الجمهـــوريـــــة الجزائـــريـــــة الديمقـــراطيـــة الشـعبيـــة
République Algérienne Démocratique et Populaire
وزارة التـــعلـــيـــــم العـــــالـــــي والبـــحـــــث العـلمـــــي
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

جامعة وهران 2 محمدبن أحمد
Université d'Oran 2 Mohamed Ben Ahmed

معهد الصيانة والأمن الصناعي
Institut de Maintenance et de Sécurité Industrielle

Département de Maintenance en Instrumentation

MÉMOIRE

Pour l'obtention du diplôme de Master

Filière : Génie industrielle

Spécialité: Ingénierie de la Maintenance en Instrumentation

Thème

Conception et réalisation d'une pointeuse biométrique

Encadré par :

BENAYAD Ahmed

Présenté et soutenu publiquement par :

CHEHIDA Habib

SEDDJAR Nasreddine

Devant le jury composé de :

Nom et Prénom	Grade	Etablissement	Qualité
ZEBIRATE Soraya	**Professeur**	**IMSI**	**Présidente**
HASSINI Abdelatif	**Professeur**	**IMSI**	**Examinateur**

Juin 2016

Dédicaces

A ma mère

Pour son amour et son courage

A mon père

Pour m'avoir inculqué les valeurs auxquelles je tiens tant

A mes sœurs et à mon frère

Vous êtes dans mon cœur

A mon binôme, et non moins frère Habib

A ma famille et aux gens que j'aime

Nasreddine

Remerciement

Nous tenons à remercier les personnes les plus chères à nos cœurs, à nos familles d'exceptions pour leurs soutiens moraux et leurs présences permanentes.

En premier lieu, Nous tenons à exprimer notre profonde gratitude à monsieur Benayad Ahmed, Directeur de l'Institut de maintenance et sécurité industrielle pour nous avoir encadré avec un grand cœur, pour sa disponibilité, pour les précieux conseils constructifs et n'oublions pas sa patience et gentillesse.

Nous tenons aussi à exprimer nos remerciements et sentiments les plus respectueux a Madame Zebirate Soraya, Professeur à l'Institut de maintenance et sécurité industrielle, pour nous avoir fait l'honneur de présider le jury de soutenance.

Nos très vifs remerciements vont aussi à Monsieur Hassini Abdelatif, Professeur à l'Institut de maintenance et sécurité industrielle, pour sa participation à l'évaluation de ce mémoire à titre de membre du jury.

Enfin, nous adressons nos plus sincères remerciement à tous nos amis, qui nous ont toujours soutenu et encouragé au cours de la réalisation de ce modeste travail

Merci

الملخص:

البيومترية هو مصطلح علمي يشير إلى القياس الحيوي وهو علم يختص بتحديد هوية الافراد بناءا على سماتهم البيولوجية. وهذا المجال التكنولوجي النامي اصبح له تأثيرات عميقة في حياتنا اليومية مع ارتباطه باثبات الهوية الذي يشكل بدوره جزء لا يتجزء من حياتنا. وتستخدم هذه التقنية أكثر فأكثر اليوم في تحديد هوية الافراد في العديد من التطبيقات المختلفة. هذا العلم يمكن ادماجه مع مسجل الوقت، ولهذا الغرض فان البحث مقدم في هذه المذكرة يعالج قضية دمج البيومترية في مسجل الوقت. على وجه التحديد، فإن الهدف من هذا العمل هو انجاز مسجل الوقت البيومتري آلي ببصمات الاصابع مع امكانية التحكم على واجهة متعددة الاستخدام.

الكلمات الاساسية: البيومترية ، مسجل الوقت ، بصمات الأصابع، اردوينو، راسبيري باي 2

Résumé :

La **biométrie** est une mesure des caractéristiques biologiques pour l'authentification d'un individu à partir de certaines de ses caractéristiques.

Cette technique est utilisée de plus en plus aujourd'hui pour établir la reconnaissance de la personne dans un grand nombre d'applications diverses. Cette science trouve une application pratique avec la **pointeuse** biométrique. En conséquence, les travaux de recherche présentés dans ce mémoire traitent la problématique d'intégration de la biométrie dans la pointeuse. Plus précisément, l'objectif de ce travail est de réaliser une pointeuse biométrique par **empreinte digital** permettant la gestion automatique de la tâche du pointage avec une interface multiplateforme.

Mots clés : biométrie, pointeuse, empreinte digitale, Arduino, Raspberry PI2.

Table des matières

Introduction générale

Introduction générale

Il est nécessaire de rappeler les notions de pointeuse et de biométrie et ceci dans le but que le lecteur puisse comprendre la suite de notre mémoire.

La pointeuse à l'origine était une machine qui permet d'enregistrer le temps de travail d'un salarié. Aujourd'hui elle n'est plus confiées uniquement à ce rôle, cependant elle peut enregistrer le début et la fin d'une tache, ou juste sa durée ; elle peut contenir la liste entière des tâches à accomplir pour mener à bien un projet ou un programme. Ces informations peuvent être utilisées pour les fiches de paie, les factures, et pour valider les titres de transports ou autre.

La biométrie est une science qui permet d'identifier, répertorier et quantifier statistiquement la physiologie du corps humain et son évolution dans le temps, telle que la biométrie de la reconnaissance de la main qui est une solution très conviviale et facile à mettre en œuvre. Elle est largement utilisée dans divers domaines que ce soit dans le contrôle d'accès, la gestion d'entrée et de sortie, etc.

Cette science trouve une application pratique avec la pointeuse biométrique, dispositif qui utilise des données issues de la physiologie humaine pour procéder à des tâches de contrôle. Elle est très utilisée par le secteur public et entreprise car les données qu'elle utilise sont des caractéristiques humaines inimitables, ce qui garantit leur fiabilité et leur constance.

La pointeuse biométrique s'est généralisé et perfectionné au cours du temps à tel point qu'aujourd'hui un même terme désigne des systèmes différents souvent éloignés, par leurs caractéristiques et performances, de la pointeuse d'origine.

Parmi les systèmes de pointage développés, on trouve différents types de pointeuses :

- pointeuse mécanique ;
- pointeuse numérique ;
- badgeuse ;
- pointeuse mobile ;
- pointeuse biométrique.

Actuellement, le type de pointeuse le plus avancé est la pointeuse biométrique, grâce à ça technique basée sur des données physiologiques personnelles. Cet instrument, de par ces avantages qualitatifs et quantitatifs, fait l'objet d'un grand nombre de recherches en ce moment.

On peut dire d'une façon générale que la biométrie regroupe : « l'ensemble des techniques informatiques visant à reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales ». Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN (acide désoxyribonucléique), empreintes digitales, etc.). Elles se rapprochent ainsi de ce qui pourrait être défini comme un « identificateur unique universel », permettant, de fait, le traçage généralisé des individus.

Le but de la biométrie dans le contrôle d'accès est de gérer les accès physiques ou logiques afin d'accroître la sécurisation des accès à des locaux de tous types mais aussi sécuriser l'accès à des stations informatiques et aux dossiers et fichiers présents sur ces dernières. La biométrie commence à être utilisée également afin d'authentifier un utilisateur lors de transactions bancaires pour sécuriser les paiements via des terminaux physiques ou encore pour des paiements en ligne.

Il existe de nombreux systèmes biométriques pour le contrôle d'accès que nous pouvons séparer en 2 grandes familles : avec ou sans contact physique.

La biométrie avec contact physique est très répandue. Elle comprend la reconnaissance de l'empreinte digitale, de la morphologie de la main ou encore en mode multimodal avec analyse combinée et simultanée de l'empreinte digitale et du réseau veineux du doigt. Dans le monde, l'une des technologies les plus utilisées est la biométrie via l'empreinte digitale, autant au niveau du contrôle des individus (passeport, carte d'identité et permis de conduire biométrique) qu'au niveau du contrôle d'accès.

Au niveau des technologies sans contact, il existe des systèmes à reconnaissance faciale, de l'iris et du réseau veineux de la paume de la main.

L'exploitation de ces données elle aussi a évolué. A l'origine, l'exploitation des données imprimées sur le carton de pointage se faisait manuellement (lecture des heures imprimées + addition et totalisation/récapitulation) sans l'appui d'un système automatique ; ensuite, les pointeuses réalisaient elles-mêmes les totalisations ; et actuellement, l'introduction de « puces » avec calculateur intégré épargne tout souci de calcul, quel qu'il soit.

L'objectif principal dans notre travail est de permettre à des entreprises l'auto-gérance du pointage de ses fonctionnaires tout en assurant un contrôle intelligent de cette opération en temps réel. Ceci passe inévitablement par, étudier, analyser et proposer un système de pointage complet et flexible.

C’est dans ce cadre que s’inscrit notre mémoire de master, retraçant une conception et une réalisation d'un système de pointage intelligent qui répond aux attentes des utilisateurs. Ainsi notre choix s’est porté sur la pointeuse biométrique.

Notre travail demandé dans le cahier de charge, nous l’avons scindé en deux parties :

Première partie :

- Etude générale des pointeuses ;
- Etude de la pointeuse biométrique.

Deuxième partie :

- Conception et réalisation de la pointeuse biométrique.

Chapitre I
La pointeuse

La pointeuse

I.1. Introduction

Ce chapitre est consacré entièrement à l'historique et à la description de quelques pointeuses tout en donnant le principe de fonctionnement et aussi leur évolution avec le temps.

Une pointeuse ou badgeuse, également appelée timbreuse, est une machine qui permet d'enregistrer le temps de travail d'un salarié. Elle est à l'origine d'un système mécanique d'horlogerie qui enregistre le début et la fin de la séquence de travail et imprime sur un support matériel de papier ou de carton ce qu'elle a enregistré.

L'apparition des pointeuses à la fin du 19^{e} siècle est une conséquence de la révolution industrielle. L'une des premières pointeuses a été inventée par Willard Bundy Le Grand le 20 Novembre 1888. Son brevet de 1890 parle d'enregistreurs de temps mécaniques pour les travailleurs dans des termes qui suggèrent que les enregistreurs antérieurs existaient déjà, mais Bundy a fait plusieurs améliorations; par exemple, chaque travailleur avait sa propre clé. Un an plus tard, son frère, Harlow Bundy, a créé la Bundy Manufacturing Company, pour pouvoir commercialiser la nouvelle pointeuse [1].

Figure I-1. La pointeuse de Bundy

Certains employeurs se sont retrouvés à la tête de fabriques regroupant des centaines de personnes payées au temps. Un temps de travail qu'il convenait de mesurer pour :

- **contrôler** la réalité et la quantité de la prestation de travail de l'ouvrier ;
- le **payer** selon les heures qu'il avait véritablement effectuées.

Avec ce système, le salarié glissait dans la pointeuse un carton (portant son nom) lorsqu'il prenait son poste, geste qu'il répétait en partant.

I.2. Chronographie

I.2.1. Les pointeuses à carton de type cisaillées

A chaque pointage un couteau découpait un petit bout de carton permettant de décaler la ligne d'écriture pour le pointage suivant.

La pointeuse à cartons était une base de temps reliée à un système d'impression de différents types selon leurs années de conception.

La première pointeuse avait une poignée manuelle sur laquelle l'utilisateur appuyait après avoir introduit sa carte de pointage. Ce type de pointeuses était souvent à remontage mécanique car non reliées sur le secteur.

Figure I-2. Horloges Pointeuses à cartes cisaillées 1905 (environ).

La deuxième évolution fût de pouvoir relier la pointeuse sur le secteur ce qui permet d'y ajouter un moteur de remontage automatique du ressort barillet et de proposer à l'utilisateur un pointage automatique à introduction de la carte de pointage, des micros contacts détectaient la présence de la carte et actionnaient un électro-aimant pour déclencher la frappe au bon endroit

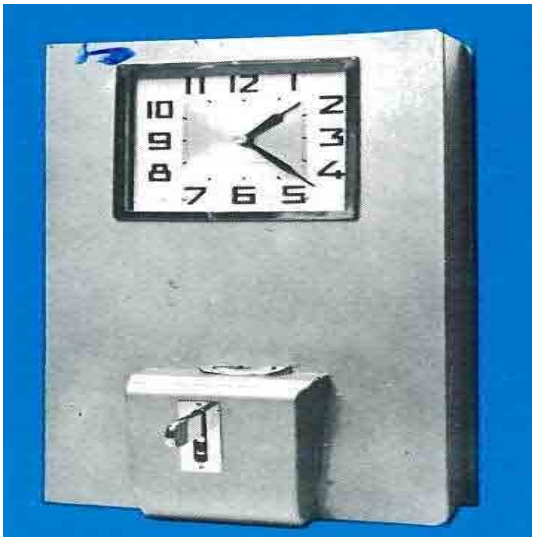

Figure I-3. Horloge Pointeuse à cartes cisaillées à partir de 1948

La troisième évolution fût bien sur l'arrivée du quartz, le principe de fonctionnement était le même mais la base de temps était régulée par ce fameux quartz remplaçant définitivement les mouvements d'horlogeries mécaniques sur toutes les pointeuses. Par contre Lambert continue à fabriquer des pointeuses à déclenchement manuel car elles sont très robustes et peuvent fonctionner dans les endroits les plus hostiles et même à l'extérieur [2].

Figure I-4. Pendule Pointeuse à cartes cisaillées (1978)

I.2.2. Les pointeuses type horodateurs

Ce système fonctionne comme un composteur et il permet d'inscrire l'heure et la date sur tous les documents. Il est aujourd'hui encore utilisé pour le courrier ou pour les bons de travaux en atelier. Ils servaient aussi beaucoup dans les assurances pour valider les prises de contrats, ils étaient alors plombés afin que personne ne puisse modifier l'heure [2].

Figure I-5. Pendule Pointeuse Horodateur (1905)

Figure I-6. Pendule Pointeuse Horodateur (2005)

I.2.3. Les pointeuses à carton de type cadastrées par programmation

La carte de pointage est divisée en plusieurs cases, généralement 6 colonnes (entrée matin / sortie matin / entrée après-midi / sortie après-midi / et 2 colonnes pour les pointages irréguliers) certaines pointeuses affichaient tout le mois sur la même face, d'autres étaient recto / verso (Première et deuxième quinzaine).

Sur les premiers modèles le pointage était mécanique (marteau de frappe relié à un électro-aimant) aujourd'hui l'impression de toutes pointeuses se fait grâce à une imprimante à aiguilles.

Lors de la mise en service de la pointeuse l'utilisateur programme l'heure des changements de colonne

- *Exemple* : Horaire de l'entreprise 8H00 12H00 13H30 17H30 dans ce cas la programmation sera la suivante :
    - Pointage en première colonne de 00H00 à 10H00
    - Pointage en deuxième colonne de 10H01 à 12H30
    - Pointage en troisième colonne de 12H31 à 15H30
    - Pointage en quatrième colonne de 15H31 à 23H59

Sur les premières pointeuses cadastrées le changement de colonne se faisait grâce à des cames sur lesquels un palpeur venait se caler, le système était entièrement mécanique.

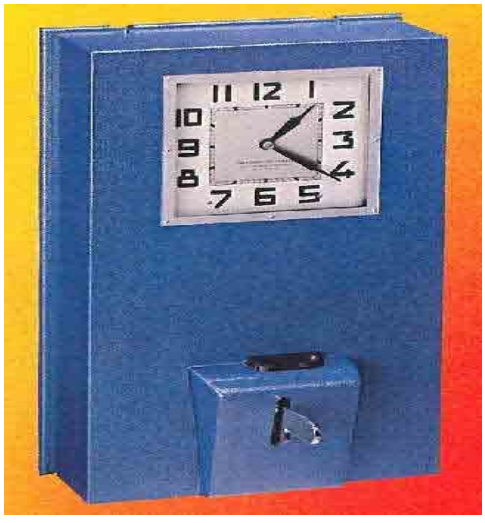

Figure I-7. Pendule Pointeuse à cartes cadastrées (1970-1978)

Par la suite une roue de programmation munie de taquets que l'on déplaçait faisait le rôle de programmateur sur la pointeuse.

Figure I-8. Pendule Pointeuse à cartes cadastrées (1978-1985)

Les dernières générations de pointeuses cadastrées sont maintenant totalement électroniques [2].

Figure I-9. Pendule Pointeuse à cartes cadastrées (2003)

I.2.4. Les pointeuses type compteur horaires variables individuelles

Chaque utilisateur dispose de son propre compteur électromécanique et de sa propre clé de mise en marche. Lorsque l'utilisateur prend son poste il lui suffit alors de donner un tour de clés pour mettre son compteur en route, il fait l'opération inverse lors du départ de son poste. Il suffit de relever les compteurs en fin de période pour obtenir un résultat d'heures.

Des centaines de ce type de systèmes furent installés notamment dans les administrations et les grands groupes dès l'arrivée des horaires variables [2].

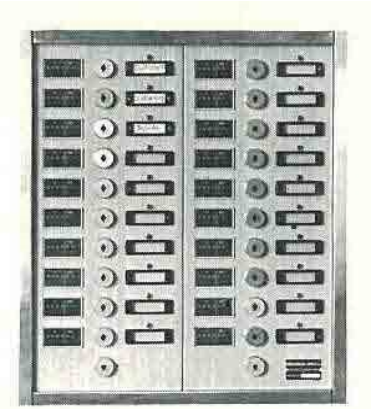

Figure I-10. Pointeuse compteurs d'horaires variables (1976)

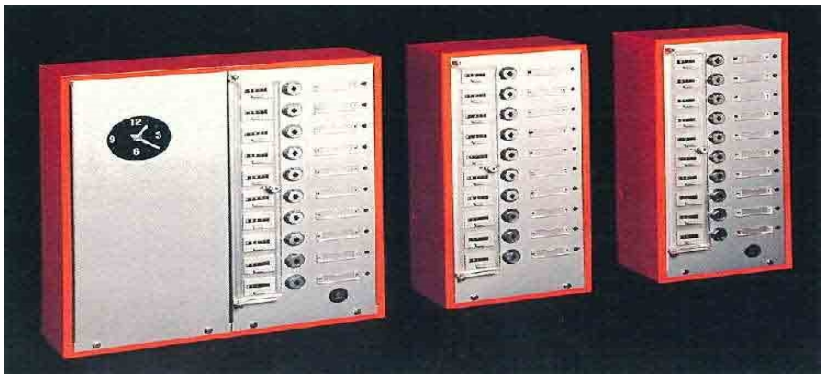

Figure I-11. Pointeuse compteurs d'horaires variables (1984)

I.2.5. Les pointeuses à détection automatique de colonne de pointage

Chaque fiche de pointage comporte un code unique grâce à un codage.

La pointeuse garde en mémoire les pointages de chaque fiche et peut donc savoir combien de pointage a déjà été effectué depuis le début de la journée, il n'y a donc plus de programmation à faire et il n'y a plus aucun risque de superposition de pointage.

Ce type de pointeuse peut même dans certain cas effectuer des calculs de cumuls journaliers [2].

I.3. Les différents types de la pointeuse

Il existe différents types de pointeuse, le choix de cette dernière est basé sur un cahier des charges établi par l'entreprise. Dans ce qui suit, nous présentons les principaux types existants.

I.3.1. La pointeuse mécanique

Elle possède un système d'horlogerie interne, qui permet d'enregistrer l'heure d'entrée et l'heure de sortie des employés. Il suffira simplement à ceux-ci de se munir d'une carte, qu'ils insèreront dans le boitier de la pointeuse. L'heure ainsi « pointée » sera retranscrite sur un support papier. Les salaires des employés seront calculés sur base des heures prestées.

Cependant, ce type de pointeuse a une faille : il est impossible de vérifier que ce soit bien la bonne personne qui insère la carte dans la pointeuse. Donc, il faut veiller à instaurer une vérification à l'endroit où se trouvera la pointeuse, afin d'éviter les abus [3].

Figure I-12. Pointeuse mécanique

I.3.2. La pointeuse numérique

Quand le numérique se mêle de la gestion des horaires, cela peut engendrer une petite révolution technologique. La pointeuse numérique fonctionne à la manière d'un modèle mécanique : insertion de carte dans la machine, système d'horlogerie, etc. Mais l'atout majeur de la pointeuse numérique réside dans le fait qu'elle traite elle-même les données enregistrées, via un logiciel de gestion des horaires. Fini les calculs à n'en plus finir, la pointeuse s'en charge. Mais la pointeuse numérique n'a hélas pas résolu le problème de la vérification d'identité [3].

Figure I-13. Pointeuse numérique

I.3.3. La pointeuse badgeuse

Contrairement aux pointeuses mécaniques et numériques, la pointeuse badgeuse utilise, comme son nom l'indique, des badges. Ceux-ci sont des cartes au format carte de banque, qu'il sera facile d'insérer dans la machine afin d'y codifier les heures de prestation des employés. Mais, comme les précédents types de pointeuses, le problème de vérification de l'identité n'est pas résolu pour autant. La pointeuse badgeuse entraine un investissement important (achat de la machine en elle-même, du logiciel de gestion et des badges rigides) pouvant se montrer toutefois rapidement rentable [3].

Figure I-14. Pointeuse badgeuse (RFID)

I.3.4. La pointeuse biométrique

La pointeuse biométrique est activée par identification d'un détail humain numérisé et stocké dans sa mémoire informatique.

Elle diffère donc d'une pointeuse mécanique ou d'une badgeuse dont le fonctionnement est activé par une sollicitation matérielle : glisser un carton dans une fente ou passer un badge contre une borne.

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 :

- Des empreintes digitales ;
- Le contour d'une main ;
- Un visage ;
- Un iris ;
- La voix.

Ce système de pointage permet de résoudre le problème que rencontraient les autres pointeuses. Grâce à la pointeuse biométrique, la vérification de l'identité des employés est impeccablement assurée.

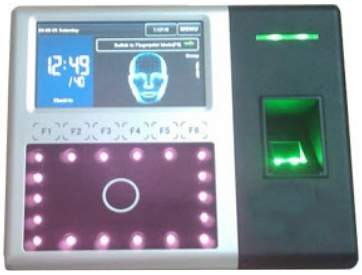

Figure I-15. Pointeuse biométrique

I.3.5. La Pointeuse mobile

La pointeuse mobile n'est pas un modèle de pointeuse pouvant être facilement démonté, transporté et remonté ailleurs : il ne s'agit pas d'un type de matériel.

La pointeuse mobile est une modalité d'organisation du pointage du personnel appliquée aux salariés travaillant en majorité en dehors des locaux de l'entreprise qui les emploie.

Il faudrait plutôt parler de pointage à distance ou « télépointage », car les solutions mises sur le marché recourent à des technologies misant sur la communication à distance.

Par leur nature, ces solutions concernent principalement des salariés non-sédentaires ou intervenants sur des sites et/ou dans des locaux qui ne sont pas ceux de leur employeur [4].

Le pointage mobile concerne principalement :

- Les commerciaux ;
- Le personnel participant à des opérations de sous-traitance et/ou de mise à disposition de main d'œuvre et/ou savoir-faire : SSII, maintenance, SAV, sécurité, nettoyage industriel ou non, etc.

Figure I-16. Pointeuse mobile

I.4. Conclusion

Dans ce chapitre, nous avons présenté l'évolution des pointeuses avec le temps et ceci en fonction des cahiers des charges imposés par les utilisateurs pour une meilleure prise en charge.

Nous remarquons que les premières pointeuses étaient destinées pour contrôler la réalité de la prestation de travail de l'ouvrier, et au fils des années, pour le contrôle des individus grâce à la biométrie.

La biométrie est un domaine émergeant où la technologie améliore la capacité à identifier une personne. Cette science est très utilisée actuellement, malgré ces limites d'utilisation où tout simplement il faut des autorisations car on touche l'être humain.

L'avantage de l'identification biométrique est que chaque individu a ses propres caractéristiques physiques qui ne peuvent être changées, perdues ou volées.

De plus, elle représente une économie, car il n'est pas nécessaire de renouveler ou remplacer sans cesse le matériel, à la différence d'un badge par exemple. La méthode d'identification biométrique peut aussi être utilisée en complément ou remplacement avec les autres types de pointeuses.

Grace à ces avantages, nous avons choisi cette technologie pour l'utiliser dans notre pointeuse.

Dans le chapitre suivant, nous allons essayer de donner beaucoup plus de détails sur cette science car c'est le thème de notre mémoire.

Chapitre II
La pointeuse biométrique

La pointeuse biométrique

II.1. Introduction

La pointeuse biométrique est un système automatique de mesure basé sur la reconnaissance de caractéristiques propres à un individu : physique, comportement…

Dans ce qui suit nous allons définir le mot biométrie, citer les différentes techniques utilisées dans cette sciences ainsi que de présenter la pointeuse biométrique et son principe de fonctionnement.

II.2. Biométrie

II.2.1. Définition

Le mot « biométrie » utilisé dans le domaine de la sécurité est une traduction du mot anglais « biométrics » qui correspond en fait au mot français anthropométrie.

Le mot anthropométrie signifie « sciences de la mesure physique des caractéristiques humaines »

Le mot biométrie signifie « mesure + vivant » ou « mesure du vivant », et désigne dans un sens très large l'étude quantitative des êtres vivants.

Le mot français biométrie définit aussi « l'étude mathématique des variations biologiques à l'intérieur d'un groupe déterminé ».

L'usage de ce terme se rapporte de plus en plus à l'usage de ces techniques à des fins de reconnaissance, d'authentification et d'identification, le sens premier du mot biométrie étant alors repris par le terme biostatistique [5].

Parmi les principaux domaines d'application de la biométrie, on peut citer l'agronomie, l'anthropologie, l'écologie et la médecine.

Dans la suite de notre mémoire pour plus de clarté, nous utiliserons la définition « anglaise » du terme qui est basée sur le langage de la « sécurité ».

La biométrie est basée sur l'analyse de données liées à l'individu et peut être classée en trois grandes catégories :

- Analyse basée sur l'analyse morphologique (Empreinte digitale, forme de la main, traits du visage, réseau veineux de la rétine, iris de l'œil, voix).
- Analyse de traces biologiques (Odeur, salive, sang, ADN).

- Analyse basée sur l'analyse comportementale (Dynamique du tracé de signature, frappe sur un clavier d'ordinateur).

Tout d'abord il est important de définir les termes employés. Il est rappelé que l'identité d'un individu est l'ensemble des données de fait et de droit qui permettent d'individualiser quelqu'un. On peut citer :

- La vérification de l'identité conduit à l'identification,
- La preuve de l'identité conduit à l'authentification.

- *Le mot* ***identification*** : la vérification de l'identité est faite à partir d'une pièce d'identité (document officiel) : ni l'iris de l'œil, ni l'empreinte, ni la voix ne peut donner l'identité. Les personnes faisant l'objet d'une identification ont volontairement déposé leur identité.

La vérification de l'identité demande une base de référence et le but est de vérifier que l'identité de l'individu qui se présente existe bien dans la base de référence.

- *Le mot* ***authentification*** : l'authentification est réalisée en deux temps :
  - Vérification de l'identité : la personne déclare son identité en se présentant au contrôle d'accès.
  - Preuve de l'identité : les éléments biométriques (empreintes, voix, visage, iris…) de la personne sont comparés avec le gabarit de cette personne, afin de vérifier si son identité est bien la bonne.

II.2.2. Principe de fonctionnement de la pointeuse biométrique

Les systèmes biométriques s'appuient sur plusieurs processus distincts : enregistrement, capture directe, extraction et comparaison de modèle.

L'objectif de l'enregistrement consiste à collecter et archiver des échantillons biométriques, et à générer des modèles numériques pour des comparaisons ultérieures. En archivant les échantillons bruts, il devient possible de générer des modèles de remplacement, au cas où de nouveaux ou de meilleurs algorithmes de comparaison seraient introduits dans le système.

Il est vital de recourir à des pratiques favorisant l'enregistrement d'échantillons de grande qualité pour assurer la régularité de ces derniers, ainsi que pour améliorer les performances de recherche générales, ce qui s'avère tout particulièrement important pour la reconnaissance biométrique de type « identification ».

Nous pouvons distinguer la « capture directe » de l'enregistrement en la définissant comme le processus visant à collecter des échantillons biométriques en direct lors d'une tentative d'accès ou d'identification, puis à les comparer à une « galerie » de modèles précédemment enregistrés.

L'extraction de modèle nécessite un traitement du signal des échantillons biométriques bruts (ex : images ou échantillons audio) afin d'obtenir un modèle numérique. Les modèles sont habituellement générés et stockés lors de l'enregistrement pour gagner du temps lors du traitement des comparaisons ultérieures.

La comparaison de deux échantillons biométriques applique des calculs algorithmiques destinés à évaluer leur similarité. Lors de la comparaison, un score de correspondance est attribué. S'il est supérieur à un seuil donné, les modèles sont considérés comme identiques.

En règle générale, les algorithmes d'extraction de modèle biométrique et de comparaison sont propriétaires (différents et secrets), aussi, ils ne peuvent pas être utilisés au sein d'un même système avec ceux d'autres fournisseurs (ex : pour comparer des modèles générés par différents produits, ou pour utiliser un algorithme de recherche de correspondance d'une société afin de comparer des modèles générés par les algorithmes d'une autre société).

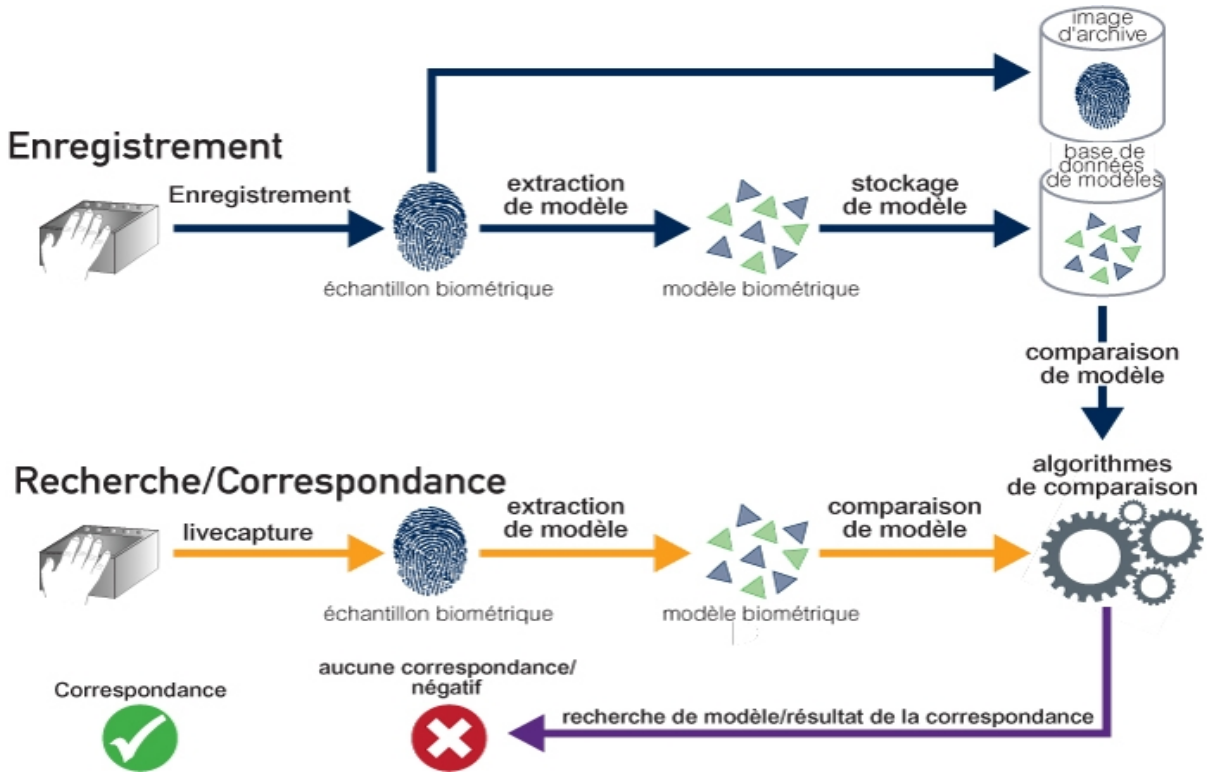

Figure II-1. Schéma d'illustration d'un système biométrique

Il existe cependant des exceptions, comme les générateurs de modèle d'empreinte digitale par point caractéristique et les algorithmes de recherche de correspondance certifiés MINEX (Minutiae Interoperability Exchange). Les modèles et logiciels de recherche de correspondance de cette catégorie ont été conçus, testés et certifiés en toute indépendance par NIST (National Institute of Standards and Technology) pour être interopérables dans le cadre de vérifications biométriques, et sont donc parfaits pour un stockage compact sur des cartes à puce ou des documents de voyage.

On peut aussi schématiser le cycle d'un processus d'identification biométrique par le schéma synoptique suivant:

Le fonctionnement s'enchaine comme suivant :

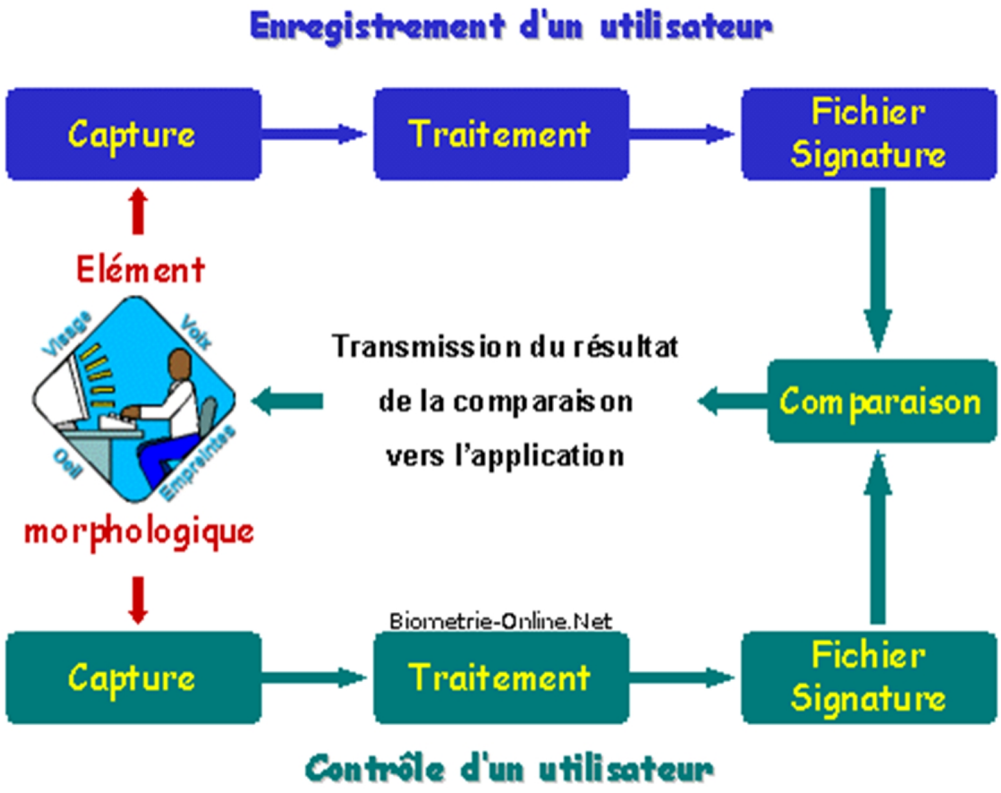

Figure II-2. Cycle d'un processus d'identification biométrique

- Capture de l'information à analyser (image ou son).
- Traitement de l'information et création d'un fichier "signature/gabarit" (éléments caractéristiques de l'image), puis mise en mémoire de ce fichier de référence sur un support (disque dur, carte à puce, code barre).

- Dans la phase de vérification, l'on procède comme pour la création du fichier "signature/gabarit" de référence, ensuite on compare les deux fichiers pour déterminer leur taux de similitude et prendre la décision qui s'impose.

On remarque qu'à travers ces deux schémas synoptiques le traitement de l'information est pratiquement identique.

II.3. Les techniques utilisées dans la pointeuse biométrique

II.3.1. Empreintes digitales

II.3.1.1. Introduction

La technique des empreintes digitales est une des techniques les plus anciennes, elle a été développée vers la fin du 19ème siècle par Alphonse Bertillon, fondateur de la police scientifique en France. A cette époque et jusqu'à récemment, une tablette et un encreur sont le matériel utilisé pour la capture d'empreinte.

Le premier système automatique d'authentification a été commercialisé au début des années 1960 [5].

II.3.1.2. Définitions

Il est nécessaire de donner quelques définitions techniques pour la compréhension des schémas des empreintes digitales.

Les empreintes digitales possèdent des motifs différents. En tenant compte de ces derniers, il est possible d'établir un classement. En effet, il existe 3 grandes familles d'empreintes qui regroupent à elles seules 95% des doigts humains :

- Les arcs ou les arches ;
- Les boucles (à droite ou à gauche) ;
- Les tourbillons.

Boucles *Tourbillons* *Arches*

Figure II-3. Les familles d'empreintes

Les motifs les plus répandus sont « les boucles » qui représentent 60% des doigts humains : Dans ce type d'empreinte, les lignes se replient sur elles même soit vers la droite, soit vers la gauche.

Ils viennent ensuite les « tourbillons », qui correspondent à 30% des doigts humains : Cette empreinte, dite en verticille, comprend des lignes qui viennent s'enrouler autour d'un point, formant un genre de tourbillon [6].

Pour finir, les motifs les moins répandus sont « les arches » qui regroupent seulement 5% des doigts humains : Cette empreinte, en arc, contient des lignes disposées les unes au-dessus des autres qui forment des A.

On remarque que quelle que soit sa forme, une empreinte digitale possède des points précis différents. On les appelle : minuties. Plus précisément, une minutie est un point qui se situe sur le changement de continuité des lignes papillaires. Ce sont grâce à elles que les empreintes digitales peuvent être différenciées.

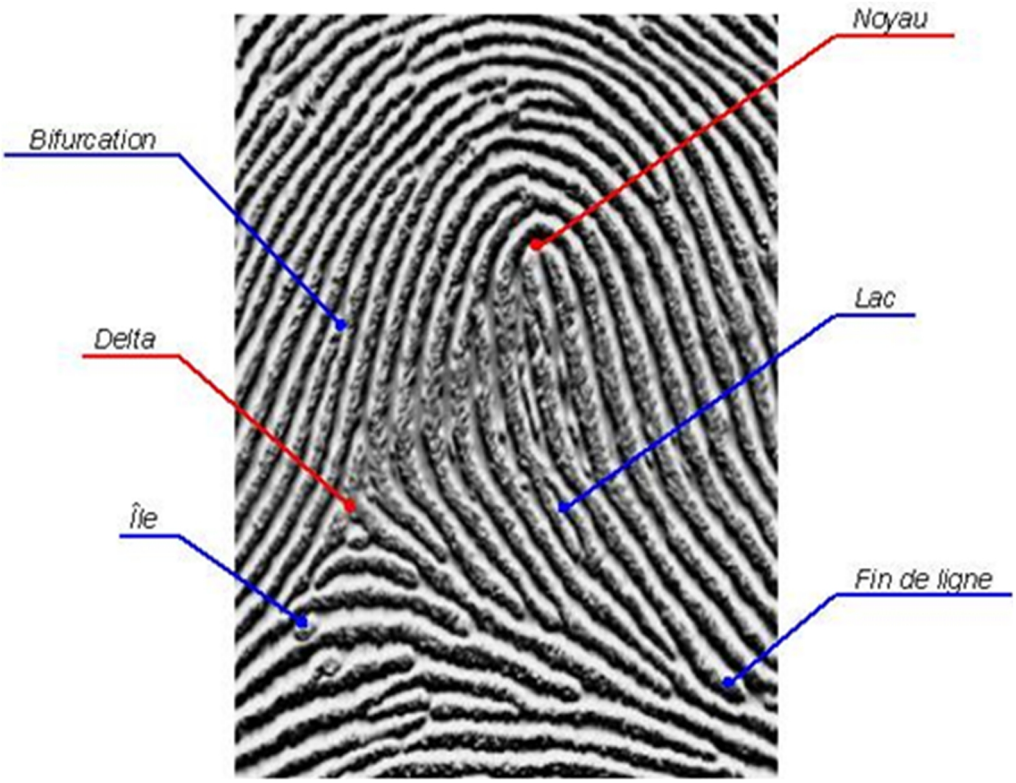

Figure II-4. Les minuties des empreintes digitales

- ***Les minuties*** : Dans les techniques de biométrie, ce terme désigne les particularités des empreintes digitales (bifurcations ou arrêts de sillons, espaces clos, etc...) qui seront traitées dans le processus d'authentification. Ils ont étés codifiées à la fin des années 1800 en « caractéristiques de Galton ».

- ***Le noyau*** est le point intérieur, situé en général au milieu de l'empreinte. Il sert souvent de point de repère pour situer les autres minuties. D'autres termes sont également rencontrés : le lac, l'île, le pont, le croisement, le delta, la vallée, le pore.

Le schéma ci-dessous donne le grossissement des différents types de minuties :

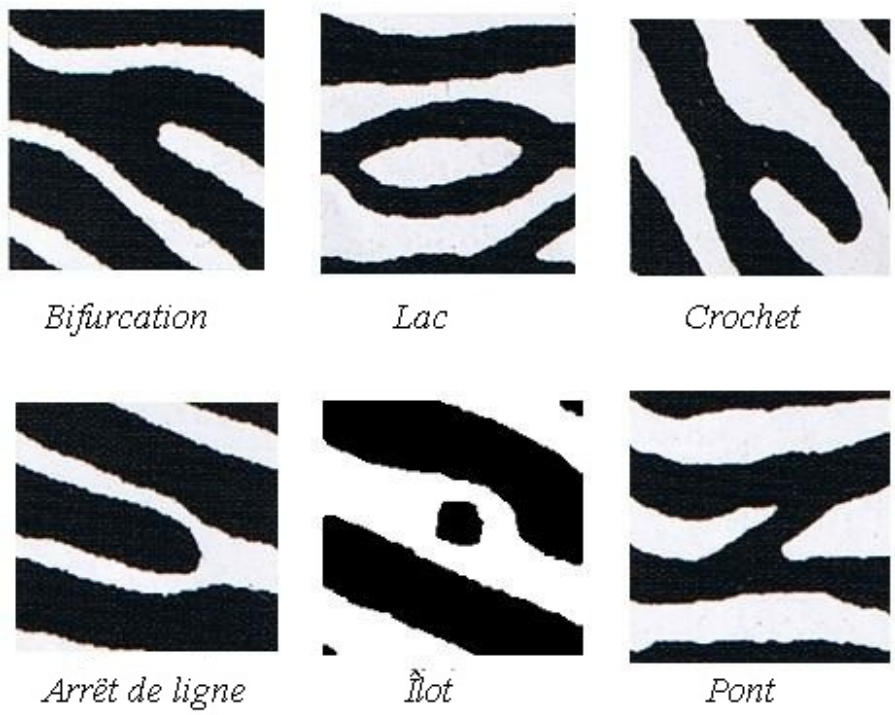

Figure II-5. Différents types de minuties

Pour valider une identification, il est nécessaire de mettre en évidence 12 points de comparaison (autrement appelés points caractéristiques ou minuties). Selon les calculs de Francis Galton effectués en 1892, la probabilité que deux personnes aient la même empreinte digitale est de 1 sur 64 milliard, ce qui est très faible à l'échelle de la population humaine et donc quasiment impossible [6].

II.3.1.3. Principe de fonctionnement

L'authentification par les empreintes digitales repose sur la concordance entre le fichier d'enregistrement, ou « signature », obtenu lors de l'enrôlement et le fichier obtenu lors de l'authentification.

Ces deux fonctions se décomposent chacune en plusieurs étapes :

- ***Enrôlement*** *:*
    - Capture de l'image de l'empreinte. Les données d'un doigt sont en principe suffisantes à l'enrôlement, mais la plupart des systèmes enregistrent au moins deux doigts (un par main par exemple) pour parer l'indisponibilité résultant de petites blessures.
    - Numérisation de l'image afin d'extraire les minuties, ou éléments caractéristiques.
    - Enregistrement sur un support. (Carte à puce, disque dur…).
- ***Authentification*** :
    - Capture de l'image de l'empreinte.
    - Numérisation de l'image afin d'extraire les minuties, ou éléments caractéristiques.
    - Comparaison entre l'échantillon et le gabarit « signature ».
    - Prise de décision.

Lors de la capture de l'image, celle-ci est toujours constituée à partir des points de contact du doigt sur le capteur.

- ***Etapes de traitement*** :
    - Lorsque la capture de l'image est réalisée, elle doit être convertie dans un format approprié. L'extraction des minuties est réalisée grâce à différents algorithmes. Il s'agit ensuite par une technique mathématique (segmentation) d'éliminer les informations non utiles au système : niveau de bruit trop élevé (image sale, doigt mal placé).
    - L'image est numérisée. Afin de localiser précisément les terminaisons et les bifurcations, les crêtes sont affinées de 5 à 8 pixels à 1 pixel. À ce stade, l'image a des distorsions et de fausses minuties, qui peuvent être dues à des cicatrices, de la sueur, un défaut de propreté du doigt comme du capteur. Les minuties vont être filtrées afin de ne conserver que les plus fiables.

Les avis divergent sur le rapport de proportion entre minuties extraites pour l'enrôlement et minuties suffisamment fiables pour la vérification. A partir de 31 minuties extraites, seulement 10 pourront correspondre lors de l'authentification.

A titre informatif, une empreinte numérisée occupe en moyenne entre 250 et 1000 octets.

II.3.1.3.1. La technique optique

C'est après l'encre, la technique la plus ancienne et qui a fait ses preuves.

Le principe physique utilisé est celui de « la réflexion totale frustrée » : Le doigt est placé sur un capteur éclairé par une lampe. Une caméra CMDs (Charge Modulation Device) avec CCD (Charged Coupled Device / en français : DTC : Dispositif à Transfert de Charge) convertit l'image, composée de crêtes foncées et de vallées claires, en un signal vidéo retraité afin d'obtenir une image utilisable.

Nous pouvons différencier les terminaux en lumière visible à fenêtre sèche et à fenêtre à film liquide (la fenêtre est l'emplacement où l'utilisateur pose le doigt). Dans ce dernier cas, la fenêtre est nettoyée avant chaque prise de vue par un mélange d'eau et d'éthanol injecté sous le doigt. Des terminaux à image infrarouge par capteur linéaire intégré sont parfois utilisés, mais présentent les mêmes inconvénients que ceux à lumière visible.

Tableau II-1. Les avantages et les inconvénients de la technique optique

Avantages	Inconvénients
• Son ancienneté et sa mise à l'épreuve. • Sa résistance aux changements de température, jusqu'à un certain point. • Son coût abordable.	• Il est possible que l'empreinte d'utilisateurs précédents reste latente, d'où une possibilité de dégradation de l'image par surimpression. • Apparition possible de rayures sur la fenêtre. • D'autre part, le dispositif CCD peut s'user avec le temps et devenir moins fiable

II.3.1.3.2. La technique silicium

Cette technique est apparue à la fin des années 90. Le doigt est placé sur un capteur CMDS[5].

L'image est transférée à un convertisseur analogique-numérique, l'intégration se faisant en une seule puce.

Cette technique produit des images de meilleure qualité avec une surface de contact moindre que pour la technique optique. Les données fournies sont très détaillées. Elle possède une bonne résistance dans des conditions non-optimales.

Cette technique est adaptée à un développement de masse, notamment par ses coûts réduits.

Tableau II-2. Les avantages et les inconvénients de la technique silicium

Avantages	Inconvénients
• Coût assez bas.	• Capteur vulnérable aux attaques extérieures fortuites ou volontaires.

II.3.1.3.3. La technique ultrason

Très peu utilisée à ce jour, elle repose sur la transmission d'ondes acoustiques et mesure l'impédance entre le doigt, le capteur et l'air [5].

Cette technique permet de dépasser les problèmes liés à des résidus sur le doigt ou sur le capteur.

Cette technique peut aussi être utilisée par des scanners à ultrasons qui construisent par échographie une image ultra sonore. Elle est considérée comme la plus fiable.

Tableau II-3. Les avantages et les inconvénients de la technique ultrason.

Avantages	Inconvénients
• Facilité d'usage avec de grandes plaques • Capacité à surmonter des conditions de lecture non optimales (les poussières sont souvent transparentes aux ultrasons)	• Aucun inconvénient technique significatif n'a pu être identifié à ce jour au travers des textes et des témoignages des experts. • Coût élevé.

II.3.2. Forme de la main

La silhouette de la main est une caractéristique de chaque individu. La forme de la main est acquise par un scanner spécialisé. Des paramètres tels que la longueur des doigts, leur épaisseur et leur position relative sont extraits de l'image et comparés à la base de données.

Figure II-6. Contour de la main

Pour la capture de l'image, la personne pose sa main sur une platine où les emplacements du pouce, de l'index et du majeur sont matérialisés.

Une caméra CCD prend l'image, reliée à un lecteur où sont enregistrées les informations. Ce lecteur inclut des logiciels de traitement et de codage [5].

Figure II-7. Reconnaissance de la forme de la main.

Quatre-vingt-dix caractéristiques sont examinées parmi lesquelles la forme tridimensionnelle de la main, la longueur et la largeur des doigts ainsi que la forme des articulations, et constituent un fichier d'environ neuf octets de mémoire.

Cette technique, très répandue aux USA, a été utilisée lors des J.O. d'Atlanta.

Tableau II-4. Les avantages et les inconvénients de la technique de la forme de la main.

Avantages	Inconvénients
• Le résultat est indépendant de l'humidité des doigts et de souillures éventuelles car il n'y a pas de contact direct avec le capteur ou une fenêtre, donc pas de risque d'encrassement. • Facilité de l'enrôlement du point de vue de l'usager et bonne acceptation psychologique. • Faible volume de stockage par fichier.	• Système encombrant. • Risque élevé du taux de fausses acceptations et faux rejets, par exemple à cause d'une blessure ou pour les jumeaux ou les membres d'une même famille. • Cette technique n'a pas évoluée depuis plusieurs années. • Le lecteur est plus cher que pour les autres types de capture de données physiques.

II.3.3. Reconnaissance faciale

La reconnaissance à partir du visage se base sur les caractéristiques jugées significatives comme l'écart entre les yeux, la forme de la bouche, le tour du visage et la position des oreilles.

Il existe plus de 60 critères fondamentaux [5]. Une méthode consiste à décomposer le visage selon plusieurs images en différentes nuances de gris : chaque image met en évidence une caractéristique particulière comme la montre la **Figure II-8**.

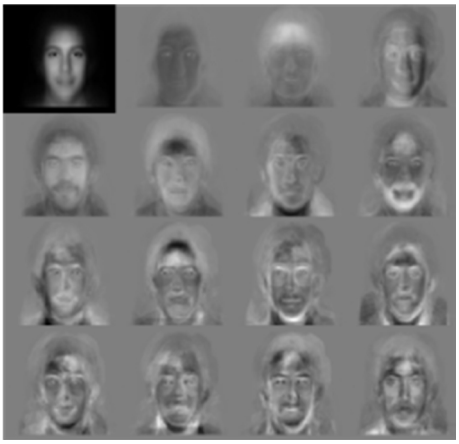

Figure II-8. La méthode faciale

D'autres méthodes dérivent de la méthode précédente et ajoutent des informations telles que l'écart entre les yeux, etc.

La plupart des systèmes d'identification du visage utilisent du matériel classique du marché : un ordinateur et une caméra pour capturer l'image. L'image est enregistrée dans une base de données exigeant approximativement 100 octets de mémoire par image.

La capture de l'image s'effectue à partir d'une caméra CCD.

L'utilisation de cette technique dans les aéroports, certains grands magasins, sort du cadre de cette étude, orientée contrôle d'accès [5].

Tableau II-5. Les avantages et les inconvénients de la technique de la reconnaissance faciale.

Avantages	Inconvénients
• Technique peu coûteuse, peu encombrante. • Absence de contact avec le capteur, méthode non intrusive pour la personne ; pas de risques pour la santé.	• Les vrais jumeaux ne sont pas différenciés. • En tant que contrôle d'accès, le visage n'est pas traditionnellement reconnu comme un mécanisme fiable d'authentification. • Tout élément tel que lunettes de soleil, chapeau, moustache, barbe, percing, blessure peut causer des anomalies avec des systèmes d'identification du visage.

II.3.4. Reconnaissance vocale

La reconnaissance de la voix n'est pas intrusive pour la personne et n'exige aucun contact physique avec le lecteur du système. Le logiciel de reconnaissance peut être centralisé et la voix transmise par le réseau, d'où un impact de réduction des coûts. Le dispositif nécessite un micro en source de capture [5].

Les systèmes d'identification de la voix sont basés sur les caractéristiques de voix, uniques pour chaque individu. Ces caractéristiques de la parole sont constituées par une combinaison des facteurs comportementaux (vitesse, rythme) et physiologiques (Tonalité, âge, sexe, fréquence, accent, harmoniques).

Pour être stockée, la voix est numérisée puis segmentée par unités échantillonnées. Les méthodes sont basées sur des algorithmes mathématiques (Shannon).

Les systèmes d'identification de la voix utilisent soit un texte libre, soit un texte imposé, les mots doivent être lus devant un micro.

Tableau II-6. Les avantages et les inconvénients de la technique de la reconnaissance vocale.

Avantages	Inconvénients
• Disponible via le réseau téléphonique. • L'imitateurs utilisent les caractéristiques vocales sensibles au système auditif humain, mais ne sont pas capables de récréer les harmoniques de la voix, servant de base à l'identification. Il est quasi impossible d'imiter la voix stockée dans la base de données. • Non intrusif.	• L'utilisation d'un micro nécessite un dispositif adapté présent sur l'environnement. • Sensibilité à l'état physique et émotionnel d'un individu. • Sensibilité aux conditions d'enregistrement du signal de parole : bruit ambiant, parasites, qualité du microphone utilisé, qualité de l'équipement, lignes de transmission. • Fraude possible en utilisant un enregistrement de la voix de la personne autorisée, facilitée dans le cas de système basé sur la lecture d'un texte fixe.

- ***Remarque :***

Les inconvénients signalés montrent que ce système est vulnérable et doit être utilisé couplé avec un autre système d'identification (lecteur de badges par exemple).

II.3.5. Examen de l'œil

Pour les deux techniques suivantes, il faut tout d'abord faire la distinction entre l'iris et la rétine.

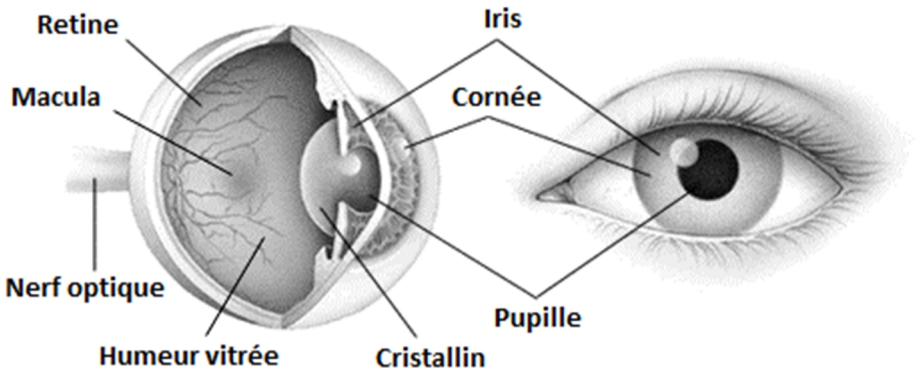

Figure II-9. Anatomie de l'œil

II.3.5.1. Iris

Les premières traces d'une proposition d'utilisation du motif de l'iris comme moyen de reconnaissance remonte à un manuel d'ophtalmologie écrit par James Doggarts et datant de 1949. On dit même que l'ophtalmologiste Frank Burch en avait émis l'idée dès 1936. Durant les années 80, l'idée reparut dans différents films de James Bond (Never Say Never Again, 1993), mais elle restait du domaine de la science-fiction. Ce n'est donc qu'en 1987 que deux ophtalmologistes (AranSafir et Leonard Flom) déposèrent un brevet sur cette idée et demandèrent à John Daugman (enseignant à cette époque à l'université de Harvard) d'essayer de trouver un algorithme d'identification basé sur le motif de l'iris. Cet algorithme a été breveté en 1994. Il est la base de tous les systèmes de reconnaissance d'iris actuels [5].

Figure II-10. L'iris

La personne qui cherche à se faire identifier doit simplement fixer l'objectif d'une caméra qui récupère instantanément le dessin de son iris. L'iris est un motif très dense qui n'est pas dicté par les gènes. Chaque œil est unique. Dans toute photographie de l'iris, on compte plus de 200

variables indépendantes, ce qui fait une probabilité très faible de confondre 2 individus. On doit cette méthode à quelques ophtalmologues qui ont remarqué dès les années 80, que la couleur de l'iris peut varier, mais rarement son motif. Cette méthode d'identification évoluera certainement avec le temps, probablement autant que les empreintes digitales, au moins autant que l'évolution des caméras.

Pour capturer l'image de cette membrane colorée, pas besoin d'éclairer la rétine. Par contre, l'éclairage de l'iris pose un problème de reflets, on utilise souvent un éclairage artificiel (diodes électroluminescentes) calibré tout en atténuant le plus possible l'éclairage ambiant. L'éclairage est d'autant mieux toléré qu'il peut-être infrarouge, peu visible pour l'œil.

Le système peut être trompé à partir d'une photo ou d'une lentille de contact reproduisant l'iris de la personne dont on souhaite usurper l'identité. Mais la résolution demandée est très importante (distance iris / caméra faible, évolution rapide de la technologie des capteurs CCD/CMOS (Complementary Metal Oxide Semiconductor)). De plus il est possible de repérer, par filtrage, que l'iris présenté est constitué d'une suite régulière de points et non d'un motif varié. Enfin, il existe de nombreuses techniques qui permettent de s'assurer que l'iris présenté est humain (ou très ressemblant) :

- Si l'on fait varier l'éclairage, le diamètre de la pupille varie. Les temps de latence et vitesse de variation sont mesurables.
- Il est possible d'éclairer des U.V. (Ultraviolet) à l'I.R. (Infrarouge) et d'observer les images obtenues. L'œil est opaque dans l'IR lointain (proche du thermique) ainsi qu'aux UV. Ainsi, il semble difficile de fabriquer un faux iris complet (variations de la pupille, réactivité à l'IR,...).

La biométrie par l'iris est une des technologies (avec la rétine) qui assure un haut niveau de sécurité. L'iris procure une unicité très élevée (1 sur 10 puissance 72) et sa stabilité est étendue jusqu'à la mort des individus, d'où une fiabilité extraordinaire.

Tableau II-7. Les avantages et les inconvénients de la technique de l'iris.

Avantages	Inconvénients
• Fiable. • Pas de risque identifié pour la santé.	• Système intrusif mal accepté psychologiquement. (hygiène, proximité de l'objectif) • Contraintes d'éclairage.

II.3.5.2. La rétine

La rétine est la couche sensorielle de l'œil qui permet la vision. Cette zone est parcourue par des vaisseaux sanguins qui émergent au niveau de la papille optique, où l'on distingue l'artère et la veine centrale de la rétine qui se divisent elles-mêmes en artères et veines de diamètre plus faible pour vasculariser les cellules qui permettent la vision. La grande variété de configurations des vaisseaux sanguins présenterait la même diversité que les empreintes digitales. L'aspect des vaisseaux peut être modifié par l'âge ou la maladie, mais la position respective des vaisseaux reste inchangée durant toute la vie de l'individu. Une caméra est utilisée pour capturer la cartographie des vaisseaux, pour cela il est nécessaire d'illuminer le fond de l'œil [5].

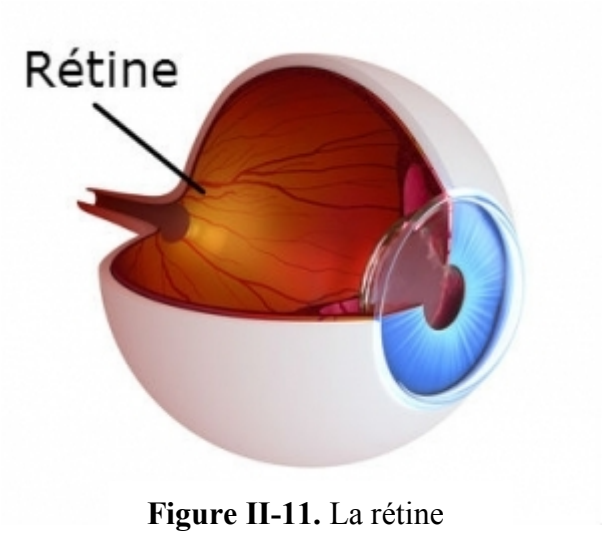

Figure II-11. La rétine

Réputé comme étant le plus fiable moyen biométrique, il souffre d'une réticence psychologique de l'usager. On accepte difficilement l'idée d'un rayon lumineux, même inoffensif, dans l'œil.

Cette carte vasculaire, propre à chaque individu diffère entre 2 jumeaux et évolue peu avec l'âge. Les systèmes identifient jusqu'à cent quatre-vingt-douze points de repères.

La biométrie par la rétine procure un haut niveau en matière de reconnaissance. Elle est bien adaptée pour des applications de haute sécurité (sites militaires, salles de coffres forts). La disposition des veines de la rétine assure une bonne fiabilité, et une haute barrière contre la fraude. Mais le frein psychologique produit par cette technologie est énorme et fait l'objet de sa faible percée dans les milieux de la sécurité privée.

Tableau II-8. Les avantages et les inconvénients de la technique de la rétine.

Avantages	Inconvénients
• Résistant à la fraude, difficile et long à imiter. • Unicité même chez les vrais jumeaux. • Technique fiable.	• Nécessité de placer ses yeux à très faible distance du capteur, donc système intrusif mal accepté psychologiquement. • Coût. • Difficile à utiliser en cas de contrôle d'une population importante (temps important). • Installation délicate (hauteur)

II.4. Critères de choix d'une technique biométrique

Les principales contraintes liées à la biométrie sont dues à l'ergonomie et à l'acceptabilité de certaines modalités.

Plutôt que de comparer les performances des diverses technologies (empreintes, visage, main…), il faut surtout tenir compte de l'environnement de leur usage, (facilité de : saisie, d'analyse, de stockage, de vérification).

Chaque technologie possède des avantages et des inconvénients, acceptables ou inacceptables suivant les applications. Ces solutions ne sont pas concurrentes, elles n'offrent ni les mêmes niveaux de sécurité ni les mêmes facilités d'emploi.

En comparaison aux systèmes d'authentification utilisant un objet ou un mot de passe, qui offrent une réponse stable (oui ou non, 0% ou 100%) ; les informations biométriques sont plus fluctuantes et donnent des réponses en termes de pourcentage de similitude (entre 0% et 100%, le 100% n'étant jamais atteint). Cette variation des résultats d'identification d'un individu est plus liée à la qualité de la capture de l'information biométrique (on n'a jamais deux images où deux sont identiques), qu'à la modification de la caractéristique biométrique de l'individu qui est généralement stable dans le temps.

Il faut donc définir un seuil de décision (acceptation ou refus) compris entre 0% et 100% de similitude au sein d'application. Ce seuil peut être différent pour chaque personne.

Une étude comparative des principales technologies biométriques réalisée par la société IBG (International Biometric Group) de 2003 permet de définir quel est le système le mieux adapté à l'application à sécuriser.

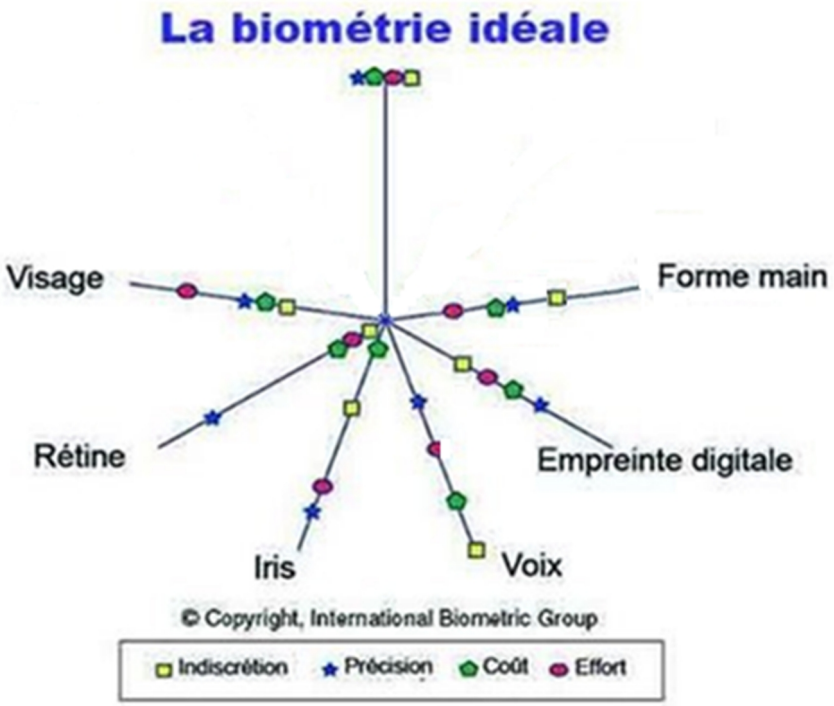

Figure II-12. Schéma de comparaison entre les principales techniques biométriques

- ***Effort*** : effort requis par l'utilisateur.
- ***Indiscrétion*** : niveau de perception par l'utilisateur du test comme intrusif.
- ***Coût*** : coût de la technologie (lecteurs, capteurs, etc.).
- ***Précision*** : efficacité de la méthode (capacité à identifier quelqu'un).

Il est important de comprendre que, dans le choix d'un moyen biométrique à exploiter, différents facteurs doivent être pris en compte.

II.4.1. Fiabilité des systèmes biométriques

La fiabilité d'un système biométrique se mesure généralement à l'aide d'une courbe « caractéristique de la performance d'un test » ou « courbe ROC (receiver operating characteristic) » indiquant son « taux de faux positifs (FMR) » et son « taux de faux négatifs (FNMR) » par rapport à une galerie d'échantillons biométriques.

Le taux de faux positifs est la fréquence à laquelle des échantillons biométriques de différentes sources sont incorrectement considérés comme originaires d'une même source. Le

taux de faux négatifs est la fréquence à laquelle des échantillons d'une même source sont incorrectement considérés comme originaires de sources différentes.

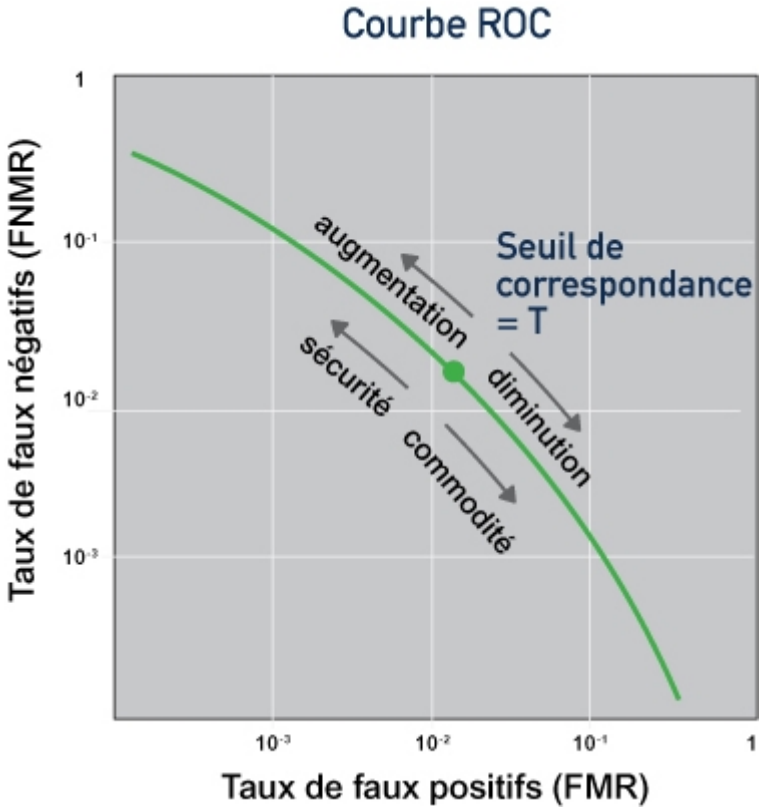

Figure II-13. Courbe ROC pour un système de recherche de correspondance biométrique

Un système biométrique performant se caractérise par des résultats rapides et un faible taux de faux positifs et de faux négatifs. La fiabilité d'un système est égale au point de la courbe ROC dont l'emplacement est fonction du "seuil" de correspondance appliqué. Un seuil de correspondance élevé réduit le taux de faux positifs mais augmente le taux de faux négatifs (plus de sécurité, moins de commodité). Un seuil de correspondance faible réduit le taux de faux négatifs mais augmente le taux de faux positifs (plus de commodité, moins de sécurité ; voire la **Figure II-13**). Un grand nombre de données (exemple : plus d'empreintes digitales) et des échantillons de grande qualité (très réguliers) sont nécessaires pour les identifications, contrairement aux vérifications.

Il est important de reconnaître que la fiabilité des systèmes biométriques dépend largement de la nature des données biométriques du système. Chaque galerie de données biométriques par rapport à laquelle est effectuée une comparaison d'échantillons donnera une courbe ROC de fiabilité différente. Il existe des galeries biométriques dans le domaine public, qui servent de références afin de comparer différents algorithmes de correspondance.

Cependant, les algorithmes peuvent être “entraînés” pour fonctionner plus efficacement sur des bases de données connues, ce qui revient à voir les questions d’un test avant de le passer. Leur fiabilité comparative s’en trouvera ainsi améliorée sur les bases de données connues, sans que cela indique forcément la performance du système sur des données inconnues, comme c’est le cas en situation réelle. Le meilleur moyen de prédire le comportement d’un système biométrique lors d’un déploiement en situation réelle consiste donc à tester ses performances sur des données pour lesquelles il n’a pas été expressément entraîné.

Figure II-14 démontre le score de comparaison entre:

- des échantillons provenant de différentes sources et ;
- des échantillons provenant des mêmes sources, montrant le TFP et le TFN.

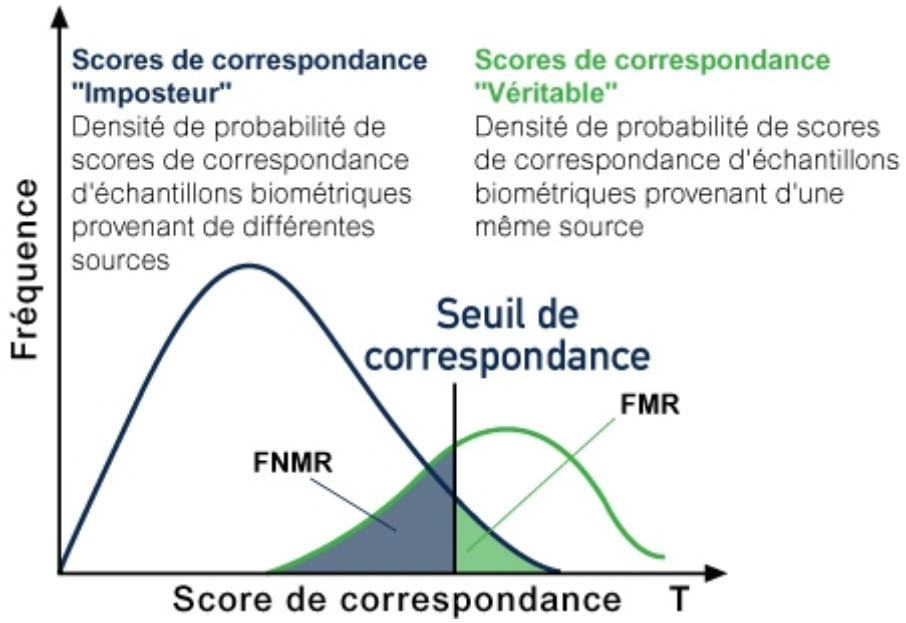

Figure II-14. Densité de probabilité de scores de correspondance

II.5. Conclusion

Pour réussir, un système biométrique doit présenter une logique de marché, c'est-à-dire qu'il doit exploiter le même sens que le périphérique auquel il est joint.

Par exemple, la reconnaissance vocale est plus justifiée dans le cadre de l'utilisation du téléphone cellulaire.

De même, l'authentification d'une personne à l'aide de sa rétine ou de son iris est plus naturelle lorsque celle-ci désire accéder à son compte bancaire via un guichet automatique, la plupart étant déjà muni d'une caméra. Un système biométrique qui analyse l'empreinte digitale est plus normalement incorporé à un clavier ou une souris reliant l'ordinateur.

L'analyse des performances des solutions biométriques peuvent s'analyser avec trois taux qui vont dépendre de la qualité des systèmes mais également du niveau de sécurité désiré. Ces taux sont :

- ***Taux de faux rejets*** *(T.F.R.):* Pourcentage de personnes rejetées par erreur.
- ***Taux de fausses acceptations*** *(T.F.A.):* Pourcentage d'acceptations par erreur.
- ***Taux d'égale erreur*** *(T.E.E.):* donne un point sur lequel le T.F.A. est égal au T.F.R.

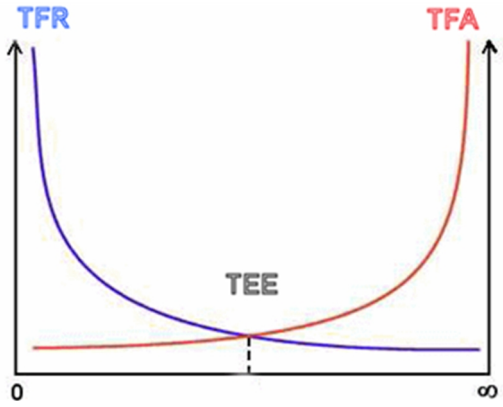

Figure II-15. Taux d'erreur des systèmes biométriques

Lorsqu'on compare différents systèmes biométriques entre eux, un T.F.A. bas est essentiel si le haut niveau de sécurité du système est le critère recherché. Toutefois, si la commodité est la préoccupation première alors un T.F.R. bas sera à surveiller.

Contrairement aux autres technologies biométriques, l'empreinte digitale est la technologie la plus employée à travers le monde. Et nous voyons fleurir des solutions de plus en plus abordables et performantes.

En basant sur les tableaux des avantages et inconvénients de chaque technique de biométrie présentée dans ce chapitre, nous avons constaté que l'empreinte digitale est la technique la plus adéquate pour notre application (pointeuse biométrique), car elle est en même temps fiable, inoffensive et rapide. Pour cela notre prochain chapitre traite la conception et la réalisation de la pointeuse biométrique par empreinte digitale.

Chapitre III
Conception et réalisation de la pointeuse biométrique

Conception et réalisation de la pointeuse biométrique

III.1. Introduction

D'après de ce que nous avons abordé dans les deux chapitres précédents, l'étude comparatif des différents techniques qui existes nous a permis de choisir la technique adéquate pour notre pointeuse. Par conséquent, nous avons opté pour la technique biométrique par empreinte digital. Dans ce chapitre nous allons présenter deux parties à savoir l'étude conceptuelle de notre système et sa réalisation.

III.2. Etude conceptuelle

Cette partie comporte une étude sur les différents sous-systèmes de notre pointeuse et la raison pour laquelle nous les avons utilisé.

Le schéma synoptique suivant montre les différentes parties de notre système et l'emplacement de chaque partie par rapport à l'autre.

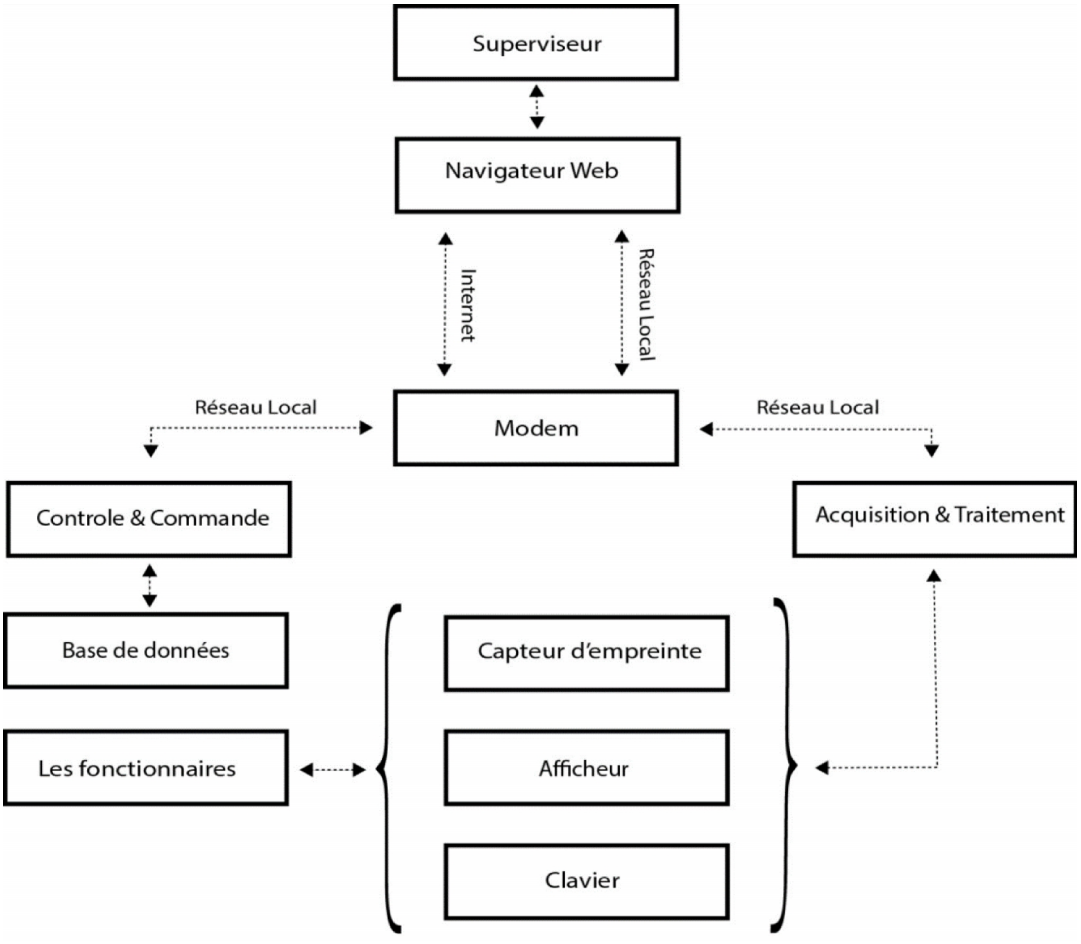

Figure III-1. Schéma synoptique de notre système

Chaque bloc de ce schéma sera détaillé dans ce chapitre.

III.2.1.Alimentation

III.2.1.1. Introduction

L'électronique en général que nous utilisons fonctionne avec du courant continu et le réseau électrique nous fournit du courant alternatif « $230v/50Hz$ ». Il va donc falloir transformer ce courant alternatif en continu et modifier la valeur fournie en valeur désirée. C'est pour cela qu'une alimentation est nécessaire.

Cette dernière transforme les caractéristiques de l'énergie délivrée par le réseau (secteur) pour les adapter aux conditions souhaitées.

Les alimentations secteur bon marché sont généralement constituées d'un transformateur, d'un pont de diode et d'un condensateur de filtrage. Ce type d'alimentation présente l'inconvénient majeur de délivrer une tension de sortie pouvant varier dans de grandes proportions en fonction du courant consommé, car non régulée.

Il est toujours possible d'utiliser ce type d'alimentation pour des montages "délicats", à condition de lui adjoindre une régulation un peu plus digne.

Dans la pratique il existe d'innombrables possibilités pour réaliser ce transfert énergétique avec toutes les variantes possibles et imaginables. Chacune a ses avantages, ses inconvénients, ses limitations, sa complexité, son coût, son domaine de prédilection, etc. Elle est principalement composée de :

- Un transformateur (Adaptation) ;
- Un redresseur ;
- Un filtre ;
- Un stabilisateur.

Les différentes fonctions présentées sont schématisées par la figure suivante :

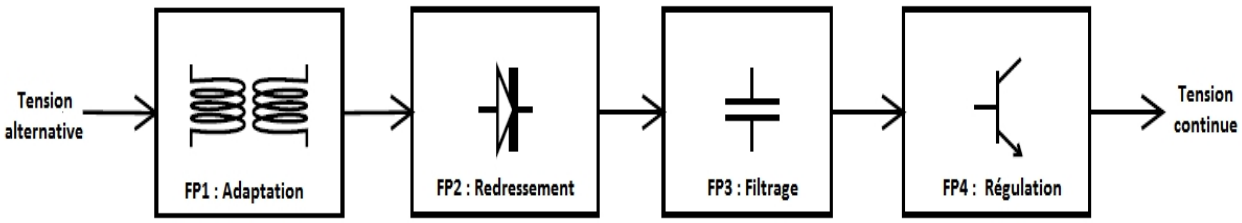

Figure III-2. Schéma synoptique d'une alimentation stabilisée

Dans ce qui suit, nous essayons de rappeler le principe de fonctionnement de chaque partie de ce schéma.

III.2.1.2. Transformateur

C'est un appareil statique à induction électromagnétique destiné à transformer un système de courants variables en un ou plusieurs autres systèmes de courant variable d'intensité et de tension généralement différentes et de même fréquence.

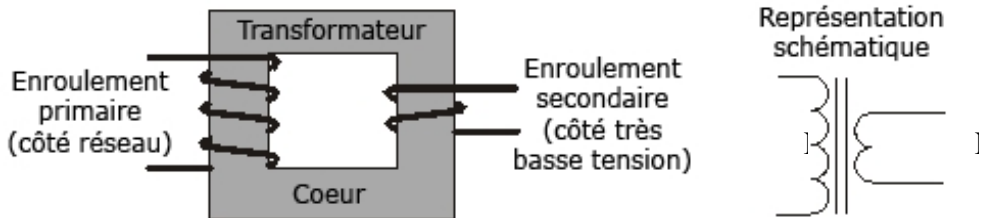

Figure III-3. Schéma synoptique d'un transformateur

Avec :

- N_1 : Nombre de spire du primaire branché directement sur le secteur.
- N_2 : Nombre de spire du secondaire relié généralement à la charge.

Le transformateur rempli deux fonctions:

- Isoler le récepteur et le secteur ; le transfert d'énergie se fait par le champ magnétique.
- Transformer la tension alternative du réseau déterminée par le rapport entre le nombre de spire de la bobine du secondaire et celui du primaire, c'est à dire soit d'abaisser ou d'élever la tension.

A partir de la relation : $K = \frac{N_2}{N_1}$ (III-1)

on peut conclure que si le rapport :

- $K > 1$: le transformateur est un élévateur de tension.
- $K < 1$: le transformateur est un abaisseur de tension.

Le rendement est donné par la relation suivante : $\eta = \frac{P_S}{P_e}$ (III-2)

Avec :

- P_S : Puissance au secondaire du transformateur.
- P_e : Puissance au primaire du transformateur.

III.2.1.3. Redresseur

Le redressement du courant alternatif est l'opération qui consiste à appliquer une tension alternative à un organe de conductibilité unilatérale. Ce détecteur ne se laisse traverser que par les alternances de même sens (positives ou négatives, selon le sens de connexion du détecteur).

L'organe le plus utilisé comme détecteur des alternances est la diode. Il y a deux types de redressement :

- Le redressement simple alternance.
- Le redressement double alternance.

Pour notre étude, on se limite uniquement au redressement double alternance avec deux diodes.

Pour ce type de redressement, on utilise un transformateur à point milieu et deux diodes pour le redressement du signal. Le schéma de ce type de redresseur est donné par la **Figure III-4**.

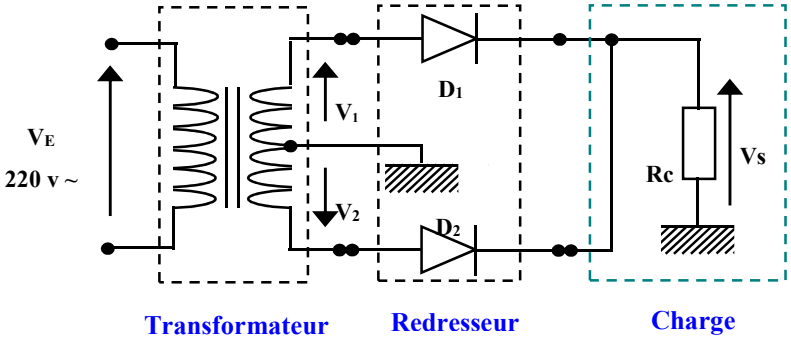

Figure III-4. Montage redresseur double alternance

Le transformateur fourni deux tensions sinusoïdales en sortie identique et de sens opposées V_1 et V_2 comme le montre la **Figure III-5**.

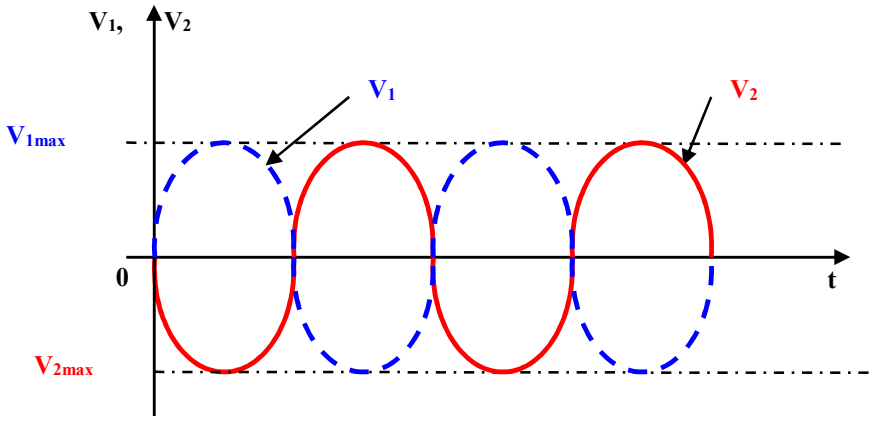

Figure III-5. Forme des signaux d'entrées

Leurs expressions mathématiques sont de la forme :

- $V_1 = V_{1\max} \sin \omega t$ (III-3)
- $V_2 = V_{2\max} \sin(\omega t + \varphi)$ (III-4)

Avec $\varphi = \pi$: déphasage entre les deux tensions.

- ***Principe de fonctionnement***
  - $0 < \omega t < \pi$: la diode D_1 conduit et la diode D_2 est bloquée. On a $V_S = V_1$.
  - $\pi < \omega t < 2\pi$: la diode D_1 se bloque et la diode D_2 conduit. On a $V_S = V_2$.

Les formes des signaux d'entrée et de sortie sont représentées par la Error! Reference

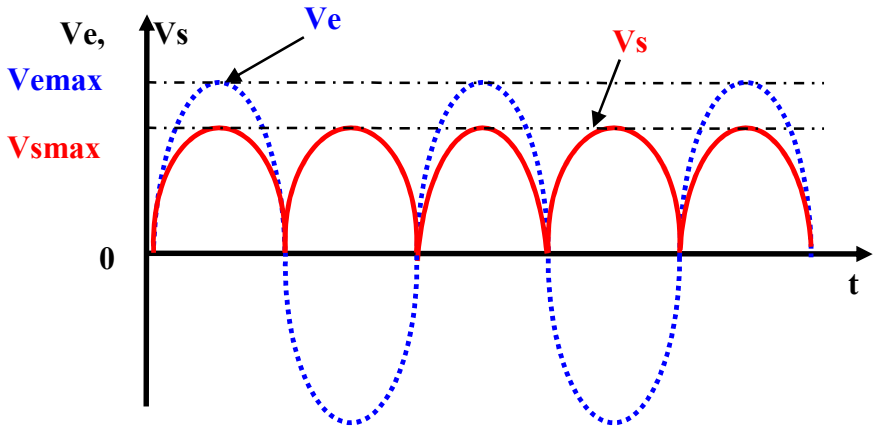

Figure III-6. Forme des signaux d'entrée et de sortie

source not found..

La valeur moyenne du signal redressé : $I_{moy} = 2 \times \frac{I_{\max}}{\pi} = 0{,}637\ I_{\max}$ (III-5)

La valeur efficace : $V_{moy} = 2 \times \frac{V_{\max}}{\pi} = 0{,}637\ V_{\max}$ (III-6)

III.2.1.4. Filtrage

Le filtrage a pour rôle de faire disparaître l'ondulation de la tension de sortie. Cette ondulation d'amplitude plus ou moins importante a un grand inconvénient lors de son utilisation dans les étages amplificateurs (car elle sera amplifiée). C'est pour cela qu'on utilise un circuit de filtrage pour l'éliminer ou au moins pour l'affaiblir.

Le principe de fonctionnement repose essentiellement sur le phénomène de la charge et de la décharge d'un condensateur à travers une résistance.

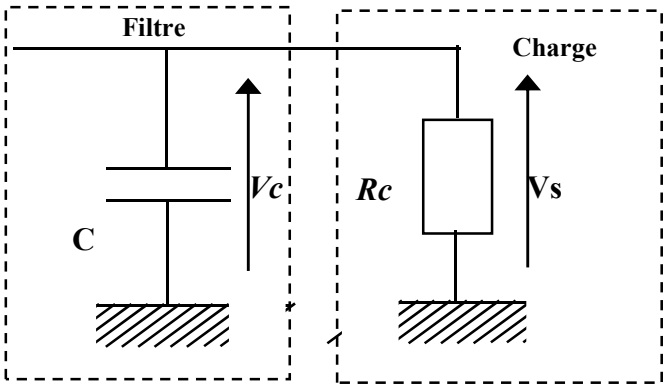

Figure III-7. Représentation du circuit de filtrage

Pour ce type de filtrage, on a le cas :

- Avec charge en sortie ;
- Sans charge en sortie.

- *Premier cas* : Sans charge à la sortie

Le condensateur est déchargé à l'instant ($t = 0$), pendant la première demi alternance, le condensateur va se charger à la valeur crête, et pendant l'autre demi alternance la capacité reste chargé à sa valeur maximale. La courbe de la **Figure III-8** montre ce fonctionnement.

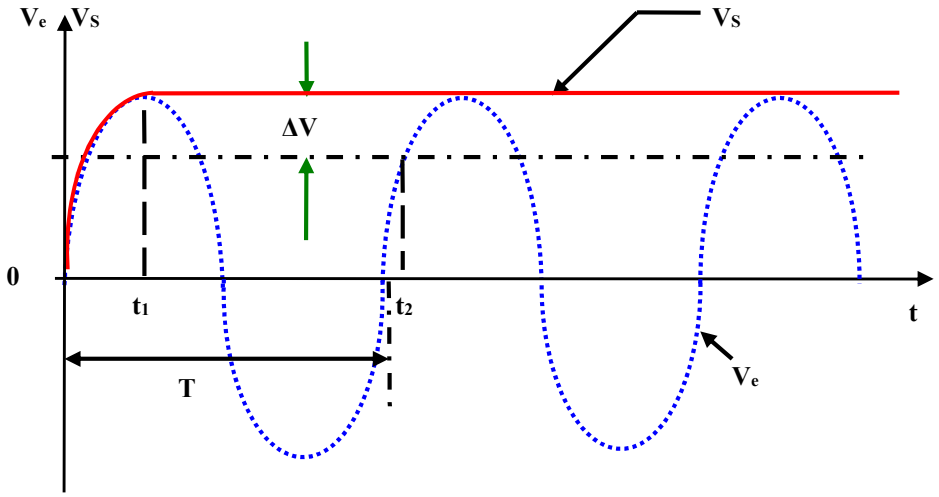

Figure III-8. Courbes de filtrage avec charge

- ***Deuxième cas*** : Avec charge à la sortie

Le condensateur est déchargé à l'instant ($t = 0$), pendant la première demi alternance, le condensateur va se charger à la valeur crête, et pendant l'autre demi alternance la capacité se décharge à travers la charge R_C .

Au cours de la seconde demi-alternance, le condensateur se charge de nouveau à la valeur crête récupérant ainsi le courant cédé.

Donc le condensateur joue le rôle d'un accumulateur ou réservoir car il est capable de se charger puis restituer une partie ou la totalité de sa charge. La courbe de la **Figure III-8** résume ce fonctionnement.

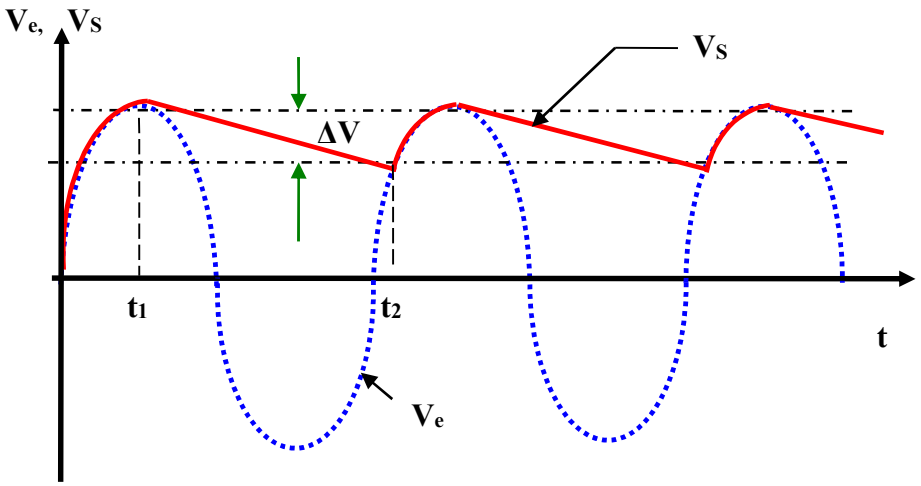

Figure III-9. Courbes du Filtrage avec charge

Pour ce type de redressement, il est nécessaire de connaître la tension d'ondulation ou la valeur efficace de cette tension qui est donnée par la relation suivante :

$$\Delta V = \frac{V_{\max} T}{2 R_C C} \qquad \text{(III-7)}$$

Avec :

- ΔV : La valeur efficace de la tension d'ondulation,
- R_C : La charge,
- C : La capacité
- T : La période du signal de l'ondulation.

III.2.1.5. Stabilisation

Une alimentation stabilisée est un dispositif destinée à délivrer une tension constante quelles que soit les variations de la tension d'entrée ou de la charge. Nous citons dans ce qui suit quelques stabilisateurs élémentaires.

- Régulation par diode Zener ;
- Régulation par transistor et diode Zener ;
- Régulation par circuit intégré.

Le circuit de base d'un régulateur utilise un amplificateur opérationnel pour porter une tension de référence à une fraction de la tension de sortie, et pour contrôler un élément série qui règle la tension de sortie.

L'élément de sortie, qui est constitué du transistor intégré limite le courant de la sortie. La figure ci-après représente un circuit intégré d'un régulateur de tension.

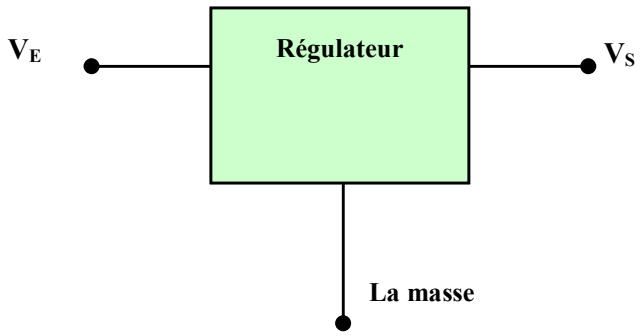

Figure III-10. Représentation d'un circuit régulateur de tension

Ces régulateurs intégrés ont l'avantage d'avoir :

- Un faible bruit.
- Un fort taux de filtrage avec un bon rendement.
- Un montage relativement simple avec une haute stabilité.
- Une possibilité d'avoir une tension de sortie positive ou négative.

III.2.2.Le capteur d'empreinte

Il existe plusieurs types de capteur d'empreinte, citant quelques-uns : optique, thermique et ultrasonique, notre choix s'est porté sur un capteur d'empreinte optique .La disponibilité du marché nous a imposé deux produits de capteur d'empreinte optique qui sont le GT511C3 et le ZFM-20.

Figure III-11. Le capteur d'empreinte GT511C3

III.2.2.1. Le capteur d'empreinte GT511C3

III.2.2.1.1. Présentation

Le GT511C3 est équipé d'un microcontrôleur Cortex M3 et permet d'enregistrer jusqu'à 20 empreintes. Il communique avec un autre microcontrôleur via une liaison série UART (Universal Asynchronous Receiver Transmitter).

III.2.2.1.2. Caractéristiques

Tableau III-1. Les caractéristiques du capteur GT511C3

Alimentation	3,3 à 6 Vcc
Consommation	130 mA
Liaison série	Uart 9600 bauds
Nombre d'empreintes	20 max
Taux d'erreur	- bonne empreinte: <0,1 % - mauvaise empreinte: <0,001 %
Temps d'identification	environ 1,5 seconde
Résolution	216 x 240 pixels (450 dpi)
Dimensions	36 x 18 x 8 mm

III.2.2.2. Le capteur d'empreinte ZFM-20

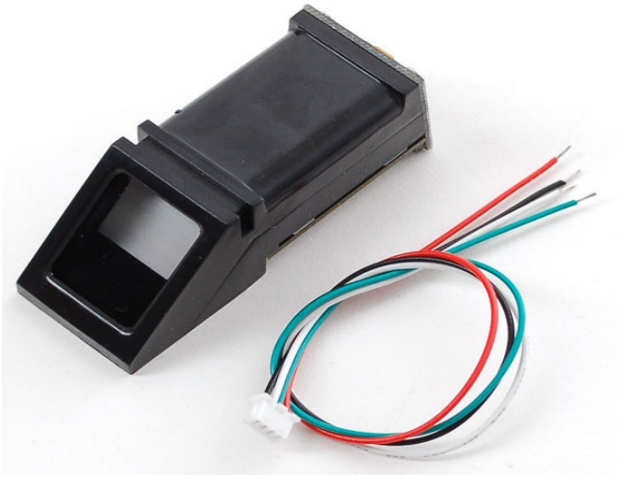

Figure III-12. Le capteur d'empreinte ZFM-20

III.2.2.2.1. Présentation

Le module ZFM-20 est un capteur d'empreintes digitales expérimental, destiné à être interfacé avec un microcontrôleur externe via une liaison série. Conçu sur la base d'un puissant DSP (Digital Signal Processor), il est capable de mémoriser jusqu'à 170 empreintes différentes dans sa mémoire flash.

III.2.2.2.2. Caractéristiques

Tableau III-2. Les caractéristiques du capteur ZFM-20

Alimentation	3,6 à 6 Vcc
Consommation	120 mA (150 mA maxi)
Temps d'identification	< 1 seconde
Sensibilité	1 à 5
Taux d'erreur	bonne empreinte: <1.0 % (sensibilité à 3) mauvaise empreinte: <0,001 % (sensibilité à 3)
Interface	série
Vitesse	9600, 19200, 28800, 38400 ou 57600 (57600 par défaut)
Température de service	-20 à +50 °C
Dimensions	21 x 21 mm

III.2.2.3. Le choix du capteur d'empreinte optique

Le choix du capteur n'a pas été pris à la légère vue la similitude d'utilisation des deux produits .D'après les caractéristiques décrites précédemment, nous avons finie par choisir le module ZMF-20 grâce à ces hautes performances en temps d'identification (moins d'une seconde) et en capacité de mémorisation d'empreinte (jusqu'à 170 empreintes).De plus , le ZMF-20 procède une librairie compatible pour une utilisation avec une carte Arduino, cela veut dire qu'il présente une facilité d'intégration dans notre projet par rapport au GT511C3. Ainsi, le ZMF-20 est le produit le plus conforme à notre projet.

III.2.2.4. Notre capteur d'empreinte

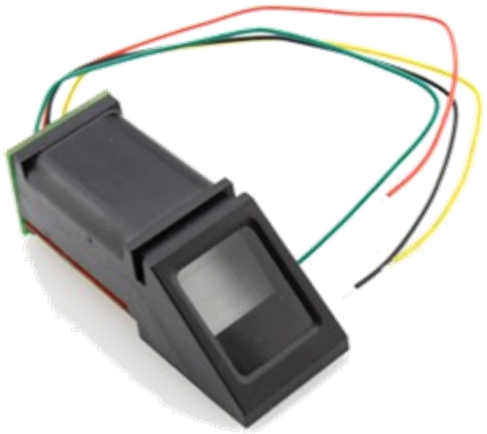

Figure III-13. Le capteur d'empreinte ZFM-20

III.2.2.4.1. Présentation

ZFM-20 est un module d'identification des empreintes digitales distincte proposé par Hangzhou Zhian Technologies Co., Ltd., qui utilise le DSP de Synochip comme un processeur principal et le capteur optique de Zhian pour capturer les images. Le module effectue plusieurs fonctions comme l'enregistrement des empreintes digitales, le traitement d'image, la recherche et le stockage des modèles.

- ***Principe de fonctionnement***

Le traitement des empreintes digitales se fait en deux étapes, l'enrôlement et la comparaison des empreintes digitales.

Lors de l'enrôlement, l'utilisateur doit poser son doigt sur le capteur deux fois. Le système traite les deux images du même doigt, si les deux prises sont identiques, le capteur génère un

modèle du doigt en fonction des résultats du traitement et enregistre le modèle dans sa base de données (maximum 170 modèles). Sinon, l'utilisateur ressaye de nouveau.

Lors de la comparaison, l'utilisateur met son doigt sur le capteur, le système va générer un modèle du doigt, le compare avec les modèles enregistrés et renvoyer le résultat correspondant (succès ou échec).

III.2.2.4.2. Principaux paramètres

Tableau III-3. Les principaux paramètres de notre capteur

Alimentation	DC 3.6V-6.0V	**Interface**	UART (TTL logical level)/ USB 1.1
Courant de fonctionnement	Typical: 100mA Peak: 150mA	**Mode de comparaison**	1:1 and 1:N
Vitesse de transmission	(9600*N) bps	**Taille d'un modèle**	512 bytes
Temps d'acquérir une image	<1s	**Niveau de sécurité**	5
Capacité de stockage	170	**T.F.R**	<0.1%
T.F.A	<0.001%	**Dimension de la fenêtre**	14mm*18mm
Temps de recherche moyen	< 1s	**Dimension**	56*20*21.5mm
Environnement opérationnel	Temp.: -10°C- +40°C		
	RH: 40%-85%		

III.2.3.Microcontrôleur

III.2.3.1. Introduction

Pour collecter et traiter des données provenant du capteur nous avons besoin d'un organe qui assure cette fonction, l'organe le plus adapté pour ces taches est le microcontrôleur.

III.2.3.2. Définition

Un microcontrôleur, est un composant électronique qui rassemble tous les éléments d'un "mini-ordinateur" et qui se présente sous la forme d'un circuit intégré. Il permet de réaliser des systèmes et montages électroniques programmés. Cela veut dire que l'on pourra, avec le même

montage, réaliser des fonctions très différentes qui dépendront du programme qui aura été programmé dans le microprocesseur [7].

Le microcontrôleur correspond au cerveau. C'est lui qui va traiter les informations provenant des capteurs et qui va donner la réponse voulue.

III.2.3.3. Structure

En général les microcontrôleurs sont composés de quatre parties :

- Un microprocesseur qui va prendre en charge la partie traitement des informations et envoyer des ordres. Il est lui-même composé d'une unité arithmétique et logique(UAL) et d'un bus de données. C'est donc lui qui va exécuter le programme embarqué dans le microcontrôleur.
- Une mémoire de données (Random Access Memory (RAM)) dans laquelle seront entreposées les données temporaires nécessaires aux calculs. C'est en fait la mémoire de travail qui est donc volatile.
- Une mémoire programmable (Read Only Memory (ROM)), qui va contenir les instructions du programme pilotant l'application à laquelle le microcontrôleur est dédié. Il s'agit ici d'une mémoire non volatile puisque le programme à exécuter est à priori toujours le même. Il existe différents types de mémoires programmables que l'on utilisera selon l'application. Notamment:
    - OTPROM (One-Time Programmable Read Only Memory) : programmable une seule fois mais ne coute pas très cher.
    - UVPROM (Ultraviolet Programmable Read Only Memory) : on peut la préfacer plusieurs fois grâce aux ultraviolets.
    - EEPROM (Electrically-Erasable Programmable Read-Only Memory) : on peut la préfacer plusieurs fois de façon électrique comme les mémoires flash.
- La dernière partie correspond aux ressources auxiliaires. Celles-ci sont généralement :
    - Ports d'entrées / sorties parallèle et série.
    - Des timers pour générer ou mesurer des signaux avec une grande précision temporelle.
    - Des convertisseurs A/N (analogiques/ numériques) pour traiter les signaux analogiques.

La structure interne d'un microcontrôleur est représentée par la figure suivante :

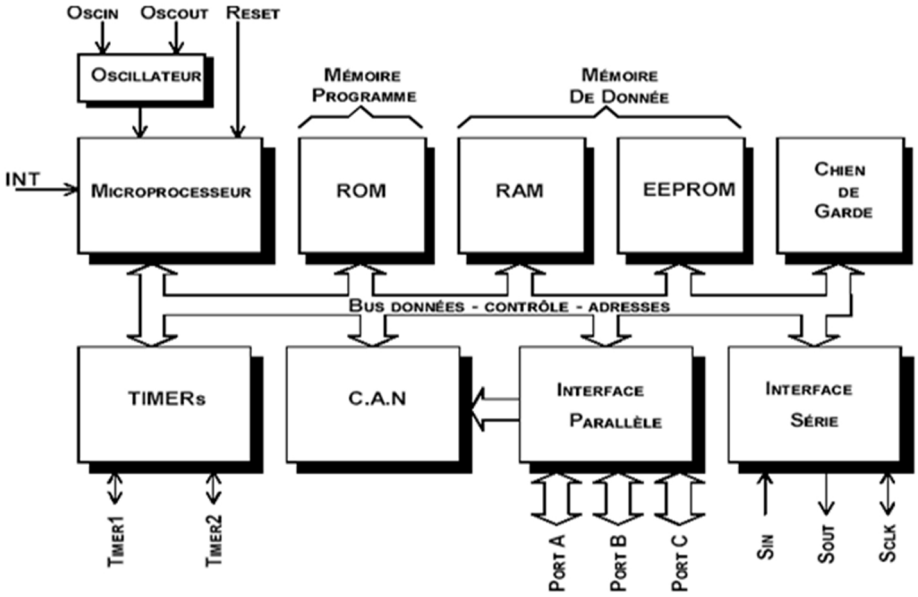

Figure III-14. Structure interne du microcontrôleur

Un microcontrôleur est cadencé par une horloge qui fixe la vitesse d'exécution des instructions de base.

III.2.3.4. Différents microcontrôleurs

Il existe plusieurs microcontrôleurs dans le marché dont lesquelles deux prouvent être utiliser dans notre pointeuse, citant ainsi le PIC 16F887 et l'ATMEGA328P (utilisé dans Arduino). Dans ce qui suit nous allons présenter ces deux microcontrôleurs.

III.2.3.4.1. PIC 16f887

16F877 est le nom d'un microcontrôleur Microchip de la famille PIC 16Fxxx.

Figure III-15. PIC16F877

- ***Désignation***

Le numéro 16 signifie qu'il fait partie de la famille "MID-RANGE". C'est un microcontrôleur de la famille 8 bits. Cela veut dire que l'ALU (Arithmetic and Logique Unit ou Unit Arithmétique et Logique en français) traite naturellement des mots de 8 bits maximum.

La lettre F indique que la mémoire programme de ce PIC est de type "Flash". Chaque ligne de mémoire est un mot de 14 bits.

Les trois derniers chiffres permettent d'identifier précisément le PIC, ici c'est un PIC de type 877.

La référence 16F877 peut avoir un suffixe du type "-XX" dans lequel XX représente la fréquence d'horloge maximale que le PIC peut recevoir [9].

- ***Caractéristiques***

Le **Tableau III-4** présente les principales caractéristiques du microcontrôleur PIC16f877[8].

Tableau III-4. Caractéristiques du microcontrôleur PIC16F877

Fabricant	Microchip
Catégorie du produit	Microcontrôleurs 8 bits
Largeur du bus de données	8 bits
Fréquence de l'horloge max.	20 MHz
Type de la mémoire programme	Flash
Nombre d'horloges/de compteurs	3 Timer
Taille de la mémoire du programme	14 kilo Bytes
Taille de la RAM de données	368 Bytes
Résolution CAN (convertisseur analogique/nemerique)	10 bits
Tension d'alimentation de fonctionnement	2 Volts to 5.5 Volts
Température de fonctionnement max.	+ 125 C
Type de la RAM de données	SRAM (Static random-access memory)
Taille de la ROM de données	256 Bytes
Nombre d'E/S (entrée /sortie)	33 I/O (Input / output)

- *Applications*

Le microcontrôleur PIC 16F877 est devenu un microcontrôleur très populaire dans l'électronique loisir. Sa simplicité, son prix, et l'accessibilité des outils de programmation peuvent expliquer sa popularité [9].

- ***Programmation***

Les méthodes de programmations disponibles (il en existe peut-être d'autres) sont :

- Écrire directement un fichier en Hexadécimal (comme dans les années 1960) ;
- Écrire en assembleur ;
- Écrire en C.

III.2.3.4.2. ATmega328P

- ***Définition***

L'ATmega328P est un microcontrôleur 8 bits, de la famille megaAVR MCU, développé par Atmel. Il fournit un équilibre délicat entre la performance et la stabilité.

- ***Caractéristiques***

Le **Tableau III-5** présente les principales caractéristiques de ce microcontrôleur [10].

Tableau III-5. Caractéristiques du microcontrôleur ATmega328P

Fabricant	Atmel
Catégorie du produit	Microcontrôleurs 8 bits
Cœur	AVR
Largeur du bus de données	8 bits
Fréquence de l'horloge max.	20 MHz
Type de la mémoire programme	Flash
Nombre d'horloges/de compteurs	3 Timer
Taille de la mémoire du programme	32 kilo Bytes
Taille de la RAM de données	2 kilo Bytes
Résolution CAN	10 bits
Tension d'alimentation de fonctionnement	1.8 Volts to 5.5 Volts
Température de fonctionnement max.	+ 85 C
Type de la RAM de données	SRAM
Taille de la ROM de données	1 kilo Bytes
Nombre d'E/S	23 I/O

- ***Application***

Aujourd'hui, l'ATmega328P est couramment utilisé dans de nombreux projets et systèmes autonomes. Son utilisation la plus courante est sur la populaire plate-forme de développement Arduino, à savoir les modèles Arduino Uno et Arduino Nano [10].

- ***Programmation***

La plus courante méthode de programmation de l'ATmega328P est en langage C avec le logiciel Arduino.

III.2.3.5. Choix du microcontrôleur

ATmega328P est intégré dans la carte Arduino Uno. Cette dernière est utilisée dans notre pointeuse. Dans ce qui suit nous allons voir pourquoi choisir l'Arduino.

III.2.3.5.1. Taille de la mémoire du programme

Le microcontrôleur utilisé par Arduino a une taille de mémoire du programme suffisante pour notre system contrairement aux autres microcontrôleurs.

III.2.3.5.2. La liberté

C'est un bien grand mot, mais elle définit de façon assez concise l'esprit de l'Arduino. Elle constitue en elle-même deux choses :

- Le logiciel : gratuit et open source, développé en Java, dont la simplicité d'utilisation relève du savoir cliquer sur la souris.
- Le matériel : cartes électroniques dont les schémas sont en libre circulation sur internet.

III.2.3.5.3. La compatibilité

Le logiciel, tout comme la carte, est compatible sous les plateformes les plus courantes (Windows, Linux et Mac), contrairement aux autres outils de programmation du commerce qui ne sont, en général, compatibles qu'avec Windows [11].

III.2.3.5.4. La communauté

La communauté Arduino est impressionnante et le nombre de ressources à son sujet est en constante évolution sur internet. De plus, on trouve les références du langage Arduino ainsi qu'une page complète de tutoriels sur le site arduino.cc (en anglais) et arduino.cc/fr (en français) [11].

III.2.3.6. Présentation d'Arduino

III.2.3.6.1. Qu'est-ce que c'est ?

Arduino est un projet créé par une équipe de développeurs, composée de six individus : Massimo Banzi, David Cuartielles, Tom Igoe, Gianluca Martino, David Mellis et Nicholas Zambetti. Cette équipe a créé le "système Arduino" comme outil qui va permettre aux débutants, amateurs ou professionnels de créer des systèmes électroniques plus ou moins complexes [11].

III.2.3.6.2. Le but et l'utilité

Le système Arduino, nous donne la possibilité d'allier les performances de la programmation à celles de l'électronique. Plus précisément, nous allons programmer des systèmes électroniques. Le gros avantage de l'électronique programmée c'est qu'elle simplifie grandement les schémas électroniques et par conséquent, le coût de la réalisation, mais aussi la charge de travail à la conception d'une carte électronique.

III.2.3.6.3. Applications

Le système Arduino nous permet de réaliser un grand nombre de choses, qui ont une application dans tous les domaines ! Par exemple :

- contrôler les appareils domestiques ;
- fabriquer votre propre robot ;
- communiquer avec l'ordinateur.

III.2.3.6.4. Les outils Arduino

Arduino est composé de deux choses principales, qui sont :

- le matériel.
- le logiciel.

Avec ces deux outils réunis, il nous sera possible de faire n'importe quelle réalisation.

- ***Le matériel***

Il s'agit d'une carte électronique basée autour d'un microcontrôleur Atmega328P du fabricant Atmel et de composants complémentaires qui facilitent la programmation et l'interfaçage avec d'autres circuits, et dont le prix est relativement bas pour l'étendue possible des applications [11]. La carte est montrée par la **figure III-16**.

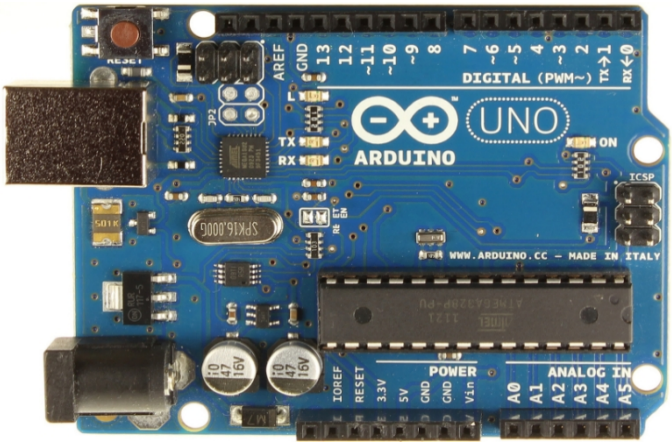

Figure III-16. Carte Arduino "Uno" utilisée pour la réalisation

La figure suivante montre les différents composants de la carte Arduino UNO.

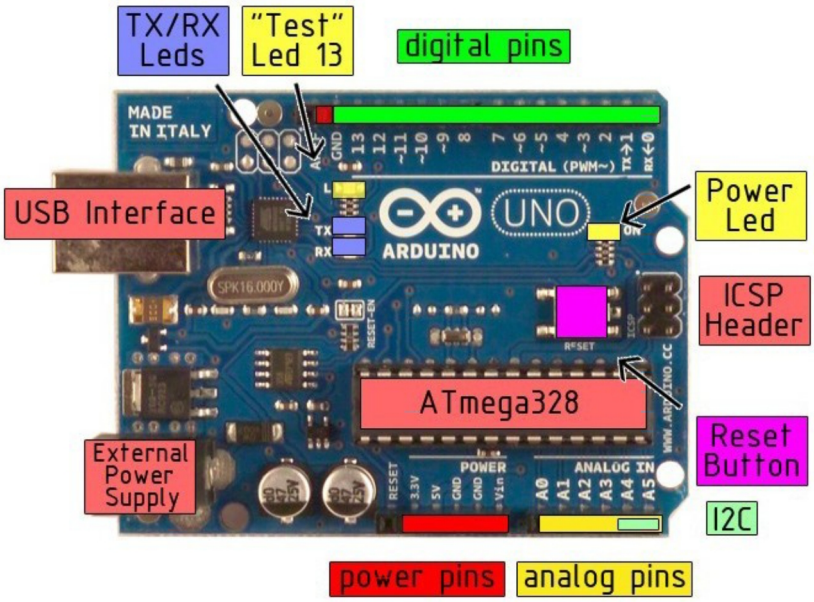

Figure III-17. Les principaux composants de la carte Arduino UNO

- ***Les « shields »***

Il existe de nombreux shields que l'on traduit parfois dans les documentations par «boucliers». Un « shield » Arduino est une petite carte qui se connecte sur une carte Arduino pour **augmenter ses fonctionnalités**. Quelques exemples de « shields » :

- Afficheur graphique ;
- Ethernet et carte SD ;
- GPS (Global Positioning System) ;
- Carte de prototypage (type labdec).

Dans notre pointeuse nous allons utiliser Ethernet Shield pour que notre arduino puisse communiquer avec notre serveur. La figure ci-dessous montre notre Ethernet shield monté sur l'Arduino Uno.

Figure III-18. Arduino UNO + Shield Ethernet

- ***Le logiciel***

Le logiciel de programmation des modules Arduino est une application Java multiplateformes (fonctionnant sur tout système d'exploitation), servant d'éditeur de code et de compilateur, et qui peut transférer le firmware (et le programme) au travers de la liaison série (RS232, Bluetooth ou USB (Universal Serial Bus) selon le module) [11].

De très nombreux exemples sont fournis et sont vraiment bien documentés. Ils permettent de coder des choses très compliquées sans trop d'efforts. Les bibliothèques fournies permettent d'utiliser des composants complexes très simplement en quelques lignes très claires.

La **Figure III-19** montre une partie de la programmation du logiciel Arduino. Ce logiciel, il faut juste le comprendre et l'utiliser.

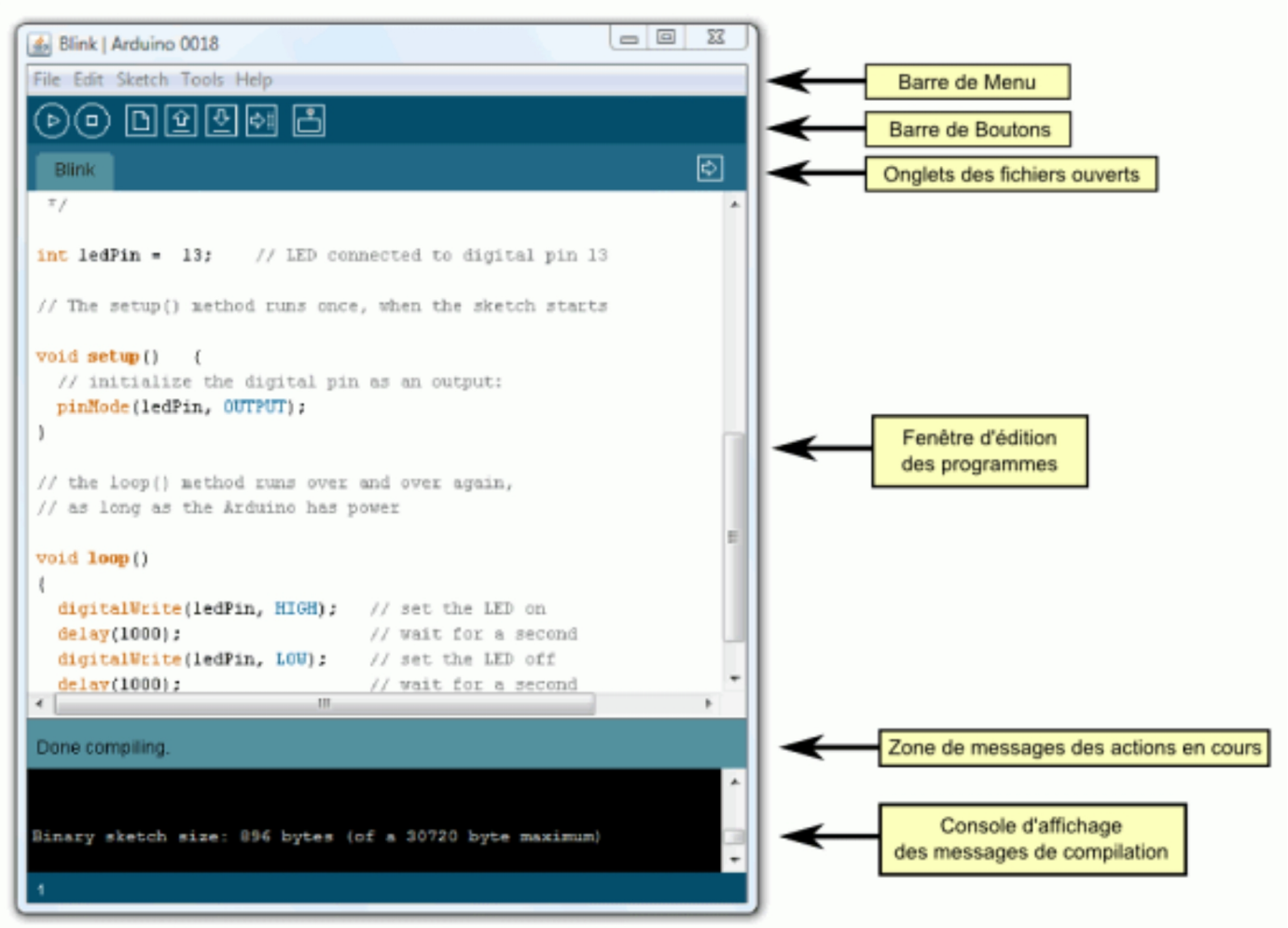

Figure III-19. Logiciel Arduino

Le logiciel comprends aussi un moniteur série (équivalent à hyperterminal) qui permet d'afficher des messages textes émis par la carte Arduino et d'envoyer des caractères vers la carte Arduino (en phase de fonctionnement).

La **Figure III-20** illustre la fonction de chaque bouton dans la barre de boutons.

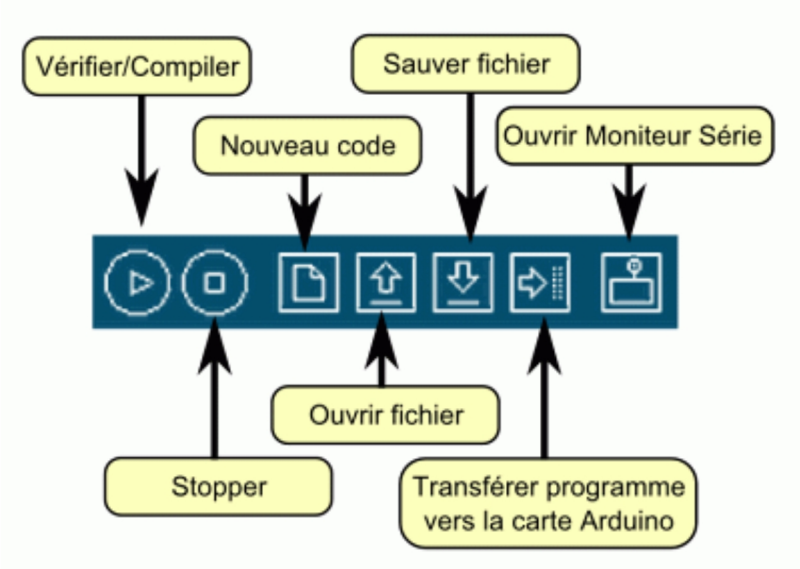

Figure III-20. Barre de boutons du logiciel Arduino

III.2.3.7. Conclusion

L'Arduino Uno, nous l'avons jugé l'outil idéal pour notre pointeuse. Son utilisation va rendre notre système plus efficace.

III.2.4.Control et traitement

III.2.4.1. Introduction

Dans cette partie nous allons parler de ce qui concerne le control et le traitement des informations émis par notre Arduino.

Les informations de l'empreinte acquises par le capteur sont transférées par l'Arduino vers notre contrôleur via Ethernet Shield et un câble RJ45 sous le Protocol TCP/IP. Ces informations vont être traitées et traduites par notre contrôleur.

L'objectif principal de notre contrôleur est d'enregistrer la date et l'heure du pointage d'un employé en assurant une surveillance en temps réel par une application web. Pour cela nous avons besoin d'un serveur qui gère la communication avec l'Arduino et l'utilisateur, et d'une base de données rapide et efficace pour stocker l'historique du pointage.

Pour cela nous avons opté pour des logiciels puissants et gratuits, ces logiciels sont connus sous le nom de LAMP serveur et seront installés sur le RASPBERRY PI2.

III.2.4.2. Serveur « LAMP »

Le serveur « LAMP » est un acronyme désignant un ensemble de logiciels libres permettant de construire des serveurs de sites web [12]. L'acronyme original se réfère aux logiciels suivants :

- « Linux », le système d'exploitation constituant la base du système (GNU/Linux) ;
- « Apache », le serveur Web qui gére la communication avec le client ;
- « MySQL ou MariaDB », le système de gestion de base de données ;
- « PHP », « Perl » ou « Python », les langages de script utilisé pour générer les pages dynamiques [12].

Même si les auteurs de chacun de ces programmes ne se sont pas coordonnés pour construire des plates-formes LAMP, cette combinaison de logiciels s'est popularisée du fait du faible coût de l'ensemble et de la présence de tous ces composants dans la plupart des distributions GNU/Linux.

Cet acronyme a été inventé par Michael Kunze qui l'a utilisé pour la première fois en 1998 dans le magazine allemand « c't ». L'article en question voulait démontrer qu'un ensemble de logiciels libres pouvait concurrencer les offres commerciales disponibles [12].

III.2.4.2.1. Architecture

Les rôles de ces quatre composants sont les suivants :

- Linux assure l'attribution des ressources aux autres composants (Rôle d'un Système d'exploitation ou OS pour Operating System) ;
- Apache est le serveur web « frontal » : il est « devant » tous les autres et répond directement aux requêtes du client web (navigateur) ;
- MySQL est un système de gestion de bases de données (SGBD). Il permet de stocker et d'organiser des données ;
- Le langage de script PHP permet la génération de pages web dynamiques et la communication avec le serveur MySQL.

La figure suivante montre l'architecture du LAMP serveur en général :

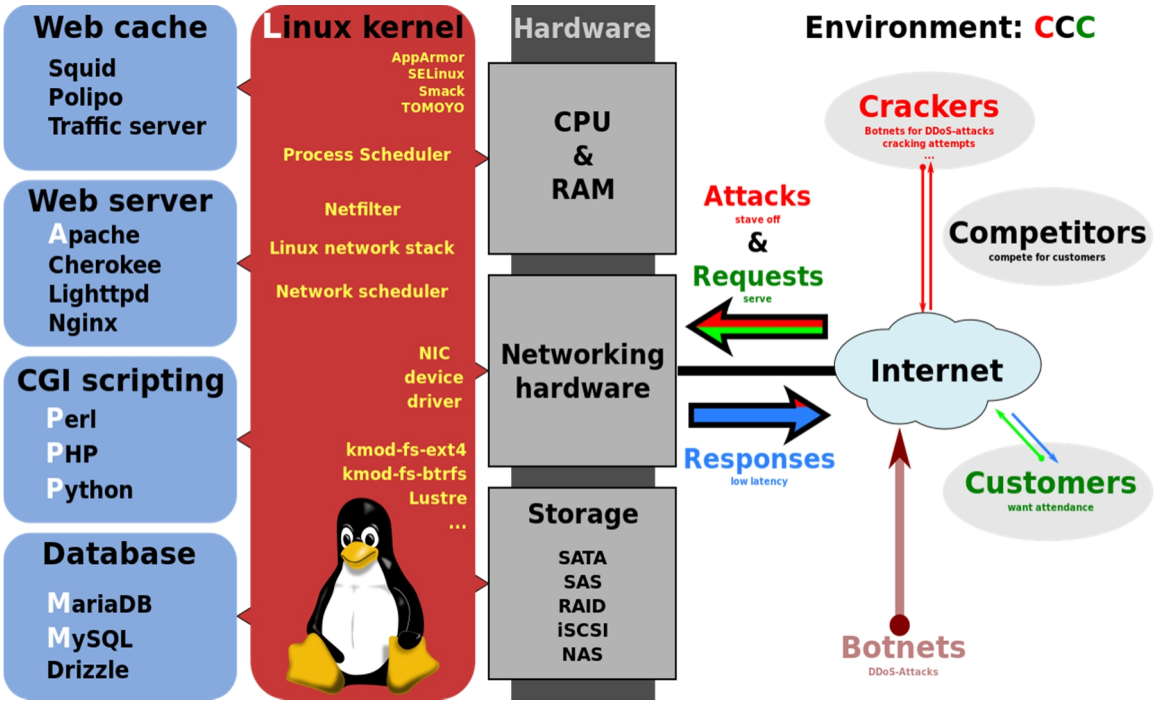

Figure III-21. Architecture du serveur LAMP [12]

Tous les composants peuvent être situés :

- Sur une même machine ;
- Sur deux machines, généralement Apache et le langage de script d'un côté et MySQL de l'autre ;
- Sur de nombreuses machines pour assurer la haute disponibilité.

III.2.4.2.2. Serveur HTTP Apache 2

Le logiciel libre Apache HTTP Server (Apache) est un serveur http (HyperText Transfer Protocol) créé et maintenu au sein de la fondation Apache. C'est le serveur HTTP le plus populaire du World Wide Web [13].

Figure III-22. Logo de la Fondation Apache Software

- ***Qu'est-ce que le Web ?***

Le Web est un des nombreux services disponibles sur Internet. Il s'agit de l'ensemble des documents accessibles par le protocole HTTP (par un navigateur Web). Une caractéristique essentielle du Web est la capacité de passer d'un document à un autre par des liens hypertexte [13]. Un site Web est quant à lui un ensemble de pages Web, liées entre elles.

Un site Web a une adresse, comme celle du site Google : http://google.dz.

- ***Mode de fonctionnement sommaire***

Au moment de son démarrage, Apache charge les fichiers de configuration de la machine locale et se met en attente de requêtes sur les interfaces réseaux.

Lorsque vous utilisez votre navigateur Web (un client HTTP), que vous cliquiez sur un lien ou que vous rentriez directement l'adresse dans la barre d'adresse, vous effectuez une requête :

- Le client détermine et se connecte au serveur;
- Le client effectue une requête HTTP sur le serveur, par la méthode GET du protocole HTTP : il lui demande une page ;
- Après l'analyse de la requête, le serveur renvoie la page concernée sous forme de code dont on peut spécifier le format de données ;
- Une fois toutes les données envoyées, le serveur ferme la connexion ;
- Parallèlement, le client analyse et construit l'affichage à partir du code reçu.

Voilà, comment fonctionnent le protocole HTTP et APACHE2 (sans entrer dans les détails) [13].

III.2.4.2.3. MySQL

MySQL est un Système de Gestion de Bases de Données Relationnelles (abrégé SGBDR). C'est-à-dire un logiciel qui permet de gérer des bases de données, et donc de gérer de grosses quantités d'informations. Il utilise pour cela le langage SQL. Il s'agit d'un des SGBDR les plus connus et les plus utilisés (Wikipédia et Adobe utilisent par exemple MySQL) [14].

Figure III-23. Logo de MySQL

MySQL peut donc s'utiliser seul, mais est la plupart du temps combiné à un autre langage de programmation : PHP par exemple pour de nombreux sites web, mais aussi Java, Python, C++, et beaucoup d'autres [14].

- ***Base de données***

Une base de données informatique est un ensemble de données qui ont été stockées sur un support informatique, et organisées et structurées de manière à pouvoir facilement consulter et modifier leur contenu.

Prenons l'exemple d'un site web avec un système de news et de membres. On va utiliser une base de données MySQL pour stocker toutes les données du site : les news (avec la date de publication, le titre, le contenu, éventuellement l'auteur,…) et les membres (leurs noms, leurs emails,…).

Tout ceci va constituer notre base de données pour le site. Mais il ne suffit pas que la base de données existe. Il faut aussi pouvoir la gérer, interagir avec cette base**.** Il faut pouvoir envoyer des messages à MySQL (messages qu'on appellera "requêtes"), afin de pouvoir ajouter des news, modifier des membres, supprimer, et tout simplement afficher des éléments de la base.

- ***Le langage SQL***

Le SQL (*Structured Query Language en français langage de requête structurée*) est un langage informatique qui permet d'interagir avec des bases de données relationnelles**.** C'est le langage pour base de données le plus répandu, et c'est bien sûr celui utilisé par MySQL. C'est donc le langage que nous allons utiliser pour dire au client MySQL d'effectuer des opérations sur la base de données stockée sur le serveur MySQL [14].

III.2.4.2.4. PHP

PHP: Hypertext Preprocessor, plus connu sous son sigle PHP, est un langage de programmation libre, principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP, mais pouvant également fonctionner comme n'importe quel langage interprété de façon locale. PHP est un langage impératif orienté objet [15].

Figure III-24. Logo de PHP

PHP a permis de créer un grand nombre de sites web célèbres, comme Facebook, Wikipédia, etc. Il est considéré comme la base de la création des sites Internet dits dynamiques.

- ***Fonctionnement***

PHP appartient à la grande famille des descendants du C, dont la syntaxe est très proche. En particulier, sa syntaxe et sa construction ressemblent à celles des langages Java et Perl, à ceci près que du code PHP peut facilement être mélangé avec du code HTML (Hypertext Markup Language) au sein d'un fichier PHP [15].

Dans une utilisation destinée à l'internet, l'exécution du code PHP se déroule ainsi : lorsqu'un visiteur demande à consulter une page de site internet, son navigateur envoie une requête au serveur HTTP correspondant. Si la page est identifiée comme un script PHP (généralement grâce à l'extension .php), le serveur appelle l'interprète PHP qui va traiter et générer le code final de la page (constitué généralement d'HTML ou de XHTML (Extensible HyperText Markup Language), mais aussi souvent de feuilles de style en cascade et de JavaScript). Ce contenu est renvoyé au serveur HTTP, qui l'envoie finalement au client. Ce schéma explique ce fonctionnement :

Figure III-25. Schéma de l'exécution du code PHP [15]

Une étape supplémentaire est souvent ajoutée : celle du dialogue entre PHP et la base de données. Classiquement, PHP ouvre une connexion au serveur de SGBD voulu, lui transmet des requêtes et en récupère le résultat, avant de fermer la connexion.

L'utilisation de PHP en tant que générateur de pages Web dynamiques est la plus répandue, mais il peut aussi être utilisé comme langage de programmation ou de script en ligne de commande sans utiliser de serveur HTTP ni de navigateur. Il permet alors d'utiliser de nombreuses fonctions du langage C et plusieurs autres sans nécessiter de compilation à chaque changement du code source [15].

III.2.4.2.5. GNU/Linux

GNU/Linux est le nom parfois donné à un système d'exploitation associant des éléments essentiels du projet GNU et d'un noyau Linux. C'est une terminologie créée par le projet Debian et reprise notamment par Richard Stallman, à l'origine du projet de travail collaboratif GNU, lequel manquait encore d'un noyau de système d'exploitation pour en faire un système d'exploitation complet lors de la création du noyau Linux en 1991. Des systèmes complets prêts à l'emploi, réunissant les deux pièces, sont alors apparus, comme la distribution Debian.

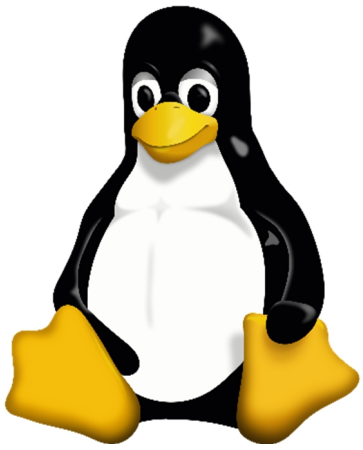

Figure III-26. Logo de Linux

Dans le langage courant on trouve souvent l'emploi du terme « Linux » seul pour désigner une distribution du système d'exploitation GNU/Linux, ce qui peut porter à confusion étant donné qu'il existe quelques systèmes fondés sur Linux mais pas sur GNU (par exemple : Android, ceci lui permettant d'éviter certaines clauses de la licence GNU) [16].

- ***Ubuntu***

Ubuntu est un système d'exploitation open source basé sur la distribution Linux Debian. Son nom provient d'un ancien mot bantou qui signifie « je suis ce que je suis grâce à ce que nous sommes tous ». Dans le même ordre d'esprit, les utilisateurs sont encouragés à étudier son fonctionnement, le modifier, l'améliorer et enfin de le redistribuer. En 2011, une estimation donne plus de 25 millions d'utilisateurs des différentes versions pour ordinateurs [17].

Figure III-27. Logo de Ubuntu

- ***Utilisation***

  - **Serveur**

En raison de la relation de GNU/Linux avec UNIX, GNU/Linux s'est très rapidement imposé sur le marché des serveurs informatiques. Un point crucial a été la possibilité d'utiliser un système d'exploitation de type UNIX sur du matériel compatible PC, beaucoup moins cher que les solutions à base d'UNIX propriétaire et de matériel spécifique. De nombreux logiciels serveurs très demandés et très utilisés (serveur HTTP, base de données, groupware, serveur de messagerie électronique, etc.) étant disponibles gratuitement, en général sans aucune limitation, et fiables, la part de marché de GNU/Linux dans ce domaine a en conséquence crû rapidement.

Le GNU/Linux ayant une réputation de stabilité et d'efficacité dans la maintenance, il remplit les exigences posées à tout système d'exploitation pour serveurs.

Les serveurs GNU/Linux sont exploités dans à peu près tous les domaines. Un des exemples les plus connus est résumé par l'acronyme LAMP, où GNU/Linux propulse un serveur web Apache associé à la base de données MySQL et au langage de programmation PHP (alternativement : Perl ou Python) [16].

- **Sécurité réseau**

Le GNU/Linux, qui jouit d'une bonne réputation en matière de sécurité et de performance (passage à l'échelle) est très utilisé dans le domaine des réseaux informatiques, par exemple comme passerelle, comme routeur, proxy ou comme pare-feu [16].

- **Ordinateur central**

L'aspect libre du code source, et la possibilité qui en découle d'adapter le système à une tâche précise, a permis à GNU/Linux de faire son entrée dans les centres de calculs. Sur ce marché des ordinateurs centraux, gros ordinateurs très fiables optimisés pour le traitement massif de données, omniprésents dans les banques, les sociétés d'assurances et les grandes entreprises, GNU/Linux fait de plus en plus concurrence aux systèmes UNIX propriétaires qui étaient autrefois la norme [16].

- **Embarqué**

Linux se trouve au cœur de nombreux appareils informatiques ou électroniques grand public, et parfois sans que l'usager le sache. Il s'agit notamment d'équipement réseau et de petits appareils numériques destinés à la consommation de masse, équipés en général d'un processeur spécialisé économe en énergie et d'une mémoire flash.

Le succès de Linux dans ce domaine tient, ici comme ailleurs, à ce que les fabricants apprécient de pouvoir d'une part adapter le logiciel à leurs besoins (consommation, interface, fonctions annexes, etc.) et d'autre part de bénéficier de l'expérience et du travail d'une communauté active. Linux est aussi apprécié dans ce domaine pour sa fiabilité, sa résistance aux attaques des pirates informatiques sur les réseaux et bien sûr sa gratuité [16].

- **Réseaux et communication**

Linux fait tourner plusieurs routeurs dont certains modèles de Linksys, ainsi que divers terminaux fournis par des fournisseurs d'accès à Internet (comme la Freebox, la Neufbox de SFR ou la Livebox en France) [16].

- **Robotique**

Le marché décollant des systèmes de robots ludiques utilise un OS Linux [16].

III.2.4.3. Raspberry Pi 2

Le Raspberry Pi est un nano-ordinateur monocarte à processeur ARM (Advanced RISC Machine) conçu par le créateur de jeux vidéo David Braben, dans le cadre de sa fondation Raspberry Pi. Cet ordinateur, qui a la taille d'une carte de crédit, est destiné à encourager l'apprentissage de la programmation informatique; il permet l'exécution de plusieurs variantes du système d'exploitation libre GNU/Linux et des logiciels compatibles [18].

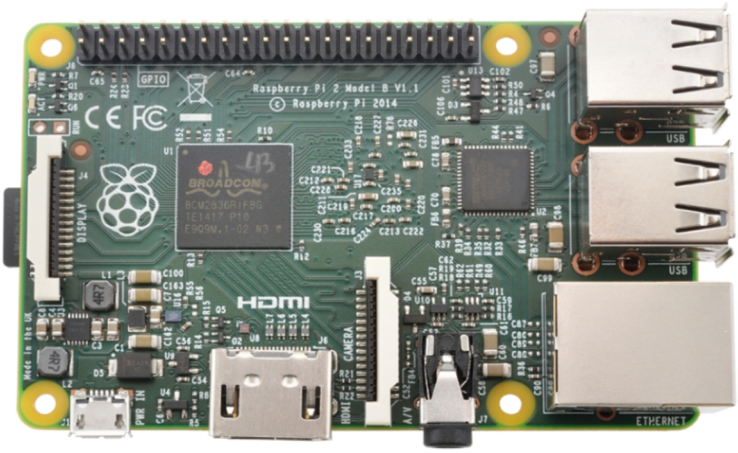

Figure III-28. Raspberry PI2

Il est fourni nu (carte mère seule, sans boîtier, alimentation, clavier, souris ni écran) dans l'objectif de diminuer les coûts et de permettre l'utilisation de matériel de récupération.

III.2.4.3.1. Spécifications

Le 2 février 2015, la fondation Raspberry Pi annonce la sortie du Raspberry Pi 2, plus puissant que Raspberry Pi A et B, il est équipé de :

- Processeur Broadcom BCM2836, quatre cœurs ARMv7 à 900 MHz, accompagné de 1 Go de RAM ;
- 2 Sorties vidéo : Composite et HDMI (High Definition Multimedia Interface) ;
- 1 Sortie audio stéréo Jack 3,5 mm (sortie son 5.1 sur la prise HDMI) ;
- Unité de lecture-écriture de carte mémoire : SDHC / MMC / SDIO ;
- GPIO 40 broches ;
- 1 port réseau Fast Ethernet (10/100 Mbit/s) ;
- Support I2C ;
- GPIO 40 broches ;
- 4 ports USB 2.0 ;
- Lecteur micro SD.

III.2.5. Les algorithmes

Dans cette section nous allons présenter les algorithmes par lesquels notre pointeuse fonctionne.

III.2.5.1. L'algorithme de l'Arduino

Entrées :

- Les données venant du capteur d'empreinte.
- Les commandes depuis le serveur.

Sorties :

- Des commandes vers le capteur et la commande électrique.
- Des données vers le serveur.

Reconnaissance de l'empreinte digitale

Si le mode de fonctionnement est de scanner une empreinte digitale

Si une empreinte est détectée

Si l'empreinte est reconnue

Alors envoyer le message au serveur contenant l'Identifiant (ID) de l'empreinte et alimenter la commande électrique

Fin de Si

Sinon retourne au début

Fin de Si

Sinon Si le mode de fonctionnement est d'enregistrer une empreinte digitale

Si une empreinte est détectée

Alors traiter l'empreinte, l'enregistre et lui affecter un ID

Sinon attendre jusqu'à ce qu'une empreinte soit détecter ou attendre un intervalle de temps avant que celui-ci passe à l'étape suivante.

Fin de Si

Sinon retourne au début

Fin de Si

L'ouverture de la porte

Si le client demande l'ouverture de porte à distance

Alors alimenter la commande électrique

Fin de Si

III.2.5.2. L'algorithme du serveur

Entrées :

- Les données venant de l'Arduino.
- Les commandes depuis le navigateur Web.

Sorties :

- Des commandes vers l'Arduino.
- Des données vers la base de données.

Si une donnée reçue depuis l'Arduino contenant un ID

Alors rechercher l'ID dans la base de données et récupérer les informations qui appartiennent à cet ID et les affichées.

Si le fonctionnaire entre dans l'entreprise

Alors ajouter à la base de données de pointage une nouvelle entrée contenant l'ID avec la date et l'heure d'entrée

Sinon ajouter l'heure de sortie à la base de données de pointage dans l'entrée qui contient le dernier même ID sans une heure de sortie.

Fin de Si

Sinon Si l'utilisateur lance une recherche sur un fonctionnaire

Alors rechercher l'ID dans la base de données et récupérer les informations qui appartiennent à cet ID.

Sinon Si l'utilisateur ajoute un nouveau fonctionnaire

Alors ajouter à la base de données des fonctionnaires une nouvelle entrée contenant l'ID, le nom et le prénom de ce dernier.

Sinon Si l'utilisateur ajoute un nouvel utilisateur

Alors ajouter à la base de données des utilisateurs une nouvelle entrée contenant le nom d'utilisateur et le mot de passe.

Sinon Si l'utilisateur clique sur ouvrir la porte

Alors envoyer à l'Arduino l'ordre d'alimenter la commande électrique

Sinon retourne au début

Fin de Si

III.3. Réalisation

III.3.1. Introduction

Nous allons vous présenter dans cette partie le SAP retenu pour la gestion de la pointeuse biométrique.

III.3.2. Définition

Le SAP est l'acronyme de *Système d'Auto-gérance de Pointage*, destiné aux entreprises de tous les secteurs d'activité qui ont besoin de suivre la présence des employés. Il comporte deux aspects :

- L'application web SAPweb.
- Les instruments d'acquisition

Figure III-29. Logo du SAP

III.3.3. Application SAPweb

Le SAPweb est une application d'aide à la gestion du pointage pour les gestionnaires d'entreprise et de ressources humaines.

L'application est désignée pour effectuer le suivi des heures de travail de l'employé. Elle nous permet également, en quelques clics, d'avoir des informations sur un employé et de son historique de pointage.

Pour sécuriser l'application, il nous a été nécessaire de sécuriser l'application par des mots de passe comme le montre la **Figure III-30**. Chaque utilisateur aura son propre mot de passe qui lui permettra d'accéder uniquement aux informations fixées par le cahier de charge.

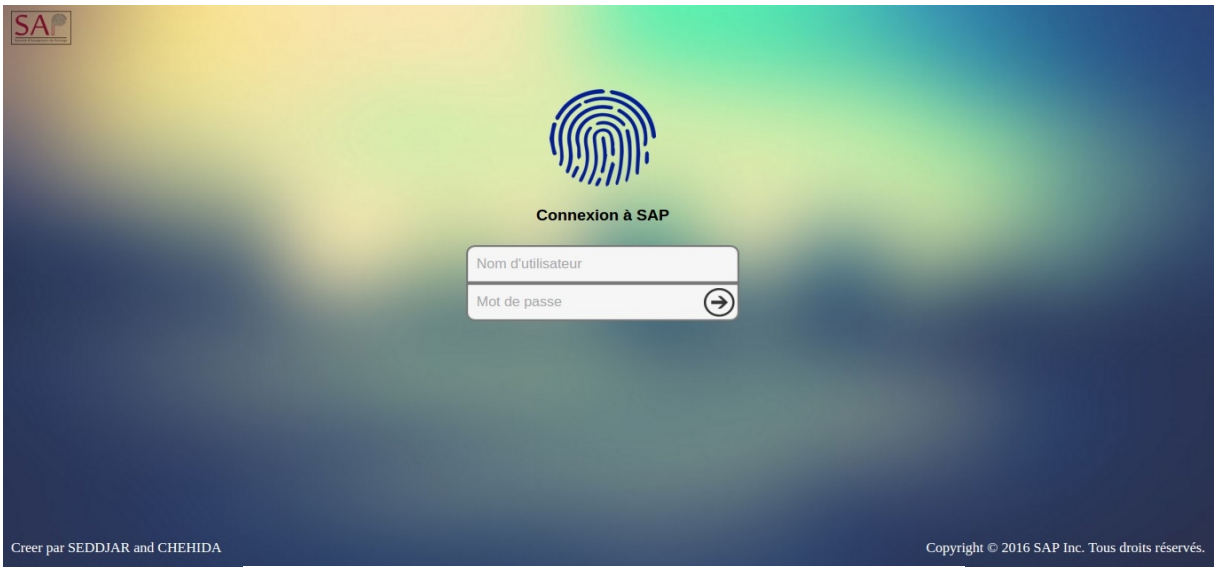

Figure III-30. Page d'identification de SAPweb

La **Figure III-31** montre la page d'accueil de l'application SAPweb utilisé pour notre application et imposé par le cahier de charge.

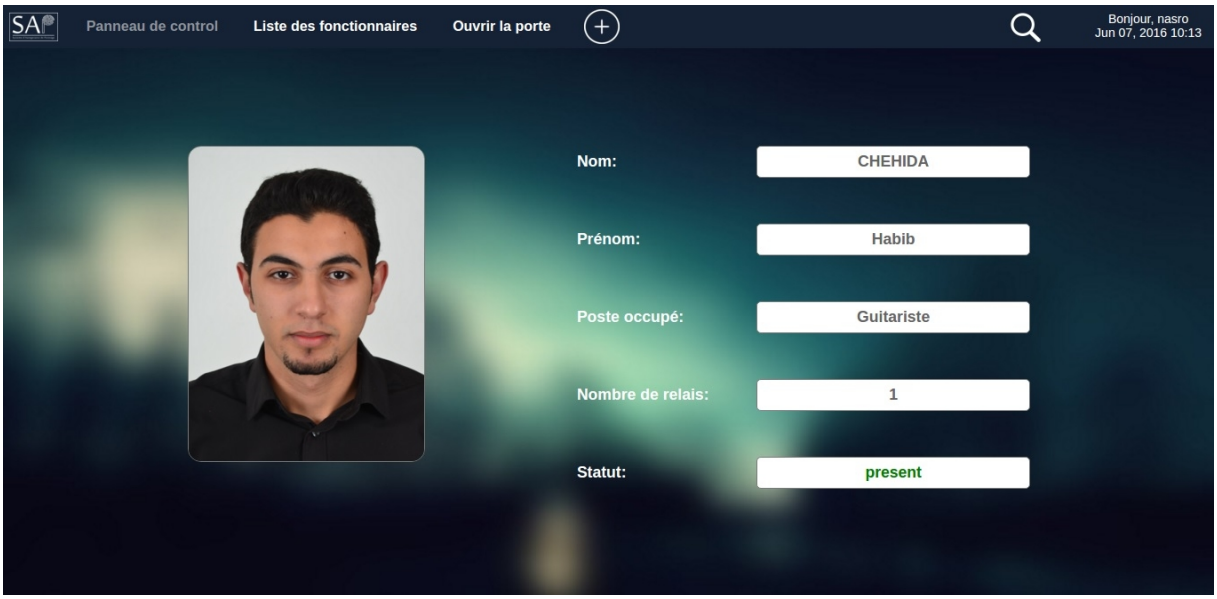

Figure III-31. Panneau de contrôle de l'application

III.3.4. Les instruments d'acquisition et de traitement

La maquette conçue pour l'ouverture d'une porte est représenté par les figures suivantes :

Figure III-33. La maquette en porte ouverte

Le point rouge sur la photo c'est le capteur.

Figure III-32. La maquette

Les instruments d'acquisition et de traitement que nous avons cité dans le chapitre III sont installés dans le tiroir de cette maquette comme le montre la photo ci-dessous.

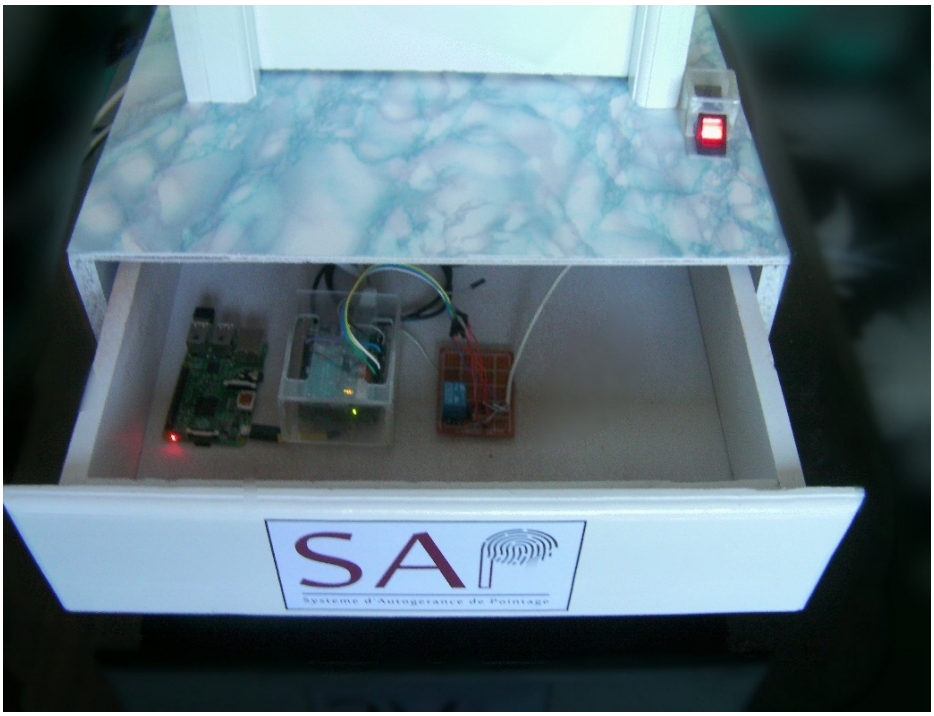

Figure III-34. Les instruments d'acquisition installés

III.4. Conclusion

L'étude conceptuelle de la pointeuse biométrique par empreinte digital nous a permis de bien choisir les différents outils, les méthodes et aussi composants pour sa conception dans un premier temps et ensuite pour sa réalisation dans un deuxième temps.

Le schéma synoptique présenté par la **Figure III-35** montre la représentation finale de notre pointeuse.

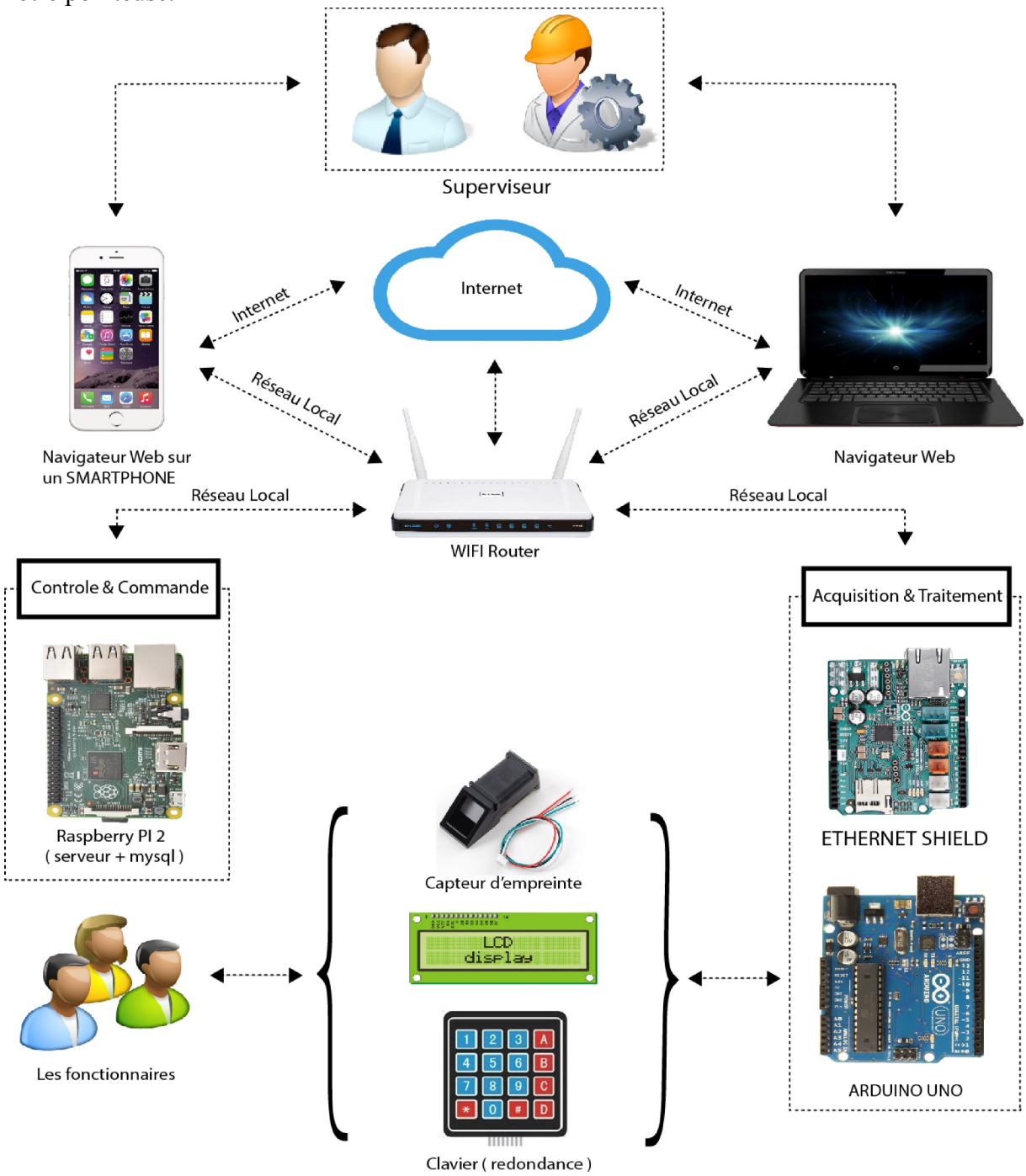

Figure III-35. Schéma synoptique du système SAP

Conclusion générale

Conclusion générale

Étant donné l'omniprésence des préoccupations en matière de sécurité et de fiabilité dans le monde d'aujourd'hui, il est peu probable que les systèmes de reconnaissance biométrique disparaissent. Ils deviendront sans doute dans tous les établissements où la sécurité est un enjeu.

Une analyse des différentes techniques biométriques développées au cours de ces dernières années a été présentée, et cela pour mettre en évidence les particularités ainsi que les avantages et les inconvénients de chacune d'entre elles.

Dans ce mémoire, nous nous sommes intéresses aux problèmes de l'authentification, le control d'accès et la gestion de la paperasse liée au personnel d'un établissement.

Pour cela nous avons utilisé un capteur d'empreinte digitale pour valider l'identité et ne donner l'accès qu'aux personnes autorisées.

Après l'étude et le choix de tous les éléments essentiels constituant notre système, nous avons enfin, réalisé une maquette, qui permet de tester notre système en réalité.

Le système présenté peut être utilisé dans tous les établissements où on aura besoin d'un système de pointage et de contrôle d'accès fiable et rapide.

Le choix du capteur d'empreinte digitale dépend de la technologie biométrique que le client souhaite mettre en place. Tout dépend fortement de l'environnement. Le taux d'erreur (EER = Equal-Error-Rate) dépend de l'ensemble joué par les algorithmes et le capteur d'empreinte digitale.

Les systèmes de reconnaissance biométrique sont des dispositifs de sécurité intrusifs. Certaines personnes s'opposent donc carrément à leur utilisation, alors que d'autres sont d'avis qu'ils peuvent être nécessaires dans certains cas, mais seulement si des mesures de sécurité et des mesures juridiques appropriées sont en place pour protéger les renseignements personnels de nature délicate recueillis.

En guise de perspectives, une extension de ce travail peut être réalisée en développant des algorithmes qui permettent de centralisé et sécurisé les données biométriques afin de rendre le system capable de communiquer avec plusieurs capteurs d'empreinte dans des différents endroits. Aussi, nous voulons intégrer des caméras de surveillance dans notre système, ainsi que le control à distance de l'éclairage et les chauffages.

Annexe I

1. L'écran LCD

LCD est l'abréviation anglaise de "liquid crystal display" qui veut dire : afficheur à cristaux liquides. Il consomme peu d'énergie.

L'écran LCD qu'on utilise est un écran permettant l'affichage de 16x2 caractères, c'est-à-dire deux lignes de 16 caractères.

1.1. Le branchement

L'afficheur LCD utilise 6 à 10 broches de données ((D0 à D7) ou (D4 à D7) + RS + E) et deux d'alimentations (+5V et masse). La plupart des écrans possèdent aussi une entrée analogique pour régler le contraste des caractères. Nous brancherons dessus un potentiomètre de 10 kOhms. Les 10 broches de données peuvent être placées sur n'importe quelles entrées/sorties numériques de l'Arduino.

1.2. Le montage à 4 broches de données

La figure suivante montre le montage de LCD avec l'Arduino UNO

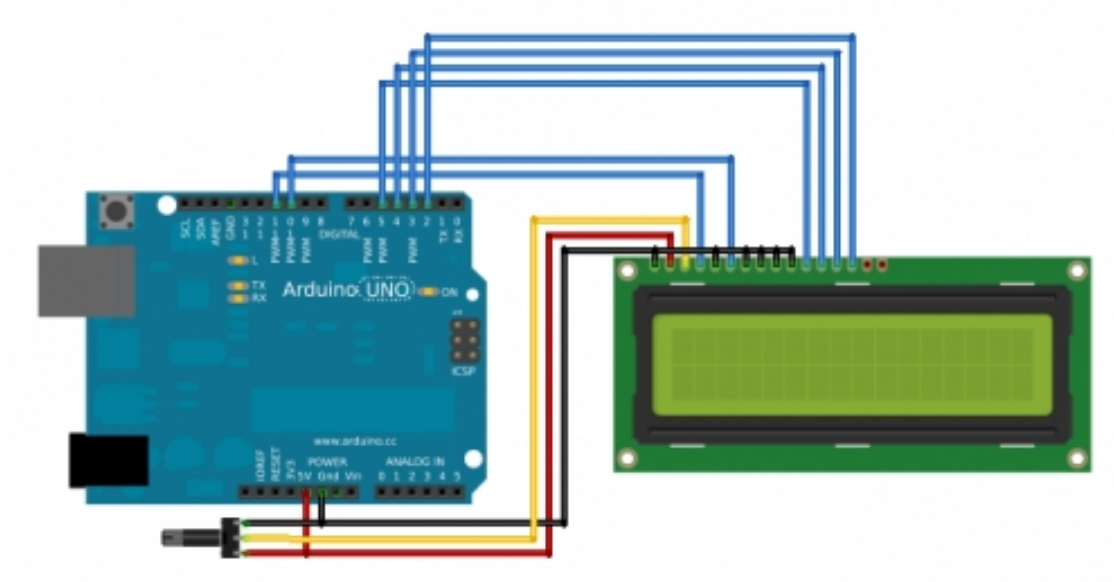

Figure A-1. Représentation du câblage de LCD

Annexe II

1. Le relais et l'Arduino

Une bobine de relais demande un certain ampérage, parfois important. Les sorties Arduino sont données à 40mA maxi, voire 20mA conseillé, donc on ne pilotera pas directement la bobine avec la sortie sous peine de griller notre carte. Il y a deux possibilités, soit nous utilisons une alimentation extérieure pour piloter la carte, soit nous utilisons le pin VIN. Tout dépend de ce que vous voulez faire, si vous avez plusieurs relais, il faudra surement utiliser une alimentation extérieure, si vous en avez un faible nombre, vous pourrez probablement utiliser le pin VIN. Pourquoi probablement, car l'ampérage de VIN n'est pas donné et que l'ampérage nécessaire par les relais se calcule.

L'ampérage de VIN dépend de votre source d'alimentation de la carte. Si vous êtes en USB, vous aurez à disposition de 500mA (limité par votre ordinateur) moins environ 30mA nécessaire au fonctionnement de l'Arduino moins ce que vous pourrez avoir sur les autres sorties. Si vous êtes alimenté via un transformateur, c'est le même calcul en fonction de la puissance de votre transformateur. Si c'est une pile, vérifiez l'ampérage !

Tout ça pour dire que l'on ne pilotera pas directement notre relais. Nous piloterons donc un transistor qui lui-même pilotera le relais. Le transistor agit en quelque sorte comme un relais, mais il consomme beaucoup moins de courant, cependant il ne pourrait pas supporter le 240V.

1.1. Le montage

1.1.1. Le transistor

Comme dit précédemment, nous piloterons le transistor 2N2222 directement avec la sortie Arduino. Nous utiliserons la broche du transistor nommé « Base ». Entre la sortie et le transistor, nous mettrons en série une résistance de 2.2kΩ (R1). La broche nommée « émetteur » du transistor sera mis à la terre et le « collecteur » sera relié au relais.

1.1.2. Le relais

Une des bornes du relais sera reliée au 5V de VIN, l'autre sera donc reliée au collecteur. Une diode sera montée en parallèle de la bobine, cathode montée sur la borne positive.

La diode de roue libre est très importante pour la durée de vie de vos composants. Comme nous l'avons vu précédemment, un relais est composé d'une bobine, autrement appelé inductance en électronique. Lorsque l'on coupe brutalement une inductance, une surtension apparait. La diode de roue libre permet de créer une « boucle infinie » qui permet d'évacuer cette surtension dans la bobine elle-même jusqu'à ce qu'elle disparaisse. Voici comment ça se passe :

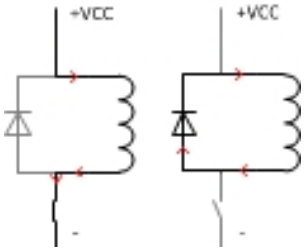

Figure B-1. Schéma diode de roue libre

1.1.3. Le schéma

Maintenant que l'on a bien dissocié toutes les fonctions, voilà le schéma de branchement et de câblage

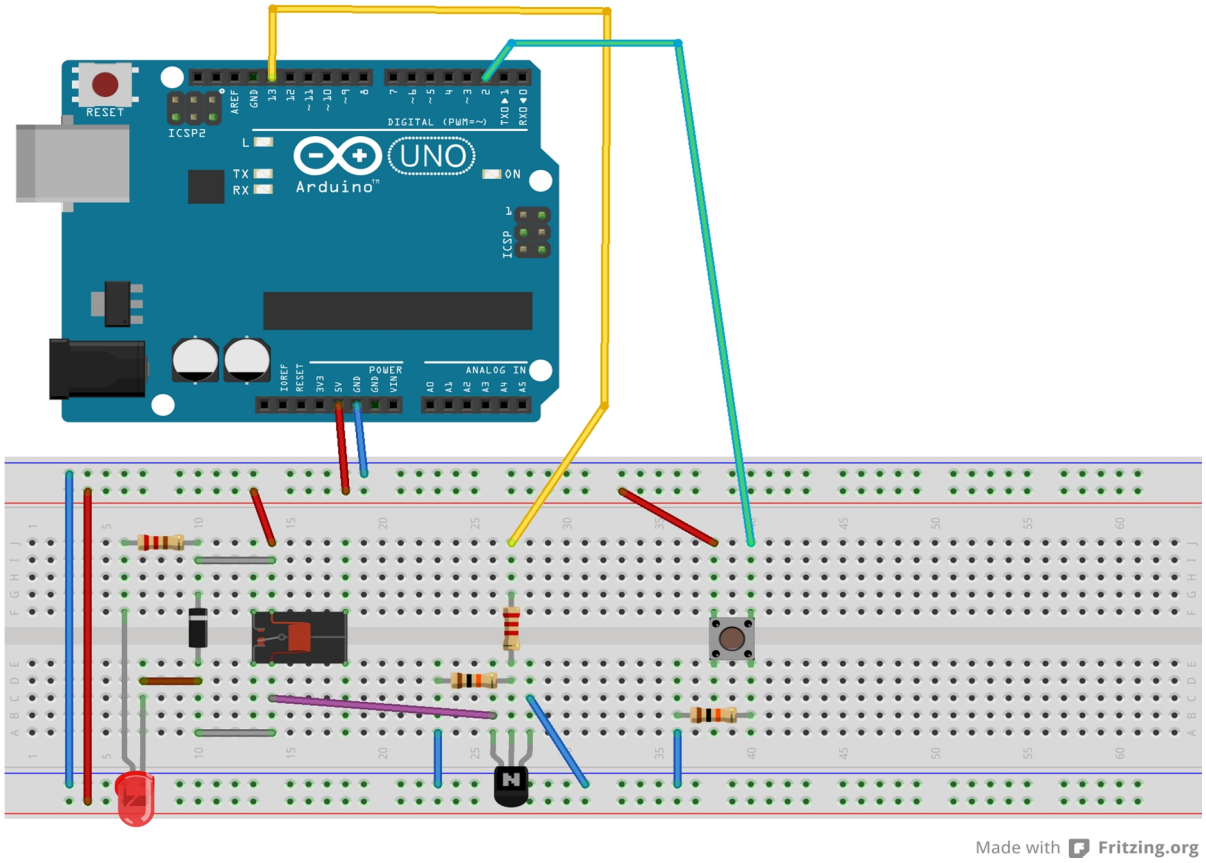

Figure B-2. Représentation de câblage du relais

Annexe III

1. Brochage du régulateur

Les brochages ci-dessous se rapportent au LM338, mais il s'agit du même brochage pour le LM350. Ces composants existent en deux boitiers différents : boitier TO3 (LM338K, c'est celui que vous devez choisir ici), et boitier TO220 (LM338T).

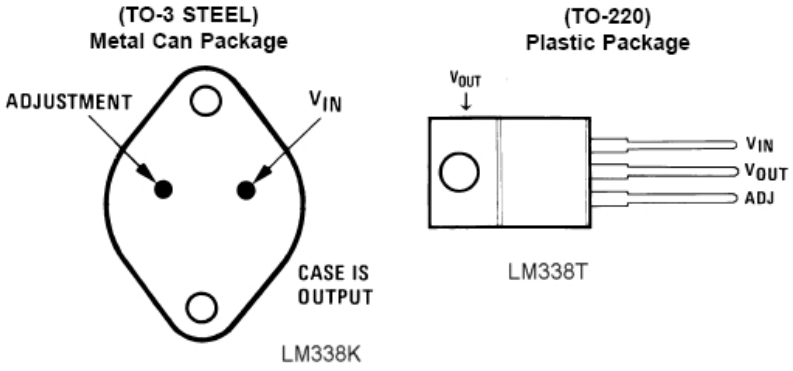

Figure C-1. Brochage du régulateur LM338

Table des figures

Références

[1] Time clock. (2016, Janvier 17). Dans Wikipedia. Page consultée le 20:28, juin 1, 2016 à partir de https://en.wikipedia.org/w/index.php?title=Time_clock&oldid=700325150

[2] Historique de la fabrication et de la commercialisation de pointeuses lambert a saint nicolas d'aliermont. Page consultée le 16:38, Mai 4, 2016 à partir de http://pointeuse.pagesperso-orange.fr/pointeuse_horodateur.htm

[3] Les différents types de pointeuses horaires. Dans Pointeuse-badgeuse. Consulté le 1 Mai 2016 à 16:50, à partir de http://www.pointeuse-badgeuse.be/pointeuses-horaires

[4] Pointeuse mobile. Dans ooreka. Page consultée le 10:25, Mai 2, 2016 à partir de https://pointage.ooreka.fr/comprendre/pointeuse-mobile

[5] Commission techniques de sécurité physique. Techniques de contrôle d'acces par biometrie. Dans clusif. En ligne. Page consultée le 22:36, Février 5, 2016 à partir de https://www.clusif.asso.fr/fr/production/ouvrages/pdf/ControlesAccesBiometrie.pdf

[6] Caractéristiques d'une empreinte digitales et différenciation. Dans La police scientifique. Page consultée le 17:00, Mai 15, 2016 partir de http://la-police-scientifique.e-monsite.com/pages/iii-identifier-le-suspect-grace-aux-empreintes/2-caracteristiques-d-une-empreinte-digitales-et-differenciation.html

[7] Microcontrôleur. (2015, décembre 8). Wikipédia. Page consultée le 03:28, Janvier 8, 2016 à partir de http://fr.wikipedia.org/w/index.php?title=Microcontr%C3%B4leur.

[8] PIC16F887. Microchip. Page consultée le 08:16, Janvier 20, 2016 à partir de http://www.microchip.com/wwwproducts/en/PIC16F887.

[9] 16F877. (2014, décembre 9). Wikipédia. Page consultée le 22:44, Janvier 22, 2016 à partir de http://fr.wikipedia.org/w/index.php?title=16F877&oldid=109800869.

[10] ATmega328. (2016, Mai 21). Wikipédia. Page consultée le 13:40, Janvier 27, 2016 à partir de https://en.wikipedia.org/w/index.php?title=ATmega328&oldid=721415213

[11] Arduino pour bien commencer en électronique et en programmation. (2012, Décembre 02). Par Eskimon et Olyte. Page consultée le 10:20, Janvier 27, 2013 à partir de www.siteduzero.com

[12] LAMP. (2015, mai 14). Wikipédia, l'encyclopédie libre. Page consultée le 21:41, juin 2, 2016 à partir de http://fr.wikipedia.org/w/index.php?title=LAMP&oldid=114990447.

[13] Serveur HTTP Apache 2. Ubuntu-fr. Page consultée le 1:41, Mars 15, 2016 à partir de https://doc.ubuntu-fr.org/apache2.

[14] MySQL. (2016, juin 2). Wikipédia. Page consultée le 11:54, Mai 4, 2016 à partir de http://fr.wikipedia.org/w/index.php?title=MySQL&oldid=126721504.

[15] PHP. (2016, mai 4). Wikipédia, l'encyclopédie libre. Page consultée le 22:10, juin 1, 2016 à partir de http://fr.wikipedia.org/w/index.php?title=PHP&oldid=125878531.

[16] Linux. (2016, mai 29). Wikipédia, l'encyclopédie libre. Page consultée le 21:20, juin 2, 2016 à partir de http://fr.wikipedia.org/w/index.php?title=Linux&oldid=126607018

[17] Ubuntu. (2016, mai 9). Wikipédia, l'encyclopédie libre. Page consultée le 22:23, juin 4, 2016 à partir de http://fr.wikipedia.org/w/index.php?title=Ubuntu&oldid=126019867.

[18] Raspberry Pi. (2016, mai 19). Wikipédia. Page consultée le 12:27, Mars 4, 2016 à partir de http://fr.wikipedia.org/w/index.php?title=Raspberry_Pi&oldid=126303739.