وزارة التعليم العالي و البحث العلمي

BADJIMOKHTAR-ANNABAUNIVERSITY

UNIVERSITE BADJI MOKHTAR ANNABA

جامعة باجي مختار- عنابة

Année : 2018/2019

Faculté: Sciences de l'Ingéniorat

Département: Electronique

MEMOIRE

Présenté en vue de l'obtention du diplôme de : LICENCE

Intitulé

Ouverture d'une serrure électrique a l'aide d'empreinte digitale

Domaine : Sciences et Technologie

Filière : Télécommunication

Par : Fernane Imed
Zabat Zineb
Chahi Rachida

DEVANT Le JURY

Directeur de mémoire :Dr.Doghmen

Remerciements :

Merci à dieu tout puissant de nous avoir donné beaucoup de force et de volonté

pour présenter ce travail. On tiens à remercier toutes les personnes qui nous ont

aidée lors de la rédaction de ce mémoire. On voudrais dans un premier temps

remercier, notre directeur de mémoire M.DOGHMEN, professeur à l'université

d'annaba , pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui

ont contribué à alimenter notre réflexion. Nos parents, et nos proches pour leur

soutien constant et leurs encouragements

I.Introduction générale

L'être humain cherche toujours à mettre en place un système de sécurité et de surveillance Fiable afin de protéger ses biens immobiliers et les locaux collectifs contre les intrusions et les Prévenir contre le vol. Les serrures ont pour but d'assurer cette tache depuis longtemps et ne Cesse pas à évoluer jusqu'au nos jours dont on trouve des serrures dites intelligentes permet de Gérer l'accès aux endroits privé d'une manière très pratique.

L'évolution technologique a permis le développement des systèmes desécurité qui deviennent de plus en plus performants. Cette évolution est due essentiellement à l'utilisation des applications de l'électronique moderne du point de vue communication entre les périphériques de commande (Bluetooth, WIFI, Infrarouge…) et coté composants (microcontrôleurs programmables, carte ARDUINO.).

Il existe une grande variété de serrures adaptées à tous types de portes et portillons, parmi eux la serrure électrique dont elle est fabriqué en acier renforcé et ne peut pas être percée ou Coupée. Cette technologie de fabrication ajoute une grande amélioration par rapport aux Serrures traditionnelles. Entre autre la sécurité représente une préoccupation au sein de l'entreprise et le commerce par l'accès à l'information.est cela pour éviter l'accès par des personnes indélicates, et avec l'explosion de l'informatique et des réseaux de communication a faitaugmenter de manière significative le besoin d identification des personnes. Jusqu'à présent lesméthodes usuelles d identification sont basées sur ce que l'on possède (carte d'identité, carte à puce badge magnétique) ou sur ce que l on sait (mot de passe, code PIN) mais ces méthodes posent degros problèmes de fiabilité (falsification de document, oubli de son code, décryptage du mot de passevia des logiciels spécifiques). Depuis les récents actes terroristes et les menaces qui pèsent sur denombreux pays, une identification fiable des personnes est devenue un problème majeur pour desraisons de sécurité (contrôle aux frontières, accès aux lieux publics, transport). Tous ces problèmesont ainsi provoqué un développement accru des techniques biométriques d identification comme en témoigne l'étude des perspectives du marché de la biométrie. La biométrie consiste en l analyse mathématique des caractéristiques biologiques d'une personne et apour objectif de déterminer son identité de manière irréfutable. Contrairement à *ce que l'on sait* ou *ceque l on possède* la biométrie est basée sur *ce que l'on est* et permet ainsi d éviter la duplication, levol, l'oubli ou la perte. Les caractéristiques utilisées doivent être *universelles* (c'est-à-dire communes àtous les individus), *uniques* (pour pouvoir différencier deux individus) et *permanentes* (c'est-à-direinvariantes dans le temps pour chaque individu).Il existe deux types de systèmes de reconnaissance biométrique : ceux basés sur la *vérification* et ceuxbasés sur l'*identification*. La vérification, également appelée authentification, consiste à confirmer ouinfirmer l'identité d'une personne (suis-je celui que je prétends être ?). Il s'agit d'une comparaison dutype *« un contre un »* ; les caractéristiques de l'individu sont comparées à celles présentes dans unenregistrement de référence. Quant à l'identification elle permet d'établir l'identité d'une personne (quisuis-je ?) à partir d'une base de données, il s'agit d'une comparaison du type *« un contre plusieurs »*.L'application qui vient immédiatement à l'esprit est l'utilisation des empreintes digitales par les forcesde l'ordre pour ficher les criminels. A titre d'exemple le FBI possèderait une base de données de250 millions d'empreintes.

II.LA SERRURE ELECTRIQUE :

II.1)_Introduction

La serrure est un système qui permet d'ouvrir ou de fermer une porte. Elle marche par l'actionnement d'une clé, d'une carte ou d'un code . La serrure électrique est fabriquée en acier renforcé et ne peut pas être percée ou coupée. Il s'agit ici d'une grande amélioration par rapport aux serrures traditionnelles.

Les serrures électriques sont utiles car elles assurent une très bonne sécurité et elles sontplus faciles à utiliser par rapport aux serrures classiques. Elles offrent également desfonctionnalités nécessaires à une sécurité absolue .

Les principales techniques de verrou électronique sont :

– Les serrures connectées Bluetooth,
– Les serrures connectées RFID (Radio Frequency Identification),
– Les serrures à infrarouge (IR),
– Les serrures à Smart code,
– Les serrures biométriques.

II.2) _DEFINITION

Serrure biométrique :

La serrure biométrique est un système de gestion des accès par l'empreinte digitale, (la rétine ou le contour des mains), seules les personnes enregistrées peuvent procéder au Déverrouillage de la porte. Il s'agit d'apporter un confort d'utilisation et une sécurité supplémentaire .Le système biométrique est composé généralement de :

– Un lecteur biométrique destiné à l'enregistrement des empreintes sur port USB,
– Une interface pour transférer les données vers la serrure biométrique.

Serrure biométrique

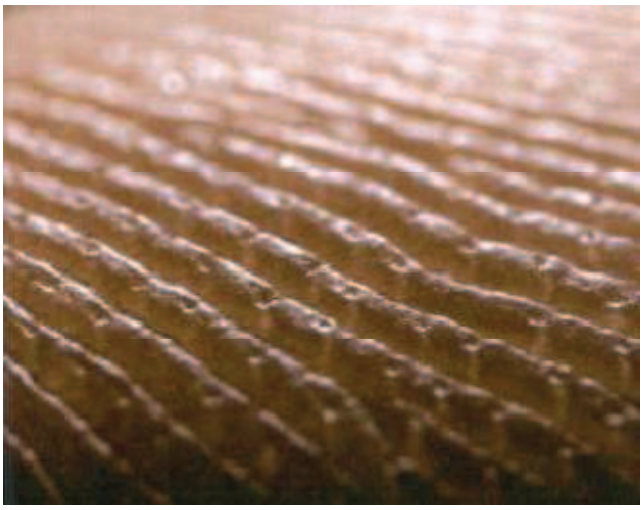
Les atouts de ce type de serrure sont :

– Grande capacité de sauvegarde d'empreinte digitale,
– Taux faible d'erreurs (acceptation ou rejet),
– Temps de vérification rapide,
– Commande simple et en temps réel de plusieurs serrures,
– Faible consommation d'énergie .

III.Empreintes digitales

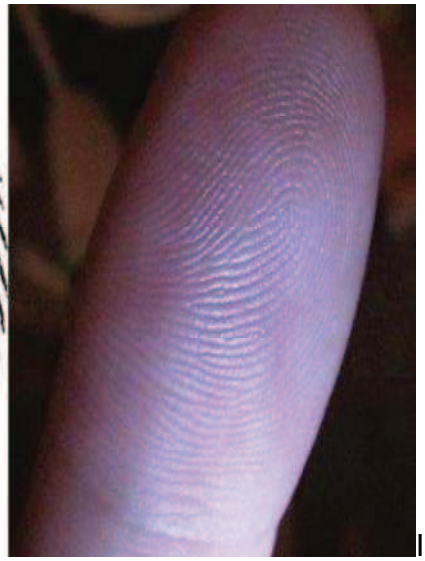
III.1. INTRODUCTION

Chez les êtres humains, les bouts des doigts ne sont pas lisses. Sur la dernière phalange de chaque doigt, ainsi que sur toute la paume de la main, la peau forme des creux et



des bosses. Les crêtes permettent une meilleure prise des objets. Les bosses quand à elles possèdent des pores qui permettent de laisser échapper la sueur créée par les glandes sudoripares.

Lorsque nous touchons un objet (ou une surface), ces liquides gras (sueurs, sécrétions grasses, acides aminés et déchets) se déposent en suivant exactement les crêtes du doigt: une empreinte digitale



apparaît comme le montre dans la figure 2. III

III.2 LES CAPTEURS DE L'EMPREINTE

III.2.1. introduction

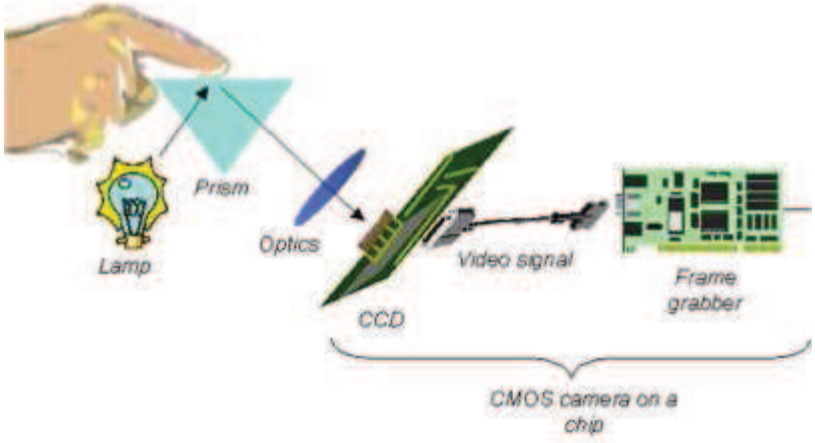
Les techniques utilisées pour capter les images des empreinte digitales sont diverses: capteurs optiques (caméras CCD), capteurs d'ultrasonique, capteurs de champ électrique, de capacité, de température...

Les difficultés générales de toutes ces techniques sont principalement :

- L'épaisseur très fine de certaines empreintes digitales dues parfois à l'origine ethnique de la personne ou encore de l'âge.

- La quantité énorme d’informations sur une très petite surface.
- L’état du doigt (humidité, sécheresse, coupures...).
- La pression plus ou moins forte exercée sur le détecteur. D’où l’importance de bien choisir l’appareil recueillant l’empreinte.

Le but de tous ces capteurs converge : La capture de l'image d'une empreinte digitale consiste à trouver les lignes tracées par les crêtes (en contact avec le capteur) et les vallées (creux)
Notre lecteur utilisé dans ce projet est Le **capteur optique** :
Ces capteurs s’assimilent à des minis-caméras : Ils sont composés d’un appareil-photo DTC(dispositif à transfert de charge) (CCD en anglais). Le doigt est apposé sur une platine enplastique dur ou en quartz, qui est en vis-à-vis de la mini caméra. Il résiste très bien auxfluctuations de température, mais est gêné par une lumière ambiante trop forte.
De plus il est assez volumineux. Son coût est intéressant, et il est intrinsèquement protégé contre les décharges électrostatiques. Il permet d’avoir des images précises et nettes.



.

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 contactavec cette dernière. Le principe de fonctionnement de ce type de capteur est représentéde manière simplifié sur la Figure ci-dessus

IV.La carte microcontrôleur (Arduino Uno R3)

IV.1. INTRODUCTION

L' "Arduino" est une carte basée sur les microcontrôleurs. Il’ y on a plus de types d' "Arduino" comme Chaque type a ses caractéristiques, et ses utilités, qui ont plusieurs avantages **:**

- Pas cher.
- Matériel Open source. C’est-à-dire : que tous les personnes qui utilise ces cartes ont la possibilité de les modifier et de les contrôlées soulons leurs besoins.
- Logiciel Open Source. C’est-à-dire:qu’on peut développer le langage d'"Arduino".
- Un environnement de programmation clair et aisé à l’utilisation.

Dans notre projet on s’intéresse à la carte "Arduino uno".
Un microcontrôleur est un circuit intégré qui rassemble les éléments essentiels
ARDUINO

IV.2. Définition du module Arduino

Le module Arduino est un circuit imprimé en matériel libre (plateforme de contrôle) dont les plans de la carte elle-même sont publiés en licence libre dont certains composants de la carte ne le sont pas : comme le microcontrôleur et les composants complémentaires.
Un microcontrôleur programmé peut analyser et produire des signaux électriques de

manière à effectuer des tâches très diverses. Arduino est utilisé dans beaucoup d'applications comme l'électrotechnique industrielle et embarquée (la domotique, le pilotage d'un robot, commande des moteurs et faire des jeux de lumières, communiquer avec l'ordinateur, commander des appareils mobiles).
Chaque module d'Arduino possède un régulateur de tension +5 V et un oscillateur à quartez 16 MHz (ou un résonateur céramique dans certains modèles). Pour programmer cette carte, on utilise l'logiciel IDE Arduino [33].

IV.3. Les gammes de la carte Arduino :

Actuellement, il existe plus de 20 versions de module Arduino, nous citons quelques un afin d'éclaircir l'évaluation de ce produit scientifique et académique :

– Le NG d'Arduino, avec une interface d'USB pour programmer et usage d'un Microcontrôleur ATmega8.
– Le NG d'Arduino plus, avec une interface d'USB pour programmer et usage d'un ATmega168.
– L'Arduino Mini, une version miniature de l'Arduino en utilisant un microcontrôleur ATmega168.

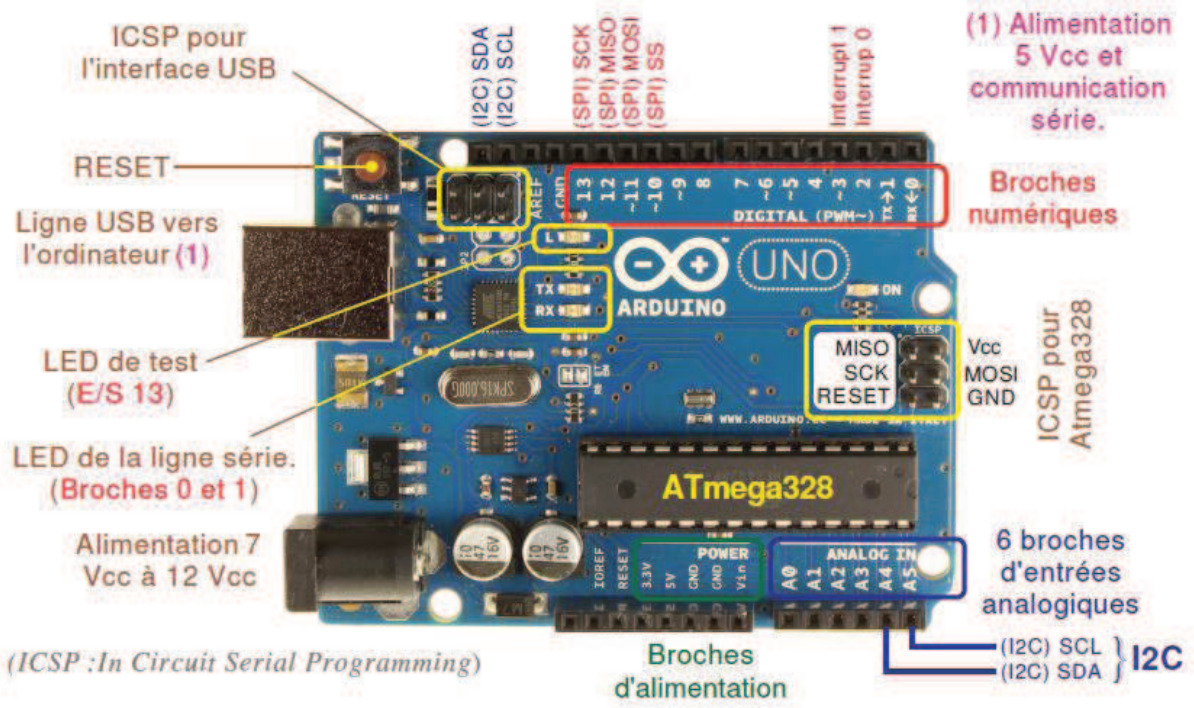
– L'Arduino Nano, une petite carte programmable à l'aide d'un porte USB, cette version utilisant un microcontrôleur ATmega168 (ATmega328 pour une plus nouvelle version).
– Le Lily Pad Arduino, une conception de minimaliste pour l'application wear able en utilisant un microcontrôleur ATmega168.
– L'Arduino Bluetooth, avec une interface de Bluetooth pour programmer en utilisant un microcontrôleur ATmega168.
– L'Arduino Diecimila, avec une interface d'USB et utilise un microcontrôleur ATmega168.
– L'Arduino Duemilanove ("2009"), en utilisant un microcontrôleur l'ATmega168 (ATmega328 pour une plus nouvelle version) et actionné par l'intermédiaire de la puissance d'USB/DC.
– L'Arduino Mega, en utilisant un microcontrôleur ATmega1280 pour I/O additionnel et mémoire.
– L'Arduino Mega2560, utilisations un microcontrôleur ATmega2560, et possède toute la mémoire à 256 KBS. Elle incorpore également le nouvel ATmega8U2.
– L'Arduino UNO, utilisations microcontrôleur ATmega328.
– L'Arduino Leonardo, avec un morceau ATmega3Ù4 qui élimine le besoin de raccordement d'USB et peut être employé comme clavier.
– L'Arduino Explora : ressemblant à un contrôleur visuel de jeu, avec un manche et des sondes intégrées pour le bruit, la lumière, la température, et l'accélération [33].

Parmi ces types, nous avons choisi une carte Arduino UNO, carte simple à manipuler, pratique et qui a un prix raisonnable.

IV.4. Une carte Arduino : est une petite carte électronique (5,33 x 6,85 cm) équipée d'un microcontrôleur, ce dernier permet, à partir d'événements détectés par des capteurs, de programmer et commander des actionneurs; la carte Arduino est donc une interface programmable

La carte Arduino UNO

Le modèle UNO de la société ARDUINO est une carte électronique dont le coeur est un microcontrôleur ATMEL de référence ATMega328. Le microcontrôleur ATMega328 est un microcontrôleur 8bits de la famille AVR dont la programmation peut être réalisée en langage C



carte Arduino UNO

IV.5 Caractéristiques techniques de la carte Arduino UNO :

– Micro contrôleur : ATmega328.
– Fréquence horloge : 16 MHz.
– Tension d'alimentation interne : 5 Vcc.
– Tension d'alimentation externe recommandée : 7-12 Vcc. (Limites : 6-20 Vcc)
– Courant max sur la sortie 3,3 V généré par le régulateur interne : 50mA.
– Entrées/sorties binaires : 14 broches.
– Courant MAX par broches en sortie : 40 mA. *(85 mA en court circuit)*
– Courant MAX cumulé par les broches en sorties : 200 mA. *(Soit 14 mA en moyenne)*
– Les E/S binaires 0 et 1 sont mobilisées par le dialogue sur la ligne série.
– S0 pour RX et S1 pour TX. Chaque broche est reliée à une LED via R = 1kΩ.
– Les E/S binaires 3, 5, 6, 9, 10, et 11 sont dédiées au mode PWM.
– L'E/S 13 est reliée sur la carte à la L ED de test via une résistance de 1kΩ.
– Entrées analogiques : 6, le niveau logique maximal doit être de +5Vcc.
– Mémoire Flash 32 KB dont 0.5 KB utilisée par le Boot loader.
– Mémoire SRAM 2 KB, Mémoire EEPROM 1 KB.
– La carte s'interface au PC par l'intermédiaire de sa prise USB.
– La carte s'alimente par le jack d'alimentation [36].

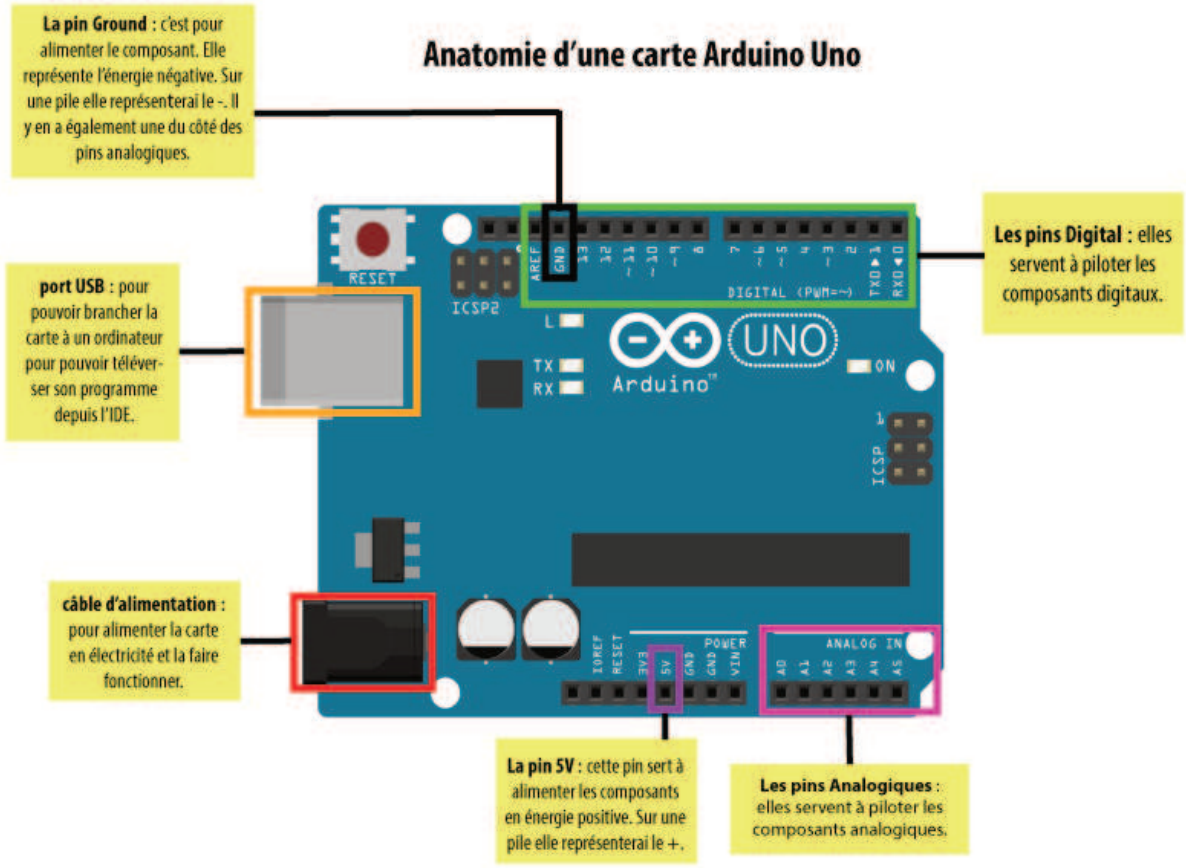
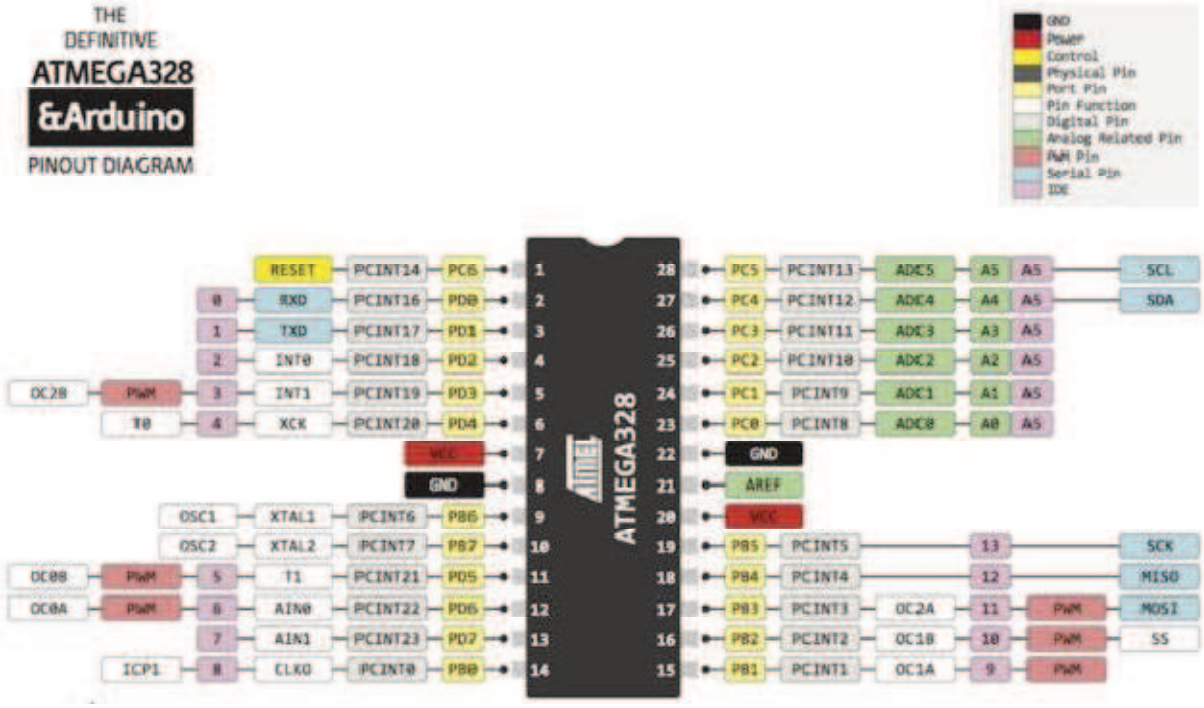


Schéma simplifié de la carte Arduino UNO :
Le microcontrôleur utilisé sur la carte Arduino UNO est un microcontrôleur ATMega328 ce dernier est un circuit intégré qui rassemble sur une puce plusieurs éléments complexes dans un espace réduit dont la programmation peut être réalisée en langage C.

Le ATMEL ATMega328 est un microcontrôleur ATMEL de la famille AVR 8bits, il se caractérise par :
– **FLASH :** mémoire programme de 32 Ko
– **SRAM :** données (volatiles) de 2 Ko
– **EEPROM :** données (non volatiles) de 1 Ko
– **Digital I/O (entrées-sorties Tout Ou Rien) :** 3 ports PortB, PortC, PortD (soit 23 broches en tout I/O)
– **Timers/Counters :** Timer 0 et Timer 2 (comptage 8 bits), Timer1 (comptage 16 bits) Chaque timer peut être utilisé pour générer deux signaux PWM. (6 broches OCxA/OCxB)
– **Plusieurs broches multi-fonctions :** certaines broches peuvent avoir plusieurs fonctions différentes choisies par programmation.
– **PWM :** 6 broches OC0A(PD6), OC0B(PD5), 0C1A(PB1), OC1B(PB3), OC2A(PB3), OC2B(PD3)
– **Convertisseur analogique-numérique (résolution 10 bits) :** 6 entrées multiplexées ADC0(PC0) à ADC5(PC5)
– **Gestion bus I2C (TWI Two Wire Interface) :** le bus est exploité via les broches **SDA(PC5)/SCL(PC4). Port série (USART) :** émission/réception série via les broches **TXD(PD1)/RXD(PD0)**
– **Comparateur Analogique :** broches AIN0(PD6) et AIN1 (PD7) peut déclencher

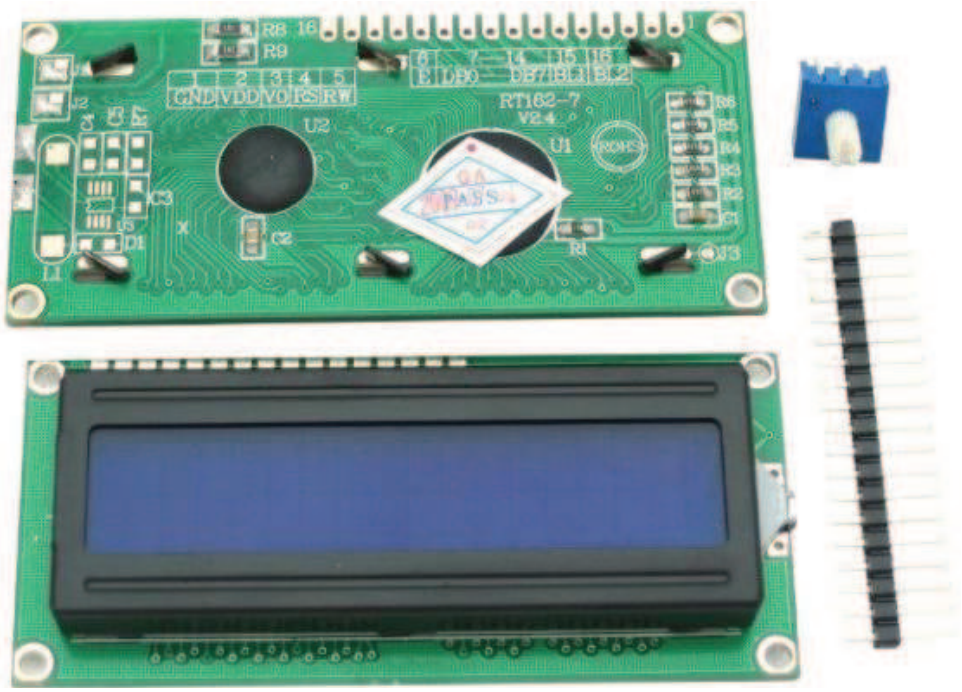
interruption Watch dog Timer programmable.
– Gestion d'interruptions (24 sources possibles (cf interrupt vectors)) : en résumé
– Interruptions liées aux entrées INT0 (PD2) et INT1 (PD3)
– Interruptions sur changement d'état des broches PCINT0 à PCINT23
– Interruptions liées aux Timers 0, 1 et 2 (plusieurs causes configurables)
– Interruption liée au comparateur analogique
– Interruption de fin de conversion ADC
– Interruptions du port série USART
– Interruption du bus TWI (I2C)



****Alimentation de la carte ARDUINO UNO :**
La carte Arduino UNO peut être alimentée via la connexion USB ou avec une alimentation externe. La source d'alimentation est automatiquement sélectionnée.
Une alimentation externe peut provenir soit d'un adaptateur AC-DC ou d'une batterie. L'adaptateur peut être connecté en branchant une prise 2.1 mm dans la prise d'alimentation de la carte ou à partir d'une batterie connectée dans le pin (ou broche) GND et V-in (alimentation externe).
Le processeur peut fonctionner sur une alimentation externe de 6 à 20 volts. Cependant, si la tension est inférieure à 7V, le pin 5V peut fournir moins de cinq volts et le processeur peut devenir instable. Si la tension est supérieure à 12V, le régulateur de tension peut surchauffer et endommager la carte. La plage recommandée est de 7 à 12 volts .

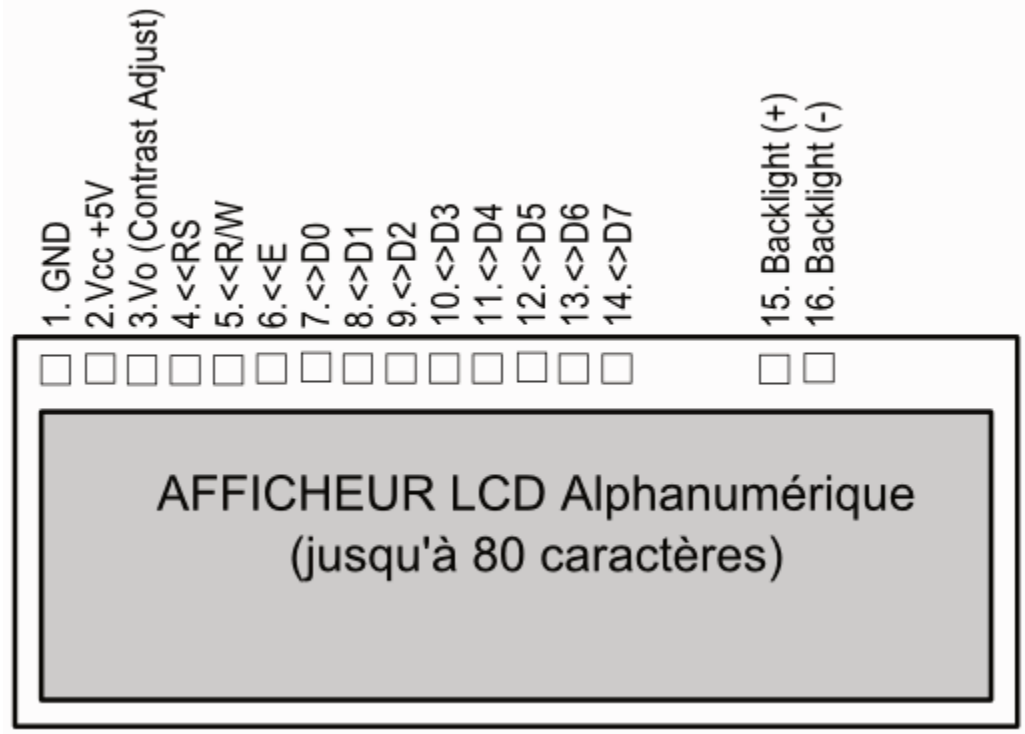
V. Unité de sortie et de communication (Afficheur **LCD**)

Les afficheurs à cristaux liquides, autrement appelés afficheurs LCD (Liquid Crystal Display), sont des modules compacts intelligents et nécessitent peu de composants externes pour un bon fonctionnement. Ils consomment relativement peu (de 1 à 5 mA), sont relativement bons marchés et s'utilisent avec beaucoup de facilité (voir Annexe 01).
Plusieurs afficheurs sont disponibles sur le marché et diffèrent les uns des autres, non seulement par leurs dimensions, (de 1 à 4 lignes de 6 à 80 caractères), mais aussi par leurs caractéristiques techniques et leur tension de service. Certains sont dotés d'un rétro éclairage de l'affichage. Cette fonction fait appel à des LED montées derrière l'écran du module, cependant, cet éclairage est gourmand en intensité (de 80 à 250 mA) .



Brochage d'un afficheur LCD

Le brochage d'un écran LCD est "normalisé" avec 14 broche (ou 16 si l'écran est rétroéclairé) pour les "petits formats" (voir Annexe 02):



Broche Nom Niveau Fonction

1 GND - Masse

2 VCC - Alimentation positive (+5V).

3 Vo 0-5V Cette tension permet, en la faisant varier entre 0 et +5V, le réglage du contraste de l'afficheur.

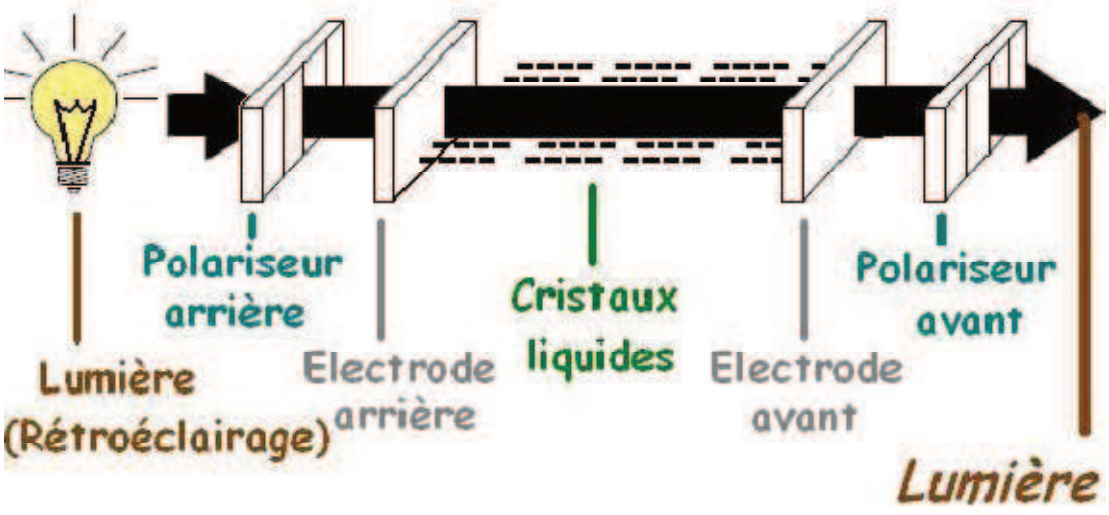
4 RS TTL Sélection du registre (Register Select) Grâce à cette broche, l'afficheur est capable de faire la différence entre une commande et une donnée. Un niveau bas indique une commande et un niveau haut indique une donnée.

5 RW TTL Lecture ou écriture (Read/Write)
L : Écriture
H : Lecture
6 E TTL Entrée de validation (Enable) active sur front descendant. Le niveau haut doit être maintenue pendant au moins 450 ns à l'état haut.
7 D0 TTL Bus de données bidirectionnel 3 états (haute impédance lorsque E=0)
8 D1 TTL
9 D2 TTL
10 D3 TTL
11 D4 TTL
12 D5 TTL
13 D6 TTL
14 D7 TTL
15 A - Anode rétro éclairage (+5V)
16 K - Cathode rétro éclairage (masse)

Ce Tableau explique le rôle et nom de chaque broche d'un afficheur LCD Tout projet qui nécessite tant de convivialité ou de contrôle pour l'utilisateur doit comporter un afficheur. En effet, celui-ci permet de manière très rapide de révéler n'importe quelle information qui pourrait être utile au programmeur ou à l'usager.

V.1Principe de fonctionnement d'un écran LCD

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



VI.Partie programmation :

Notre projet peut réaliser de deux modes :

1- Mode autonome : lorsque notre système est indépendant du pc
2- Mode semi-autonome : lorsque notre système dépend du pc

On a travaillé avec trois programmes dans les deux modes , qui sont comme suit :

- **Mode 1 :**

- **<u>Programme 1 : (mot de passe)</u>**

```
#include <EEPROM.h>
#define N 4 // ne depasse pas 63 passwords
byte possword[N][4] = {{'1','2','3','4'},
                       {'2','2','4','6'},
                       {'9','9','1','0'},
                       {'8','7','6','3'}};
void setup() {
  pinMode(13, OUTPUT);
  digitalWrite(13, LOW);
  delay(1000);
  int addr = 0;
  for(int i=0;i < N; i++) {
    for(int j=0;j < 4; j++) {
      EEPROM.write(addr, possword[i][j]);
      addr++;
    }
  }
  EEPROM.write(255, N);
  digitalWrite(13, HIGH);
}
void loop() {
}
```

Programme 2 : (enrolling(enregistrement et authentification des empreintes digitales) :

```
#include <SoftwareSerial.h>
#include <Adafruit_Fingerprint.h>
SoftwareSerial mySerial(2, 3);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
byte id = 1;
int stat;
void setup() {
  Serial.begin(9600);
  finger.begin(57600);
  if (finger.verifyPassword()) {
    Serial.println("Found fingerprint sensor!");
  } else {
    Serial.println("Did not find fingerprint sensor");
    while(1) {
      continue;
    }
  }
  Serial.println("WELCOM YOU ARE IN ENROLL MODE");
}
void loop() {
  Serial.print("Fingerprint : ");
  Serial.println(id, DEC);
  img1: stat = finger.getImage();
  if(stat == FINGERPRINT_OK) {
    stat = finger.image2Tz(1);
    if(stat == FINGERPRINT_OK) {
      img2: stat = finger.getImage();
      if(stat == FINGERPRINT_OK) {
       stat = finger.image2Tz(2);
        if(stat == FINGERPRINT_OK) {
          stat = finger.createModel();
          if(stat == FINGERPRINT_OK) {
            stat = finger.storeModel(id);
            if(stat == FINGERPRINT_OK) {
```

```
          Serial.println("CREATING and MODELING FINGERPRINT BY SCUSSED");
          id++;
          Serial.println("Type 'N' to stop enrolling or any key for continue: ");
          while(!Serial.available()){};
          char ans = Serial.read();
          if(ans == 'N') {
            Serial.println("Enrolling operation is stoped !!!");
            while(1) {};
          }
          if(id==128) {
            Serial.println("Fingerprint is FULL !!!");
            while(1) {};
          }
        } else {
          Serial.println("ERROR STORE MODEL");
          return;
        }
      } else {
        Serial.println("ERROR CREATE MODEL");
        return;
      }
    } else {
      Serial.println("ERROR CONVERT IMAGE 2");
      return;
    }
  } else {
    goto img2;
  }
 } else {
  Serial.println("ERROR CONVERT IMAGE 1");
  return;
 }
} else {
 goto img1;
}   }
```

- **Programme 3 : utilisation**

```
#include <EEPROM.h>
#include <Keypad.h>
#include <SoftwareSerial.h>
#include <Adafruit_Fingerprint.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>

#define LEN 4
#define redLED 12
#define greenLED 13

//============================================================
// Set the LCD address to 0x27 for a 16 chars and 2 line display
LiquidCrystal_I2C lcd(0x27, 16, 2);
//============================================================

//============================================================
SoftwareSerial mySerial(2, 3);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
//============================================================
const byte rows = 4; //number of the keypad's rows and columns
const byte cols = 4;

char keyMap [rows] [cols] = { //define the cymbols on the buttons of the keypad

  {'1', '2', '3', 'A'},
  {'4', '5', '6', 'B'},
  {'7', '8', '9', 'C'},
  {'*', '0', '#', 'D'}
};
byte rowPins [rows] = {8, 9, 10, 11}; //pins of the keypad
byte colPins [cols] = {4, 5, 6, 7};
Keypad myKeypad = Keypad( makeKeymap(keyMap), rowPins, colPins, rows, cols);
//============================================================================
byte N;
byte inBuffer[4];
int stat;
char Key;
void setup() {
  N = EEPROM.read(255);
  pinMode(greenLED, OUTPUT);
  pinMode(redLED, OUTPUT);
  Serial.begin(9600);
  finger.begin(57600);
  lcd.begin();
  lcd.backlight();
  digitalWrite(greenLED, LOW);
  digitalWrite(redLED, LOW);
  if (finger.verifyPassword()) {
    //Serial.println("Found fingerprint sensor!");
  } else {
    lcd.print("Not found FPS!");
    while(1) {
      continue;
    }
  }
}
void loop() {
  // lecture de password
//  Serial.println("Enter PASSWORD (4 digits)!");
//  for(int i=0; i<4; i++) {
//    while(!Serial.available()) {};
//    inBuffer[i] = Serial.read();
//  }
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print(" Enter Password ");
```

```
lcd.setCursor(6, 1);
for(int i=0; i<LEN; i++) {
  again: Key = myKeypad.getKey();
  if(Key==0) {
    goto again;
  }
  inBuffer[i] = Key;
  lcd.print("*");
}
// verification de password
int pass = 0;
int addr = 0;
for(int i=0; i<N; i++) {
  for(int j=0; j<4; j++) {
    if(inBuffer[j] != EEPROM.read(addr)) {
      pass++;
      break;
    }
    addr++;
  }
  if (i==pass) {
    break;
  }
  addr = (i+1)*4;
}

if(pass!=N) {
  // fingerprint authontification
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("GET FINGERPRINT!");
  img3: stat = finger.getImage();
  if(stat == FINGERPRINT_OK) {
    stat = finger.image2Tz();
    if(stat == FINGERPRINT_OK) {
      stat = finger.fingerFastSearch();
      if(stat == FINGERPRINT_OK) {
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("Found ID #");
        lcd.setCursor(0, 1);
        lcd.print(finger.fingerID, DEC);
        // blink green led
        digitalWrite(greenLED, HIGH);
        delay(1000);
        digitalWrite(greenLED, LOW);
        return;
      } else {
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("NOT Found!!!");
        // blink red led
        digitalWrite(redLED, HIGH);
        delay(1000);
        digitalWrite(redLED, LOW);
        return;
      }
    } else {
      //Serial.println("PUT YOUR FINGER AGAIN");
      goto img3;
    }
  } else {
    //Serial.println("PUT YOUR FINGER AGAIN");
    goto img3;
  }
} else {
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Incorrect PASS!");
  // blink red led
```

```
    digitalWrite(redLED, HIGH);
    delay(1000);
    digitalWrite(redLED, LOW);
    return;
  }
}
```

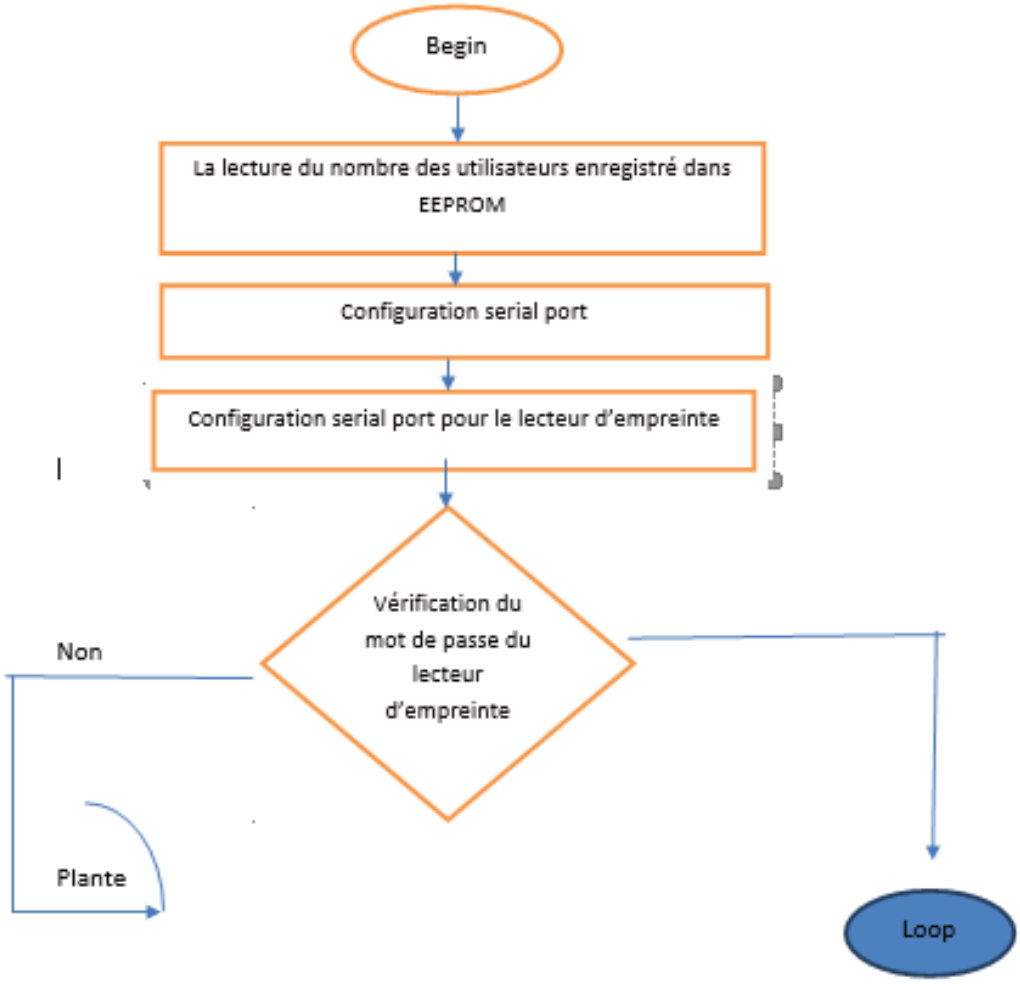
Les deux modes se diffèrent au niveau du troisième code seulement :

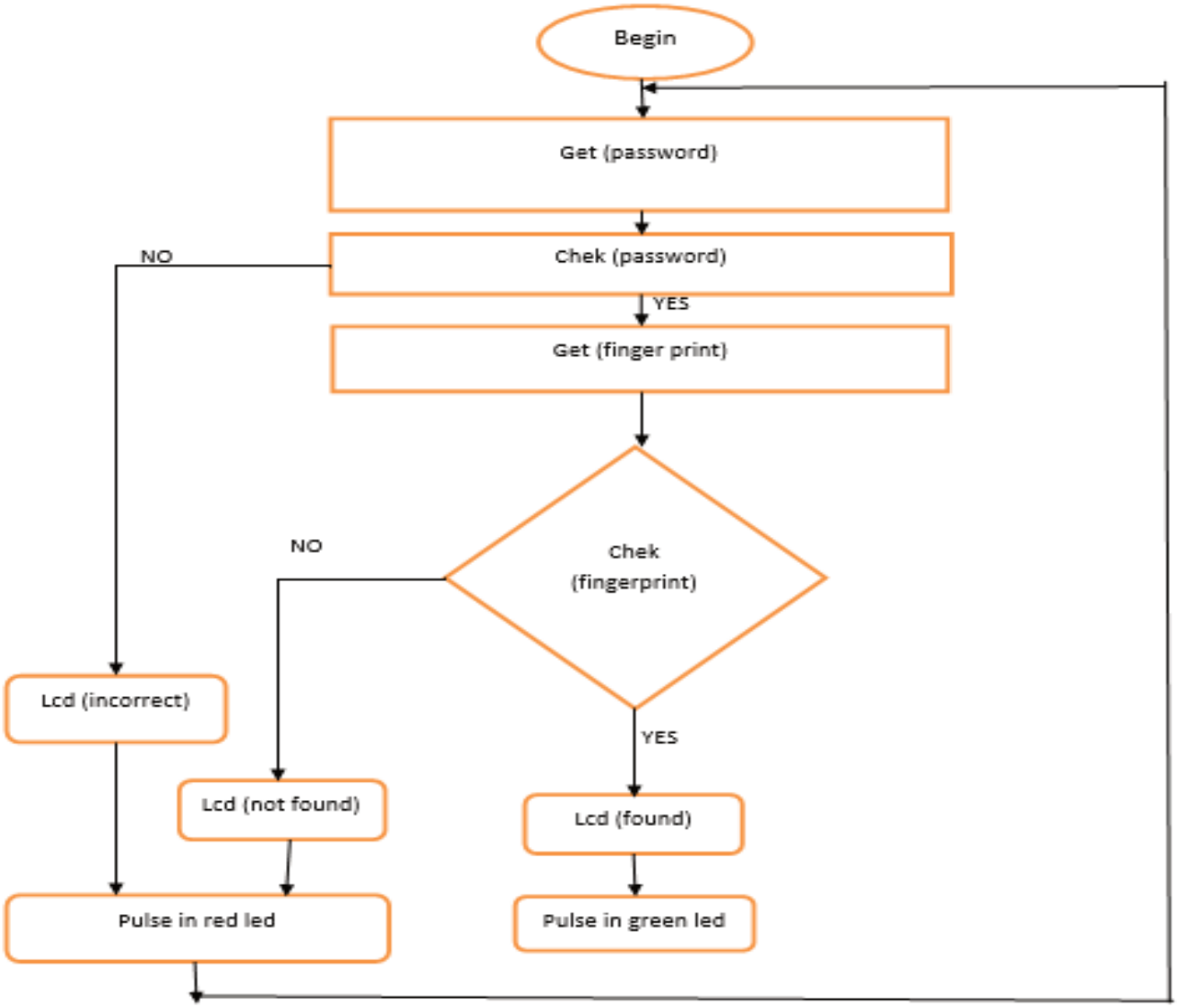
- **Mode 2 :**

```
#include <EEPROM.h>
#include <SoftwareSerial.h>
#include <Adafruit_Fingerprint.h>
//==========================================================
SoftwareSerial mySerial(2, 3);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
//==========================================================
byte N;
byte inBuffer[4];
int stat;

void setup() {
  N = EEPROM.read(255);
  Serial.begin(9600);
  finger.begin(57600);
  if (finger.verifyPassword()) {
    Serial.println("Found fingerprint sensor!");
  } else {
    Serial.println("Did not find fingerprint sensor");
    while(1) {
      continue;
    }
  }
}

void loop() {
  // lecture de password
  Serial.println("Enter PASSWORD (4 digits)!");
  for(int i=0; i<4; i++) {
    while(!Serial.available()) {};
    inBuffer[i] = Serial.read();
  }
  // verification de password
  int pass = 0;
  int addr = 0;
  for(int i=0; i<N; i++) {
    for(int j=0; j<4; j++) {
      if(inBuffer[j] != EEPROM.read(addr)) {
        pass++;
        break;
      }
      addr++;
    }
    if (i==pass) {
      break;
    }
    addr = (i+1)*4;
  }

  if(pass!=N) {
    // fingerprint authontification
    img3: stat = finger.getImage();
    if(stat == FINGERPRINT_OK) {
      stat = finger.image2Tz();
      if(stat == FINGERPRINT_OK) {
        stat = finger.fingerFastSearch();
        if(stat == FINGERPRINT_OK) {
          Serial.print("Found ID #");
          Serial.println(finger.fingerID);
          return;
        } else {
       Serial.println("NOT Found!!!");
```

```
        return;
       }
      } else {
       Serial.println("PUT YOUR FINGER AGAIN");
       goto img3;
      }
     } else {
      Serial.println("PUT YOUR FINGER AGAIN");
      goto img3;
     }
    } else {
     Serial.println("Incorrect PASSWORD!!!");
     return;
    }
}
```

- **VII.l'organigramme : partie setup et Loop :**





VIII.Réalisation pratique :

Etape 1 : assurance de tous les dispositifs électroniques nécessaires pour notre projet .

Etape 2 :le clavier, le lecteur d'empreinte et l'afficheur LCD sont tous reliés à l'ARDWINO UNO comme ci-dessous

- **le clavier :** les lignes (8 9 10 11) ; les colonnes (4 5 6 7) .
- **lecteur d'empreinte :** Rx à 2 ; Tx à 3 ; GND ; Vcc .
- **LCD :** VTS ; DTS ; GND ; Vcc .
  LE résultat de la réalisation peut se voir à l'aide de deux LED (verte pour une ouverture réussite et la rouge pour une ouverture échouée) reliées avec les pins 13et 12 respectivement .

VIIII.Conclusion

Au cours de ce projet on a vu que la sécurité d'accès présente un vrai problème. Il nous oblige de trouver des moyens pour sécuriser un endroit .
Depuis plusieurs années plusieurs techniques sont élaborées pour le faire , parmi ces techniques :
*l'accès par un code ou un mot de passe .
*l'accès biométrique (empreinte digitale …….).
La biométrie par l'empreinte digitale est la technologie la plus employée à travers le monde et on voit fleurir des solutions de plus en plus abordables et performantes.
Pour réaliser cette technique on ait utilisé une carte microcontrôleur Arduino qui possède un espace de programmation qui est très claire et simple . Cette carte sert à contrôler un lecteur d'empreinte digitale.

Résumé :

Notre projet de fin de cycle consiste à la réalisation d'une serrure électrique qui s'ouvre avec l'empreinte digital et un mot de passe à base d'arduino. Un tel système peut être semi autonome où autonome, lorsque quelqu'un veux accéder à une pièce où une maison qui utilise se système de sécurité il doit taper tout d'abord son propre mot de passe s'il est correcte il l'autorise à entrer l'empreinte donc la porte s'ouvre et si le mot est incorrecte et lui donne pas l'accès à l'empreinte et la porte ne s'ouvre pas donc notre système assure une meilleure authentification et une meilleure sécurité ce processus est utilisé pour sécuriser les portes et les coffres forts par exemple.

Our end-of-course project includes the creation of an electric lock that opens using a digital fingerprint and an Arduino-based password. This system can be semi-independent or independent. When someone wants to access a house or place that uses a security system, he must first type his password if it is correct. He will be allowed to enter the fingerprint until the door is opened and if the word is incorrect it will not allow It will not open the door so our system provides better authentication and better security. This type of system is used to ensure the security of houses and safes, for example

يتضمن مشروع نهاية الدورة الخاص بنا إنشاء قفل كهربائي يفتح باستخدام البصمة الرقمية وكلمة مرور قائمة على Arduino. يمكن أن يكون هذا النظام شبه مستقل أو مستقل ، عندما يريد شخص ما الوصول إلى منزل أو مكان يستخدم نظامًا أمنيًا ، يجب عليه أولاً كتابة كلمة المرور الخاصة به إذا كانت صحيحة ، فسيسمح له بادخال البصمة حتى يفتح الباب وإذا كانت الكلمة غير صحيحة فإنه لن يسمح له بإدخال البصمة ولن يفتح الباب حتى يوفر نظامنا مصادقة أفضل وأمن أفضل ، يتم استخدام هذا النوع من الأنظمة لضمان أمن المنازل و الخزائن على سبيل المثال..

SOMMAIRE