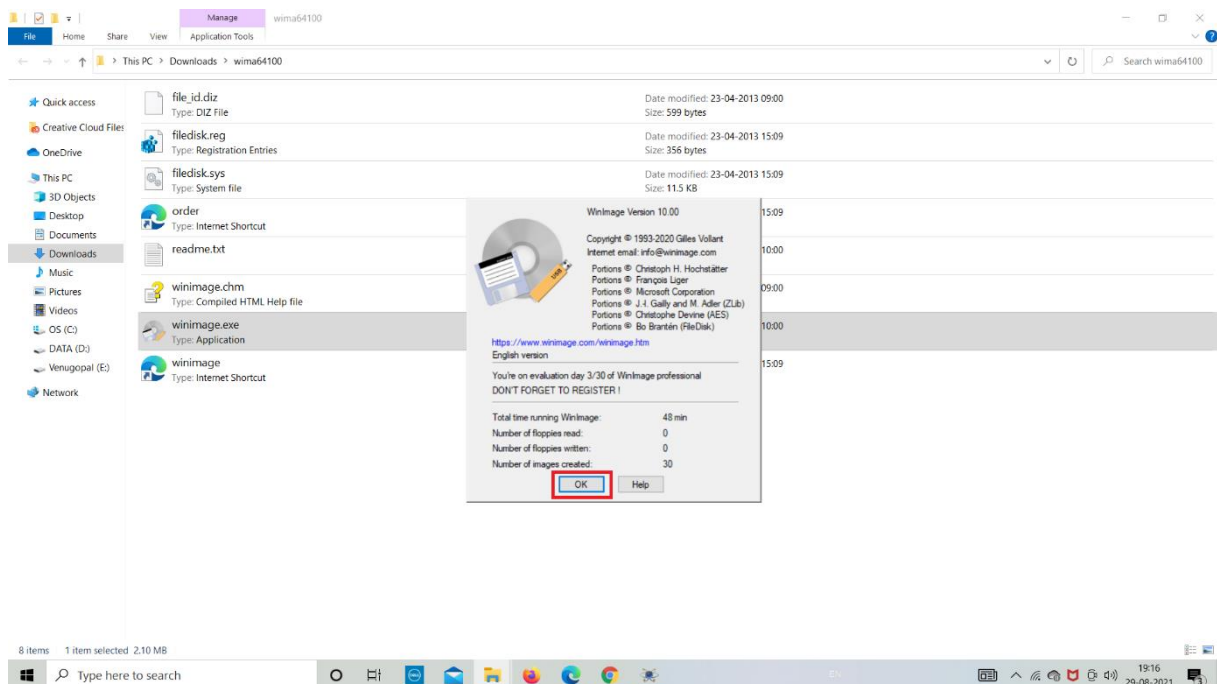
Remarque : ne modifiez aucune extension (*.IMG) lors de l'enregistrement des fichiers.

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

Etape 1 : Ouvrez le fichier "winimage.exe"

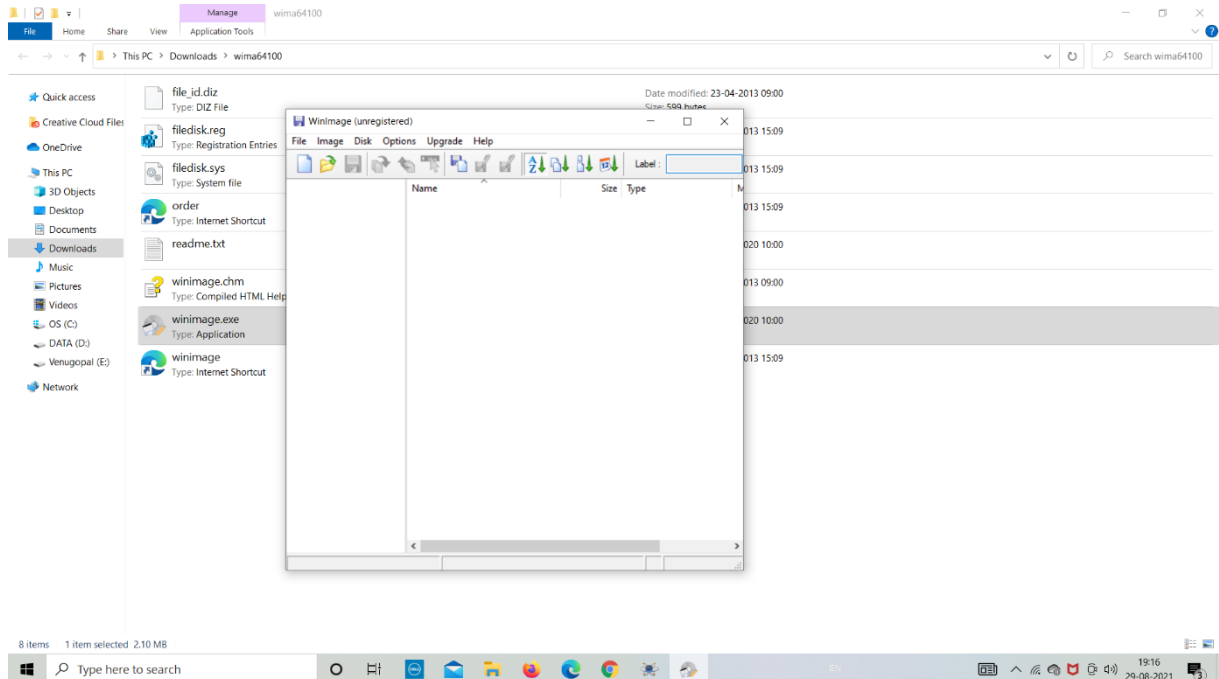


Étape 2 : Cliquez sur "OK" et continuez

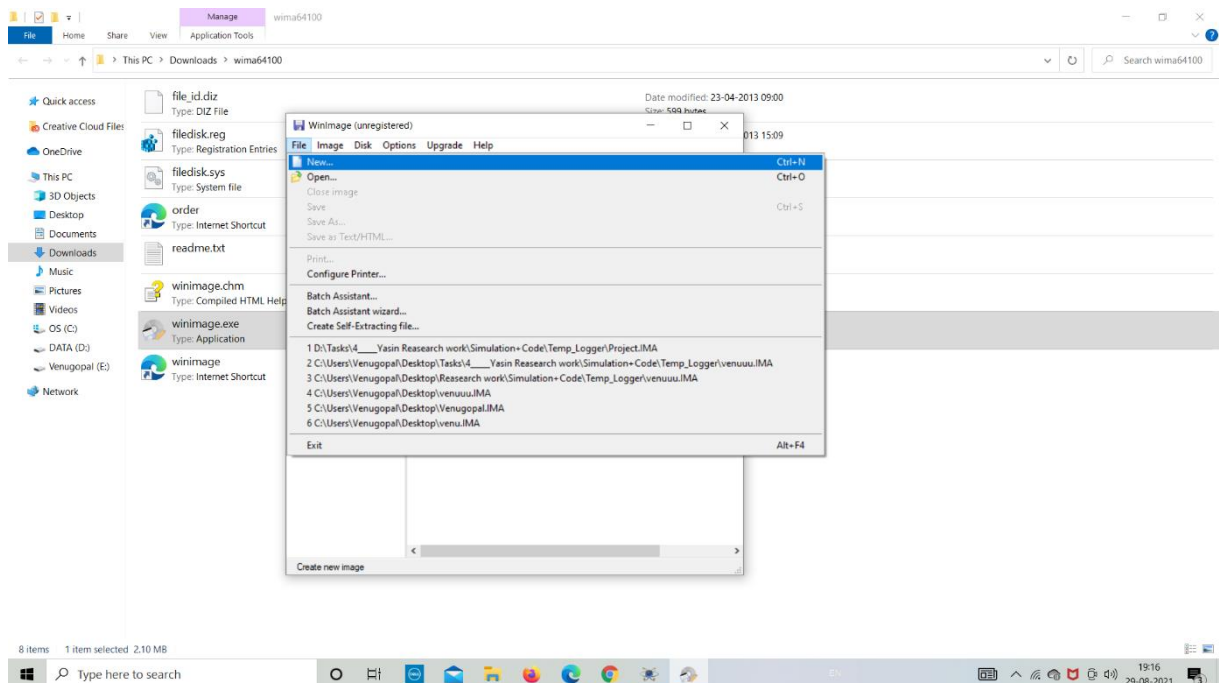


Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

Étape 3 : Allez dans "Fichier" dans le coin supérieur gauche

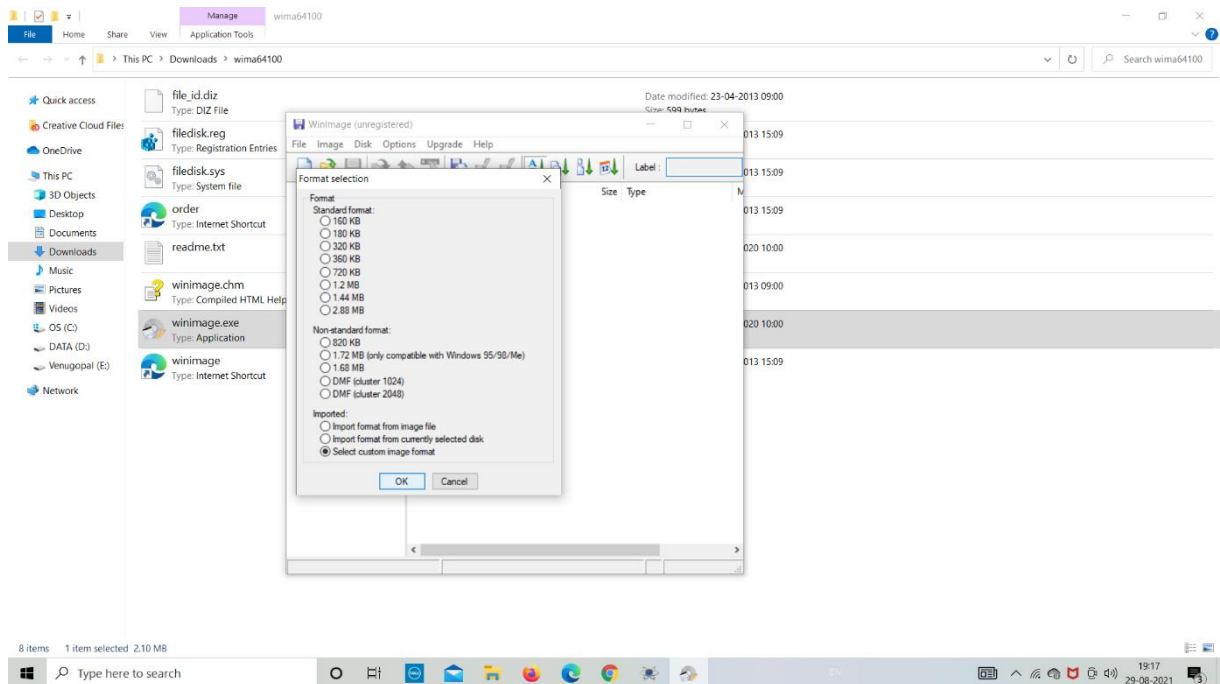


Etape 4 : Cliquez sur "Nouveau"

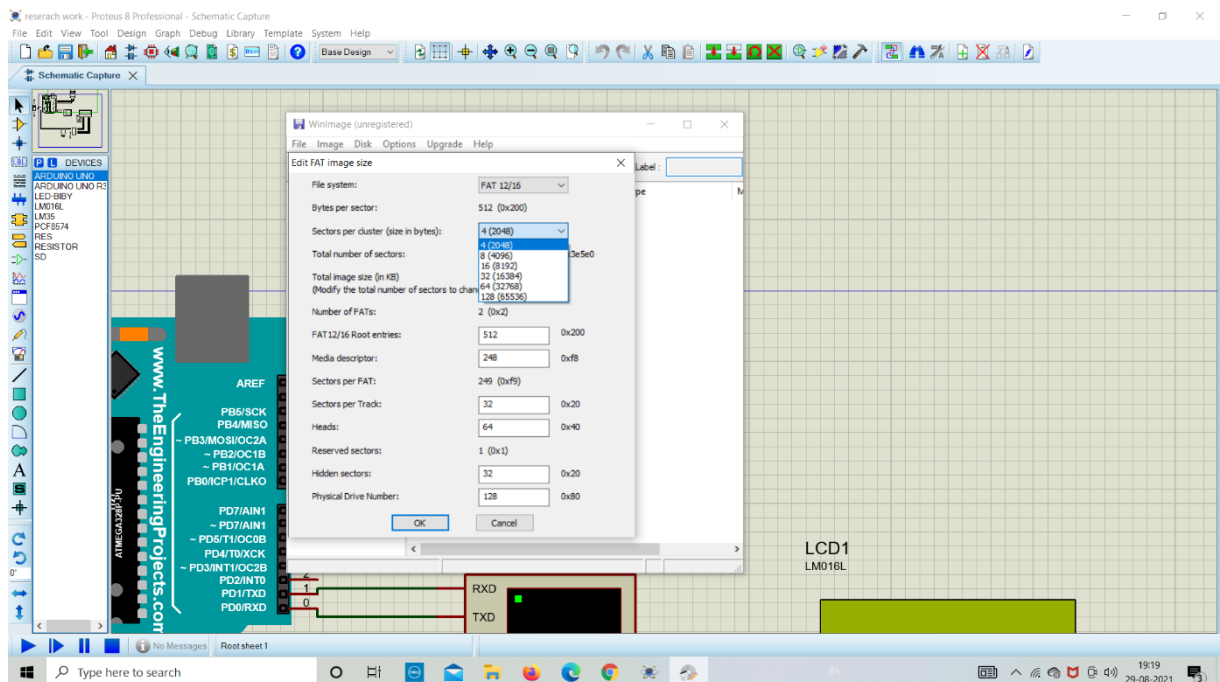


Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

Étape 5 : Cliquez sur "Sélectionner le format d'image personnalisé"

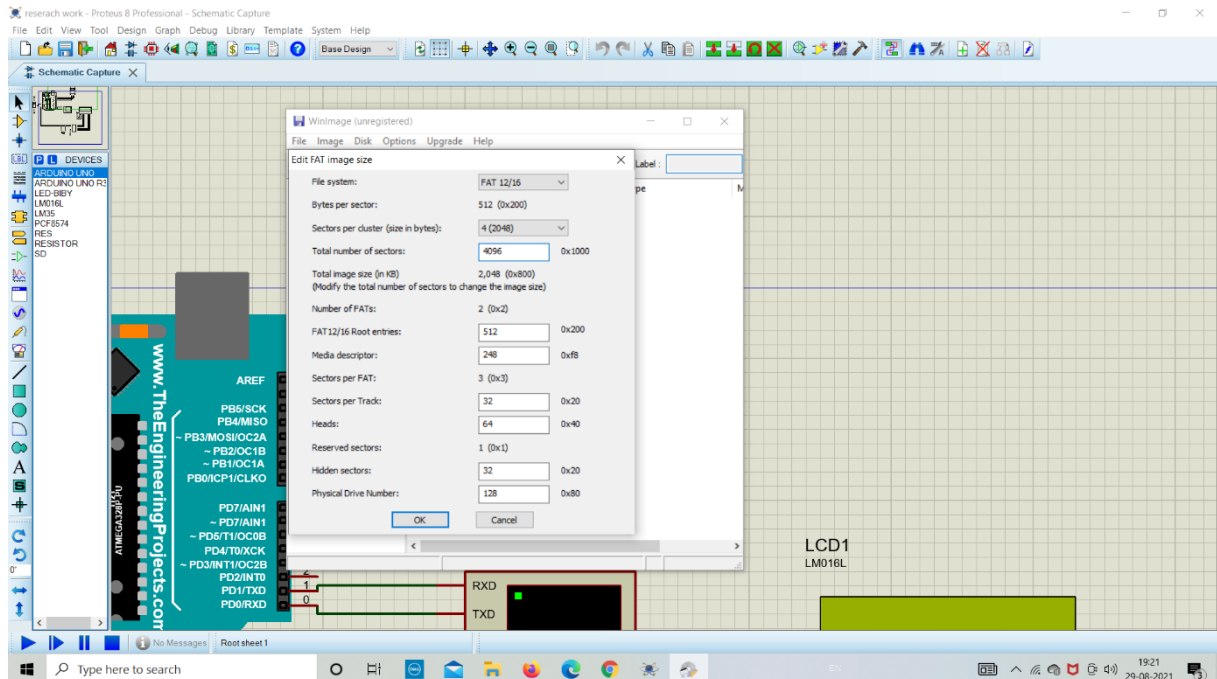


Étape 6 : Sélectionnez "4 (2048)" dans la liste déroulante

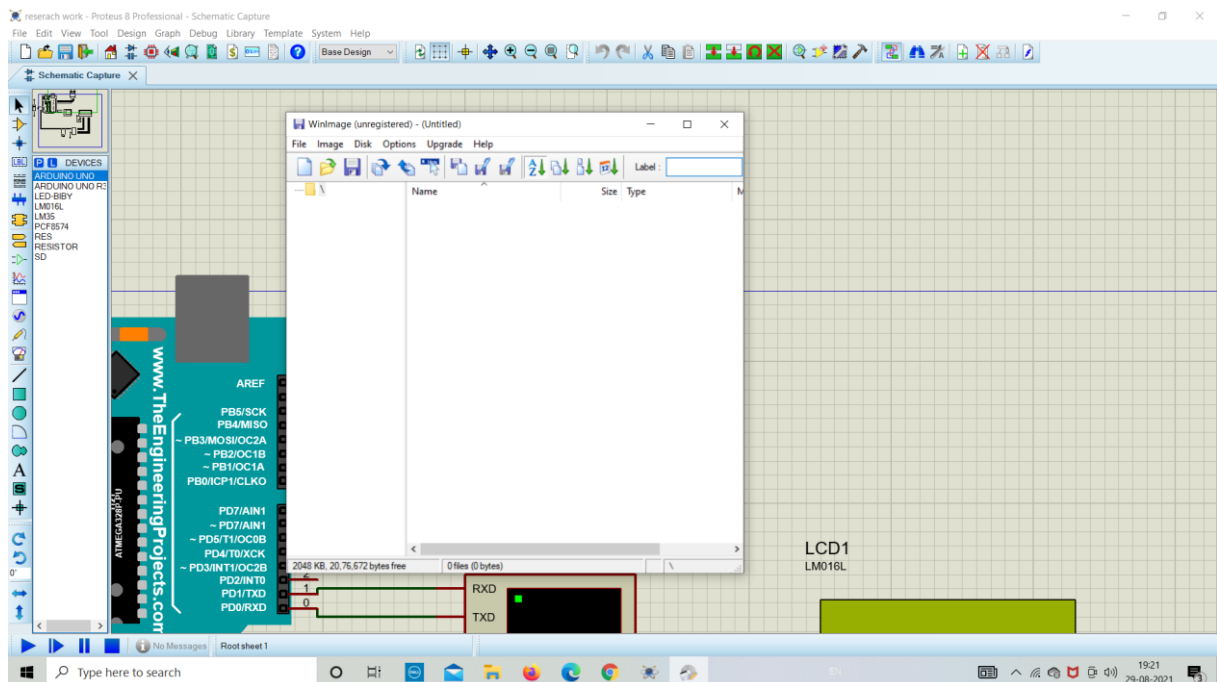


Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

Étape 7 : Gardez toustel qu'il est et cliquez sur "Ok"

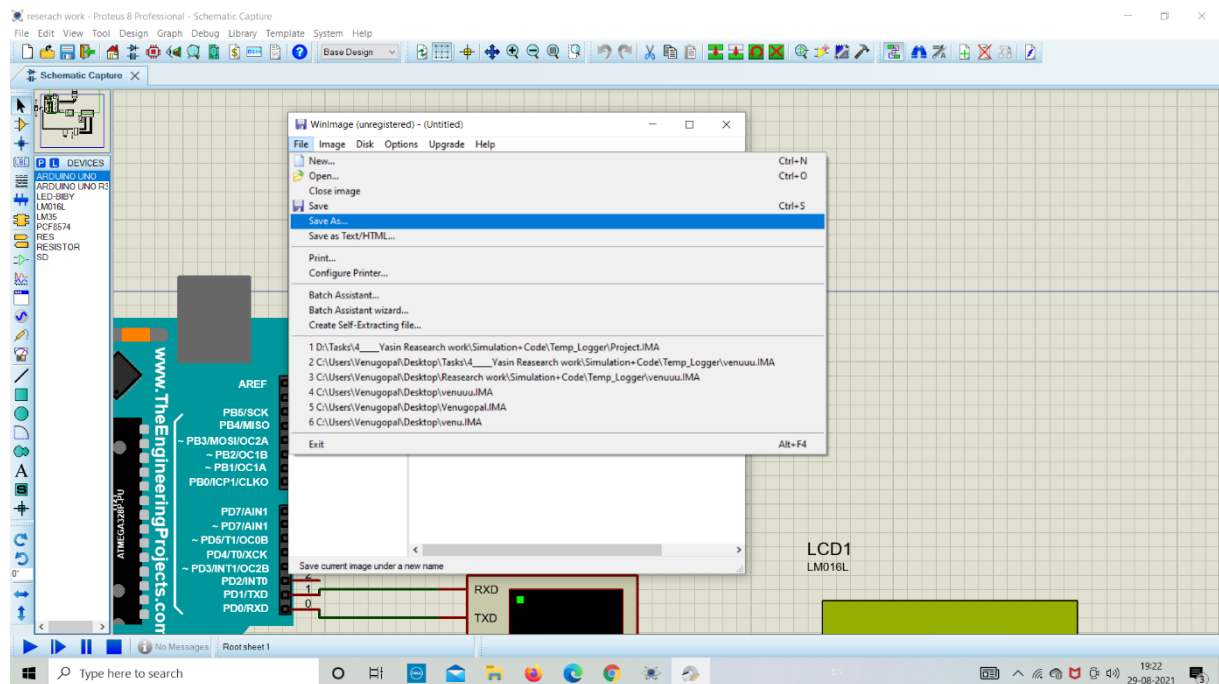


Étape 8 : Cliquez maintenant sur "Fichier" pour enregistrer le fichier



Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

Étape 9 : Maintenant "Enregistrer sous" le fichier dans le dossier de destination



III .14.Résultats pratiques:

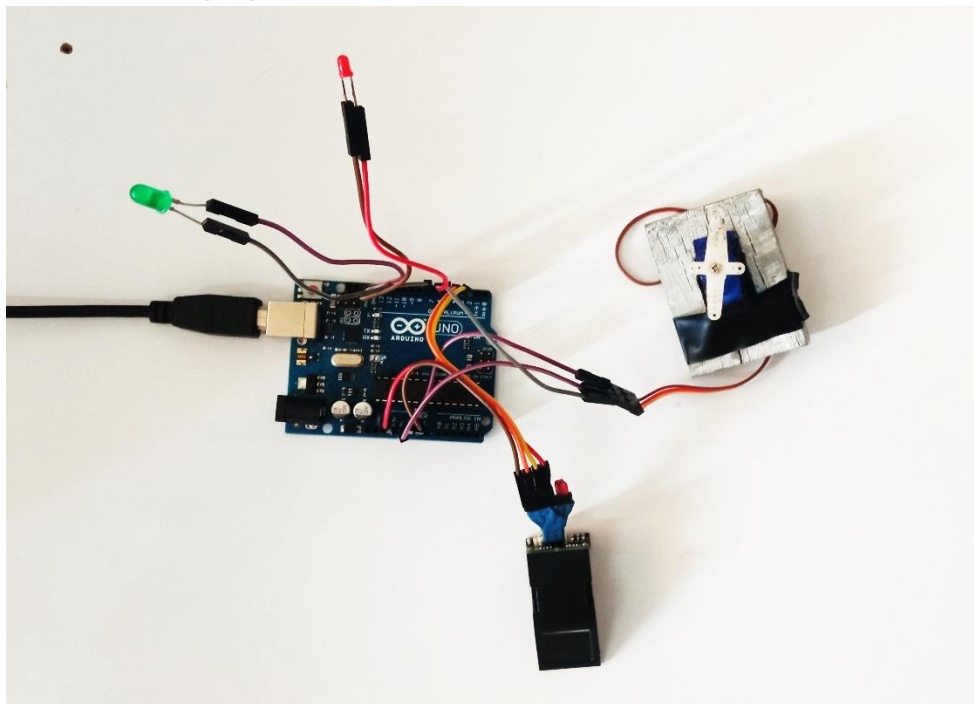
Après avoir testé le bon fonctionnement du montage de Système de pointage à base de l'ARDUINO UNO par le Simulateur Proteus, nous avons pu concrétiser notre projet.

1. Enregistrement des empreintes des utilisateurs dans la mémoire flash du capteur. (en mode administrateur)
2. Lecture de la bonne empreinte digitale via le capteur qui est connecté à arduino par les broches(2,3)
3. Si empreinte est correct, tourner le moteur (attacher au pin 5) à droite avec une valeur de 90°, et allumer la LED verte (attacher à pin 7)
4. Remettre le moteur à l'état initial après un timing de déverrouillage et revenir à l'étape 2
5. Si empreinte est incorrect: Allumer la LED rouge (attaché à pin 6).

Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

6. Si une erreur d'identification est détectée par le capteur, passé au mode saisie de mot de passe (4 chiffres) via le clavier.
7. Si une erreur d'identification est détectée après 3 tentatives, lancer l'alarme (beep)
8. Si le mot de passe est conforme, tourner le moteur (attacher au pin 5) à droite avec une valeur de 90° , et allumer la LED verte (attacher à pin 7)
9. Remettre le moteur à l'état initial après un timing de déverrouillage, et revenir à l'étape 2
10. Si empreinte de l'administrateur ou le mot de passe est détecté, le système passe en mode service (ajout ou suppression d'empreinte digitale) en fonction des empreintes ou code enregistré précédemment. A la fin revenir à l'étape 2
11. Sauvegarder sur la carte SD le journal des événements (identifiant utilisateur, date et heure d'accès, opération réalisée,...)

III .19. Le montage global :



Chapitre III conception et réalisation un système de pointage à base d'empreinte digitale

Conclusion

Cette étude permis d'approcher les différentes méthodes de traitement d'images et de comprendre les possibilités et les limites de la reconnaissance d'empreintes digitales. Nous avons pu avoir un aperçu d'une technologie complexe et d'actualités.

Notre système à bas cout est réalisé avec succès, il permet la fonction de pointage par empreinte digitale via le capteur optique. La capacité possible de stockage peut attendre 1000 empreintes, mais nous somme limité à 100 utilisateurs et de 10 empreintes fonctionnelles des administrateurs (identification, ajout d'empreinte, suppression d'empreinte, lecture de journal, effacement total, installation usine,...)

Notre objectif est atteint, avec une rapidité et une fiabilité d'exécutions de taches demandées.

La formation des empreintes au stade embryonnaire intéresse les chercheurs en morphogenèse, le pourquoi des empreintes digitales est toujours une question débattue

Conclusion Générale

Conclusion générale

CONCLUSION GENERALE

La biométrie qui s'installe de plus en plus dans notre quotidien devient la nouvelle solution pour les entreprises, sociétés et organismes scolaires pour lutter contre la fraude des employés et salariés par rapport aux heures d'arrivée et de départ en plus du temps passé à travailler au sein des entités, vérifier l'identité des étudiants lors des examens et contrôles, Utiliser un système biométrique au sein d'un organisme, permet de mieux cerner et contrôler son activité, d'avoir une vision instantanée et efficace du taux de présence/absence de son effectif.

L'objectif, en utilisant un capteur biométrique et un logiciel de gestion, est d'avoir une visibilité totale qui permettra de mettre en place des plannings parfaitement optimisés et adaptés pour une organisation et une rentabilité optimale. Le système est entièrement automatisé et apporte tous les rapports détaillés sur l'activité de chaque acteur de l'organisation.

Cette solution apporte aussi des avantages tels que la précision, la rapidité et l'efficacité dans les procédures de contrôle.

D'autres techniques peuvent être utilisées pour réduire ou éliminer le problème de résidus d'empreintes sur le capteur, à savoir la reconnaissance faciale ou l'iris d'œil.

Enfin, nous espérons que ce projet sera développé dans le futur et utilisé par notre faculté puis répandu dans toute l'université.

Références Bibliothèque

REFERENCES BIBLIOGRAPHIQUES

- [1]: “ **REZZAG Omar** ”, « Conception et réalisation un système de pointage et de contrôle d'accès à base d'empreinte digitale », Mémoire de Master, Option : Systèmes de automatique et système , Université de Ghardaïa, Juin 2022
- [2]: “ **SAYAH Manel** ” «Système de pointage par empreinte digitale », Mémoire de Master en électronique option système embarqué, Université Mohamed Khider de Biskra, juillet 2019
- [3]: “ **LEBOUKH Khadra** ”, «Conception et Réalisation d'un Enregistreur De Présence à Empreintes Digitales », Destiné aux étudiants de la 2 ère Master en génie mécanique , Université Larbi Ben Mhidi d'Oum El-Bouaghi, 2020
- [4]: “ **OUKIL Kahina** ”, «Contrôle d'accès à base d'empreinte digitale », Mémoire De fin d'étude pour l'obtention du diplôme de Master e Réseaux, Mobilités et Systèmes Embarqués, Universit MOULOU MAMMERI DETIZI-OUZOUé, septmbre 2019
- [5]: <http://biometrie-online.net/technologies/empreintes-digitales>
- [6]: <https://justaskthales.com/fr/comment-fonctionnent-les-scanners-dempreintes-digitales/>
- [7]: <https://contrat-de-travail.ooreka.fr/astuce/voir/753011/systeme-de-pointage>
- [8]: <http://www.mytopschool.net/mysti2d/activites/polynesie2/eX:eL/SIN/08/ArduinoYun/introduction.html>
- [9]: <https://www.horloges-huchez.fr/blog/tout-savoir-sur-le-pointage>
- [10]: <http://www.secu-mag.com.tn/articles/systemes-de-pointage.html>
- [11]: <https://www.horloges-huchez.fr/badgeuse>
- [12]: <https://fr.wikipedia.org/wiki/ESP32>
- [13]: <https://lastminuteengineers.com/esp32-arduino-ide-tutorial/>
- [14]: <http://repository.umy.ac.id/bitstream/handle/123456789/22709/FPM10A.pdf?sequence=13&isAllowed=>
- [15]: <https://www.electroniccomp.com/0.96-inch-i2c-iic-128x64-oled-display-module-4-pin-white-color>
- [16]: <https://lastminuteengineers.com/oled-display-arduino-tutorial/>

Références Bibliothèque

- [16]: <https://www.varta-ag.com/en/consumer/product-categories/accus/recharge-accu-power-9v-200-mah>
[17]: https://en.wikipedia.org/wiki/Arduino_IDE
[18]: <https://fr.wikipedia.org/wiki/XAMPP>