REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie
****
UNIVERSITE DE YAOUNDE I
ECOLE NORMALE SUPERIEUR D'ENSEIGNEMENT TECHNIQUE D'EBOLOWA
DEPARTEMENT DE DE GENIE INFORMATIQUE
****

REPUBLIC OF CAMEROUN
Peace – Work – Fatherland
****
UNIVERSITY OF YAOUNDE I
HIGHER TECHNICAL TEACHER TREAINING COLLEGE OF EBOLOWA
DEPARTMENT OF OF COMPUTER ENGINEERING
****

Filière
Informatique Industrielle

CONCEPTION ET REALISATION D'UN SYSTEME DE CONTRÔLE D'ACCES PAR BIOMETRIE ET RADIOFREQUENCE : CAS DE L'ENSET D'EBOLOWA

Mémoire rédigé et soutenu en vue de l'obtention du Diplôme de Professeur
d'Enseignement Technique deuxième grade (DIPET II)

Par : **ABOMO ESSINDI Jeanne Nadège**

Sous la direction de
Pr. NDJAKOMO ESSIANE Salomé
Maitre de Conférences

Année Académique : 2019 - 2020

DEDICACE

Ce travail est dédié à Madame **veuve ESSINDI née NGONO Christine**

REMERCIEMENTS

Nos remerciements vont à l'endroit de :

- **DIEU TOUT PUISSANT**, pour sa miséricorde, le don de la vie et la santé qu'il nous a donné pour la réalisation de ce travail ;
- Professeur **NDJAKOMO ESSIANE Salomé**, le Directeur de l'ENSET d'Ebolowa et notre encadreur, pour tous les efforts consentis pour la réussite de ces deux années de formation, également pour l'encadrement de ce mémoire ;
- Docteur **OLLE OLLE Georges**, chef de département du génie informatique de l'ENSET d'Ebolowa pour les conseils prodigués tout au long de notre cursus académique à l'ENSET d'Ebolowa ;
- Tout le corps enseignant de l'ENSET d'Ebolowa pour tous les conseils prodigués et enseignements dispensés particulièrement **M. NYATTE STEYVE, M. MEDZO ABA'A Charles** pour leur disponibilité ;
- **Mme Veuve ESSINDI née NGONO Christine**, pour son soutien indéfectible, son amour et tous les efforts consentis pour la réussite de ce travail ;
- **NGONO ELOUNDOU Alehandra Christine Gabrielle et SONGO Anicet,** pour leur amour et leur soutien moral;
- Toute la famille ESSINDI, pour leur soutien moral et financier ;
- **ONDOBO AMVOUNA Marie Vanessa, AWA NYASSA Ophela Barbara, ENKO SIAHEU Marie Linda, DOMENI NJANI Estelle Florentine, NGO BILONG Marie Sorelle épouse NODEM, ELESSA Corinne, NGO BAHIDA Justine Merveille,** pour leur soutien moral ;
- Toutes les personnes qui ont contribué de près ou de loin à la réalisation de cette formation et de ce mémoire en particulier **M. EBA'A Germain Moise, MASSA TOUOYEM Dimitri, NDOH NDOH Yannick Moise** et tous nos camarades promotionnaires.

TABLE DES MATIERES

LISTE DES FIGURES

LISTE DES TABLEAUX

GLOSSAIRE

- **Axone :** est le prolongement du neurone qui conduit le signal électrique du corps cellulaire vers les zones synaptiques ;
- **Balise :** est un émetteur radioélectrique permettant de se diriger ;
- **Champ électrique :** est une force associée à une charge électrique ;
- **Champ magnétique** : est une région de l'espace soumise à l'action d'une force provenant d'un aimant. Il caractérise également l'influence d'une charge électrique en mouvement et exerce, réciproquement, son action sur les charges en mouvement ;
- **Coefficient synaptique :** est un nombre qui, en multipliant les différentes valeurs des signaux reçus à l'entrée d'un neurone artificiel, sert à calculer la valeur du signal émis à la sortie ;
- **Degré d'unicité :** est la mesure d'un angle ;
- **Dentrites :** est un prolongement ramifié du neurone ;
- **Diode électroluminescente :** est un dispositif opto-électronique capable d'émettre de la lumière lorsqu'il est parcouru par un courant électrique ;
- **Gradient :** est un vecteur qui caractérise la variabilité d'une fonction au voisinage d'un point ;
- **Infrarouge** : est un rayonnement électromagnétique de longueur d'onde supérieure à celle du spectre visible mais plus courte que celle des micro-ondes **;**
- **Infrarouge :** est un rayonnement électromagnétique de même nature que la lumière visible ;
- **Logique floue :** est une branche des mathématiques qui possède des règles et des principes (valeurs de vérité des variables au lieu d'être vraies ou fausses sont des réels entre 0 et 1) ;
- **Méthode connexionniste :** est liée aux phénomènes mentaux et comportementaux ;
- **Middleware :** est un logiciel tiers qui créé un réseau d'échange d'informations entre différentes applications informatiques ;
- **Neurone :** encore appelé cellule nerveuse, est une cellule excitable constituant l'unité fonctionnelle de la base du système nerveux ;

- **Onde électromagnétique :** est le résultat de la vibration couplée d'un champ électrique et d'un champ magnétique variables dans le temps ;
- **Onde radio :** est la propagation électromagnétique d'une perturbation produisant sur son passage une variation réversible des propriétés physiques locales du milieu dont la fréquence est inférieure à 300GHz ;
- **Quantification vectorielle :** est une technique de quantification (action d'attribuer une valeur à un phénomène mesurable) souvent utilisée dans la compression de données avec pertes de données ;
- **Quartz :** est un minéral constitué de silice cristallisée et présent à l'état pur ;
- **Rayonnement électromagnétique** : est l'ensemble des radiations émises par une source qui peut être soit le soleil, soit la surface terrestre ou océanique ou l'atmosphère, ou bien encore le capteur satellitaire lui-même, sous forme d'ondes électromagnétiques ou de particules ;
- **Réseau de neurone :** est un système dont la conception est à l'origine schématiquement inspirée du fonctionnement des neurones biologiques, et qui par la suite s'est rapproché des méthodes statistiques ;
- **Réseau neuromimétique :** est un graphe de neurones interconnectés fondé sur un modèle formel de neurone ;
- **Rétro modulation :** est le passage d'une tonalité à une autre vers l'arrière ;
- **Rétro propagation :** est la réémission du signal par le lecteur, diffusé par l'étiquette après modulation, en direction de l'environnement ;
- **Rétrodiffusion :** est un phénomène par lequel un rayonnement comme la lumière, le son ou un faisceau de particules est réparti uniformément dans toutes les directions vers l'arrière ;
- **Robotique :** est l'ensemble des techniques permettant la conception et la réalisation de machines automatiques ou de robots ;
- **Synapse :** est une zone de contact fonctionnelle qui s'établit entre deux neurones, ou entre un neurone et une autre cellule (cellules musculaires, récepteurs sensoriels) ;
- **Transpondeur :** est un dispositif qui émet automatiquement un signal en réponse à un autre signal qu'il reçoit d'un appareil de radionavigation situé à distance.

LISTE DES SIGLES

- **ACP :** Atrophie Corticale Postérieure ;
- **AREF :** Arduino Reference ;
- **COM** : Communication ;
- **EEPROM :** Electrically Erasable Programmable Read-Only Memory ;
- **ENSET :** Ecole Normale Supérieure d'Enseignement Technique d'Ebolowa ;
- **FBI** : Federal Bureau of Investigation ;
- **Ghz** : Giga Hertz ;
- **GND** : Ground ;
- **HF : Haute Fréquence ;**
- **I2C** : Inter Integrated Circuit ;
- **ICSP :** In circuit Serial Programming ;
- **IDE :** Integrated Development Environment ;
- **ISM2 :** Mini Single Instrumental Set ;
- **ISO :** Internationl Organization for Standardisation ;
- **LED :** Light Emitting Diode ;
- **LF :** Large Fréquence ;
- **Mhz** : Mega Hertz ;
- **MISO :** Master In Slave Out ;
- **MLP :** MultiLayer Perceptron ;
- **Mm :** Millimètre ;
- **MOSI :** Master Out Slave In ;
- **NFC :** Near Field Communication ;
- **Nm** : Nanomètre ;
- **PWM :** Pulse Width Modulation ;
- **RC522 :** Read Card 522 ;
- **RF :** RadioFréquency ;
- **RFID :** RadioFrquency Identification ;
- **ROC :** Receiver Operating Characteristic ;
- **RTLS** : Real Time Localisation System ;

- **SCK :** Serial Clock ;
- **SDA :** Shield Data ;
- **SPI :** Serial Peripheral Interface ;
- **TBF** : Très Basse Fréquence ;
- **TTL :** Transistor Transistor Logic ;
- **TXT :** Comma-Separated Values ;
- **Txt :** Texte ;
- **UART :** Universal Asynchronous Receiver Transmitter ;
- **UHF :** Ultra Haute Fréquence ;
- **VCC :** Voltage Common Collector.

AVANT-PROPOS

L'Ecole Normale Supérieure d'Enseignement Technique (ENSET), créé par Décret Présidentiel N°2017/586 du 24 Novembre 2017, est un établissement d'Enseignement Supérieur relevant de l'Université de Yaoundé I. Il est situé au campus de Metykpwale dans la ville d'Ebolowa et abrite un bloc administratif, des salles de classes, un restaurant et bien d'autres.

L'ENSET d'Ebolowa a pour mission d'assurer :

- La formation des enseignants de l'Enseignement Secondaire Technique et des Conseillers d'Orientation Scolaire, Universitaire et Professionnelle ;
- La promotion de la recherche scientifique, technologique et pédagogique, ainsi que la valorisation des résultats de la recherche dans son implémentation ;
- L'appui au développement ;
- Le recyclage et le perfectionnement du personnel de l'Enseignement Secondaire Technique, des professionnels dans ses domaines de formation.

Dans le but de perfectionner la formation des futurs enseignants, il est prévu la rédaction d'un mémoire portant sur un projet réalisable d'où l'importance de ce travail portant sur le thème : **« Conception et réalisation d'un système de contrôle d'accès par biométrie et radiofréquence au sein du campus de cette école »**.

RESUME

Depuis plusieurs années au Cameroun, de nombreuses écoles (publiques et privées) sont créées dans le but d'assurer la formation des citoyens camerounais capables de mettre à profit leurs connaissances acquises ainsi que leurs compétences sur le marché de l'emploi. C'est ainsi que dans le cadre de la création des écoles normales au Cameroun, l'ENSET d'Ebolowa voit le jour le 24 Novembre 2017 et est à sa troisième année d'existence et de formation de futurs enseignants. Nous observons sans doute un nombre croissant de personnes pouvant s'y rendre et ayant accès au bâtiment de ladite école. De ce constat, découlent l'insécurité au sein du campus et des mouvements de va et vient qui ne sont pas toujours contrôlés. Au regard des observations susmentionnées, nous concevons un système embarqué de contrôle d'accès combiné biométrie et radiofréquence basé sur les réseaux de neurones artificiels (PMC) utilisant l'algorithme de rétro propagation du gradient. L'objectif est d'automatiser la gestion des entrées et sorties du personnel et des visiteurs au sein du campus de l'ENSET d'Ebolowa. De ce fait, nous avons travaillé avec une base de données de dix empreintes et quatre cartes RFID pour gérer l'identification et l'authentification. Afin de rendre notre système efficace et robuste, nous utilisons le PMC pour l'extraction des caractéristiques singulières (core et delta) et l'entraînement d'une empreinte ; la technologie RFID quant à elle est basée sur le couplage magnétique en champ proche utilisant une fréquence de 13,56Mhz. Des simulations sont faites grâce aux logiciels Matlab et Rsutdio pour l'utilisation du RNA afin de prédire l'une des classes d'empreintes digitales qui existent (Arc, Arc tendu, Spire, Boucle à gauche et Boucle à droite). L'apprentissage ayant été acquis, l'intégration du PMC a été faite dans l'IDE Arduino pour le fonctionnement du système dans le microcontrôleur Arduino mega2560 avec des informations qui sont sauvegardées dans un fichier au format txt pour gérer la traçabilité.

Mots clés : Contrôle d'accès – réseaux de neurones artificiels– biométrie – empreinte digitale – RFID – algorithme de rétro propagation du gradient- PMC

ABSTRACT

For several years in Cameroon, many schools (public and private) have been created in order to provide training for Cameroonian citizens capable of using their acquired knowledge and their skills on the job market. Thus as part of the creation of teacher training colleges in Cameroon, the ENSET of Ebolowa was born on November 24th, 2017 and is in its third year of existence and training of future teachers. We are probably seeing an increasing number of people who can get there and have access to the school building. From this observation, arise insecurity on campus and back and forth movements which are not always controlled. In view of the above observations, we design an on-board biometric and radio frequency access control system based on artificial neural networks (MLP) using the gradient back propagation algorithm. The objective is to automate the management of staff and visitor entry and exit within the ENSET campus of Ebolowa. As a result, we worked with a database of ten fingerprints and four RFID cards to manage identification and authentication. In order to make our system efficient and robust, we use PMC for the extraction of singular characteristics (core and delta) and the training of an imprint; RFID technology is based on near field magnetic coupling using a frequency of 13.56 MHz. Simulations are made using Matlab and Rsutdio software for the use of RNA in order to predict one of the classes of fingerprints that exist (Arc, Stretch Arc, Spire, Loop to the left and Loop to the right). The learning having been acquired, the integration of the MLP was made in the Arduino IDE for the operation of the system in the Arduino mega2560 microcontroller with information which is saved in a file in txt format to manage traceability.

Keywords: **Access control - artificial neural networks - biometry - fingerprint - RFID - gradient back propagation algorithm - MLP**

INTRODUCTION GENERALE

Dans le cadre des lancements des concours d'intégration dans la fonction publique depuis les années 60, de nombreuses écoles normales pour la formation des Professeurs de Lycées d'enseignement général et technique ont été créées à l'instar de l'ENSET d'Ebolowa depuis le 24 Novembre 2017, objet de ce travail. C'est ainsi que, depuis trois ans, nous pouvons observer un nombre sans cesse croissant de personnes accédant au bâtiment de ladite école dont les étudiants, le corps administratif, le corps enseignant et les visiteurs. Fort de ce constat et partant de la sécurisation de ce campus, est né un besoin d'identification des différents usagers qui y accèdent. L'identification faisant partie du domaine du contrôle d'accès, consiste à vérifier si une personne demandant accès au bâtiment a les droits nécessaires pour le faire. Les protocoles de vérification d'identité répondent à deux questions fondamentales : Qui suis-je ? Suis-je réellement la personne autorisée à y accéder ?

Ce travail s'inscrit dans une perspective de modernisation technologique de l'ENSET d'Ebolowa qui jusqu'ici fait face à plusieurs manquements concernant la gestion des mouvements de ses différents usagers et la sécurisation du bâtiment proprement dit.

Au rang des insuffisances qui retiennent notre attention dans le cadre de ce travail, nous avons entre autres : la non assiduité, le retard, les entrées et sorties non contrôlées, les enregistrements frauduleux des présences et heures d'arrivée et de départ sur les fiches manuelles et cahier de texte prévus à cet effet, entraînant : une rémunération aléatoire du personnel administratif et des enseignants ; des enseignements biaisés suite au retard considérable de certains enseignants voire même leur absence ; les interruptions de travail du personnel suite aux allées et venues non règlementées des visiteurs dans les bureaux administratifs. Les précédents constats nous interpellent sur la gestion efficace des mouvements des différents usagers au sein du campus de l'ENSET d'Ebolowa.

L'objectif général de ce travail est l'automatisation de la gestion des accès (entrée/sortie) du personnel administratif (permanent et temporaire), du corps enseignant et des visiteurs. Les objectifs spécifiques étant : l'identification/authentification par biométrie (empreinte digitale) et par radiofréquence utilisant la méthode des réseaux de neurones artificiels et l'algorithme de

rétro propagation du gradient pour le traitement des empreintes ; la commande automatique des portes ; la sauvegarde et la visualisation des informations d'identification/authentification pour une meilleure traçabilité ; la gestion des tentatives d'intrusion pour assurer la sécurité au sein du campus.

Plusieurs questions de recherche ont été envisagées dans le but de mieux élucider ce travail et pallier aux manquements susmentionnés : Quels sont les outils nécessaires à la conception d'un système de contrôle d'accès par biométrie et radiofréquence à l'ENSET d'Ebolowa ? Quel mécanisme opérant et crédible peut-il garantir le fonctionnement d'un tel système ? Quel peut être l'impact d'une telle innovation sur les mouvements et la sécurisation des usagers à l'ENSET d'Ebolowa ?

Dans le dessein de mieux comprendre la quintessence de ce travail, notre mémoire sera structuré en trois chapitres dont le premier portera sur les généralités des systèmes de contrôle d'accès par biométrie et radiofréquence ainsi que sur les travaux liés au même domaine en présentant la méthode des réseaux de neurones artificiels et l'algorithme de rétro propagation du gradient. Dans le second, nous présenterons une méthodologie de conception du système proposé en présentant le cahier de charges, les outils nécessaires et la méthode de conception. Dans le troisième, nous ferons une simulation tout en interprétant les résultats.

CHAPITRE I : GENERALITES SUR LES SYSTEMES DE CONTROLE D'ACCES

Ce chapitre porte sur les différents articles que nous avons parcourus et qui sont liés au domaine du contrôle d'accès par les technologies biométrique et RFID.

Aperçu

Introduction

I- La biométrie et la technologie RFID

II-Quelques travaux effectués dans le contrôle d'accès

Conclusion

Introduction

Les systèmes de contrôle d'accès ont connu une grande évolution dans le temps et de ce fait sont nées plusieurs technologies notamment la biométrie et la RFID qui font l'objet de ce travail. La revue de la littérature désigne une méthode de travail scientifique dont l'objectif principal est de résumer l'état de l'art dans un domaine bien précis comportant de nombreuses références, c'est ainsi que nous présenterons dans ce chapitre les deux technologies liées à notre thème ainsi que les différents travaux qui y ont été effectués sans oublier l'application de l'intelligence artificielle au système de contrôle d'accès ainsi que notre apport pour l'avancée technologique.

I. La biométrie et la technologie RFID

1. La biométrie

Le mot français biométrie est définit comme étant l'étude mathématique des variations biologiques à l'intérieur d'un groupe déterminé. C'est une notion qui fait référence à de nombreux domaines d'application. En effet, on l'utilise en médecine depuis des siècles pour en étudier les dimensions et la croissance des êtres vivants. Elle est également une application des méthodes statistiques à la biologie. La biométrie est aussi intimement liée à l'anthropométrie (science qui a pour objet les mensurations du corps humain) ; couplée à l'informatique, elle engendre une reconnaissance automatisée des identités et en faciliterait ainsi grandement le traitement. C'est ainsi que, dans le cadre de ce mémoire, nous l'étudions dans le sens d'une science dont l'objectif vise à reconnaître l'identité d'une personne afin de lui donner l'accès à une zone bien déterminée.

De nos jours, nous distinguons plusieurs techniques biométriques de reconnaissance d'individu qui sont classées en 2 grandes catégories à savoir : les techniques comportementales et les techniques morphologiques. La première consiste à observer et analyser le comportement des individus dans des actions répétitives et usuelles tandis que la seconde (ou physiologique) s'attache à quantifier les caractéristiques corporelles.

1.1 Les techniques morphologiques

- **L'empreinte digitale** : la reconnaissance biométrique des empreintes digitales s'effectue depuis presque un siècle dans les domaines pénal et criminel. D'ailleurs, c'est en 1924 que le FBI (Federal Bureau of Investigation) a débuté la collecte et l'analyse des empreintes pour l'identification. Auparavant manuelle, la façon de traiter les empreintes s'est automatisée depuis le développement des nouvelles technologies. La fiabilité de la reconnaissance des empreintes est considérée comme supérieure, et celle-ci sera augmentée en fonction du nombre de doigts soumis à l'évaluation. Les empreintes digitales sont généralement considérées comme étant assez intrusives (accédant aux informations sans autorisation) sur le plan de la vie privée car, elles sont associées à l'identification criminelle [1] ;
- **La géométrie de la main** : les systèmes automatisés d'authentification basés sur la géométrie de la main sont toutefois les premiers à avoir été réalisés et brevetés dès 1971[3]. Cette technique a connu une grande évolution, notamment en exploitant le profil 3D (3ème Dimension) de la main [4]. Les caractéristiques géométriques de la main sont généralement obtenues à partir des longueurs et largeurs des doigts, ainsi que la largeur et l'épaisseur de la main. Il est important de souligner que le degré d'unicité de la géométrie de la main serait relativement faible, puisqu'il pourrait exister des similarités entre les mains de différents individus ; elle est de ce fait recommandée pour l'authentification uniquement. Parmi ses autres faiblesses, nous notons l'hygiène de la main afin de ne pas nuire à la captation de l'image. Par contre, ce système résisterait à la fraude car il serait impossible de soumettre une paume de main artificielle. A titre d'exemple d'utilisation de la géométrie de la main, nous avons en 2001, le CEPSUM (Centre d'Education Physique de l'Université de Montréal) qui a mis en place un système de reconnaissance de la morphologie de la main pour l'accès à ses installations sportives. Depuis ce temps, les étudiants peuvent accéder au CEPSUM en soumettant leurs données tridimensionnelles de la main droite. Celles-ci sont saisies et comparées à celles enregistrées dans le dossier lors de l'enrôlement [2] ;
- **Les veines de la main** : en 1991, MacGregor et Welford ont eu l'idée d'utiliser le réseau vasculaire sous-cutané de la partie supérieure de la main pour la biométrie [5]. 2ans et 3ans plu tard, un prototype faible coût a été développé par Cross et Smith [6]. L'utilisation d'images thermographiques (spectre proche infrarouge : 700–1400 nm)

naît du fait que la structure veineuse de la main est difficilement discernable en lumière visible. Le traitement de reconnaissance consiste donc à segmenter l'image thermographique afin d'extraire les motifs formés par les veines. Un prétraitement par interpolation bilinéaire (qui permet de calculer la valeur d'une fonction en un point quelconque, à partir de ses deux plus proches voisins dans chaque direction) peut être envisagé pour améliorer la qualité du squelette veineux. L'étape de comparaison est réalisée par une corrélation séquentielle sous contraintes ;

- **Le visage** : il peut être défini comme étant une partie du corps humain recouverte des yeux, du nez, de la bouche, des sourcils, des cils, des pommettes. De ce fait, un être humain qui possède une grande capacité de reconnaissance des visages peut authentifier sans hésitations en moyenne 700 visages de personnes différentes [7]. Pour décrire un visage, la tendance consiste à utiliser des caractéristiques dites de haut niveau telles que la couleur des cheveux et des yeux, le profil du nez, leur position relative. Entre 1966 et 1971, les premiers travaux portant sur les systèmes automatiques de traitements de visages s'appuyaient sur l'approche géométrique, généralement moins coûteuse en calcul et en place mémoire que l'approche globale. Cette dernière apparut seulement dès 1977 avec les recherches de Kohonen [8] qui proposaient un modèle neuronal connexionniste (est une catégorie du système nerveux liée aux phénomènes mentaux ou comportementaux) pour la classification d'images de visages. Pour lui, les visages sont soit directement représentés par l'intensité de chaque pixel, soit l'information brute subit une compression à savoir, le redimensionnement par sous-échantillonnage, les visages propres (Eigenfaces), les réponses des cellules de la couche cachée d'un réseau à rétro propagation (réémission du signal émis par le lecteur, diffusé par l'étiquette après modulation, en direction de l'environnement) ou encore réponse de filtres. On note aussi une technologie avancée de représentation des visages qui vise à les modéliser par leur relief à partir d'un maillage 3D traditionnel ou triangulaire pour en simplifier la complexité et améliorer ainsi la compacité des modèles. La tâche de reconnaissance proprement dite repose généralement sur une mesure probabiliste de similarité basée sur la théorie Bayesienne. De récentes recherches, ont montré que l'utilisation d'une caméra thermique infrarouge (acquisition de thermo grammes du visage) permettait d'améliorer sensiblement les performances ;
- **La rétine** : chaque individu possède des motifs de vaisseaux sanguins au fond de l'œil qui lui sont propres. La découverte de cette technologie date des années 30 [9] et peu de

solutions exploitent aujourd'hui cette technologie du fait qu'elle nécessite un système d'acquisition relativement intrusif car, plus précise de toutes les technologies biométriques mais très coûteuse, difficile à utiliser et disposant d'un faible taux d'acceptation. À partir d'une image en niveaux de gris obtenue par réflexion d'une lumière artificielle infrarouge sur la rétine, le réseau vasculaire est alors extrait par segmentation [10] et analysé par une méthodologie comparable à l'empreinte digitale. La reconnaissance de la rétine permet d'observer les ramifications vasculaires qui tapissent le fond de l'œil (surface interne antérieure). Le capteur enregistre la disposition des veines dans l'œil en balayant la rétine à l'aide d'un faisceau lumineux dans le globe oculaire. En outre, le réseau veineux de l'œil peut se modifier légèrement en raison d'une forte alcoolémie ou du diabète ;

- **L'iris** : c'est le muscle coloré à l'intérieur de l'œil, visible à travers la cornée, placé devant le cristallin et percé en son centre de la pupille. Il s'agit d'un réseau de tubes fins dont le diamètre est inférieur à celui d'un cheveu. En 1936, l'ophtalmologiste Frank Burch met sur pieds l'utilisation de l'iris comme moyen d'identification. De nos jours, plusieurs aéroports dans le monde à l'instar de ceux du Canada, du Japon, des Pays-Bas utilisent l'iris comme systèmes de reconnaissance. Ce système fonctionne de telle sorte qu'une caméra parcourt l'œil à l'aide d'une lumière infrarouge et capture une image, afin de mesurer plusieurs caractéristiques telles que le relief, les anneaux, les sillons et la texture de l'iris. Étant donné son caractère stable et très unique, la reconnaissance de l'iris est reconnue pour sa fiabilité très élevée, le système est d'ailleurs à l'épreuve des lunettes, des verres de contacts et des fluctuations de la taille de la pupille et peut observer près de 200 points de comparaison. Sa fiabilité est due en partie à la quasi-impossibilité de le reproduire artificiellement. Toutefois, le succès du système dépendra de la qualité de l'image saisie par la caméra digitale, de la même manière que pour la rétine. Il découle de la précision de ce système un faible taux d'acceptation et son coût très élevé. Le NSTCSB (National Science and Technology Council Subcommitee on Biometrics) est plutôt d'avis que la lumière infrarouge ne serait pas assez puissante pour causer des dommages photochimiques à l'œil. Néanmoins, il semblerait qu'un dommage thermal puisse être possible pour la cornée et l'humeur aqueuse, découlant des diodes électroluminescentes émises par le rayon infrarouge si la technologie employée n'est pas utilisée correctement.

1.2 Les techniques comportementales

- **Dynamique de frappe au clavier** : R. GAINES, W. LISOWSKI furent les premiers à étudier en 1980 cette forme de biométrie. Il faudra près de dix ans pour que leurs investigations soient approfondies et qu'apparaissent les premiers systèmes automatisés de reconnaissance de dynamique de frappe au clavier. Les contributions majeures ont notamment évalué la logique floue (est une approche informatique basée sur des degrés de vérité plutôt que sur la logique booléenne habituelle sur laquelle repose l'informatique moderne), les réseaux de neurones et, ainsi que différentes techniques de reconnaissance de motifs telles que le classificateur de Bayes. La séquence de frappe, prédéterminée sous la forme d'un mot de passe ne permet qu'une vérification statique. Les différents paramètres liés à la frappe sont : la vitesse de frappe, la mesure des temps de frappe, les pauses entre chaque mot, la reconnaissance du mot précis, la pression exercée sur les touches ;
- **La signature** : la reconnaissance de signature d'un individu peut être accomplie en analysant un grand nombre de variables discriminatives à savoir : les caractéristiques globales telles que le temps d'écriture ou le nombre de touches sur la tablette avec le stylo, et/ou les caractéristiques locales telles que la position de certaines courbures ou la vitesse instantanée. L'acquisition s'effectue habituellement par un lecteur en forme de crayon sensible à la pression et une tablette à digitaliser. Les techniques de comparaison les plus connues utilisent un modèle de Markov caché ou une approche par programmation dynamique. La plus importante contribution en vérification de signature manuscrite est celle émanant depuis plus de vingt ans de la communauté de recherche IGS (International Graphonomic Society), et plus particulièrement de l'équipe Scribens ;
- **Mouvement des lèvres** : depuis la fin des années 90, les nombreuses recherches visant à exploiter les informations visuelles traduisant les gestes articulatoires du locuteur tel que le mouvement des lèvres témoignent d'une forte activité dans ce domaine. Les attributs utilisés se regroupent en deux grandes catégories : globale (holistique) et locale (spécifique). Généralement l'approche s'appuyant sur des caractéristiques globales est sensible aux conditions d'illumination, à l'angle de vue, ainsi qu'à l'orientation de la bouche. La complexité algorithmique des méthodes d'extraction de caractéristiques globales rend difficile le suivi en temps réel des mouvements des lèvres. Parmi les

méthodes les plus connues, on distingue 4 techniques : la décomposition multi-échelles par transformée en ondelettes (petites oscillations) ou par l'utilisation de filtres morphologiques non-linéaires, le calcul du flot optique moyen dans 4 régions autour de la bouche, l'analyse en composantes principales et la quantification vectorielle. L'approche s'appuyant sur des caractéristiques locales vise plutôt à obtenir une description paramétrée des contours des lèvres. Cette dernière approche est généralement préférée à celle globale du fait que l'information extraite de la bouche du locuteur est à la fois de plus faible dimension et plus facilement interprétable, même si les étapes de localisation des lèvres exigent une grande précision. Enfin, certains travaux optent pour une approche mixte apparence (globale et locale) : l'approche modèle est utilisée pour repérer les lèvres, et une fois le(s) contour(s) localisé(s), une information plus ou moins directement dérivée des valeurs des niveaux de gris (ou couleur) des pixels est extraite ;

- **Reconnaissance vocale** : depuis le début du 20ème siècle, cet intérêt pour la reconnaissance de l'identité d'un locuteur par sa voix n'a jamais cessé de se développer. La plupart des systèmes actuels utilisent des paramètres directement empruntés à la technologie de reconnaissance de la parole. Ces systèmes restent donc encore extrêmement sensibles aux changements transitoires de la voix du locuteur liés à des modifications provisoires de son état interne (fatigue, émotion, santé), en particulier, les modifications de propriétés vocales associées aux légères mais fréquentes variations de l'état émotionnel du locuteur (irritation, stress, satisfaction). On distingue les systèmes dépendants et indépendants du texte. En mode dépendant, le texte prononcé par le locuteur (pour être reconnu du système) est le même que celui qu'il a prononcé lors de l'apprentissage de sa voix. En mode indépendant du texte, le locuteur peut prononcer n'importe quelle phrase pour être reconnu. Il existe néanmoins plusieurs niveaux de dépendance au texte suivant les applications : texte libre, texte suggéré, traits phonétiques imposés dans le texte, vocabulaire limité, texte personnalisé. Les systèmes dépendants donnent généralement de meilleures performances de reconnaissance que les systèmes indépendants car la variabilité due au contenu linguistique de la phrase prononcée est alors neutralisée. Les principales méthodes qui permettent de mesurer les variabilités interlocuteurs qui proviennent des différences physiologiques (dimensions du conduit vocal, fréquence d'oscillation des cordes vocales) et de style de prononciation (accent, niveau social) sont : les méthodes algébriques qui reposent sur

des statistiques à long terme, les méthodes connexionnistes ou encore les méthodes basées sur une modélisation spécifique suivant la classe acoustique des paramètres. Afin de réduire les distorsions engendrées par le bruit ambiant et le vieillissement des modèles des locuteurs mémorisés lors de l'apprentissage, l'emploi de microphones directionnels et d'approche multi-bandes (ou multi-classificateurs) est aujourd'hui fréquente.

Ci-dessous, les différentes images liées aux techniques biométriques suscitées :

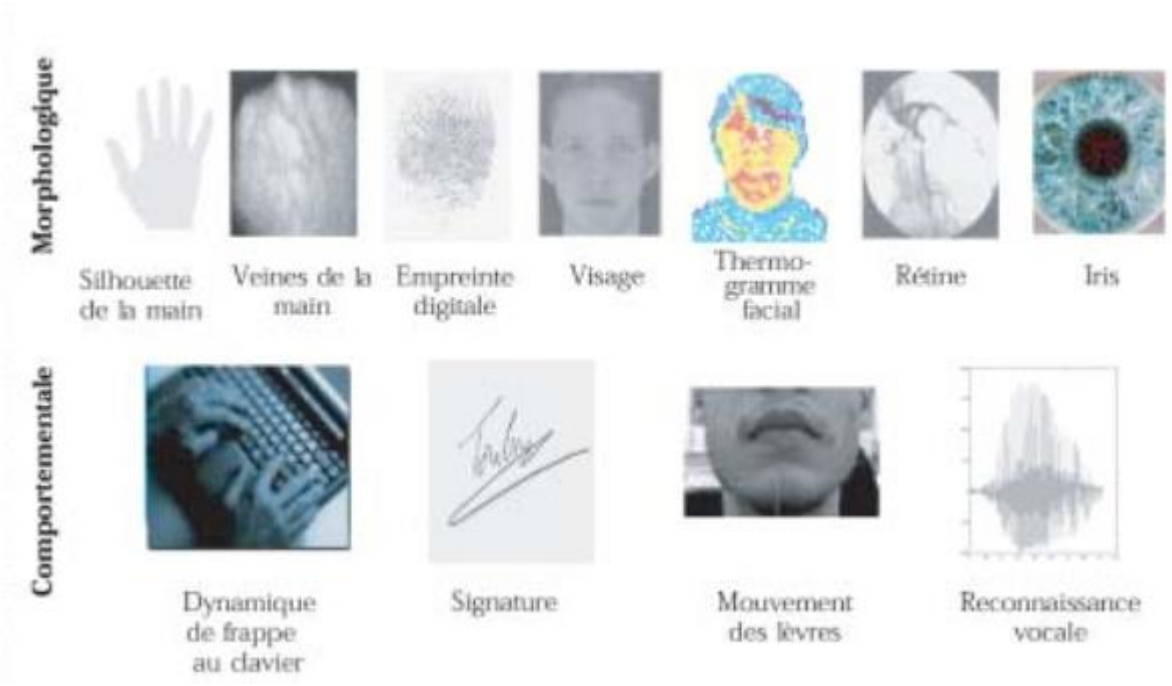


Figure I.1 : Images correspondant aux différentes techniques biométriques [13]

Remarque : Les raisons du choix de la technique biométrique par empreinte digitale pour notre étude sont regroupées dans les tableaux ci-dessous :

Tableau N°I.1 : Avantages et limites des techniques biométriques [16]

Techniques	Avantages	Inconvénients
Empreintes digitales	Coût, facilité de mise en place, taille du capteur réduite, fiabilité	Acceptabilité moyenne, possibilité d'attaques
Géométrie de la main de la main	Bonne acceptabilité	Système encombrant, coût, caractère non discriminant par rapport aux membres de la même famille
Visage	Coût, peu encombrant, bonne acceptabilité, authentification à distance	Problème des jumeaux, sensibilité au déguisement
Rétine	Fiabilité, pérennité	Coût, acceptabilité faible, installation difficile
Iris	Fiabilité	Acceptabilité faible
Voix	Fiabilité moyenne	Vulnérabilité aux attaques
Signature	Ergonomie	Dépendant de l'état d'émotion de la personne, problème de fiabilité
Dynamique de frappe au clavier	Ergonomie, ne nécessite pas de capteur	Dépendant de l'état physique de la personne

Tableau N°I.2 : Classification des techniques biométriques [13]

Biométrie	Universalité	Unicité	Permanence	Mesurabilité	Performance	Acceptabilité	Vulnérabilité
Empreintes digitales	Moyenne	Haute	Haute	Moyenne	Haute	Moyenne	Moyenne
Géométrie de la main de la main	Moyenne	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Moyenne
Visage	Haute	Faible	Moyenne	Haute	Faible	Haute	Haute
Rétine	Haute	Haute	Moyenne	Faible	Haute	Faible	Faible
Iris	Haute	Haute	Haute	Moyenne	Haute	Faible	Faible
Voix	Moyenne	Faible	Faible	Moyenne	Faible	Haute	Haute
Signature	Faible	Faible	Faible	Haute	Faible	Haute	Haute
Dynamique de frappe au clavier	Faible	Faible	Faible	Moyenne	Faible	Moyenne	Moyenne

<u>Remarque</u> : Quelques champs d'application de la biométrie

L'authentification par la biométrie est utilisée dans tous les domaines nécessitant un accès contrôlé tels que celui des institutions académiques, des applications bancaires, les endroits hautement sécurisés comme les sièges du gouvernement, parlement, armée, service de sécurité.

2. La biométrie par empreinte digitale

2.1 Description et principe de fonctionnement

- **<u>Description</u>**

Cette technique, comparativement aux autres technologies, comme indiqué dans le tableau N°I.1, se distingue comme étant une modalité bien approuvée techniquement car, pas très coûteuse et parmi les plus fiables en terme d'erreur à la reconnaissance. Une empreinte digitale est le dessin formé par les lignes de la peau des doigts. Ces lignes sont uniques et immuables (qui reste identiques, ne changent pas), elles ne se modifient donc pas au cours du temps (sauf par accident) mis à part leur qualité qui peut se dégrader. On distingue les crêtes, qui sont des lignes en contact avec une surface au touché ; et les vallées qui sont les creux entre deux crêtes.

A l'intérieur de ce motif, il y a un très grand nombre d'éléments qui nous différencient les uns des autres. Ces caractéristiques sont formées par le flux des crêtes formant l'empreinte. La figure ci-dessous illustre quelques caractéristiques d'une empreinte digitale :

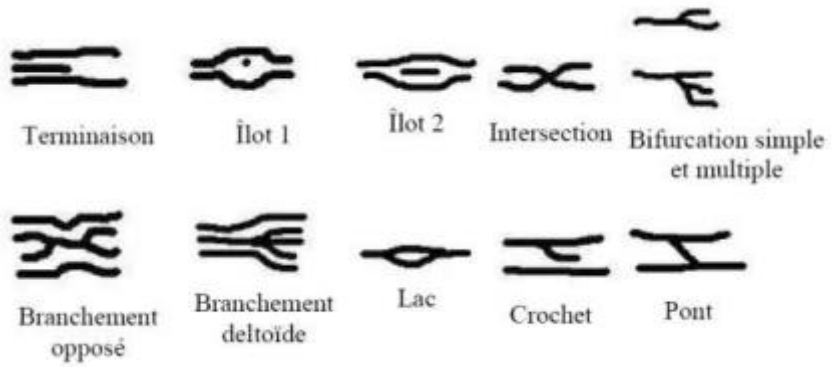


Figure I.2 : Quelques caractéristiques d'une empreinte digitale [22]

Ces éléments sont à leur tour découpés en deux familles : les minuties et les singularités. La minutie est l'arrangement particulier des lignes papillaires (crêtes et vallées) à l'origine de l'individualité des empreintes. Les minuties peuvent être de différents types comme le montre la figure I.3, mais en pratique, seulement deux types sont utilisés à savoir : les terminaisons (le point où la crête se termine) et les bifurcations (carrefour de plusieurs crêtes). Cela s'explique par le fait que les autres types sont des combinaisons de terminaisons et de bifurcations. Il existe deux points de singularités (voir figure I.4) : le core et le delta. Le delta est localisé à la confluence de trois différentes crêtes tandis que le core est le point de courbure maximale. Selon le motif (le nombre et la localisation des points delta et core), nous pouvons répertorier cinq classes d'empreintes digitales comme le montre la figure I.5 :

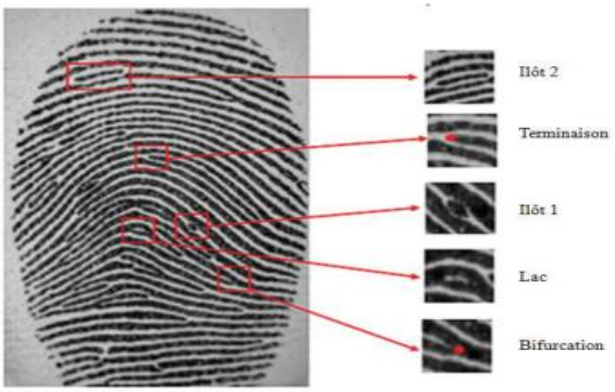


Figure I.3 : Différents types de minuties [13]

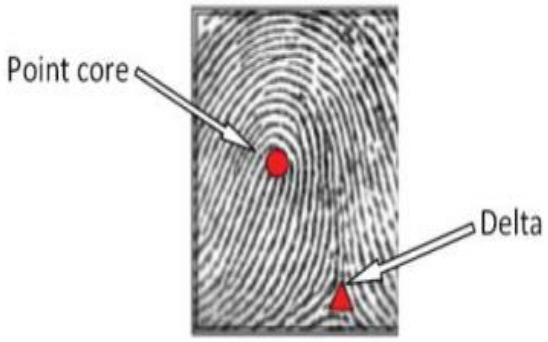


Figure I.4 : Singularités dans une empreinte [13]

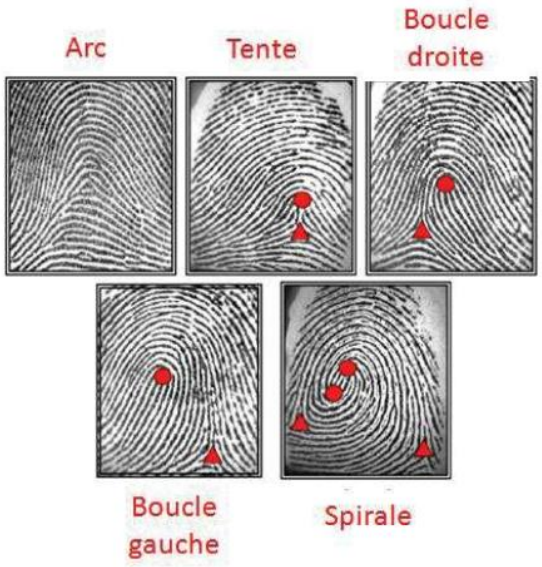


Figure I.5 : Différentes classes d'empreintes digitales [13]

- **<u>Principe de fonctionnement</u>**

Un système automatique de vérification (authentification) d'empreintes digitales est une chaîne de traitement qui se scinde en deux étapes : l'enrôlement ou enregistrement et l'authentification comme le présente le figure I.6

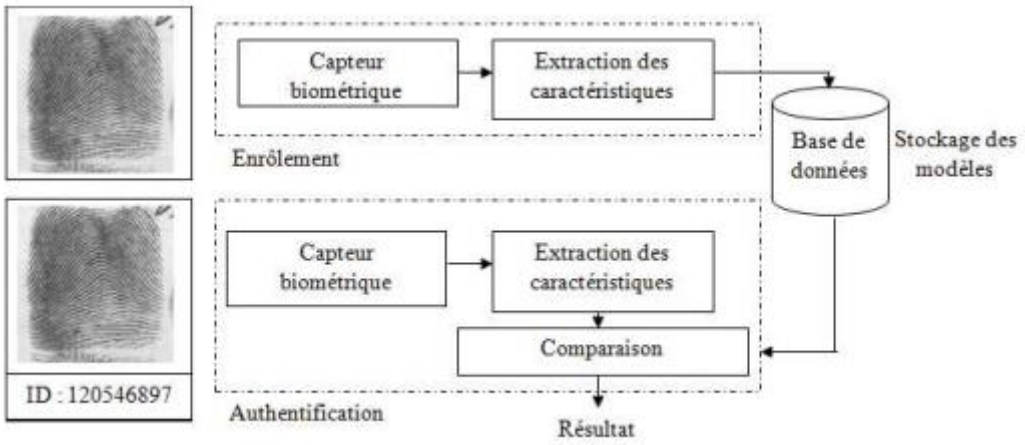


Figure I.6 : Architecture d'un système d'authentification par empreinte digitale [16]

Durant l'enrôlement, le trait biométrique de l'utilisateur est capturé (acquisition) et les caractéristiques sont extraites puis sauvegardées dans une base de données comme modèle de référence. Durant l'authentification, le même trait biométrique de l'utilisateur est de nouveau capturé et les caractéristiques sont extraites ensuite comparées avec celles dans la base de données pour calculer leur correspondance.

- **La phase de capture** : Le but de cette étape est de former l'échantillon biométrique sous la forme d'une image numérique en utilisant un dispositif spécial appelé capteur. Aujourd'hui, bon nombre de capteurs d'empreintes existent. Ils se distinguent, notamment par : leur technologie, leur coût, leur qualité d'acquisition, leur facilité d'intégration (téléphone, ordinateur portable) ou leur capacité à détourner les moulages d'empreintes ;
- **La phase d'extraction des caractéristiques** : Une empreinte apparaît comme une surface alternée de crêtes et de vallées parallèles sur la plupart des régions. Différentes caractéristiques permanentes ou semi-permanentes telles que les blessures ou les coupures sont aussi présentes sur l'empreinte. Il est nécessaire de définir une représentation invariante appelée gabarit ou modèle. Cette représentation peut être globale prenant en compte toute l'image ou, locale c'est-à-dire constituée d'un ensemble de composantes dérivées chacune d'une région restreinte sur l'empreinte. Le processus usuel d'extraction des minuties se présente comme suit :

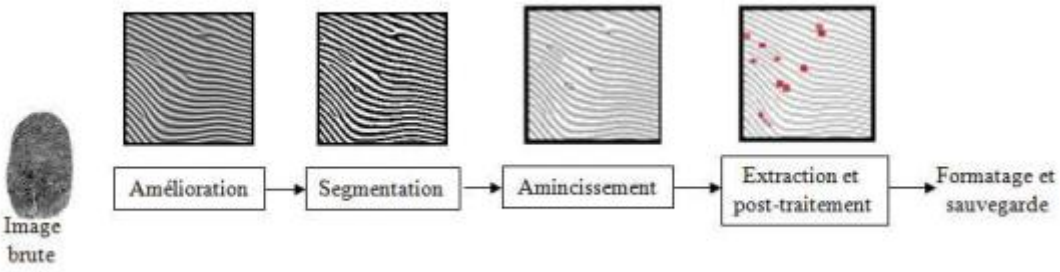


Figure I.7 : Processus usuel d'extraction des minuties [16]

Les différentes étapes de la figure I.7 sont résumées ci-dessous :

- **Amélioration :** le but de cette étape est d'améliorer la qualité des régions récupérables dans l'image ;
- **Segmentation :** l'image en niveaux de gris est convertie en image binaire pour distinguer les crêtes des vallées. Généralement, cette étape fournit de bons résultats à condition qu'elle soit appliquée à des images de bonne qualité ou après une phase d'amélioration ;
- **Amincissement :** l'image binaire est soumise à une étape d'amincissement. Quelques algorithmes comme le MINDTCT (Minutiae Detection) développé par le NIST (National Institute of Standards end Technology) pour le FBI ne requièrent pas cette étape ;
- **Extraction et post-traitement :** un simple calcul du nombre de connexions d'un pixel crête sur l'image amincie peut informer si le pixel concerné est une minutie ou non. Un post-traitement s'avère toujours utile pour éliminer les fausses alarmes ;
- **Formatage et sauvegarde :** les minuties requièrent une représentation très compacte. Chaque minutie peut être décrite par un nombre d'attributs telles que la position, l'orientation et d'autres informations susceptibles d'aider à l'appariement comme son type. Cependant, la plupart des algorithmes considèrent seulement sa position et son orientation.

- **La phase de comparaison :** la mise en correspondance entre deux images d'empreintes diffère suivant la représentation sélectionnée : image, minuties ou descripteur de crêtes, singularités.

2.2 Evaluation des systèmes biométriques

Les points à évaluer pour comparer les différents systèmes biométriques entre eux sont regroupés en trois catégories : l'évaluation de la performance du système (qui permet de mesurer les taux d'erreur du système ainsi que son efficacité) ; l'évaluation de la sécurité et du degré de préservation de la vie privée (qui mesure la robustesse du système aux différentes attaques) ; l'évaluation de l'usage (qui permet de mesurer l'acceptabilité et le taux de satisfaction des utilisateurs).

- **Performance du système**

Dans ce critère d'évaluation, nous nous intéressons aux mesures des taux d'erreur et aux courbes de performance. Comme taux d'erreur, nous avons :

- **Le taux d'échec à la capture** (Failure to Acquire Rate, FTA) qui est la proportion des tentatives de captures pour lesquelles le système ne peut pas détecter un échantillon biométrique ;
- **Le taux d'échec à l'enrôlement** (Failure To Enroll Rate, FTER) qui mesure la proportion des individus pour lesquels le système ne peut pas créer de modèle biométrique ;
- **La fausse acceptation** (False Acceptance, FA) lorsque le système déclare l'individu comme étant légitime alors que c'est un imposteur ;
- **Le faux rejet** (False Rejection, FR) lorsque le système refuse un individu alors qu'il s'agit d'un utilisateur légitime ;
- **Le taux des fausses acceptations** (False Acceptance Rate, FAR) qui mesure la proportion des fausses acceptations par rapport au nombre total d'imposteurs ;
- **Le taux des faux rejets** (False Rejection Rate, FRR) qui mesure la proportion des faux rejets par rapport au nombre total des transactions légitimes ;
- **Le taux d'égale erreur** (Equal Error Rate, ERR) qui indique le taux d'erreur lorsque le système est configuré de manière à avoir le FAR égal au FRR ;
- **Le Zéro FRR** qui est défini comme le plus faible FAR lorsqu'aucun faux rejet ne survient ;
- **Le Zéro FAR** qui est défini comme le plus faible FRR lorsqu'aucune fausse acceptation ne survient.

Dans les courbes de performance, nous distinguons :

- **La distribution intra/interclasse** : pour évaluer la performance d'un système de vérification, on doit calculer les données à partir d'un large nombre de comparaisons entre des gabarits d'un même sujet. On obtient alors la distribution intra-classe (genuine distribution). Il faut aussi collecter les données des comparaisons entre des gabarits appartenant à des sujets différents pour obtenir la distribution interclasse (impostor distribution) comme le montre la figure ci-après :

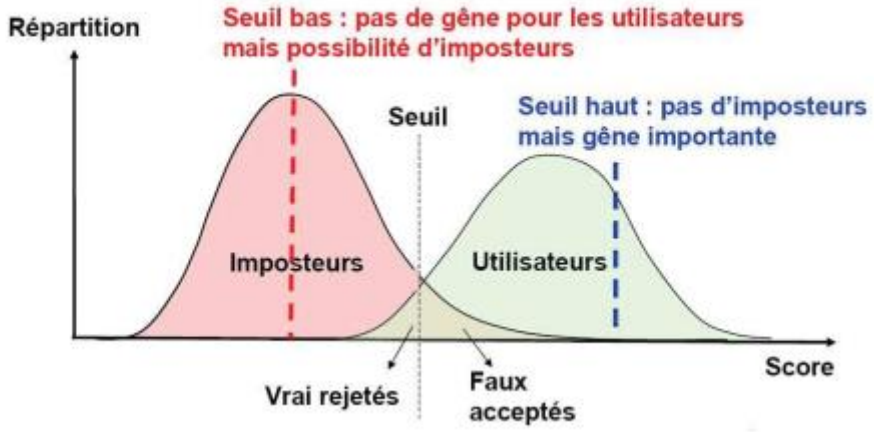


Figure I.8 : Distribution intra/interclasse [22]

- **La courbe réceptrice des caractéristiques** (ou la courbe ROC) qui est la plus couramment utilisée pour représenter les performances du système. Elle représente l'évolution du FAR en fonction du FRR suivant les différents seuils de décision possibles. Au lieu de ROC, parfois le terme DET (détection d'erreur Tradeoff) est utilisé. La courbe ci-dessous est utile pour donner une représentation globale sur le comportement du système :

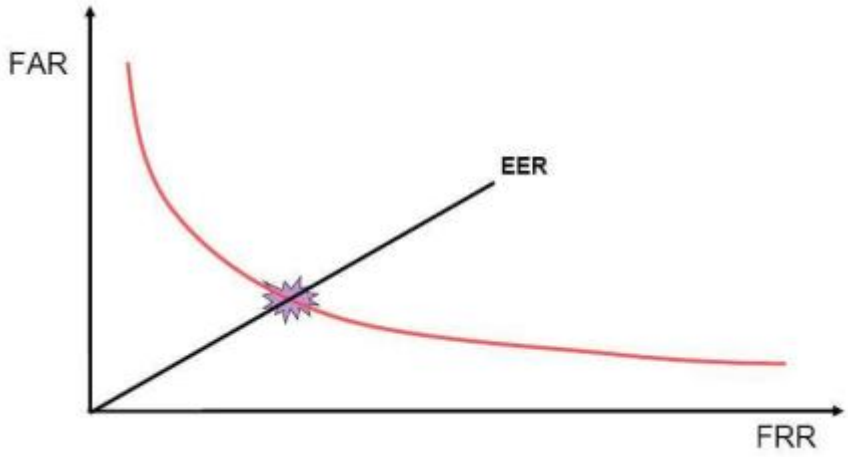


Figure I.9 : Courbe DET [22]

- **Evaluation de la sécurité des systèmes biométriques**

Il est bien connu que la méthodologie principale pour évaluer la sécurité dans les systèmes d'information est basée sur la notion de critères communs CC. Ces critères communs font l'objet d'une standardisation ISO 15408. A l'état actuel des choses ces critères ne suffisent pas pour évaluer complètement les systèmes biométriques. Ils doivent, avant tout, prendre en compte les particularités de ces systèmes. Il est proposé une méthode d'évaluation basée sur les critères communs. Pour ce faire, deux points importants par rapport auxquels un système biométrique a besoin d'une considération spéciale ont été identifiés : l'analyse des vulnérabilités et le test de performance.

3. La technologie RFID

3.1 Description et principe de fonctionnement

- **Description**

La RFID (Radiofrequency Identification) désigne un vaste ensemble d'applications pour l'identification d'objets au sens large, au moyen d'une communication par ondes radio, c'est-à-dire sans-fil. En effet, cette technologie se différencie par la fréquence d'utilisation (LF, HF, UHF), le type de fonctionnement (passif ou actif) et par l'application. Aujourd'hui, avec les avancées technologiques et la miniaturisation des composants électroniques, la RFID s'avère

être particulièrement adaptée à l'acquisition des données issues de capteurs en plus de sa fonction première d'identification. Ainsi, Tout (personnes, objets) est à priori identifiable et le terme RF (RadioFrequency) couvre tous les types de liaisons sans fil ou sans contact réalisés à l'aide d'ondes électromagnétiques, de très basses fréquences (TBF) aux infra-rouges et jusqu'à la lumière visible [11].

La technique d'identification la plus courante est le stockage d'un numéro de série dans une puce à laquelle est attachée une antenne d'émission / réception. L'ensemble puce-antenne est généralement appelé étiquette RFID. Un système RFID se compose des éléments suivants :

- **Une station de base ou élément fixe (émetteur-récepteur) :** souvent appelée reader ou lecteur ou MODEM (Modulateur/Démodulateur) [12]. Le nom technique le plus proche est interrogateur, terme retenu par l'ISO dans sa terminologie officielle RFID ;
- **Les éléments déportés** [12] **:** pouvant être nommés différemment selon les marchés et applications. On parlera de : cartes à puce sans contact, d'étiquettes électroniques ou de badges d'accès électronique. Le terme général de tag ou label est fréquemment utilisé en RFID ;

La figure suivante nous présente quelques exemples d'étiquettes RFID :

Figure I.10 : Quelques exemples de tags RFID [14]

- **Un système d'information (ordinateur) :** gérant les fonctions et processus agissant ou utilisant les données échangées avec l'étiquette.

- **Principe de fonctionnement**

La technologie RFID est basée sur l'émission de champ électromagnétique par le lecteur qui est reçu par l'antenne d'une ou de plusieurs étiquettes. Le lecteur émet un signal selon une fréquence déterminée vers une ou plusieurs étiquettes situées dans son champ de lecture (figure I.11) :

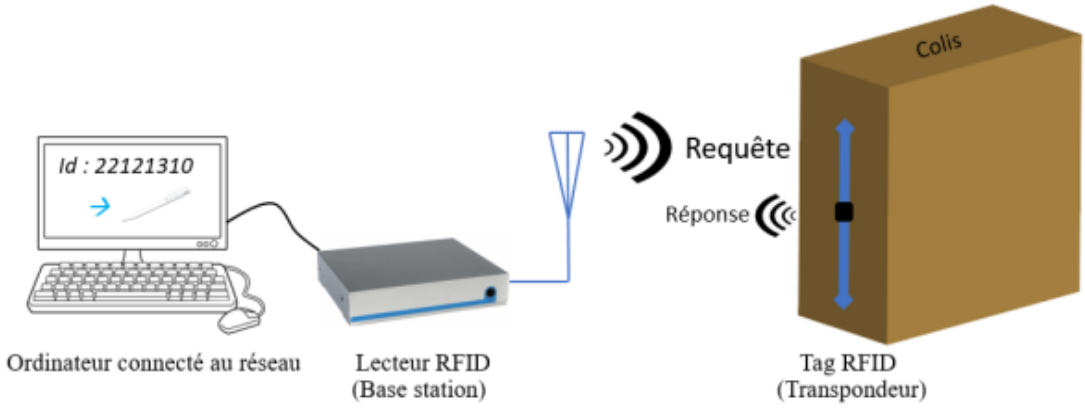


Figure I.11: principe de fonctionnement RFID [17]

- **Composition d'un Tag RFID** : un tag est composé d'un substrat sur lequel est déposé une antenne connectée à une puce RFID comme illustré sur la figure I.12. Il permet de faire le lien entre l'onde électromagnétique provenant du lecteur et l'énergie transmise à la puce. Cela permet également de communiquer avec le lecteur.

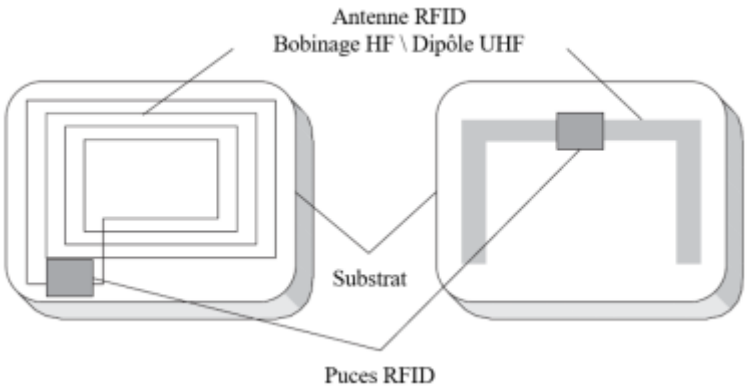


Figure I.12: Structures des étiquettes RFID passives HF (à gauche) et UHF (à droite) [17]

- **Le substrat :** c'est le support de l'antenne et de la puce RFID. Il peut être rigide ou flexible en fonction de l'application et peut être fabriqué avec différents types de matériaux. Par exemple, les tags RFID utilisés en tant que solution antivol pour les documents, nécessitent un substrat flexible afin que les étiquettes RFID puissent se plier exactement comme le papier auquel ils sont attachés ;
- **L'antenne :** celle du tag est très facile à identifier, car c'est l'élément le plus imposant du tag et elle en détermine la taille finale. L'antenne est responsable de la transmission et de la réception des ondes RF, permettant la communication. Sa géométrie dépend du type de couplage (champ proche, champ lointain) et la fréquence de fonctionnement ;
- **La puce RFID :** de nombreux fabricants proposent des puces avec des caractéristiques plus ou moins complexe. Les principaux fabricants sont : NXP, ST Microelectronic, Impinj, Electronic Marin. Les puces RFID sont composées de trois parties principales : l'interface Radio Fréquence (RF), comprenant les blocs de redressement, de modulation/démodulation, de filtrage ; la partie de contrôle numérique, comprenant des fonctionnalités telles que l'anticollision, le contrôle de lecture/écriture, le contrôle d'accès, le cryptage, la gestion mémoire et le contrôle RF ; la partie mémoire EEPROM permettant de stocker les informations, réparties en plusieurs blocs.

- **Le lecteur RFID** : encore appelé lecteur/enregistreur est constitué d'un circuit qui émet une énergie électromagnétique à travers une antenne, et d'une énergie électronique qui reçoit et décode les informations envoyées par le transpondeur et les envoie au dispositif de collecte des données. Le lecteur RFID est l'élément responsable de la lecture des étiquettes radiofréquence et de la transmission des informations qu'elles contiennent (informations d'état, clé cryptographique) vers le niveau suivant du système (middleware). Cette communication entre le lecteur et l'étiquette s'effectue en quatre étapes :
  - Le lecteur transmet par radio l'énergie nécessaire à l'activation du tag ;
  - Il lance alors une requête interrogeant les étiquettes à proximité ;
  - Il écoute les réponses et élimine les doublons ou les collisions entre réponses ;
  - Enfin, il transmet les résultats obtenus aux applications concernées.

La communication entre le lecteur et l'étiquette s'effectue via les antennes qui équipent l'un et l'autre, ces éléments étant responsables du rayonnement radiofréquence. De même, si le

lecteur s'avère de mauvaise qualité, le traitement des données sera impacté. La puissance du lecteur est donc à combiner avec l'antenne adéquate, ceci permettant de déterminer la portée optimale de la lecture. Généralement, on distingue quatre modalités : lecture de proximité entre 10 et 25 cm ; lecture de voisinage jusqu'à 1 mètre ; lecture à moyenne distance de 1 à 9 mètres ; lecture longue portée jusqu'à plusieurs centaines de mètres. Par ailleurs, le terme de lecteur RFID est en fait une impropriété, puisque ce dernier est également capable d'écrire des informations sur l'étiquette. Car, bon nombre d'étiquettes sont en lecture seule (le code qu'elles contiennent ayant été imprimé en même temps que l'étiquette elle-même), d'autres contiennent, au-delà du code de base, une zone mémoire pouvant contenir des données variables.

3.2 Technologies et types de systèmes RFID

- **Technologies RFID**

Il existe 2 grandes classes de technologies RFID ayant chacune différentes fréquences radio:

- **La technologie par couplage magnétique en champ proche** (aussi appelée couplage inductif) [15] : dont la fréquence est comprise entre 125-148 kHz et 13,56 MHz, pour des applications courte distance (jusqu'à 50 cm), comme les étiquettes standards ou les cartes à puce sans contact. Cette technologie est plus souvent liée aux systèmes passifs. Le transfert bidirectionnel de données numériques s'effectue grâce à l'énergie émise par l'interrogateur, modulée par l'étiquette ; Le schéma de couplage magnétique se résume ainsi qu'il suit :

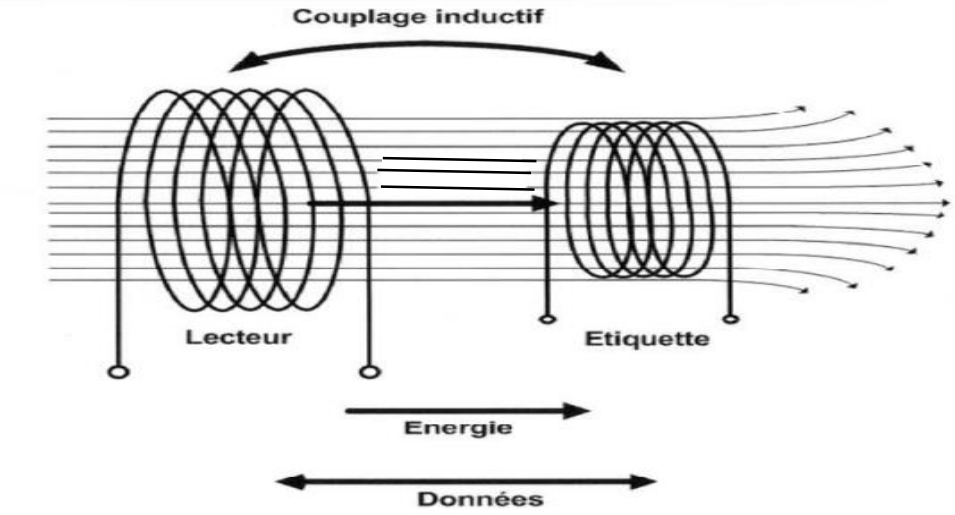


Figure I.13 : couplage magnétique en champ proche [15]

- **La technologie par couplage électrique en champ lointain (couplage radiatif) [15]:** qui fonctionne dans les bandes de 434 MHz, 860 MHz, 2,45 GHz et 5,8 GHz. Les distances de fonctionnement peuvent atteindre plusieurs mètres avec des étiquettes actives. Le transfert des données à partir de l'étiquette s'opère cette fois grâce à la rétro propagation du signal émis par le lecteur.

Les principales fréquences utilisées en RFID [15] sont regroupées dans le tableau ci-dessous:

Tableau N°I.3 : Principales fréquences RFID [15])

Classification dans le spectre des fréquences	Fréquences les plus utilisées	Types de couplage	Types d'étiquettes
LF	125 et 134,2 Khz	Inductif	Passives
HF	13.56 Mhz	Inductif	Passives
UHF	868 Mhz en Europe Et 915 Mhz aux USA	Inductif	Passives ou actives
UHF	2.45Ghz	Radiatif	Actives
SHF	5.8 et 5.9 Ghz	Radiatif	Actives

- **<u>Types de systèmes RFID</u>**

Il existe plusieurs types de systèmes RFID à savoir :

- **Le système passif [11]** : ici, les étiquettes RFID passives sont composées d'une puce électronique qui mémorise les données numériques d'identification et d'une antenne qui transmet ces informations enregistrées. L'interrogateur RFID émet des ondes électromagnétiques qui induisent un courant dans l'antenne de l'étiquette. Cette étiquette émet alors selon des fréquences bien définies une suite alphanumérique fixe servant d'identifiant à l'objet étiqueté. La portée va de quelques centimètres à quelques

mètres au plus. L'étiquette retourne des informations à l'interrogateur par rétro-modulation (en couplage inductif basse et haute fréquence) et par rétrodiffusion (en super et ultra haute fréquence) ;

- **Le système actif [11]** : ici, l'étiquette retourne des informations à l'interrogateur en produisant elle-même une onde électromagnétique (elle intègre donc un émetteur). Ils fonctionnent généralement dans la bande UHF et offrent une portée allant jusqu'à 100 mètres. En général, les étiquettes actives sont utilisées sur de gros objets, tels que les wagons, les grands conteneurs réutilisables et d'autres biens qui doivent être suivis sur de longues distances. Il existe deux principaux types de tags actifs : les transpondeurs et les balises. Les transpondeurs sont déclenchés lorsqu'ils reçoivent un signal radio d'un lecteur, puis s'allument et répondent en transmettant un signal. Comme les transpondeurs ne rayonnent pas activement les ondes radio jusqu'à ce qu'ils reçoivent un signal de lecture, ils conservent la durée de vie de la batterie. Les balises sont souvent utilisées dans les systèmes de localisation en temps réel (RTLS), afin de suivre l'emplacement précis d'un bien en continu. Contrairement aux transpondeurs, les balises ne sont pas alimentées par le signal du lecteur. Au lieu de cela, elles émettent des signaux à des intervalles prédéfinis. Selon le niveau de précision de localisation requis, les balises peuvent être réglées pour émettre des signaux toutes les quelques secondes ou une fois par jour. Le signal de chaque balise est reçu par les antennes de lecture qui sont positionnées autour du périmètre de la zone surveillée, et communique les informations d'identification et la position de l'étiquette.

Par ailleurs, il existe 2 modes d'alimentation des systèmes RFID :

- **Le mode télé-alimenté** : l'étiquette ou tag tire son énergie du rayonnement produit par l'interrogateur ;
- **Le mode alimenté par batterie** : l'interrogateur tire simplement son énergie d'une batterie intégrée au système.

Le tableau ci-dessous résume le principe de fonctionnement des classes de technologies et des éléments du système RFID :

Tableau N°I.4 : principe de fonctionnement des systèmes RFID [11]

	Basses/ Hautes fréquences	**Ultra hautes/ Super Hautes fréquences**
Principe de fonctionnement	Couplage inductif	Rayonnement/Propagation
Fonctionnement station de base vers tag	Télé-alimenté	Télé-alimenté
Fonctionnement tag vers station de base	Rétro modulation	Rétro propagation
Distance de fonctionnement	De 1 à 2 mètres	Jusqu'à 8 ou 10 mètres

Remarque : Quelques domaines d'application de la technologie RFID

Les applications en RFID sont nombreuses et concernent plusieurs secteurs d'activité. Elles s'enrichissent tous les jours de nouvelles idées, des bâtiments, du transport de marchandises ou du transport humain, chaîne de production ou des services vétérinaires qui suivent leurs troupeaux par la carte à puce), dans la justice ou dans le secteur de la sécurité (bracelet de libération conditionnelle, dans le domaine de la loi via un lecteur mobile), dans le secteur agroalimentaire (à travers les produits et articles). Par ailleurs, cette technologie présente des avantages et des limites qui sont regroupées dans le tableau ci-dessous :

Tableau N°I.5 : Avantages et limites de la technologie RFID [11]

Avantages	**Limites**
Possibilité de modification de données : Pour les étiquettes à lecture et écriture multiples, les données gravées peuvent subir des modifications à tout moment par les personnes autorisées contrairement au code à barres les données inscrites restent figées une fois qu'elles sont imprimées	**Perturbations métalliques :** La lecture des étiquettes RFID peut aussi être perturbée par la proximité dans le champ de lecture des éléments métalliques ce qui affecterait fortement la réussite de la technologie dans le domaine de production métallique
Grand volume de données : Les étiquettes RFID peuvent contenir des données dont les	

caractères peuvent aller jusqu'à plus de 15000	
Protection des contenus : Les contenus des étiquettes RFID étant des données numériques peuvent être en partie ou en tout sujets à une réglementation d'accès ou une protection par un mot de passe en lecture ou écriture. Avec cette protection contre l'accès des informations imprimées sur l'étiquette, la contrefaçon et le vol s'avèrent difficiles	
Durée de vie : Les étiquettes RFID peuvent avoir une durée de vie de dizaines d'années. Les données au cours de ces années peuvent subir de modifications plus d'un million de fois selon le type de l'étiquette avec un maximum de fiabilité	**Interchangeabilité :** La technologie RFID diffère d'une compagnie à une autre et ainsi un produit qui quitte une compagnie pour une autre ne pourra pas être lu à moins que les deux compagnies utilisent le même système RFID
Meilleure accessibilité et résistance aux effets extérieurs : Les étiquettes de la technologie RFID fonctionnant avec les ondes électromagnétiques n'ont pas besoin de contact ou de visée optique. Leur liaison avec le système est établie dès qu'elles entrent dans les champs électromagnétiques. Les étiquettes RFID sont insensibles à la poussière, aux taches, aux frottements, à l'humidité	

II. Quelques travaux effectués dans le domaine des contrôles d'accès

1. La biométrie

Plusieurs travaux ont été effectués dans le domaine du contrôle d'accès notamment ceux référencés dans la première partie de ce chapitre. Concernant le domaine de la biométrie, nous avons :

1.1 Les travaux de R. Belguechi, E.Cherrier, T.Le-goff,

R. Belguechi, E.Cherrier, T.Le-goff ont travaillé sur le thème **« Etude de la robustesse d'un système de biométrie révocable»** [20] dans un contexte général d'identification des personnes. Le problème mis en exergue par ces auteurs est l'identification simple et ergonomique des individus dans des lieux sécurisés. La solution proposée est la robustesse utilisant le biohashing (qui consiste à générer un biocode binaire pour l'enrôlement et la vérification) en effectuant les attaques réalisables par une personne malveillante. La limite présentée par ce travail est l'élaboration des attaques plus complexes pour la partie usurpation d'identité (il a été montré qu'une personne malveillante est en mesure de générer un BioCode admissible par le système d'identification).

1.2 Les travaux de Florent PERRONIN, Jean-Luc DUGELAY

Florent PERRONIN, Jean-Luc DUGELAY ont travaillé sur le thème **« Introduction à la biométrie, authentification des individus par traitement audio-visuel »** [22] dont le problème mis en exergue est similaire au précédent ; la solution proposée est un système multimodal combinant plusieurs types de techniques biométriques et basé sur une série d'algorithmes complexes tels que les algorithmes de squelettisation de Zhang et de Shapori. La limite relevée par ce système est la sauvegarde automatique des données qui est un élément fondamental pour la traçabilité des informations en cas d'enquête ou de revendication par une personne accédant au système.

2. La RFID

2.1 Les travaux de Ziani-Kerarti Samir et Kadi Oussama

Le thème sur lequel se sont appesantis ces auteurs est **« Etude et conception d'un système de présence automatique par RFID»** [12] dont le problème mis en exergue est l'identification, la localisation et le suivi des objets en utilisant l'identification visuelle. La solution qu'ils ont proposée est un système de gestion de présence exploitant la technologie RFID qui a été limité par la gestion de la bibliothèque pour les accès.

2.2 Le travail de Yassin Belaizi

Ce dernier a travaillé sur **« Etude et conception d'un capteur RFID passif en bande UHF : application à l'agroalimentaire »** [17]. Le problème mis en exergue dans ce contexte agroalimentaire est la supervision de l'environnement ; A cet effet, il a proposé un capteur RFID passif fonctionnant en bande UHF. La limite présentée par son travail est le coût du capteur géométrique utilisé.

3. Application de l'intelligence artificielle dans le contrôle d'accès par biométrie

3.1 Description

L'intelligence artificielle est l'intelligence présentée par les machines. Son but est de concevoir des systèmes capables de reproduire le comportement humain dans ses activités de raisonnement (penser, agir). L'apprentissage machine (aussi appelée apprentissage artificiel ou automatique, en anglais machine learning) est le processus par lequel un ordinateur acquiert de nouvelles connaissances et améliore son mode de fonctionnement en tenant compte des résultats obtenus lors de traitements antérieurs.

Le principe de l'apprentissage machine est de construire un modèle à partir d'un ensemble de données, soit en améliorant un modèle existant moins général, soit en créant un nouveau modèle représentatif de nouvelles données. Ils servent souvent à prendre des décisions.

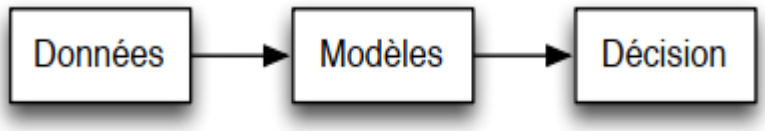


Figure I.14 : Principe de fonctionnement de l'apprentissage machine [24]

Il existe deux approches principales en apprentissage machine. La première est issue de l'intelligence artificielle syntaxique ou symbolique. Elle est fondée sur la modélisation du raisonnement logique et sur la représentation et la manipulation de la connaissance par des symboles formels. La deuxième est issue de l'intelligence artificielle statistique ; elle est qualifiée de statistique aussi parfois numérique parce que, souvent, la représentation et la

manipulation de la connaissance sont sous une forme numérique. Les tâches d'apprentissage automatique sont généralement classées en trois grandes catégories en fonction de la nature du signal d'apprentissage ou de la rétroaction dont dispose un système d'apprentissage :

- **Apprentissage supervisé** : (supervised learning en anglais) est une technique d'apprentissage automatique où l'on cherche à produire automatiquement des règles à partir d'une base de données d'apprentissage contenant des exemples. Le système observe des couples de types entrée-sortie et apprend une fonction qui permet d'aboutir à la sortie à partir de l'entrée. Cette phase est appelée phase d'apprentissage ou d'entraînement ;
- **Apprentissage non supervisé** : consiste à tirer de la valeur de données dans lesquelles l'attribut à prédire n'apparaît pas. Le système apprend alors de lui-même à organiser les données ou à déterminer des structures dans les données. La tâche d'apprentissage la plus courante est le regroupement (clustering en anglais) qui consiste à regrouper les données d'entrées selon leurs caractéristiques communes. Ce type d'apprentissage est utilisé dans le but de visualiser ou explorer des données ;
- **Apprentissage par renforcement** : se base sur des données d'entrée similaires à celles utilisées en apprentissage supervisé. Dans ce cas, l'apprentissage est guidé par l'environnement sous la forme de récompenses (positive ou négative) calculées en fonction de l'erreur commise lors de l'apprentissage. En robotique, l'apprentissage par renforcement a permis de mettre au point des robots plus autonomes et adaptatifs que ceux existants.

Quelques auteurs ont abordé l'approche de l'intelligence artificielle dans les systèmes de contrôle d'accès à l'instar de :

- **HADDAD ZEHIRA** [25] : « **Système automatique de classification pour la reconnaissance d'empreinte** » dont l'approche était basée sur le réseau de neurone flou utilisant la méthode de Takagi-Sugeno permettant d'avoir un système en temps réel, une autonomie et une intelligence ;
- **DIB Fouad** [24] : **« Identification des personnes par le réseau veineux** », proposant un système d'identification de personne où l'on doit utiliser les moments de Zernike comme caractéristiques de réseaux veineux de la main et utiliser l'approche neuronale pour l'identification ;

- **SADAOUI FETHIA, BENKADDOUR KAMEL, HAMMANI ZINEB** [27] : « **L'application des réseaux de neurones artificiels à l'identification biométrique** » proposant un système de reconnaissance de visage basé sur une méthode hybride pour la reconnaissance faciale combinant les réseaux de neurone (approche neuro ACP) avec l'analyse en composantes principales.

3.2 Présentation de la méthode des réseaux de neurones et l'algorithme de rétro propagation du gradient

Un réseau de neurones aussi appelé réseau de neurones artificiels est un modèle mathématique très simple dérivé du neurone biologique dont les composantes élémentaires sont des unités de calcul qui reçoivent des entrées pour produire des sorties. Le réseau de neurone permet une gestion plus souple et moins coûteuse des systèmes complexes en temps de calcul et en manipulation de variables. L'intérêt des réseaux de neurone réside dans leur capacité d'apprendre à partir d'exemples simples pour résoudre par la suite des problèmes assez complexes. Les réseaux de neurone sont classés en 2 catégories : le réseau de feedforward (la propagation de l'information se fait dans un seul sens : de l'entrée vers la sortie uniquement) et le réseau récurent (qui tient compte d'une dimension temporelle ou de mémoire entre l'entrée et la sortie du réseau par des connexions en boucle). Ce modèle reprend les principes du fonctionnement du neurone biologique, en particulier par la sommation des entrées et la pondération de la somme de ses entrées par des poids synaptiques (aussi appelés coefficients synaptiques) tels qu'illustrés à la figure suivante :

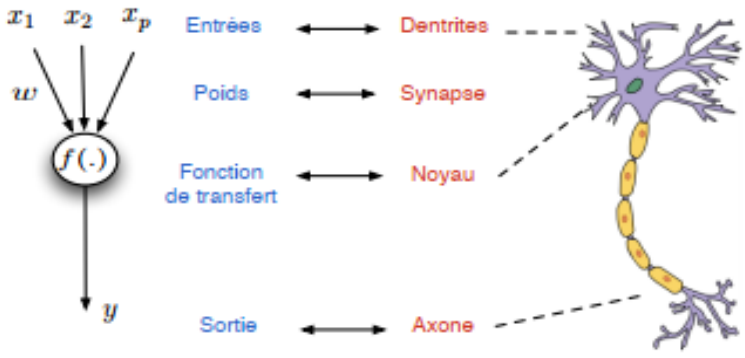


Figure I.15 : Analogie entre le neurone biologique et le neurone artificiel [24]

Dans la classification des RNA nous distinguons :

- **Le perceptron simple** : qui fournit une sortie suite à la pondération de la somme de ses entrées et l'application d'une fonction d'activation et qui présente la limite de distinguer les données non séparables linéairement ;
- **Le perceptron multicouches ou PMC** : qui est une succession de neurones organisés en plusieurs couches. La première couche est reliée aux entrées. Ensuite, on retrouve un ensemble de couches intermédiaires qui ne sont pas visibles et qui sont appelées des couches cachées. Chaque couche est reliée à la couche précédente. La dernière couche du PMC définit la réponse des neurones et produit les différentes sorties.

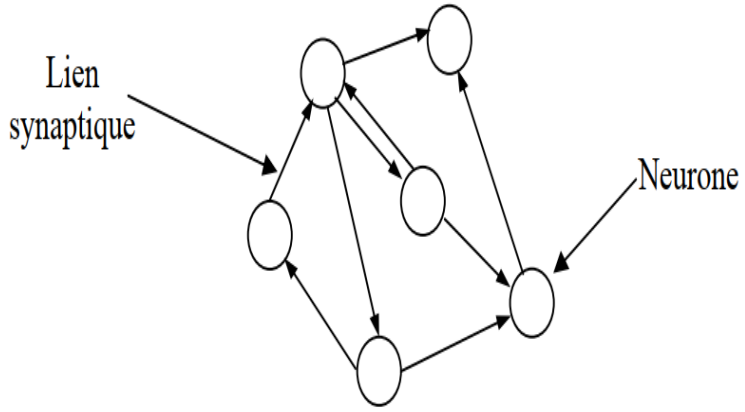


Figure I.16 : Modèle d'un réseau neuromimétique [24]

L'algorithme de rétro propagation du gradient que nous allons utiliser est issu du PMC. L'apprentissage du perceptron se fait selon la règle Delta. Cette règle a été généralisée en 1986 aux réseaux multicouches et formalisée sous l'appellation de la règle de la rétro propagation du gradient de l'erreur. Cette dernière consiste à propager l'erreur obtenue à un neurone de sortie d'un réseau à couches à travers le réseau par descente du gradient dans le sens inverse de la propagation des activations.

Cette approche interviendra dans la phase d'enrôlement pour le traitement de nos empreintes digitales afin de rendre notre système plus efficace et autonome par rapport à ceux étudiés dans la revue de la littérature. L'approche structurelle par cet algorithme utilise l'estimation de l'orientation des crêtes dans une image d'empreinte digitale. Plusieurs méthodes de classification sont associées à ce type d'approche à savoir le réseau de neurone, les k plus proches voisins, le classificateur hybride et le modèle caché de Markov. Dans cette approche, avant d'extraire les directions des crêtes, l'empreinte digitale subit un prétraitement à l'aide

d'un filtre FFT (Fourier Fast Transfrom) dans le but d'améliorer sa qualité et de pouvoir assurer une évaluation fiable de l'image d'orientation. L'entrée du réseau de neurone est l'image d'orientation des crêtes, un filtrage est fait pour assurer une bonne extraction des caractéristiques (le core et le delta). L'algorithme de rétro propagation du gradient de l'erreur est utilisé avec des réseaux de types feedforward pour l'apprentissage de fonction, la classification et la reconnaissance de forme, à chaque couple entrée/sortie, une erreur est calculée. Les étapes de cet algorithme sont :

- Initialisation des poids $W^{[q]}$ à des petites valeurs aléatoires ;
- Présentation d'une entrée x_k et de la sortie désirée d_k ;
- Calcul de la sortie actuelle par propagation à travers les couches :

$$\boldsymbol{P_i = \sum_i W_{ji}^{[q]} . x_i^{[q-1]}}$$

Où [q] est qième couche du réseau.

- Accumulation des erreurs en sortie ;
- Rétro-propagation du gradient de l'erreur depuis la dernière couche vers la première couche.

La règle de la rétro propagation du gradient de l'erreur consiste alors à mettre jour le poids entre un neurone *i* et un neurone *j* utilisant la relation suivante :

$$\boldsymbol{\Delta w_{i;j} = \eta \delta_j a_i}$$

L'algorithme se présente comme suit :

Algorithme de rétropropagation du gradient.

1. Initialiser aléatoirement les poids synaptiques
2. **Répéter**
3. **Pour** chaque $(\mathbf{x}_i, y_i) \in D$
4. **Pour** chaque couche du réseau de neurones
5. **Pour** chaque neurone de la couche considérée
6. Calculer δ_j selon les éq. 5.7 et 5.8
7. **Pour** chaque connexion w_{ij}
8. Calculer $\Delta w_{ij} = \eta \delta_j y_i$
9. **FinPour**
10. **FinPour**
11. **FinPour**
14. **FinPour**
12. **Pour** chaque connexion w_{ij} **Faire**
13. $w_{ij} \leftarrow w_{ij} + \Delta w_{ij}$
14. **FinPour**
15. **Jusqu'à** atteinte d'un critère d'arrêt

Figure I.17 : Algorithme de rétro propagation du gradient [24]

Remarque : Partant des différents travaux suscités, il nous est venu l'idée de combler certains manquements liés notamment au coût, au stockage des informations et à la gestion des personnes malveillantes tout en nous basant sur l'apprentissage machine qui relève de l'IA. Par ailleurs, l'algorithme que nous décidons d'utiliser ici pour la phase d'entraînement de nos empreintes digitales est celui de rétro propagation du gradient utilisé dans les RNA multicouches de type feedforward qui permet de pallier une carence de l'algorithme du perceptron qui est incapable de modifier les poids des couches cachées et dont l'implémentation est simple. Nous proposons ainsi un système intelligent doté de robustesse quant au temps de calcul assez important qui sera utilisé lors de l'apprentissage pour une meilleure efficacité du système ainsi que sa disponibilité en temps réel.

Conclusion

Il a été question dans ce chapitre de présenter les généralités sur les systèmes de contrôle d'accès par biométrie et RFID, quelques travaux ayant été effectués dans ce domaine et l'application de l'intelligence artificielle aux systèmes de contrôle d'accès. Il en ressort que nous distinguons 2 types de techniques biométriques dont les techniques comportementales et morphologiques ; la technologie RFID quant à elle fait intervenir 2 grandes catégories qui sont le couplage magnétique en champ lointain dont la fréquence va jusqu'à 13,56Mhz et le couplage

magnétique en champ proche dont la fréquence va jusqu'à 5,8Ghz. Par ailleurs, face aux limites telles que les coûts de développement, le stockage des informations, la disponibilité du système en temps réel, nous proposons un système intelligent combiné biométrie et RFID utilisant la méthode des RNA multicouches de type feedforward pour pallier à certaines limites des travaux présentés.

CHAPITRE II : CONCEPTION DU SYSTEME PAR EMPREINTES DIGITALE ET RFID

Dans ce chapitre, nous présenterons la méthodologie de conception du système en spécifiant tout d'abord les différentes fonctions et spécifications ainsi que les outils utilisés.

Aperçu

Introduction

I- Cahier de charges

II- Les outils

III- Application du perceptron multicouches (PMC) au système par l'algorithme de rétro propagation du gradient

Conclusion

Introduction

Chaque jour, nous remarquons un nombre croissant de personnes ayant accès au campus de l'ENSET d'Ebolowa. De ce fait, nous avons pu observer plusieurs manquements quant à la surveillance, la gestion d'entrée/sortie du personnel administratif, du corps enseignant, des visiteurs et des étudiants. Afin d'améliorer, de développer et de rendre efficace la gestion des mouvements au sein de ce campus, nous proposons un système automatique de contrôle d'accès combinant empreinte digitale et cartes RFID. Pour ce faire, nous présenterons dans ce chapitre, le cahier de charges du système, les différents outils que nous allons utiliser pour la mise en place du système et l'application de l'approche par les réseaux de neurones artificiels.

I. Cahier de charges fonctionnel du système

1. Concept général et services attendus

- **Concept général**

Le cahier des charges fonctionnel (CDCF) est un document formulant le besoin, au moyen de fonctions détaillant les services rendus par un produit et les contraintes auxquelles il est soumis. Il vise à définir et à faire valider les spécifications d'un produit ou d'un service à réaliser. Ici il s'agit d'un CDCF, formulant le besoin au moyen de fonctions détaillant les services attendus et les contraintes auxquelles le produit à fournir est soumis. Les différents éléments qui ressortent de cette partie sont les suivants :

- **La formulation du besoin** : il sera question d'assurer le rendement du personnel (administratif et enseignants) et la formation des étudiants, sécuriser le bâtiment de l'école (accès visiteurs) au moyen d'un dispositif intelligent, autonome et à moindre coût ;
- **Le client** : étant considéré ici comme le commanditaire du projet, dans ce cas il s'agit de l'ENSET d'Ebolowa ;
- **Les utilisateurs** : les différents utilisateurs de ce système seront le personnel administratif, les enseignants et les visiteurs.

- **Services attendus**

Ce sont les différentes actions qui doivent être réalisées par le système proposé à savoir :

- Permettre à chaque utilisateur de s'authentifier à l'arrivée comme au départ ;
- Permettre à la cellule informatique d'avoir une traçabilité sur les mouvements des différents utilisateurs afin d'aquilibrer la paie du personnel et des enseignants par le service comptable ;
- Permettre au service de sécurité de gérer les cas de tentative d'intrusion ;
- Etre simple d'utilisation, léger et esthétique

2. Analyse fonctionnelle du système

- **Analyse du besoin**

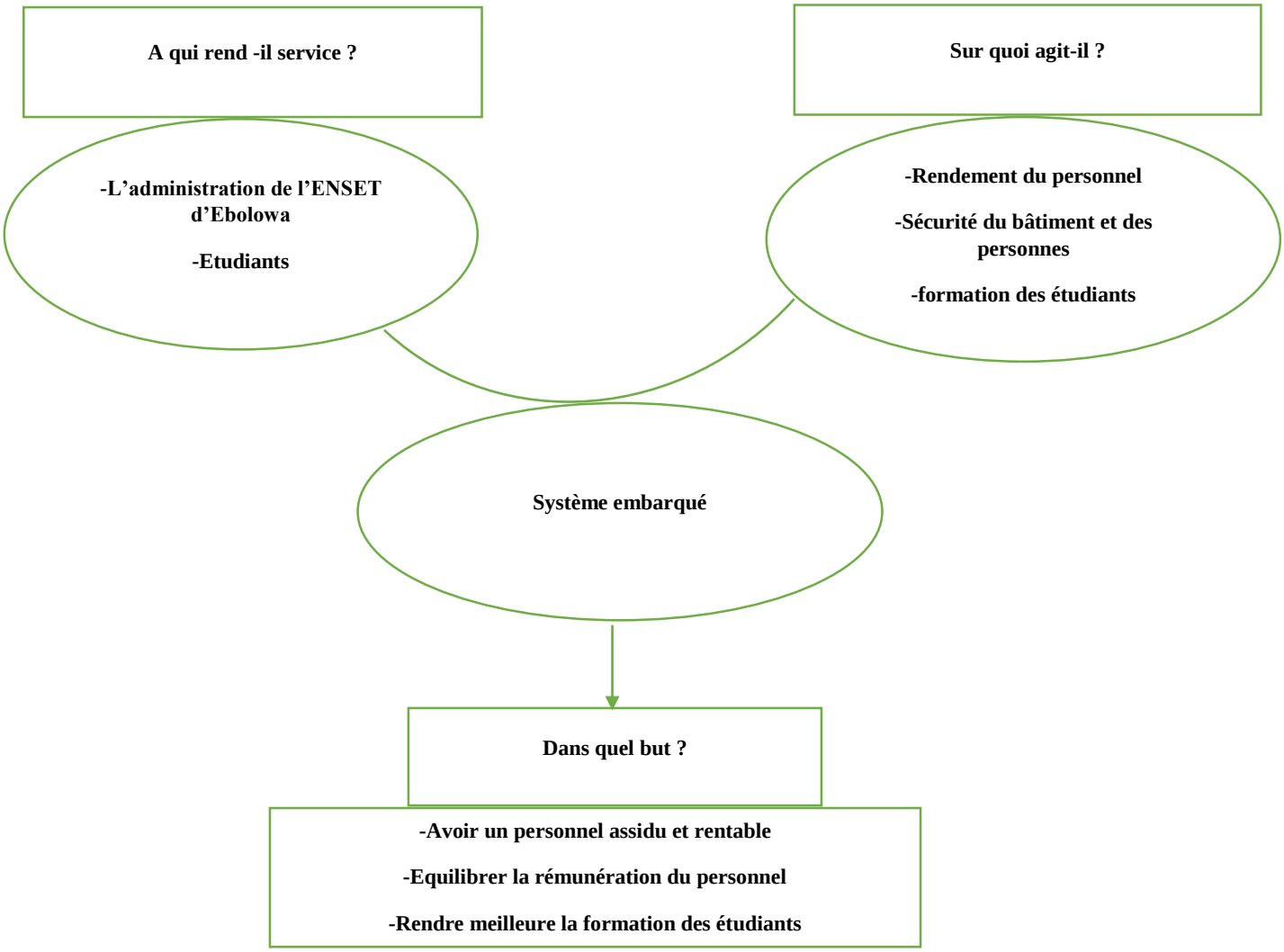


Figure II.1: Diagramme bête à corne

- **A qui le produit rend-il service ?:**le système embarqué s'adresse à l'administration de l'ENSET d'Ebolowa désirant contrôler les mouvements d'entrée et de sortie de son personnel ainsi que ceux des visiteurs. Le client doit avoir un produit répondant à toutes ses attentes : il doit être léger, facile d'utilisation, à coût réduit, utilisable à tout moment et qui doit pouvoir être esthétique ;
- **Sur quoi agit-il ? :** Il agit directement sur le rendement du personnel (surveillance des entrées et sorties) et la sécurisation du bâtiment et des personnes ;
- **Quelles sont les origines du besoin ? :** les retards, absences régulières et répétitives de certains membres du personnel, de certains enseignants, les allées et venues non contrôlées des visiteurs dans les bureaux et salles de classe ;
- **Le besoin peut-il évoluer ? :** il est impossible d'imaginer qu'un besoin n'évolue pas. En effet, les évolutions technologiques pourraient entraîner des modifications du besoin. Par exemple un nouveau système embarqué prenant en compte d'autres paramètres ;
- **Le besoin peut-il disparaître ? :** le besoin peut disparaître si :
  - L'école ferme ses portes (peu probable) ;
  - L'école prend feu ;

- **<u>Enoncé des fonctions</u>**

Les fonctions principales du système sont les suivantes :

- Assurer l'identification/authentification des utilisateurs ;
- Assurer les traçabilités des mouvements d'entrée et de sortie ;
- Assurer la gestion des cas d'intrusion ;
- Etre pratique d'utilisation ;
- Etre léger ;
- Etre facilement manipulable ;
- Etre peu encombrant ;

Les fonctions contraintes sont :

- Respecter les normes (homologation) ;
- Etre robuste ;
- Etre esthétique ;
- Avoir un coût accessible ;
- Etre durable ;
- Effectuer aisément la maintenance ;

II. Les outils

1. Le matériel

Pour la mise en œuvre de notre projet, nous allons utiliser du matériel ARDUINO qui s'impose grâce à sa simplicité, son efficacité, son faible coût et sa disponibilité sur le marché. Les principaux outils de notre projet sont :

- **Un ordinateur portable** : c'est un appareil électronique qui permet le traitement rationnel et le stockage des informations. Celui que nous allons utiliser pour la réalisation de notre projet est de marque HP ayant les caractéristiques suivantes :
  - **Système d'exploitation** : Windows 8.1 Professionnel ;
  - **Disque dur** : 500Go ;
  - **RAM** : 4 Go ;
  - **Processeur** : AMD A8 PRO 7150B R5, 10 Compute Cores 4C+6G 1.90Ghz ;
  - **Carte graphique** : AMD Radeon ™ R6 Graphics.
- **Une carte Arduino de type Mega 2560** : Arduino est une plateforme électronique open source basée sur des circuits simplifiés. Les cartes Arduino sont capables de lire les entrées et de les transformer en sortie ce qu'il faut faire en envoyant une série d'instructions au microcontrôleur. Il existe une multiplicité de cartes Arduino [14], celle que nous avons choisie d'utiliser pour notre projet est la carte Arduino Mega 2560, principalement pour le nombre de broches assez important qu'elle propose ainsi que pour sa mémoire interne compte tenu du nombre de modules que nous allons implémenter. C'est une carte à microcontrôleur basée sur un ATmega2560. Elle dispose [18] :
  - **De 54 broches numériques d'entrées/sorties** (dont 14 peuvent être utilisées en sorties PWM (largeur d'impulsion modulée)) : Chacune peut être utilisée soit comme une entrée numérique, soit comme une sortie numérique. Ces broches fonctionnent sous une tension de 5V, chacune pouvant fournir ou recevoir un maximum de 40mA d'intensité et disposant d'une résistance interne. Cette dernière s'active sur une broche en entrée ;
  - **De 16 entrées analogiques** (qui peuvent également être utilisées comme broches entrées/sorties numériques) : par défaut, ces broches mesurent entre 0V et 5V, mais il est possible de modifier la référence supérieure de la plage de mesure en utilisant la broche AREF ;

- **De 4 UART** (port série matériel) : pour une communication série de niveau TTL (5V) et qui est disponible sur les broches 0 (RX) et 1 (TX). Un circuit intégré ATmega8U2 sur la carte assure la connexion entre cette communication série de l'un des ports série de l'ATmega 2560 vers le port USB de l'ordinateur qui apparaît comme un port COM (Communication) virtuel pour les logiciels de l'ordinateur ;
- **D'un quartz 16Mhz** : qui est un composant dont la fréquence stable d'oscillation sera à 16Mhz lorsqu'il est stimulé électriquement ;
- **D'une connexion USB (Universal Serial Bus)** : qui sert d'alimentation et qui fournit 5V sous 500mA ;
- **D'un connecteur d'alimentation jack** : qui sert d'alimentation externe à la carte et fournit de 3V à 12v sous 500mA. Si on utilise plus de 12V, le régulateur de tension de la carte pourrait chauffer et endommager la carte ;
- **D'un connecteur ICSP** (programmation "in-circuit") ;
- **D'un bouton de réinitialisation** (reset).

Remarque : La carte Arduino Mega2560 utilise un Atmega8U2 programmé en convertisseur USB vers-série. Les longueurs et largeurs maximales du circuit imprimé de la carte Mega2560 sont respectivement 10.16cm et 5.33cm, avec le connecteur USB et le connecteur d'alimentation Jack s'étendant au-delà des dimensions de la carte. Plusieurs trous de vis permettent à la carte d'être fixée sur une surface ou dans un boîtier. Il est important de noter que la distance entre les broches 7 et 8 est de 0.16 pouces, et non un multiple de 0.1 pouces séparant les autres broches.

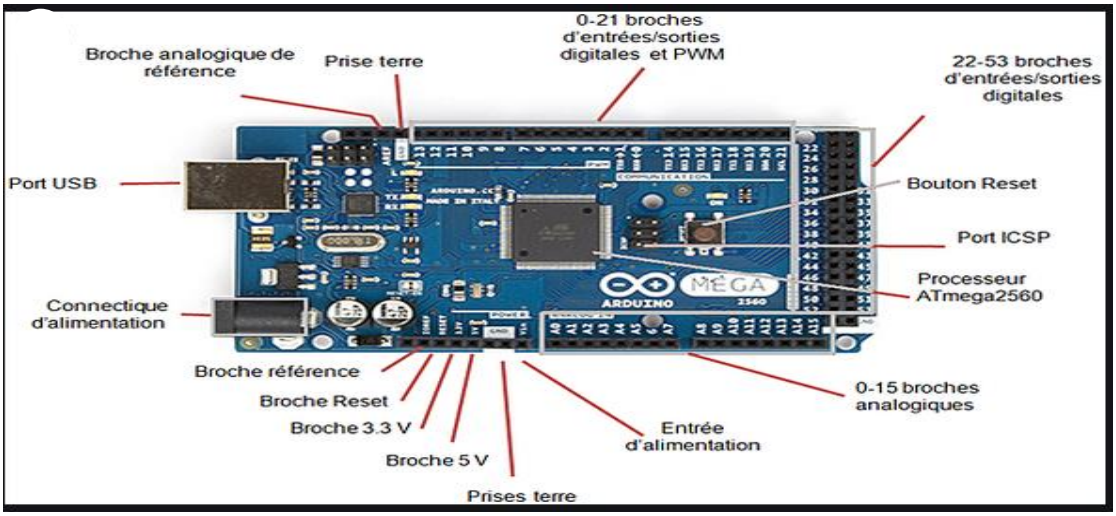


Figure II.2: Description de la carte Arduino Mega2560 [18]

- **Le capteur d'empreintes digitales AS608CHIP** : le capteur d'empreinte Arduino est un appareil qui permet de détecter les empreintes digitales. L'identification et la vérification de ces empreintes est donc très simple. Nous pouvons enregistrer jusqu'à 150 empreintes digitales et il utilise un courant d'alimentation inférieur à 60mA et une tension d'alimentation de 3.3V ; le temps d'entrée d'une image d'empreinte est inférieur à 1seconde et la surface de la fenêtre du lecteur est de 15,3 x 18,2 mm. Celles-ci seront stockées sous forme digitale dans la mémoire flash embarquée. Ce capteur de type optique présente une LED verte ou rouge dans la lentille qui s'allume durant la prise des empreintes. Il utilise 6 câbles dont 4 sont reliés à la carte Arduino à savoir : le câble rouge pour la tension de 5V, le noir pour la masse, le blanc pour la broche 11 de la carte Arduino Mega2560, le vert pour la broche 10. Il est important de mentionner que les câbles blanc et vert ne se relient pas de la même façon sur les autres types de carte Arduino. La figure ci-dessous nous présente les faces avant et arrière du capteur d'empreinte digitale AS608CHIP :

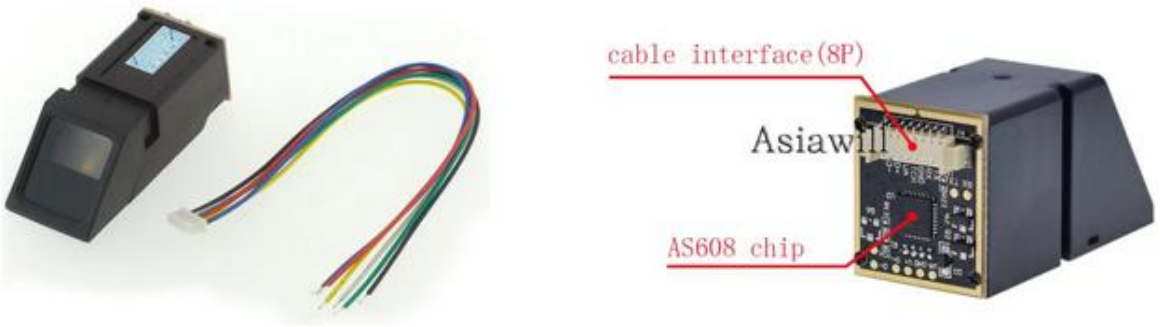


Figure II.3: Capteur optique d'empreinte digitale [19]

- **Le module RFID RC522** : Il est constitué :
  - **De l'étiquette RFID** : représentée ici par une carte blanche et un dispositif bleu (figure II.4). Également nommée étiquette intelligente, étiquette à puce ou tag est un support d'identification électronique. Son utilisation est de ce fait très attractive pour répondre aux exigences en matière de traçabilité. L'étiquette RFID est le support RFID le plus utilisé, il consiste à abriter un numéro de série ou une série de données sur une puce reliée à une antenne. L'étiquette est activée

par un signal radio émis par le lecteur RFID, les étiquettes transmettent les données qu'elles contiennent en retour.

- **Du lecteur RFID** : il permet l'identification sans contact des tags RFID. Il est basé sur le circuit intégré Philips RC522. Il utilise la bande ISM2 13.56MHz, la distance de communication peut aller jusqu'à 6 cm, mais la plupart des modules NFC fonctionnent très bien avec 1cm de distance. La description des broches est représentée dans le tableau ci-dessous :

Tableau N°II : Caractéristiques des broches du lecteur RFID [18]

Symboles	Description	Broches sur la carte Mega2560
3.3V	VCC	3.3V
GND	Ground	GND
RST	Reset	49
IRQ	Interrupt request	-
MISO	Interface SPI	50
MOSI	Interface SPI	51
SCK	Interface SPI	52
SDA	Sélection esclave	53

Figure II.4: Etiquettes RFID utilisées [18]

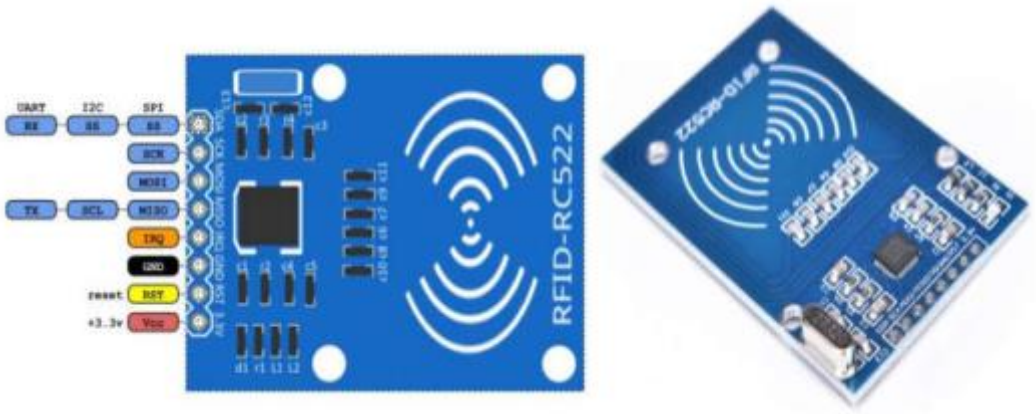


Figure II.5: Lecteur RFID RC522 [18]

- **Module RTC (Real Time Clock) :** celui que nous utiliserons ici est le DS3231, équipé d'une pile (CR2025 à 3V) lui permettant de compter le nombre de tic émis par le quartz et de conserver les informations même en cas de coupure de l'alimentation de l'Arduino. Il est capable de gérer l'heure (heures, minutes, secondes) et la date (jours, mois, année) tout en s'occupant des mois de 30 ou 31 jours, des années bissextiles. Il nous permettra de gérer le pointage des heures d'arrivée et de départ du personnel de l'ENSET d'Ebolowa et des visiteurs ainsi que les dates qui y seront associées pour une meilleure traçabilité. Il est constitué de 4 broches :
  - **SDA** : pour l'enregistrement des données ;
  - **SCL** : pour l'heure ;
  - **GND** : pour la masse ;
  - **VCC** : pour l'alimentation.

Remarque : Le calendrier intégré dans le module DS3231est valable de l'an 2000 à l'an 2100. Il faut juste prévoir une initialisation avant l'utilisation de l'horloge RTC pour avoir la bonne date et la bonne heure.

Figure II.6: Module RTC [18]

- **Un buzzer** : ou un beeper est un composant électronique dont le principal but est de générer un son caractéristique lorsqu'on lui applique une tension (qui peut être de deux types : actif et passif). Il nous servira également d'alerte sonore lorsqu'il y'a intrusion dans un service. Il possède 2 broches dont une est reliée au GND et l'autre à une broche numérique de la carte Arduino. Il est représenté par la figure ci-dessous :

Figure II.7: Buzzer [18]

Remarque : Tous ces composants seront connectés sur la plaque à essai (qui permet de réaliser le prototype d'un circuit électronique) et reliés par des fils de connexion appelés jumpers.

2. **Les outils logiciels**

- **RSTUDIO 1.2.5033** : qui est un logiciel utilisé pour le traitement de données et l'analyse statistique. Dans le cadre de ce projet, nous l'utiliserons pour le traitement et la classification des empreintes digitales dans un réseau de neurones ;

- **IDE Arduino 1.8.12** : logiciel de programmation en C qui permet d'écrire des codes, de les compiler et les envoyer dans le circuit imprimé Arduino. Il nous permettra de définir les différentes fonctionnalités de notre système ainsi que les règles d'accès ;
- **PROTEUS 8.8** : pour la simulation sur le fonctionnement de notre système ;
- **Matlab R2015a** : pour les simulations liées à l'apprentissage du RNA ;
- **Serial Port Monitor 7.0.342** : utilisé pour récupérer les informations du moniteur série qui sont sauvegardées dans la carte SD.

III. Application du perceptron multicouches (PMC) au système par l'algorithme de rétro propagation du gradient

1. Description et algorithme

- **Description**

Comme énoncé dans l'introduction générale, l'objectif principal de ce travail est d'automatiser la gestion des entrées et sorties au sein du campus de l'ENSET d'Ebolowa et les objectifs spécifiques sont :

- L'identification/authentification par empreinte digitale et RFID des utilisateurs ;
- La sauvegarde et la visualisation des informations d'identification/authentification pour une meilleure traçabilité ;
- La gestion des tentatives d'intrusion pour assurer la sécurité au sein du campus.

Notre système sera constitué de :

- **2 modules d'identification / authentification** (par empreinte et carte RFID) : qui permettront d'identifier chaque utilisateur et leur donner ou non accès ;
- **Un module temps et sauvegarde** : qui permettront de gérer la fonction de pointage pour une meilleure traçabilité des mouvements d'entrée/sortie de chacun ;
- **Un module d'alerte** : qui permettra de prévenir la sécurité en cas de tentative d'intrusion

Actuellement, l'intérêt de la classification des empreintes digitales est stimulé par son utilisation dans les systèmes de reconnaissance automatique afin de réduire le temps de recherche et la complexité de calcul. La classification de Henry basée sur la forme globale de l'empreinte considère cinq classes d'empreintes (confère chapitre 1). Plusieurs approches pour la classification ont été développées à savoir : approche basée sur le modèle, la structure, la

fréquence et sur la syntaxe. Celle que nous choisissons d'implémenter ici est l'approche structurelle.

Cette approche utilise l'estimation des crêtes dans une image d'empreinte digitale afin de classifier cette dernière dans l'un des types connus. Plusieurs méthodes telles que le réseau de neurones sont associées à cette approche. La classification est faite à l'aide d'un réseau de neurone MLP qui comprend 192 neurones d'entrée, 20 dans la couche cachée et 5 dans la couche de sortie et le réseau de neurone est entraîné à l'aide de l'algorithme de rétro propagation :

- La couche d'entrée : est la première couche du réseau qui reçoit les valeurs d'entrée ;
- La couche de sortie : est la dernière couche du réseau qui contient autant de neurones que de sorties désirées ;
- Les couches intermédiaires : nommées couches cachées, elles sont situées entre les couches d'entrée et celles de sortie.

Nous travaillerons avec la famille des singularités qui regroupe le core et le delta. La couche d'entrée de notre réseau de neurone sera constituée de 3 neurones qui sont : le nombre de core (Nbcore), le nombre de delta (Nbdelta) et la position du delta par rapport au core (Posdelta). Le nombre de core et de delta variant entre 0 et 2 et la position du delta par rapport au core sera codée comme suit : centre =0, centre =-1, droite =1. La couche de sortie quant à elle sera constituée des 5 classes d'empreintes digitales que nous rappelons ici : Arc (A), Arc Tendu (AT), Boucle à gauche (BG), Boucle à droite (BD), Spire (S). Pour faciliter l'entraînement des données ainsi que les tests, les différentes valeurs attribuées à ces classes seront : A = 0.1 ; AT = 0.2 ; BG = 0.3 ; BD = 0.4 ; S = 0.5.

La structure de notre système de classification d'empreintes digitales se présente comme suit :

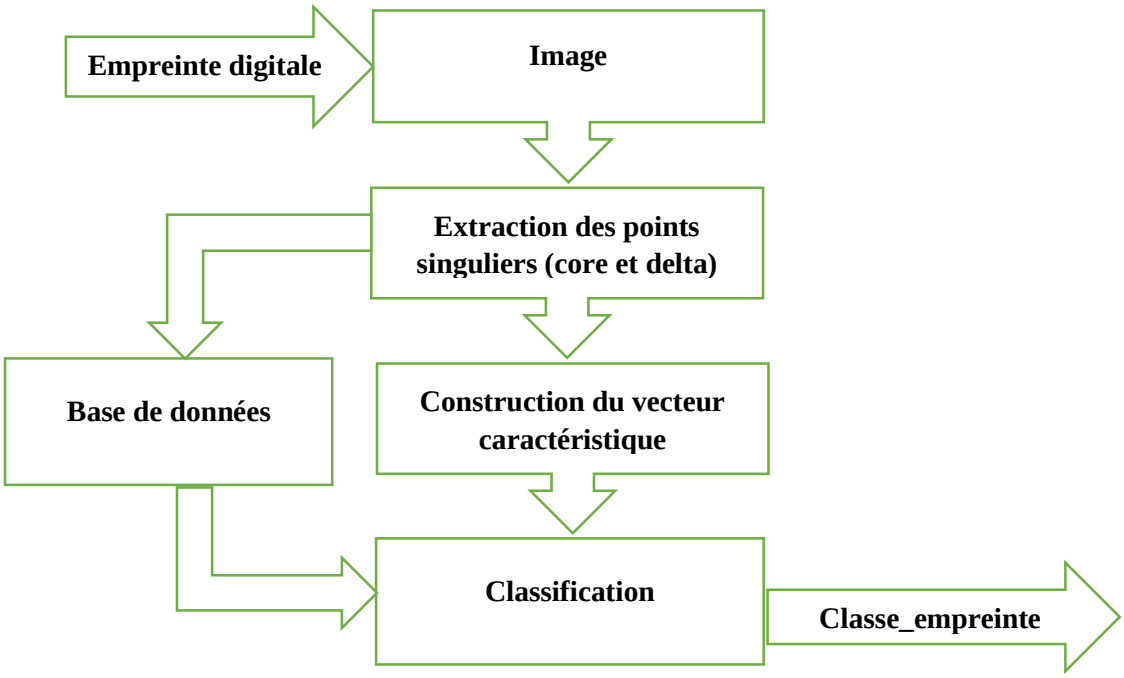


Figure II.8: Structure de classification d'empreintes digitales

- **Algorithme d'apprentissage**

L'algorithme d'apprentissage par rétro propagation du gradient de notre réseau de neurones est présenté plus bas :

Début

Affecter toutes les entrées et sorties

Initialisation des poids synaptiques entre -3 et 1

Répéter

Pour chaque (entrée, sortie) appartenant à l'ensemble d'entraînement

Pour chaque couche du réseau de neurones

Pour chaque neurone de la couche considérée

1- Calcul du gradient local pour les connexions aboutissant aux neurones de sortie
2- Calcul du gradient local pour par descente du gradient pour les couches cachées

Pour chaque connexion entre un neurone i et un neurone j

Calculer la règle d'apprentissage delta généralisée

FinPour

FinPour

FinPour

FinPour

Pour chaque connexion du poids entre un neurone i et un neurone j

Calculer la somme entre le poids des 2 neurones et la règle d'apprentissage delta généralisé

FinPour

Jusqu'à neurone de sortie classifié dans l'une des classes prédéfinies (A, AT, BG, BD, S)

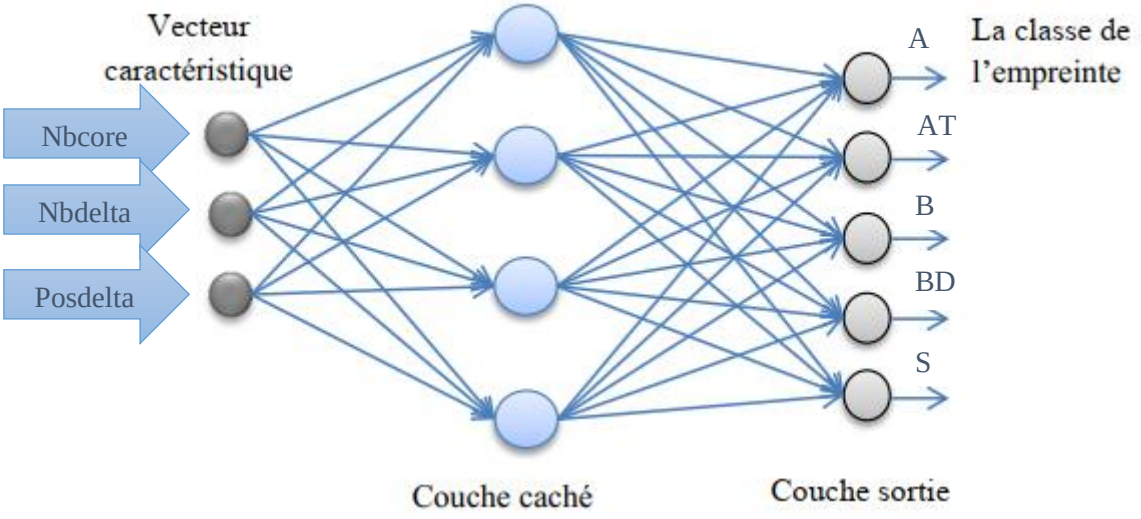


Figure II.9: Modèle du réseau neuronal implémenté

Remarque : Pour la technologie RFID, nous utiliserons le couplage magnétique en champ proche décrit au chapitre 1.

2. Le diagramme des composants et le principe de fonctionnement du système

- **Le diagramme des composants**

L'interaction entre les composants de notre système est représentée comme suit :

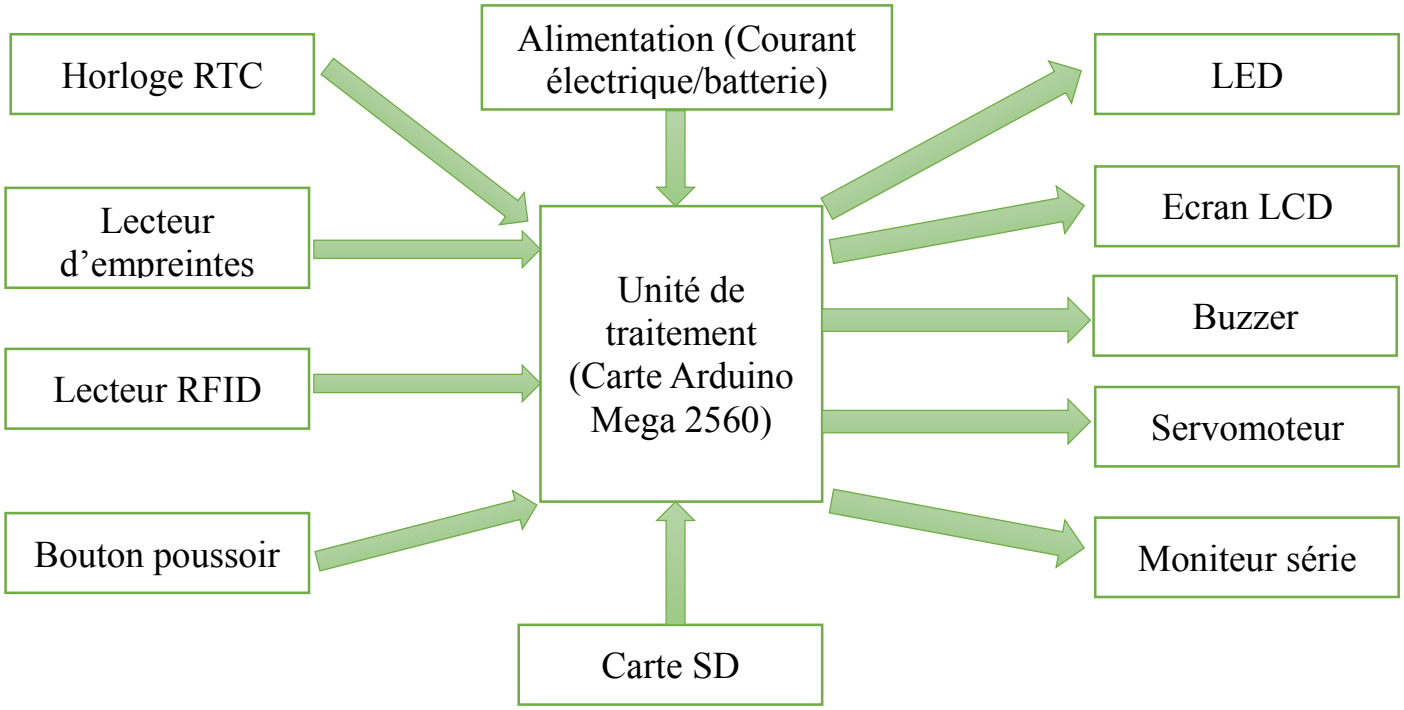


Figure II.10 : Diagramme des composants

- **Principe de fonctionnement du système**

Notre système combiné RFID et biométrie par empreinte digitale fonctionnera comme suit :

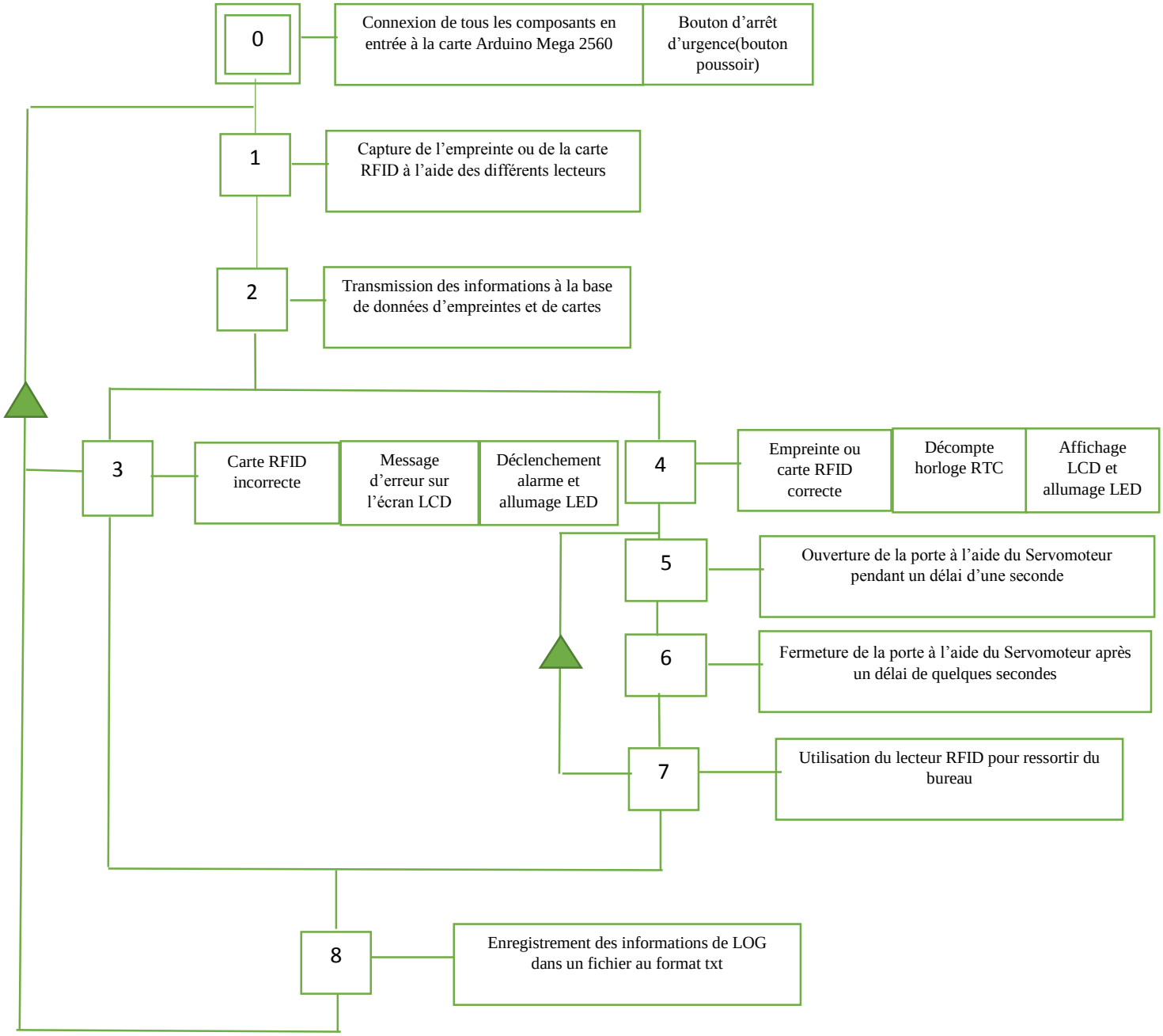


Figure II.11 : Grafcet de fonctionnement de notre système

- **<u>Circuit électronique du système</u>**

Les différents composants ont été reliés au microcontrôleur arduino mega2560 au moyen de plusieurs câbles d'interconnexion :

- **L'écran LCD** : est relié aux broches 2 à 6 ainsi qu'à l'alimentation de 5v et à la masse ;

- **Le lecteur RFID** : représenté ici par un booléen a été relié à la broche 14 (car le logiciel PROTEUS 8.8 ne possédant pas un composant de type RFID)
- **Le lecteur d'empreinte** : de même type que celui de la RFID mais relié à la broche 15 ;
- **L'horloge RTC** : la broche RST reliée au pin 19, SDA à 20 et SCL à 21, l'alimentation à 5V ;
- **Le servomoteur** : relié à la broche 9, à 5V et à la masse ;
- **Le buzzer** : relié à la broche 7 et à la masse ;
- **Le bouton poussoir** : relié avec une résistance (pour réduire le courant électrique dans le circuit) à la broche 6 et à la masse ;
- **Les LED** : connectées avec des résistances reliées aux broches 7 et 8 ainsi qu'à la masse ;

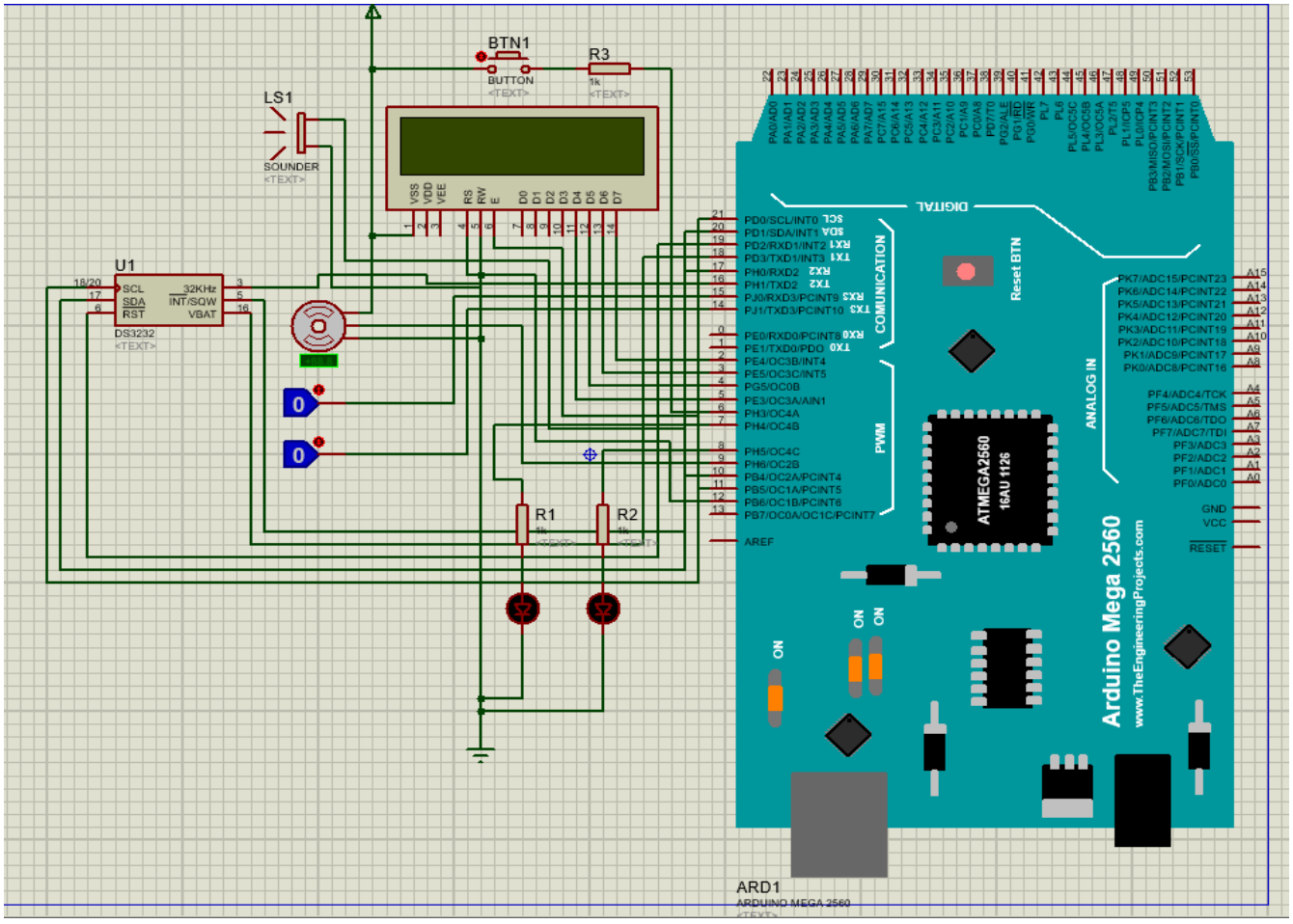


Figure II.12 : Circuit électronique du système

Conclusion

Il a été question dans ce chapitre de présenter la méthodologie de conception de notre système. Tout d'abord, nous avons élaborés un cahier de charges fonctionnel afin de circonscrire le projet et définir les différents services et fonctionnalités. Par ailleurs, les différents outils matériels et logiciels qui seront utilisés pour la réalisation. Nous rappelons ici que l'approche que nous avons utilisée pour la modélisation est celle du PMC basé sur l'algorithme de rétro propagation du gradient pour une meilleure classification de nos empreintes digitales et le couplage magnétique en champ proche fonctionnant à une fréquence de 13.56Mhz pour la RFID.

CHAPITRE III : RESULTATS ET INTERPRETATIONS

Dans ce chapitre, nous présenterons les résultats de nos différentes simulations effectuées.

Aperçu

Introduction

I- Simulation du système neuronal

II- Intégration de l'intelligence sur le matériel

Conclusion

Introduction

La mise en œuvre de ce système combiné biométrie et RFID passe par l'utilisation de plusieurs outils que nous avons présentés dans le chapitre précédant. Par ailleurs, il ne suffit pas de lister ces outils mais également de pouvoir les manipuler d'où l'importance de ce chapitre qui nous permettra de passer par une simulation des réseaux de neurones afin de valider notre méthode d'intelligence artificielle dans les logiciels Matlab et Rstudio présentés précédemment. Les résultats des tests sont très importants pour une meilleure compréhension et utilisation du système par l'utilisateur final.

I. Simulation du système neuronal

1. Architecture du réseau de neurone et prétraitement des données

- **Architecture du réseau de neurone**

Pour dessiner notre architecture sur Matlab, nous allons travailler avec un RNA supervisé de type feedforward à deux couches, avec une fonction de transfert sigmoid dans la couche cachée et une fonction de transfert linéaire dans la couche de production. Le nombre optimal de neurones cachés est mis à 4 :

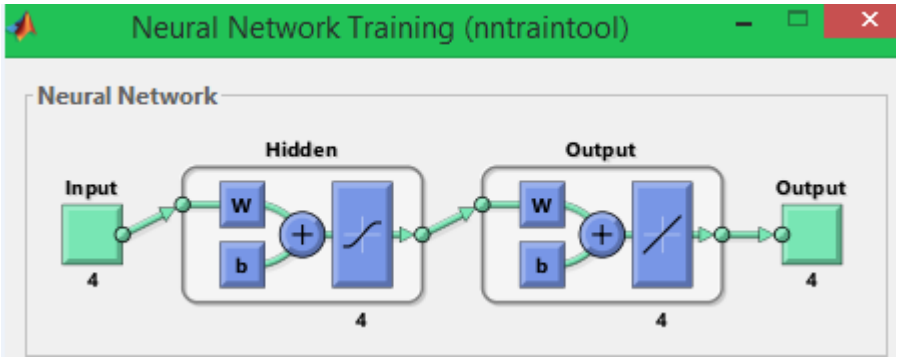


Figure III.1 : Architecture du réseau de neurone

Remarque : Notre base de données d'empreintes est constituée de dix empreintes différentes afin de mieux en extraire les caractéristiques qui sont uniques à chaque individu. Les données d'entrée et de sortie ont été enregistrées dans le fichier « empreintedigitale.xlsx » afin de pouvoir les charger dans le logiciel RSTUDIO.

- **Prétraitement des données d'empreintes**

Dans cette présente étude, on a considéré pour réaliser le modèle de réseaux de neurones trois données d'entrée (Nbcore, Nbdelta, Posdelta) et une donnée de sortie qui est la classe d'empreinte. Le fichier excel qui sera chargé dans le logiciel RSTUDIO se présente comme suit :

	A	B	C	D
1	Nbcore	Nbdelta	Posdelta	Classe_empreinte
2	0	0	-1	0,1
3	0	0	-1	0,2
4	0	0	-1	0,3
5	0	0	-1	0,4
6	0	0	-1	0,5
7	0	0	0	0,1
8	0	0	0	0,2
9	0	0	0	0,3
10	0	0	0	0,4
11	0	0	0	0,5

Figure III.2 : Extraction des points singuliers (core et delta)

2. Entraînement des données d'empreintes et simulations

- **Entraînement des données**

Dans la phase d'entraînement des données, plusieurs commandes ont été saisies dans le logiciel RSTUDIO (confère annexe 3), le réseau de neurone obtenu est le suivant :

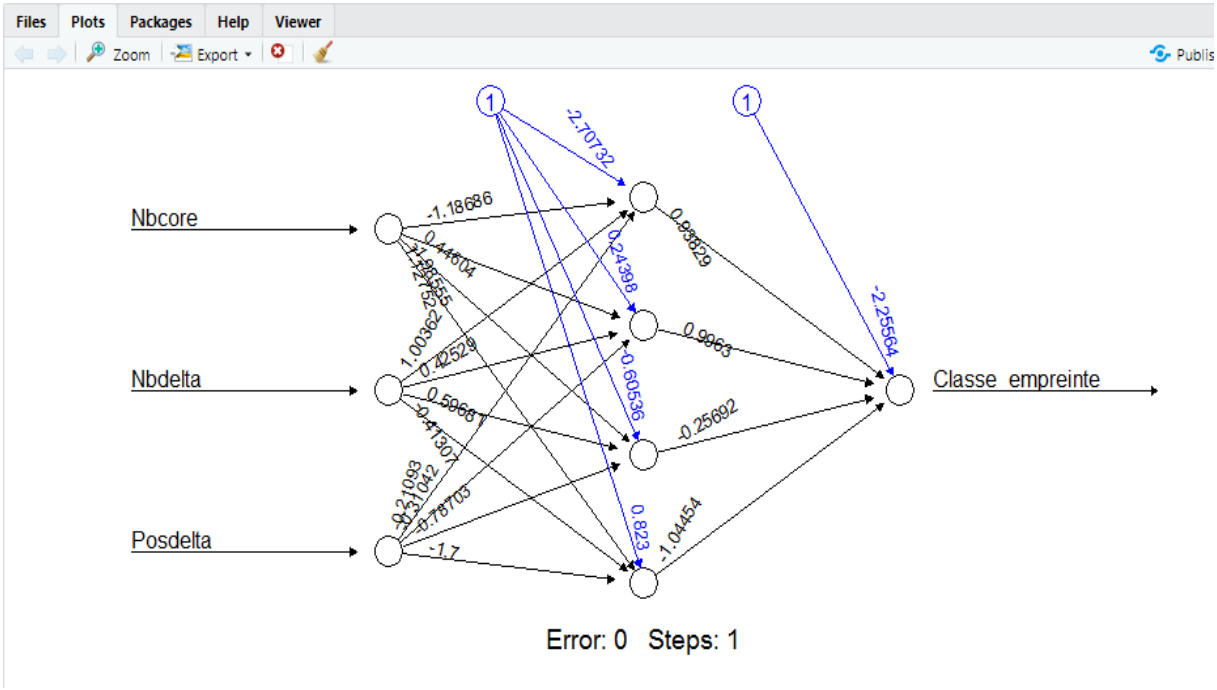


Figure III.3 : Réseau de neurone conçu dans RSTUDIO

La matrice de confusion obtenue se présente comme suit :

```
$result.matrix
                                    [,1]
error                          0.0000000
reached.threshold              0.0000000
steps                          1.0000000
Intercept.to.1layhid1         -2.7073179
Nbcore.to.1layhid1            -1.1868570
Nbdelta.to.1layhid1            1.0036238
Posdelta.to.1layhid1          -0.2109309
Intercept.to.1layhid2          0.2439776
Nbcore.to.1layhid2             0.4460369
Nbdelta.to.1layhid2            0.4252941
Posdelta.to.1layhid2          -0.3104202
Intercept.to.1layhid3         -0.6053598
Nbcore.to.1layhid3            -1.9855474
Nbdelta.to.1layhid3            0.5968077
Posdelta.to.1layhid3          -0.7870287
Intercept.to.1layhid4          0.8229971
Nbcore.to.1layhid4             1.1275153
Nbdelta.to.1layhid4           -0.4130709
Posdelta.to.1layhid4          -1.7000044
Intercept.to.Classe_empreinte -2.2556385
1layhid1.to.Classe_empreinte   0.9382879
1layhid2.to.Classe_empreinte   0.9963014
1layhid3.to.Classe_empreinte  -0.2569236
1layhid4.to.Classe_empreinte  -1.0445392
```

Figure III.4 : Matrice de confusion dans RSTUDIO

Interprétation : Nous avons un RN prenant en compte tous les paramètres définis au départ à savoir 3 neurones en entrée, 4 cachés et la classe d'empreinte qui représente notre neurone de sortie. La matrice de confusion nous présente une erreur à zéro ce qui est un résultat satisfaisant pour l'apprentissage donc les différents cas de faux rejets et de vrais rejets ont été bien appris par le système. Par ailleurs, après calcul avec des données de prédiction de la matrice de confusion, nous obtenons un résultat de 0.94.

- **Simulation dans Matlab**

Les différentes courbes obtenues sont les suivantes :

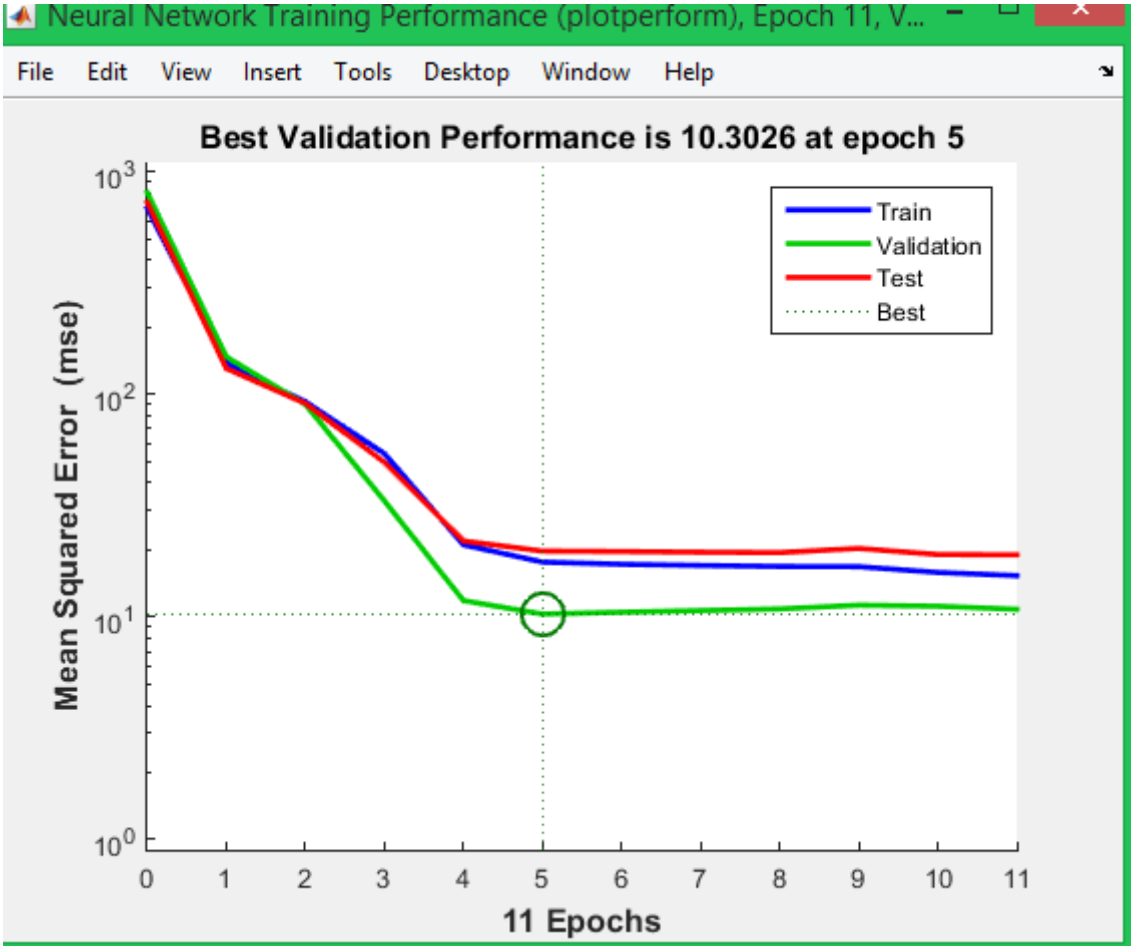


Figure III.5 : Courbe de performance

Interprétation : Un affichage des erreurs d'entraînement, de validation et de test apparaît, comme indiqué dans la figure III.5. On remarque que le résultat est raisonnable à cause des considérations suivantes :

- Pas de sur-ajustement significatif obtenu par l'itération 5 (où on a obtenu la meilleure performance de validation qui est de 10.3026) ;
- Les ensembles test et d'entraînement ont des caractéristiques semblables.

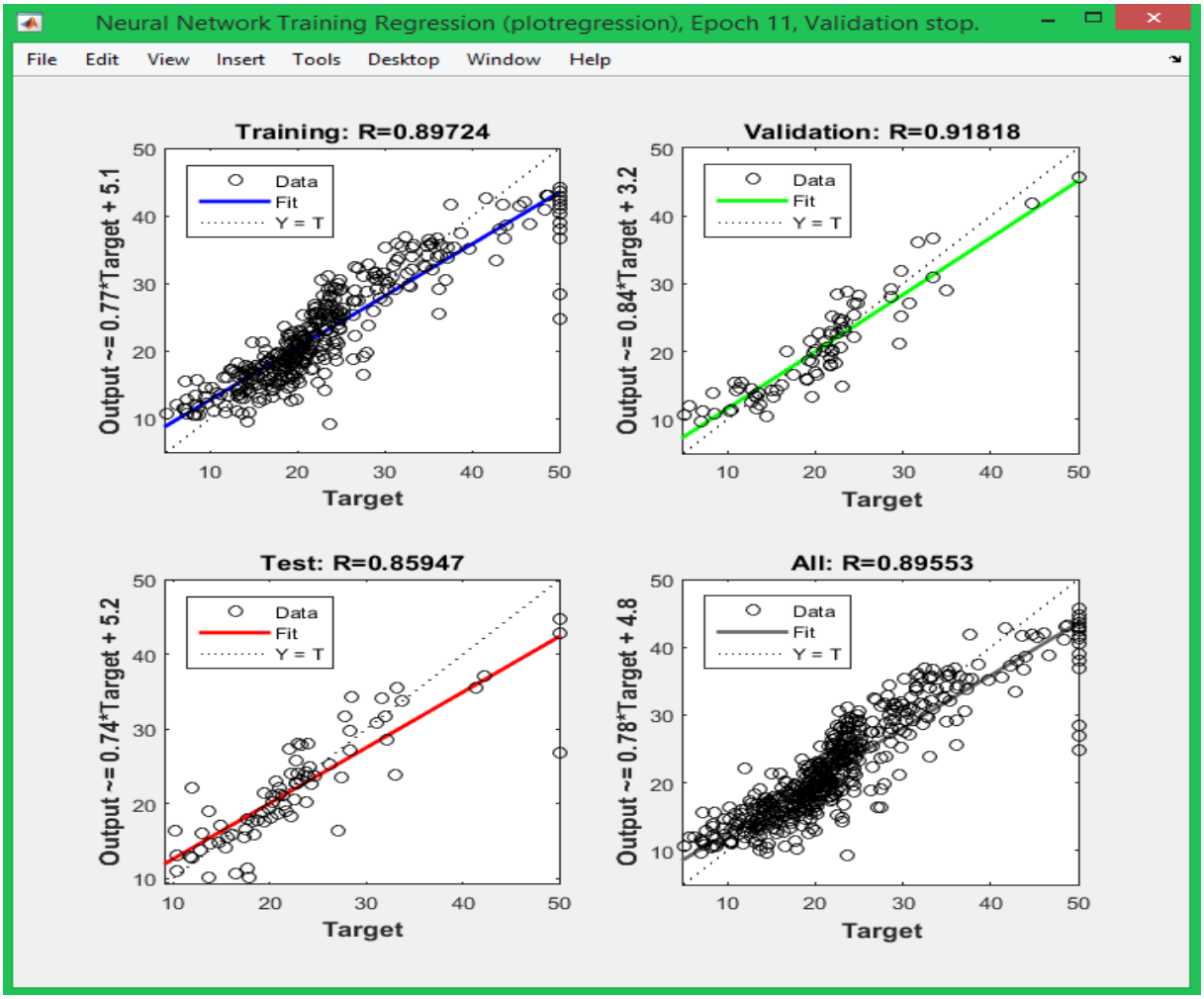


Figure III.6 : Droites de régression

Interprétation : La Figure III.6 montre les résultats des différentes parcelles de régression. Si le coefficient de corrélation R est à 0,8, il est généralement décrit comme solide, tandis qu'un coefficient de corrélation inférieure à 0,5 est décrit comme faible. Ces valeurs peuvent varier en fonction du type des données en cours d'examen. Les parcelles de régression affichent les sorties du réseau par rapport à des cibles pour des ensembles d'entraînement, de validation et de test. Dans notre cas, l'ensemble d'entraînement a un R=0.89, l'ensembles de validation 0.91 l'ensemble de test 0.85. La parcelle de régression total R (All) est égale à 0.89 ce qui est une bonne valeur pour l'entraînement.

- **L'entraînement** consiste tout d'abord à calculer les pondérations optimales des différentes liaisons, en utilisant un échantillon. Elle se passe par rétro propagation : on insère des valeurs des cellules d'entrée et en fonction de l'erreur obtenue en sortie (le delta), on corrige les poids accordés aux pondérations. Lors de l'apprentissage de nos données nous remarquons bien que la courbe de régression est presque confondue avec la première bissectrice ;
- **Les tests** concernent la vérification des performances d'un réseau de neurones hors échantillon et sa capacité de généralisation, la validation est parfois utilisée lors de l'apprentissage. Une fois le réseau calculé, il faut toujours procéder à des tests afin de vérifier que notre réseau réagit correctement.

Les matrices de confusion obtenues sont les suivantes :

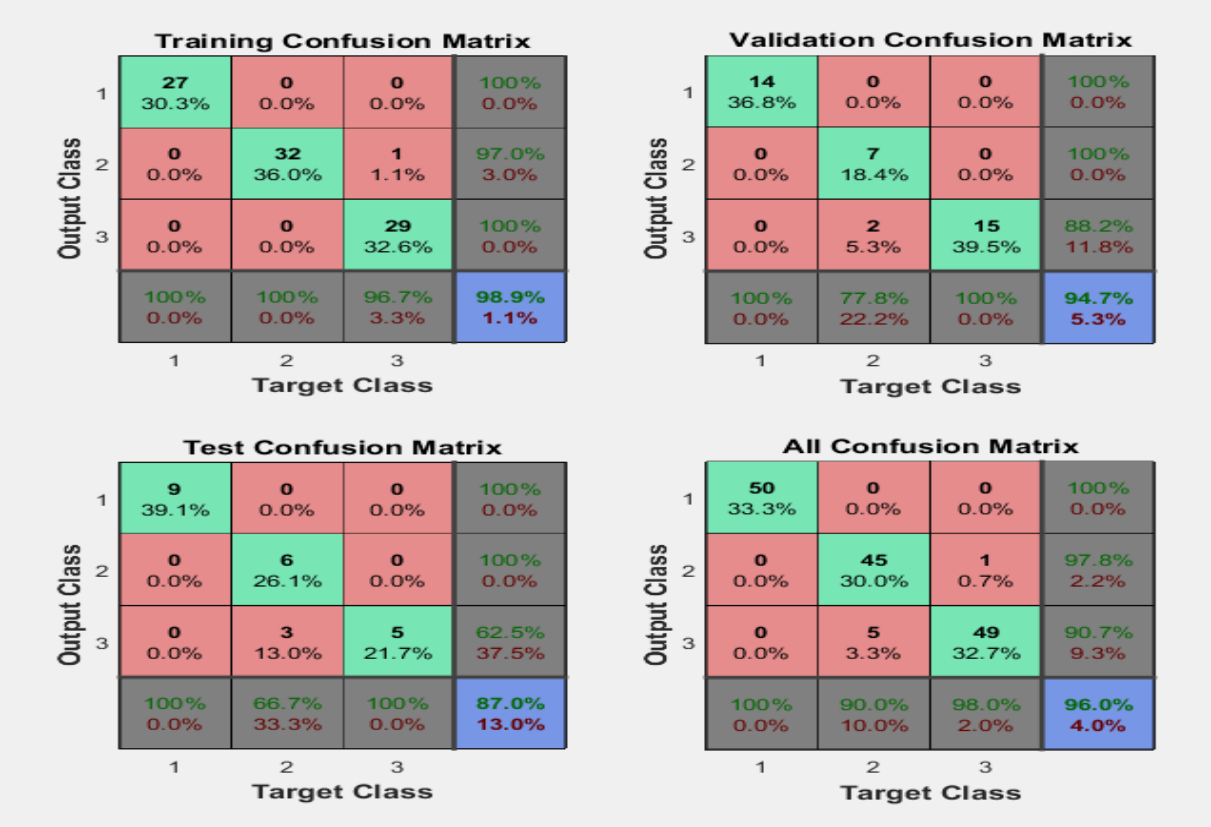


Figure III.7 : Matrices de confusion sur Matlab

Interprétation : La matrice de confusion est considérée comme bonne lorsqu'on a un pourcentage supérieur ou égal à 80%. Dans notre cas, la matrice totale nous présente un résultat

des données d'entraînement, de test et de validation à 96%, ce qui n'est pas loin du résultat obtenu dans Rstudio. Nous pouvons donc conclure que notre RNA est performant.

II. Intégration de l'intelligence sur le matériel

1. Simulation sur Proteus

- **Etat initial du système**

Lorsque le système est au repos, il se présente comme suit :

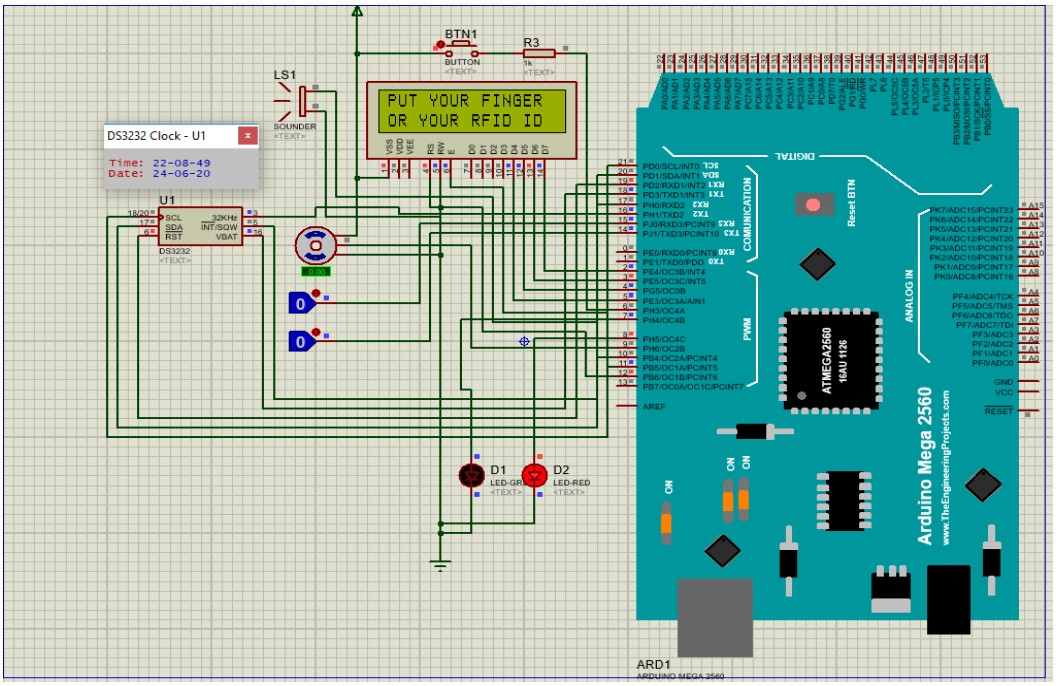


Figure III.8 : Etat initial du système

- **Authentification par empreinte digitale**

Lorsque l'utilisateur pointe par empreinte, le message sur l'écran LCD lui souhaite la bienvenue, le servo moteur ouvre la porte, l'horloge RTC enregistre l'heure et la date, la LED verte s'allume et les informations d'authentification et d'identification sont enregistrées dans la carte SD :

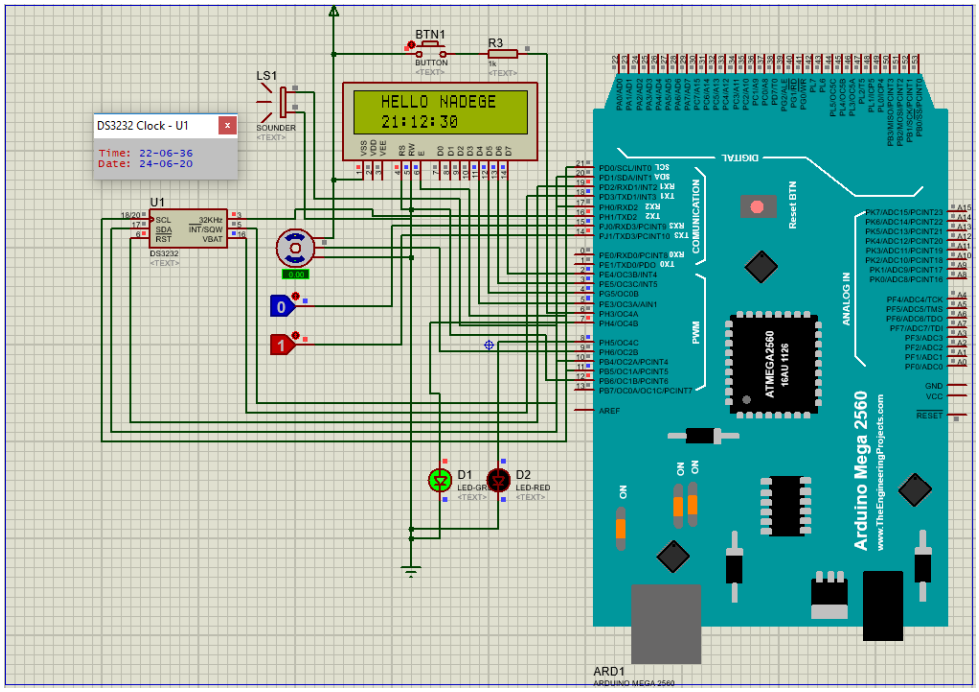


Figure III.9 : simulation de l'empreinte digitale

- **Authentification par carte RFID**

Le système réagit de la même façon qu'avec l'empreinte digitale :

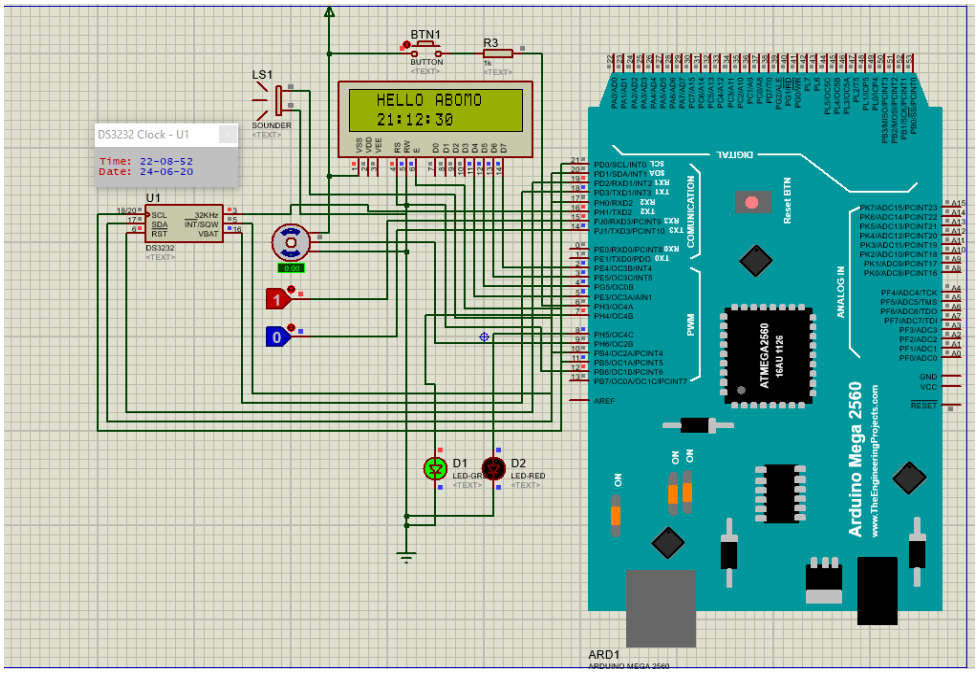


Figure III.10 : simulation de la carte RFID

2. Implémentation sur Arduino

Il s'agit de vérifier notre simulation sur du matériel de façon concrète. Cette implémentation va se faire sur une carte arduino mega2560. Il est question d'implémenter le PMC par l'algorithme de rétro propagation du gradient sur cette carte. Ici l'arduino récupère les informations liées aux empreintes et cartes RFID à l'aide des différents lecteurs prévus à cet effet, sauvegarde les informations dans une carte SD et donne une traçabilité sur le temps à l'aide du module RTC.

Remarque : Un extrait du programme en C Arduino se trouve en annexe 4.

Conclusion

Il a été question dans ce chapitre de présenter les différents résultats de simulation de notre travail et d'en interpréter les résultats. Il en ressort que l'intelligence artificielle utilisée dans notre système respecte tous les critères énumérés dans le CDCF. Par ailleurs, les résultats obtenus lors de l'apprentissage dans RSTUDIO montrent que le résultat obtenu dépend du taux d'apprentissage choisi.

CONCLUSION GENERALE ET PERSPECTIVES

L'objectif de ce mémoire est la conception d'un système automatique de gestion des entrées et sorties au sein du campus de l'ENSET d'Ebolowa utilisant les techniques biométrique et RFID basé sur le PMC par l'algorithme de rétro propagation du gradient. Cette approche nous a permis d'utiliser l'apprentissage supervisé dans notre système embarqué pour gérer les identifications/ authentifications du personnel, enseignant et visiteurs dans le campus de cette école. Il est composé de plusieurs modules dont : le module d'identification/authentification (empreinte digitale et carte RFID), le module de gestion du temps (pour avoir une meilleure visibilité sur le pointage des différents utilisateurs), le module d'alerte afin de gérer les cas de tentative d'intrusion et le module de sauvegarde pour une meilleure traçabilité des informations.

Il est donc question de considérer toutes les caractéristiques singulières qu'on retrouve sur une empreinte afin d'éliminer tous les cas de faux rejets par le système. L'atteinte de notre objectif a nécessité l'utilisation de plusieurs outils logiciels et matériels de l'IA tels que les réseaux de neurones par rétro propagation du gradient pour la mise en œuvre et la simulation (qui nous a permis de valider nos hypothèses de départ) du système embarqué.

Néanmoins, il existe des points à gérer l'entraînement des données d'empreintes digitales, il s'agit par exemple des cas de brûlure, de malformations dues à des accidents.

Comme perspectives à cette recherche, nous souhaitons :

- Réaliser ce système en temps réel en intégrant d'autres fonctionnalités telles que : la connexion de plusieurs lecteurs d'empreintes et de cartes rfid à une seule unité de commande, le calcul automatique des heures de départ et heures d'arrivée avant extraction dans un fichier excel ;
- Intégrer la logique floue à ce système afin de le rendre encore meilleur ;
- Prendre en compte les cas de brûlure, de malformations dues à des accidents ;
- Avoir un serveur de stockage des données en ligne afin de permettre à la cellule informatique d'avoir les informations en temps réel sur leur smartpone quel que soit leur position géographique ;

ANNEXES

Annexe 1 : Evaluation financière du système

Matériels	Quantité	Prix unitaire (F CFA)	Prix total (F CFA)
Bouton poussoir	1	500	500
Breadboard	2	2000	4000
Buzzer	1	500	500
Carte Arduino Mega 2560	1	15500	15500
Carte RFID vierge	2	1000	1000
Connecteur 9V	1	500	500
Ecran LCD	1	5000	5000
Jumpers mâle/femelle	1	2000	2000
Jumpers mâle/mâle	1	2000	2000
Module empreintes digitales	1	25000	25000
Module RFID	1	5500	5500
Module RTC	1	3000	3000
Piles 9V	1	1000	1000
Servo moteur	1	3000	3000
LED	2	200	400
Shield data SD card	1	5000	5000
TOTAL (FCFA)			**73900**

Annexe 2 : Quelques images d'empreintes traitées dans Matlab

Les images ci-dessous représentent des images d'orientation de 3 types d'empreintes traitées dans Matlab avant extraction des points singuliers (core et delata), les différents types de la gauche vers la droite sont : Arc tendu, Arc et Spire

Annexe 3 : Commandes d'apprentissage dans RSTUDIO

```
> getwd();
[1] "F:/ENSET EBWA/5EME ANNEE/MEMOIRE DE FIN DETUDE/CHAP2 OUTILS UTILISES"
> install.packages("readxl");
WARNING: Rtools is required to build R packages but is not currently installed. Please download and install the appropriate version o
f Rtools before proceeding:

https://cran.rstudio.com/bin/windows/Rtools/
Installing package into 'C:/Users/user/Documents/R/win-library/3.6'
(as 'lib' is unspecified)
essai de l'URL 'https://cran.rstudio.com/bin/windows/contrib/3.6/readxl_1.3.1.zip'
Content type 'application/zip' length 1529121 bytes (1.5 MB)
downloaded 1.5 MB

package 'readxl' successfully unpacked and MD5 sums checked

The downloaded binary packages are in
        C:\Users\user\AppData\Local\Temp\RtmpsZyTMF\downloaded_packages
> library("readxl");
Warning message:
le package 'readxl' a été compilé avec la version R 3.6.3
> empreinte<- read_excel("empreintedigitale.xlsx",sheet=1);
> str(empreinte);
Classes 'tbl_df', 'tbl' and 'data.frame':       165 obs. of  4 variables:
 $ Nbcore          : num  0 0 0 0 0 0 0 0 0 0 ...
 $ Nbdelta         : num  0 0 0 0 0 0 0 0 0 0 ...
 $ Posdelta        : num  -1 -1 -1 -1 -1 0 0 0 0 0 ...
 $ Classe_empreinte: chr  "0.1" "0.2" "0.3" "0.4" ...
> empreinte$Nbcore<-(empreinte$Nbcore-min(empreinte$Nbcore))/(max(empreinte$Nbcore)-min(empreinte$Nbcore)) ;
> empreinte$Nbdelta<-(empreinte$Nbdelta-min(empreinte$Nbdelta))/(max(empreinte$Nbdelta)-min(empreinte$Nbdelta)) ;
> empreinte$Posdelta<-(empreinte$Posdelta-min(empreinte$Posdelta))/(max(empreinte$Posdelta)-min(empreinte$Posdelta)) ;
> empreinte$Classe_empreinte<-(empreinte$Classe_empreinte-min(empreinte$Classe_empreinte))/(max(empreinte$Classe_empreinte)-min(empre
inte$Classe_empreinte)) ;
```

Annexe 4 : Extrait du programme Arduino

```
//inclusion des différentes bibliothèques du projet
#include <DS3231.h>// librairie de l'horloge rtc de type DS3231
#include "RTClib.h" // librairie de l'horloge rtc
#include <Servo.h>// librairie du servo moteur
#include <Adafruit_Fingerprint.h> // librairie de l'empreinte digitale
RTC_DS3231 rtc;// déclaration de l'horloge rtc
SoftwareSerial mySerial(10, 11);//connexion des broches du module d'empreinte: pin10 pour le fil vert et pin 11 pour le balnc
#include <Wire.h> //librairie Ecran LCD
#include <LiquidCrystal_I2C.h> // librairie de l'écran LCD
#include <SPI.h>
#include <MFRC522.h>//importation pour les librairie de la RFID
LiquidCrystal_I2C lcd(0x27,16,2); //déclaration de l'écran LCD 16 colonnes et 2 lignes
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);//déclaration du module d'empreinte digitale
//declararion des variables pour la RFID et les empreintes digitales
//definition des broches du module RFID
#define RST_PIN 49
#define SS_PIN 53
DS3231 monRTC(SDA, SCL);
MFRC522 module_rfid(SS_PIN, RST_PIN);
//declaration du servo moteur commandé par le lecteur d'empreinte et le module RFID
Servo myservo;
DateTime now;
// fonction permettant de démarrer les différents modules
void setup()
{
lcd.init();                    // initialisation de l'écran lcd
lcd.setCursor(0,0);// affichage de démarrage du système sur la première colonne première ligne
lcd.print("BIENVENUE A");
lcd.setCursor(0,1);//affichage de démarrage du système sur la première colonne deuxième ligne
lcd.print("L'ENSET EBWA");
lcd.backlight();
myservo.attach(8);// broche sur laquelle le servo moteur est connecté sur la carte arduino
```

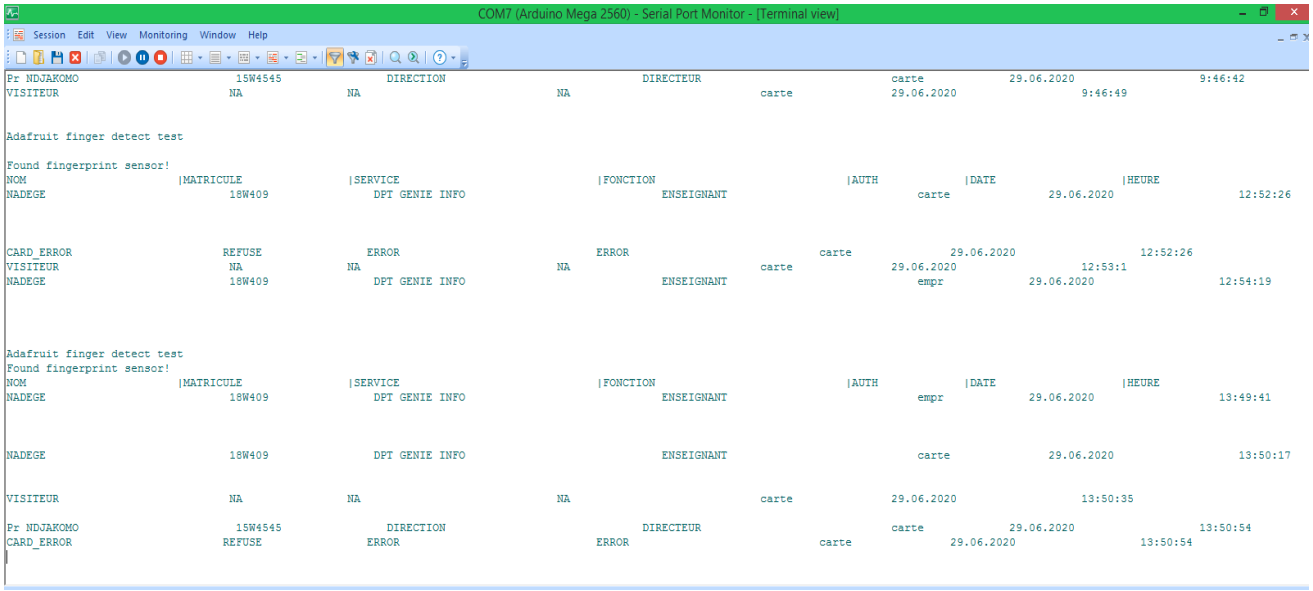
```
void loop()
{
now = rtc.now();// le module rtc prend en compte les informations du système: date et heure
getFingerprintIDez();// fonction du lecteur d'empreinte
gestionRFID(); // fonction du lecteur d'empreinte
delay(50); //délai de 50ms
}
uint8_t getFingerprintID() {
uint8_t p = finger.getImage();// récupération de l'image d'empreinte
// capture de l'image d'empreinte
switch (p) {
case FINGERPRINT_OK:
Serial.println("Image taken");
break;
case FINGERPRINT_NOFINGER:
Serial.println("No finger detected");
return p;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Communication error");
return p;
case FINGERPRINT_IMAGEFAIL:
Serial.println("Imaging error");
return p;
default:
Serial.println("Unknown error");
return p;
if(finger.fingerID==1){

lcd.setCursor(0,0);
lcd.print("BONJOUR NADEGE "); // affichage sur l'écran LCD lorsque l'empreinte ayant pour ID 1 est reconnue par le lecteur d'empreinte
heure = String(now.hour());// récupération de l'heure du système par le rtc
minute_init = String(now.minute());// récupération des minutes du système par le rtc
```

La liste des informations sauvegardées dans la carte SD se présente comme suit :

A	B	C	D	E	F	G	H
NOM	|MATRICULE	|SERVICE		|FONCTION	|AUTH	|DATE	|HEURE
VISITEUR	NA	NA		NA	carte	23.06.2020	02:20:04
NADEGE	18W409	DPT GENIE INFO		ENSEIGNANT	carte	23.06.2020	02:20:10
Pr NDJAKOMO	15W4545	DIRECTION		DIRECTEUR	carte	23.06.2020	02:20:16
CARD_ERROR	REFUSE	ERROR		ERROR	carte	23.06.2020	02:20:17

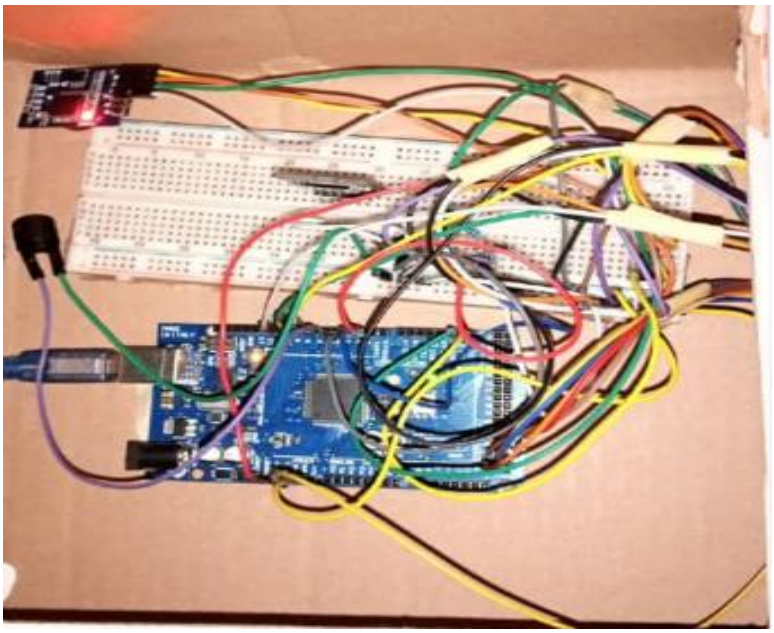
<u>Annexe 5</u> : Interface des informations sur Serial Port Monitor



<u>Annexe 6</u> : Dispositif final

Le dispositif final est représenté ci-dessous par la vue de face et le câblage :


PUT YOUR FINGER
OR YOUR ID CARD
ENSET
SYSTEME DE CONTRÔLE D'ACCES PAR BIOMETRIE ET RADIOFREQUENCE: CAS DE L'ENSET D'EBOLOWA
Réalisé par:
ABOMO ESSINDI Jeanne Nadège
Filière:
Informatique Industrielle 5
Promotion 2020



REFERENCES

[1] SIR FRANCIS GALTON, « Personal identification and description », Nature, 28 juin 1888 ;

[2] Julie M. GAUTHIER, « Cadre juridique de l'utilisation de la biométrie au Québec : sécurité et vie privée », Avril 2014 ;

[3] I.H. JACOBY & A.J. GIORDANO, « Hand ID system », US Patent n° 3576537, 1972 ;

[4] A.K. JAIN, A. ROSS et S. PANKANTI, « A prototype hand geo metry-based verification system », 2nd International Conference on Audio and Video-based Biometric Person Authentication (AVBPA), Washington D.C., pp. 166-171, March 22-24, 1999 ;

[5] P. MACGREGOR et R. WELFORD, « Veincheck: imaging for security and personnel identification », Advanced Imaging, Vol. 9, n°7, pp 52-56, 1991 ;

[6] J.M. CROSS, C.L. SMITH, « Thermographic imaging of the subcutaneous vascular network of the back of the hand for biometric identification », Security Technology, 1995. Proc. Institute of electrical and electronics engineers 29th annual 1995 international carnahan conference on (1995) ;

[7] T. ALLISON, G. GINTER et al., « Faces recognition in human extrastriate cortex », Journal of Neurophysiology, Vo.71, 1994 ;

[8] T. KOHONEN, « Associative memory : a system theoretic approach », Berlin Springer-Verlag Ed., 1977 ;

[9] http://www.retina-scan.com/retina_scan_technology.htm ;

[10] A. PINZ, S. BERNOGGER, P. DATLINGER et A. KRUGER, « Mapping the human retina », IEEE Transactions on Medical Imaging, vol.17, n°4, August 1998 ;

[11] Martin GUESPEREAU, « Les systèmes d'identification par radiofréquence, évaluation des impacts sanitaires », Décembre 2008 ;

[12] ZIANI-KERARTI Samir, KADI Oussama « Etude et conception d'un système de présence automatique par RFID », 2014 ;

[13] C.L. Tisse, L. Torres, L. Martin et M. Robert, « Systèmes biométriques pour la vérification d'individu. Un exemple : l'iris », Juillet 2004

[14] Oubira Bilal, Djoualil Abdel halim, « Etude et conception d'un système d'accès sécurisé par la technologie RFID », Juillet 2019 ;

[15] Jean-Pierre HAUET, « L'identification par radiofréquence, techniques et perspectives », Novembre 2006 ;

[16] BENCHENNANE Ibtissam, « Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus », 2016 ;

[17] Yassin Belaizi, « Etude et conception d'un capteur RFID passif en bande UHF : application à l'agroalimentaire », Mai 2019 ;

[18] https://www.cours-gratuit.com/

[19] https://www.timamady.com/index.php?main_page=product_info&products_id=167213

[20] R. Belguechi, E.Cherrier, T.Le-goff et C.Rosenberger, « Etude de la robustesse d'un système de biométrie révocable», 2011

[21] Christel-Loïc TISSE, Lionel MARTIN, Lionel TORRES, Michel ROBERT « Système automatique de reconnaissance d'empreintes digitales. Sécurisation de l'authentification sur carte à puce », Décembre 2006

[22] Florent Perronin, Jean-Luc DUGELAY, « Introduction à la biométrie, authentification des individus par traitement audio-visuel » ; 2007

[23] https://f-leb.developpez.com/tutoriels/arduino/bus-i2c/

[24] DIB Fouad, « Identification des personnes par le réseau veineux de la main », 2013

[25] HADDAD ZEHIRA, « Système automatique de classification pour la reconnaissance des empreintes digitales », 2015

[26] SADAOUI FETHIA, BENKADDOUR KAMEL, HAMMANI ZINEB, « Application des réseaux de neurones artificiels à l'identification biométrique », 2015