REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE.

MINISTERE D'ENSEIGNEMENT SUPERIEUR

ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE -YAHIA FARES - MEDEA
FACULTE DES SCIENCES

DEPARTEMENT DE MATHEMATHIQUES ET INFORMATIQUE

PROJET DE FIN D'ÉTUDE :
PRÉSENTÉ POUR L'OBTENTION DU DIPLÔME DE
MASTER EN INFORMATIQUE

SPÉCIALITÉ : Ingénierie de Systèmes et Technologies de Web

Thème :

Conception et mis en œuvre d'une application de contrôle biométrique d'identité pour autoriser l'assistance à un examen au sein d'université de Médéa

Préparé et Présenté par :

- **Ben bekhti Messaouda**
- **Khaldi Hamid**

Encadreur :

- **Mr Boudjebbour Karim**

Co-Encadreur :

- **Mr Toubal El Bahi**

2021/2022

Dédicace :

A mes très chers parents

- *A **Mon père que** dieu lui fasse miséricorde.*
- *A mon exemple éternelle, mon soutien moral et source de joie et bonheur qu'elle n'a jamais cessée de m'encourager, qui m'a soutenu durant ces années d'études, **Ma Mère** qui a fait beaucoup pour moi que Dieu la protèges est la garde.*
- ***A** mes chères **sœurs** « Hanane Roukia Fayza Fatima Zineb et Meriem ».*
- ***A** mes chers **frères «** Ramag et Lakhdar **»***
- ***A** mes **oncles** mes **grands parents** et Ceux qui ont partagé avec moi tous les moments d'émotion lors des années d'études. Ils m'ont chaleureusement supporté et encouragé tout au long de mon parcours.*
- ***A** ma famille, mes nièces, mes neveux, mes proches et à ceux qui me donnent de l'amour.*
- ***A** mon binôme « Hamid »*
- ***A** mon amis « abde nour » merci énormément*
- ***A** tous mes amis qui m'ont toujours encouragé, et à qui je souhaite plus de succès.*

***M**erci* **BEN BEKHTI MESSAOUDA**

Dédicace :

A mes très chers parents

- *A la source de mes efforts qu'il me souhaite le plus de succès et de développement* ***Mon père .***
- *A mon exemple éternelle, mon soutien moral et source de joie et bonheur qu'elle n'a jamais cessée de m'encourager, qui m'a soutenu durant ces années d'études,* ***Ma Mère*** *qui a fait beaucoup pour moi que Dieu la protèges est la garde.*
- ***A*** *ma chère* ***sœurs*** *«****Douaa****».*
- ***A mes chers frères.***
- ***A*** *ma famille, mes proches et à ceux qui me donnent de l'amour.*
- ***A*** *ma binôme « Messaouda»*
- ***A*** *tous mes amis qui m'ont toujours encouragé, et à*

  qui je souhaite plus de succès.

- ***A*** *tous travailleurs municipaux*

- ***A*** *Le conseil municipal, a le maire*

M*erci*

KHALDI HAMID

Remerciement :

Tout d'abord nous remercions le grand Dieu pour la santé, l'intelligence, le courage qu'Il nous avons accordé tout au long de nos cursus en particulier durant la période de ce projet. Notre profonde gratitude et sincères remerciements vont à notre Encadreur M^r^ Boudjebbour Karim qui nous a fait l'honneur de diriger ce travail pour sa disponibilité, sa positivité et sa motivation, et surtout pour la confiance qu'il nous avons toujours accordé. Nous adressons nos remerciements aux membres des jurys, devant qui nous avons l'honneur d'exposer notre travail, et qui ont pris la peine de lire ce mémoire pour juger son contenu. Nous remercions notre Co-Encadreur monsieur M^r^ Toubal El Bahi, On tient à remercier tous les enseignants qui ont assuré notre formation.

Enfin, on exprime notre reconnaissance envers toute notre famille, et tous ceux qui ont contribué de prés ou de loin pour réaliser ce travail.

Résumé

Résumé :

Les empreintes digitales sont une forme biologique de la main des humains, c'est une science qui utilise les caractéristiques physiques et biologiques des individus pour déterminer leur identité. De nos jours, la nécessité d'apprendre à connaître les gens de manière fiable est devenue un gros problème. Là où les méthodes traditionnelles (carte à puce, mot de passe) ont montré leurs limites (falsification, perte), la biométrie tente de vérifier ou d'identifier un individu à partir de caractéristiques biologiques (ex. ADN), comportementales (ex. voix) ou morphologiques (ex. empreintes digitales) sans erreur. L'un des endroits où les systèmes de reconnaissance sont nécessaires est l'environnement universitaire dans lequel circulent des personnes qui partagent un espace commun, principalement les étudiants. Tous les étudiants doivent passer des tests pour évaluer leurs connaissances. Cependant, certains d'entre eux tentent de tricher de diverses manières, notamment en se faisant remplacer (surtout dans les épreuves du rattrapage) ou en changeant le lieu d'exam. Notre travail consiste à mettre en place un system de contrôle d'identité à base d'empreinte digitale pour assurer des examens sans tricherie au sein de l'université de Médéa.

Mots clés : empreintes digitales, biométrie, contrôle d'identité,

Abstract:

Fingerprinting is a biological form of human hand, it is a science that uses physical and biological characteristics of individuals to determine their identity. Nowadays, the need to get to know people reliably has become a big problem. Where traditional methods (smart card, password) have shown their limitations (forgery, loss), biometrics attempts to verify or identify an individual based on biological (e.g. DNA), behavioral (e.g. voice) or morphological (e.g. fingerprints) characteristics without error. One of the places where recognition systems are needed is in the university environment where people who share a common space, primarily students, move around. All students must take tests to assess their knowledge. However, some of them try to cheat in various ways, such as by being replaced (especially in resit exams) or by changing the exam location. Our work consists in setting up an identity control system based on fingerprints, to ensure exams without cheating within the University of Medea.

Keywords : fingerprints, biometrics, identity control

ملخص:

بصمات الأصابع هي شكل بيولوجي لليد البشرية، وهي علم يستخدم الخصائص الفيزيائية والبيولوجية للأفراد لتحديد هويتهم. في هذه الأيام، أصبحت الحاجة إلى التعرف على الناس بشكل موثوق أمرًا كبيرًا. حيثما أظهرت الطرق التقليدية (البطاقة الذكية، كلمة المرور) حدودها (التزييف، الضياع)، تحاول القياسات الحيوية التحقق من هوية الفرد أو تحديده على أساس بيولوجي (مثل الحمض النووي) ، أو سلوكي (مثل الصوت) أو شكلي (مثل بصمات الأصابع) دون أخطاء. من الأماكن التي تكون فيها أنظمة التعرف ضرورية هي

البيئة الجامعية التي يتنقل فيها الأشخاص الذين يتشاركون مساحة مشتركة، وخاصة الطلاب. يجب على جميع الطلاب إجراء اختبارات لتقييم معرفتهم. ومع ذلك، يحاول بعضهم الغش بطرق مختلفة، بما في ذلك الاستبدال (خاصة في الاختبارات العلاجية) أو تغيير مكان الامتحان. تتمثل مهمتنا في إنشاء نظام للتحكم في الهوية يعتمد على بصمات الأصابع لضمان إجراء الامتحانات دون الغش داخل جامعة المدية.

الكلمات المفتاحية: بصمات الأصابع، القياسات الحيوية، التحقق من الهوية،

liste des abréviations:

ADN : Acide Désoxyribonucléique

DNA :deoxyribonucleic acid

CN : connectivité

Bdd : base de données

Msg : message

EFS : examen fin de semestre

RFS : rattrapage fin de semestre

SUP : supérieure

IOS: iPhone Operating System

PIN :Personal Identification Number

MLD : Modèle Logique des Données

PHP : Hypertext Preprocessor

Num : numéro

MAJ : mettre à jour

sommaire

Liste des figures
Liste des tableaux
Introduction générale……...…….....……...01

Chapitre I : la biométrie et la reconnaissance des empreintes digitales

1.Introduction.....….....03
2.La biométrie…….……..……..…….…….…….....03
2.1.Définition de biométrie……..……..…….....…….....….03
2.2.Architecture de biométrie.....…….....….04
2.2.1.Module d'apprentissage.....……..……04
2.2.2. Module de reconnaissance .....…….……04
2.2.3.Module d'adaptation …….....……...……05
2.3.Les moyens biométrique……..…….....……...…..……05
2.3.1. Moyens biométriques physiques ..…….…….....……..…...……05
2.3.1.1. L'empreinte digitale…….…….....……..…….....…05
2.3.1.2. La forme de la main …...…….....…..06
2.3.1.3. Le visage …...…….…….....…..07
2.3.1.3.1. Les modes de fonctionnement (Surveillance ou Recherche) …….…….....07
2.3.1.3.1.1. Mode Surveillance …...…….....…..07
2.3.1.3.1.2. Mode Recherche ……...……...……..08
2.3.1.4. L'iris…...…….……..08
2.3.1.5. La rétine…...……....……..09
2.3.2. Moyens biométriques Comportementaux..…...…….....…….…..10
2.3.2.1. La voix…...…….……...10
2.3.2.2. La signature numérique…...…….....…….....…...10
2.3.2.2.1. Le fonctionne la signature numérique…...…….....…….....11
2.3.3. Moyens biométriques Expérimentaux……...…….....…..11
2.3.3.1. L'ADN…...…….…..…..11
2.3.3.2. L'oreille…...……...…….……..12
3. Reconnaissance empreinte digitale...…...……....…..12
3.1. Définition de l'empreinte digitale...…...……....…..13
3.2. Historiques de l'empreinte digitale …...……...……....…...14
3.3. Points caractéristiques d'empreinte digitale (les minuties).…...…….....….14
3.3.1. Les points singuliers globaux…...…...……....….15

3.3.2. Les points singuliers locaux (minutiers)…..……..……..15
3.3.3. les classes de l'empreinte digitale...…..……..…….....15
3.4. Algorithme de Caractérisation par minutie…...…….....…..……..16
3.4.1. Introduction.…….…..... 16
3.4.2. Les Algorithme de Marthon.……..….....16
3.4.2.1. Algorithme de Marthon…….....16
3.4.2.2. Algorithme de Zhang et Suen …...……...……...……..16
3.4.3. Extraction minutier…...……...…….....17
4. Conclusion ...…...…….……..19

Chapitre II : Conception

1. Introduction..…….....…….…… 21
2. Problématique..…….....…….… 21
3. Solution Proposée :…….....…….…… 21
4. La Méthode UML...……..…….....….....22
4.1.Définition……..... 22
5. Définition des diagrammes ……...…..……..…….23
5.1. Les diagrammes dynamiques ……...……...…….……23
5.1.1. défifnition de diagramme de cas d'utilisation..…….....……..…….....…23
5.1.1.1. Quelques définition de base..……...……..…..……..……23
5.1.1.2. Scénario de contrôle biométrique d'identité d'un étudiant pour autoriser l'assistance a un examen au sein d'université du Médéa.....24
5.1.1.3. Diagramme de cas d'utilisation.....24
5.2. Diagrammes statiques.....…….....….26
5.2.1 .définition de diagramme de classe:…….....….....26
5.2.1.1. Quelques définition de base ……...…….....……..…...…….26
5.2.1.2. diagramme de classe……...…….....…….…...…….....26
5.2.1.2.1. Description de la classe ...……...…….....……..…...…….....28
6. Model relationnel : MLD……...…….....……...…...……..... 30
7. Conclusion..……..…….....…32

Chapitre III : Implémentation et résultats

1.Introduction.....…….....34
2.Architecteur de développement..…….....…..……..34
3. Technologie utilisées.....…..…….....……..34
3.1.partie materiel.…….....…… ……...…….34
3.2.partie logicielles …….....…..…… ……..…….34
3.2.1. Visual Studio Code :...…...…….....…….……..34

3.2.2. Dart…..…….…….....…….....35
3.2.3. Android Studio …..…….…….....…….....……..……..36
3.2.4. Flutter…..…….…….…….....……..…… ……..36
3.2.5. StarUML …..…….…….…..…..…….....……..…….…..36
3.2.6. XAMPP…..…….…….…….....……..…… ….……..37
3.2.7. PHP ‘HypertePreprocessor ‘…..…….…….…..…….....……...……..37
3.2.8.la BDD …….…….....…… ……....……38
4. Travail réalisé..…….…….....…….....…….....……...…….....38
4.1.la fonctionnement du l’application avec la BDD ……...…….…….....…….38
4.2. Icone de l’application « fingerprint_identity » …….....…….....…….....…….....38
4.2.1. Informations sur « fingerprint_identity » …….…….....…….....39
4.3. Interface de « login » …….…….....…….…….....…….....39
4.4. Interface d’accueil …….…….....….....…….....…….....40
4.5. Interface de contrôle …….…….....…….....…….....40
5.Conclusion…….....…….....…..…….....…….…….....44
Conclusion générale :.....….....……..…..……46
Réferences…..……..…….....……...

liste des figures:

Chapitre I :

Figure 1 : Différentes modalités..... 3

Figure2 : Architecture d'un système biométrique.... 4

Figure3: Empreinte digitale... 5

Figure 4 : Lecteur de la forme de la main.. 6

Figure 5 : Caractéristiques du visage.... 7

Figure 6 : Vue détaillée de l'œil humain 8

Figure 7 : Détail d'une rétine.....9

Figure 8: Signal de la voix.....10

Figure 9 : création de la signature numérique.. 11

Figure 10: représentation de L'information génétique d'un individu. 12

Figure11 : les empreintes d'oreille 12

Figure12 : Les parts de marché biométrique par technologie.....13

Figure 13: Empreinte digitale 13

Figure 14 : Étude du dessin digitale. 14

Figure15 : Francis Galton.. 14

Figure 16: Différents positions de Delta. 15

Figure17.1 : Les Coupures.....15

Figure 17.2 : Les Divisions. 15

Figure 17.3: Les Anneaux.....15

Figure 17.4: Les îlots..... 15

Figure18: Les formes des crêtes à la zone centrale de l'empreinte..... 16

Figure 19: Les minuties en empreinte digitale..... 18

Figure 20: Les terminaisons et les bifurcations..... 18

Figure 21 : Détermination de la direction des minuties..... 18

Chapitre II

Figure 22 : Diagramme de cas d'utilisation.....25

Figure 23 : Diagramme de classe.....27

Figure 24 : model relationnel de notre Bdd 31

Chapitre III

Figure 25 : architecture de Modèle-vue-contrôleur.....34
Figure 26 : L'icône de l'éditeur « Visual Studio ».....35
Figure 27 :L'icône de Dart 35
Figure 28 : L'icône de l'Android studio.....36
Figure 29 : L'icône de Flutter 36
Figure 30 : l'icône de starUML.....36
Figure 31 :L'icône de Xampp.....37
Figure 32 : L'icône de PHP 37
Figure 33 : L'icône de « fingerprint_identity ».....38
Figure 34 : capteur sur les informations du l'application installé 39
Figure 35 : L'interface d'authentification.....39
Figure 36 : L'interface d'accueil 40
Figure 37 : l'interface de contrôle 40
Figure 38 : l'interface de contrôle après la sélection des cordonnes.....41
Figure 39 : capteur sur « moyenne sup à 10 ».....41
Figure 40 : capteur sur « moyenne d'unité sup à 10 ».....42
Figure 41 : capteur sur « moyenne de semestre sup à 10 ».....42
Figure 42 : capteur sur « salle d'affectation est déférente ».....43
Figure 43 : capteur sur « la moyenne d'un module inf à 10 ».....43

liste des tableaux :

Table 1 : Table des conditions à chaque itération.....17

Table 2 : Identification d'une minutie à partir du calcul de CN.....17

Table 3 : description des classes.....28

Introduction générale

Introduction générale :

Il ne fait désormais plus aucun doute que l'informatique est la révolution la plus importante et la plus innovante qui a marqué la vie de l'humanité moderne. En effet, les logiciels informatiques proposent maintenant des solutions à tous les problèmes de la vie aussi bien dans des domaines professionnels que pour des applications personnelles. Et leurs méthodes de conception et de développement ont vu l'avènement d'autant de technologies qui facilitent leur mise en place et leurs donnent des possibilités et des fonctionnalités de plus en plus étendues.

La nécessité de la sécurité civile et la lutte contre les fraudes d'une part et l'explosion de l'informatique et la croissance des moyens de communication d'autre part ont fait augmenter le besoin de sécurisé et de s'assurer l'identité des individus. Les systèmes d'authentification traditionnels (mots de passe, codes pin, badges, clefs,...etc.) ne sont pas vraiment fiables (faciles à falsifier) à cause de leur inhabilité à différencier entre une personne autorisée et une personne non autorisée (intrus), problème qui provoque l'apparition des systèmes biométriques.

En fait l'utilisation de la biométrie pour des fins de reconnaissance n'est pas vraiment récente, cependant les procédures manuelles et la gestion des bases de données rendent le travail long et coûteux. Les applications biométriques sont nombreuses et permettent d'apporter un niveau de sécurité supérieur dans plusieurs domaines, tels que, le contrôle d'accès physique à des lieux protégés, et le contrôle d'accès virtuel à des réseaux d'ordinateurs. L'université est l'une des endroits ou on peut profiter au maximum des bénéfices de cette technologie biométrique. L'un des domaines est le contrôle d'identité pour autoriser l'assistance à un examen au sein de l'université. l'objectif de notre projet est la réalisation d'une application Android, interactive, fiable, conviviale et facile à intégrer dans l'environnement de travail de l'université assurant l'identification biométrique de l'étudiant à l'aide des empreintes digitales pour assurer la présence réelle d'un étudiant dans une salle d'examen de toute les matières. Aussi, elle permet de valider les enseignants surveillants dans chaque salle.

Nous présentons en détail les étapes que nous avons suivies pour réaliser notre application. Ce mémoire est présenté en trois chapitres décrits ci-dessous :

Dans le premier chapitre, nous introduisons quelques définitions de la biométrie, puis nous détaillons les différents modules d'un système biométrique et les différents médias biométrie (physique, comportementaux et expérimentaux). Ce chapitre est consacré à faire une description détaillée sur l'empreinte digitale et son traitement jusqu'au l'extraction des minutiers. Le deuxième chapitre concerne la problématique et la solution informatique suivie par la phase de conception par la présentation de toutes

les méthodes utilisées pour la réalisation de l'application. Le troisième chapitre est dédié à l'implémentation et la mise en œuvre de notre système. Nous terminons ce mémoire par une conclusion générale.

Chapitre I:

La biométrie et la reconnaissance des empreintes digitales

1. Introduction :

La biométrie constitue l'ensemble des technologies qui exploitent des caractéristique biométriques (physiques, comportementales ou biologiques) comme des moyens d'identification des individus. Ces technologies exploitent les caractéristiques qui sont uniques chez les individus et ne peuvent êtres perdues ni volées ni reconstituées contrairement aux moyens classiques reposant sur des mots de passe ou des cartes magnétiques. C'est pour cette raison que la biométrie apparaît comme l'une des meilleures technologies contre la fraude à l'identité. Le présent chapitre donne un aperçu sur les notions de biométrie de manière générale.Nous insisterons plus particulièrement sur l'utilisation des empreintes digitales dans les systèmes d'identification de personnes. Pour plus de connaissance nous détaillerons de reconnaissance d'empreintes

2. La biométrie :

2.1. Définition de biométrie :

La biométrie est l'étude quantitative des êtres vivants, plus précisément dans notre contexte : c'est la reconnaissance et l'identification des individus en utilisant des informations étroitement liés à leurs caractéristiques. Les méthodes biométriques, impliquent l'utilisation des empreintes digitales, du visage, de la voix, de l'iris ou de l'ADN...etc. Elles possèdent chacune ses propres avantages et ses limitations. Certaines méthodes sont rigoureuses mais sont également très contraignantes (coût élevé, collaboration de la personne indispensable dans la majorité des cas, etc.) alors que d'autres sont plus conviviales mais souffrent de problèmes de précision. Pour que les caractéristiques, propre à chaque individu, puissent être qualifiées de modalités biométriques, elles doivent être :

*__universelles__(existent chez tous les individus).

* **uniques** (possibilité de différencier un individu par rapport à un autre).

*__permanentes__ (peuvent évoluer dans le temps) .

*__enregistrables__ (possibilité d'enregistrer les caractéristiques d'un individu avec son accord).

*__mesurables__ (possibilité de comparaisons futures).

L'empreinte digitale, la géométrie de la main, l'iris, la rétine, le visage, l'empreinte palmaire, la géométrie de l'oreille, l'ADN, la voix, la démarche, la signature ou encore la dynamique de frappe au clavier sont autant de modalités biométriques différentes. [1]

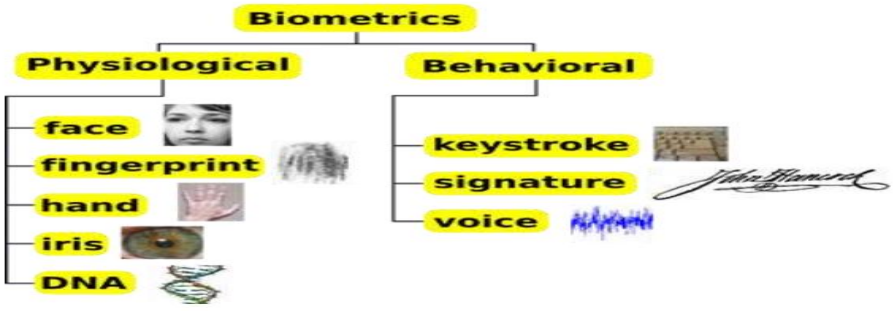


Figure 1 : Différentes modalités [1]

2.2 .Architecture de biométrie :

Il y a toujours au moins deux modules dans un système biométrique :

- Le module d'apprentissage
- le module de reconnaissance [2].
- le troisième module (facultatif) est le module d'adaptation.

Au cours de l'apprentissage, le système acquiert une ou plusieurs mesures biométriques qui serviront à construire un modèle de l'individu.

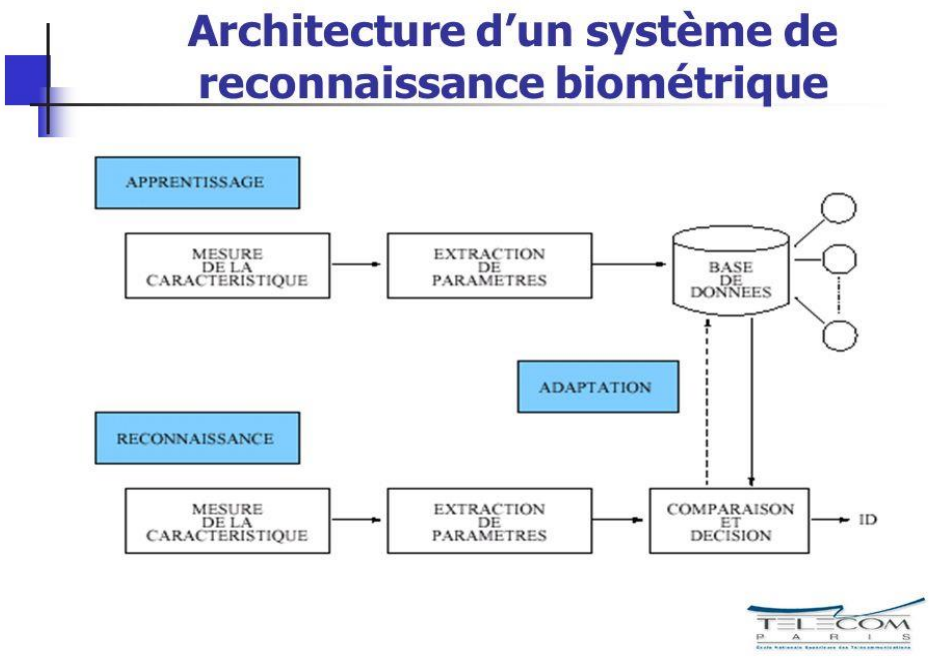


Figure2 : Architecture d'un système biométrique. [15]

2.2.1. Module d'apprentissage :

Lors de l'apprentissage, la fonctionnalité biométrique est avant tout mesurée à l'aide d'un capteur , on parle d'acquisition ou de capture. Généralement cela la capture n'est pas stockée directement et des transformations lui sont appliquées. Dans En effet, le signal contient des informations inutiles pour la reconnaissance et seule la Les paramètres pertinents sont extraits.

2.2.2. Module de reconnaissance :

Lors de la reconnaissance, la caractéristique biométrique est mesurée et un ensemble de paramètres est extrait comme lors de l'apprentissage. Le capteur utilisé doit avoir des propriétés aussi proches que possible du capteur utilisé lors de la phase d'apprentissage. Si les deux capteurs ont des propriétés très différentes, il sera généralement nécessaire d'appliquer un prétraitement supplémentaire pour limiter la dégradation des performances. Le reste de la reconnaissance sera différent selon le mode de fonctionnement du système d'identification ou de vérification. En mode identification, le système doit deviner l'identité de la personne. Répondez alors à une question du type : « Qui suis-je ? ". Dans ce mode, le système compare le signal mesuré avec les différents modèles contenus dans la base de données. En général, lorsque l'on parle d'identification, on suppose que le problème est fermé, c'est-à-dire que

toute personne qui utilise le système possède un modèle dans la base de données.

2.2.3. Module d'adaptation :

Pendant la phase d'apprentissage, le système biométrique ne capture souvent que quelques instances d'un même attribut afin de limiter la gêne pour l'utilisateur. Il est donc difficile de construire un modèle assez général capable de décrire toutes les variations possibles de cet attribut. De plus, les caractéristiques de cette biométrie ainsi que ses conditions d'acquisition peuvent varier. L'adaptation est donc nécessaire pour maintenir voire amélioré la performance d'un système utilisation après utilisation.

2.3. Les moyens biométriques :

2.3.1. Moyens biométriques physiques :

2.3.1.1. L'empreinte digitale

- **Définition :**

Les empreintes digitales sont le dessin formé par les lignes de la peau des doigts, ils appelées aussi dermatoglyphes - sont une signature que nous laissons derrière nous à chaque fois que nous touchons un objet. Les motifs dessinés par les crêtes et plis de la peau sont différents pour chaque individu , c'est ce qui motive leur utilisation par la police criminelle depuis le 19è siècle. On distingue deux types d'empreintes : ***l'empreinte directe ou visible*** qui laisse une marque visible à l'œil nu et l'empreinte ***latente ou invisible*** qui est composée de lipides, de sueur et de saletés déposés sur un objet touché. Une empreinte digitale se compose principalement de crêtes (Ridges) et de vallées (Valleys). On regroupe ces points clés de l'empreinte sous le terme de minuties. C'est l'étude des minuties qui permet d'identifier de façon certaine un individu.[3]

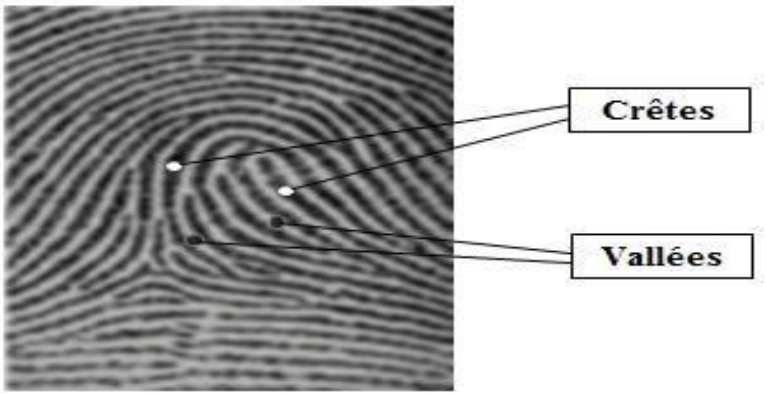


Figure3: Empreinte digitale [3]

❖ **Avantages**

- C'est la technologie la plus connue et la plus éprouvée.
- Son lecteur étant de petite taille, il facilite son intégration dans la plut part des systèmes.
- Faible coût des lecteurs
- Se traite rapidement
- Taux de faux rejets et de fausses acceptantes acceptable
- La plus ancienne et la plus connue des utilisateurs

- Facile à mettre en œuvre
- technologie viable et exécution rapide. [4]

❖ **Inconvénients :**

- Indispensabilité de la coopération de l'individu
- Stéréotype de l'empreinte comme étant à usage policier
- Acceptante d'un moulage de doigt ou un doigt coupé
- Moyennement accepté par la société.
- Problème d'universalité (Certaines personnes ne possèdent ou pas d'empreinte digitales ou détruites dans le temps) [4]

2.3.1.2. La forme de la main

▪ **Définition :**

La biométrie par la forme de la main est une technologie populaire qui est largement employée pour le contrôle d'accès physique ou le pointage horaire. Le système prend une photo de la main et examine 90 caractéristiques, y compris la forme tridimensionnelle de la main, de la longueur et de la largeur des doigts et de la forme des articulations. Pour utiliser la géométrie de la main, l'utilisateur place sa main sur une platine possédant des guides pour positionner les doigts Les lecteurs du contour de la main offrent un niveau très raisonnable d'exactitude, mais peuvent avoir des taux de fausse acceptation élevée pour des jumeaux ou d'autres membres de la même famille.[3]



Figure 4: Lecteur de la forme de la main [20][24]

❖ **Avantages**

- Très bien accepté par les individus à identifier ou vérifier
- Simple à utiliser
- Pas d'effet en cas d'humidité ou d'impropriété des doigts[1]

❖ **Inconvénients**

- Encombrant pour les bureaux, dans une voiture ou un téléphone
- Risque de fausse acceptation pour des jumeaux ou des membres d'une même famille [1]

2.3.1.3. Le visage

- **Définition :**

Rien n'est plus naturel qu'utiliser le visage pour identifier une personne. Les images faciales sont probablement la caractéristique biométrique la plus communément employée par l'homme pour effectuer une identification personnelle.L'utilisation d'une caméra permet de capter la forme du visage d'un individu et d'en dégager certaines particularités. Selon le système utilisé, l'individu doit être positionné devant l'appareil ou peut être en mouvement à une certaine distance. Les données biométriques qui sont obtenues sont par la suite comparées au fichier référence. [3]



Figure 5 : Caractéristiques du visage [25]

2.3.1.3.1. Les modes de fonctionnement (Surveillance ou Recherche) :

2.3.1.3.1.1. Mode Surveillance :

Le système peut détecter automatiquement la forme d'un visage, en extraire l'image, exécuter l'identification en s'appuyant sur une base de données d'individus préenregistrés. Il calcule rapidement le degré de recoupement entre l'empreinte du visage réel qui vient d'être capté et ceux associés aux individus connus enregistrés dans une base de données biométrique d'images faciales. Il peut retourner une liste d'individus possibles triée par score décroissant (images ressemblantes) ou il peut simplement retourner l'identité du sujet (résultat le plus haut) et un niveau de confiance associé. Ceci paramétrable au choix de l'opérateur. En mode Surveillance il fonctionne en temps réel et dans le même temps, capte les images et recherche dans la base de données. L'architecture technique mise en place pour cela est fonction des besoins de l'application (nombre d'individus enregistrés, vitesse de défilement devant la caméra, flux…) ‹Une autre fonction du mode Surveillance permet de trouver des visages humains n'importe où dans le champ de vision du système et à toute distance. Il peut les suivre de façon continue et les extraire de l'image, en comparant le visage ainsi isolé avec une liste de visages stockés.[3]

2.3.1.3.1.2. Mode Recherche :

Le mode Recherche peut être utilisé en mode IDENTIFICATION (un à plusieurs) ou en mode VERIFICATION (un à un). [3]

❖ **Avantages**

- Bien accepté par les usagers
- Ne demande aucune action de l'usager, pas de contact physique
- Elle n'est pas très coûteuse [3]
- Bien accepté par les usagers
- Ne demande aucune action de l'usager, pas de contact physique [1]

❖ **Inconvénients**

- Sensible à l'environnement (éclairage, position, expression du visage etc.)
- Problème de différentiation entre les vrais jumeaux
- Sensible aux changements (barbe, moustache, lunette, piercing, chirurgie etc.)[3]
- Sensible à l'environnement (éclairage, position, expression du visage etc.)
- Problème de différentiation entre les vrais jumeaux
- Sensible aux changements (barbe, moustache, lunette, piercing, chirurgie etc.)[1]

2.3.1.4. L'iris

▪ **Définition :**

L'iris est la région annulaire située entre la pupille et le blanc de l'œil. Les motifs de l'iris se forment au cours des deux premières années de la vie et sont stables. Les iris sont uniques et les deux iris d'un même individu sont différents. Dans l'iris de l'œil, il est possible de compter plus de 200 paramètres indépendants.[5]



Figure 6: Vue détaillée de l'œil humain [23]

❖ **Avantages**

- L'iris contient une grande quantité d'information
- Pas de confusion pour les vrais jumeaux **[1]**
- Performance et fiabilité très élevée
- La texture de l'iris est parfaitement stable au cours du temps et passe à travers les lunettes, lentilles
- Différencie entre deux vrais jumeaux [3]

❖ **Inconvénients**

- Méthode invasive et non conviviale
- L'iris peut être facilement photographié [1]

- Technologie très couteuse
- Besoin de la coopération de l'utilisateur
- La fiabilité diminue proportionnellement à la distance entre l'œil et le capteur [3]

2.3.1.5. La rétine

- **Définition :**

La rétine est la couche sensorielle de l'œil qui permet la vision. Cette zone est parcourue par des vaisseaux sanguins qui émergent au niveau de la papille optique, où l'on distingue l'artère et la veine centrale de la rétine qui se divisent elles mêmes en artères et veines de diamètre plus faible pour vascularisé les cellules qui permettent la vision. La grande variété de configurations des vaisseaux sanguins présenterait la même diversité que les empreintes digitales. L'aspect des vaisseaux peut être modifié par l'âge ou la maladie, mais la position respective des vaisseaux reste inchangée durant toute la vie de l'individu. [4]

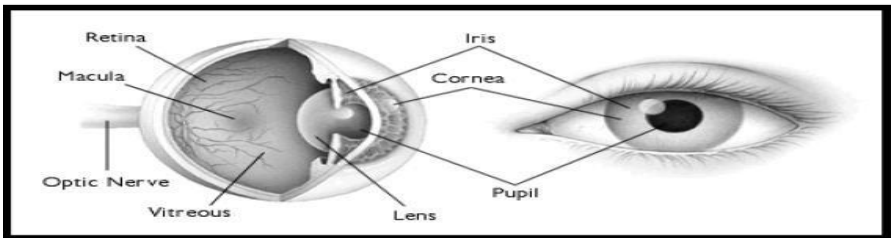


Figure 7 : Détail d'une rétine [3]

La reconnaissance de la rétine est actuellement considérée comme une des méthodes biométriques les plus sûres. L'image est obtenue en projetant sur l'œil un rayon lumineux de faible intensité dans les fréquences visibles ou infrarouges. L'œil doit être situé très près de la tête de lecture et l'utilisateur doit fixer son regard sur un point déterminé pendant plusieurs secondes ce qui demande une grande coopération de sa part. [3]

❖ **Avantages**

- Performance et fiabilité très élevée
- Durable dans le temps
- Les risques de fraude sont quasi nuls, puisque la partie du corps exploitée n'est pas apparente. [4]

❖ **Inconvénients**

- Technologie coûteuse
- Système intrusif et peu agréable
- Ne passent pas à travers des lunettes et peut, de plus les réseaux sanguins peuvent être modifiés (forte alcoolémie, diabète). [4]

2.3.2. Moyens biométriques Comportementaux :

2.3.2.1. La voix

- **Définition :**

Chaque personne possède une voix propre caractérisée par une fréquence, une intensité et une tonalité et que l'on peut analyser par enregistrement avec un microphone. Même si deux voix peuvent sembler

similaires pour l'oreille, le traitement informatique permet de les isoler. La reconnaissance du locuteur vise à déterminer les caractéristiques uniques de la voix de chaque individu. Cette biométrie est en général très bien acceptée car la voix estun signal naturel à produire. [3]

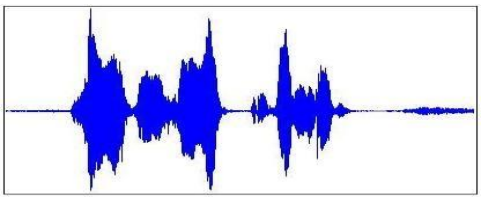


Figure 8: Signal de la voix [3]

❖ **Avantages**

- les lecteurs sont facilement protégés
- Seule information utilisable via le téléphone
- Impossibilité d'imitation de la voix
- Elle n'est pas intrusive [1]
- Système non intrusif
- Faible coût
- Très bien acceptées par les populations [4]

❖ **Inconvénients**

- Sensible à l'état physique et émotionnel de l'individu
- Fraude possible par enregistrement
- Sensible aux bruits ambiants
- Taux de faux rejet et fausse acceptation élevés [1]
- Sensible aux bruits ambiants
- Fraude possible par enregistrement
- Dépend de l'état de l'utilisateur (physique et émotionnel) [4]

2.3.2.2. La signature numérique

▪ **Définition :**

Désigne un ensemble de protections de chiffrement servant à déterminer l'authenticité d'un document ou d'un logiciel. Autrement dit, il s'agit d'une méthode complexe permettant de s'assurer qu'un document n'a pas été manipulé pendant son transfert entre l'expéditeur et le signataire. Les signatures numériques peuvent être utilisées pour identifier et vérifier les signataires individuels, et garantir la sécurité et l'intégrité des données concernées. [6]

L'analyse des empreintes génétiques est une méthode extrêmement précise d'identification, issue directement de l'évolution de la biologie moléculaire.

- ✓ L'information génétique d'un individu est unique car aucun membre de l'espèce ne possède la même combinaison de gènes codés dans l'acide désoxyribonucléique (ADN).
- ✓ Trace individuelle unique : l'ADN est l'outil d'identification par excellence.
- ✓ L'analyse ADN : l'analyse des empreintes génétiques est devenue en quelques années l'un des outils majeurs de la criminalistique, la science de l'identification des indices matériels. L'analyse de l'ADN est couramment utilisée en criminologie pour identifier une personne à partir d'un morceau de peau d'un cheveu ou d'une goutte de sang. [5]

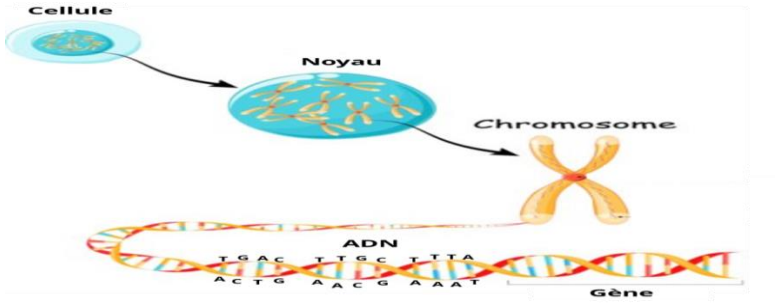


Figure 10: représentation de L'information génétique d'un individu [22]

2.3.3.2. L'oreille

- **Définition :**

Cette technique consiste à comparer les empreintes d'oreille que peuvent laisser certains individus dans le cadre d'un délit.

Cette méthode est uniquement utilisée par la police, mais est admissible devant une cour de justice. [5]

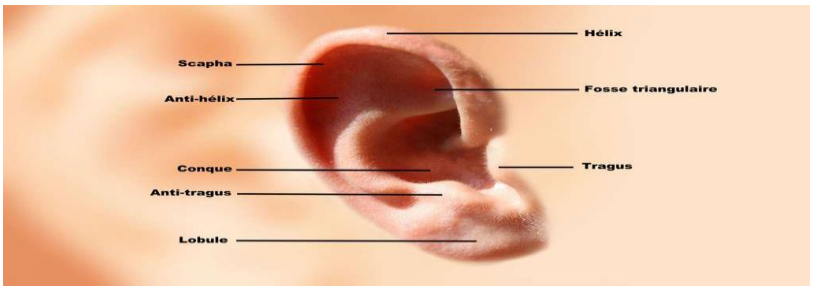


Figure11 : les empreintes d'oreille [21]

3. Reconnaissance empreinte digitale :

Parmi les nombreuses méthodes d'identification biométrique l'utilisation des empreintes digitales est la méthode la plus aboutie avec 31% de parts démarché, Les systèmes biométriques utilisant l'empreinte digitale sont les plus utilisés. [7] Des solutions de plus en plus abordables et performantes sont proposées par les constructeurs. On voit de plus en plus placer des lecteurs d'empreintes digitales sur des micros ordinateurs ou des téléphones portables pour sécuriser leurs utilisations et cela devient de plus en plus commode et accepté par le grand public. [3]

L'empreinte digitale est très efficace pour l'identification d'un individu, car il est impossible de trouvé deux empreintes similaires, Les jumeaux venant de la même cellule, auront des empreintes très proches



Figure 9 : création de la signature numérique [19]

2.3.2.2.1. Le fonctionne la signature numérique :

La signature numérique fait appel à un chiffrement à clé publique. Deux clés liées de façon mathématique sont générées. L'une est publique et l'autre privée. La personne qui crée la signature numérique utilise la clé privée pour chiffrer toutes les données en rapport avec la signature, tandis que la clé publique du signataire lui permet de déchiffrer les données. La signature numérique n'est authentifiée que lorsque le destinataire parvient à ouvrir le document avec la clé publique du signataire. Si le destinataire ne parvient pas à ouvrir le document, c'est signe qu'il y a un problème avec le document ou la signature. [6]

❖ **Avantage :**

- Le principal avantage est la sécurité. Avec ce système, un document ne peut pas être altéré à l'insu du destinataire. Cela garantit également la légitimité des signatures. En plus de la signature numérique, les fonctionnalités de sécurité HelloSign comme les codes secrets, les mots de passe, le chiffrement asymétrique, les pistes d'audit et les horodatages font que les documents envoyés et reçus pour signature avec HelloSign sont aussi sécurisés que possible. [6]

❖ **Inconvénients :**

- Elle est sensible aux émotions de l'individu
- Non utilisable pour les contrôles d'accès

2.3.3. Moyens biométriques Expérimentaux :

2.3.3.1. L'ADN

▪ **Définition :**

L'acide désoxyribonucléique ou ADN est une macromolécule biologique présente dans toutes les cellules d'un être vivant [9] et son analyse est une méthode extrêmement précise d'identification, issue directement de l'évolution de la biologie moléculaire. Cependant l'identification d'une personne grâce à son ADN est assez couteuse à mettre en place et lente à réaliser. L'information génétique d'un individu est unique (aucun membre de l'espèce ne possède la même combinaison de gènes codés l'ADN). Le profil génétique, aujourd'hui couramment utilisé pour des identifications judiciaires où il présente une percée majeure dans la criminalistique pour l'identification des personnes inconnues ou pour déterminer la source des échantillons biologiques laissées dans les lieux de crime. Le profil génétique fut introduit officiellement pour la première fois dans une affaire criminelle en 1986 par l'universitaire anglais Alec Jeffreys [10,11]. [4]

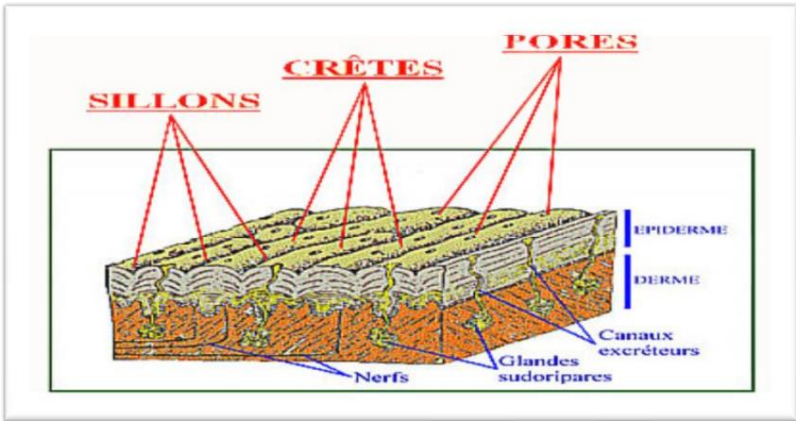


Figure 14 : Étude du dessin digitale [3]

3.2. Historiques de l'empreinte digitale :

Les premières traces d'utilisation d'empreintes digitales ont été découvertes en Égypte et datent de l'époque des pyramides il y a plus de 4000 ans.

Les Chinois ont aussi utilisé très tôt ce moyen pour signer les documents officiels (le plus vieux document signé date du troisième siècle avant Jésus Christ) mais ils ne savaient sûrement pas que les empreintes étaient uniques pour chaque personne et permettaient ainsi une identification fiable.

C'est en 1856 que l'anglais William Hershel , après avoir utilisé les empreintes en guise de signature sur la population indienne qu'il dirigeait, comme ça à comprendre quels empreintes étaient uniques et constantes dans le temps. En 1888 le britannique Francis Galton publia une étude sur les empreintes digitales où il établit leurs caractéristiques (unicité, invariance, minuties, classification) et en 1901 la technique d'identification au moyen des Chapitre I: La biométrie et les empreintes digitales.7 empreintes fut adoptée officiellement en Angleterre dans le système judiciaire .Cette technique fut ensuite largement développée dans les enquêtes criminelles et permit de résoudre un bon nombre d'affaires.

De nos jours les empreintes sont toujours largement utilisées et reconnues comme méthode d'identification fiable. [7]



Figure15: Francis Galton [3]

3.3. Points caractéristiques d'empreinte digitale (les minuties) :

Les pointes caractéristiques ou les crêtes sont utilisées pour différencier deux empreintes digitales et aussi faires une classification selon les points singuliers globaux et les points singuliers locaux **[3]**

mais pas semblables, et aujourd'hui les empreintes sont reconnues comme méthodes d'identification fiable [3] .Le principe de la Reconnaissance des Empreintes Digitales consiste à comparer 2 empreintes fournies au système à une ou plusieurs autres empreintes aussi appelé « Template» ou signatures, le système biométrique renvoie un résultat positif au cas où l'empreinte fournie à l'entrée correspond à l'un des Template, et un résultat négatif dans le cas contraire. [3]

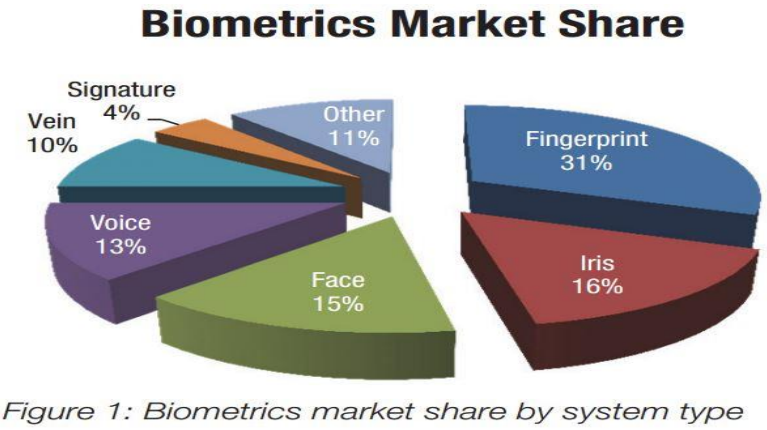


Figure12 : Les parts de marché biométrique par technologie[14]

3.1. Définition de l'empreinte digitale :

L'empreinte digitale est le dessin formé par un doigt sur un support suffisamment lisse pour qu'y restent marqués, les dermatoglyphes et elles sont uniques à chaque individu et chaque doigt a son empreinte propre. La probabilité que deux personnes aient les mêmes empreintes digitales est infinitésimale : une chance sur 64 milliards [8].L'identification par cette caractéristique est la technique la plus anciennement utilisée. En fait, c'était toujours le choix biométrique évident pour les services de police depuis plus de 100 ans. Il existe plusieurs types de système de capture d'empreinte digitale : optique, thermique, électromagnétique et ultrasons [9].



Figure 13: Empreinte digitale [13]

L'empreinte digitale scientifiquement est composée des crêtes qui contiennent des pores et des sillons, et les pores permettent de sortir 80% eaux et 20% matières organiques, ces matières laissent des marques sous formes des lignes.[3]

3.3.1. Les points singuliers globaux :

On distingue les points caractéristiques globaux par le Core et le Delta. **[3]**

Le Core : centre ou le noyau contient de courbure maximale deslignes de l'empreinte.

Le Delta : est proche du lieu où se deux lignes, aussi est le lieude divergence des lignes les plus internes. (voir Figure 16)

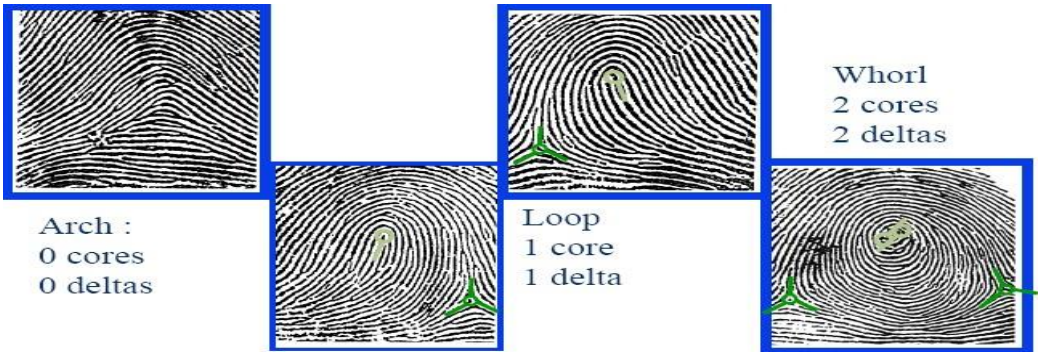


Figure 16: Différents positions de Delta [3]

3.3.2. Les points singuliers locaux (minutiers)

En chaque empreinte il y a des minuties spécifiques permettent de différencier et classer les empreintes, et il ya plusieurs formes des minutiers généralement on a quatre types **[3]** :

Les coupures : terminaison à droite ou à gauche, minuties située en fin de stries. (voir Figure17.1)

Les divisions : Bifurcation à droite ou à gauche, intersection de deux stries. (voir Figure 17.2)



Figure17.1 : Les Coupures [3]



Figure 17.2 : Les Divisions [3]

Les anneaux : Lac, assimilée à deux bifurcations. (voir Figure 17.3)

Les ilots : assimilés à deux terminaisons. (voirII.Figure17.4)



Figure 17.3: Les Anneaux [3]

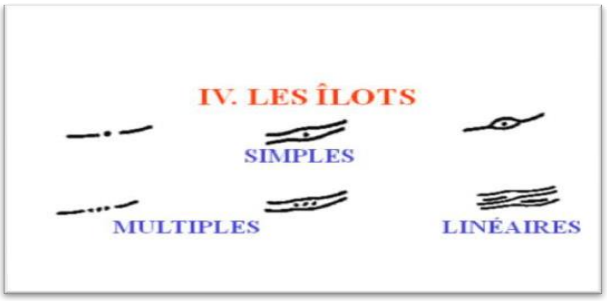


Figure 17.4: Les îlots [3].

3.3.3. les classes de l'empreinte digitale :

Français Galton (1822-1916) ont été faites les premières études scientifiques sur les classifications des

empreintes digitales, ces études ont affiné par Edward Henry (1850-1931), il est classé les empreintes en cinq classes : arc, arc tendu,boucle à gauche, boucle à droite, et spire.[3]

- **Classe 1**:il contient en maximum un Delta et au moins une crête montre unecourbure élevée, est une classe poubelle. [10]
- **Classe 2**:il contient un Delta à droite et des boucles situé en côté à gauche del'empreinte.
- **Classe 3**:il contient un Delta à gauche et des boucles situé en côté à droite del'empreinte.
- **Classe 4**:il contient un Delta à gauche et d'autre à droite avec un centre spirale.[11]
- **Classe 5**:il contient trois Delta autour de forme besace
- **Classe 6:**il contient des empreintes invisibles.

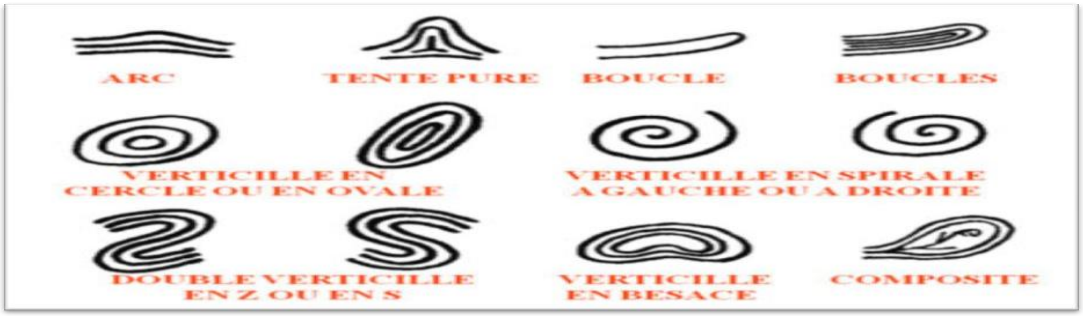


Figure18: Les formes des crêtes à la zone centrale de l'empreinte [3]

3.4. Algorithme de Caractérisation par minutie

3.4.1. Introduction :

Le traitement de l'image de l'empreinte, il est effectué par un ensemble desalgorithmes qui sont permettent de trouver des caractéristiques spécial à chaque empreinte digitale. Parmi de ces algorithmes on trouve algorithme de Marthon, algorithme de Zhang et Suen[3]

3.4.2. Les Algorithme de Marthon :

3.4.2.1. Algorithme de Marthon :

C'est un algorithme de suppression de points.[3]

Soit le point M considéré de coordonnées (x, y). Soit l'ensemble M_i (x_i, y_i) de ses points voisins en n-connexité, la conservation ou non du point M lors de la squelettisation dépend des deux valeurs X et Y définies comme suit :

$X = (x_1-x) + (x_2-x) +...+ (x_n-x)$.....N°=(1)

$Y = (y_1-y) + (y_2-y) +...+ (y_n-y)$.....N°=(2)

Si un point est intérieur à l'objet alors |X|+|Y| est petit. Si le point est au bord del'objet alors |X|+|Y| est grand. En conséquence,

- ✓ Si |X|+|Y| = 4, alors le point M est supprimé.
- ✓ Si |X|+|Y|<=2, alors le point M est conservé.
- ✓ Si |X|+|Y| = 3, alors le point M est conservé ou supprimé suivant le nombre deses voisins. [12]

3.4.2.2. Algorithme de Zhang et Suen :

L'algorithme de Zhang et Suen introduit deux critères pour décider si un pixel P doit être éliminé. En

premier lieu, il s'assure que le pixel considéré est un pixel noir etau moins l'un de ses voisins est blanc. La 1ère itération pour transformer le pixel en pixel blanc si les conditions suivantes dans (t) sont réalisées. (Voir **Table 1**)

A la 2ème itération les conditions (1) et (2) ne changent pas plus les conditions suivantes dans (t) sont réalisées. (Voir **Table 1)** [3]

Critère 1(première itération)	Critère 2(deuxième itération)
1.La connectivité est égale à 1 2.Il y a au moins 2 et au plus 6voisins de valeur noir. 3.Au moins l'un des pixels P2,P4, P6 est blanc. 4.Au moins l'un des pixels P4,P6, P8 est blanc.	1. Au moins l'un des pixels P4, P2, P8est blanc. 2. Au moins l'un des pixels P2, P6, P8 est blanc

P1	P2	P3
P8	P	P4
P7	P6	P5

Table 1 : Table des conditions à chaque itération [3]

Les pixels réalisant ces conditions doivent être supprimés. A la fin s'il n'y a aucunpixel à supprimer, alors l'algorithme s'arrête. [12]

3.4.3. Extraction minutier :

Les minuties de l'empreinte digitale sont extraites à partir de son squelette en calculant la « connectivité » ***CN*** en chaque point de l'image *P* de la manière suivante :

$$CN = 0.5 \sum_{i=1}^{8} |P_i - P_{i+1}| \text{.....N°=(3)}$$

En effet le coefficient *CN* présente des caractéristiques (tableau 2) qui permettentd'identifier la nature d'une minutie en fonction du résultat obtenu lors du calcul de *CN*.[3]

CN	Nature de la minutie en P
0	Erreur ====> point isolé
1	Terminaison
2	Erreur ====> point appartient sillon
3	Bifurcation
4	Erreur ====> minutie à 4 branches

Table 2 : Identification d'une minutie à partir du calcul de CN [3]

Le résulta obtenu :

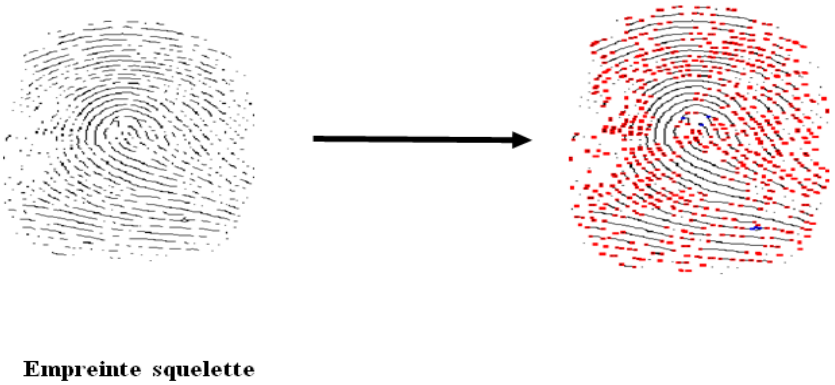


Figure 19: Les minuties en empreinte digitale. [3]

Les points rouges : fin de ligne (Terminaison).

Les points blues : intersection de deux lignes (Bifurcation).

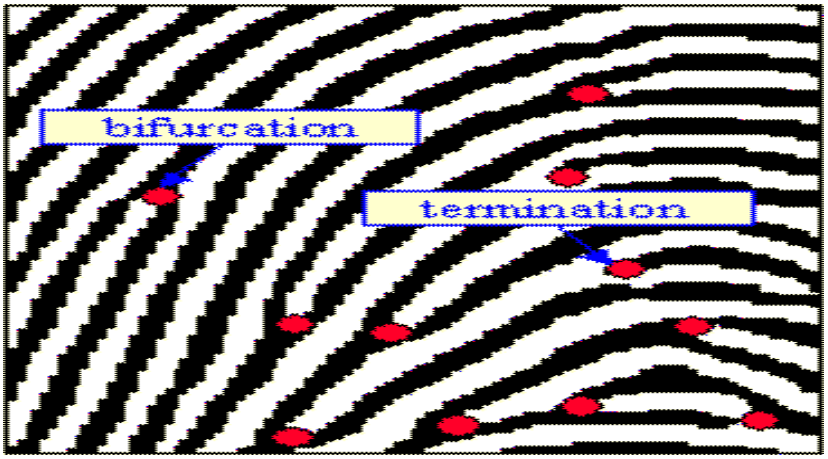


Figure 20: Les terminaisons et les bifurcations. [3]

Les minuties présentes au sein de l'image de l'empreinte digitale, que l'on sauvegarde dans un liste L1 en associant à chacun d'entre eux la position absolue (xP,yP) correspondante et le type de minutie dont il s'agit (terminaison ou divergence). [3]

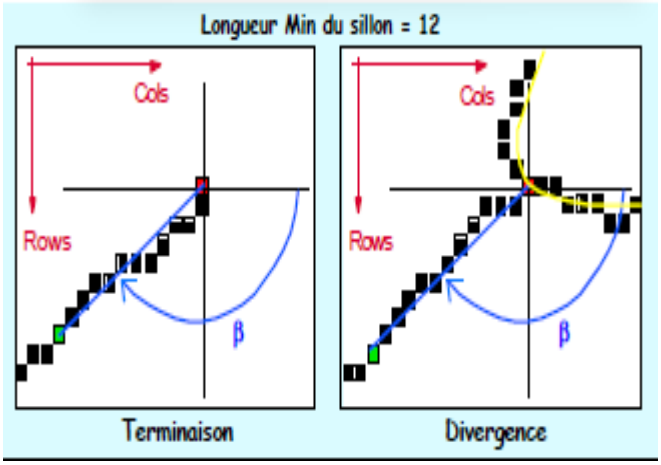


Figure 21: Détermination de la direction des minuties. [3]

4. Conclusion :

La recherche en biométrie est donc un domaine à très fort potentiel, bien que la reconnaissance des empreintes digitales fasse ses preuves aujourd'hui, des améliorations doivent encore être apportées dans ce domaine. L'inefficacité des systèmes automatiques face aux empreintes de mauvaise qualité et le temps nécessaire au système pour identifier une empreinte font actuellement l'objet de plusieurs recherches.

Chapitre II :

Conception

1. Introduction :

Au terme de ce chapitre, on commence par une solution informatique proposé pour résoudre le problème de l'identification après on modélise le fonctionnement détaillé de notre application ainsi que son architecture globale à travers les différents diagrammes d'UML. Mais, au préalable nous allons préciser quelques éléments clés sur le langage de modélisation UML.

2. Problématique :

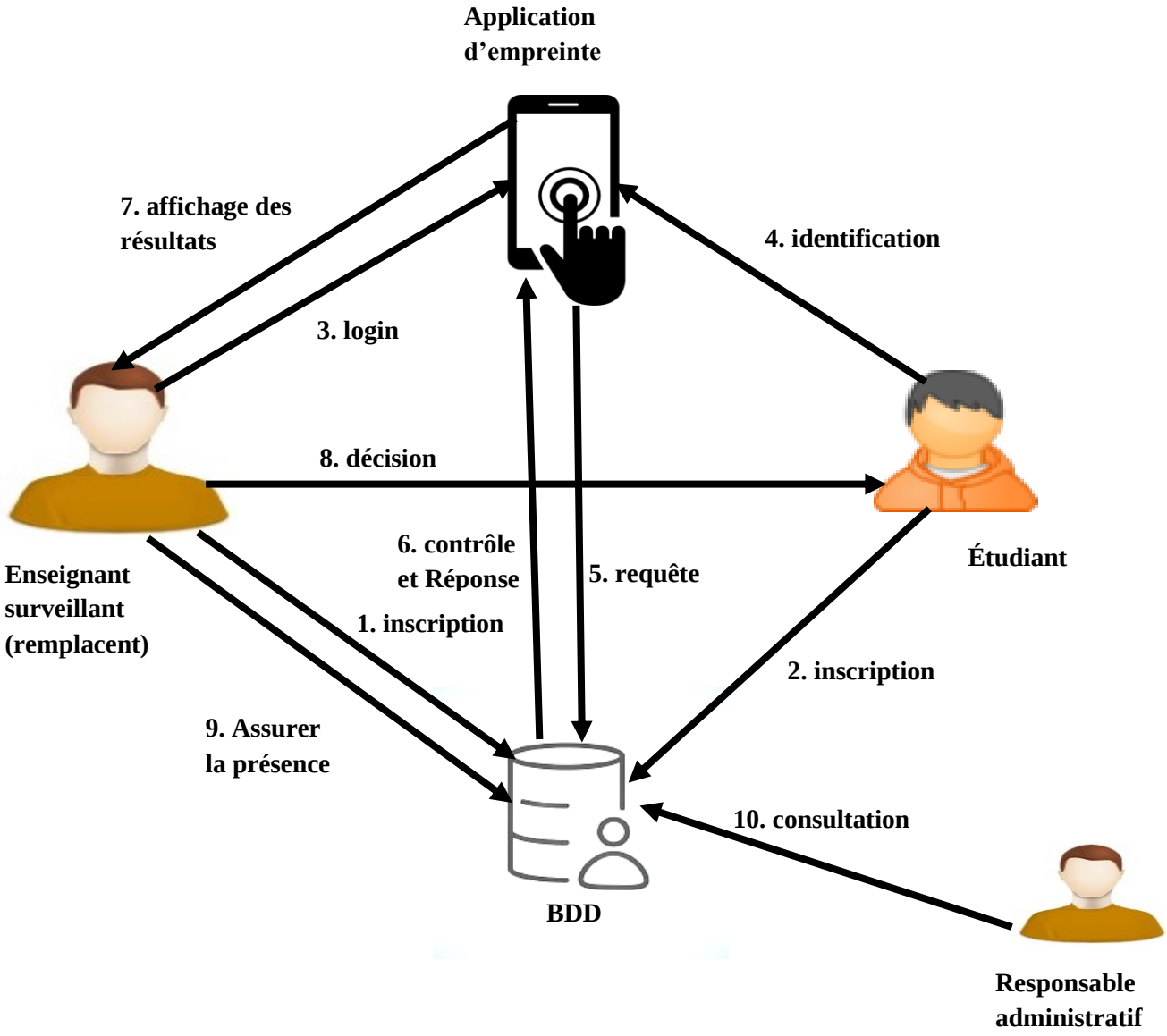
Le progrès technologique ouvre de nouvelles opportunités dans les différents environnements dans lequel il s'applique, en s'adaptant aux besoins de chaque moment et de chaque personne.
Le terme de biométrie est originaire d'une contraction des deux anciens termes grecs : « bios » qui signifie : la vie « métrique » qui se traduit par : mesure. C'est-a-dire « mesure du vivant ». La biométrie consiste a vérifier ou déterminer l'identité d'un individu a partir de ses caractéristiques biologiques (comme l'ADN), comportementales (comme la voix) ou morphologiques (comme l'empreinte digitale).
Les techniques biométriques permettent la mesure et la reconnaissance de ce que l'on est, à la différence d'autres techniques de mêmes finalités, mais permettant de mesurer où vérifier ce que l'on possède (cadre, badge, document.) ou ce que l'on sait (mot de passe, code pin.) [34]
L'université est un environnement où il y a un flux de personne qui partage un espace commun. Tous les étudiants doivent passer des examens afin d'évaluer leur connaissance. Cependant certains étudiants essayent toujours de tricher par différentes méthodes, notamment le remplacement par une autre personne (surtout dans les épreuves de rattrapage) où le changement du lieu d'affectation lors du passage de l'examen (pour former des groupes de tricheurs au sein de la salle d'évaluation), et malgré le contrôle effectué par la carte d'étudiant, la réalité et les échos montre que beaucoup d'étudiants ont réussi leur tentative de tricherie, ce qui laisse la porte ouverte pour d'autres tentatives.

3. Solution Proposée :

Le travail consiste à la conception et la mise en œuvre d'un système de contrôle d'identité des étudiants rapide et efficace au sein de l'université afin de s'assurer que les candidats passant les examens sont bien les inscrits et pas des tricheurs
La solution proposée par notre travail est de réaliser une application Android qui permet de répondre aux besoins demandés. Pour cela notre système permet :

- L'accès sécurisé à l'application aux informations par les enseignants surveillants des examens.
- Recherche d'un étudiant et affichage de ses informations.
- Contrôle de présence de l'étudiant dans une salle d'examen (y compris les étudiants dettes).
- Vérification de l'état de l'étudiant par rapport a un examen programmé en termes de matière, unité ou semestre acquis pour valider sa présence à la salle.
- Prise d'empreinte des étudiants afin de les identifier.

- Mettre une solution alternative en cas de panne du lecteur d'empreinte ou bien un autre problème. Dans la lecture de l'empreinte par une autre méthode sécurisé d'identification (exemple : entrer du matricule et affichage des informations de l'étudiants avec sa photo).
- Facilité la possession de l'état du passage de l'examen pour chaque salle à tout moment.
- L'application doit connecter avec une BDD locale .cette dernière comporte les facultés d'université, les départements, les salles, les informations des étudiants inscrits(matricule ,nom prénom, état étudiant , empreinte , photo) section ,groupe ,promo ,spécialité ,semestre ,module a une année universitaire et leurs photos et leurs empreintes sous formes des images, les images sont codée par le matricules des étudiants.(comme expliquée dans le MLD)
- La BDD est met a jour chaque début d'Anne par un responsable administratif



4. Méthode UML :

4.1. Définition :

UML (langage de modélisation unifié) est issu de l'unification de nombreux langages de modélisation graphique à base des concepts orientés objets, Il est apparu dans le monde du génie logiciel. Couramment utilisé dans les projets logiciels, il peut être appliqué à toutes sortes de systèmes ne se limitant pas au

domaine informatique.

Les diagrammes UML permettent de communiquer l'architecture d'un système aux concepteurs, développeurs et à toutes personnes externes à l'aspect technique d'un système.

5. Définition des diagrammes :

Les diagrammes sont des éléments graphiques. On distingue deux types de diagrammes :

5.1. Diagrammes dynamiques :

Montrant le fonctionnement du système.

5.1.1. Définition de Diagramme de cas d'utilisation :

Il Permet de décrire l'interaction entre l'acteur et le système.il permet de définir les limites du système et les relations entre un système et l'environnement. Chaque résultat possible de l'exécution d'un cas d'utilisation est appelé scénario.

5.1.1.1. Quelques définitions de base :

- **Acteur:**

  Représente un rôle que peut jouer l'utilisateur dans le système. L'acteur est associé à un cas d'utilisation, c'est-à-dire qu'il peut interagir avec lui et participer à son scénario en fournissant de l'information en entrée et /ou la reçoit en sortie. Il existe 2 types d'acteurs [16]

  - **Primaire :**

    Est le destinataire « privilégié » de l'application. Il est actif en ce sens que c'est lui qui initie les interactions.

  - **Secondaire :**

    Un acteur pour lequel l'application n'offre qu'un service marginal. Il est passif en ce sens qu'il ne fait que répondre à des sollicitations du système.

- **Cas d'utilisation :**

  Le cas d'utilisation est un des outils importants d'UML. Un cas d'utilisation, c'est simplement la description des interactions entre l'utilisateur et le système. En produisant une collection des cas d'utilisation, on arrive à décrire l'ensemble des fonctionnalités à développer d'une façon claire et compréhensible pour tous les intervenants d'un projet. Il s'agit donc là d'une conception du système centrée sur l'utilisateur et sur les tâches qu'il peut accomplir. [16]

- **Scénario**

  C'est un chemin logique traversant le cas d'utilisation. Un scénario est une instance de cas d'utilisation. [16]

- **La relation inclue :**

  Une relation inclusion d'un cas d'utilisation A par rapport à un cas d'utilisation B, signifie qu'une instance de A contient le comportement décrit dans B, le cas d'utilisation A ne peut pas être utilisé seul. [16]

5.1.1.2. Scénario de contrôle biométrique d'identité d'un étudiant pour autoriser l'assistance a un examen au sein d'université du Médéa :

1. un examen programmé a une salle et cette salle est un prof surveillant et port un group, un étudiant associé a ce groupe
2. l 'étudiant viendra pour passer l'examen
3. le prof faire le 'login'
4. le prof choisi les cordonnes du ' faculté', 'département', 'filière ', ' spécialité' , 'promotion' , 'semestre' 'module ','salle' .
5. le prof présente l'appareil, l'étudiant faire l'empreinte ou matricule
6. la dernière exécution afficher un message comporte les cordonnes d'étudiant, « OK » ou « NO» et sa photo personnel
7. si le msg afficher « OK » c-a-d : l'étudiant est affecté a cette salle et la moyen de module et unité et semestre inf à 10
8. l'étudiant peut terminer l'examen
9. le prof assure la présence et passer a un autre étudiant
10. si le msg « NO » c-a-d :
    - Moyenne du semestre supérieure à 10
    - Moyenne d'unité supérieure à 10
    - Moyenne du module supérieure à 10
    - La Salle d'affectation est différente
11. l'application faire la recherche sur l'étudiant après l'accès à la bdd du promotion du spécialité lui mm
12. l'application affiché msg concerne les cordonnes du l'étudiant, sa photo et salle d'affectation
13. le prof dirigé l'étudiant à la salle affiché
    - Étudiant n'existe pas
14. afficher le msg étudiant n'existe pas
15. le prof doit demander à l'étudiant pour quitter l'examen et la salle
16. un prof remplaçant peut remplacer le prof surveillant et il peut faire tous la fonction qu'il peut faire ce dernier

5.1.1.3. Diagramme de cas d'utilisation :

Ce diagramme de cas d'utilisation a été construit par le scenario qui présente les étapes du contrôle biométrique d'identité pour autoriser l'assistance à un examen au sein d'université

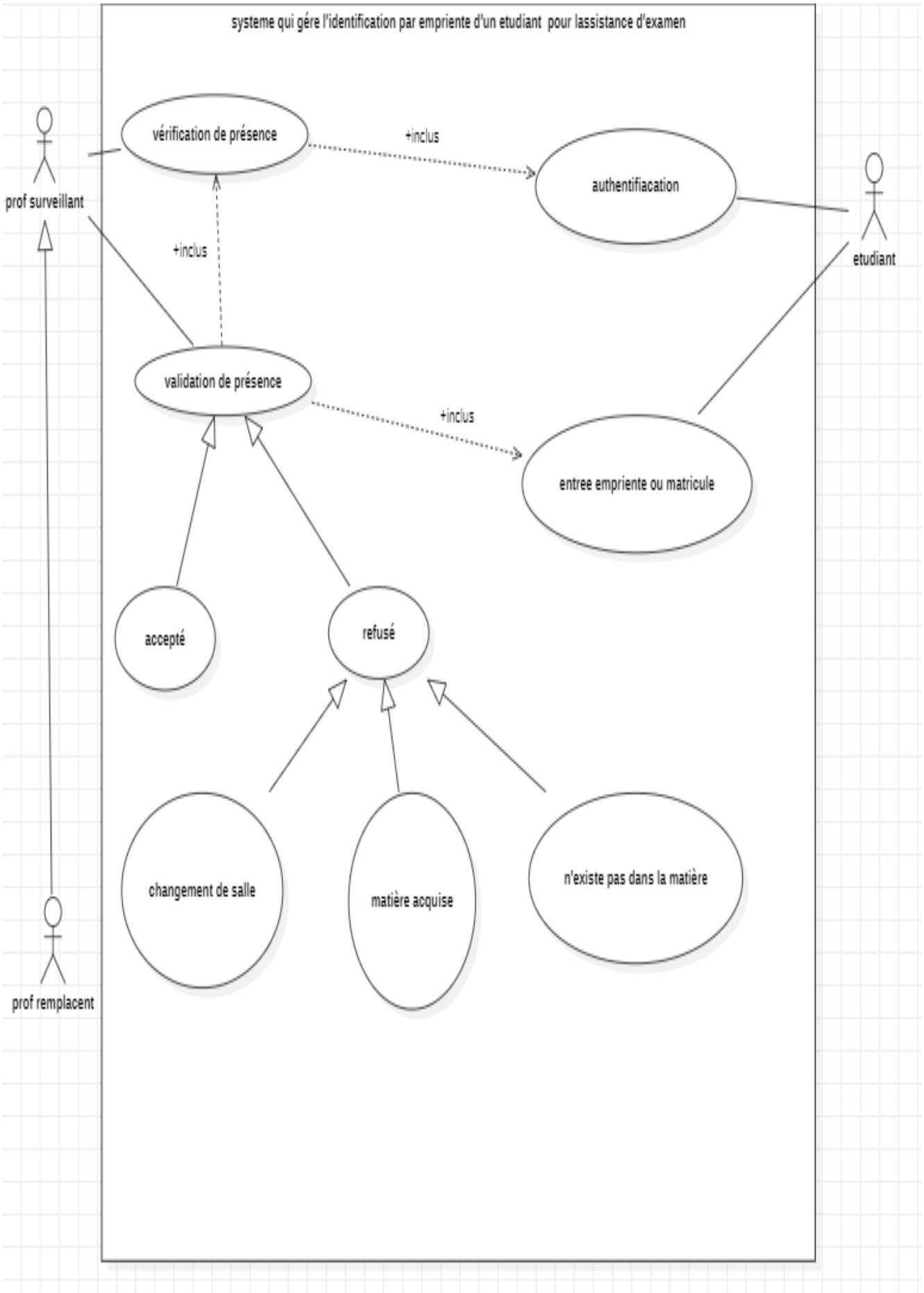


Figure 22 : Diagramme de cas d'utilisation

5.2. Diagrammes statiques :

C'est-à-dire représentant le système physiquement

5.2.1. Définition Diagramme de classe :

Le diagramme de classes est représentation de la structure interne du logiciel ou est un schéma utilisé pour présenter les classes et les interfaces des systèmes ainsi que les différentes associations entre celles-ci permettent d'exprimer une connexion sémantique bidirectionnelle entre deux classes qui sont liées. [17]

5.2.1.1. Quelques définitions de base :

- **Classe :**
  regroupement d'objet de même nature (mêmes attributs mêmes opérations).
- **Méthodes :**
  c'est-à-dire l'ensemble des actions (appelées opérations) que l'objet est à même de réaliser. Ces opérations permettent de faire réagir l'objet aux sollicitations extérieures (ou d'agir sur les autres objets). De plus, les opérations sont étroitement liées aux attributs, car leurs actions peuvent dépendre des valeurs des attributs, ou bien les modifier.
- **Association :**
  relation binaire (en général) nomme l'extrémité dune association, permet d'accéder aux objets liés par l'association a un objet donné. [18]
- **Attribut :**
  propriété partagée par tous les objets de la classe, associe à chaque objet une valeur. [17]
- **Cardinalité :**
  contraint le nombre d'objet lies par l'association. .

5.2.1.2. Diagramme de classe :

Le diagramme si dessous exprimer la structure générale de la base de données de notre application :

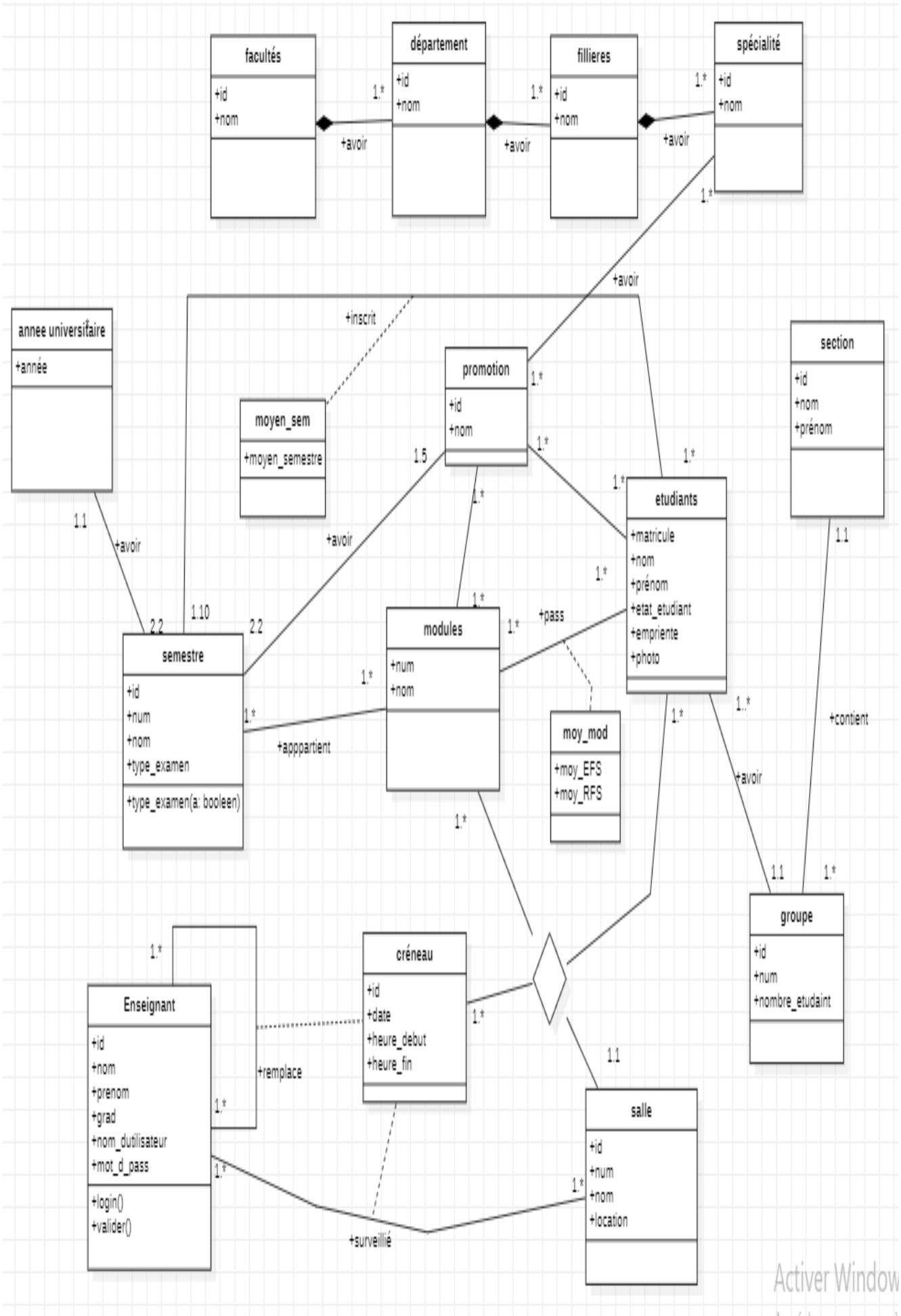


Figure 23 : Diagramme de classe

5.2.1.2.1. Description de la classe :

Classe :	Attribut / Méthode :	Type :	Description :
facultés	Id	Entier	Identification
	Nom	Chaine de caractère	Nom de faculté
département	Id	Entier	Identification
	Nom	Chaine de caractère	Nom de département
fillieres	Id	Entier	Identification
	Nom	Chaine de caractère	Nom de filière
spécialité	Id	Entier	Identification
	nom	Chaine de caractère	Nom de spécialité
annee universitaire	année	Date	Nom de l'année universitaire de promotion
Semestre	Id	Entier	Identification
	Num	Chaine de caractère	Existe il 10 semestre numéroté de 1 jusqu'à 10 a l'ordre croissant chaque promotion avoir 2 semestre
	Nom	Chaine de caractère	Nom de semestre
	type_examen	Chaine de caractère	Concernent les sessions d'Anne soit : normale /rattrapage
	type_examen (a : booléen)	Booléen	True : examen False : rattrapage
Moy_sem	moyen_semestre	Réel	Précision de session de validation de semestre
promotion	Id	Entier	Identification
	nom	Chaine de caractère	Nom de promotion
modules	Num	Chaine de caractère	Identification

	Nom	**Chaine de caractère**	**Nom de modules**
	moy_unité	**Reel**	**l'unité sup a 10 c-a-d : l'étudiant n'a pas le droit de passer RFS de ses modules**
	moy_module	**Reel**	**Si la moyenne de module est sup a 10 L'étudiant n'a pas le droit de passer le RFS de ce module**
Enseignant	**Id**	**Entier**	**Identification**
	Nom	**Chaine de caractère**	**Nom de l'enseignant**
	Prénom	**Chaine de caractère**	**Prénom de l'enseignant**
	Grade	**Chaine de caractère**	**Grade d'enseignant (titulaire , vacataire ,docteur)**
	Nom_dutilisateur	**Chaine de caractère**	**Nom d'utilisateur crée par l'enseignant exprimé un droit d'accès**
	mot_d_pass	**Chaine de caractère**	**Mot de passe crée par l'enseignant exprimé un droit d'accès**
	login()	**Chaine de caractère**	**Une opération faite pour l'accès privé aux donnes de la faculté**

Classe	**Attribut / Méthode :**	**Type :**	**Description :**
créneau	**id**	**Entier**	**Identification**
	date	**date**	**Date de jour de l'examen**
	heure_debut	**Date**	**Heur début d'examen**
	heure_fin	**Date**	**Heure fin d'examen**
etudiants	**matricule**	**Chaine de caractère**	**Identification**
	nom	**Chaine de caractère**	**Nom d'étudiant**
	prénom	**Chaine de caractère**	**Nom d'étudiant**

	etat_etudiant	**Chaine de caractère**	**État d'étudiant est : soit (normale /dette)**
	empreinte	**Longblob**	**L'empreinte d'étudiant est stocké dans la bdd sous forme image**
	photo	**Longblob**	**Photo personnalisé d'étudiant est stocké dans la bdd sous forme photo**
Moy_mod	**moy_EFS** **moy_RFS**	**Entier**	**Moyenne EFS : moyenne d'examen** **Moyenne RFS : moyenne de rattrapage**
section	**id**	**Entier**	**Identification**
	nom	**Chaine de caractère**	**Nom de section**
groupe	**id**	**Entier**	**Identification**
	num	**Chaine de caractère**	**Numéro de groupe dans la section**
	nombre_etudaint	**Entier**	**Nombre d'étudiant dans un seul groupe**
Salle	**id**	**Entier**	**Identification**
	num	**Chaine de caractère**	**Numéro de salle**
	nom	**Chaine de caractère**	**Nom de salle**
	localisation	**Chaine de caractère**	**La localisation de la salle dans la zone d'université**

Table 3 : description des classes

6. Model relationnel : MLD

La figure si dessous exprimer la structure générale de la base de données par la représentation du « model relationnel » de notre application :

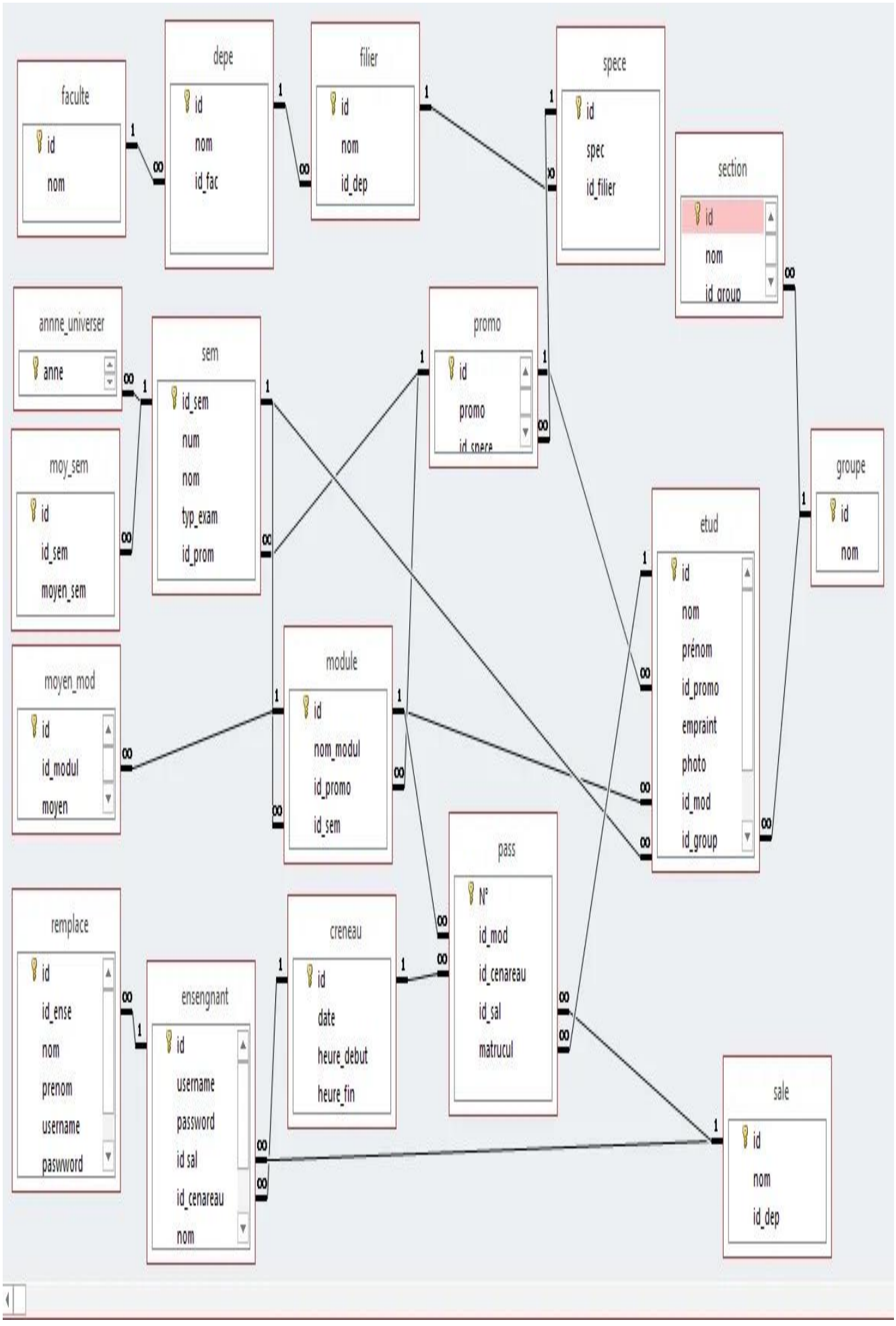


Figure 24 : model relationnel de notre Bdd

7. Conclusion :

Après avoir essayer de recenser les problèmes rencontrés dans les salles d'examen en terme de contrôle d'identité, nous avons fixé les objectifs souhaités et ainsi explorer quelques présentations d'UML fournis pour la conception statique et dynamique de l'application en établissant les diagrammes de cas d'utilisation, et de classes pour faciliter la réalisation de notre application. Dans le chapitre suivant nous montrerons les étapes, plus en détails, que nous avons suivies pour implémenter et réaliser notre solution.

Chapitre III :

Implimentation et résultat

1. Introduction :

Informatiser le système d'information est aujourd'hui le souci de tout établissement pour suivre le développent de la technologie et améliorer le rendement du travail. Plus particulièrement, et dans la cadre de notre travail, nous nous intéressons à conception et mise en œuvre d'une application androïde de contrôle biométrique d'identité pour autoriser l'assistance à un examen au sein d'université de Médéa.

2. Architecture de développement :

L'architecteur d'application que nous décrivons est plutôt MVC ou **Modèle-vue-contrôleur** ou est un motif d'architecture logicielle destiné aux interfaces graphiques. Le motif est composé de trois types de modules ayant trois responsabilités différentes : les modèles, les vues et les contrôleurs.

- Un modèle (Model) contient les données à afficher.
- Une vue (View) contient la présentation de l'interface graphique.
- Un contrôleur (Controller) contient la logique concernant les actions effectuées par l'utilisateur. [26]

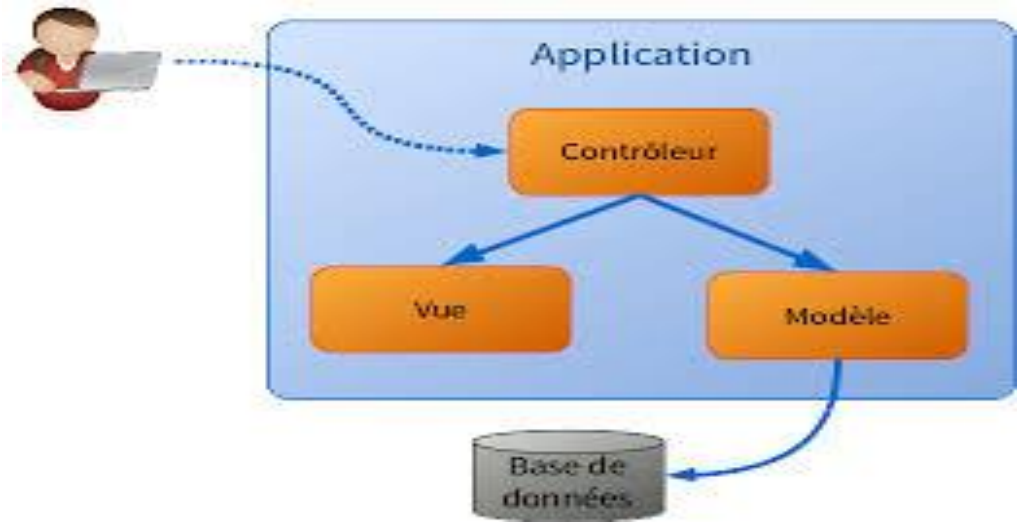


Figure 25 : architecture de modèle-vue-contrôleur [26]

3. Technologie utilisée :

3.1. Partie matériel :

On utilise :

-Un micro portable « lenovo » de processeur i5

-Un lecteur d'empreinte

3.2. Partie logicielles :

3.2.1.Visual Studio Code :

Visual Studio Code est un éditeur de code simplifié, qui est gratuit et développé en open source par Microsoft. Il fonctionne sous Windows, mac OS et Linux. Il fournit aux développeurs à la fois un

environnement de développement intégré avec des outils permettant de faire avancer les projets techniques, de l'édition, à la construction, jusqu'au débogage

Visual Studio Code permet également aux développeurs de créer et d'utiliser des extensions grâce à son API, afin de personnaliser leur utilisation de l'outil. Il est livré avec un support pour JavaScript, TypeScript et Node.js. [27]

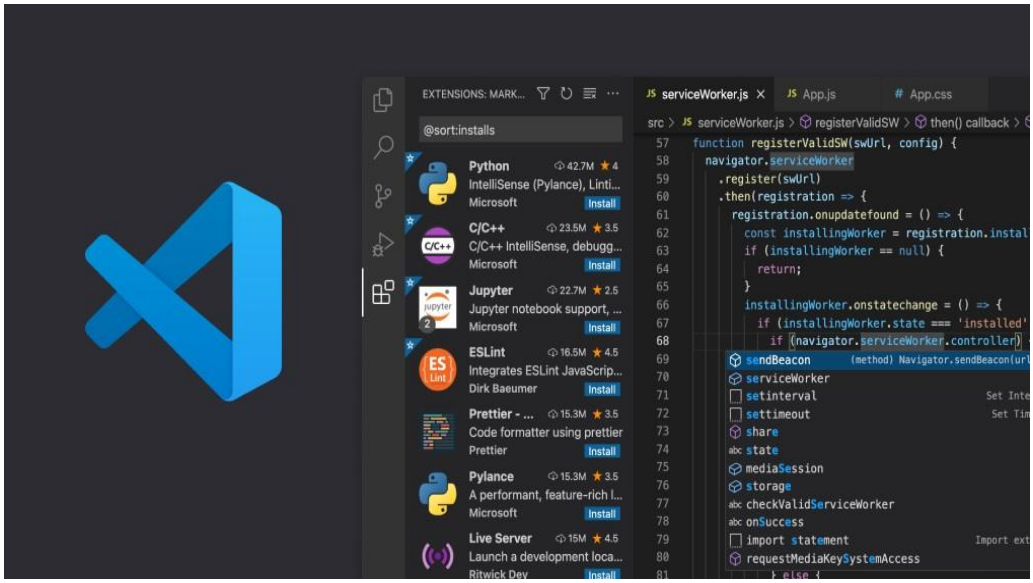


Figure 26 : L'icône de l'éditeur « Visual Studio » [28]

3.2.2. Dart :

Dart est un langage de programmation, qui a été et est développé principalement par Google. Il est standardisé par Ecma (Ecma est une organisation internationale de normalisation des systèmes d'information et de communication ainsi que des appareils électroniques grand public). La programmation dans Dart doit être une **alternative attrayante à JavaScript** dans des navigateurs Web modernes. D'après les développeurs de Dart, les faiblesses de JavaScript ne peuvent plus être corrigées par son développement. [29]



Figure 27 :L'icône de Dart [29]

3.2.3. Android Studio :

est un environnement de développement pour développer des applications mobiles Android. Il est basé sur IntelliJ IDEA et utilise le moteur de production Gradle. Il peut être téléchargé sous les systèmes d'exploitation Windows, macOS, Chrome OS et Linux). [30]



Figure 28 : L'icône de l'Android studio [30]

3.2.4. Flutter :

Flutter est un framework opensource de développement d'applications mobiles natives créé par Google en 2017. Il permet d'écrire des applications Android et iOS en un seul code partagé, à la manière de Xamarin.Forms. Flutter utilise des SDK d'Android et d'iOS afin d'avoir un rendu natif, que ce soit en utilisant le Material Design ou Cupertino. Il est ainsi possible d'avoir un rendu d'application utilisant le material design sur iOS, ainsi qu'une application cupertino sur Android. Comme pour tout développement d'application iOS, une machine macOS est nécessaire pour compiler l'application iOS.[31]



Figure 29 : L'icône de Flutter [31]

3.2.5. StarUML :

Est un logiciel de modélisation UML (Unified Modeling Language) open source qui peut remplacer dans bien des situations des logiciels commerciaux et coûteux comme Rational Rose1 ou Together2. Étant simple d'utilisation, nécessitant peu de ressources système, supportant UML 2, ce logiciel constitue une excellente option pour une familiarisation à la modélisation. Cependant, seule une version Windows est disponible. [32]



Figure 30 : L'icône de StarUML [32]

3.2.6. XAMPP :

est un ensemble de logiciels servant à mettre en place aisément un serveur Web, un serveur FTP et un serveur de messagerie électronique. C'est une distribution de logiciels libres (X Apache MySQL Perl PHP) offrant une bonne souplesse d'utilisation, reconnue pour son installation simple et rapide. Ainsi, il est à la portée de la plupart de personnes dans la mesure où il ne requiert pas de connaissances spécifiques et fonctionne, qui plus est sur les dispositifs d'exploitation les plus communs.

Il est distribué avec différentes bibliothèques logicielles qui élargissent la palette des services de façon notable : OpenSSL, Expat (parseur XML), PNG, SQLite, zlib, ... mais aussi différents modules Perl et Tomcat. Bon nombre de personnes critiquent la quantité d'extensions ajoutées qui sont pour la majorité inutiles aux débutants. Une version lite à donc été mise en place [33]



Figure 31 :L'icône de Xampp [33]

3.2.7. PHP 'Hypertext Preprocessor ':

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

PHP a permis de créer un grand nombre de sites web célèbres, comme Facebook et Wikipédia. Il est considéré comme une des bases de la création de sites web dits dynamiques mais également des applications web.[34]



Figure 32 : L'icône de PHP [34]

3.2.8. La BDD :

On importe une BDD locale comporte les cordonnes des étudiants déjà inscrits et leurs photo personnelles et leurs empreintes sous formes des images. (On explique tous les détails dans la partie conception), La BDD est met a jour chaque début d'Anne par un responsable administratif

4. Travaille réalisée :

Dans ce qui suit nous présentons les différentes interfaces de l'application en citant les détails de chacune.

4.1. La fonctionnement du l'application avec la BDD :

-Une fois l'étudiant est inscrit dans l'Université il faut prendre leur empreinte et stocké sous formes images dans la BDD

-Les empreintes et les photos sont prendre les matricules des étudiants comme noms

-l'étudiant faire l'empreinte dans « fingerprint_identity » sur le smartphone

-l'application « fingerprint_identity » compare l'empreinte entrée avec les empreintes stockées

-retourner les résultats sous forme msg

4.2. Icone de l'application « fingerprint_identity » :

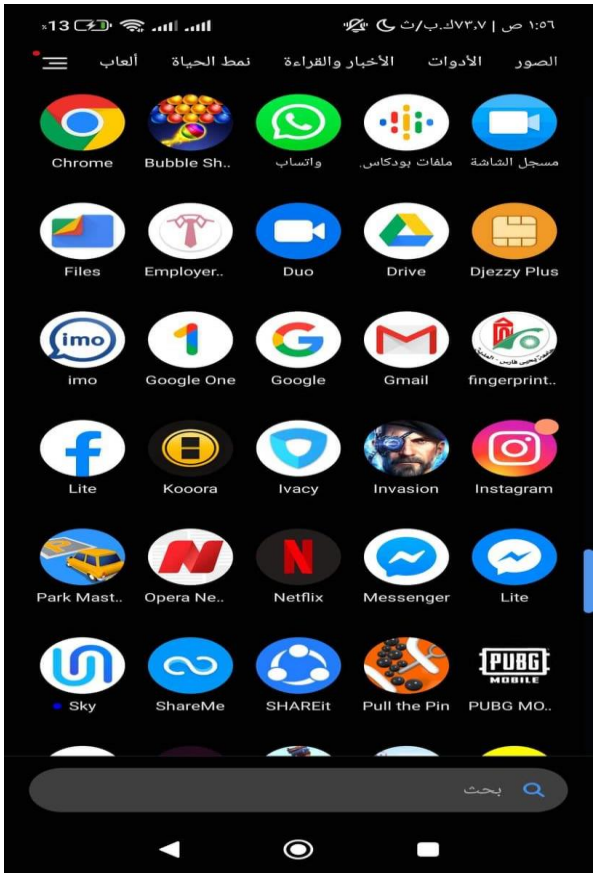


Figure 33 : L'icône de « fingerprint_identity »

4.2.1. Informations sur « fingerprint_identity » :

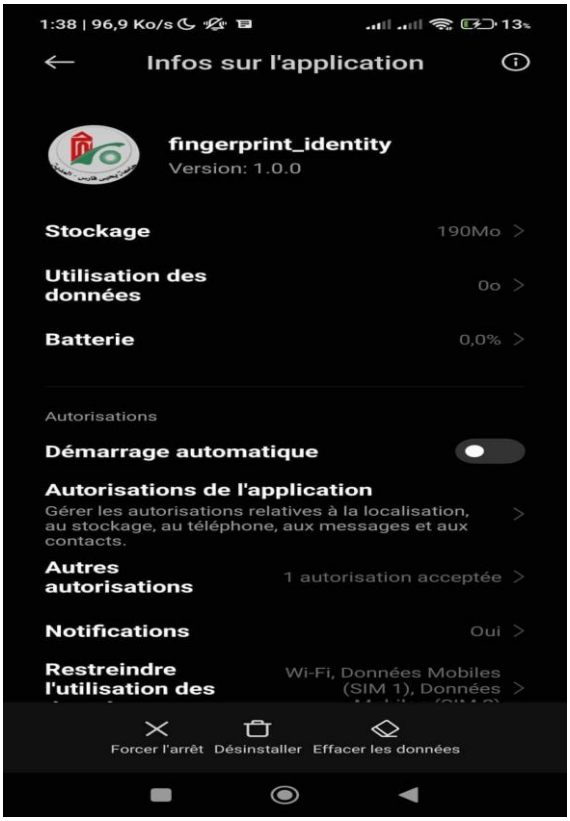


Figure 34 : capteur sur les informations du l'application installé

4.3. Interface de « login » :

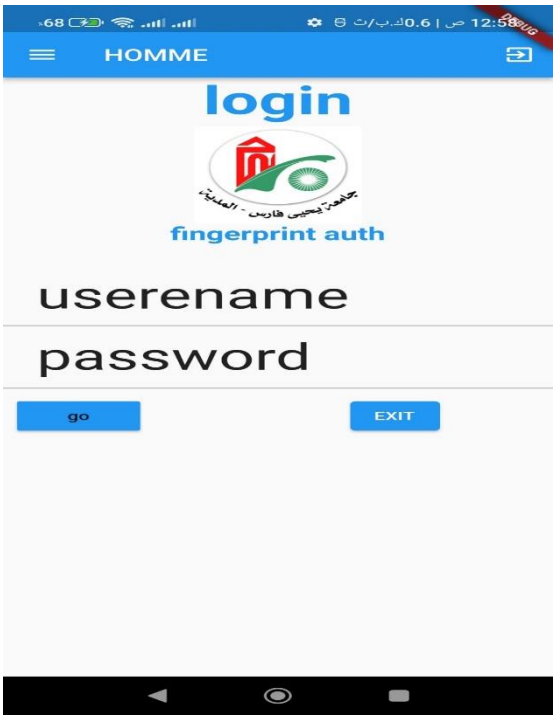


Figure 35 : L'interface d'authentification

Cette interface spéciale pour le prof surveillant (remplaçant) inscrit déjà dans la bdd qui permet de faire le contrôle d'assistance des étudiants d'un examen

4.4. Interface d'accueil :

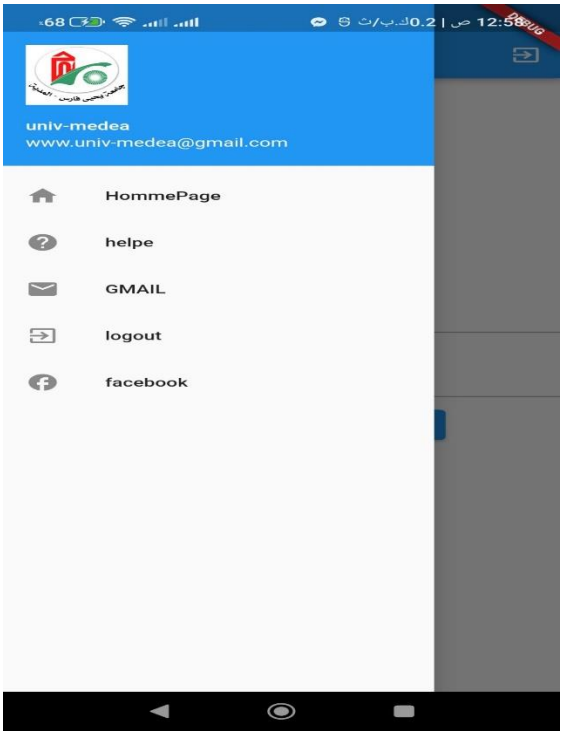


Figure 36 :L'interface d'accueil

4.5. Interface de contrôle :

Dans cette page l'enseignant doit choisir les cordonnes du

' Faculté', 'département', 'filière ', 'spécialité',

'Promotion' , 'semestre' 'module ','salle'

NB : pas d'obligatoire de sélectionne l'année universitaire

Car Le responsable administratif de BDD faire MAJ et

Donne l'accès a l'année scolaire en cours

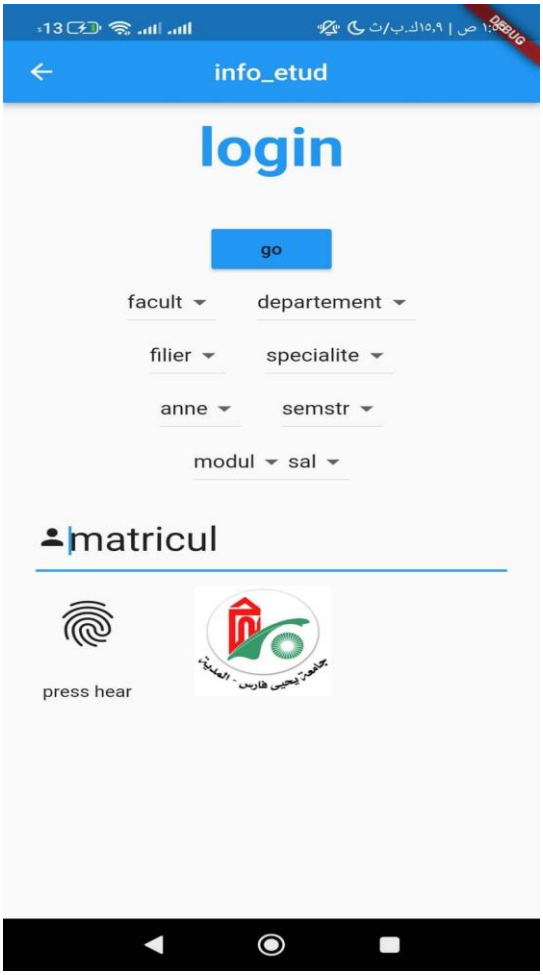


Figure 37 : l'interface de contrôle

Ex :

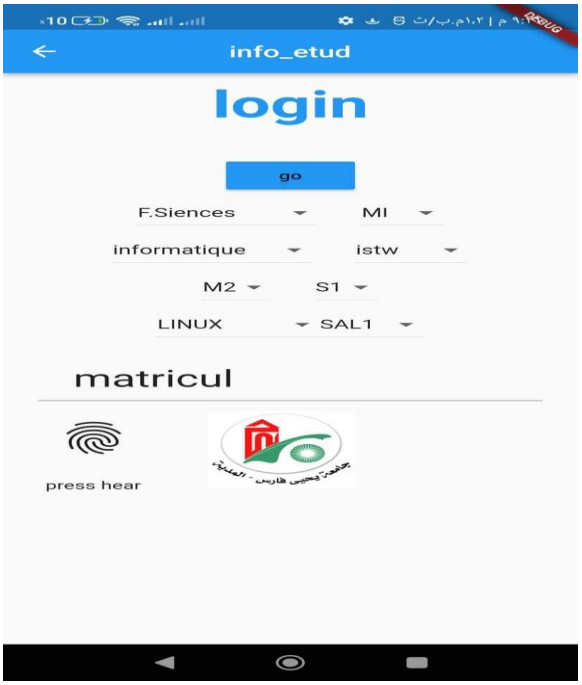


Figure 38 : l'interface de contrôle après la sélection des cordonnes

On fait un test :

L'étudiant faire l'empreinte ou matricule : (le matricule doit entrer en cas de panne de l'empreinte)

NB : en tout les cas l'application affiche la photo d'étudiant.

Le msg apparaît quelques instants puis disparaît.

1ère cas : l'étudiant ayant la moyenne d'un module sup à 10 :

Résultats :



Figure 39 : capteur sur « moyenne sup à 10 »

Dans ce cas l'étudiant doit quitter l'examen

2eme cas : l'étudiant ayant la moyenne d'unité sup à 10 :

Résultats :

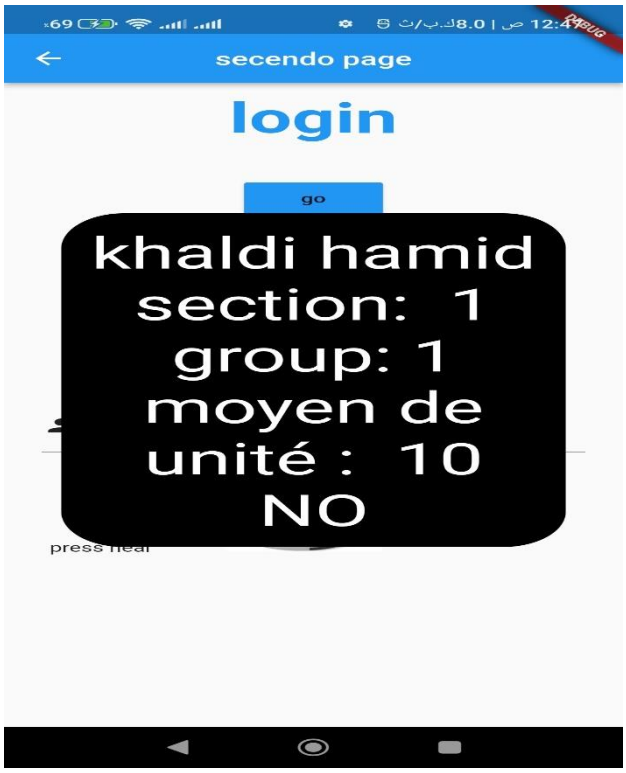


Figure 40 : capteur sur « moyenne d'unité sup à 10 »

Dans ce cas l'étudiant doit quitter l'examen

3eme cas : l'étudiant ayant la moyenne de semestre sup à 10 :

Résultats :

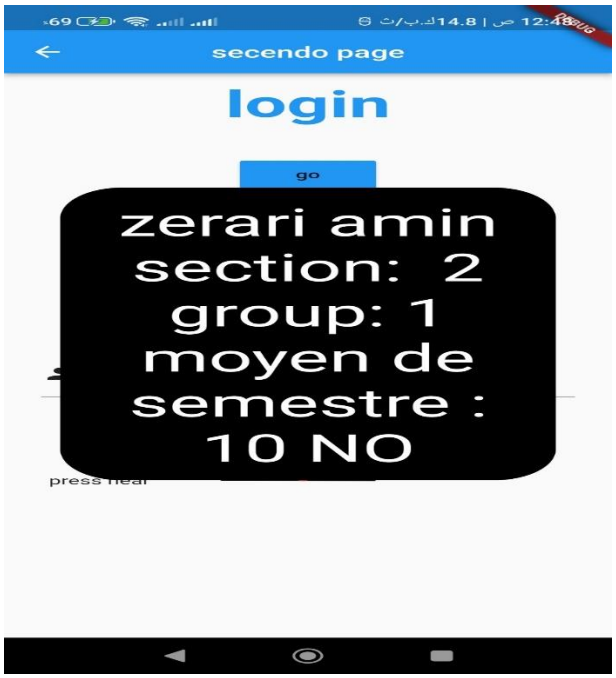


Figure 41 : capteur sur « moyenne de semestre sup à 10 »

Dans ce cas l'étudiant doit quitter l'examen

4eme cas : l'étudiant a affecté à déférente salle :

Résultats :



Figure 42 : capteur sur « salle d'affectation est déférente »

Dans ce cas l'étudiant doit changer la salle et va a la salle num ' 13 ' (l'application ne voit pas la moyenne)

52eme cas : l'étudiant ayant la moyenne d'un module inf à 10 :

Résultats :

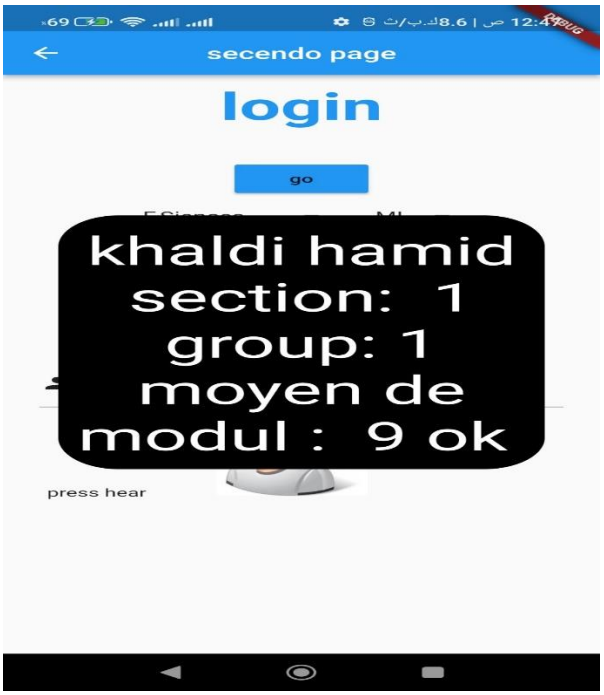


Figure 43 : capteur sur « la moyenne d'un module inf à 10 »

L'étudiant est affecté à cette salle et la moyen de module (l'application est précisé si la moyenne d'unité ou semestre ou module) inf à 10

5.Conclusion :

La partie de réalisation détermine une idée plus claire sur les taches qui sont réalisé dans cette application nous avons présenté les différentes interfaces de l'application ainsi que les captures des résultats de test ,Le temps n'était pas de notre côté, car nous avons pu ajouter un état de sortie, qui est une feuille de présence numérique qui est placée avec les feuilles de réponses.

Enfin avec ce chapitre presque on termine la phase de développement de notre application dans laquelle la porte d'amélioration reste ouverte.

Conclusion générale

Conclusion générale :

Le contrôle par empreinte digitale est domaine qui reste nouveau dans les applications des étudiants. Notre projet fin d'étude consiste à concevoir une application de Reconnaissance des empreintes digitales qui permet de réaliser un système biométrique qui fait l'authentification des étudiants selon leurs empreintes digitales. Son application peut être utilisé dans plusieurs thèmes. Nous avons appliqué cette technique dans un système utile qui élimine beaucoup de problèmes dans l'université, à savoir la mise en œuvre d'une application biométrique à base d'empreintes digitales permettant le contrôle d'accès des étudiants aux examens.Ce système fonctionnée au cour de compraison des images des emprientes.

La réalisation parfaite d'une telle application nécessite un temps considérable En raison des contraintes, nous n'avons pas pu compléter cette demande, car nous pouvons augmenter les cas exceptionnels des étudiants, comme les étudiants endettés ou l'ajout de quelques états de sortie comme la feuille de présence, qui est la preuve tangible de la présence de l'étudiant à l'examen.
Cela veut dire que notre travail ouvre une fenêtre à d'autres sujets dans le domaine tel que l'identification par d'autres moyens ou bien l'identification hybride ainsi que l'utilisation de cette identification dans d'autres structures.

Références:

[1] : Mr. AKROUF S, Une Approche Multimodale pour l'Identification du Locuteur

THESE de doctorat en informatique, université ferhat abbas Sétif, 2011

http://dspace.univ-setif.dz:8888/jspui/bitstream/123456789/28/1/Thèse%20Samir%20Akrouf.pdf

[2]:A. Jain, R. Bolle, S. Pankanti, « Biometrics: Personal Identification in Networked Society », Kluwer, New York, Michigan university , 1998

https://books.google.dz/books?hl=fr&lr=&id=XPC9ucFbddsC&oi=fnd&pg=PP11&dq=A.+Jain,+R.+Bolle,+S.+Pankanti,+%C2%AB+Biometrics:+Personal+Identification+in+Networked+Society+%C2%BB,+Kluwer,+New+York,+1998&ots=zKdkhQ9a-V&sig=fBwHdK2_BRp21nRkOpqcSQydiR0&redir_esc=y#v=onepage&q=A.%20Jain%2C%20R.%20Bolle%2C%20S.%20Pankanti%2C%20%C2%AB%20Biometrics%3A%20Personal%20Identification%20in%20Networked%20Society%20%C2%BB%2C%20Kluwer%2C%20New%20York%2C%201998&f=false

[3]:Ben Hamed A , Medjadji O , Mémoire de Master en Informatique , Reconnaissance des Empreintes

http://dspace.univtlemcen.dz/bitstream/112/8105/1/Reconnaissance_des_Empreintes_Digitales.pdf

[4] : Boussa R , Boussad F , Mémoire de master en Informatique , Développement d'un système biométrique multimodal basé sur la fusion des scores de matching

https://www.ummto.dz/dspace/bitstream/handle/ummto/13212/Boussa%20R.%3B%20Boussad%20F..pdf?sequence=1&isAllowed=y

[5] : http://www.biometrie-online.net

[6] : https://fr.hellosign.com/what-is-hellosign/digital-signature-free#:~:text=Une%20signature%20numérique%20désigne%20un,l'expéditeur%20et%20le%20signataire

[7] : https://tel.archives-ouvertes.fr/tel-00009742

Étude d'un système complet de reconnaissance d'empreintes digitales pour un capteur microsystème à balayage N. Galy

[8] : Clémence Carron, « Les vrais jumeaux ont-ils les mêmes empreintes digitales ? », Pour la science, o 396,.

[9]: P. Meenen, R. Adhami, "Fingerprinting for Security", IEEE potentials, vol. 20, n°3, p. 33-38, 2001.

[10]: DGSN :la Police scientifique de Tlemcen

[11] : H. V. DANG, " Biométrie pour l'Identification". Rapport final du tipe, Institut de la Francophonie pour l'Informatique, 2005.

[12]: F.Jaam, M.Rebaiaia et A.Hasnah. " A Fingerprint Minutiae Recognition System Based on Genetic Algorithms ". The Internationnal Arab Journal of Information Technology, Vol.3, No.3, pp.243-245, July 2006

[13] : G.Nedjma S.Karima, Mémoire de master, Développement d'un système biométrique pour la reconnaissance de visages, basé sur les ondelettes et les réseaux de neurones, universite mouloud mammeri de tizi-ouzou

[14]: https://1.bp.blogspot.com/-zUYVmTAGKXI/VpVjfdfjd0I/AAAAAAAAOWw/pHCviXf_f8s/s1600/TI+Biometrics.JPG

[15]: https://slideplayer.fr/slide/465924/1/images/9/Architecture+d%E2%80%99un+syst%C3%A8me+de+reconnaissance+biom%C3%A9trique.jpg%EF%BF%BC

[16]: Slemane F , Si Randane N , Mémoire de licence en informatique, conception et réalisation d'un site web pour une clinique privée cas : clinique pluridisciplinaire 'SLIMANA' Tizi-Ouzou.2009-2010 .

[17]: Boudaoud r , Mémoire de licence en informatique, Conception et réalisation d'un site web dynamique pour une agence immobilière Cas: agence AKILI Tizi-Ouzou.2008-2009.

[18]: cours deuxième année système d'information 'génie logiciel '

[19] : https://megastuces.com/wp-content/uploads/2015/05/signature.jpg

[20] : http://www.zalix.fr/images/stories/produits/ZX-50/lecteur-biometrique-morphologie-main-handkey2-ZX-50-1.jpg

[21] : https://cdn.futura-sciences.com/buildsv6/images/mediumoriginal/c/d/2/cd2b7e5d7f_118506_album-oreille15.jpg

[22] : https://www.elysia-bioscience.com/wp-content/uploads/2020/12/adn-nucleaire-1-1006x1024.png

[23] : https://i.ytimg.com/vi/bBrxtXwUdUA/maxresdefault.jpg

[24] : https://www.hellopro.fr/lecteur-biometrique-handkey-2008231-82224-produit.html

[25] : https://www.arotek.mg/web/image/3068-65abc8b7/reconnaissance%20faciale%20arotek.jpg

[26] : https://fr.wikipedia.org/wiki/Modèle-vue-contrôleur

[27] : https://www.blogdumoderateur.com/tools/visual-studio-code/

[28] : https://www.blogdumoderateur.com/tools/visual-studio-code/#images-1

[29] : https://www.ionos.fr/digitalguide/sites-internet/developpement-web/le-langage-de-programmation-dart/

[30] : https://www.encyclopedie.fr/definition/Android_Studio

[31] : https://blogs.infinitesquare.com/posts/mobile/flutter-un-nouvel-espoir

[32] : http://inf1410.teluq.ca/teluqDownload.php?file=2014/01/INF1410-PresentationStarUML.pdf

[33] : http://www.standard-du-web.com/xampp.php

[34] : Benchennane I , Etude et mise au point d'un procédure biométrique multi-modale pour la reconnaissance des individus , University of sciences and technology in Oran, 2015.