REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'enseignement Supérieur et de la Recherche Scientifique

Université du 20 Aout 1955 - Skikda

Faculté des sciences

Département informatique

Mémoire de fin d'étude :

En vue de l'obtention du diplôme de Master

En informatique

Option : intelligence Artificielle

Thème

Conception et réalisation d'un système de reconnaissance facial en milieu scolaire

Encadré par :

Dr. CHEIKH Ramande

Réalisé par :

Mr.BOUTAGHANE Ahcene

Mr.TALHA Abdelhadi

Promotion : 2023/2024

Session Juin 2024

Remerciements

« Avant toutes choses, nous remercions DIEU Grand et Puissant de nous avoir donné la volonté et le courage d'accomplir notre cursus universitaire et de mener ce travail jusqu'à la fin et cela en dépit des difficultés.

Nous remercions notre Encadreur DR. CHEKH Ramdane pour son suivi tout au long de ce travail, pour ses encouragements et sa bonté.

Nos remerciements vont également aux membres du jury, vous nous faites honneur en jugeant notre humble travail. Veuillez accepter notre profonde reconnaissance.

Enfin, nous tenons à exprimer nos vifs remerciements à tous ceux qui ont contribué de près ou de loin à l'élaboration de ce travail ».

Dédicaces

En témoignage de ma profonde affection et de ma reconnaissance, je dédie ce modeste travail :

À mes parents, je leurs dits merci du fond de mon cœur pour tous les sacrifices consentis pour mon éducation et ma formation.

À tous mes frères et sœurs, ainsi que leurs enfants.

À toute ma famille.

À tous les étudiants.

À tous mes amis et collègues.

À tous ceux qui me connaissent et qui m'ont encouragé de Près ou de loin…

Boutaghane ahcene.

Dédicaces

En témoignage de ma profonde affection et de ma reconnaissance, je dédie ce modeste travail :

À mes chers parents, je leurs dits merci du fond de mon cœur pour tous les sacrifices consentis pour mon éducation et ma formation.

À ma femme.

À tous mes frères et sœurs.

À toute ma famille.

À tous mes amis et collègues.

À tous ceux qui me connaissent et qui m'ont encouragé de Près ou de loin…

Talha abdelhadi

Résumé

La reconnaissance faciale est largement considérée comme l'un des moyens biométriques les plus efficaces pour identifier et authentifier les individus. Et vu que la gestion de la présence et de l'absentéisme dans les écoles avec les méthodes traditionnelles actuelles ne parviennent pas souvent à fournir des données de fréquentation précises et en temps réel, il nécessite de trouver des alternatives.

Cette problématique est devenue une préoccupation majeure, ayant un impact sur les élèves, les enseignants et le système éducatif dans son ensemble.

Pour faire face à ces défis nous avons développé un système intelligent qui automatise le processus de vérification d'identité et de suivi de la présence des élèves, tout en remplaçant les méthodes traditionnelles actuellement utilisées dans les établissements d'enseignement.

À cet égard, pour répondre aux besoins des institutions éducatives, les responsables doivent prendre des mesures appropriées et rechercher constamment des solutions pour utiliser les méthodes avancées de l'intelligence artificielle(IA), telles que l'apprentissage automatique et l'apprentissage profond. Dont, ces techniques permettent d'automatiser les processus de suivi et offre une gestion efficace de suivi de la présence.

À la fin, on note que les résultats obtenus à travers notre étude sont jugés meilleurs par rapport à l'utilisation des méthodes classiques qui posent certaines difficultés en termes de temps, de fiabilité et précision.

Mot clés : Moyens biométriques, Intelligence artificielle(IA), Reconnaissance faciale(RF), apprentissage automatiques, apprentissage profond,

Abstract

Facial recognition is widely regarded as one of the most effective biometric means to identify and authenticate individuals. Given that managing attendance and absenteeism in schools with current traditional methods often fails to provide accurate and real-time attendance data, alternative solutions need to be found.

This issue has become a major concern, impacting students, teachers, and the education system as a whole. To address these challenges, we have developed an intelligent system that automates the identity verification process and tracks student attendance, while replacing the currently used traditional methods in educational institutions.

In this regard, to meet the needs of educational institutions, administrators must take appropriate measures and constantly seek solutions to use advanced artificial intelligence (AI) methods, such as machine learning and deep learning. These techniques enable the automation of tracking processes and offer effective attendance management.

In conclusion, the results obtained through our study are considered well compared to the use of traditional methods, which cause certain number of difficultés in terms of time, reliability, and accuracy.

Keywords : Biometric methods, Artificial Intelligence (AI), Facial Recognition (FR), machine Learning(ML), deep Learning(DL).

ملخص :

التعرف على الوجه يُعَتَبَر على نطاق واسع واحدة من أكثر تقنيات البيانات الحيوية فعالية لتحديد هوية الأفراد ومصداقيتها. ونظرًا لأن إدارة الحضور والغياب في المدارس باستخدام الأساليب التقليدية الحالية غالبًا ما لا تتمكن من توفير بيانات دقيقة وفي الوقت الحقيقي، فإنه يتطلب إيجاد بدائل

أصبح هذا التحدي قضية رئيسية تؤثر على الطلاب والمعلمين والنظام التعليمي بشكل عام.

للتغلب على هذه التحديات، قمنا بتطوير نظام ذكي يُوَتِّر عملية التحقق من الهوية وتتبع حضور الطلاب، ويحل محل الأساليب التقليدية المستخدمة حاليًا في المؤسسات التعليمية.

في هذا الصدد، يجب على المسؤولين اتخاذ إجراءات مناسبة والبحث باستمرار عن حلول لاستخدام أساليب الذكاء الاصطناعي المتقدمة مثل التعلم الآلي والتعلم العميق لتلبية احتياجات المؤسسات التعليمية. تلك التقنيات تُمَكِّن من تَأْتير عمليات التتبع وتوفِّر إدارة فعالة لتتبع الحضور.

في النهاية، يجدر بنا أن نذكر أن النتائج التي تم الحصول عليها من خلال دراستنا تعتبر أفضل بالمقارنة مع استخدام الأساليب التقليدية التي تواجه بعض الصعوبات فيما يتعلق بالوقت والموثوقية والدقة..

كلمات مفتاحية : وسائل التحقق البيومترية ، الذكاء الاصطناعي، التعرف على الوجه، التعلم الآلي، التعلم العميق.

Liste des Figures

Liste des Tableaux

Liste des Acronymes et Abréviations

IA	Intelligence Artificielle
RF	Reconnaissance Faciale
2D	Deux dimensions
3D	Trois Dimension
FD	Face Detection
FE	Feature Extraction
ROI	Region of Interest
KACP	Analyse en Composantes Principales à Noyaux
SVM	Support vector machine
KICA	Kernel independent component analysis
LPP	Locality preserving projection
LBP	Local Binary Patterns
HOG	**Histogramme Orienté Gradient**
LCA	Local Composant Analysis
ADN	Acide Désoxyribonucléique
PIN	Personal Identification Number
ATM	Automated Teller Machines
ISO	International Organization for Standardization
NIST	l'Institut national des normes et de la technologie
CNRS	Centre national de la recherche scientifique
PC	Personal Computer
FA	Faux positifs
FN	Faux négatifs
EER	Taux d'erreur d'égalisation
FRR	False Rejet Rate
FAR	False Accept Rate
TID	Taux d'Identification
UML	Unified Modeling Language
UP	Unified Prtocess

CU	Cas d'Utilsation
LBPH	Local Binary Patterns Histograms
IDE	Integrated Development Environments

Introduction Générale

INTRODUCTION GENERALE

Le monde a connu ces dernières années un développement considérable, notamment dans le domaine de l'intelligence artificielle (IA) et plus précisément dans la reconnaissance faciale. Il est devenu donc inévitable pour toutes les institutions, y compris les institutions éducatives, de disposer d'outils de gestion et de contrôle. Ces outils offrent un potentiel significatif, tel que le contrôle d'accès, la réduction de l'absentéisme et l'amélioration de la sécurité des élèves à travers l'identification rapide des personnes non autorisées ou indésirable dans les établissements scolaires.

A cet égard, la gestion des présences et d'absentéisme scolaire dans les écoles peut causer un dysfonctionnement pour le succès académique des élèves et entrave le bon fonctionnement du système éducatif dans son ensemble bien sûr. Alors, il est, important de prendre des mesures adéquates et de chercher continuellement, des outils et des méthodes très avancées de l'**IA** à savoir l'identification des individus grâce aux techniques de reconnaissance faciales et de détection de visage, afin de mieux gérer la présence des élèves et d'automatiser le processus de suivi. Evidemment dans le but de simplifier les tâches administratives

Cependant, avec l'avènement de la technologie de la RF, et la numérisation, et vu que le volume des données à traiter est en constante augmentation du jour au jour, nous nous sommes sur le point de juger que les méthodes traditionnelles actuelles sont devenues classique ne répondant plus aux besoins du quotidien d'une part, et ne fournissent plus des données précises et en temps réel d'autre part. En effet, en raison de l'inefficacité de ces méthodes classiques dans ce domaine, qui reposent généralement sur des techniques traditionnelles et primitives, telles que les feuilles de présence manuelles ou les cartes d'identité, cela nous amène systématiquement à la perte de temps, et la non fiabilité, en terme d'efficacité d'efficience. Les arguments que nous avons fournies (décrits) précédemment nous a conduits à la réflexion de présenter la **reconnaissance faciale**, et la technologie de la biométrie comme alternative et solution pour vérifier l'identité des étudiants.

Les limites des méthodes classiques nous obligent de réaliser un **système intelligent** capable d'automatiser le processus de vérification d'identité et de suivi de la présence des élèves tout en remplaçant ces méthodes traditionnelles et de répondre aux besoins du quotidien.

Ce système intelligent qu'on va procéder à mettre en œuvre s'appuie sur l'exploitation de la technologie de la reconnaissance faciale à travers l'application des techniques de la technologie de l'IA, parmi ses avantages, d'identifier les élèves avec une haute précision, dont, les données collectées par ce système peuvent être utilisées à des fins de de traçabilité et de surveillance.

Dans ce mémoire, nous avons structurés notre travail en quatre chapitres, dans le premier chapitre nous allons abordés le système de reconnaissance de visage d'une manière générale, subdivisé en deux parties, la première partie s'articule sur la reconnaissance faciale, et fondement théoriques, et la deuxième traite l'intégration de la reconnaissance faciale et l'importance du contrôle d'accès et de la sécurité en milieu scolaire.

Le deuxième chapitre vise à définir et à cerner les généralités sur la biométrie, le système biométrique ainsi que les outils d'évaluation biométrique, ensuite dans le troisième chapitre nous décrirons le processus d'élaboration et de conception du système de RF dans un établissement d'enseignement.

Et Enfin, le quatrième chapitre sera consacré à l'étude pratique, la réalisation du système, où nous exposerons les résultats obtenus, que nous comparerons aux résultats attendus conformément aux objectifs de ce travail.

Au final, on clôturera notre travail par une conclusion générale.

Chapitre I :

Système De Reconnaissance De Visage

Partie 1 : La reconnaissance faciale

1 Introduction

Dans cette section, nous abordons divers aspects de la reconnaissance faciale. Nous commençons par une introduction, suivie de définitions et d'un historique pour mieux comprendre le sujet. Ensuite, nous explorons les différentes applications et usages de la reconnaissance faciale, ainsi que l'architecture de base d'un système de reconnaissance de visages. Nous examinons également le fonctionnement de ce système, en mettant en évidence ses avantages et inconvénients. Nous passons ensuite en revue les techniques de détection et de reconnaissance de visage, en mettant l'accent sur les techniques de reconnaissance de visage 2D et 3D. Nous abordons également les principales difficultés rencontrées dans le domaine de la reconnaissance faciale.

2 La reconnaissance faciale

La reconnaissance faciale est une tâche que les humains effectuent naturellement et sans effort dans leurs vies quotidiennes. La grande disponibilité d'ordinateurs puissants et peu onéreux ainsi que des systèmes informatiques embarqués ont suscité un énorme intérêt dans le traitement automatique des images et des vidéos numériques au sein de nombreuses applications, incluant l'identification biométrique, la surveillance, l'interaction homme-machine et la gestion de données multimédia. La reconnaissance faciale, en tant qu'une des technologies biométriques de base, a pris une part de plus en plus importante dans le domaine de la recherche, ceci étant dû aux **avances rapides** dans des technologies telles que les appareils photo numériques, Internet et les dispositifs mobiles, le tout associé à des **besoins en sécurité** sans cesse en augmentation[1].

2.1 Définitions

La reconnaissance faciale est une technologie de traitement d'images qui vise à identifier et à vérifier l'identité d'une personne en analysant les caractéristiques distinctives de son visage de manière automatisée. Elle fait partie du domaine de la vision par ordinateur et consiste à utiliser des algorithmes pour extraire des informations faciales telles que la forme, la structure et les caractéristiques uniques d'une personne à partir d'une image ou d'une vidéo.

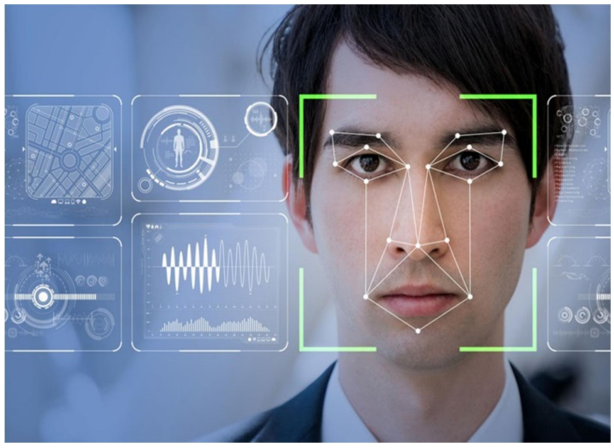
[1] Nicolas MORIZET, « Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris », Thèse de doctorat, École Doctorale d'Informatique, Télécommunications et Électronique de Paris, France, p 32,2009.

La reconnaissance faciale trouve de nombreuses applications dans divers domaines tels que la sécurité, la biométrie, la surveillance vidéo, la robotique, l'indexation d'images et de vidéos, ainsi que la recherche d'images en fonction de leur contenu. Elle peut être utilisée pour des tâches telles que l'authentification d'identité, la détection de visages dans des images en temps réel, la recherche de similitudes faciales dans des bases de données volumineuses, et même pour des fonctionnalités de divertissement, telles que les filtres de réalité augmentée sur les réseaux sociaux[1].

La reconnaissance faciale est une technologie d'intelligence artificielle (**IA**) offrant la possibilité d'analyser, grâce à des algorithmes, les traits de visages des personnes et de les comparer à des images stockées dans une base de données. A partir d'une image numérique ou d'un flux vidéo en direct, il est donc possible :

- D'authentifier un individu, autrement dit de vérifier qu'il s'agit bien de celui qu'il prétend être ;
- D'identifier une personne, c'est-à-dire de retrouver une personne au sein d'un groupe.

Figure (N° 01-I) : Exemple d'Authentification et d'identification d'un individu.



[1] https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_reconnaissance_faciale.

2.2 Historique

Les premières recherches sur la reconnaissance faciale ont débuté dans les années 1960, avec des travaux pionniers de chercheurs tels que **Woody Bledsoe** et **Helen Chan**.
Dans les années 1970, l'avènement de l'informatique a permis de développer des algorithmes automatisés pour la reconnaissance faciale. L'une des premières percées majeures a été la mise au point de la méthode Eigenfaces par **Matthew Turk** et **Alex Pentland** en 1991. Cette méthode utilisait l'analyse en composantes principales pour représenter les visages en tant que vecteurs de nombres, ce qui permettait de les comparer et de les identifier plus facilement.

Les années 1990 ont également vu le développement de bases de données de visages, telles que LaFace de Carnegie Mellon University, qui a permis aux chercheurs de tester et d'améliorer leurs algorithmes.

Au cours des années 2000, la reconnaissance faciale est devenue plus précise et fiable grâce à l'amélioration des algorithmes et à l'augmentation de la puissance de calcul. Cela a conduit à un large éventail d'applications, notamment la vérification d'identité, la vidéosurveillance et le contrôle d'accès.

Les années 2010 ont vu l'émergence de la reconnaissance faciale sur les smartphones et les réseaux sociaux. Facebook a lancé sa fonction de reconnaissance faciale en 2011, et Apple a intégré la reconnaissance faciale dans FaceID en 2017.

Depuis fin 2018, les annonces et études se multiplient faisant entrer progressivement la reconnaissance faciale dans le quotidien. En 2019, Cydral Technology diffuse un système utilisable depuis un simple téléphone ; il propose de ce fait le tout premier moteur de recherche grand public13 fonctionnant à l'image de la recherche inversée proposée par Google mais pour l'identification de profils exclusivement[1].

Aujourd'hui, la reconnaissance faciale est l'une des technologies de biométrie les plus populaires au monde. Elle est utilisée dans une variété d'applications, des smartphones aux aéroports. Cependant, la reconnaissance faciale soulève également des inquiétudes concernant la vie privée et les abus potentiels. Il est important de peser soigneusement les avantages et les risques de cette technologie avant de la déployer.

[1] https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_reconnaissance_facial.

3 Les applications de la Reconnaissance Faciale

La reconnaissance faciale est appliquée dans divers secteurs, avec plusieurs utilisations couramment observées, telles que [1] :

Identification de personnes inconnues ou disparues : La reconnaissance faciale peut être utilisée pour comparer les visages capturés avec une base de données de visages connus afin d'identifier des individus inconnus ou retrouver des personnes disparues.

- **Contrôle d'accès automatique :** Ce système permet de contrôler l'accès aux lieux ou aux véhicules en vérifiant l'identité des personnes à l'aide de la reconnaissance faciale. Il peut être utilisé dans les entreprises, les aéroports, les centres commerciaux, etc.
- **Journalisation :** La reconnaissance faciale peut également être utilisée pour enregistrer les activités des machines et des dispositifs en identifiant les personnes qui les utilisent. Cela peut être utile pour des raisons de sécurité et de suivi.
- **Maintien de l'ordre et sécurité nationale :** Les forces de l'ordre peuvent utiliser la reconnaissance faciale pour détecter, suivre et identifier les personnes suspectes ou recherchées. Cela peut contribuer à la prévention et à la résolution des crimes.
- **Systèmes de surveillance basés sur l'IA** : Peut être intégrée à des systèmes de surveillance alimentés par l'intelligence artificielle. Ces systèmes peuvent analyser en temps réel les visages des personnes capturées par les caméras de surveillance pour détecter des comportements suspects ou prévenir les incidents.
- **Gestion du temps et des présences :** Certains systèmes de reconnaissance faciale sont utilisés pour enregistrer automatiquement les temps de présence des employés dans les entreprises, éliminant ainsi le besoin de cartes ou de badges.
- **Paiements sans carte :** Elle est peut-être utilisée pour authentifier les utilisateurs lors de transactions sans carte de crédit ou de débit. Cela permet des paiements plus rapides et sans contact physique.

3.1 Usage de la Reconnaissance Faciale :

Ces exemples d'application mettent en évidence la polyvalence et l'importance croissante de la reconnaissance faciale dans divers domaines :

3.1.1 La détection des fraudes :

[1] Recueillis sur la présentation du cours chapitre 1, « introduction aux systèmes de Reconnaissance de visage », Dr CHEIKH Ramdane, Université du 20 Août 1955 – Skikda 2024.

La reconnaissance faciale peut être utilisée pour vérifier l'identité des individus lors de transactions financières ou d'authentification en ligne, contribuant ainsi à réduire les risques de fraude.

Figure (N° 02-I) : Détection des fraudes.

Source : https://stratex-afrique.com/formation-detection-de-fraude-analyse-de-donnees/

4 La cyber-sécurité :

En intégrant la reconnaissance faciale dans les systèmes d'authentification, les entreprises peuvent renforcer la sécurité de leurs infrastructures informatiques en limitant l'accès aux utilisateurs autorisés et en détectant les tentatives d'intrusion.

4.1 Autres usages [1] :

Elle peut être utilisée pour certaines applications spécifiques comme les :

- **Soins médicaux :** Les établissements de santé peuvent utiliser la reconnaissance faciale pour identifier rapidement les patients et accéder à leur dossier médical électronique, améliorant ainsi la précision des soins et la sécurité des données médicales.
- **Contrôle d'accès aux bâtiments professionnels :** La reconnaissance faciale peut servir de méthode d'authentification sécurisée pour contrôler l'accès aux zones sensibles des entreprises, remplaçant ainsi les méthodes traditionnelles telles que les badges d'identification ou les codes PIN.

[1] https://www.caducee.net/DossierSpecialises/systeme-information-sante/dmi.asp.

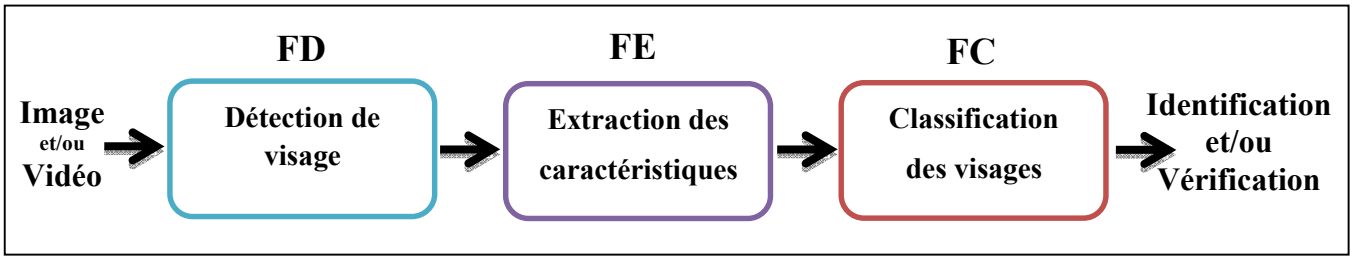
- **Le contrôle des aéroports :** En intégrant la reconnaissance faciale dans les systèmes de sécurité des aéroports, les autorités peuvent identifier les individus à risque et renforcer les mesures de sécurité pour prévenir les menaces potentielles.

5 Architecture de base d'un système de reconnaissance de visages :

La mise en place d'un système de reconnaissance faciale complet requiert trois étapes majeures, soit la détection de visage (Face Detection, **FD**) à partir des images ou séquences vidéo, l'extraction de caractéristiques (Feature Extraction, **FE**) permettant de décrire et encoder l'apparence d'un visage sous forme numérique ou binaire, et finalement, la classification de visages (Face Classification, FC) pour accomplir la reconnaissance faciale qui permet d'identifier ou de vérifier la présence d'un individu dans une scène en entrée[1].

La Figure représente cette architecture sous sa forme typique et simplifiée.

Figure (N° 03-I) : **Architecture fondamentale des systèmes de reconnaissance de visages.**



5.1 Système de reconnaissance de visage :

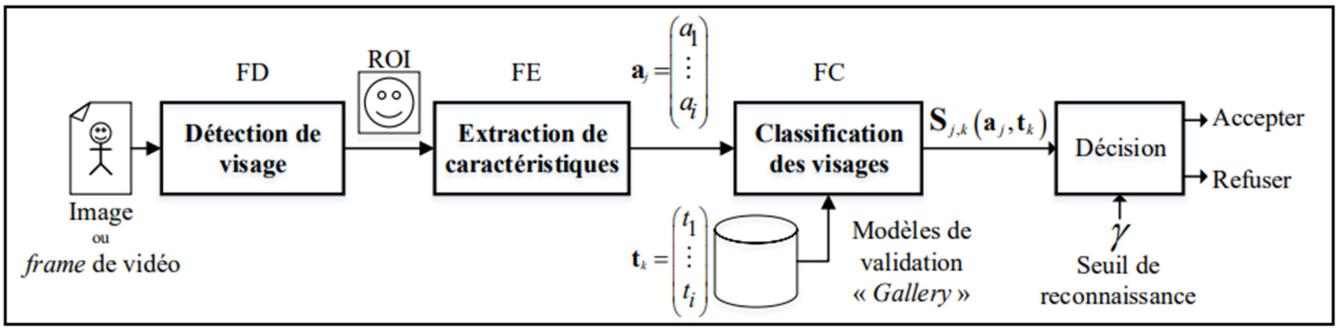
Les systèmes de reconnaissance faciale fonctionnent au minimum en deux étapes, soit la phase **d'entraînement** (enrollment phase) et la phase **d'opération** (operational phase). La première étape consiste à préparer des modèles de visage permettant de discriminer les individus à reconnaître entre eux lors de la seconde étape. Ainsi, la phase initiale effectue d'abord une détection de visage afin d'obtenir des régions d'intérêt (ROI) qui précisent l'emplacement du visage recherché à travers l'intégralité d'une image ou une trame de vidéo.

Évidemment, lorsqu'il s'agit de représentation globale du visage, la ROI englobe l'ensemble du visage, alors que les approches locales obtiennent les sections du visage spécifiquement à leur application. Ensuite, les descripteurs $\boldsymbol{tk}$ représentant les visages détectés y sont extraits, afin d'entraîner des classificateurs de visages performants pour discriminer entre les visages d'individus à reconnaître. Les modèles caractérisant les individus

[1] X. Tan, S. Chen, Z.-H. Zhou, and F. Zhang, "Face recognition from a single image per Person : A survey," Pattern recognition, vol. 39(9), pp. 1725-1745, 2006.

d'intérêt obtenus de cet entraînement sont alors inscrits dans une base de référence intitulée **gallery**. Celle-ci deviendra la base à laquelle les nouvelles représentations de visages encore non identifiés **a*j*** seront comparés et testés lors de la phase d'opération. Ainsi, lorsque l'on passe à la deuxième phase, les nouveaux visages captés en entrée subissent le même procédé de détection de visage et d'extraction de caractéristiques, de sorte à les comparer selon la même forme que sauvegardés préalablement à la première phase, tel qu'illustré à la figure (N° 04-I).

Figure (N° 04-I) : Schéma plus détaillé d'un système de reconnaissance de visages.



Le système de reconnaissance faciale peut être utilisé selon deux modes : le mode temps réel (en ligne) ou le mode a posteriori (hors ligne). En mode hors ligne, le système collecte les informations de chaque visage détecté et les enregistre dans une base de données facilement accessible. Lorsqu'il est utilisé en ligne, un utilisateur peut accéder à cette base de données et sélectionner un visage spécifique pour une authentification ou une identification.

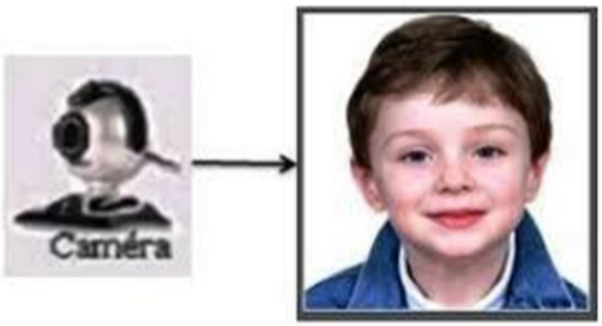
Dans les deux modes, le système effectue plusieurs opérations essentielles, notamment l'acquisition de l'image, le prétraitement, la détection, l'extraction des caractéristiques (features), la classification et la prise de décision (authentification - reconnaissance)[1].

4.1.1 Acquisition de l'image :

C'est la première étape dans le processus, l'acquisition d'image qui consiste à acquérir une image ou une vidéo du visage d'un individu à l'aide d'une caméra, d'un Smartphone ou d'une autre source d'image.

[1] AKCHA Ikram & AMARI Amira Mémoire de master « Développement d'un système de reconnaissance faciale», Université Saad Dahleb De Blida, p20, 2020.

Figure (N° 05-I) : Exemple d'acquisition d'une image.

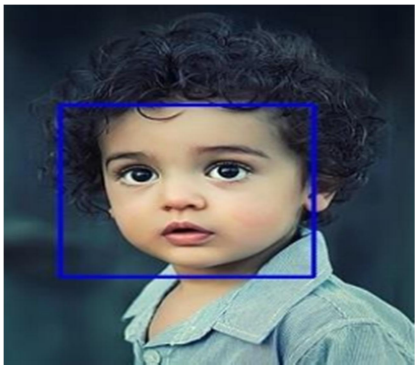


4.1.2 Détection de visages :

L'étape qui consiste à localiser et à délimiter le visage dans l'image ou la vidéo à l'aide d'un algorithme de détection de visage qui sert à chercher les caractéristiques faciales (les yeux, le nez, la boucle, les sourcils, la bouche, les lèvres, les oreilles, etc.).

Un visage est considéré correctement détecté si la taille d'image extraite ne dépasse pas 20% de la taille réelle de la région faciale comme illustré dans la figure, Cette étape peut faire la détection de la couleur de peau, la forme de la tête et il existe plusieurs méthodes détectant les différentes caractéristiques du visage[1].

Figure (N° 06-I) : Détection de visage.



[1] ASSADI NADJETTE « Mise au point d'une application de reconnaissance faciale », Mémoire de master en informatique, Université Mohamed Khider – BISKRA, 2017-2018».

4.1.3 Extraction des caractéristiques :

Le but est d'extraire les caractéristiques du visage qui peuvent le rendre à la fois différent de celui des autres personnes et robuste aux variations de la personne elle-même. C'est l'information nécessaire pour que le visage d'une personne ne ressemble pas à celui d'une autre personne et en même temps qu'il ressemble à lui-même dans d'autres conditions d'acquisition. Au début des travaux sur la reconnaissance de visage, on a estimé qu'une représentation du visage devait passer par utilisation de la bouche, des yeux, du nez, de leurs positions relatives et de leur géométrie. Mais cette procédure a montré ses limites. Il faut alors une analyse plus poussée du visage pour trouver d'autres caractéristiques. Dans certaines méthodes, on n'utilise d'ailleurs que la détection des yeux pour normaliser le visage et on fait ensuite une étude globale du visage[1].

4.1.4 Comparaison des caractéristiques :

Les caractéristiques extraites sont ensuite comparées aux caractéristiques stockées dans une base de données d'un ensemble de visage connus, elle contient des photos des personnes ainsi que leurs informations d'identité (Nom, prénom âge).

4.1.5 La Décision (confirmation de l'identité) :

Dans cette étape le système compare la similitude entre les caractéristiques du visage d'entrée et les caractéristiques stockées dans la base de données, et si la similitude est suffisamment élevée, le système identifie la personne correspondante, sinon il indique qu'il ne peut pas identifie la personne.

Un système d'identification consiste à trouver le modèle qui correspond le mieux au visage pris en entrée à partir de ceux stockés dans la base de données, il est caractérisé par son taux de reconnaissance. Par contre, dans un système de vérification il s'agit de décider si le visage en entrée est bien celui de l'individu (modèle) **proclamé** ou il s'agit d'un **imposteur**. Pour estimer la différence entre deux images, il faut introduire une mesure de similarité[2] .

[1] Samia Mekkani, «Reconnaissance de visage», Mémoire de licence, Université Larbi Ben M'hidi Oum El Bouaghi, Juin 2014.
[2] Mebarka Belahcen: «Authentification et identification en biométrie ». Thèse de doctorat, Université Mohamed khider Biskra, 2013.

6 Avantages et inconvénients de la Reconnaissance de Visage :

La reconnaissance faciale est une technologie qui présente à la fois des avantages et des inconvénients. Voici une liste de quelques-uns d'entre eux,

6.1 Avantages de la reconnaissance faciale[1] .

Sécurité améliorée : La reconnaissance faciale peut renforcer la sécurité en permettant l'identification rapide et précise des individus. Elle est utilisée dans des domaines tels que la sécurité des frontières, la lutte contre la criminalité et le contrôle d'accès aux installations sensibles.

1. Automatisation des processus : La reconnaissance faciale peut automatiser des tâches telles que le déverrouillage de téléphones, l'accès à des services en ligne et même le paiement dans certains cas. Cela peut rendre les interactions plus rapides et plus pratiques.
2. Prévention de la fraude : En utilisant la reconnaissance faciale comme mesure de sécurité, il devient plus difficile pour les personnes mal intentionnées de se faire passer pour quelqu'un d'autre, que ce soit pour accéder à des comptes en ligne ou pour commettre des fraudes.

6.2 Inconvénients de la Reconnaissance de Visage[2] .

1. Vie privée et protection des données : La collecte et le stockage des données biométriques, y compris les informations du visage, soulèvent des préoccupations en matière de vie privée. Les bases de données pourraient être exposées à des failles de sécurité, ou les données pourraient être utilisées de manière abusive.
2. Biais et discrimination : Certains systèmes de reconnaissance faciale peuvent présenter des biais, en particulier lorsqu'ils sont utilisés pour l'identification de personnes appartenant à des groupes minoritaires. Cela peut entraîner une discrimination et des conséquences négatives pour certaines communautés.
3. Erreurs de reconnaissance : Les systèmes de reconnaissance faciale ne sont pas infaillibles et peuvent parfois commettre des erreurs, en particulier lorsque les

[1] Article The Pros and Cons of Facial Recognition Technology" - Security Magazine 2020, https://www.securitymagazine.com/articles/91847-cybersecurity-response-to-the-california-consumer-privacy-act.
[2] opcit.

conditions d'éclairage ou d'angle de vue sont défavorables. Ces erreurs peuvent entraîner des conséquences indésirables, telles que des erreurs d'identification ou un accès refusé à des personnes autorisées.

Le tableau comparatif suivant montre les avantages et les inconvénients de la reconnaissance de visage :

Tableau (N°01-I) : Avantages et inconvénients de la Reconnaissance faciale.

Avantages	**Inconvénients**
Technologie bien acceptée par le public	Technologie sensible à l'environnement (éclairage, expression du visage).
En position fixe et éclairée, les taux de reconnaissance sont effectivement très élevés	Technologie sensible au changement (barbe, moustache, chirurgie, perçage...).
Technique peu coûteuse	Les vrais jumeaux ne sont pas identifiés.

Source : Hadj Atou Abdelkader et Bouizzouldjallal « Simulation d'un système d'identification de personnes par le visage et la voix », mémoire de master, université Saad Dehleb Blida, Algérie, année 2017-2018, p08

7 Techniques de détection et de reconnaissance de visage :

Comme mentionné précédemment, un système de reconnaissance faciale automatique est composé de trois sous-systèmes : détection faciale, extraction des caractéristiques et reconnaissance faciale. Cependant, la mise en place d'un système fiable et automatisé de reconnaissance faciale reste un défi technologique non résolu.

Au cours des dernières années, de nombreuses méthodes de reconnaissance faciale ont été proposées. La reconnaissance faciale est un domaine de recherche ouvert qui attire des chercheurs issus de diverses disciplines telles que la psychologie, la reconnaissance de formes, les réseaux neuronaux, la vision artificielle et l'infographie.

Dans ce qui suit, nous présenterons les approches les plus connues en matière de reconnaissance faciale, qui peuvent être regroupées en trois catégories distinctes : les approches globales (holistiques), les approches locales et les approches hybrides.

7.1 Les approches globales :

Ces approches connues sous le nom de méthodes de reconnaissance faciale basées sur l'apparence, sont des approches qui utilisent l'image complète d'un visage comme entrée pour le système de reconnaissance. Le principe de ces méthodes est que : chaque image de visage, d'une dimension (NxM), est représentée par un vecteur simple de dimension NM. Ce vecteur est obtenu en concaténant les valeurs des niveaux de gris de tous les pixels de l'image du visage. L'espace qui contient tous les vecteurs d'images de visages est appelé espace des images. L'un des avantages de cette représentation est qu'elle préserve implicitement les informations de texture et de forme nécessaires à la reconnaissance des visages. De plus, elle permet de capturer de manière plus efficace l'aspect global du visage par rapport aux représentations locales[1]. Cette catégorie de techniques peut être classée en deux groupes distincts : linéaire et non linéaire.

6.1.1 Les techniques linéaires :

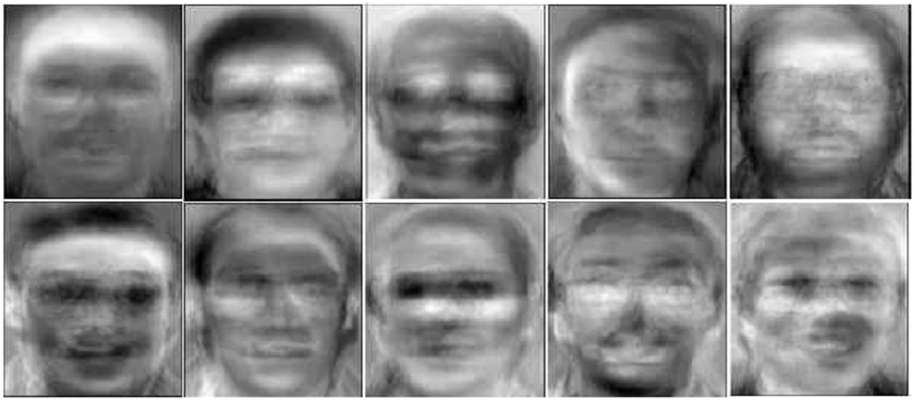
Ces techniques consistent à projeter linéairement une image de grande dimension dans un espace de plus petite dimension. Cependant, une telle projection ne peut pas préserver les variations de visage non convexes qui permettent de distinguer différentes personnes. De plus, la distance euclidienne ne peut pas être utilisée pour comparer les pixels car cela ne serait pas efficace pour la classification des visages et des non-visages, ce qui entraînerait une détection et une reconnaissance insatisfaisantes. Les techniques les plus couramment utilisées sont les suivantes :

7.1.1.1 Eigenfaces :

Cette technique repose sur le principe de : à partir d'un ensemble d'images de visages exemples, il est d'abord nécessaire de trouver les composantes principales de ces visages. Cela revient à déterminer les vecteurs propres de la matrice de covariance formée par l'ensemble des images exemples. Chaque visage exemple peut ensuite être décrit par une combinaison linéaire de ces vecteurs propres. Pour construire la matrice de covariance, chaque image de visage est transformée en vecteur, où chaque élément du vecteur correspond à l'intensité lumineuse d'un pixel[2].

[1] P.Buyssens « Fusion de différents modes de capture pour la reconnaissance du visage appliquée aux transactions » Université de Caen-2011.
[2] M.Chihaoui, A.Elkefi, W.Bellil and C.Ben Amar « A Survey of 2D Face Recognition Techniques » University of Sfax, National School of Engineers (ENIS) -2016.

Figure (N° 07-I) : Représentation de 10 valeurs d'Eigenface



Source : https://www.researchgate.net/figure/First-10-eigenfaces-with-highest-eigenvalues_fig4_264167711]. Consulté le 06/05/2024 09 :14

7.1.1.2 Techniques non linéaires :

Des techniques globales non linéaires ont été développées, qui sont souvent dérivées de techniques linéaires en utilisant la fonction « **kernel** » pour étendre leur portée. Quelques exemples de ces techniques non linéaires sont les suivants :

- Analyse en Composantes Principales à Noyaux (**KACP**) [1].
- Support vector machine (**SVM**)[2].
- Kernel independent component analysis (**KICA**) [3].
- Locality preserving projection (**LPP**)[4].

7.2 Les approches locales :

Les approches locales de la reconnaissance faciale sont basées sur des modèles et utilisent un traitement séparé appliqué aux différentes régions de l'image contenant un visage. Ce processus permet d'obtenir un vecteur

[1] H.Hoffmann « Kernel PCA for novelty detection » Pattern Recognit-2007.

[2] N.Vladimir « The Nature of Statistical Learning Theory » New York, NY, USA-1995.

[3] F.Bach, M.Jordan « Kernel independent component analysis » Learn. Res-2002.

[4] Y.Hu « Learning a locality preserving subspace for visual recognition ». In Proceedings of the 9th IEEE International Conference on Computer Vision, Nice, France, 13–16 October- 2003.

caractéristique pour chaque région du visage[1]. Ces approches peuvent être classées sen deux catégories : les méthodes basées sur l'apparence locale et les méthodes basées sur les points d'intérêt.

6.2.1 Méthodes basées sur l'apparence locale :

Les approches locales de la reconnaissance faciale reposent sur des modèles et exploitent des connaissances préalables que nous possède de la morphologie faciale. Elles impliquent la détection des traits distinctifs du visage, tels que les yeux, la bouche, le nez et les oreilles, et ensuite mesurent la position de chaque point dans l'espace facial. Ensuite, ces positions sont comparées avec les paramètres extraits des autres visages pour effectuer la reconnaissance.

Les méthodes locales de reconnaissance de visages offrent un avantage majeur en étant capables de traiter efficacement les variations de pose, d'illumination et d'expressions auxquelles un visage peut être soumis (robustes). Elles parviennent à modéliser ces variations de manière aisée. Cependant, leur mise en place est plus complexe, car elles exigent généralement le placement manuel de nombreux points d'intérêt pour obtenir une précision optimale, ce qui rend leur implémentation plus laborieuse. Parmi les méthodes locales, les plus couramment utilisées sont les Local Binary Patterns(LBP)[2].

6.2.2 Local Binary Patterns (LBP) :

Pour caractériser des motifs de textures spécifiques dans une image, le Descripteur LBP utilise les niveaux de gris. Il fonctionne en seuillant les pixels autour d'une valeur centrale dans une fenêtre locale, ce qui permet d'encoder les données binaires en fonction de la comparaison des pixels voisins avec cette valeur centrale.

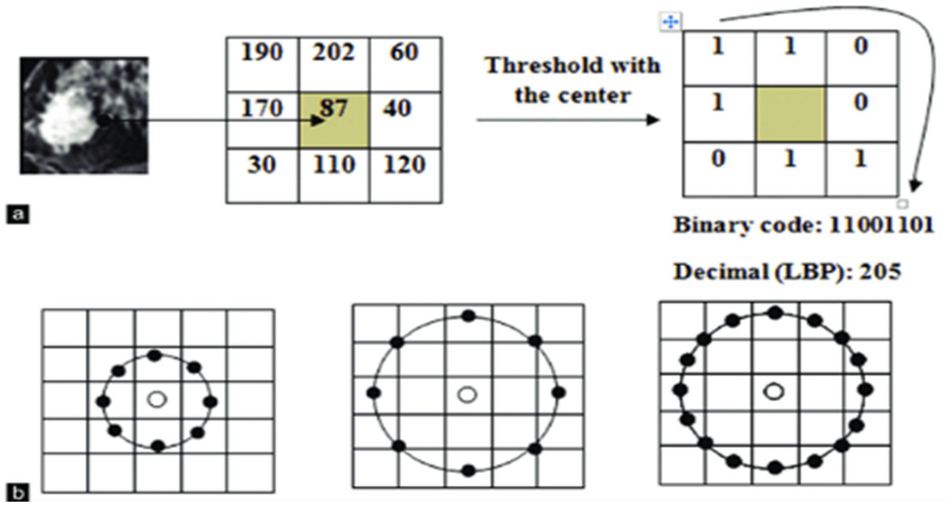
Les combinaisons binaires observées dans l'image sont ensuite comptabilisées dans un histogramme. Pour éviter les motifs irréalistes, un filtrage est appliqué pour limiter le nombre de caractéristiques à un maximum de 59, en se basant sur des observations réalisées dans des conditions réelles.

---

[1] Bouzit Dhikra, « Reconnaissance de visage basée sur une approche triangulaire », Mémoire de master, Université de 8 Mai 1945 – Guelma -,2019

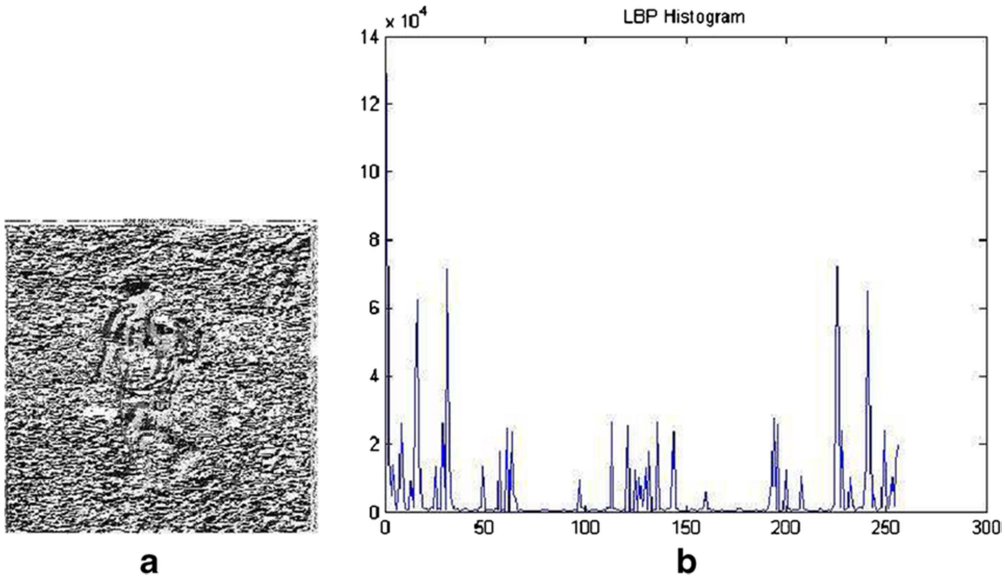
[2] AKCHA Ikram et ammari amira ; Université De Blida 1 – Saad Dahleb, Mémoire de master Développement d'un système de reconnaissance facial, PAGE 27, 2020.

Figure (N° 08-I) : Calcul de modèle binaire local (LBP). (a) Exemple de l'opérateur LBP de base. (b) Exemples de quartiers LBP circulaires communs : (8,1), (8,2) et (16,2) respectivement



Et la figure Histogramme de caractéristique LBP illustré en ci-dessous :

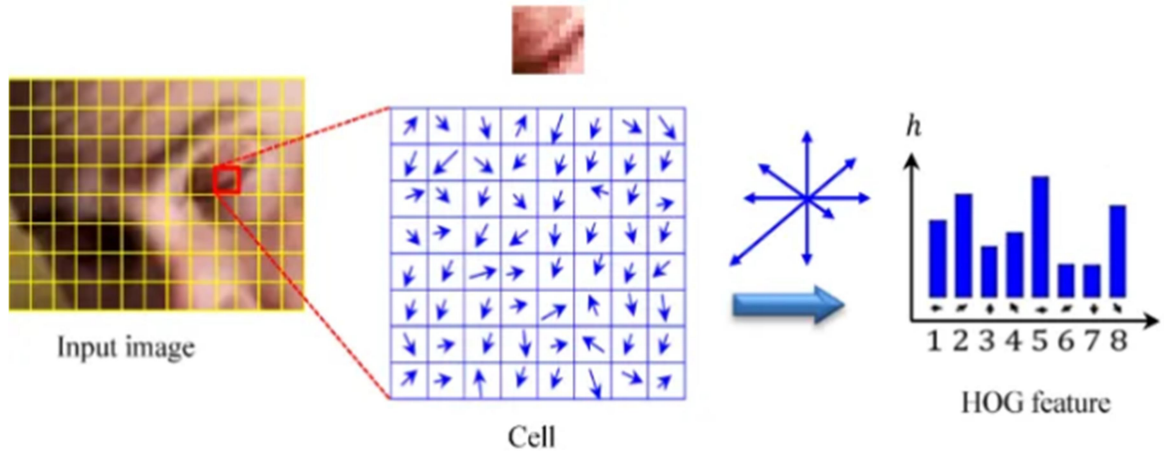
Figure (N° 09-I) : Histogramme de caractéristique LBP. (a)LBP Image (b) LBP Histogramme.



6.2.3 HOG (Histogramme Orienté Gradient) :

La méthode HOG est une approche utilisée pour extraire des caractéristiques à partir d'une image. Elle est largement utilisée dans des applications telles que le domaine de la reconnaissance faciale, la détection de piétons et la reconnaissance d'objets[1]. Son principe de fonctionnement consiste à parcourir l'image pixel par pixel et à comparer l'intensité de chaque pixel avec celle de ses pixels voisins. Ensuite, une flèche représentant le gradient est dessinée, indiquant la direction dans laquelle l'image devient plus sombre. Les gradients sont ensuite regroupés par orientations communes, en utilisant des sous-divisions de l'image telles que des fenêtres, des blocs et des cellules. Enfin, les gradients sont concaténés pour former un vecteur de caractéristiques (Figure).

Figure (N° 10-I) : **Descripteur de gradient orienté(HOG).**



7.3 Les approches hybrides :

Les approches hybrides sont des méthodes qui tirent parti des caractéristiques globales et locales pour améliorer les performances. Les caractéristiques globales se réfèrent aux traits généraux du visage, tels que la forme générale du visage, la disposition des yeux et des sourcils, tandis que les caractéristiques locales se concentrent sur les détails spécifiques, tels que les textures de la peau et les motifs des iris. En combinant ces deux types de caractéristiques, les méthodes hybrides offrent plusieurs avantages. Elles permettent d'améliorer la stabilité de la performance de reconnaissance face aux variations telles que les

[1] O. Déniz, G. Bueno, J. Salido, and F. De la Torre « Face recognition using Histograms of Oriented Gradients » Pattern Recognition Letters – 2011.

changements de pose, d'éclairage et d'expressions faciales etc. Ainsi, ces nouvelles méthodes de fusion ont pour objectif d'améliorer cette capacité d'adaptation afin d'obtenir des résultats plus fiables et précis.

Grâce à cette approche, les méthodes hybrides offrent une meilleure robustesse et une plus grande précision dans la reconnaissance faciale, ce qui les rend particulièrement utiles dans des environnements où les conditions peuvent varier.

- **Analyse en Composantes Locales (LCA)**[1] : cette technique réalise plusieurs analyses en composants principales pour extraire les caractéristiques qui sont ensuite combinées avec une autre méthode pour minimiser l'erreur de reconstruction.
- **HMM-LBP** [2] : cette technique permet de faire une classification des images 2D en utilisant la technique locale LBP pour l'extraction des caractéristiques et les HMM pour la classification.

7.4 Les principales difficultés de la reconnaissance faciale :

Le processus de reconnaissance des visages est une tâche visuelle complexe pour le cerveau humain. Bien que les humains puissent détecter et identifier des visages dans une scène avec facilité, créer un système automatique capable de réaliser de telles tâches représente un défi considérable. Ce défi est encore plus difficile lorsque les conditions de capture des images varient considérablement. Ces variations peuvent être classées en deux catégories : les variations inter-sujets et les variations intra-sujets. Les variations inter-sujets sont limitées en raison de la similarité physique entre les individus, tandis que les variations intra-sujets sont plus étendues. Ces dernières sont causées par plusieurs facteurs que nous analysons ci-dessous :

6.4.1 Changement d'illumination :

[1] AKCHA Ikram et Ammari amira, « Développement d'un système de reconnaissance faciale », mémoire de master, Université De Blida 1 – Saad Dahleb, PAGE 27, 2020.

[2] M.Chihaoui, A.Elkefi, W.Bellil and C.Ben Amar « A Survey of 2D Face Recognition Techniques » University of Sfax, National School of Engineers (ENIS) -2016.

L'éclairage est un facteur important qui peut affecter considérablement les performances des systèmes de reconnaissance faciale. Les variations d'éclairage peuvent modifier l'apparence d'un visage de plusieurs façons, ce qui peut rendre difficile pour un système de reconnaissance faciale d'identifier correctement une personne.

Figure (N° 11-I) : Exemple de Changement d'illumination.

Source : https://phototrend.fr/2014/09/comment-leclairage-peut-changer-la-perception-dune-personne/] le 08/06/2024 01 :08

6.4.2 Variations de la pose :

La pose, qui correspond à l'orientation et à l'inclinaison de la tête, est un autre facteur important qui peut affecter les performances des systèmes de reconnaissance faciale. Lorsque la pose d'un visage change, les caractéristiques faciales peuvent apparaître différentes, voir l'exemple dans la figure :

Figure (N° 12-I) : Exemple d'un visage d'une même personne subissant des variations de pose.

Source : https://www.researchgate.net/figure/Exemple-dun-visage-dune-meme-personne-subissant-des-variations-de-pose-hors-plan_fig3_291345615] consulté le 08/06/2024 01 : 41

6.4.3 Changement des expressions faciales :

Les expressions faciales qui résultent des mouvements des muscles du visage, représentent un élément essentiel pouvant impacter les performances des systèmes de reconnaissance faciale. Lorsqu'une personne change d'expression faciale, les traits de son visage peuvent sembler différents, rendant ainsi plus complexe l'identification précise par un système de reconnaissance faciale.

Figure (N° 13-I) : Exemples de changement d'expressions faciales.

Source : https://www.realites-dermatologiques.com/../La-dynamique-faciale-et-les-expressions-faciales-%C3%A9motionnelles.jpg consulté le 08/06/2024 01 :53

6.4.4 Effet des occultations :

Les occlusions, telles que les parties du visage masquées par des objets ou des cheveux, posent un défi majeur aux systèmes de reconnaissance faciale. Lorsque certaines parties du visage sont dissimulées, il devient difficile pour un système de reconnaissance faciale d'obtenir des caractéristiques faciales suffisantes pour une identification précise de la personne.

Figure (N° 14-I) : Exemples d'occlusion du visage.

Source : https://www.researchgate.net/figure/Exemples-docclusion-du-visage-Image-recueillie-a-partir-dInternet_fig5_291345615 consulté le 08/06/2024 01 :59

6.4.5 Les vrais jumeaux :

La reconnaissance faciale peut poser des difficultés particulières lorsqu'il s'agit de distinguer les vrais jumeaux qui partagent un **ADN** presque identique, ce qui signifie qu'ils ont des caractéristiques faciales très similaires. Et cela peut rendre difficile pour les systèmes de reconnaissance faciale de les différencier de manière fiable[1].

Figure (N° 15-I) : Exemples de vrais jumeaux.

[1] Yang, M., & Yang, J. Réseaux neuronaux convolutifs profonds pour la reconnaissance faciale avec des représentations convolutives compressées, dans les actes de la conférence IEEE sur la vision par ordinateur et la reconnaissance de formes ,p 2470-2479, 2018.

8 Conclusion

Cette section nous a permis de revenir sur les fondements et l'évolution de la reconnaissance faciale (RF). Nous avons rappelé les définitions et les aspects historiques de cette technologie. Nous avons abordé les limites inhérentes à la reconnaissance faciale, Cependant, malgré ces défis, nous avons souligné les nombreuses applications et utilisations de la RF, démontrant ainsi son potentiel dans divers domaines En examinant l'architecture de base d'un système de reconnaissance de visages, nous avons pu comprendre les différentes étapes et composants nécessaires à la mise en œuvre de cette technologie. Nous avons également pris connaissance des avantages et des inconvénients associés à l'utilisation de cette dernière, De plus, nous avons exploré les techniques de détection et de reconnaissance de visages (2D et 3D). Ces techniques nous ont permis de mieux appréhender les méthodes utilisées pour extraire les caractéristiques faciales et les comparer aux données enregistrées.

Enfin, nous avons abordé les principales difficultés rencontrées dans le domaine de la reconnaissance faciale,

La prochaine section abordera l'intégration de la reconnaissance faciale comme moyen de contrôle d'accès et de renforcement de la sécurité dans les écoles.

Partie 2 : Intégration de la reconnaissance au niveau des écoles

1 Introduction

Dans cette section, nous abordons plusieurs aspects liés à la sécurité scolaire et au contrôle de d'accès des élèves dans les écoles. Tout d'abord, nous examinons les risques et les menaces pour la sécurité scolaire, mettant en évidence l'importance de garantir un environnement sûr et sécurisé pour les élèves. Ensuite, nous soulignons l'importance de contrôler la présence des élèves dans les écoles. Nous explorons les méthodes traditionnelles de surveillance de la fréquentation, qui ont leurs propres limites et défis. Pour surmonter ces défis, nous explorons l'intégration de la reconnaissance faciale dans les écoles. Nous examinons, ainsi, les avantages et les inconvénients de l'utilisation de cette technologie pour la surveillance de la fréquentation. Enfin, nous discutons les différents types d'implémentation de la reconnaissance faciale pour la surveillance de la fréquentation, et de la possibilité de combiner différentes technologies pour renforcer la sécurité scolaire.

2 Risques et menaces pour la sécurité scolaire :

Il existe divers risques et menaces qui peuvent compromettre la sécurité dans les écoles. Chaque menace possède ses propres caractéristiques distinctes et peut avoir des conséquences graves sur la sécurité et le bien-être de la communauté scolaire. Voici une liste de ces menaces[1] :

- La violence en milieu scolaire peut prendre différentes formes, notamment les bagarres entre élèves, les actes d'intimidation et les agressions physiques ou verbales, qui peuvent perturber le climat d'apprentissage et toucher le sentiment de sécurité des élèves.
- Une mauvaise gestion des situations d'urgence tels que : les accidents à savoir, les chutes, les incendies ou les blessures sportives, peuvent entraîner des conséquences graves sur le personnels et les élèves [2].
- Les intrusions d'individus non autorisés dans les locaux scolaires peuvent être motivées par diverses intentions, allant du vol à des actes de violence planifiés. Ces

[1] Mme Nefissa Khiari-Hili, « Biométrie multimodale basée sur l'iris et le visage », Ecole nationale d'ingénieurs de Tunis Et L'université Paris-Saclay préparée à l'Université d'Evry Val d'Essonne, Thèse doctorale, Evry, France 2016.
[2] Meramria Nabila : «Reconnaissance de visages par Analyse Discriminante Linéaire(LDA)», Mémoire de master, Université Badji Mokhtar Annaba, 2016.

intrusions mettent en péril la sécurité de tous ceux qui se trouvent dans l'établissement[1].

En comprenant pleinement ces risques et ces menaces, les écoles peuvent mettre en œuvre des stratégies de prévention et des mesures de sécurité appropriées pour protéger leur communauté éducative[2].

3 Importance de la sécurité scolaire :

La sécurité scolaire occupe une place primordiale pour favoriser l'apprentissage et la réussite des élèves. Afin d'assurer cela, les écoles doivent mettre en place des mesures de protection visant à prévenir les menaces et à protéger les élèves et le personnel. Ces mesures comprennent l'embauche d'agents de sécurité, l'installation de caméras de surveillance, la mise en place de contrôles d'accès, l'élaboration de plans d'urgence et la formation continue des élèves et du personnel. Cependant, les écoles peuvent être confrontées à différents types de menaces en matière de sécurité, tels que la violence, l'usage de drogue, les armes à feu, les incendies, les catastrophes naturelles et les intrusions, entre autres.

Mettre en œuvre ces mesures peut toutefois être un défi, car cela peut être coûteux et prendre du temps. Il est donc essentiel pour les écoles de trouver un équilibre entre la sécurité et la liberté, afin de ne pas créer un environnement scolaire inquiétant ou ennuyeux.

Dans les années à venir, la technologie jouera un rôle de plus en plus important dans la sécurité scolaire. Des avancées telles que la reconnaissance faciale et l'analyse des données seront utilisées pour identifier les menaces potentielles. De plus, nous pouvons nous attendre à ce que des technologies encore plus sophistiquées soient utilisées pour protéger les écoles.

4 Enjeu Primordial de la surveillance de la présence des élèves :

La surveillance, le suivi de la présence et de l'assiduité des élèves en milieu scolaire présentent d'avantages en termes de réussite académique, de bien-être des élèves et de gestion efficace des ressources pédagogiques. Dans cette analyse, nous allons examiner les aspects clés de cette importance, en mettant en lumière les points suivants :

[1] Editeur : Université de « North Alabama Digital Press », un guide pratique pour les éducateurs : « Sécurité et sûreté dans les écoles primaires et secondaires», « Violence scolaire et prévention primaire», septembre 2023.
[2] Paul Timm, « Sécurité dans les établissements scolaires du primaire et du secondaire » : Guide pratique pour les éducateurs, pages 25- 40. Publié en 2018.

- **Évaluation de l'assiduité et de l'engagement des élèves :** La surveillance de la fréquentation permet aux écoles d'évaluer l'assiduité des élèves et leur niveau d'engagement dans le processus éducatif. Une présence régulière en classe est un indicateur important de l'implication des élèves dans leur apprentissage et de leur motivation à réussir.
- **Identification précoce des problèmes de comportement ou d'apprentissage :** La fréquentation irrégulière peut indiquer des problèmes sous-jacents tels que des défis en matière d'apprentissage, des troubles du comportement ou des difficultés familiales, en surveillant de près la fréquentation des élèves, les écoles peuvent repérer ces problèmes **précocement** et mettre en place des **interventions appropriées** pour les résoudre.
- **Optimisation des ressources pédagogiques :** Une compréhension approfondie de la fréquentation des élèves permet aux écoles d'améliorer la répartition des ressources pédagogiques, y compris le personnel enseignant et les programmes de soutien. En repérant les périodes de faible fréquentation ou les groupes d'élèves présentant un risque d'absentéisme, les écoles peuvent prendre des mesures pour renforcer le soutien et la supervision requis.
- **Amélioration de la réussite académique :** Des études ont démontré une forte corrélation entre la fréquentation régulière et la réussite académique **(Smith, 2018).** Les élèves qui sont fréquemment absents ont tendance à obtenir des résultats scolaires inférieurs et sont plus enclins à abandonner leurs études (**Jones & Brown, 2019**). En surveillant attentivement la présence des élèves et en mettant en place des mesures pour encourager une assiduité régulière, les écoles peuvent jouer un rôle essentiel dans l'amélioration des performances scolaires et la réduction du taux de décrochage (**Garcia et al. 2020**).
- **Promotion d'un environnement scolaire sûr et inclusif :** En garantissant une présence régulière de tous les élèves à l'école, les établissements scolaires favorisent un environnement d'apprentissage sûr, inclusif et respectueux **(Roberts et al, 2017).** La surveillance de la fréquentation permet de repérer rapidement les cas d'absentéisme non justifié et de mettre en place les interventions appropriées pour garantir la sécurité et le bien-être de tous les élèves **(Gonzalez & Lopez, 2019).**

5 Méthodes traditionnelles de surveillance de la présence :

Il convient de mentionner que les méthodes classiques couramment utilisées par les écoles et les enseignants pour collecter et gérer les données de fréquentation sont illustrées sur : **(Annexe N°01).**

5.1 Limitations et défis des méthodes traditionnelles :

Les méthodes traditionnelles sont souvent utilisées dans divers domaines, que ce soit en sciences, en recherche, en gestion de projet ou dans d'autres disciplines. Cependant, elles présentent également des limitations et des défis qu'il est important de prendre en compte.

Cette analyse approfondie se penchera sur ces limitations et défis, mettant en évidence les raisons pour lesquelles elles peuvent être problématiques et suggérant des alternatives ou des améliorations potentielles.

- Erreurs humaines et manque de fiabilité : Les méthodes traditionnelles telles que les listes de présence manuelles sont sujettes à des erreurs humaines, ce qui peut compromettre la fiabilité des données de fréquentation (Smith, 2018).
- Temps et travail intensif : La collecte et la gestion manuelles des données de présence peuvent être chronophages pour le personnel enseignant et administratif, entraînant une utilisation inefficace des ressources (Jones & Brown, 2019).
- Difficulté à traiter de grandes quantités de données : Les écoles avec un grand nombre d'élèves peuvent trouver difficile de gérer efficacement les données de fréquentation à grande échelle à l'aide de méthodes traditionnelles (Garcia et al, 2020).
- Manque de précision et de réactivité : Les méthodes traditionnelles ne permettent pas toujours une surveillance en temps réel de la fréquentation, ce qui peut entraîner des retards dans la détection des tendances d'absentéisme ou des problèmes potentiels (Roberts et al, 2017).
- Défi de la surveillance non intrusive **:** Les méthodes traditionnelles telles que les listes de présence manuelles peuvent ne pas être efficaces pour surveiller la fréquentation de manière non intrusive, ce qui peut affecter la confidentialité et le respect de la vie privée des élèves (**Gonzalez & Lopez, 2019**).

Nous ne soulignons que les méthodes classiques de suivi de présence telles que les appels nominaux manuels ou les feuilles de présence en papier sont souvent sujettes à des risques d'erreurs et d'inefficacités. Dont, l'intégration de la technologie de reconnaissance faciale dans

ces processus nécessite la mise en place de systèmes capables d'identifier et d'authentifier les élèves lors de leur arrivée en classe ou à l'école. Les données de présence collectées par ces systèmes permettent ensuite de générer des états et des rapports précis et à jour servant à l'exploitation administrative.

5.2 Avantages et inconvénients de l'utilisation de la reconnaissance faciale dans les écoles :

L'utilisation de la reconnaissance faciale dans les écoles présente à la fois des avantages et des inconvénients.

Voici quelques-uns des principaux points à considérer illustré sur les tableaux :

Nous allons explorer les avantages potentiels et fournir une description détaillée

Tableau (N°02-I) : Avantages potentiels de la reconnaissance faciale dans les écoles.

Avantage	Description
Amélioration de la précision des données de fréquentation	Réduction des erreurs et des données de fréquentation plus fiables
Gain de temps et d'efficacité	Automatisation des tâches chronophages et libération du temps des enseignants et des administrateurs
Identification rapide des absences	Intervention rapide en cas d'absences injustifiées et pour s'assurer de la sécurité des élèves
Détection des absences non justifiées	Amélioration de la discipline scolaire et réduction de l'absentéisme
Suivi des présences individuelles	Identification des élèves à risque d'abandon ou nécessitant un soutien supplémentaire

Ensuite, nous allons examiner les inconvénients mentionnés dans le tableau :

Tableau (N°03-I) : Inconvénients et défis potentiels de la reconnaissance faciale dans les écoles.

Inconvénient	Description
Préoccupations en matière de vie privée	Collecte et stockage de données biométriques sensibles
Discrimination et biais algorithmique	Erreurs d'identification et injustices potentielles
Coût des systèmes de reconnaissance faciale	Obstacle pour les écoles disposant de ressources limitées
Fiabilité des systèmes de reconnaissance faciale	Erreurs d'identification possibles, notamment dans des conditions défavorables
Impact psychologique sur les élèves	Sentiment de surveillance constante et atteinte au sentiment de vie privée

Source : recueillis sur internet

En fin de compte, nous présenterons un récapitulatif dans un tableau comparatif qui inclura les critères, les avantages et les inconvénients.

Tableau (N°04-I) : récapitulatif des critères, avantages et inconvénients de l'utilisation RF dans les écoles.

Critère	Avantages	Inconvénients
Précision des données de fréquentation	Plus élevée	Moins élevée
Gain de temps et d'efficacité	Oui	Non
Identification rapide des absences	Oui	Non
Détection des absences non justifiées	Oui	Non
Suivi des présences individuelles	Oui	Non
Vie privée	Risque accru	Protection accrue
Discrimination et biais algorithmique	Risque accru	Protection accrue
Coût	Élevé	Faible
Fiabilité	Moins élevée	Plus élevée
Impact psychologique sur les élèves	Négatif	Positif

Source : « Ministère de l'Education Nationale, de la Jeunesse et des Sports - absentéisme scolaire » https://dictionnaire.reverso.net/francais-definition/non+valide

5.3 Types d'implémentation de la reconnaissance faciale pour la surveillance de la fréquentation :

A propos de ce sujet, nous présenterons différents exemples d'utilisation de la technologie de reconnaissance faciale dans les écoles, nous aborderons trois types d'implémentations courantes : les systèmes de pointage biométriques, la surveillance par caméra avec reconnaissance faciale et les applications mobiles de suivi de la fréquentation. En explorant la diversité de ces applications dans le domaine de l'éducation, nous pourrons acquérir une meilleure compréhension de la manière dont la reconnaissance faciale est employée pour contrôler l'assiduité des élèves.

Les tableaux ci-dessous résument les différents types d'implémentations, les technologies utilisées, ainsi que les avantages et les limites associés à chacun.

Tableau (N°05-I) : Types d'implémentation de la reconnaissance faciale pour la surveillance de la présence des élèves et technologie utilisée.

Type d'implémentation	Description	Avantages	Inconvénients
Systèmes de pointage biométrique	Les élèves s'identifient à l'aide de leur visage, de leurs empreintes digitales ou de leur iris pour enregistrer leur présence et leur heure d'arrivée.	Précision élevée, Gain de temps, Automatisation de la collecte des données de fréquentation.	Coût élevé, Problèmes de confidentialité, Risque de discrimination algorithmique.
Surveillance par caméra avec reconnaissance faciale	Des caméras intelligentes avec des logiciels de reconnaissance faciale identifient les élèves et enregistrent leur présence et leurs déplacements.	Surveillance en temps réel, Capacité à identifier les élèves absents ou en retard, Possibilité de détecter des comportements suspects.	Préoccupations majeures en matière de vie privée, Risque de surveillance excessive, Coût élevé des systèmes et du stockage des données.
Applications mobiles de suivi de la fréquentation	Les élèves utilisent une application mobile pour signaler leur présence en classe en se prenant en photo ou en utilisant leur GPS.	Facilité d'utilisation * Accessibilité, Possibilité de signaler les absences en temps réel.	Dépendance des smartphones, Problèmes de fiabilité de la géolocalisation, Nécessité d'une connexion internet stable.

Source : recueillis sur internet

Tableau (N°06-I) : Comparaison des différents types d'implémentation de la reconnaissance faciale.

Critère	Systèmes de pointage biométrique	Surveillance par caméra avec reconnaissance faciale	Applications mobiles de suivi de la fréquentation
Précision	Élevée	Moyenne à élevée	Moyenne
Gain de temps	Oui	Oui	Modéré
Automatisation	Oui	Oui	Modérée
Vie privée	Risque modéré	Risque élevé	Risque modéré
Coût	Élevé	Élevé	Modéré
Surveillance en temps réel	Non	Oui	Non
Identification des absences	Oui	Oui	Modérée
Détection des comportements suspects	Non	Oui	Non

Source : « Génération Identité - Reconnaissance faciale : vers une surveillance généralisée des citoyens » https://cordis.europa.eu/article/id/203856-cuttingedge-facial-recognition-goes-mainstream/fr)

Conclusion :

Les éléments abordés dans cette section nous permettent de mieux comprendre les enjeux de la sécurité scolaire et les différentes approches pour contrôler la présence des élèves dans les écoles.

Le chapitre suivant abordera la biométrie et le système biométrique en général.

Chapitre II :

La Biométrie et le Système Biométrique

1 Introduction à la biométrie

La biométrie est une technologie qui utilise les caractéristiques distinctives physiques ou comportementales de chaque individu, telles que les empreintes digitales, la signature, l'iris, la voix, le visage ou la démarche, pour les identifier de manière unique. Contrairement aux mots de passe ou aux codes PIN, qui peuvent être oubliés ou utilisés de manière frauduleuse, et aux clés ou aux cartes magnétiques, qui peuvent être facilement volées, copiées ou perdues, les caractéristiques biométriques sont propres à chaque individu, ce qui rend difficile leur substitution par d'autres personnes. La pertinence de la biométrie dans les sociétés modernes a été augmentée à cause du grand besoin de la sécurité et à la nécessité des systèmes de management (gestion) d'identités à grande échelle, qui s'appuient fonctionnellement sur la détermination précise de l'identité d'un individu, dans un contexte d'applications largement interconnectées[1]. Actuellement, les technologies biométriques sont considérées comme les plus efficaces en termes de sécurité. Elles offrent également un niveau de confort supplémentaire, car elles n'exigent pas de transporter des éléments distincts tels que des cartes ou des clés. Par conséquent, elles sont largement utilisées pour l'identification et l'authentification dans divers systèmes tels que les guichets automatiques (ATM), les ordinateurs et même l'accès aux bâtiments.

Dans ce chapitre, nous introduisons tout d'abord quelques notions de bases liées à la biométrie, nous décrivons le principe de fonctionnement d'un système biométrique ainsi que les outils d'évaluations utilisés pour mesurer leurs performances, nous donnons un bref aperçu des modalités biométriques les plus répandues, tout en accordant une attention particulière à la reconnaissance par visages.

2 La biométrie :

2.1 Définitions :

Le mot biométrie signifie littéralement « mesure du vivant » et désigne dans un sens très large l'étude quantitative des êtres vivants. Parmi les principaux domaines d'application de la biométrie, on peut citer l'agronomie, l'anthropologie, l'écologie et la médecine[2].

La biométrie est une discipline qui utilise des mesures physiques ou comportementales pour identifier et authentifier de manière unique les individus. Elle repose sur le principe que

[1] Amir BENZAOUI, « Identification Biométrique par Descripteurs de Texture Locaux : Application au Visage & Oreille », thèse de doctorat Université 08 Mai 1945 – Guelma page 22,2015.
[2] https://fr.wikipedia.org/wiki/Biom%C3%A9trie.

chaque personne possède des caractéristiques biologiques uniques qui peuvent être utilisées pour la reconnaissance et la vérification de l'identité.

La biométrie Selon **l'Organisation internationale de normalisation (ISO)** : "est l'automatisation des processus de reconnaissance d'individus basée sur des caractéristiques biologiques ou comportementales uniques.

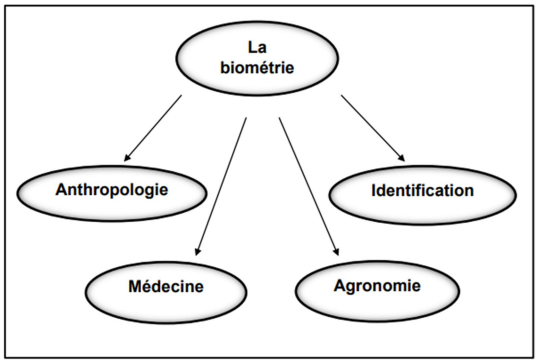
Et selon le **National Institute of Standards and Technology (NIST**) des États-Unis : "La biométrie est l'automatisation des méthodes utilisées pour reconnaître une personne basée sur des caractéristiques physiques ou comportementales uniques.

Ainsi, selon le **Centre national de la recherche scientifique (CNRS)** en France : "La biométrie fait référence aux techniques qui permettent d'identifier de manière automatique et fiable les individus à partir de leurs caractéristiques physiques ou comportementales."

2.2 Les différents domaines de la biométrie :

La biométrie est présente dans divers domaines tels que l'anthropologie, l'identification, la médecine et l'agronomie. Cette diversité est illustrée dans la figure x :

Figure (N° 01-II) : Les différents domaines de la biométrie.



2.3 Les avantages de la biométrie :

La biométrie offre plusieurs avantages dans divers domaines, notamment en matière de sécurité, d'identification et de gestion des données. On cite quelques-uns de ces avantages :

- **Sécurité accrue :** Les caractéristiques biométriques sont uniques à chaque individu, ce qui les rend très fiables pour l'identification. Comparé aux mots de passe ou aux

cartes d'identité, qui peuvent être oubliés, perdus ou volés, les données biométriques offrent une méthode d'authentification plus sûre[1].

- **Confort facilité d'utilisation :** Les systèmes biométriques sont souvent conviviaux, nécessitant simplement une interaction physique avec le capteur, comme placer un doigt sur un scanner d'empreintes digitales ou regarder une caméra pour la reconnaissance faciale. Cela les rend accessibles aux personnes de tous âges et de toutes compétences techniques[2]. Ces systèmes éliminent le besoin de se souvenir de mots de passe complexes, ce qui rend l'authentification plus pratique pour les utilisateurs. De plus, la reconnaissance biométrique est souvent rapide et ne nécessite pas d'effort conscient de la part de l'utilisateur[3].
- **Réduction des coûts liés à la gestion des mots de passe :** En remplaçant les méthodes traditionnelles d'authentification basées sur les mots de passe, la biométrie peut réduire les coûts associés à la réinitialisation des mots de passe oubliés et à la gestion des comptes utilisateurs[4].
- **Intégration multi-secteurs :** La biométrie est utilisée dans une variété de secteurs tels que la sécurité, les services financiers, les soins de santé, et les transports, ce qui démontre sa polyvalence et son potentiel dans différents domaines[5].
- **Réduction de la fraude :** En raison de leur caractère unique et intrinsèque, les caractéristiques biométriques réduisent considérablement le risque de fraude et d'usurpation d'identité. Cela est particulièrement important dans les secteurs financiers, gouvernementaux et de la santé, où l'authentification précise des individus est cruciale[6].
- **Augmentation de l'efficacité :** Les systèmes biométriques peuvent améliorer l'efficacité des processus d'identification et de vérification, réduisant ainsi les temps d'attente et les files d'attente. Par exemple, les contrôles de sécurité biométriques aux frontières peuvent accélérer les procédures d'embarquement des passagers[7].

[1] Jain, A. K., Ross, A., & Nandakumar, K. « Introduction to Biometrics »,2016.
[2] Ratha, N. K., Connell, J. H., & Bolle, R. M, « Enhancing security and privacy in biometrics-based authentication systems », 200.
[3] Rattani, A., & Cavoukian, A, « Biometric Encryptions : A Positive-Sum Technology That Achieves Strong Authentication, Security AND Privacy ». Springer, 2016.
[4] Haghighat, M., Zonouz, S. A., & Abdel-Mottaleb, M .CloudID: « Trustworthy cloud-based and cross-enterprise biometric identification ». Expert Systems with Applications, p 63, 255-264, 2016.
[5] Rathgeb, C., & Busch, C. « How biometric system interoperability enables identity management applications », IEEE Security & Privacy, 16(1), p 60-67, 2018.
[6] Sain, A. K., Ross, A., & Nandakumar, K, « Introduction to Biometrics »,2016.
[7] Kim, H., & Hong, S. « Development of a biometric identification system based on image processing », 2018.

- **Personnalisation des services :** La biométrie permet une personnalisation accrue des services en reconnaissant les utilisateurs individuels et en adaptant les expériences en fonction de leurs préférences et de leurs besoins. Par exemple, les assistants vocaux basés sur la reconnaissance vocale peuvent fournir des réponses personnalisées en fonction de l'utilisateur[1].

On souligne que ces avantages mettent en lumière l'essor significatif de la biométrie dans une gamme variée de domaines, mettant en évidence ses retombées positives sur la sécurité, l'efficacité et la personnalisation des services.

2.4 Défis de la biométrie :

Malgré les nombreux avantages qu'elle présente la biométrie, elle pose également un nombre de défis qui nécessitent une considération approfondie avant d'envisager son déploiement à grande échelle.

Principaux défis de la biométrie :

Nous ci-dessous énumérons les principaux défis de la biométrie :

- **Collecte et stockage des données :** La collecte et le stockage de données biométriques soulèvent des préoccupations majeures en matière de confidentialité et de vie privée. Ces données sont uniques et sensibles, et leur altération pourrait avoir des conséquences graves pour les individus.

Il est primordial de mettre en place des mesures de protection des données robustes pour préserver la confidentialité des individus[2]..

- **Faux positifs et faux négatifs :** Les systèmes biométriques peuvent parfois produire des résultats incorrects, tels que des faux positifs (identification incorrecte d'un individu comme authentique) ou des faux négatifs (rejet incorrect d'un individu légitime), ce qui peut compromettre la fiabilité et la sécurité des systèmes[3].
- **Vulnérabilités à la falsification :** Bien que les caractéristiques biométriques soient uniques, certaines méthodes de falsification, telles que la contrefaçon d'empreintes

[1] Turk, M., & Pentland, A. Face recognition using eigenfaces, 1991.
[2] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S, « Handbook of fingerprint recognition ». Springer Science & Business Media. 2009.
[3] Jain, A. K., Ross, A., & Nandakumar, K, « Introduction to Biometrics ». Springer, 2016.

digitales ou la reconstruction de visages à partir de données biométriques, peuvent compromettre la sécurité des systèmes biométriques[1].

- **Complexité et coûts d'implémentation :** La mise en place de systèmes biométriques peut être coûteuse et complexe en raison de l'investissement initial dans l'acquisition de matériel et de logiciels spécialisés, ainsi que des défis liés à l'intégration avec les infrastructures existantes et à la formation du personnel[2].

3 Le Système biométrique :

3.1 Définition d'un système biométrique :

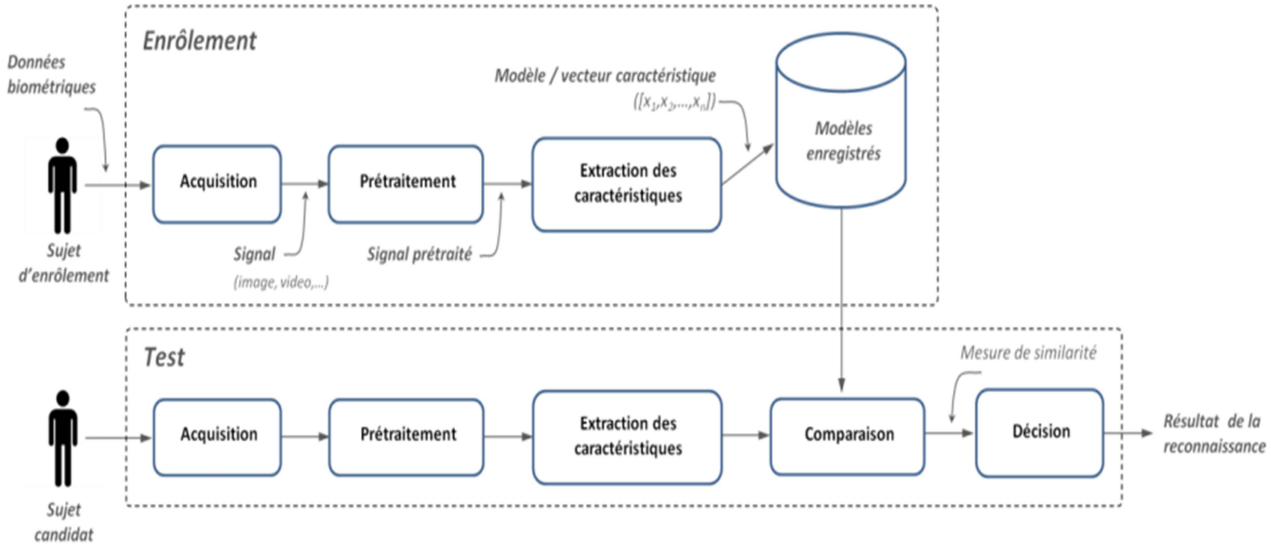
Un système biométrique est un système automatique de mesure basé sur la reconnaissance de caractéristiques propres à l'individu dans le but de vérifier son identité. En effet, ce système fonctionne en acquérant des données biométriques à partir d'un individu, extrayant un ensemble de caractéristiques à partir des données acquises, et comparant ces caractéristiques contre la signature dans la base de données[3].

3.2 Processus de fonctionnement d'un système biométrique :

Un système biométrique est essentiellement un système de reconnaissance de formes qui fonctionne en quatre étapes. La première est celle de l'acquisition des données biométriques de l'utilisateur. Ensuite, vient l'étape d'extraction des caractéristiques à partir des données acquises, éventuellement précédée d'une phase de prétraitement. La troisième étape se fait à travers la comparaison des caractéristiques extraites contre le modèle figurant dans la base de données et ce en vue de générer des mesures de similarité. En dernier lieu, une étape de décision sert à conclure sur l'identité de l'utilisateur.

[1] Opcit.
[2] Ratha, N. K., Connell, J. H., & Bolle, R. M, « Enhancing security and privacy in biometrics-based authentication systems ». IBM Systems Journal, 40(3), p 614-634, 2001.
[3] N.Morizet, « Reconnaissance biométrique par fusion multimodale du visage et de l'iris », Thèse Doctorat. École doctorale d'informatique, télécommunication et électronique de paris, France, 2009.

Figure (N° 02-II) : Processus de fonctionnement d'un système biométrique.



Le point de départ pour le système biométrique est la phase d'enrôlement. Dans cette phase, les données biométriques d'un utilisateur sont initialement collectées et traitées dans un modèle, forme sous laquelle elles sont ensuite stockées pour une utilisation permanente. Les modèles ne sont pas des données brutes ou des images numérisées d'un échantillon biométrique, mais ils sont une représentation mathématique de caractéristiques distinctives extraites par le système biométrique[1].

3.3 Modes de fonctionnement d'un système biométrique :

Il existe deux modes possibles pour un système biométrique : le mode d'identification qui répond à la question « **Qui suis-je** ? » et le mode de vérification (ou d'authentification) qui répond à la question « **Suis-je la personne que je déclare être** ? »[2] .

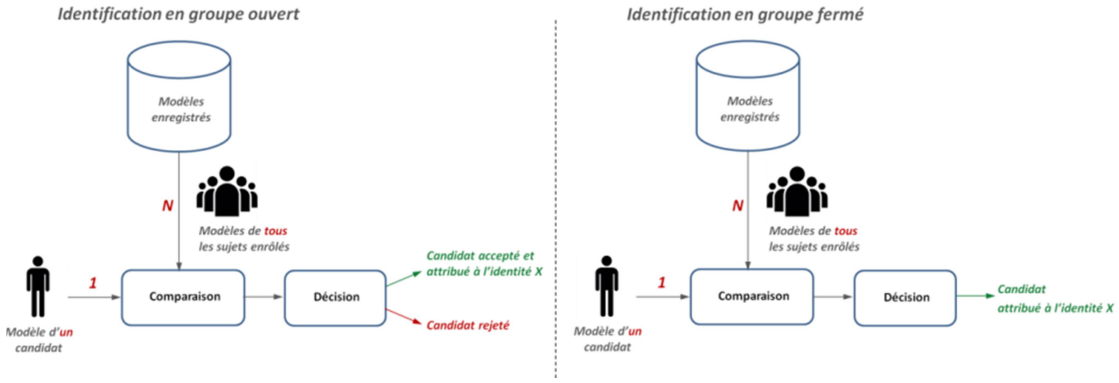
Le Mode d'identification :

Dans le processus d'identification, également connu sous le nom de reconnaissance « **one-to-many** », il s'agit de comparer le modèle biométrique du candidat avec ceux de tous les utilisateurs enregistrés dans la base d'enrôlement. Deux scénarios sont envisageables. Le premier consiste à opérer dans un environnement de groupe fermé, où l'on est certain que le candidat fait partie des utilisateurs autorisés, et le défi réside dans m'identification de l'identité correspondante au candidat. Le deuxième contexte scénario est celui d'un groupe

[1] Jain 2007.
[2] Mme Nefissa KHIARI-HILI, « Biométrie multimodale basée sur l'iris et le visage », Ecole Nationale D'ingénieurs De Tunis et Evry Essone paris, Thèse De doctorat mai 2016. https://www.biblio.univ-evry.fr/theses/2016/2016SACLE014.pdf

ouvert, où il est possible que le candidat soit un imposteur qu'il faut rejeter. Par conséquent, le système peut générer deux types de décisions : le rejet ou l'acceptation accompagnée de l'identification de l'identité du candidat.

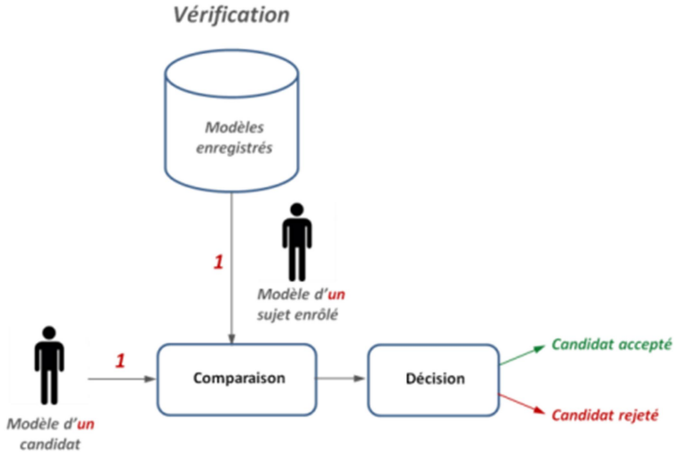
Figure (N° 03-II) : Systèmes en mode d'identification en groupe ouvert et en groupe fermé.



Le mode de vérification :

Dans le mode de vérification, également connu sous le nom d'authentification, le contexte est toujours celui d'un groupe ouvert, ce qui signifie qu'il n'est pas certain que l'identité du candidat soit réellement connue par le système. En pratique, le candidat revendique l'identité d'un des individus enregistrés dans la base de données. La comparaison se fait alors uniquement entre le modèle biométrique du candidat et les modèles de l'individu déclaré. Ainsi, il s'agit d'une reconnaissance "**one-to-one**" . Tous les systèmes biométriques proposés dans le cadre de cette étude relèvent du mode de vérification.

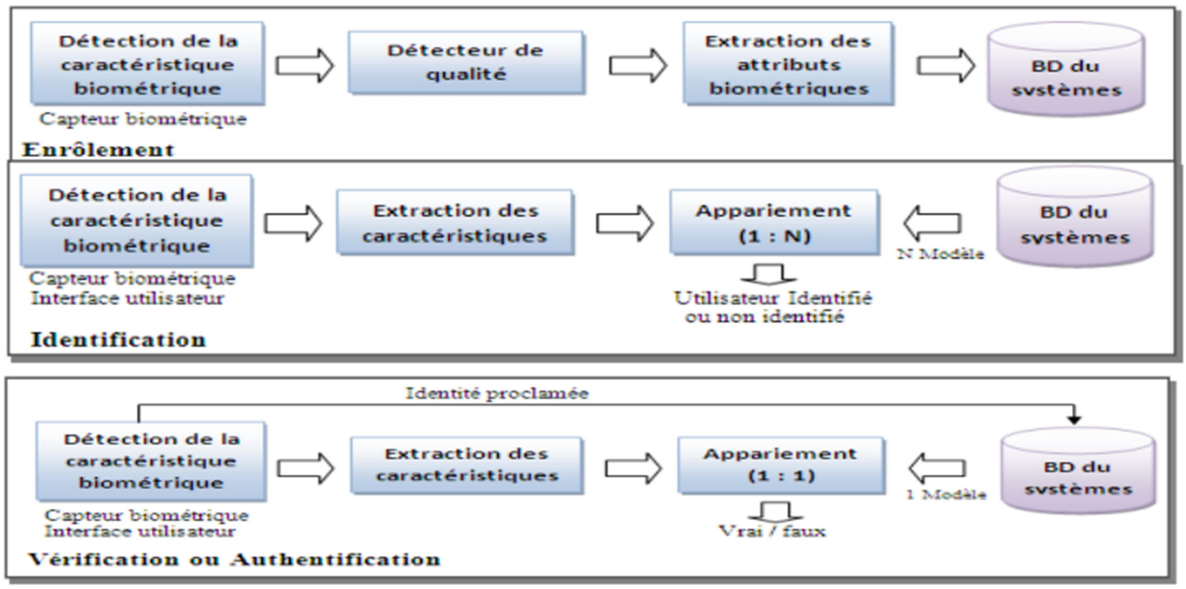
Figure (N° 04-II) : Système en mode vérification.



3.4 Les principaux modules d'un système biométriques :

Un système biométrique typique peut être représenté par quatre modules principaux :

Figure (N° 05-II) : Les différents modules d'un système biométriques



Source : internet.

3.4.1 Le module de capture :

Cet élément du système permet d'acquérir l'information biométrique. C'est l'entrée du système. C'est une caméra dans notre cas. Il varie selon les applications : scanner d'empreintes digitales, un microphone pour un système de reconnaissance vocale, etc.

3.4.2 Le module d'extraction des caractéristiques :

Il reçoit les informations du capteur, il n'en extrait que les données pertinentes. De ces dernières, ce module effectue une nouvelle représentation des données. Dans le cas idéal,

Cette nouvelle représentation doit être unique pour chaque visage et relativement invariante aux variations intra-classes.

3.4.3 Le module de correspondance :

Ce module est le troisième dans la chaine des éléments du système biométrique. Il se charge d'effectuer la comparaison de l'ensemble des caractéristiques extraites avec les modèles enregistrés dans la base des données. Il détermine ainsi le degré de ressemblance ou de dissemblance.

3.4.4 Le module de décision :

C'est au niveau de ce module que l'identité de la personne est déterminée. Cela se basant sur le degré de ressemblance entre les caractéristiques extraites et les modèles présents dans la base.

4 Domaines d'application de la biométrie :

Les principaux domaines d'application de la biométrie (source internet) :

A propos du contrôle d'accès :

- **Bâtiments et installations :** La biométrie peut être utilisée pour contrôler l'accès aux bâtiments et aux installations, en utilisant des empreintes digitales, des scans de la reconnaissance faciale ou des scans de l'iris. Cela peut aider à améliorer la sécurité et à prévenir les intrusions non autorisées.

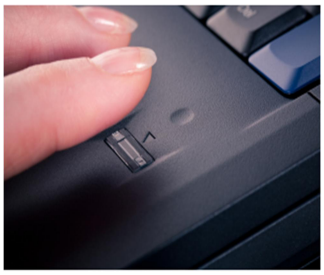
Figure (N° 06-II) : Contrôle d'accès biométrique.

source https://m.media-amazon.com/ consulté le 11/05/2024 13 :15

- **Ordinateurs et appareils :** La biométrie peut être utilisée pour protéger les ordinateurs et les appareils, en utilisant des empreintes digitales, des mots de passe

faciaux ou des scans de l'iris. Cela peut aider à prévenir le vol de données et l'utilisation non autorisée.

Figure (N° 07-II) : Authentification biométrique des ordinateurs.



source https://media.kasperskydaily.com consulté le 11/05/2024 13 :20

A propos de la Vérification de l'identité :

- **Passeports et visas :** La biométrie est de plus en plus utilisée dans les passeports et les visas, ce qui permet de s'assurer que les documents de voyage sont authentiques et que les titulaires sont bien les personnes qu'ils prétendent être.

Figure (N° 08-II) : Passeport biométrique source.

- **Vérification de l'identité des électeurs :** La biométrie peut être utilisée pour vérifier l'identité des électeurs, ce qui peut aider à prévenir la fraude électorale.

Figure (N° 09-II) : Vérification de l'identité des électeurs par la biométrie.

Source : https://www.thalesgroup.com/fr/markets/digital-identity-and-security/government/identity/enrolment/election-biometrique consulté le 11/05/2024 13 :23

A propos d'authentification des transactions :

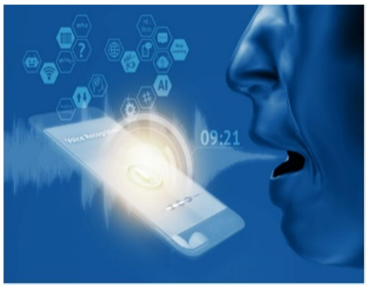
- **Paiements par carte :** La biométrie peut être utilisée pour authentifier les paiements par carte, ce qui peut aider à prévenir la fraude.

Figure (N° 10-II) : Authentification des paiements par carte par la biométrie

Source : https://cdn.next.ink/inpactv7/data-next/images/bd/wide-linked-media/7811.jpg

- **Accès aux comptes bancaires :** La biométrie peut être utilisée pour accéder aux comptes bancaires en utilisant la voix, ce qui peut aider à protéger les données financières contre les accès non autorisés (Sécuriser et faciliter l'accès aux comptes bancaires).

  Figure (N° 11-II) : Accès aux comptes bancaires par la biométrie.



Source :https://point-banque.fr/wp-content/uploads/2019/10/shutterstock_694633963.jpg

Ainsi on peut citer d'autres applications de la biométrie tels que :

- **Suivi du temps et de la présence** : La biométrie peut être utilisée pour suivre le temps et la présence des employés, ce qui peut aider à améliorer la productivité et la gestion des présences.
- **Sécurité des aéroports :** La biométrie peut être utilisée pour la sécurité des aéroports, en identifiant les passagers et en vérifiant leurs identités.
- **Application de la loi :** La biométrie peut être utilisée par les forces de l'ordre pour identifier les criminels et les suspects.

5 Les avantages et les limites de la biométrie :

5.1 Les avantages de la biométrie :

L'usage de la biométrie est un complément de l'utilisation des méthodes d'authentification comme des mots de passe, des badges, des cartes à puce…etc, cette technique possède plusieurs avantages parmi eux[1] :

- Suppression des mots de passe, suppressions des clés : au lieu de retaper son mot de passe dès que le PC se met en veille, une simple pression de l'empreinte digitale sur le capteur suffit et permet facilement de changer la session d'utilisateur.
- Utilisation d'une signature biométrique : Grande sécurité, intransmissible à une autre personne. Une identité vérifiée (Le destinataire est bien la personne autorisée à visualiser ou à utiliser les données). Lors de transactions financières, il est capital de savoir quel moyen de paiement du consommateur est le plus sûr
- Rehaussement de l'intégrité des informations et la sécurité.
- Réduction des attaques à l'égard des programmes gouvernementaux.
- Croissance de la confiance envers les systèmes de sécurité.
- Diminution des frais administratifs
- Accélération des services.

5.2 Les limites de la biométrie :

Selon le l'Institut national des normes et de la technologie(**NIST**) et l'Organisation internationale de normalisation (**ISO**), la biométrie est associée à plusieurs inconvénients et présente certaines limites majeures. Voici quelques-unes des principales limites de la biométrie :

[1] AIT AMIRAT Sofiane, MERZOUG Ziane, « Développement d'un système biométrique pour la reconnaissance de visages basé sur les ondelettes et une combinaison de deux types de réseaux neuronaux », Thèse de master université de Tizi-Ozou, p 37,2017-2018.

1. Erreurs et imprécisions :

- **Faux positifs (FA) :** Le système identifie par erreur une personne comme étant quelqu'un d'autre.
- **Faux négatifs (FN) :** Le système ne parvient pas à identifier correctement une personne autorisée.
- Taux d'erreur d'égalisation (EER) : Le point où les taux de FA et de FN sont égaux. **Variations intra-individuelles :** Les caractéristiques biométriques d'une personne peuvent changer avec le temps, en raison de facteurs tels que l'âge, les blessures ou les conditions médicales**.**
- **Qualité des données :** La précision de la biométrie dépend fortement de la qualité des données d'empreintes digitales, d'iris ou de visages capturés.

2. Vulnérabilité aux attaques :

- **Vol de données biométriques :** Les empreintes digitales, les scans d'iris ou les modèles de visages peuvent être volés à partir de bases de données ou de systèmes piratés.
- **Attaques par présentation :** De fausse empreinte digitale, des images d'iris ou des masques faciaux peuvent être utilisés pour tromper les systèmes biométriques. Attaques par rétro-ingénierie : Il est possible de reconstituer des données biométriques à partir de leurs représentations stockées, comme les modèles mathématiques.

3. Questions éthiques et de confidentialité[1] .

- **Collecte et stockage de données biométriques :** La collecte et le stockage de données biométriques soulèvent des occupations en matière de protection de la vie privée et de libertés individuelles. Discrimination et biais : Les systèmes biométriques peuvent être biaisés envers certains groupes démographiques, ce qui peut entraîner une discrimination.
- **Manque de transparence et de contrôle :** Les utilisateurs peuvent ne pas savoir comment leurs données biométriques sont collectées, utilisées et stockées.

6 Mesure de la performance d'un système biométrique :

L'évaluation des performances d'un système biométrique est essentielle pour déterminer son efficacité et sa fiabilité dans les modes de vérification et d'identification. Dans ci-après, on évoque les mesures couramment utilisées pour évaluer ces performances :

[1] Article The Ethics of Biometrics" by Simone Gaskell.

- ✓ **En mode vérification**, les performances d'un système biométrique sont données par la mesure de deux taux d'erreurs, le FRR (False Rejet Rate ou Taux de Faux Rejet) et le FAR (False Acceptation Rate ou Taux de Fausse Acceptation).

Le FRR : le taux de faux rejet ("False Reject Rate" ou FRR).

Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système.

Le FAR : le taux de fausse acceptation ("False Accept Rate" ou FAR).

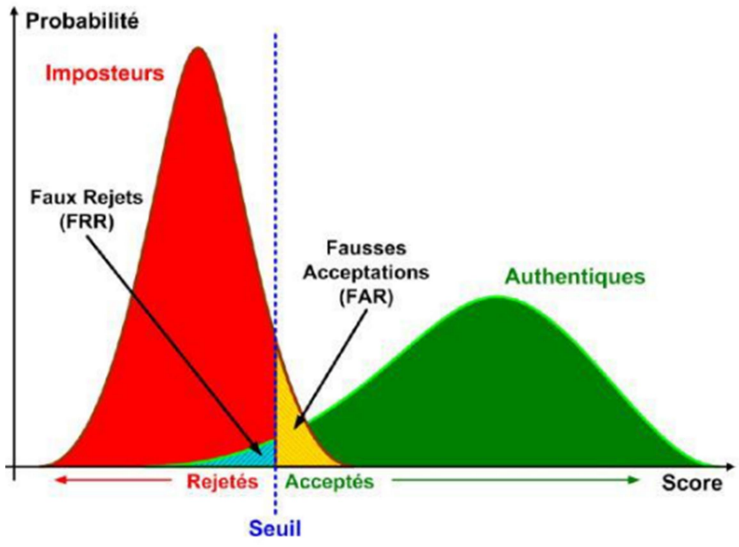
$$\mathbf{FRR = \frac{nombres\ des\ clients\ rejeté}{nombre\ total\ de\ test\ clients}}$$

Ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système.

$$\mathbf{FAR = \frac{nombres\ des\ imposteurs\ accépté}{nombre\ total\ de\ test\ imposteur}}$$

Le EER : le taux d'égale erreur ("Equal Error Rate" ou EER). Ce taux est calculé à partir des deux premiers critères et constitue un point de mesure de performance courant. Ce point correspond à l'endroit où **FRR = FAR**, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations.

Figure (N° 12-II) : Courbe de distribution des scores imposteurs et authentiques.



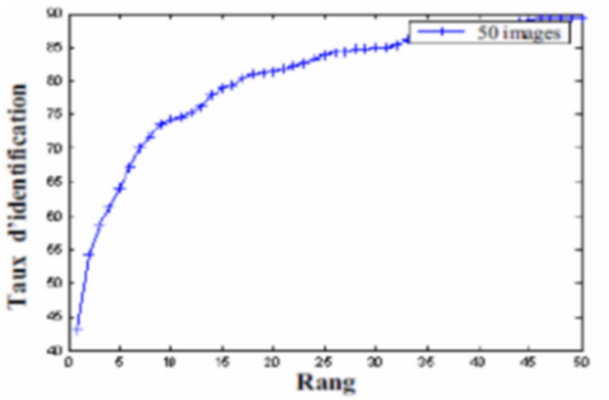
La figure illustre le FRR et le FAR à partir de distributions des scores authentiques et imposteurs[1] .

- ✓ **En mode Identification**, les performances sont mesurées par le pourcentage des personnes bien reconnues par rapport au nombre de tests, appelé le Taux d'Identification (**TID)** qui est définie par la formule suivante[2] .

$$\mathbf{TID} = \frac{\textbf{nombre de tests qui ont conduit a une bonne identification}}{\textbf{nombre total de tests}}$$

Ou peut aussi utiliser la courbe CMC qui indique le taux d'identification (TID) en fonction d'une variable qu'on appelle le rang ; on dit qu'un système reconnaît au rang 1 lorsqu'il choisit la plus proche image comme résultat de la reconnaissance. On dit qu'un système reconnaît au rang 2, lorsqu'il fait une bonne identification, parmi deux premières images choisis, etc. On peut donc dire que plus le rang augmente, plus le taux de reconnaissance augmente[3].

Figure (N° 13-II) : Courbe CMC.



[1] AIT AMIRAT Sofiane, MERZOUG Ziane, « Développement d'un système biométrique pour la reconnaissance de visages basé sur les ondelettes et une combinaison de deux types de réseaux neuronaux », Thèse de master université de Tizi-Ozou, p 24,2017-2018.
[2] AIT AMIRAT Sofiane, MERZOUG Ziane, « Développement d'un système biométrique pour la reconnaissance de visages basé sur les ondelettes et une combinaison de deux types de réseaux neuronaux », Thèse de master université de Tizi-Ozou, p 24,2017-2018.
[3] M.Bellili & M.FARSI. «Application de la DCT modifiée et GMM Orthogonale pour la Vérification du visage ». Mémoire pour l'obtention du diplôme d'ingénieur d'état en informatique. ESI, Algérie. 2012.

6.1 Mesures pour minimiser les erreurs biométriques :

Les erreurs biométriques peuvent avoir de graves conséquences pour les individus et les organisations. Il est donc important de prendre des mesures pour minimiser ces erreurs. Voici ci-après quelques-unes des mesures à prendre pour réduire le risque d'erreurs biométriques :

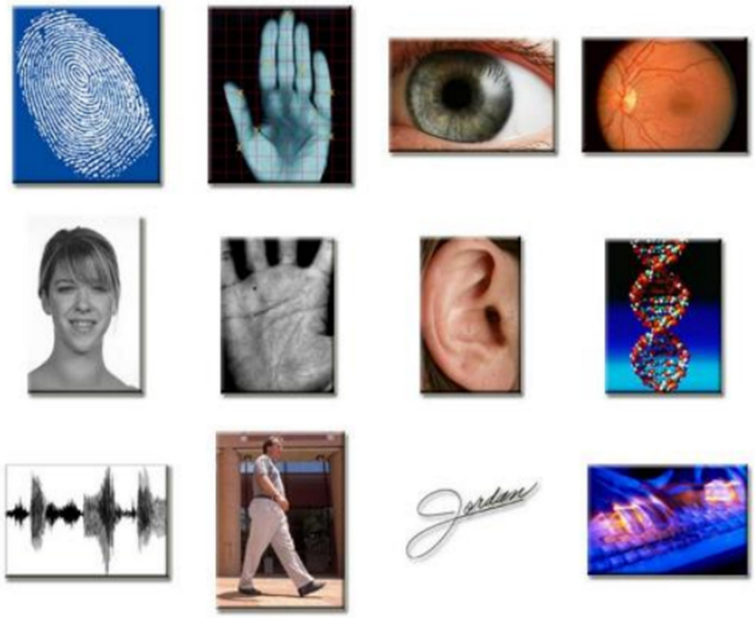
- ✓ **Choisir la technologie biométrique appropriée :** Il est important de choisir une technologie biométrique adaptée à l'application et à l'environnement dans lesquels elle sera utilisée.
- ✓ **Assurer la qualité des données biométriques :** Il est important de collecter et de stocker des données biométriques de haute qualité. Cela peut inclure la formation des utilisateurs sur la façon de présenter correctement leurs empreintes digitales ou leur visage au scanner.
- ✓ **Mettre en place des contrôles de qualité :** Des contrôles de qualité réguliers doivent être effectués pour garantir que les systèmes biométriques fonctionnent correctement.
- ✓ **Surveiller les performances du système :** Les performances des systèmes biométriques doivent être surveillées en permanence afin d'identifier et de corriger les problèmes potentiels.
- ✓ **Mettre à jour les systèmes biométriques :** Les systèmes biométriques doivent être mis à jour régulièrement avec les dernières technologies et correctifs de sécurité.

7 Les différentes techniques de la biométrie :

Les techniques biométriques utilisées dans différentes applications et secteurs peuvent être regroupées en trois catégories principales :

1. **Biométrie basée sur les caractéristiques physiques :** telles que : la reconnaissance de l'iris, du visage, de la main et de l'empreinte digitale).
2. **Biométrie basée sur les caractéristiques comportementales** : comprend des techniques telles que la reconnaissance vocale et la signature).
3. **Biométrie basée sur la physiologie interne** : englobe des techniques qui utilisent des informations biométriques internes, telles que les empreintes **veineuses** ou la reconnaissance de l'**ADN**.

Figure (N° 14-II) : Différentes techniques et modalités biométriques



Source : recueille sur internet

On peut énumérer quelques techniques dans ci-après :

- ✓ **Reconnaissance d'empreintes digitales :** Cette technique utilise les motifs uniques des empreintes digitales pour identifier les individus. Elle est largement utilisée dans les applications de sécurité et de contrôle d'accès[1].
- ✓ **Reconnaissance faciale :** La reconnaissance faciale analyse les caractéristiques faciales d'une personne pour l'identification. Elle est utilisée dans divers domaines, notamment la sécurité, la surveillance et la biométrie mobile[2].
- ✓ **Reconnaissance de l'iris :** Cette technique utilise les motifs uniques présents dans l'iris de l'œil pour l'identification. Elle est réputée pour sa précision et est souvent utilisée dans les systèmes de sécurité haut de gamme [3].
- ✓ **Reconnaissance de la voix :** La reconnaissance de la voix analyse les caractéristiques vocales d'un individu, telles que le timbre, la tonalité et les modèles de parole, pour

[1] Jain, A. K., Ross, A., & Nandakumar, K. (). « Introduction to Biometrics ». Springer, 2016.
[2] Li, S. Z., & Jain, A. K. (). « Handbook of Face Recognition ». Springer, 2011.
[3] Daugman, J. G. (). « How Iris Recognition Works ». IEEE Transactions on Circuits and Systems for Video Technology, 14(1), p 21-30, 2004.

l'identification. Elle est utilisée dans les systèmes de contrôle d'accès et les applications de téléphonie[1] .

- ✓ **Reconnaissance de la rétine :** Cette technique analyse les motifs uniques présents dans la rétine de l'œil pour l'identification. Bien que moins répandue que la reconnaissance de l'iris, elle est utilisée dans certains environnements de sécurité sensibles[2].
- ✓ **Reconnaissance de la démarche :** Cette technique utilise des capteurs pour mesurer la manière dont une personne marche. La démarche de chaque individu est unique et peut être utilisée comme moyen d'identification.
- ✓ **Reconnaissance de la signature :** Cette technique analyse les caractéristiques de la signature manuscrite pour l'authentification des individus. Elle est souvent utilisée dans les applications bancaires et juridiques[3].

Une récapitulation sur **(Annexe N°02)** montrant les avantages et les inconvénients des différentes techniques biométrique les plus répandus :

[1] Huang, Z., & Acero, A. (). « Spoken Language Processing: A Guide to Theory, Algorithm and System Development ». Prentice Hall, 2001.
[2] Wildes, R. P. (). « Iris Recognition : An Emerging Biometric Technology. Proceedings of the IEEE », 85(9), p 1348-1363, 1997.
[3] Plamondon, R., & Srihari, S. N. (). « Online and Off-line Handwriting Recognition : A Comprehensive Survey ». IEEE Transactions on Pattern Analysis and Machine Intelligence, 22(1), p 63-84, 2000.

Conclusion :

Dans ce chapitre, nous avons présenté des généralités sur la biométrie, ses différentes applications dans divers domaines. Après une introduction sur la biométrie, nous avons examiné les avantages et les inconvénients tout en reconnaissant les défis auxquels elle est confrontée, nous avons décrit également le fonctionnement d'un système biométrique, son processus de fonctionnement, ainsi que les différentes modalités utilisées dans un système biométrique, tout en soulignant les avantages et les inconvénients de chacune, Ensuite , nous nous sommes intéressées à la mesure des performances en examinant les critères utilisés pour évaluer son efficacité. Nous avons également abordés les mesures préconisées pour minimiser les erreurs biométriques. Enfin, nous avons évoqués les différentes techniques utilisées en biométrie, suivie par une en brève description des principaux types tels que la reconnaissance faciale, l'empreinte digitale, la reconnaissance de l'iris et la reconnaissance vocale.

Le prochain chapitre sera consacré à la conception système objet d'étude.

Chapitre III :

Conception du système

1 Introduction

Il est important de souligner qu'UML n'est pas une méthode de développement, mais plutôt un langage utilisé dans le cadre du développement logiciel. Ainsi, afin de passer des besoins initiaux à un code final, il est nécessaire d'avoir un processus de développement en place. Dans notre cas, nous avons choisi d'utiliser le processus UP (Unified Process).

Dans ce chapitre, nous proposons une démarche pragmatique et simplifiée pour mener l'activité d'analyse d'un système d'information. Cette démarche permet de formaliser le système à développer et se traduit par la création de plusieurs diagrammes qui offrent une représentation à la fois statique et dynamique du système. Notre démarche est structurée en six étapes distinctes. Dans les paragraphes suivants, nous allons expliquer en détail chacune de ces étapes.

2 Démarche simplifiée pour l'analyse

La démarche est structurée en cinq (5) étapes :

Etape 1 : Etude préliminaire

- Présentation général du projet.
- Description du contexte du système :
  - ✓ Identification des acteurs.
  - ✓ Réalisation du diagramme de contexte.

Etape 2 : Identification et représentation des cas d'utilisation.

Etape 3 : Description et représentation des scénarios.

Etape 4 : L'identification des classes et des objets.

Etape 5 : Elaboration du diagramme de classe.

2.1 Etude préliminaire

2.1.1 Objectifs :

Cette première étape du processus de développement consiste à positionner précisément le champ du système étudié et à faire un premier repérage des besoins (les besoins peuvent être fonctionnels ou opérationnels), en utilisant principalement le texte. Cette étape prépare l'activité de description des besoins par les cas d'utilisation (C.U).

2.1.2 Présentation générale du projet

Les objectifs globaux de notre système sont les suivants :

- Identifier et reconnaitre les visages des étudiants de manière automatique.
- Optimiser le temps d'exécution, de traitement et l'obtention des données.
- Contrôler l'accès et assurer la sécurité des informations.
- Automatiser les tâches manuelles et simplifie le processus de prise de présence des étudiants.
- L'administrateur peut effectuer la mise à jour régulière du système.
- Améliorer, l'efficacité, la sécurité et convivialité du processus de prise de présence des étudiants.

2.2 Description du contexte du système

➢ L'identification des acteurs :

Les acteurs principaux sont :

- **L'utilisateur (***Agent-Surveilance***)** : est la personne qui lance l'application et interagit avec celleci.il s'authentifier en utilisant un nom d'utilisateur et un mot de passe valide ; son rôle de contrôler la présence des étudiants, voir état présence.
- **L'Administrateur** : Responsable de la gestion global du système, aura la possibilité de d'effectuer des mises à jours régulières du système, de gérer les données des étudiants et de contrôler l'accès au système (Ajouter, supprimer, modifier ; afficher).

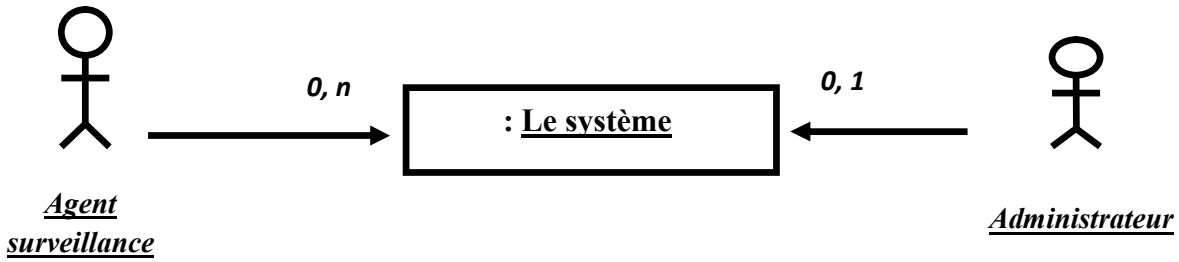
➢ Réalisation du diagramme de contexte :

A partir des informations obtenues lors des deux précédentes, nous allons modéliser le contexte de notre application.

- **Diagramme de contexte statique :**

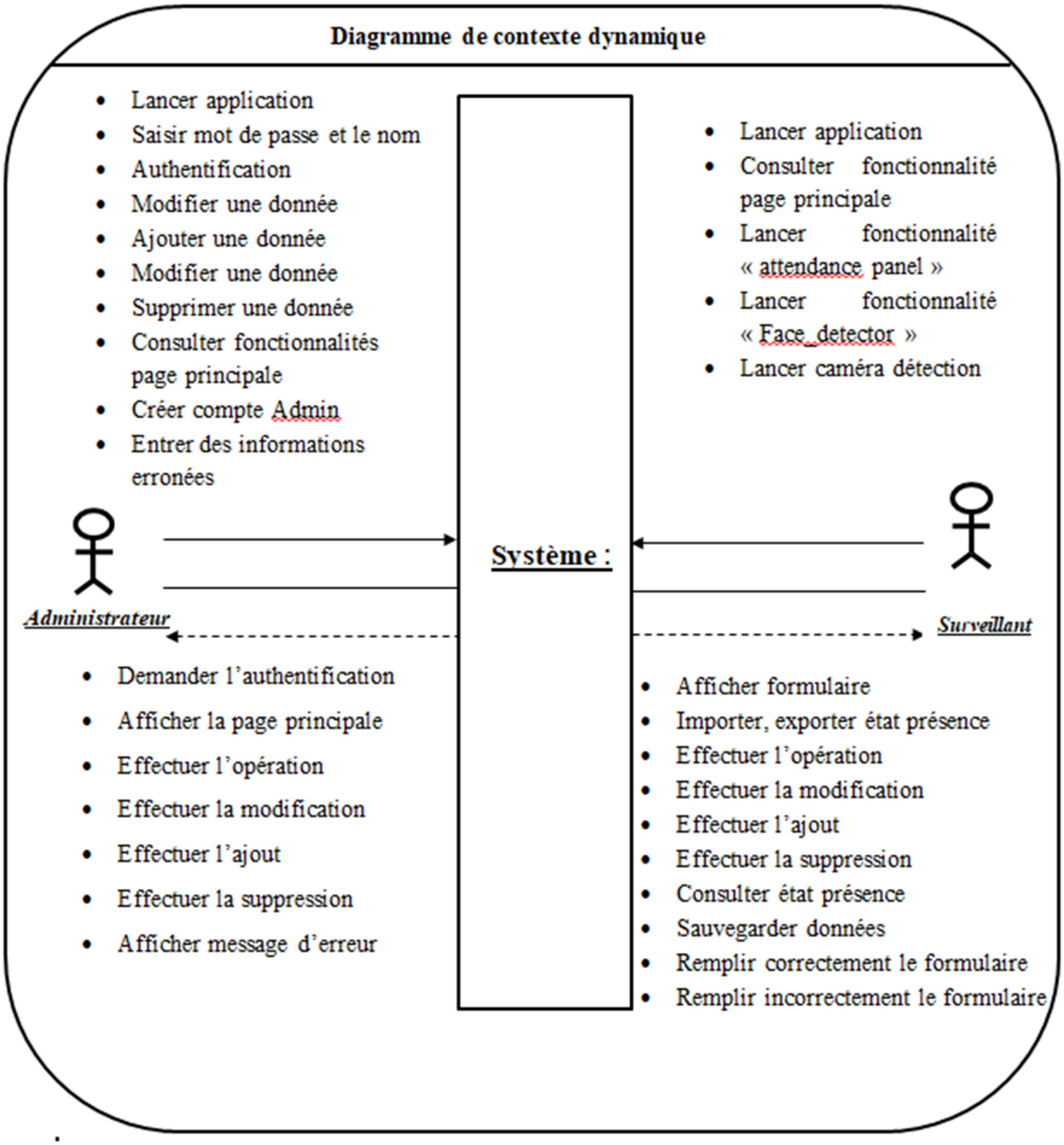
Ce diagramme représente principalement le nombre d'utilisateurs (*Agent-Surveilance*) qui pouvant accéder à l'application, ainsi que le nombre d'administrateurs.

Figure (N° 01-III) : Diagramme de contexte statique.



- **Diagramme de contexte dynamique :**

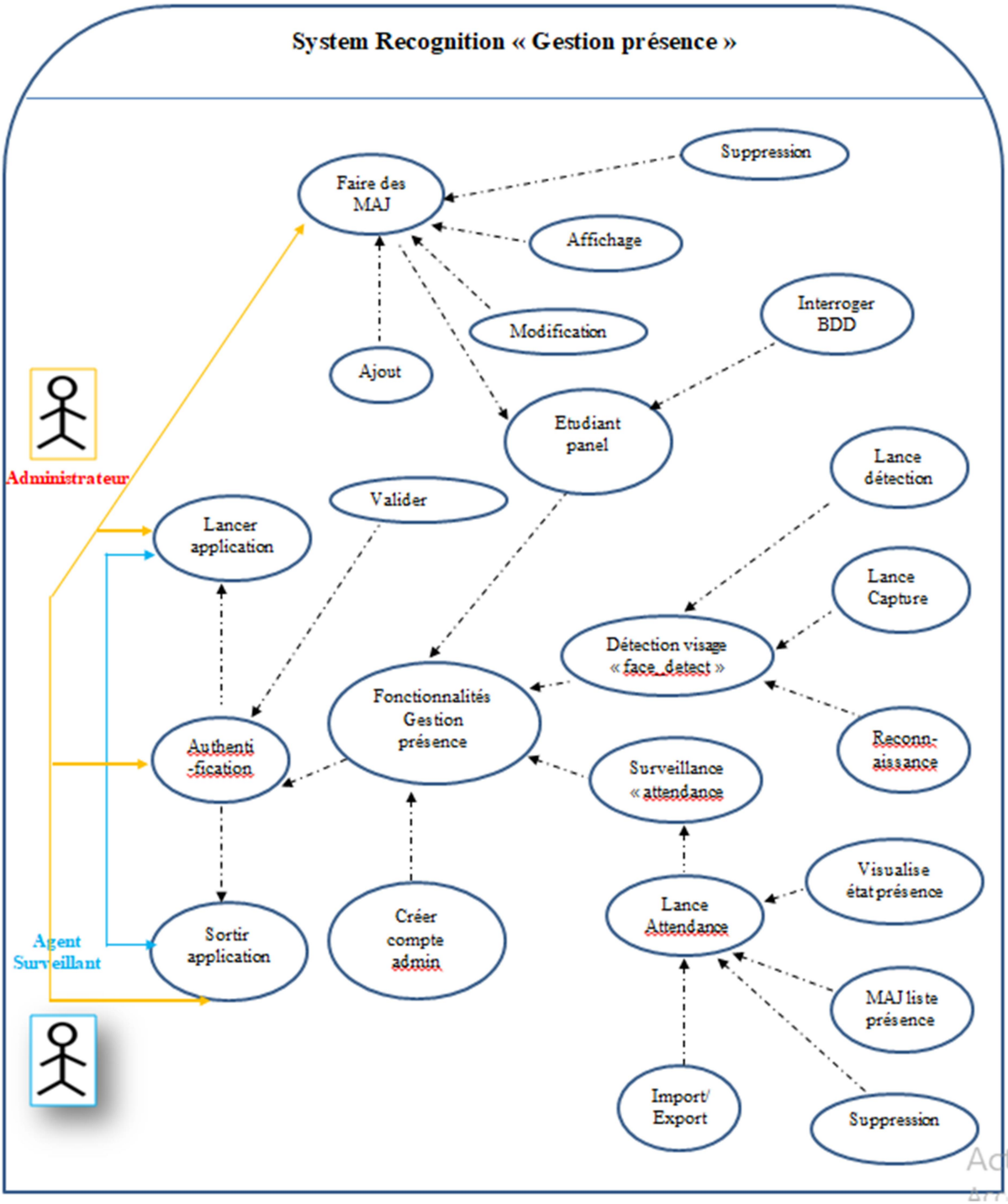
Figure (N° 02-III) : Diagramme de contexte dynamique.



3 Identification et représentation des cas d'utilisation

L'identification des cas d'utilisations, nous donne un aperçu des fonctionnalités futures que doit implémenter le système.

Figure (N° 03-III) : Diagramme de cas d'utilisation.



4 La description et la représentation des scénarios

Nous allons maintenant détailler chaque cas d'utilisation qui doit faire l'objet d'une définition a priori qui décrit l'intention de l'acteur lorsqu'il utilise le système et les séquences d'actions principales qu'il est susceptible d'effectuer.

❖ ***Remarque*** **:** dans cette étape nous allons présenter pour chaque cas d'utilisation :

- ✓ La fiche descriptive.
- ✓ Le diagramme d'activité.
- ✓ Le diagramme de séquence.

4.1 Les fiches descriptives

Les descriptions vont être organisées de la façon suivante :

Nom du cas d'utilisation
Objectif du cas d'utilisation
Liste des acteurs
Scénario nominal : < action en début > < action en cours > < action enfin >

Dans ce chapitre, nous allons expliquer deux cas d'utilisateur le reste sera présenté en Annexe

➢ Cas d'utilisation ***: «*** **Authentification Admin»**

Authentification
Ce cas d'utilisation permet à l'administrateur de s'authentifier.

L'administrateur
Début : • Faire Introduire le login user et mot de passe • Le système vérifier la validité d'authentification. **En cours :** **Si** le user et mot de passe sont valides **alors** • Le système affiche l'interface principale : « gestion des présence reconnaissance faciale » • Le système vérifie les informations entrées : **Sinon** • Le système affiche un message d'erreur. • Le système affiche login pour réessayer. **En fin :** Le système autorise l'accès à l'application avec succès.

- Cas d'utilisation **« créer compte Admin»**

créer compte Admin
Ce cas d'utilisation permet à l'administrateur de créer un compte Admin
L'administrateur
Début : • Faire Introduire user et mot de passe pour rendre accès l'application • Le système vérifier la validité d'authentification. **En cours :** • Le système affiche l'interface principale • l'administrateur fait appel à la fonctionnalité « **Register »**. • Le système affiche un formulaire pour saisir les informations • L'administrateur remplit le formulaire « **Register »** et valide les données. **Si** le formulaire est remplit correctement **alors** le système affirme à l'utilisateur que les informations entrées sont enregistrées avec succès

Sinon

- Le système affiche un message d'erreur.
- Le système vous donne la possibilité à réessayer de remplir le formulaire.

En fin :

• Le système enregistre les données saisies et termine la création du compte avec succès.

- Cas d'utilisation **« GESTION étudiant»**

GESTION étudiant
Ce cas permet saisir l'administrateur et Agent surveillance de remplir le formulaire étudiant
Administrateur et Agent surveillance
Début • Faire entrer user et le mot de passe (uniquement pour Admin) • Le système vérifier la validité d'authentification. **En cour** • Le système affiche l'interface principale et la fonctionnalité « student panel » • L'utilisateur rend accès à la fonctionnalité « student panel » • Le système affiche un formulaire pour la saisie des informations de l'étudiant **Si** le formulaire est remplit correctement **alors** le système affirme à l'utilisateur que les informations entrées sont enregistrées avec succès **Sinon** • Le système affiche un message d'erreur.

• Le système vous affiche de réessayer de saisir le formulaire. **En fin** • le système enregistre les données saisies avec succès. • le système affiche le formulaire de renseignements pour une nouvelle saisie.

➢ Cas d'utilisation **« détection de visage»**

Détection visage « face_detector »
Ce cas d'utilisation permet à l'administrateur et Agent surveillance de vérifier la présence
L'administrateur et Agent surveillance
Début : • Faire Introduire le user et le mot de passe • Le système vérifier la validité d'authentification. **En cours :** • Le système affiche l'interface principale • L'utilisateur « Agent surveillant » demande accès à la fonctionnalité « **face_detector** » • Le système affiche la scène de capture d'image. • L'utilisateur « Agent surveillant » lancer la caméra • Le système utilise méthode de détection- reconnaissance • Le système affiche les informations (nom, prénom, ID,Roll_no sur le visage étudiant identifié) • Le système n'affiche rien si la personne n'a pas été reconnue **En fin :** Le système est terminé avec succès, le processus de détection se fait en temps réel

- Cas d'utilisation **« Control de Présence « Attendance »**

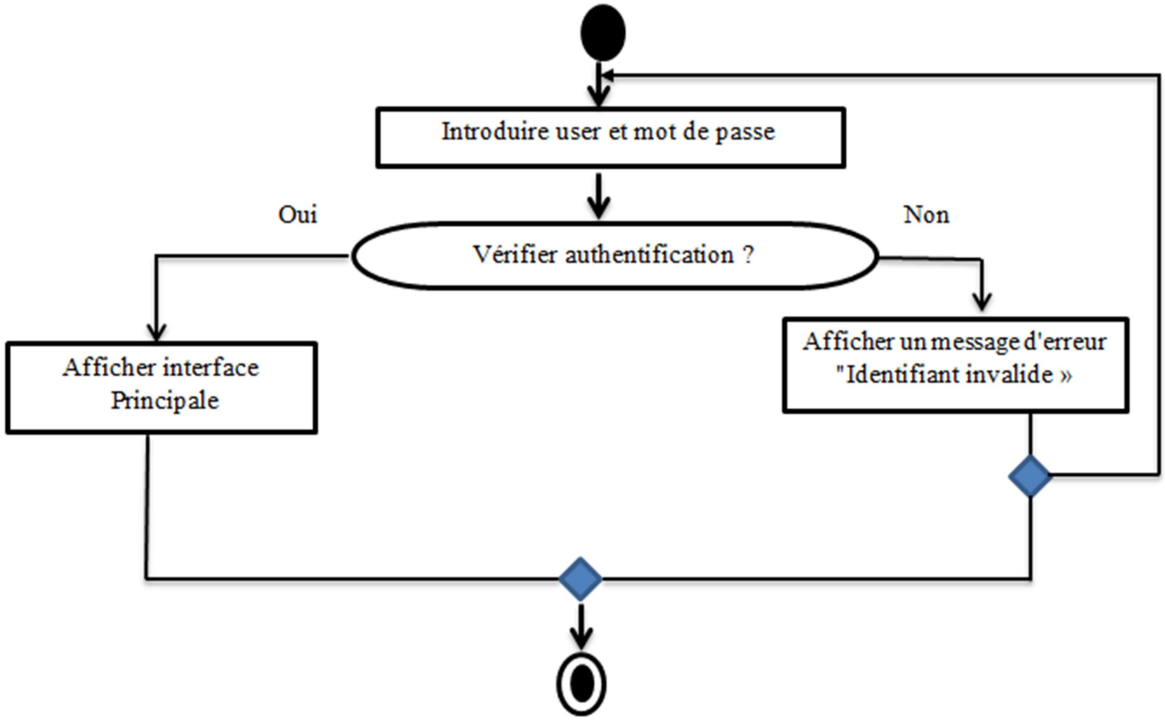
Control de Présence « Attendance »
Ce cas d'utilisation permet à l'administrateur et attendant de contrôler la présence
L'administrateur et Agent surveillance
Début : • Faire Introduire le user et le mot de passe (uniquement Admin) • Le système vérifier la validité d'authentification. **En cours :** • Le système affiche l'interface principale • L'utilisateur « agent surveillance » demande accès la fonctionnalité « Attendance » • Le système redirige l'utilisateur et affiche la page de visualisation d'état de présence • l'utilisateur visualise l'état de présence des étudiants. • L'utilisateur exploite l'état de présence (importer, exporter). • L'utilisateur mettre à jour l'état de présence (modifier ; supprimer) **En fin :** Le système est terminé avec succès avec état présence généré

4.2 Les diagrammes d'activité

Pour chaque cas d'utilisation , nous allons présenter un diagramme d'activité qui permet de présenter graphiquement le déroulement du cas d'utilisation.

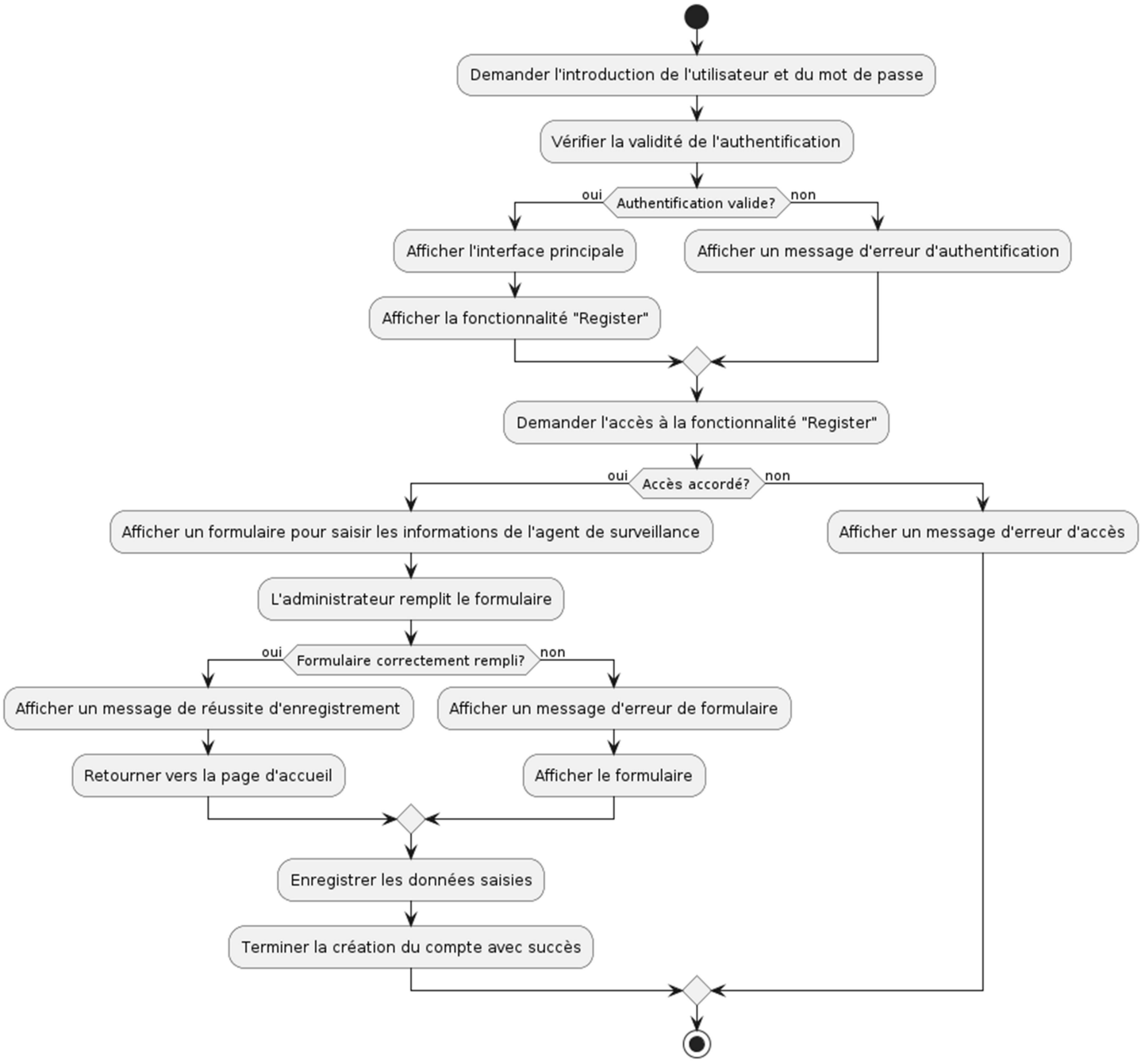
- Cas d'utilisation *: «* **Authentification»**

Figure (N° 04-III) : Diagramme d'activité pour CU "Authentification".



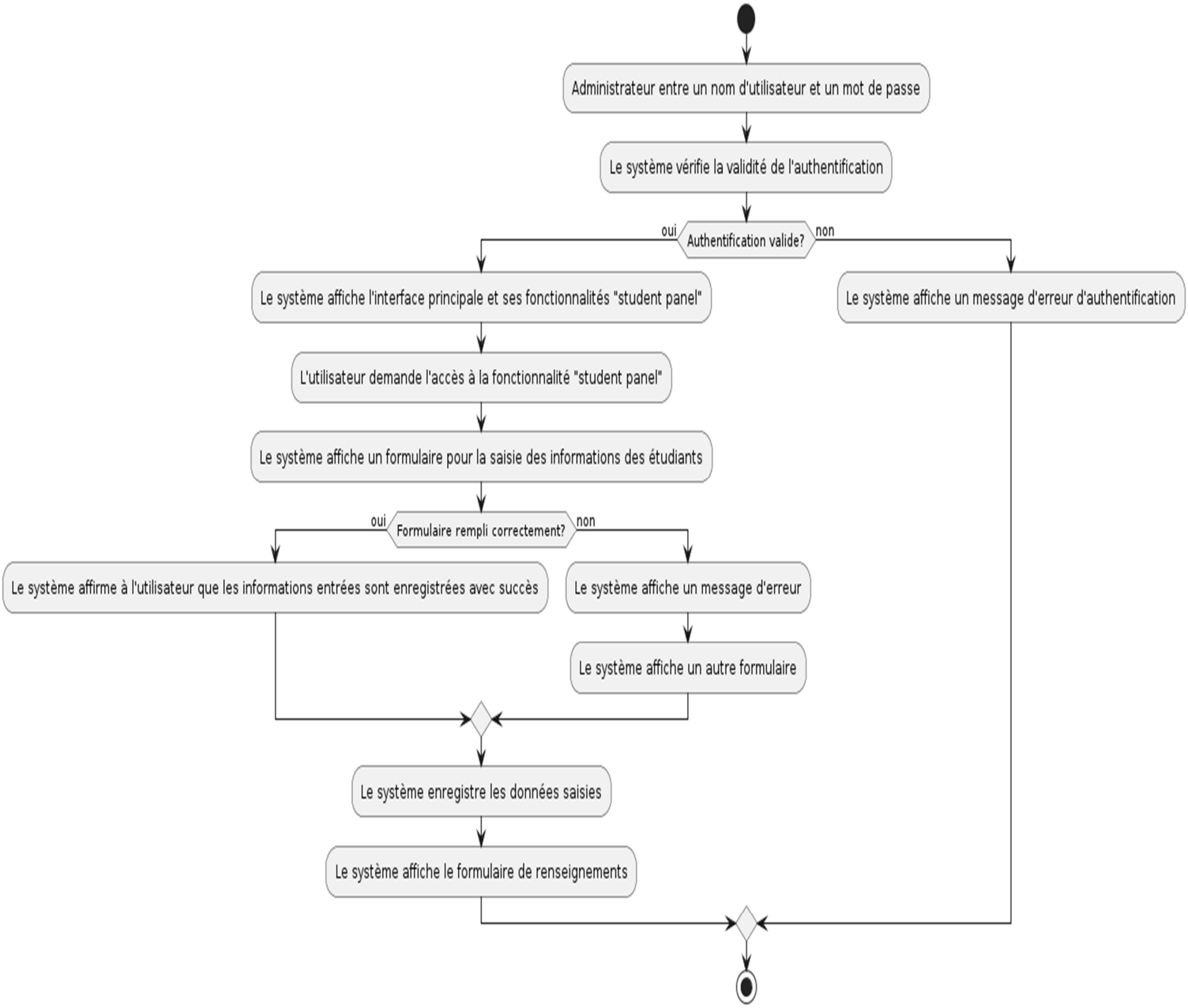
Cas d'utilisation *:* « Cas d'utilisation **« Créer compte Admin»**

Figure (N° 05-III) : Diagramme d'activité pour CU " Cas d'utilisation « Créer compte Admin»".



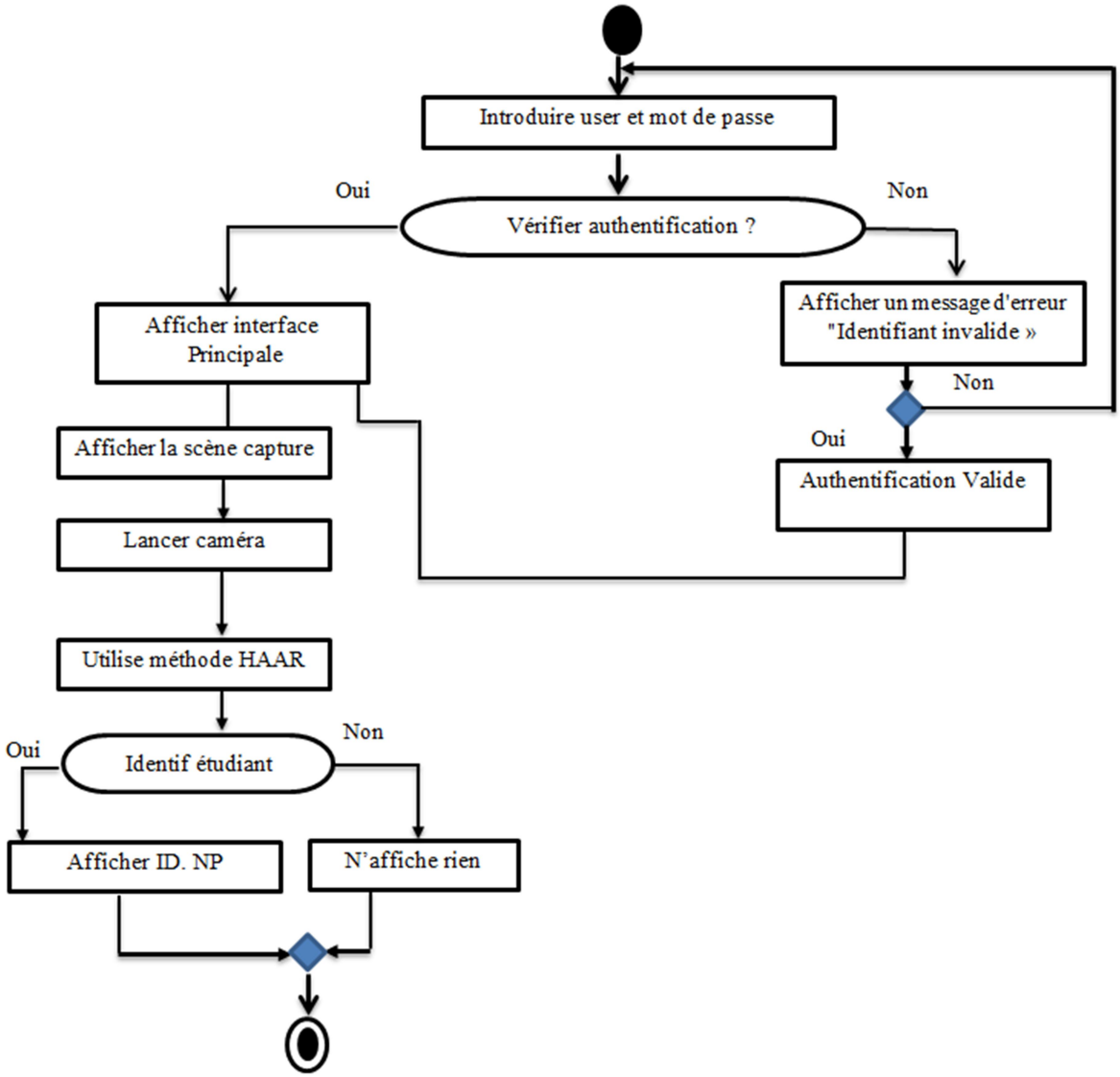
- Cas d'utilisation *: «* Cas d'utilisation **« GESTION étudiant»**

Figure (N° 06-III) : **Diagramme d'activité pour CU " Cas d'utilisation « GESTION étudiant»".**



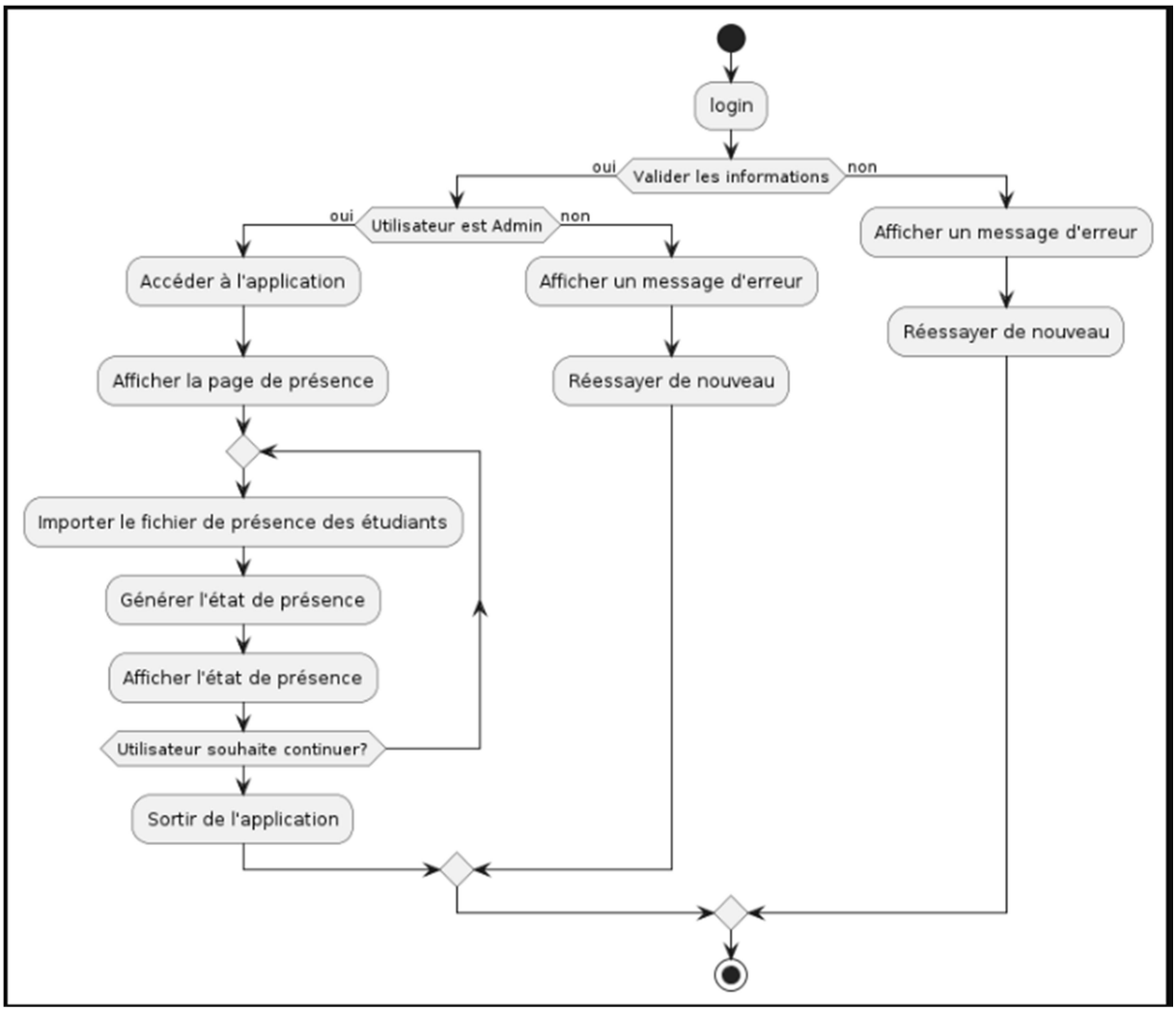
Cas d'utilisation *:* « Cas d'utilisation **« détection de visage»**

Figure (N° 07-III) : Diagramme d'activité pour CU Cas d'utilisation «détection de visage»".



Cas d'utilisation *: «* Cas d'utilisation **« control présence»**

Figure (N° 08-III) : Diagramme d'activité pour CU " Cas d'utilisation «control présence»".

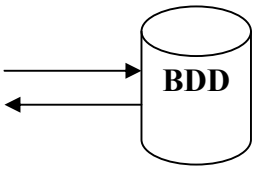


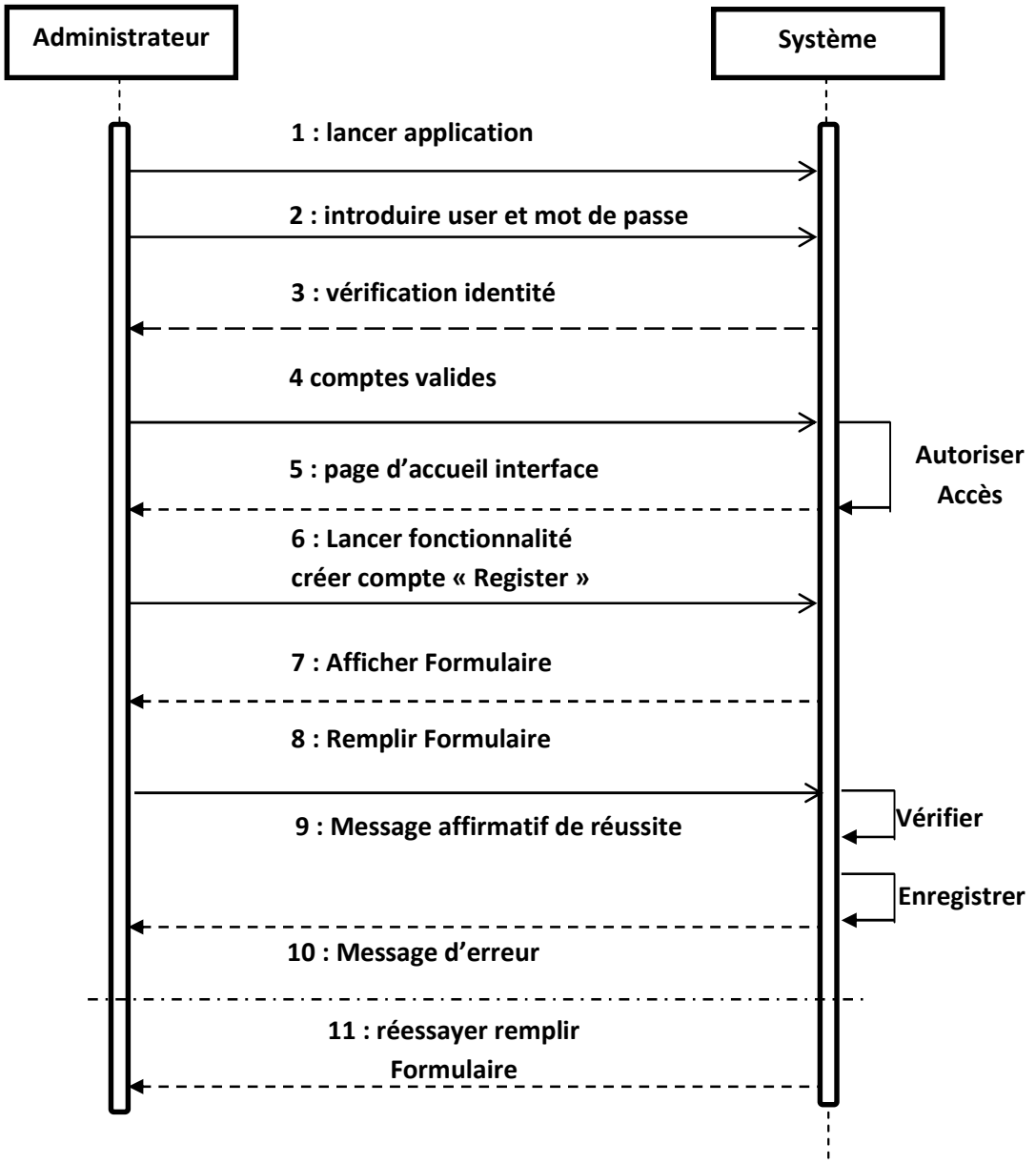
4.3 Les diagrammes de séquences

Pour chaque cas d'utilisation, nous allons présenter un diagramme de séquence qui permet d'attribuer précisément les responsabilités de comportement aux classes d'analyse.

- Cas d'utilisation ***: «*** **Créer compte Admin »**

Figure (N° 09-III) : Diagramme séquence pour CU " créer compte Admin ".

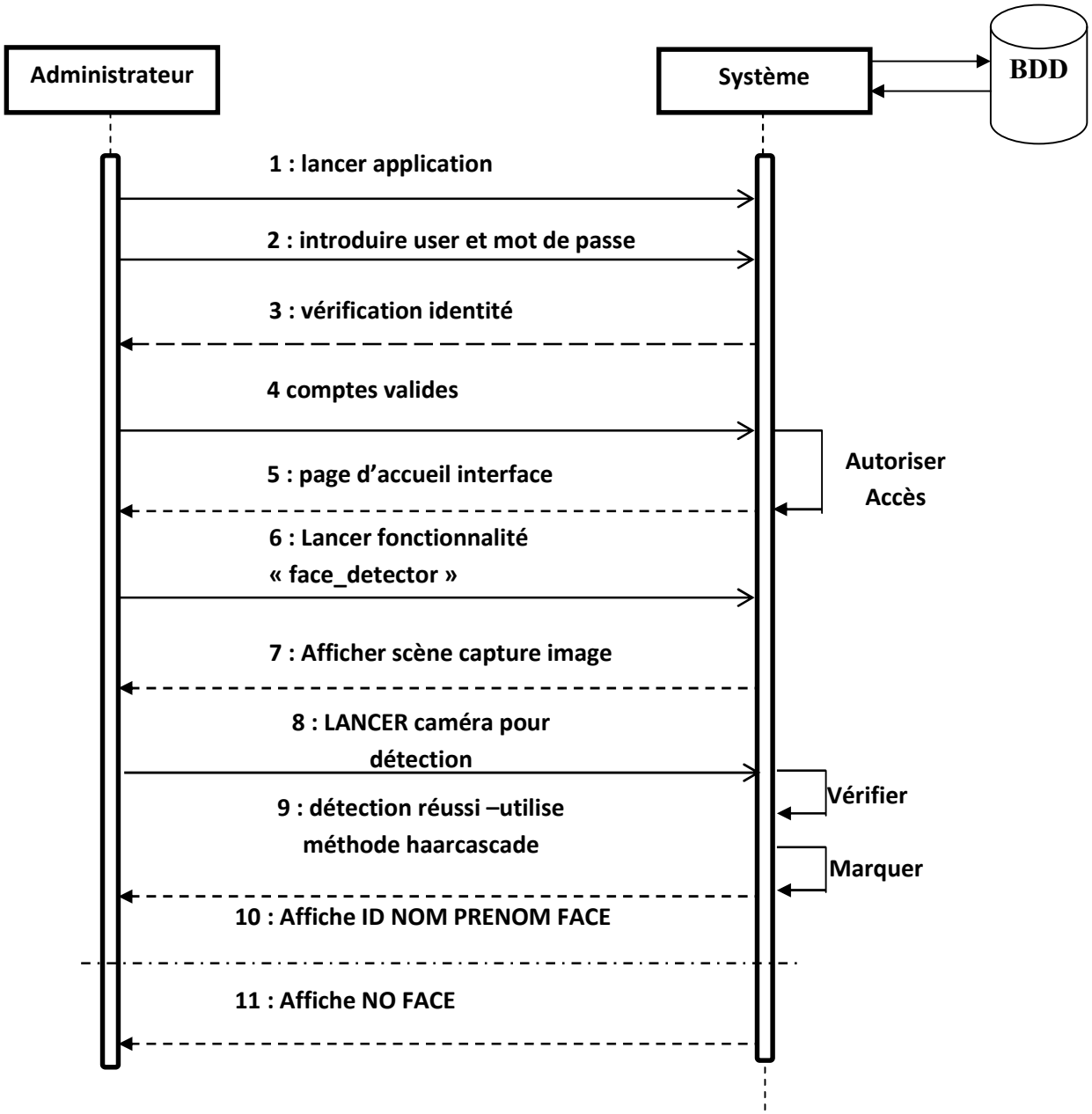




- Les cas d'utilisation CU entrainement des données (Train Data) et CU Gestion Etudiants (Stuent Panel) sont illustrés sur **Annexes 3 et 4** respectivement.

- Cas d'utilisation *:* **« Détection de visage »**

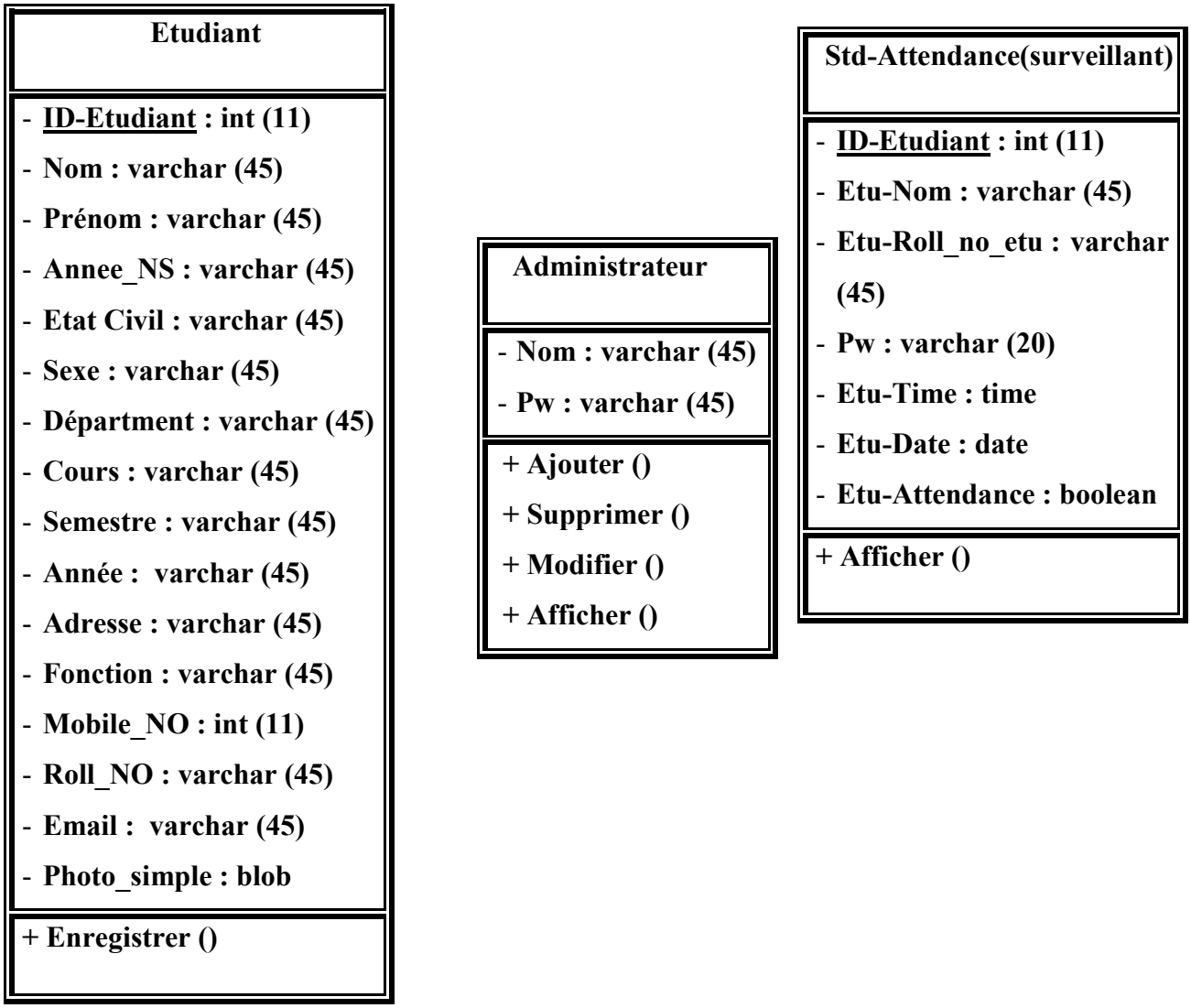
Figure (N° 10-III) : Diagramme séquence pour CU "détection de visage".



5 Identification des classes et des objets

A partir de diagramme de séquence, nous allons extraire les classes (ce sont les abstractions des objets métiers ou entités informationnelles liés aux domaines).

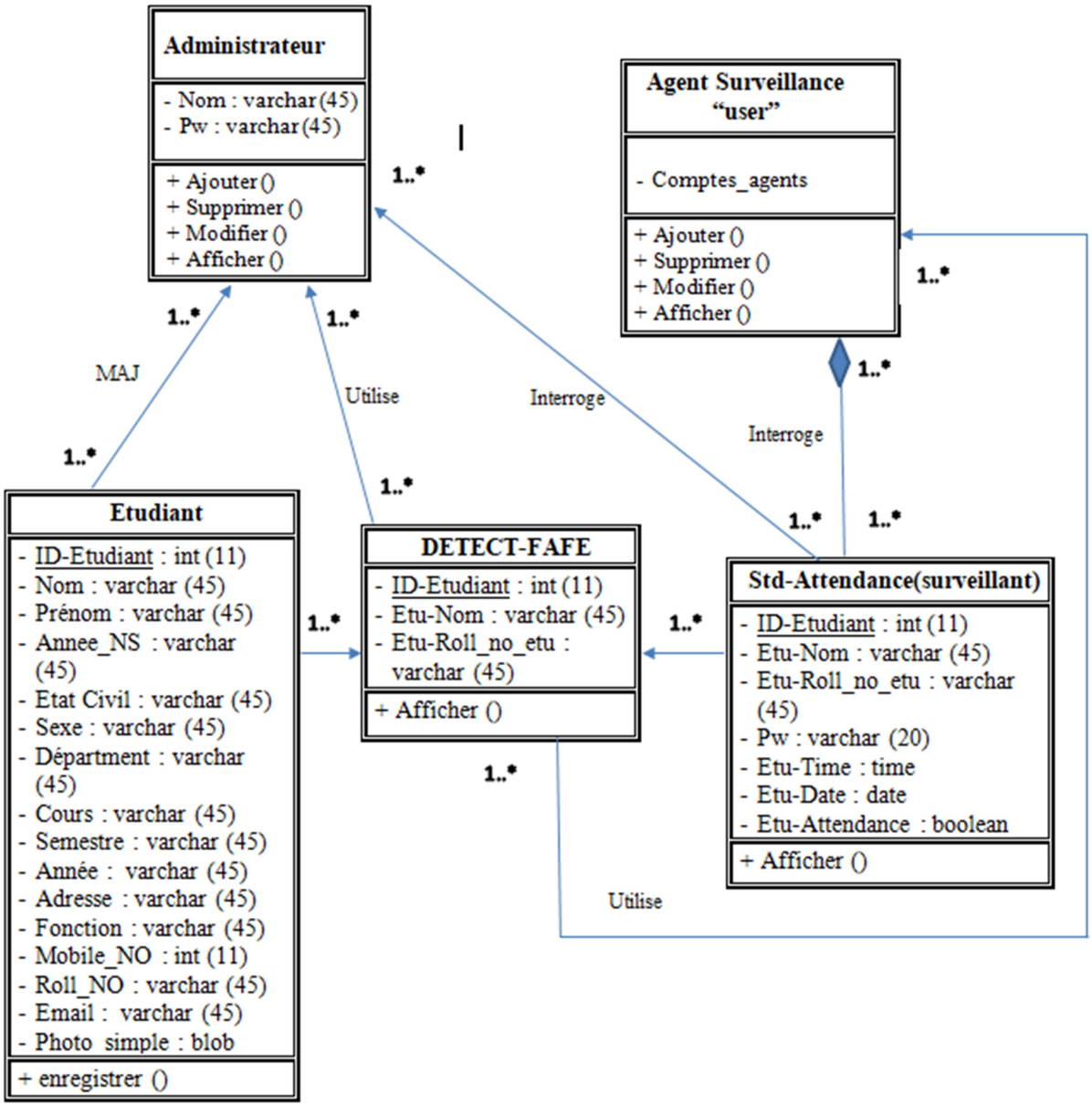
Dans ce dernier, nous allons détailler nos classes en ajoutant les attributs et les opérations (Méthodes). Voici des exemples de ses classes, nous avons choisi les classe Administrateur. Etudiant, et –Attendance-Etudiant.



6 Elaboration du diagramme de classe

Le diagramme de classe de notre application est présenté dans la figure 35 :

Figure (N° 11-III) : Diagramme de classe.


Administrateur
- Nom : varchar (45)
- Pw : varchar (45)
+ Ajouter ()
+ Supprimer ()
+ Modifier ()
+ Afficher ()
Agent Surveillance "user"
- Comptes_agents
+ Ajouter ()
+ Supprimer ()
+ Modifier ()
+ Afficher ()
Etudiant
- ID-Etudiant : int (11)
- Nom : varchar (45)
- Prénom : varchar (45)
- Annee_NS : varchar (45)
- Etat Civil : varchar (45)
- Sexe : varchar (45)
- Département : varchar (45)
- Cours : varchar (45)
- Semestre : varchar (45)
- Année : varchar (45)
- Adresse : varchar (45)
- Fonction : varchar (45)
- Mobile_NO : int (11)
- Roll_NO : varchar (45)
- Email : varchar (45)
- Photo_simple : blob
+ enregistrer ()
DETECT-FAFE
- ID-Etudiant : int (11)
- Etu-Nom : varchar (45)
- Etu-Roll_no_etu : varchar (45)
+ Afficher ()
Std-Attendance(surveillant)
- ID-Etudiant : int (11)
- Etu-Nom : varchar (45)
- Etu-Roll_no_etu : varchar (45)
- Pw : varchar (20)
- Etu-Time : time
- Etu-Date : date
- Etu-Attendance : boolean
+ Afficher ()
MAJ
Utilise
Interroge
Interroge
Utilise
1..*

7 Conclusion

Ce chapitre a été consacré à la présentation de notre conception en appliquant la démarche UP et les différents diagrammes UML vus nécessaires pour notre projet.

Dans le prochain chapitre, nous allons présenter les différents outils de développement employés pour l'implémentation de notre application.

Chapitre V

Implémentation du système

Chapitre IV : Implémentation du système

1 Introduction

Ce chapitre sera consacré à l'étude pratique qui consiste à implémenter d'un système de suivi des présences des étudiants, en temps réel, en abordons quelques généralités sur le langage de développement, les bibliothèques utilisés avec lesquels nous avons travaillés, ensuite nous justifierons le choix des outils utilisés et l'implémentation du programme avec évidemment une description de l'algorithme utilisé et en fin en va discuter les résultats obtenus avec une conclusion. Puis on donne quelques captures d'écrans de notre application démontrant les résultats obtenus.

2 Présentation du système

Le système développé est un système automatisé de gestion des présences s'appuie sur les différentes techniques de reconnaissance faciale (RF). Pour cela, nous avons décidés d'intégré impérativement une caméra (webcam) connecté avec le machine afin de capturer les photos nécessaires. Ensuite avec des algorithmes avancés tels que haarcascade et LBPH (Local Binary Patterns Histograms) pour la localisation des visages, le système va automatiquement procéder à un prétraitement des images en les convertissant en niveaux de gris, extraire les caractéristiques pertinentes, puis effectuer une analyse et une classification pour prendre une décision.

Pour notre système, nous avons choisi la méthode « **LBPHFaceRecognizer »**, un modèle algorithmique disponible dans la bibliothèque OpenCV. L'avantage de cet algorithme est sa capacité à tolérer les variations d'éclairage, de mise à l'échelle, de rotation et de translation, ce qui le rend robuste dans des conditions changeantes.

3 Configuration requise

La configuration requise pour implémenter notre système de reconnaissance faciale pour la surveillance de la fréquentation des élèves dépendra de plusieurs facteurs, notamment la taille de l'école, le nombre d'élèves à surveiller, les fonctionnalités spécifiques du système, et les exigences de performance. Cependant, voici une configuration de base recommandée :

3.1 Matériel :

- **Ordinateur :** Un ordinateur moderne avec un processeur multi-cœur (de préférence Intel Corei5 ou supérieur) et au moins 4 Go de RAM.
- **Caméras :** Des caméras haute résolution capables de capturer des images claires des visages des élèves. Les caméras IP ou les caméras de vidéosurveillance peuvent être utilisées en fonction des besoins spécifiques de l'école.

3.2 Logiciel :

- **Système d'exploitation :** Windows, Linux ou macOS, en fonction des préférences et de la compatibilité du logiciel de reconnaissance faciale choisi.
- **Bibliothèques logicielles :** Utilisation de bibliothèques de vision par ordinateur telles que OpenCV (Open Source Computer Vision Library) pour la détection et la reconnaissance faciale.
- **Environnement de développement :** Un environnement de développement intégré (IDE) tel que, Visual Studio Code ou Jupyter Notebook pour écrire et exécuter du code Python. MySQL Workbench.

  .

4 Logiciel et langage d'implémentation

4.1 Python :

Le logiciel utilisé pour le développement et l'implémentation est un aspect crucial de tout projet. Dans ce contexte, nous utilisons le langage de programmation Python, largement reconnu pour sa simplicité, sa polyvalence et sa richesse en bibliothèques et en frameworks. Python offre une syntaxe claire et concise qui permet de développer rapidement des solutions tout en maintenant un code facilement compréhensible et maintenable.

Nous avons choisi **Python Version .3.11.5** comme langage de programmation pour plusieurs raisons. Tout d'abord, sa popularité croissante dans le domaine de l'apprentissage automatique et de l'intelligence artificielle, en fait un choix idéal pour les projets de reconnaissance faciale. De plus, il dispose de nombreuses bibliothèques puissantes telles que **OpenCV**, Dlib et **Tkinter**, **Numpy**, et **mysql.connector** qui facilitent le développement d'applications de reconnaissance faciale avancées. En ce qui concerne l'environnement de travail, nous utilisons généralement des IDE (Environnements de Développement Intégré) tels que, **Visual Studio** Code ou Jupyter Notebook pour écrire, tester et déboguer notre code Python. Ces environnements offrent des fonctionnalités avancées telles que la coloration syntaxique, la complétion automatique, le débogage interactif et la gestion de projets, ce qui facilite le processus de développement [1].

4.2 OpenCV :

OpenCV (Open Computer Vision) est une bibliothèque graphique spécialisée dans le traitement d'image développée principalement en langage de programmation C++ avec des interfaces disponibles pour Python, Java et d'autres langages. Elle offre une multitude de fonctionnalités pour le traitement d'images, y compris la détection de visages, la reconnaissance d'objets, le suivi de mouvement, etc. OpenCV est largement utilisée dans l'industrie et la recherche pour une variété d'applications, y compris la reconnaissance faciale[2].

Figure (N° 01-V): OpenCV bibliothèque logo.

[1] DGUECHI Intissar « Biométrie d'empreinte digitale », mémoire de master, université de Carthage, Tunis, ISSAT Mateur ; institut supérieur des sciences appliquées et de technologie Mateur, p 13,2013.
[2] J.Smith, & Jones, A. : « Python Programming for Facial Recognition Applications » Journal of Computer Vision and Image Processing, Vol 10, N° 2, p 150-165, 2020.

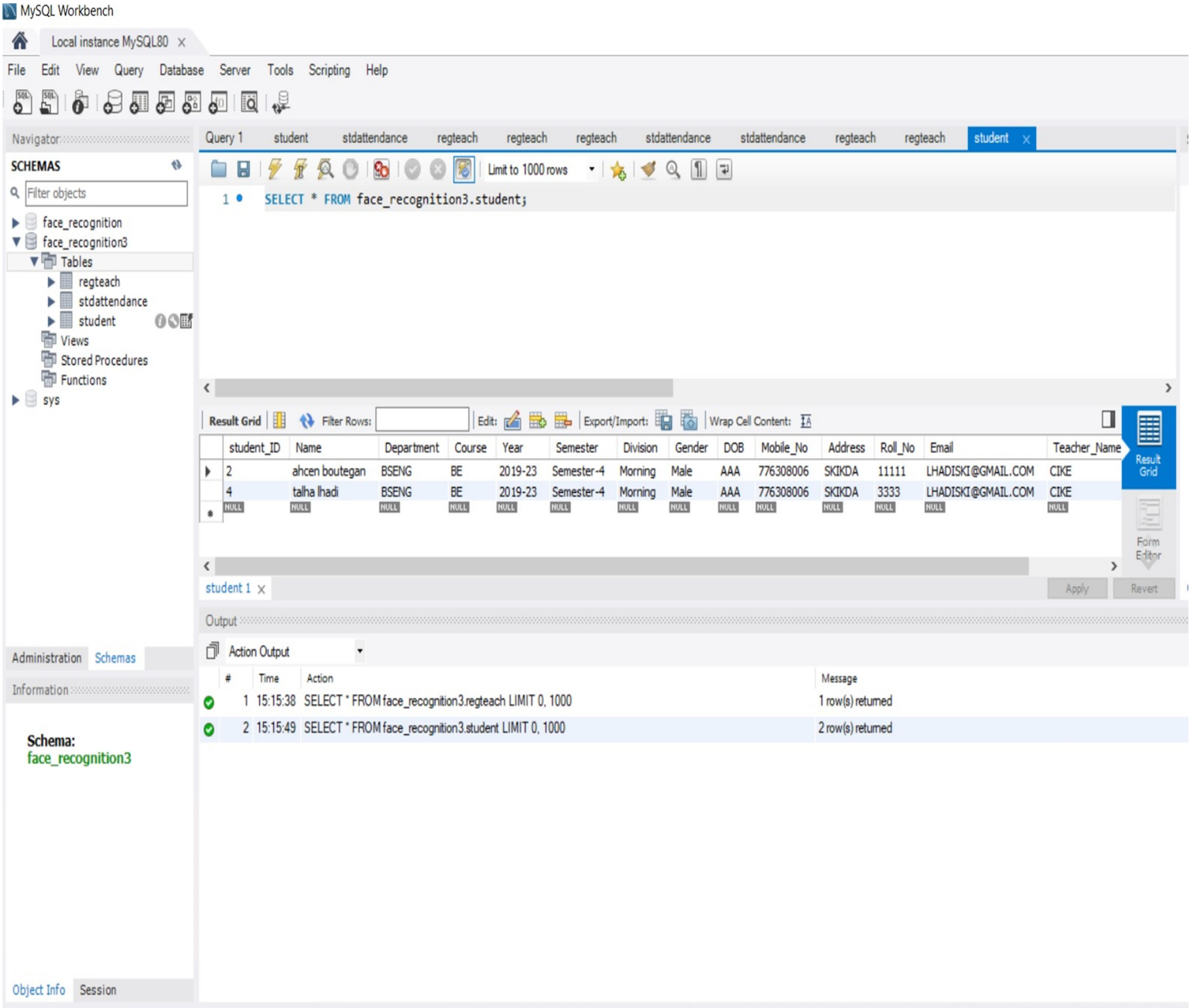
4.3 MySQL :

Pour gérer notre base de données, nous avons utilisés l'outil de gestion de bases de données relationnelles **MySQL Workbench,** et pour obtenir la version de MySQL Workbench 8.0 CE, on suivra les étapes suivantes :

1. On doit aller vers le site officiel de **MySQL** [1].
2. On Clique sur l'onglet "Téléchargements" dans la barre de navigation supérieure.
3. Dans la section "MySQL Workbench", on sélectionne notre système d'exploitation dans la liste déroulante.
4. Une fois la sélection effectuée, on verra une liste de téléchargements disponibles. Et on clique sur le lien de téléchargement correspondant à la version de MySQL Workbench 8.0 CE pour notre système d'exploitation.
5. On exécute le fichier d'installation et on suit les instructions d'installation de MySQL Workbench.

[1] Site officiel MySQL https://www.mysql.com.

Figure (N° 02-V) : Plateforme MySQL Workbench interface.

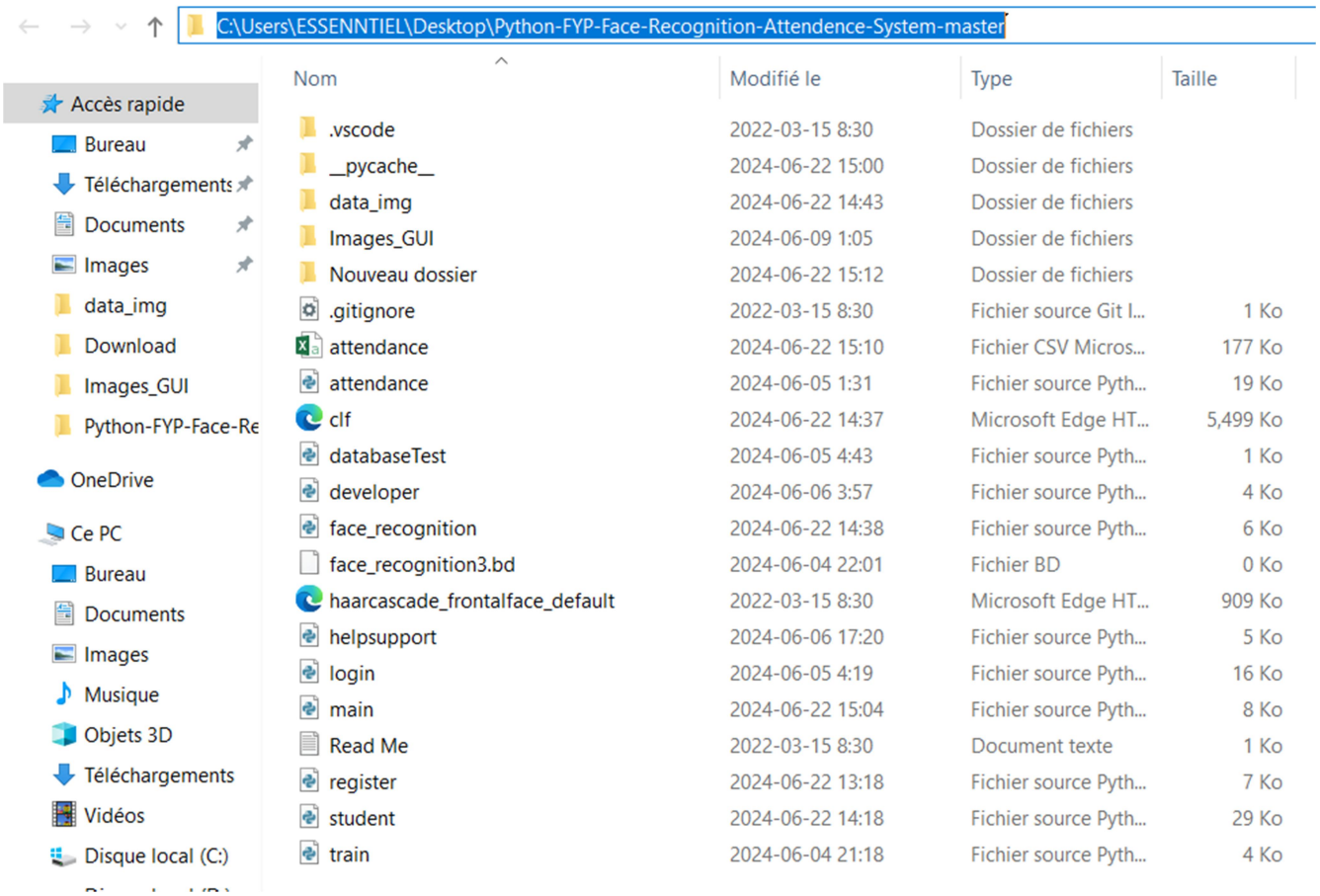


5 Création de la base de données :

Pour enregistrer la présence des étudiants, nous avons besoin d'une base de données contenant leurs photos faciales dont leurs informations seront enregistrées, pour pouvoir les utiliser par le système dans les traitements (nom, prénom, ID, etc.

- Après avoir pris les échantillons, le programme crée un dossier et y stocke les données.

Figure (N° 03-V) : Création de la base de données « chemin ».



Comme notre projet de vision par ordinateur repose sur la quantité de données disponibles, il est recommandé de capturer plusieurs photos de chaque élève dans diverses positions et conditions d'éclairage. Cela nous permettra d'extraire le maximum de données possible.

- **Entrainement de modèle de reconnaissance :**

a) détection visage(Haarcascade) :

La méthode de détection d'objets utilisant des classificateurs en cascade basée sur les caractéristiques Haar, est une approche efficace proposée par Paul Viola et Michael Jones dans leur article "Rapid Object Detection using a Boosted Cascade of Simple Features" en 2001. Cette méthode repose sur l'apprentissage automatique, où une fonction en cascade est

entrainée à partir d'un ensemble étendu d'images positives et négatives. Par la suite, elle est exploitée pour la détection d'objets dans d'autres images. Ici, nous allons nous occuper de la détection des visages. OpenCV contient déjà de nombreux classificateurs pré-entraînés pour les visages, les yeux, les sourires, etc. Ces fichiers XML sont disponibles en tant que fichiers open source. Pour ce projet nous utiliserons "**haarcascade_frontalface_default.xml".**

Afin de repérer les visages des individus déjà enregistrés dans la base de données, nous procédons d'abord à leur conversion en niveaux de gris. Ensuite, nous utilisons le modèle pré-entraîné de la Haar-cascade pour détecter les visages dans ces images converties. Voici un exemple illustrant la détection de visages à l'aide de la Haar-cascade.

Exemple :

Figure (N° 04-V) : Conversion d'une image en échelle de gris.

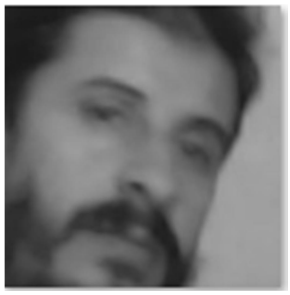
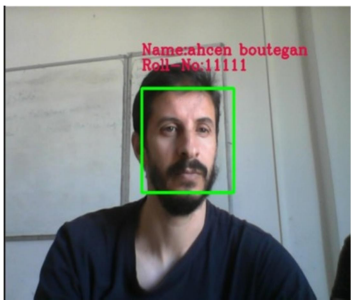


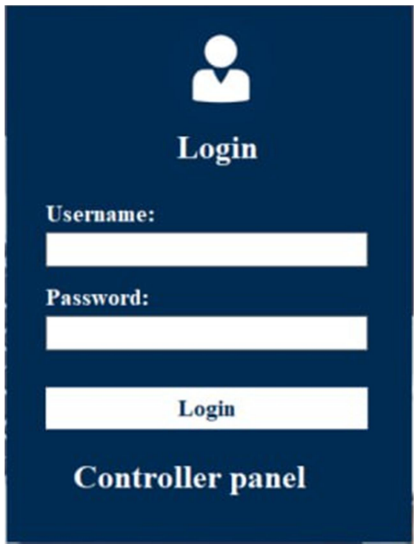
Figure (N° 05-V) : Détection des visages via « Haar-cascade ».



6 Présentation de l'application :

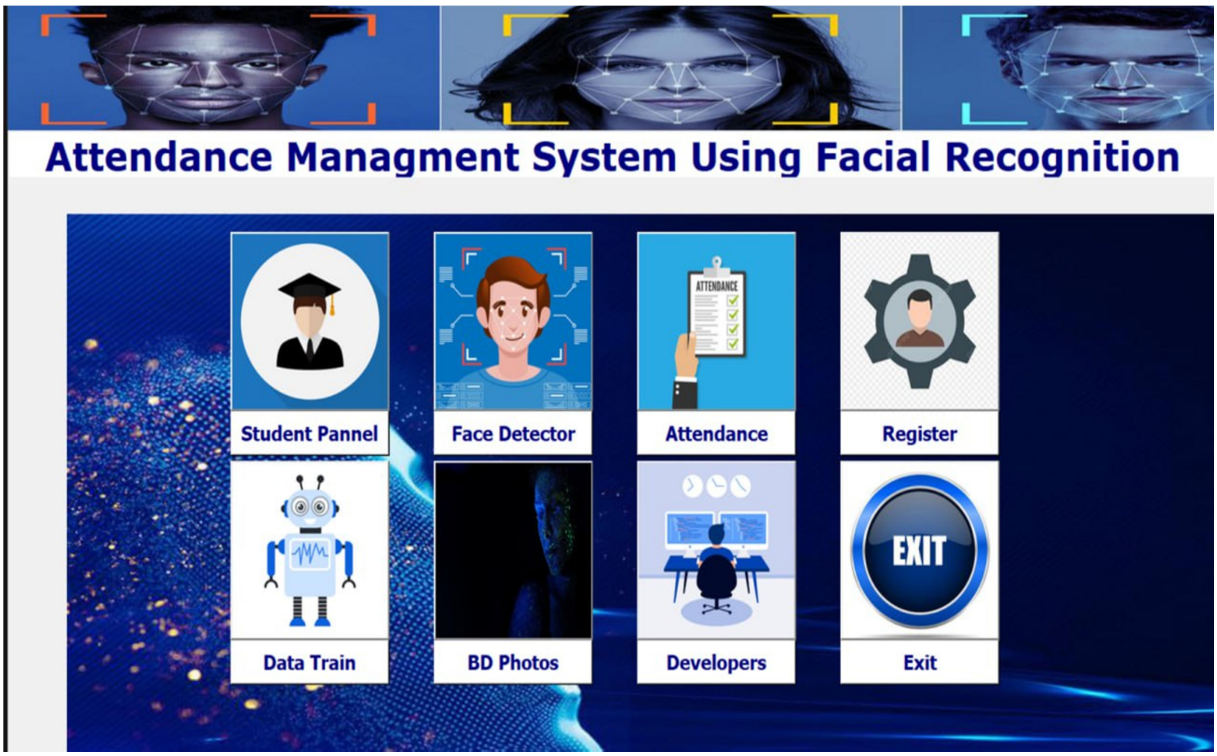
La première action est l'identification dès que l'application est lancée « **Authentification** ».

Figure (N°06- IV) : demande d'Authentification.



6.1 Interface principale de l'application

Figure (N° 07-V) : Interface principale de l'Application.



Cette interface s'affichera après introduction d'un nom d'utilisateur et de son mot de passe (Administrateur de gestion de système) qui doivent être valide, sinon vous ne serez plus autoriser d'y accédée. Dont, la capture d'écran montrée en ci-dessous représente la page d'accueil de notre application. Cette interface facilite la manipulation fluide des fonctionnalités principales de notre programme, et offrant une illustration claire des processus clés.

6.2 Etape et processus d'exécution du système de détection faciale :

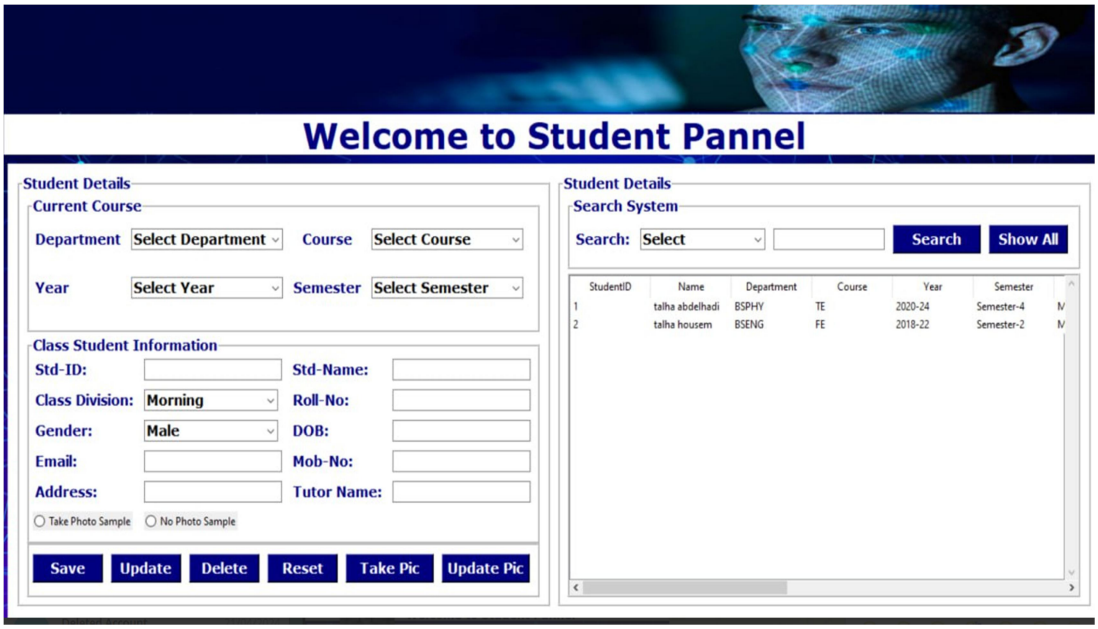
BASE DE DONNEES : une base connecté avec **MySQL** Connecteur où se trouvant toutes les photos capturées évidemment bien sur les informations saisies de nos étudiants.

CREATION COMPTE SURVEILLANCE :

Figure (N° 08-V) : Création compte Agent surveillance.

STUDENT PANNEL : vous donner la possibilité d'intégrer la liste de tous les étudiant appartenons à un établissement spécifique, y compris de leurs cordonnées personnels et scolaires (nom, prénom, code, département, spécialité, niveau, adresse, etc).

Figure (N° 09-V) : Sous-interface gestion étudiant.

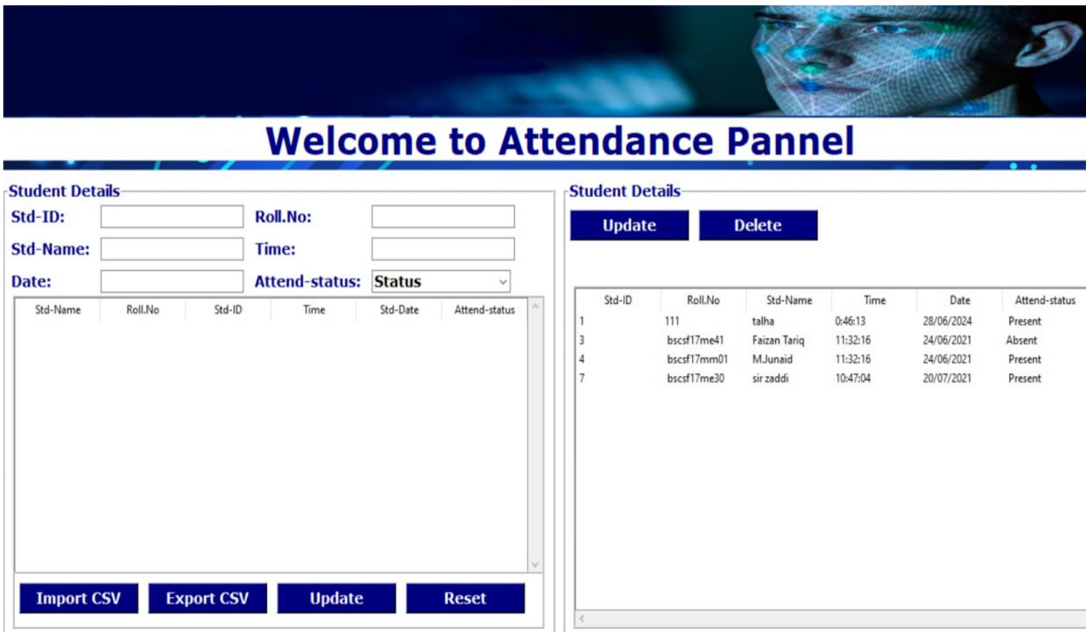


ATTENDANCE : pour contrôler et générer l'état de présence servant pour exploitation administrative (fichiers CSV, Excel).

Figure (N° 10-V) : Sous-interface surveillance.

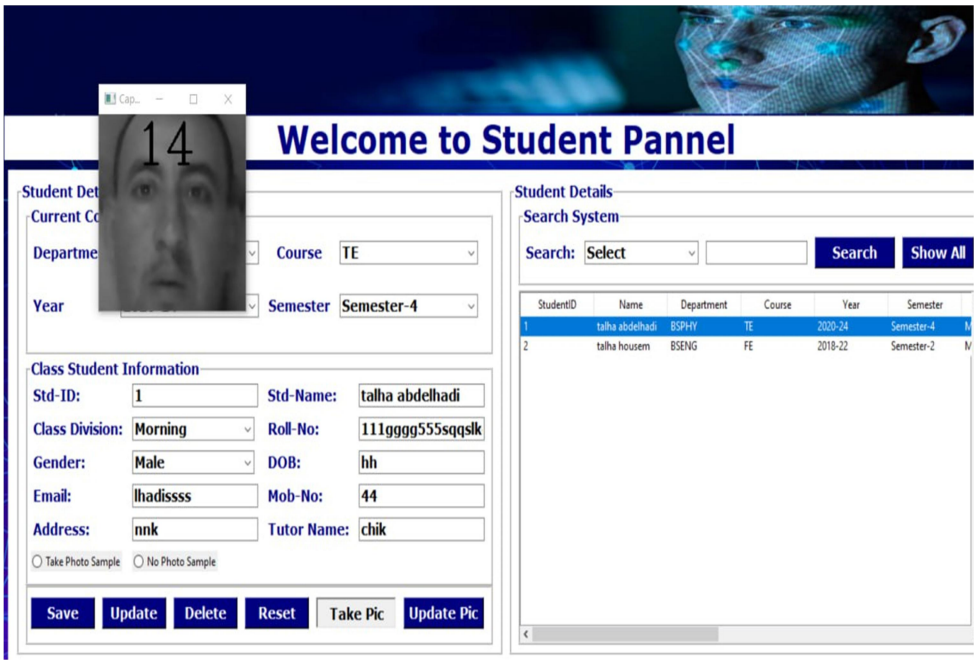
A la fin du processus, l'agent surveillant peut voir l'état de présence de tous les étudiants enregistrés sur la base de données après importation du fichier présence « Attendance ».

Figure (N° 11-V) : Affichage état de présence.



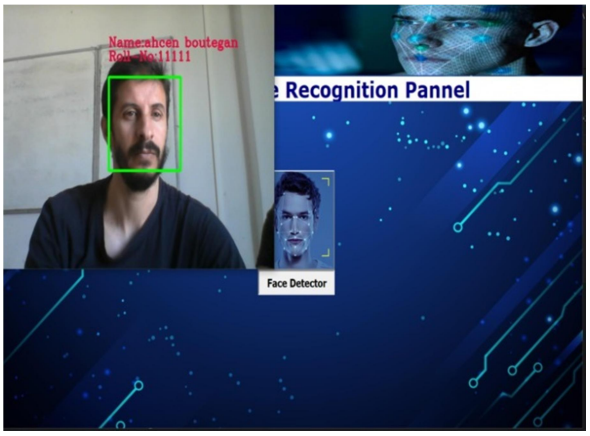
FACE DETECTOR : Pour acquérir la vidéo à partir de la caméra l'utilisateur lance la capture en cliquant sur la fonctionnalité **Face_detector.** Dans la mésure à entrainer par la suite.

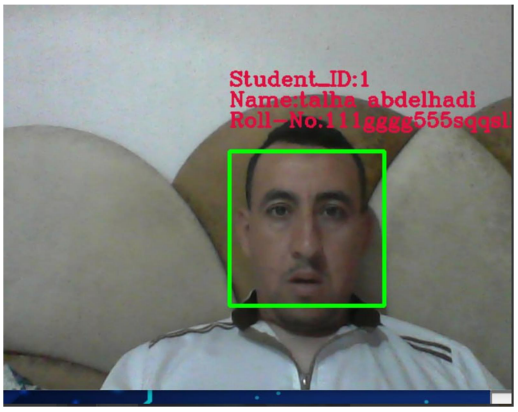
Figure (N° 12-V) : Lancement de la scène vidéo.



L'étudiant doit se devons se présenter devant la caméra à l'entrée pour pouvoir tester si le système reconnaitre la personne ou non, on a fait des essais, qui serons couronnées avec succès sur un taux de confiance de plus **77%.**

Figure (N° 13-V) : Détection et reconnaissance de visage.





TRAINDATA : dans cette fonctionnalité l'entrainement du modèle aux données par le classifieur Haarcacade, on doit faire des captures de plus de **30 photos** dans toute les positons et orientations afin faciliter la détection et la reconnaissance.

Figure (N° 14-V) : Sous-interface entrainement des données.

Tout d'abord, l'administrateur système (surveillant) doit cliquer sur le la fonctionnalité **TrainData** pour commencer le processus de détection.

Figure (N° 15-V) : Captures normalisées en « Haarcascade » avec plusieurs positons.

Initialisation du Classifieur :

Comme mentionné précédemment, la première étape de la reconnaissance des visages consiste à détecter les visages. Grâce à la bibliothèque OpenCV, il est relativement simple d'effectuer cette détection en utilisant le détecteur de visage Haar Cascade, également connu sous le nom de méthode de Viola-Jones. Ainsi, pour démarrer la détection.

Dans notre cas, nous avons choisi d'utiliser le fichier **haarcascade_frontalface_alt.xml** comme classifieur Haar Cascade provenant d'OpenCV.

```
@FXML
protected void haarSelected(Event event)
{
        faceDetect.setClassifier("haar/haarcascade_frontalface_alt.xml");
        cameraActive= true;
        // now the video capture can start
        startCam.setDisable(false);
}
```

Avant la détection d'un visage, Il est important d'appliquer diverses techniques de prétraitement d'images afin de normaliser les images que nous soumettons à notre système de reconnaissance faciale,

Tout d'abord :

- Rendre toutes les images en niveaux de gris :

```
grayImage = cvCreateImage(cvGetSize(grabbedImage), 8, 1);


cvCvtColor(grabbedImage, grayImage, CV_BGR2GRAY);
```

❖ Rendre toutes les images en même dimension :

```
smallImage = cvCreateImage(cvSize(grabbedImage.width() / 4, grabbedImage.height() / 4), 8, 1

cvResize(grayImage, smallImage, CV_INTER_AREA);
```

DEVELOPPERS : où vous vous aurez accès aux renseignements des développeurs de l'application.

Figure (N° 16-V) : Sous-interface développeurs.

SUPPORT ET HELP : lorsqu'on clique à celle-là, me système va systématiquement vous redirige vers une page d'assistance à propos de l'application ainsi, **où** on pourra contacter les développeurs par exemple (email, page Facebook, Youtube Chanel..).

Exit : il vous propose de quitter l'application et sortir du système.

6.3 Avantage du nouveau système :

➢ Le calcul du taux d'absentéisme est plus simple et plus précis ; tous les calculs sont effectués par ordinateur plutôt que manuellement.

- Il n'y aura aucune paperasse impliquée ; tous les processus sont effectués par ordinateur. Cela aidera à nous protéger contre la perte de données.
- Les processus informatisés seront exécutés plus rapidement et avec plus de précision que le système classique.
- Le système proposé supprime le tableau d'affichage. Les taux d'absentéisme peuvent être consultés à chaque instant facilement via l'application.
- Toutes les données sont enregistrées sur une de base de données scolaire et sur une feuille Excel. Cela permettra une surveillance facile des données.

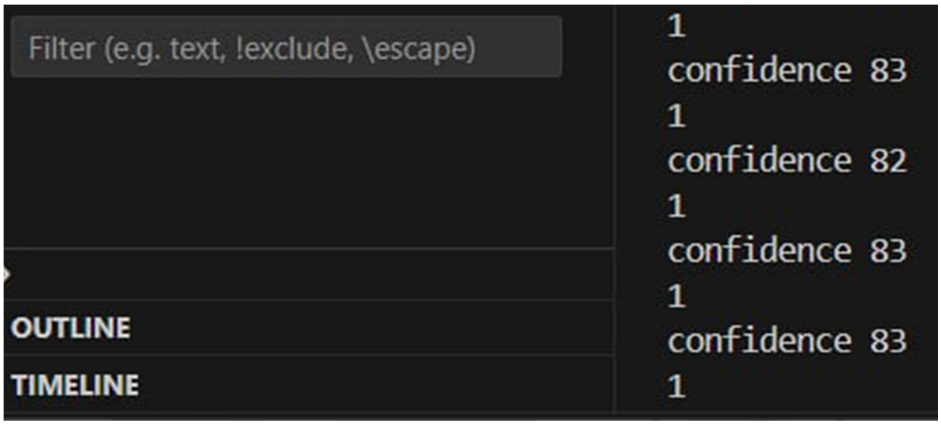
7 Résultat et Discussions :

7.1 Résultats :

Précision et Fiabilité du Système :

Le système de reconnaissance faciale développé a été testé dans un environnement scolaire simulé. Les résultats montrent une précision de reconnaissance de **83 %**, dépassant ainsi le seuil minimal de **77 %** que nous avions fixé. Le système a été capable d'identifier correctement les élèves dans la majorité des cas, avec un faible taux de fausses reconnaissances. Les résultats obtenus après un test dans la figure (à prendre en compte l'éclairage et luminosité).

Figure (N° 17-V) : Affichage taux de confiance après exécution.



Temps d'exécution :

Le temps moyen de traitement par image s'est avéré être de 2 seconde, ce qui est acceptable pour une utilisation en temps réel. Cela permet une intégration fluide dans les routines quotidiennes des écoles sans perturber le déroulement des classes.

7.2 Discussions :

Des entretiens et des questionnaires ont été menés auprès des élèves et des enseignants pour recueillir leurs impressions sur l'utilisation du système. La majorité des utilisateurs ont exprimé une satisfaction quant à la facilité d'utilisation et à la rapidité du système. Cependant, quelques préoccupations ont été soulevées concernant la confidentialité des données personnelles.

Comparaison avec les Attentes Initiales :

Les résultats obtenus dépassent les attentes initiales en termes de précision et de temps de d'exécution. Cela démontre la viabilité technique de la reconnaissance faciale pour la gestion de la présence des élèves. Toutefois, il est important de noter que ces résultats ont été obtenus dans des conditions contrôlées et qu'une évaluation continue dans des conditions réelles est nécessaire.

Limites du système :

Quelques limitations ont été identifiées à savoir :

- La sensibilité aux changements d'éclairage : Le système a montré une diminution de précision en cas de variations importantes de lumière.
- La Diversité des expressions faciales : Certaines expressions faciales non prévues dans la phase d'apprentissage ont causé des erreurs de reconnaissance.
- Besoin d'une base de données à jour : Le système nécessite une mise à jour régulière des données pour maintenir sa précision.

Recommandations

Pour améliorer le système, plusieurs pistes peuvent être envisagées :

- Utilisation de réseaux de neurones plus avancés pour accroître la robustesse face aux variations d'éclairage et d'expressions faciales.
- Intégration de méthodes de cryptage pour sécuriser les données biométriques.
- Sensibilisation et formation des parties prenantes pour renforcer la confiance et l'acceptation du système.

8 Conclusion

Nous sommes parvenus à développer un système de reconnaissance faciale qui permet d'effectuer des traitements sur un visage identifié et de le comparer aux visages préalablement définis dans notre base d'apprentissage. Ce système utilise les techniques de Haarcascade et de l'algorithme LBPH. Ce qui le distingue, c'est sa capacité à gérer les variations d'éclairage, de mise à l'échelle, de rotation et de translation, ce qui lui confère une robustesse dans des environnements changeants. Il est par conséquent, en comparant nos résultats à ceux obtenus par le système classique, nous pouvons confirmer que notre système donne des résultats satisfaisants.

Conclusion Générale

Conclusion générale

La reconnaissance faciale, en tant que technologie émergente, offre des perspectives intéressantes pour les établissements scolaires, notamment dans la gestion de la présence des élèves. Au cours de ce mémoire, nous avons abordé les différentes facettes de cette technologie, de son fonctionnement à son implémentation pratique, en passant par les défis qu'elle pose.

Notre étude a révélé que la reconnaissance faciale peut améliorer significativement l'efficacité administrative des écoles en automatisant la gestion de la présence des élèves. Le système que nous avons développé a montré des résultats remarquables en termes de précision et de fiabilité, avec un taux de reconnaissance satisfaisant qui répond aux exigences opérationnelles.

Cependant, l'adoption de la reconnaissance faciale dans un contexte scolaire peut poser des défis importants. A propos de la protection de la vie privée, à la sécurité des données. Il est impératif que les établissements qui souhaitent utiliser cette technologie mettent en place des mesures strictes pour garantir la confidentialité et la sécurité des informations des élèves.

Pour améliorer et favoriser l'acceptation de la reconnaissance faciale en milieu scolaire, plusieurs pistes peuvent être envisagées. L'intégration de techniques d'intelligence artificielle plus avancées pourrait augmenter la précision et l'efficacité des systèmes de reconnaissance faciale. Par ailleurs, une collaboration étroite avec toutes les parties prenantes : élèves, parents, enseignants et administrateurs est indispensable pour élaborer des politiques claires et transparentes concernant l'utilisation de ces technologies.

Pour améliorer le système, plusieurs recommandations peuvent être envisagées :

- L’utilisation de réseaux de neurones plus avancés pour accroître la robustesse face aux variations d'éclairage et d'expressions faciales.
- L’intégration de méthodes de cryptage pour sécuriser les données biométriques.
- La sensibilisation et la formation des parties prenantes pour renforcer la confiance et l'acceptation du système.

En conclusion, bien que la reconnaissance faciale représente une avancée technologique encourageante pour les établissements scolaires, son implémentation doit être menée avec

prudence et responsabilité. Les bénéfices potentiels en termes de gestion administrative et de sécurité doivent être équilibrés avec les impératifs de respect de la confidentialité.

Bibliographie

Bibliographie

[1] Nicolas MORIZET, « Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris », Thèse de doctorat, École Doctorale d'Informatique, Télécommunications et Électronique de Paris, France, p 32,2009.

[2] https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_reconnaissance_faciale.

[3] https://intelligence-artificielle.com.

[4] https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_reconnaissance_facial.

[5] recueillis sur Présentation cours chapitre 1 « introduction aux systèmes de Reconnaissance de visgae, dr CHEIKH Ramdane Université 20 Août 1955 – Skikda 2024.

[6] https://www.caducee.net/DossierSpecialises/systeme-information-sante/dmi.asp.

[7] X. Tan, S. Chen, Z.-H. Zhou, and F. Zhang, "Face recognition from a single image per Person : A survey," Pattern recognition, vol. 39(9), pp. 1725-1745, 2006.

[8] Francis CHARETTE MIGNEAULT rapport de projet Conception De Système De Reconnaissance De Visages Spatio-Temporelle Sur Vidéos A Partir D'une Seule Image De Référence Ecole De Technologie Supérieure Université Du Québec P57 Montréal, 2017.

[9] AKCHA Ikram & AMARI Amira Mémoire de master « Développement d'un système de reconnaissance faciale», Université Saad Dahleb De Blida, p20, 2020.

[10] ASSADI NADJETTE « Mise au point d'une application de reconnaissance faciale », Mémoire de master en informatique, Université Mohamed Khider – BISKRA, 2017-2018» -

[11] Samia Mekkani: «Reconnaissance de visage», Mémoire de licence, Université Larbi Ben M'hidi Oum El Bouaghi, Juin 2014.

[12] Mebarka Belahcen: «Authentification et identification en biométrie ». Thèse de doctorat, Université Mohamed khider Biskra, 2013.

[13] Article The Pros and Cons of Facial Recognition Technology" - Security Magazine 2020, https://www.securitymagazine.com/articles/91847-cybersecurity-response-to-the-california-consumer-privacy-act.

[14] opcit.

[15] P.Buyssens « Fusion de différents modes de capture pour la reconnaissance du visage appliquée aux transactions » Université de Caen-2011.

[16] M.Chihaoui, A.Elkefi, W.Bellil and C.Ben Amar « A Survey of 2D Face Recognition Techniques » University of Sfax, National School of Engineers (ENIS) -2016.

[17] H.Hoffmann « Kernel PCA for novelty detection » Pattern Recognit-2007.

[18] N.Vladimir « The Nature of Statistical Learning Theory » New York, NY, USA-1995

[19] F.Bach, M.Jordan « Kernel independent component analysis » Learn. Res-2002

[20] Y.Hu « Learning a locality preserving subspace for visual recognition ». In Proceedings of the 9th IEEE International Conference on Computer Vision, Nice, France, 13–16 October-2003.

[21] Bouzit Dhikra, « Reconnaissance de visage basée sur une approche triangulaire », Mémoire de master, Université de 8 Mai 1945 – Guelma -,2019

[22] AKCHA Ikram et ammari amira ; Université De Blida 1 – Saad Dahleb, Mémoire de master Développement d'un système de reconnaissance facial, PAGE 27, 2020.

[23] O. Déniz, G. Bueno, J. Salido, and F. De la Torre « Face recognition using Histograms of Oriented Gradients » Pattern Recognition Letters - 2011

[24] AKCHA Ikram et Ammari amira, « Développement d'un système de reconnaissance faciale », mémoire de master, Université De Blida 1 – Saad Dahleb, PAGE 27, 2020

[25] M.Chihaoui, A.Elkefi, W.Bellil and C.Ben Amar « A Survey of 2D Face Recognition Techniques » University of Sfax, National School of Engineers (ENIS) -2016.

[26] Yang, M., & Yang, J. Réseaux neuronaux convolutifs profonds pour la reconnaissance faciale avec des représentations convolutives compressées, dans les actes de la conférence IEEE sur la vision par ordinateur et la reconnaissance de formes ,p 2470-2479, 2018.

[27] Mme Nefissa Khiari-Hili, « Biométrie multimodale basée sur l'iris et le visage », Ecole nationale d'ingénieurs de Tunis Et L'université Paris-Saclay préparée à l'Université d'Evry Val d'Essonne, Thèse doctorale, Evry, France 2016.

[28] Meramria Nabila : «Reconnaissance de visages par Analyse Discriminante Linéaire(LDA)», Mémoire de master, Université Badji Mokhtar Annaba, 2016.

[29] Editeur : Université de « North Alabama Digital Press », un guide pratique pour les éducateurs : « Sécurité et sûreté dans les écoles primaires et secondaires», « Violence scolaire et prévention primaire», septembre 2023.

[30] Paul Timm, « Sécurité dans les établissements scolaires du primaire et du secondaire » : Guide pratique pour les éducateurs, pages 25- 40. Publié en 2018,

[31] Amir BENZAOUI, « Identification Biométrique par Descripteurs de Texture Locaux : Application au Visage & Oreille », thèse de doctorat Université 08 Mai 1945 – Guelma page 22,2015.

[32] https://fr.wikipedia.org/wiki/Biom%C3%A9trie.

[33] Jain, A. K., Ross, A., & Nandakumar, K. « Introduction to Biometrics »,2016.

[34] Ratha, N. K., Connell, J. H., & Bolle, R. M, « Enhancing security and privacy in biometrics-based authentication systems », 200.

[35] Rattani, A., & Cavoukian, A, « Biometric Encryptions : A Positive-Sum Technology That Achieves Strong Authentication, Security AND Privacy ». Springer, 2016.

[36] Haghighat, M., Zonouz, S. A., & Abdel-Mottaleb, M .CloudID: « Trustworthy cloud-based and cross-enterprise biometric identification ». Expert Systems with Applications, p 63, 255-264, 2016.

[37] Rathgeb, C., & Busch, C. « How biometric system interoperability enables identity management applications », IEEE Security & Privacy, 16(1), p 60-67, 2018.

[38] Sain, A. K., Ross, A., & Nandakumar, K, « Introduction to Biometrics »,2016.

[39] Kim, H., & Hong, S. « Development of a biometric identification system based on image processing », 2018.

[40] Turk, M., & Pentland, A. Face recognition using eigenfaces, 1991.

[41] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S, « Handbook of fingerprint recognition ». Springer Science & Business Media. 2009.

[42] Jain, A. K., Ross, A., & Nandakumar, K, « Introduction to Biometrics ». Springer, 2016.

[43] Jain, A. K., Ross, A., & Nandakumar, K., « Introduction to Biometrics ». Springer, 2016

[44] Ratha, N. K., Connell, J. H., & Bolle, R. M, « Enhancing security and privacy in biometrics-based authentication systems ». IBM Systems Journal, 40(3), p 614-634, 2001.

[45] N.Morizet. « Reconnaissance biométrique par fusion multimodale du visage et de l'iris ». Thèse Doctorat. École doctorale d'informatique, télécommunication et électronique de paris, France. 2009.

[46] Jain 2007.

[47] Mme Nefissa KHIARI-HILI, « Biométrie multimodale basée sur l'iris et le visage », Ecole Nationale D'ingénieurs De Tunis et Evry Essone paris, Thèse De doctorat mai 2016. https://www.biblio.univ-evry.fr/theses/2016/2016SACLE014.pdf

[48] AIT AMIRAT Sofiane, MERZOUG Ziane, « Développement d'un système biométrique pour la reconnaissance de visages basé sur les ondelettes et une combinaison de deux types de réseaux neuronaux », Thèse de master université de Tizi-Ozou, p 37,2017-2018.

[49] Article The Ethics of Biometrics" by Simone Gaskell.

[50] AIT AMIRAT Sofiane, MERZOUG Ziane, « Développement d'un système biométrique pour la reconnaissance de visages basé sur les ondelettes et une combinaison de deux types de réseaux neuronaux », Thèse de master université de Tizi-Ozou, p 24,2017-2018.

[51] op.cit.

[52] M.Bellili & M.FARSI. «Application de la DCT modifiée et GMM Orthogonale pour la Vérification du visage ». Mémoire pour l'obtention du diplôme d'ingénieur d'état en informatique. ESI, Algérie. 2012.

[53] [Jain, A. K., Ross, A., & Nandakumar, K. (). « Introduction to Biometrics ». Springer, 2016.

[54] Li, S. Z., & Jain, A. K. (). « Handbook of Face Recognition ». Springer, 2011.

[55] Daugman, J. G. (). « How Iris Recognition Works ». IEEE Transactions on Circuits and Systems for Video Technology, 14(1), p 21-30, 2004.

[56] Huang, Z., & Acero, A. (). « Spoken Language Processing: A Guide to Theory, Algorithm and System Development ». Prentice Hall, 2001.

[57] Wildes, R. P. (). « Iris Recognition : An Emerging Biometric Technology. Proceedings of the IEEE », 85(9), p 1348-1363, 1997.

[58] Plamondon, R., & Srihari, S. N. (). « Online and Off-line Handwriting Recognition : A Comprehensive Survey ». IEEE Transactions on Pattern Analysis and Machine Intelligence, 22(1), p 63-84, 2000.

[59] DGUECHI Intissar « Biométrie d'empreinte digitale », mémoire de master, université de Carthage, Tunis, ISSAT Mateur ; institut supérieur des sciences appliquées et de technologie Mateur, p 13,2013.

[60] J.Smith, & Jones, A. : « Python Programming for Facial Recognition Applications » Journal of Computer Vision and Image Processing, Vol 10, N° 2, p 150-165, 2020.

[61] Site officiel MySQL https://www.mysql.com.

Table des Matières

Annexes

Annexe N°01 : les approches traditionnelles utilisées par les écoles.

Approches utilisées par les écoles	description	fonctionnement	avantages	limites
Liste de présence manuelle	Les enseignants utilisent des listes de présence papier pour enregistrer manuellement la présence des élèves en classe	Les élèves sont identifiés par leur nom et leur présence est cochée à la main à chaque cours.	Facile à mettre en œuvre, ne nécessite pas de matériel technologique spécial	Sujette aux erreurs humaines, peut être chronophage, difficile à gérer pour les classes nombreuses.
Appels téléphoniques aux parents	Les enseignants ou le personnel administratif appellent les parents des élèves absents pour vérifier les raisons de leur absence.	Les enseignants contactent les parents par téléphone ou par d'autres moyens de communication pour obtenir des informations sur l'absence de l'élève.	Permet de recueillir des informations sur les raisons de l'absence, peut encourager les parents à surveiller la présence de leur enfant.	Chronophage, dépendant de la coopération des parents, peut ne pas être efficace pour les élèves dont les parents ne sont pas disponibles ou ne répondent pas.
Systèmes de gestion de l'information scolaire (SGI)	Les écoles utilisent des logiciels de gestion de l'information scolaire pour suivre et gérer les données de fréquentation des élèves.	Les enseignants ou le personnel administratif saisissent les données de présence des élèves dans le SGI, où elles sont stockées et traitées.	Permet une collecte et une gestion centralisées des données de présence, peut générer des rapports et des analyses.	Nécessite une formation pour l'utilisation du logiciel, peut être coûteux à mettre en place et à entretenir, peut être limité dans sa capacité à fournir une surveillance en temps réel.
Méthodes de suivi basées sur les cartes d'identité ou les badges	Les élèves utilisent des cartes d'identité ou des badges magnétiques pour enregistrer leur présence à l'école ou en classe.	Les élèves scannent leur carte ou leur badge à un point de contrôle à l'entrée de l'école ou de la classe pour enregistrer leur présence.	Peut fournir une méthode automatisée et précise de suivi de la présence, peut être intégré à d'autres systèmes de gestion.	Nécessite une infrastructure matérielle et logicielle, peut être coûteux à mettre en place, peut soulever des préoccupations concernant la confidentialité et la vie privée.

Annexe N°02 : Les différentes techniques biométriques

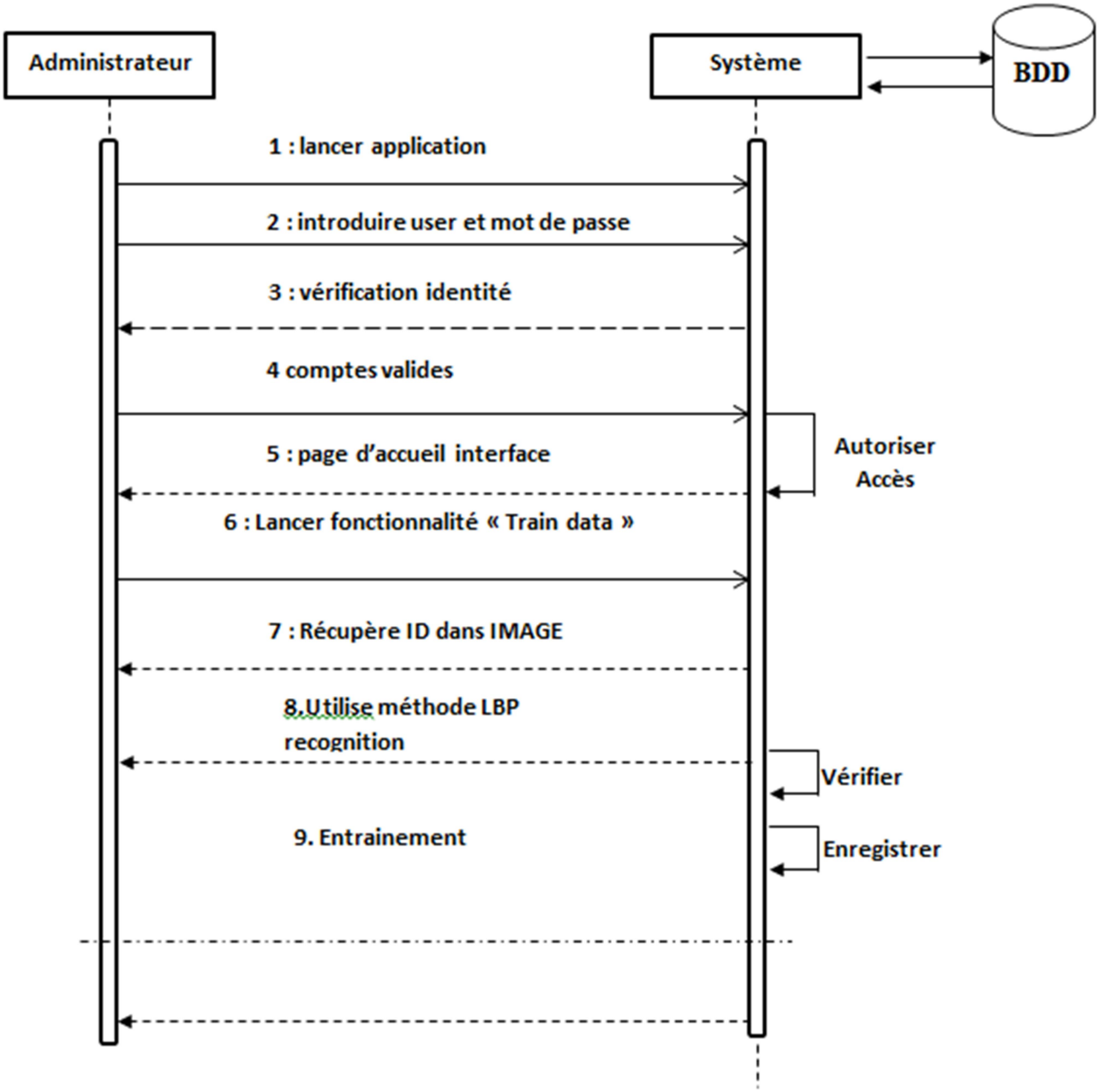
Eléments analysé	Description	Avantages	Inconvénients
ADN	Analyse du patrimoine Génétique	L'ADN est facile à obtenir (cheveux, salive)	Couteux et long
Démarche	Identification des mouvements	Transparente pour l'utilisateur	Technique encore au stade expérimentale
Dessin digitale	Analyse de l'empreinte digitale	Technique éprouvée et rapide	Des doigts sales ou abime peuvent affecter la lecture
Empreinte palmaire	Analyse de la géométrie de la main	Simple à utiliser	Capteur encombrant et cher
Empreinte thermographique	Cartographie thermique du visage	Faible te d'usage aisé	Technique encore au stade expérimentale
Iris	Analyse du motif de l'iris	Fiable	Acquisition contraignante
Rétine	Analyse de la cartographie des vaisseaux	Fiable	Acquisition contraignante
Signature	Analyse de la pression et de la vitesse d'exécution	Rapide	Peu fiable
Visage	Analyse morphologique du visage	Usage aisé	Doit tenir compte des changements tels une barbe ou des lunettes
voix	Analyse fréquentielle de la voix	Technique simple et peu couteuse	La voix change facilement

Source : *DGUECHI intissar « Biométrie d'empreinte digitale », mémoire de master, université de carthage, tunis, ISSAT Mateur ; institut supérieur des sciences appliquées et de technologie Mateur, p 13,2013*

Annexe N°03 : cas d'utilisation Entrainement des données « Train data »

Entrainement des données **« Train data »**
Ce cas d'utilisation permet au système d'entrainer les donées au modèle
Le système
Début : • Faire Introduire le user et le mot de passe • Le système vérifier la validité d'authentification. **En cours :** • Le système affiche l'interface principale • l'Admin /user « Agent surveillant » rend accès à la fonctionnalité « **Train data** » • Le système lance entrainement. • Le système récupère l'ID à partir des images captures • Le système utilise la methode **LBP Recongntion** **En fin :** Le système est terminé avec succès, le processus de d'entrainement est fait.

Annexe N°04 : Diagramme séquence pour CU entrainement des données (Train data).



Annexe N°05 : Diagramme séquence pour CU gestion étudiants « Student Panel »