REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université de Mohamed El-Bachir El-Ibrahimi - Bordj Bou Arreridj

Faculté *des Sciences et de la technologie*

Département d'Electronique

Mémoire

Présenté pour obtenir

LE DIPLOME DE MASTER

FILIERE : **Electronique**

Spécialité : Electronique des systèmes embarqués

Par

- **BOUNABI Abdelghani**
- **KHELLAF Mohammed**
- **SIDI SALAH Sghira Ahlem**
- **BENGUEDDOUDJ Mustapha**

Intitulé

Système d'intelligence artificielle pour la gestion des accès aux zones sécurisées et semi-sécurisées

Soutenu le : 01 juillet 2024

Devant le Jury composé de :

Nom & Prénom	*Grade*	*Qualité*	*Etablissement*
Mme. Fouzia HAMMADACHE	*MAA*	*Président*	*Univ-BBA*
Dr. Rabah HAMDINI	*MAB*	*Encadreur*	*Univ-BBA*
Dr. Nacira DIFFELLAH	*MCA*	*Encadreur*	*Univ-BBA*
Dr. BEKOUCHE Toufik	*MCA*	*Co-Encadreur*	*Univ-BBA*
Dr. ZERROUGUI Raouf	*MAB*	*Examinateur*	*Univ-BBA*

Année Universitaire 2023/2024

REMERCIEMENTS

Nous tenons à exprimer notre profonde gratitude à toutes les personnes qui ont contribué à la réalisation de ce projet de fin d'études.

Tout d'abord, nous remercions chaleureusement nos encadreurs, Dr.Rabah Hamdini et Dr.Nacira Diffellah, pour leur précieuse guidance, leur soutien constant et leurs conseils avisés tout au long de ce projet. Leur expertise et leur patience ont été déterminantes dans l'accomplissement de ce travail. Nous tenons également à remercier notre co-encadreur, M. Toufik Bekouche, pour son assistance et ses précieuses recommandations.

Nous souhaitons également remercier l'ensemble du corps professoral du département d'électronique des systèmes embarqués pour la qualité de leur enseignement et leur dévouement. Leur passion pour la discipline a été une source d'inspiration et de motivation.

Nos remerciements vont également à nos collègues et amis, pour leur camaraderie, leur aide précieuse et les moments de partage. Leur soutien moral a été inestimable et a rendu cette expérience encore plus enrichissante.

Enfin, nous exprimons notre reconnaissance à nos familles respectives, dont l'amour et le soutien inconditionnels nous ont permis de mener à bien ce projet. Leur confiance en nous a été une source de motivation et de force inépuisable.

DÉDICACE

Nous dédions ce boulot :

A nos familles, qui ont toujours cru en nous et nous ont soutenus tout au long de ce parcours. À nos parents, pour leur amour, leur patience et leurs encouragements constants. À nos frères et sœurs, pour leur soutien et leur compréhension.

Nous dédions également ce projet à tous nos enseignants, en particulier à Dr.Rabah Hamdini, Dr.Nacira Diffellah et Dr.Toufik Bekouche, dont l'accompagnement a été essentiel à la réalisation de ce travail. Merci pour votre confiance et votre dévouement.

Enfin, nous dédions ce mémoire à tous ceux qui poursuivent leurs rêves avec passion et persévérance, en espérant que ce travail puisse inspirer et encourager d'autres étudiants à suivre leur propre chemin avec détermination.

Ahlem & Abdelghani & Mohammed & Mustapha

ملخص

في هذا البحث لنيل درجة الماستر، نقدم نظام ذكاء اصطناعي مصمم لإدارة الوصول إلى المناطق المؤمنة وشبه المؤمنة باستخدام تقنية التعرف على الوجه. هذه التطبيق البرمجي يقوم بأتمتة تتبع الحضور وإدارة الدخول والخروج، مما يلغي الحاجة إلى الطرق اليدوية التي تكون غالباً مرهقة وعرضة للأخطاء.

يقوم النظام بالتعرف على الأفراد باستخدام كاميرا ويقارن وجوههم بتلك المخزنة في قاعدة البيانات. يتم تسجيل الحضور تلقائيًا، بالإضافة إلى أوقات وتواريخ الدخول والخروج. يمكن تخزين البيانات محليًا أو على خادم بعيد مثل Firebase .

بمعدل دقة يصل إلى 99.38% ، يوفر نظامنا حلاً موثوقًا وفعالًا يمكنه استبدال طرق إدارة الوصول التقليدية. هذه الدقة تضمن إدارة آمنة وحديثة لعمليات الدخول والخروج، مما يلبي المتطلبات الحالية للأمن ومراقبة الحضور.

كلمات مفتاحية ـ أتمتة تتبع الحضور، المناطق المؤمنة، قاعدة البيانات ، نظام ذكاء اصطناعي.

Résumé

Dans cette mémoire de master, nous présentons un système d'intelligence artificielle conçu pour gérer les accès aux zones sécurisées et semi-sécurisées en utilisant la reconnaissance faciale. Cette application logicielle automatise la prise de présence et la gestion des entrées et sorties grâce à la technologie de reconnaissance faciale, supprimant ainsi le besoin de méthodes manuelles, souvent fastidieuses et sujettes aux erreurs. Le système permet d'identifier une personne à l'aide d'une caméra, en comparant son visage avec ceux enregistrés dans une base de données. Les présences, ainsi que les heures et dates d'entrée et de sortie, sont ainsi automatiquement enregistrées. Les données peuvent être stockées localement ou sur un serveur distant, tel que Firebase. Avec un taux de reconnaissance de 99,38 %, notre système offre une solution fiable et efficace, capable de remplacer les méthodes traditionnelles de gestion des accès. Cette précision garantit une gestion sécurisée et moderne des entrées et sorties, répondant aux exigences actuelles en matière de sécurité et de contrôle de la présence.

Mots-clés : Automatisation du suivi de présence, base de données, système d'intelligence artificielle, zones sécurisées .

Abstract

In this master's thesis, we present an artificial intelligence system designed to manage access to secure and semi-secure areas using facial recognition technology. This software application automates attendance tracking and entry-exit management, eliminating the need for manual, often tedious, and error-prone methods. The system identifies individuals using a camera and compares their faces with those stored in a database. Attendance records, along with the times and dates of entry and exit, are automatically recorded. Data can be stored either locally or on a remote server, such as Firebase. With a recognition rate of 99.38%, our system offers a reliable and efficient solution capable of replacing traditional access management methods. This accuracy ensures a secure and modern management of entries and exits, meeting current requirements for security and attendance control.

Keywords : Attendance tracking automation, database, artificial intelligence system, secure zones.

TABLE DES MATIÈRES

TABLE DES FIGURES

INTRODUCTION GÉNÉRALE

"Le secret d'un bon discours, c'est d'avoir une bonne introduction et une bonne conclusion. Ensuite, il faut s'arranger pour ces deux parties ne soient pas très éloignées l'une de l'autre."

George Burns

Introduction générale

En 1948, George Orwell dépeignait dans son roman "1984" une société dystopique où un régime totalitaire, symbolisé par le "Big Brother", surveillait étroitement chaque citoyen. Dans ce monde, les caméras omniprésentes surveillaient les moindres faits et gestes des individus, et ces derniers étaient punis en fonction de leurs actions, voire de leurs pensées. Ce récit visionnaire soulève aujourd'hui des questions cruciales au sein de nos sociétés. Alex Türk, ancien directeur de la Commission nationale de l'informatique et des libertés (CNIL), prévoit que nous serons tous inévitablement soumis à une surveillance constante dans une société où il sera impossible de travailler, de se divertir, de se déplacer ou même de vivre sans être constamment tracés[20].

L'utilisation du contrôle d'accès par reconnaissance faciale soulève une série de questions et de défis majeurs qui nécessitent une réflexion approfondie. Tout d'abord, cette technologie empiète-t-elle sur la vie privée des individus ? La collecte et le traitement des données biométriques posent des questions fondamentales sur le droit à la vie privée et à l'autonomie individuelle. De plus, quelles sont les implications en termes de sécurité des données ? Les bases de données contenant des informations sensibles sur les visages des individus peuvent être vulnérables aux piratages et aux abus, ce qui soulève des préoccupations majeures en matière de sécurité. En outre, la reconnaissance faciale peut-elle engendrer des biais et des discriminations ? Des études ont montré que ces systèmes peuvent être moins précis pour certains groupes ethniques ou selon le genre, ce qui soulève des inquiétudes quant à l'équité et à la justice de leur utilisation. Enfin, quel est l'impact sur la liberté individuelle et la société dans son ensemble ? La normalisation de la surveillance constante peut entraîner une société de surveillance où la liberté individuelle est compromise au nom de la sécurité, ce qui pose des questions essentielles sur les valeurs démocratiques et les droits fondamentaux. Ainsi, l'introduction du contrôle d'accès par reconnaissance faciale soulève des défis complexes qui nécessitent une approche équilibrée et éthique pour garantir son utilisation responsable et respectueuse des droits de l'homme[21].

En tirant parti des progrès technologiques dans les domaines de la vision par ordinateur et du traitement d'image, cette mémoire propose l'implémentation d'un système de contrôle d'accès par reconnaissance faciale, offrant ainsi une solution efficace et pratique pour identifier les individus autorisés à accéder à des zones sécurisées. En remplaçant les méthodes conventionnelles telles que les cartes d'identité ou les codes d'accès, la reconnaissance faciale offre la promesse d'une expérience d'accès plus fluide et d'une sécurité renforcée. Ce mémoire est organisé en deux parties. Dans le premier chapitre, nous fournirons un aperçu général de la biométrie et de l'utilité de la reconnaissance faciale dans divers domaines. Dans le deuxième chapitre, nous présenterons notre application proposée pour le pointage automatisé, accompagnée d'une discussion détaillée des différentes spécifications de cette application.

CHAPITRE 1

LA BIOMÉTRIE

«La théorie est grisante, mais rien ne vaut l'épreuve du réel.»

Karl Marx

Chapitre 1. La biométrie

La biométrie est une discipline technologique qui exploite des caractéristiques physiologiques ou comportementales uniques à chaque individu pour leur identification ou leur authentification. Elle trouve des applications dans divers domaines tels que la sécurité nationale, la gestion de l'identité, l'administration, le contrôle d'accès, la santé électronique, et même le confort personnel. Parmi les technologies biométriques les plus couramment utilisées, on trouve la reconnaissance faciale, digitale, vocale, palmaire, de l'iris et l'ADN (voir Figure 1.1).

FIGURE 1.1 – Les technologies biométriques [27]

La problématique de la biométrie réside dans sa fiabilité et la protection de la vie privée. Malgré son haut niveau de sécurité et d'efficacité, la biométrie reste vulnérable aux piratages et aux contournements. Par exemple, des experts en cybersécurité ont montré qu'il était possible de tromper les dispositifs de reconnaissance des veines de la main en utilisant une main artificielle en cire. De plus, les bases de données contenant des informations biométriques peuvent être compromises, exposant ainsi les victimes à des risques d'usurpation d'identité préjudiciables [1].
La solution à ces problèmes passe par l'amélioration des technologies biométriques et la mise en place de mesures de protection des données adéquates. Les systèmes biométriques doivent être conçus pour détecter et prévenir les tentatives de piratage en temps réel. Les bases de données contenant des informations biométriques doivent être sécurisées, et les victimes d'usurpation d'identité doivent être indemnisées.
De plus, les organisations proposant des solutions biométriques doivent analyser précisément la nature du problème à résoudre et vérifier si le système proposé est approprié et proportionné.

I Types d'identifiants biométriques

Dans le domaine de la biométrie, les identifiants font référence aux caractéristiques biologiques ou comportementales uniques utilisées pour identifier et vérifier l'identité

d'une personne. Voici quelques types d'identifiants biométriques couramment utilisés :

I.1 La reconnaissance de l'iris

La reconnaissance de l'iris est une technique biométrique utilisée pour identifier et vérifier l'identité d'une personne en analysant les motifs uniques présents dans l'iris de l'œil. Pour effectuer la reconnaissance de l'iris, un système de reconnaissance d'iris capture une image de l'iris à l'aide d'une caméra spéciale, puis analyse les caractéristiques uniques de l'iris pour créer un modèle biométrique(voir Figure 1.2). Ce modèle est ensuite comparé à une base de données contenant des modèles d'iris enregistrés pour vérifier l'identité de la personne. La reconnaissance de l'iris est largement utilisée dans les systèmes de sécurité, les contrôles d'accès et les applications de gestion de l'identité [2].

FIGURE 1.2 – La reconnaissance de l'iris [28]

I.2 La reconnaissance des veines de la paume de la main

La reconnaissance des veines de la paume de la main est une technique biométrique qui utilise les motifs de veines visibles sous la peau de la paume de la main pour identifier et vérifier l'identité d'une personne. Cette méthode repose sur le fait que les motifs veineux sont uniques à chaque individu et relativement stables dans le temps [3].
Le processus de reconnaissance des veines de la paume de la main implique généralement la capture d'une image infrarouge de la paume de la main à l'aide d'une caméra spéciale. Les caractéristiques distinctives des veines, telles que leur forme, leur distribution et leur densité, sont ensuite extraites de l'image et utilisées pour créer un modèle biométrique unique pour chaque individu (voir Figure 1.3).

La reconnaissance des veines de la paume de la main est utilisée dans divers domaines, notamment la sécurité physique, les contrôles d'accès aux bâtiments, les transactions financières sécurisées et les systèmes d'authentification biométrique. Elle est appréciée pour sa fiabilité, sa précision et sa résistance aux tentatives de contrefaçon. De plus, comme les veines sont situées sous la peau, cette méthode offre

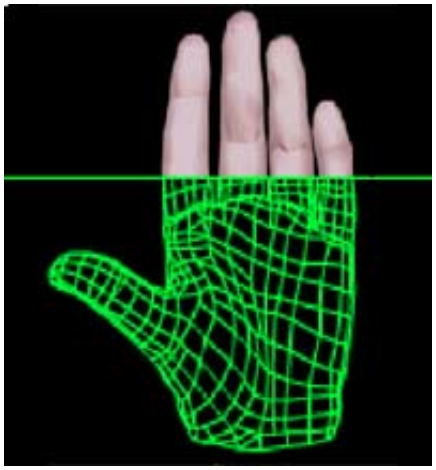

FIGURE 1.3 – La reconnaissance des veines de la paume de la main [29]

un niveau supplémentaire de sécurité et de confidentialité par rapport aux caractéristiques biométriques externes telles que les empreintes digitales ou la reconnaissance faciale.

I.3 La Lecture des empreintes digitales

La lecture des empreintes digitales est une technique biométrique qui utilise les caractéristiques uniques des empreintes digitales pour identifier les individus [4]. Les étapes principales de ce processus incluent la capture de l'empreinte, l'extraction de ses caractéristiques distinctives, le stockage sécurisé du modèle numérique correspondant dans une base de données biométrique, et enfin la comparaison avec les empreintes présentées pour l'authentification. Cette méthode est largement utilisée dans la sécurité, le contrôle d'accès et la gestion de l'identité en raison de sa fiabilité et de sa facilité d'utilisation. Elle est considérée comme l'une des méthodes biométriques les plus établies et les plus fiables (voir Figure 1.4).

FIGURE 1.4 – La lecture des empreintes digitales [4]

I.4 La reconnaissance vocale

La reconnaissance vocale est une technologie de biométrie qui utilise les caractéristiques uniques de la voix d'une personne pour identifier et vérifier son identité. Cette technique repose sur l'analyse des paramètres vocaux, tels que la fréquence, le timbre, la cadence et l'intonation, pour créer un modèle vocal distinctif pour chaque individu [5].
Le processus de reconnaissance vocale commence par la capture de l'échantillon vocal de l'utilisateur, généralement sous la forme d'un enregistrement audio. Les caractéristiques vocales de cet échantillon sont ensuite extraites et analysées pour créer un modèle vocal unique, souvent appelé "empreinte vocale".
Lorsqu'une personne tente de s'authentifier à l'aide de la reconnaissance vocale, son échantillon vocal est comparé au modèle vocal enregistré dans la base de données. Si les deux correspondent avec une certaine tolérance, l'authentification est réussie et l'accès est accordé (voir Figure 1.5).

FIGURE 1.5 – Processus de reconnaissance vocale[5]

La reconnaissance vocale est utilisée dans une variété d'applications, notamment la sécurité des transactions, l'authentification des utilisateurs sur les appareils mobiles, les centres d'appels automatisés et les systèmes de dictée vocale. Cette méthode biométrique est appréciée pour sa facilité d'utilisation, sa non-intrusivité et sa résistance aux tentatives de contrefaçon. Cependant, elle peut être sensible aux variations de la voix dues à des facteurs tels que l'âge, la santé ou l'émotion.

I.5 La reconnaissance faciale

La reconnaissance faciale est le dernier type de contrôle d'accès biométrique. Elle implique l'utilisation d'un algorithme pour extraire et analyser les caractéristiques d'un visage humain à partir d'une vidéo ou d'une photo. En quelques millisecondes, ces caractéristiques sont enregistrées et converties en un code unique (voir Figure 1.6). Ensuite, ce code est comparé à ceux stockés dans une base de données par le logiciel de reconnaissance faciale. Si une correspondance est trouvée, l'algorithme identifie l'individu dans l'image et détermine s'il doit autoriser ou refuser l'accès.

Cette méthode permet une identification rapide et précise des personnes en se basant sur leurs traits faciaux distinctifs [6].

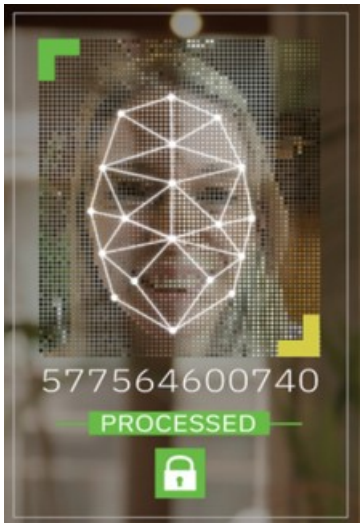

FIGURE 1.6 – Identification Numérique : Visage codé [6]

II La reconnaissance faciale Pour contrôle d'accès biométrique

La reconnaissance faciale trouve une variété d'applications. Dans notre mémoire de master, nous nous concentrons spécifiquement sur son utilisation dans le contrôle d'accès. Cependant, il est important de noter qu'elle peut également être utilisée dans d'autres domaines. Voici quelques-unes de ses applications :

II.1 La surveillance de masse

La surveillance de masse implique la surveillance systématique et à grande échelle d'un grand nombre de personnes dans des espaces publics ou semi-publics. La reconnaissance faciale est une technologie de surveillance qui peut être utilisée dans le cadre de la surveillance de masse pour identifier et suivre les individus à partir de leurs caractéristiques faciales uniques[7].
Dans le contexte de la surveillance de masse, la reconnaissance faciale est souvent utilisée dans les systèmes de vidéosurveillance déployés dans les lieux publics tels que les gares, les aéroports, les stades, les centres commerciaux, etc. Les caméras de surveillance captent des images des visages des personnes dans ces endroits, puis des algorithmes de reconnaissance faciale analysent ces images pour identifier les individus en comparant leurs caractéristiques faciales à une base de données de visages connus(voir Figure 1.7).

L'utilisation de la reconnaissance faciale dans la surveillance de masse peut avoir plusieurs objectifs :

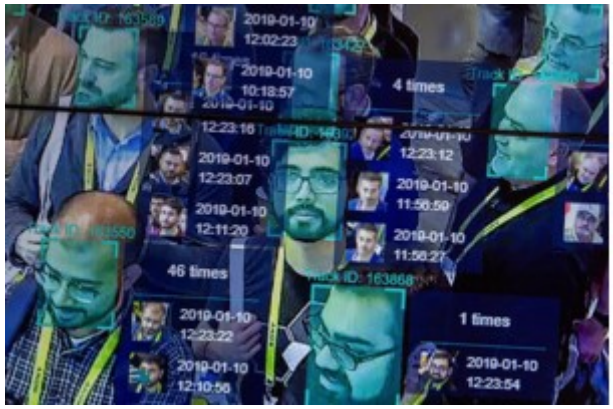

FIGURE 1.7 – Surveillance de masse : Visages sous Veille [7]

1. **La sécurité publique :** Elle peut aider à repérer et à suivre les personnes recherchées ou suspectes en temps réel, permettant ainsi aux autorités de prévenir les crimes ou les incidents.
2. **Le gestion des foules :** La technologie peut être utilisée pour surveiller et gérer les flux de personnes lors d'événements de masse, ce qui peut être utile pour assurer la sécurité et la gestion des crises.
3. **La prévention du terrorisme :** En identifiant rapidement les individus potentiellement dangereux ou recherchés, la reconnaissance faciale peut contribuer à renforcer la sécurité dans les lieux sensibles et à prévenir les actes terroristes.
4. **L'identification des personnes disparues :** Elle peut également être utilisée pour aider à retrouver des personnes disparues en identifiant leur présence dans des zones surveillées.

Cependant, l'utilisation de la reconnaissance faciale dans la surveillance de masse soulève des questions importantes concernant la vie privée, les libertés civiles et le potentiel d'abus de pouvoir par les autorités. Les préoccupations liées à la collecte et à l'utilisation des données biométriques, ainsi qu'à la précision et à la fiabilité de la technologie, sont également au centre des débats sur son utilisation dans la société.

II.2 L'authentification individuelle

L'authentification individuelle est le processus de vérification de l'identité d'une personne, tandis que la reconnaissance faciale est une méthode de biométrie utilisée pour identifier et vérifier l'identité des individus en analysant les caractéristiques du visage.
Dans le cadre de l'authentification individuelle, la reconnaissance faciale peut être utilisée comme méthode de vérification biométrique. Plutôt que de se baser sur des mots de passe, des codes PIN ou des cartes d'identité, la reconnaissance faciale utilise des algorithmes pour analyser les caractéristiques uniques du visage d'une personne. Ces caractéristiques peuvent inclure la forme du visage, la disposition des yeux, du nez et de la bouche, ainsi que d'autres détails spécifiques (voir Figure 1.8).

Lorsqu'un individu souhaite s'authentifier, un système de reconnaissance faciale capture une image de son visage et la compare à une base de données contenant des images faciales autorisées. Si les caractéristiques du visage correspondent à celles stockées dans la base de données avec une certaine marge d'erreur acceptable, l'authentification est réussie et l'accès est accordé [8].

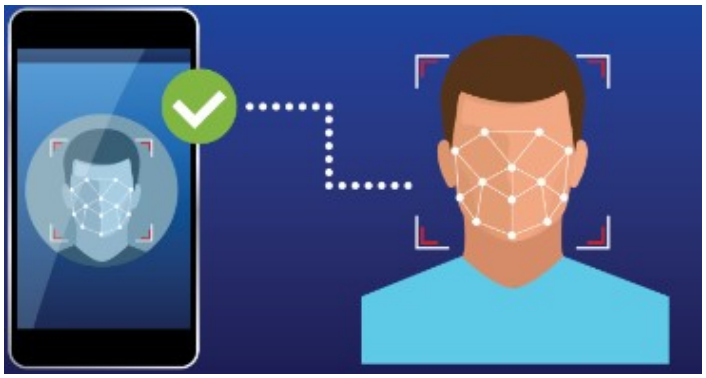

FIGURE 1.8 – Authentification individuelle [8]

La reconnaissance faciale est utilisée dans de nombreux domaines pour l'authentification individuelle, tels que le déverrouillage des téléphones mobiles, le contrôle d'accès aux bâtiments, la sécurité des données personnelles, les transactions financières en ligne, et bien d'autres. Elle offre un moyen pratique et sécurisé d'authentifier les individus en se basant sur leurs caractéristiques faciales uniques. Cependant, il est important de noter que la reconnaissance faciale n'est pas infaillible et peut être sujette à des erreurs, notamment en cas de mauvaise illumination, de changements dans l'apparence du visage (comme la barbe ou les lunettes), ou de falsification d'images.

II.3 Les enquêtes médico-légales

Les enquêtes médico-légales se concentrent sur l'examen des preuves médicales et légales dans le cadre d'affaires judiciaires, tandis que la reconnaissance faciale est une technologie de biométrie utilisée pour identifier et vérifier l'identité des individus en analysant les caractéristiques du visage. Bien que ces deux domaines puissent sembler distincts, ils peuvent parfois se chevaucher dans certains contextes, notamment lors d'enquêtes sur des cas de violence, d'agression ou de décès impliquant des blessures faciales [9].
Dans le cadre d'une enquête médico-légale, la reconnaissance faciale peut être utilisée pour identifier les victimes ou les suspects à partir d'images ou de vidéos récupérées sur les lieux de l'incident. Les experts médico-légaux peuvent analyser les blessures faciales des individus impliqués et les comparer aux images des suspects ou des témoins pour aider à établir des preuves médico-légales (voir Figure 1.9).

De plus, la reconnaissance faciale peut également être utilisée pour l'identification post-mortem des victimes dans les cas de décès où l'identification visuelle est difficile

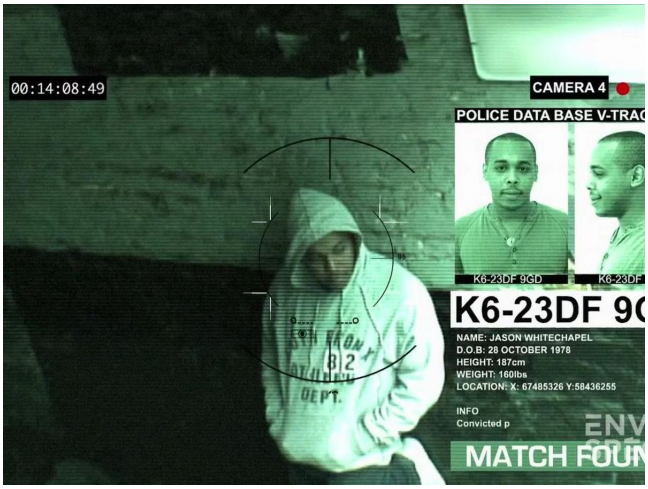

FIGURE 1.9 – Application de la reconnaissance faciale dans les enquêtes médico-légales [9]

ou impossible en raison de l'état du corps. Les médecins légistes peuvent utiliser la reconnaissance faciale pour comparer les caractéristiques faciales des victimes avec des images d'archives ou des bases de données pour confirmer leur identité

II.4 Le contrôle d'accès

Enfin, la reconnaissance faciale peut être exploitée dans des systèmes de contrôle d'accès, où elle joue un rôle crucial. Dans ce type de configuration, il est primordial que le logiciel soit capable de comparer en temps réel les données provenant de multiples caméras avec celles stockées dans la base de données. Pour ce faire efficacement, surtout avec des bases de données volumineuses. Un serveur dédié est souvent déployé afin de garantir une vérification rapide de l'autorisation. Si une correspondance est établie, l'accès est alors autorisé et le point d'accès peut être déverrouillé [10].

III Avantage du contrôle d'accès par reconnaissance faciale

La reconnaissance faciale offre plusieurs avantages, parmi lesquels on peut mentionner :

III.1 Circulation fluidifiée

La fluidification de la circulation peut bénéficier de l'intégration de la reconnaissance faciale. Cette technologie peut être utilisée pour identifier les individus dans les zones de passage et faciliter ainsi les processus de contrôle d'accès (voir Figure 1.10). En automatisant l'identification des personnes, la reconnaissance faciale permet des contrôles plus rapides et plus efficaces, réduisant ainsi les files d'attente et les temps d'attente aux points de contrôle. De plus, elle offre une sécurité accrue en permettant

de détecter rapidement les personnes non autorisées ou les intrus. En résumé, en intégrant la reconnaissance faciale dans les systèmes de gestion de la circulation, il est possible de fluidifier les déplacements tout en renforçant la sécurité.

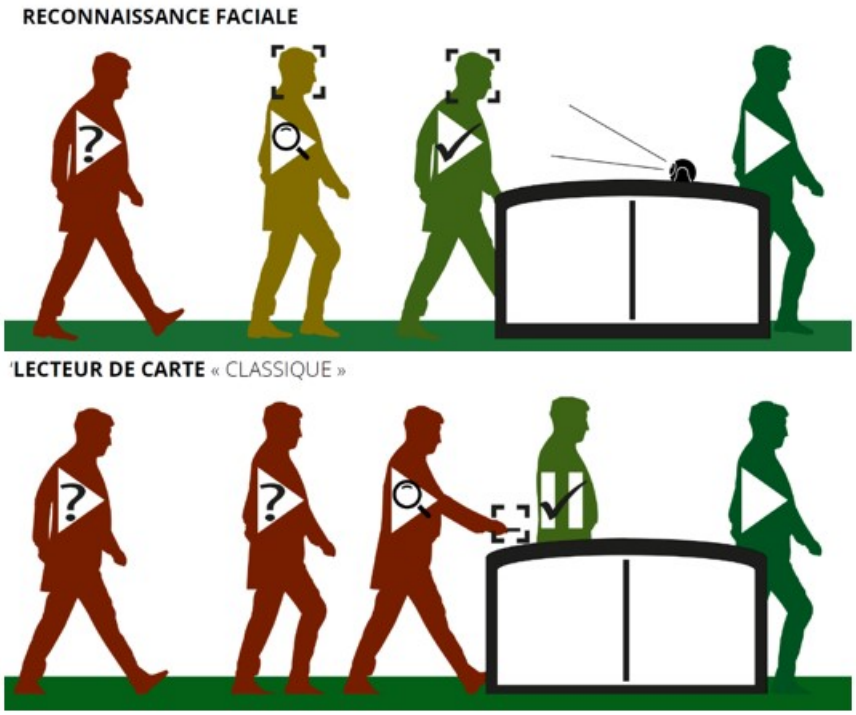

FIGURE 1.10 – La fluidification de la circulation grâce à la reconnaissance faciale

III.2 Accès rapide en tout temps

La reconnaissance faciale offre un accès rapide et pratique en tout temps (voir Figure 1.11), permettant d'identifier rapidement les individus en analysant leurs caractéristiques faciales uniques. Cette méthode d'authentification instantanée évite le besoin de se rappeler des mots de passe ou de transporter des cartes d'identification, ce qui est particulièrement avantageux dans les environnements où l'efficacité est primordiale, tels que les entreprises, les institutions publiques ou les événements à forte affluence. De plus, la reconnaissance faciale fonctionne à tout moment, garantissant un accès sécurisé continu, indépendamment des conditions d'éclairage.
Un autre avantage majeur est que la technologie ne nécessite quasiment aucune action de la part de l'utilisateur lors du point de contrôle d'accès. Dès qu'un visage entre dans le champ de vision de la caméra, le logiciel peut vérifier automatiquement si la personne est autorisée. Cette approche supprime le besoin de badges d'accès, éliminant ainsi le risque de les oublier. De plus, les utilisateurs ne sont plus confrontés à des files d'attente dues à la recherche de badges par d'autres personnes, et conservent leurs mains libres pour manipuler leurs effets personnels.

FIGURE 1.11 – Authentification d'accès par reconnaissance faciale[29]

III.3 Aucun partage de badges d'accès

La reconnaissance faciale élimine le besoin de partager des badges d'accès physiques dans les systèmes de contrôle d'accès. Au lieu de cela, les individus sont identifiés et autorisés à accéder à des zones sécurisées en se basant sur leurs caractéristiques faciales uniques. Cette approche réduit les risques liés à la perte, au vol ou à la falsification des badges d'accès physiques, tout en offrant une méthode plus pratique et sécurisée pour gérer l'accès aux installations (voir Figure 1.12).

FIGURE 1.12 – Authentification d'accès par badges d'accès [30]

III.4 Aucun contact requis avec les solutions biométriques

La reconnaissance faciale, offrent l'avantage de ne nécessiter aucun contact direct avec l'utilisateur. Dans le cas de la reconnaissance faciale, aucune manipulation physique n'est requise. L'utilisateur n'a pas besoin de toucher un appareil ou d'insérer une carte, ce qui rend le processus d'authentification plus rapide, pratique et hygiénique, notamment dans les contextes où l'hygiène et la sécurité sont primordiales, comme dans les environnements médicaux ou les zones à haut risque de contamination (voir Figure 1.13).

FIGURE 1.13 – Contrôle d'accès dans un lieu semi-public

IV Éléments constitutifs d'un système de reconnaissance faciale

Lorsque le contrôle d'accès par reconnaissance faciale est choisi, il convient de noter que le système sera composé de plusieurs éléments. Ces éléments sont généralement fournis par différentes parties et doivent être interconnectés. Il est donc essentiel d'examiner quels fournisseurs peuvent collaborer pour construire un système fonctionnant de manière fluide. En général, les composants suivants devront être interconnectés :

IV.1 Caméras et autres capteurs

Les caméras jouent un rôle essentiel dans les systèmes de reconnaissance faciale. Elles capturent les images des visages des individus pour permettre à l'algorithme de reconnaissance faciale d'analyser et d'identifier les caractéristiques uniques du visage (voir Figure 1.14). Ces caractéristiques sont ensuite comparées à une base de données pour vérifier l'identité de l'utilisateur.

FIGURE 1.14 – Caméra de surveillance

Effectivement, lors du choix des caméras pour les systèmes de reconnaissance faciale, plusieurs facteurs doivent être pris en considération en plus du nombre de mégapixels. La sensibilité à la lumière est un aspect crucial, car elle détermine la capacité de la caméra à capturer des images claires dans des conditions d'éclairage variables, notamment dans des environnements faiblement éclairés ou en pleine lumière. Le type d'objectif est également important, car il influe sur la netteté et la qualité des images capturées. De plus, la capacité de traitement de la puce de la caméra est essentielle pour assurer un traitement rapide et efficace des données, ce qui peut affecter les performances globales du système de reconnaissance faciale [11]. En outre, des capteurs supplémentaires peuvent être ajoutés pour améliorer la capacité du système à distinguer un visage réel d'une photographie ou d'une vidéo. Ces capteurs peuvent détecter des signaux tels que la température corporelle ou les mouvements, ce qui permet de renforcer la sécurité et d'éviter les tentatives de fraude ou de contournement du système.
En résumé, le choix des caméras pour les systèmes de reconnaissance faciale doit être soigneusement étudié, en tenant compte de divers facteurs tels que la sensibilité à la lumière, le type d'objectif, la capacité de traitement de la puce et l'ajout éventuel de capteurs supplémentaires. Une sélection judicieuse des caméras contribuera à garantir des performances optimales du système de reconnaissance faciale dans une variété de conditions environnementales et opérationnelles.

IV.2 Logiciel de reconnaissance faciale

Le logiciel de reconnaissance faciale est au cœur des systèmes de reconnaissance faciale. Il comprend un ensemble d'algorithmes et de technologies conçus pour analyser, identifier et comparer les caractéristiques faciales des individus à partir des images capturées par les caméras [12]. Voici quelques éléments clés à considérer lors du choix d'un logiciel de reconnaissance faciale :

1. **La précision :** La précision de l'algorithme de reconnaissance faciale est cruciale pour garantir des résultats fiables et précis. Un logiciel de haute qualité devrait être capable de reconnaître les visages avec un haut degré de précision, même dans des conditions variables telles que des angles de vue différents, des changements d'éclairage et des expressions faciales variées.
2. **La vitesse :** La vitesse de traitement des images est également importante, surtout dans les applications en temps réel telles que le contrôle d'accès ou la surveillance de masse. Un logiciel capable de traiter les images rapidement permet une identification rapide des individus et une réponse en temps opportun aux événements.
3. **L'adaptabilité :** Le logiciel devrait être adaptable à une variété de conditions environnementales et opérationnelles, ainsi qu'à différents types de matériel et de configurations système. Il devrait être capable de s'intégrer facilement à d'autres composants du système, tels que les caméras, les bases de données et les systèmes de contrôle d'accès.
4. **La sécurité :** La sécurité des données et la protection de la vie privée des individus sont des préoccupations majeures lors de l'utilisation de la

reconnaissance faciale. Le logiciel doit être doté de fonctionnalités de sécurité robustes pour garantir la confidentialité et l'intégrité des données biométriques.

5. **Les mises à jour et support :** Un bon fournisseur de logiciel de reconnaissance faciale devrait fournir des mises à jour régulières pour améliorer les performances et la sécurité du logiciel, ainsi qu'un support technique fiable pour répondre aux besoins des utilisateurs et résoudre les problèmes éventuels.

En résumé, le logiciel de reconnaissance faciale est un élément essentiel des systèmes de reconnaissance faciale, et le choix du bon logiciel est crucial pour garantir des performances optimales, une précision élevée et la sécurité des données.

IV.3 Système de contrôle d'accès

Un système de contrôle d'accès par reconnaissance faciale est une solution de sécurité qui utilise la technologie de reconnaissance faciale pour authentifier et autoriser l'accès des individus à des zones sécurisées ou à des ressources sensibles [13]. Voici comment fonctionne généralement un tel système :

1. **Capture d'images :** Des caméras spéciales capturent les images des visages des individus qui souhaitent accéder à une zone sécurisée.
2. **Analyse des caractéristiques faciales :** Les caractéristiques du visage, telles que la forme du visage, les yeux, le nez et la bouche, sont extraites et analysées à l'aide d'algorithmes de reconnaissance faciale (voir Figure 1.15).
3. **Comparaison avec la base de données :** Les caractéristiques faciales extraites sont comparées aux données stockées dans une base de données sécurisée, qui contient les informations biométriques des personnes autorisées à accéder à la zone sécurisée.
4. **Décision d'accès :** Si une correspondance est trouvée entre les caractéristiques faciales de l'individu et celles stockées dans la base de données, l'accès est accordé et la porte ou le point d'accès est déverrouillé. Sinon, l'accès est refusé.
5. **Audit et suivi :** Le système enregistre les tentatives d'accès, y compris les visages identifiés et les actions prises (accès autorisé ou refusé), ce qui permet un suivi précis de l'utilisation du système.

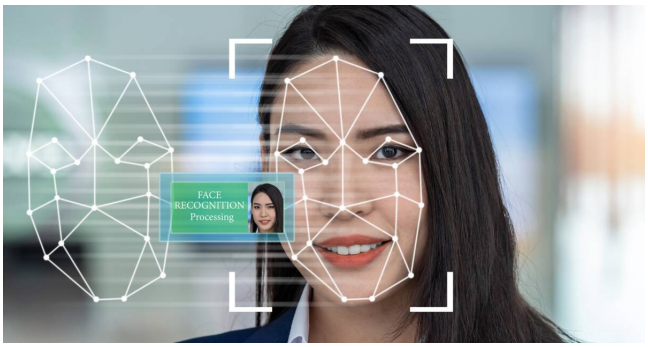

FIGURE 1.15 – Technologie de Reconnaissance Faciale : Sécurité et Anonymat

Les systèmes de contrôle d'accès par reconnaissance faciale offrent plusieurs avantages, notamment une identification rapide et précise des individus, une réduction du risque de fraude liée aux cartes d'identité ou aux mots de passe perdus ou volés, et une amélioration globale de la sécurité. Cependant, il est important de tenir compte des préoccupations liées à la vie privée et à la sécurité des données lors de la mise en œuvre d'un tel système.

IV.4 Contrôle d'accès physique

Dans les systèmes de contrôle d'accès, la reconnaissance faciale est souvent intégrée à une solution de contrôle d'accès physique. En effet, sécuriser l'accès aux personnes non autorisées nécessite l'instauration de barrières efficaces. Ces barrières peuvent prendre diverses formes, chacune offrant ses propres niveaux de sécurité [14]. Les composants du système peuvent être configurés de différentes manières. Certains produits de contrôle d'accès physique intègrent déjà une solution de reconnaissance faciale, tandis que d'autres éléments peuvent être achetés séparément pour être ajoutés au système (voir Figure 1.16).

FIGURE 1.16 – Accès Autorisé : La Reconnaissance Faciale en Action

V Aspects techniques de la reconnaissance faciale

Les aspects techniques de la reconnaissance faciale peuvent être synthétisés par les points suivants :

V.1 Conditions d'éclairage

Les conditions d'éclairage pour la reconnaissance faciale varient selon les technologies utilisées et les environnements spécifiques. Cependant, voici quelques principes généraux :

1. **Éclairage uniforme :** Un éclairage uniforme sur le visage réduit les ombres et les variations de luminosité, ce qui facilite la détection des caractéristiques du visage
2. **Éviter les reflets :** Les reflets provenant de sources de lumière directe peuvent perturber les capteurs et rendre la reconnaissance faciale moins précise.
3. **Éviter les contre-jours :** Les contre-jours peuvent obscurcir le visage et rendre difficile la détection des caractéristiques faciales.
4. **Lumière naturelle préférable :** La lumière naturelle offre souvent une meilleure qualité d'image que la lumière artificielle, en particulier la lumière du jour diffuse.
5. **Éviter les ombres :** Les ombres, en particulier sur les parties critiques du visage comme les yeux, le nez et la bouche, peuvent interférer avec la détection des caractéristiques.
6. **Éclairage adaptatif :** Certaines technologies de reconnaissance faciale intègrent des algorithmes capables de s'adapter à diverses conditions d'éclairage, mais des conditions idéales restent préférables pour une performance optimale
7. **Éclairage suffisant :** Assurez-vous qu'il y a suffisamment de lumière pour capturer des images de haute qualité. Un éclairage insuffisant peut entraîner des images floues ou bruitées, ce qui peut affecter la précision de la reconnaissance faciale.

En résumé, un éclairage uniforme, évitant les reflets, les contre-jours et les ombres excessives, avec une préférence pour la lumière naturelle, contribue à des conditions optimales pour la reconnaissance faciale.

V.2 Mise au point de la caméra

La mise au point de la caméra est considérée comme cruciale dans le contexte de la reconnaissance faciale afin de garantir la netteté des images capturées et la précision de la détection des caractéristiques faciales. Voici quelques points à considérer :

1. **Focus automatique :** Une caméra équipée d'une fonction de mise au point automatique doit être utilisée pour garantir que les visages sont capturés avec netteté, même lorsque la distance entre la caméra et le sujet varie.
2. **Précision de la mise au point :** Il est important de s'assurer que la mise au point est précise pour capturer les détails du visage avec clarté. Une mise au point floue peut compromettre la précision de la reconnaissance faciale
3. **Contrôle manuel** Dans certaines situations, un contrôle manuel de la mise au point de la caméra peut être nécessaire pour garantir la netteté des visages, notamment si la fonction de mise au point automatique ne fonctionne pas correctement dans certaines conditions.
4. **Prévention de la dégradation de la mise au point** Évitez les conditions susceptibles d'entraîner une dégradation de la mise au point, telles que les vibrations de la caméra ou les changements brusques de température

5. **Réglages de l'appareil photo** Certains paramètres de l'appareil photo, tels que l'ouverture et la vitesse d'obturation, peuvent influencer la mise au point. Assurez-vous que ces réglages sont optimisés pour capturer des visages nets
6. **Calibrage régulier** Il peut être nécessaire de calibrer régulièrement la mise au point de la caméra pour garantir des performances optimales, en particulier dans le cas des systèmes de reconnaissance faciale en continu ou à grande échelle.

En résumé, une mise au point précise et fiable de la caméra est essentielle pour garantir la qualité des images capturées et la précision de la reconnaissance faciale. Il est recommandé d'utiliser des caméras dotées d'une fonction de mise au point automatique pour une expérience optimale.

VI La mise en œuvre de système de contrôle d'accès

La mise en œuvre d'un système de contrôle d'accès implique la configuration et l'intégration de dispositifs de reconnaissance, tels que les caméras et les scanners biométriques, avec des logiciels spécialisés. Cette méthode garantit une identification précise et rapide des individus autorisés, renforçant ainsi la sécurité des installations.

VI.1 Circulation des utilisateurs

La mise en œuvre de couloirs rapides de contrôle d'accès dans le cadre de la reconnaissance faciale peut être réalisée en suivant quelques étapes clés :

FIGURE 1.17 – Passage Futuriste

1. **Conception du couloir :** L'emplacement et la conception physique du couloir rapide de contrôle d'accès doivent être définis. Il peut être constitué d'un passage délimité par des barrières ou des portiques équipés de caméras de reconnaissance faciale (voir Figure 1.17).
2. **Installation des équipements :** Les équipements nécessaires, tels que les caméras de reconnaissance faciale, les capteurs de mouvement et les dispositifs de sécurité, doivent être installés pour assurer le bon fonctionnement du couloir.
3. **Configuration du logiciel :** Le logiciel de reconnaissance faciale pour le couloir rapide doit être configuré de manière à ce qu'il puisse capturer et traiter rapidement les visages des utilisateurs entrants.
4. **Calibration :** Les caméras et les capteurs doivent être calibrés pour s'assurer qu'ils fonctionnent correctement et qu'ils peuvent détecter et suivre les visages avec précision.
5. **Tests et ajustements :** Des tests approfondis doivent être effectués pour s'assurer que le couloir rapide fonctionne comme prévu. Des ajustements doivent être effectués si nécessaire pour optimiser la précision et la vitesse de la reconnaissance faciale.
6. **Formation du personnel :** Le personnel chargé de surveiller et de gérer le couloir rapide doit être formé pour savoir comment réagir en cas de problème ou d'incident.
7. **Communication avec les utilisateurs :** Les utilisateurs doivent être informés clairement des instructions à suivre lorsqu'ils passent par le couloir rapide, y compris les informations sur la reconnaissance faciale et la confidentialité des données.
8. **Surveillance continue :** Le fonctionnement du couloir rapide doit être surveillé en continu pour détecter et résoudre rapidement tout problème éventuel.

En suivant ces étapes, des couloirs rapides de contrôle d'accès basés sur la reconnaissance faciale peuvent être mis en œuvre efficacement pour gérer la circulation des utilisateurs de manière sécurisée et efficace.

VI.2 Présentation du visage

Dans un système de reconnaissance faciale, les utilisateurs n'ont pas besoin d'effectuer des actions supplémentaires pour accéder, mais ils doivent être conscients que leur visage doit être scanné par le logiciel de reconnaissance. Cela signifie que les utilisateurs doivent positionner leur visage clairement devant la caméra pour permettre le processus de reconnaissance. Cependant, certains obstacles comme le port d'un masque ou le fait de regarder dans une autre direction peuvent entraver l'accès. Ainsi, la coopération des utilisateurs est nécessaire pour garantir le bon fonctionnement du système.

VI.3 Interaction avec l'utilisateur

L'interaction avec l'utilisateur joue un rôle crucial dans la reconnaissance faciale, contribuant à plusieurs aspects essentiels. Tout d'abord, une interface conviviale et des instructions claires facilitent l'utilisation du système, améliorant ainsi l'expérience utilisateur. De plus, une interaction engageante encourage la coopération des utilisateurs et réduit les erreurs grâce à une communication précise sur la manière de positionner correctement le visage devant la caméra. Une interaction transparente renforce également la confiance des utilisateurs dans la technologie de reconnaissance faciale. Enfin, une conception centrée sur l'utilisateur assure l'accessibilité du système à tous les utilisateurs, quelles que soient leurs capacités. En résumé, une interaction efficace avec l'utilisateur dans la reconnaissance faciale est essentielle pour améliorer l'expérience, encourager l'adhésion, réduire les erreurs, renforcer la confiance et garantir l'accessibilité pour tous.

VII Sécurité numérique

La sécurité numérique est une préoccupation majeure dans notre ère technologique, où les données personnelles et sensibles sont souvent stockées et échangées en ligne. Elle englobe un large éventail de pratiques, outils et mesures visant à protéger les systèmes informatiques, réseaux, appareils et données contre les menaces telles que les cyberattaques, le vol d'identité, le piratage informatique et les logiciels malveillants.

VII.1 Cryptage

Le cryptage du logiciel de reconnaissance faciale revêt une importance capitale pour plusieurs raisons cruciales :

1. **Confidentialité des données :** Le cryptage assure la protection des données biométriques sensibles, comme les empreintes faciales, contre tout accès non autorisé, préservant ainsi la vie privée des individus et prévenant la divulgation ou la manipulation de leurs informations personnelles.
2. **Protection contre les cyberattaques :** Les algorithmes de reconnaissance faciale sont des cibles potentielles pour les cyberattaques en raison de la sensibilité des données qu'ils traitent. Le cryptage renforce la sécurité des systèmes en rendant les données illisibles pour les individus non autorisés, réduisant ainsi les risques de violation de sécurité.
3. **Conformité aux réglementations :** De nombreuses juridictions ont mis en place des réglementations strictes concernant la protection des données personnelles, telles que le RGPD en Europe. Le cryptage est souvent une exigence pour être conforme à ces réglementations et éviter les sanctions potentielles en cas de non-respect.
4. **Intégrité des données :** Le cryptage garantit également l'intégrité des données en empêchant toute altération non autorisée. Cela garantit que les informations utilisées par le système de reconnaissance faciale sont fiables et non altérées, ce qui améliore la précision et la fiabilité du système.

5. **Confiance des utilisateurs :** En mettant en œuvre des mesures de sécurité telles que le cryptage, les fournisseurs de solutions de reconnaissance faciale peuvent renforcer la confiance des utilisateurs dans leurs produits et services. Les utilisateurs seront plus enclins à utiliser des systèmes qui garantissent la protection de leurs données personnelles.

VII.2 Détection de la fraude

La détection de la fraude est essentielle dans la reconnaissance faciale en raison de sa prévalence et de ses implications. Elle permet de prévenir les fraudes potentielles, telles que l'utilisation de visages falsifiés, qui pourraient compromettre la sécurité des données et les transactions financières. Une détection efficace renforce la confiance des utilisateurs en démontrant la fiabilité des systèmes de reconnaissance faciale, ce qui est crucial pour maintenir la satisfaction client et l'intégrité commerciale. En résumé, la détection précoce de la fraude garantit l'intégrité des systèmes de reconnaissance faciale et préserve la confiance des utilisateurs, contribuant ainsi à la protection des données et à une expérience utilisateur sécurisée.

VII.3 Règlement général sur la protection des données (RGPD)

Le Règlement général sur la protection des données (RGPD) est une législation de l'Union européenne qui vise à renforcer et à unifier la protection des données des individus au sein de l'UE. Entré en vigueur le 25 mai 2018, le RGPD établit des règles strictes concernant la collecte, le traitement et la conservation des données personnelles. Il accorde également aux individus un contrôle accru sur leurs propres données et renforce les obligations des organisations qui les traitent.
Le RGPD impose des principes fondamentaux de protection des données, tels que la nécessité d'obtenir un consentement explicite pour la collecte et l'utilisation des données, la limitation de la finalité du traitement des données, la minimisation des données collectées et la garantie de leur exactitude. De plus, il exige que les organisations mettent en place des mesures de sécurité appropriées pour protéger les données contre tout accès non autorisé ou toute divulgation.
Les entreprises et les organisations qui ne respectent pas les dispositions du RGPD peuvent être soumises à des amendes importantes, pouvant aller jusqu'à %4 du chiffre d'affaires annuel mondial ou 20 millions d'euros, selon le montant le plus élevé. Le RGPD a donc incité les entreprises du monde entier à revoir leurs pratiques de traitement des données et à renforcer leurs mesures de protection de la vie privée, afin de se conformer aux normes strictes établies par cette réglementation.

VIII Conclusion

Dans ce chapitre, nous avons exploré divers aspects de la biométrie, en mettant en lumière la reconnaissance faciale comme une modalité essentielle. Nous avons examiné son utilisation dans le contrôle d'accès, la surveillance et l'authentification individuelle. De plus, nous avons abordé les avantages de la reconnaissance faciale et

les éléments techniques essentiels. Enfin, nous avons survolé la sécurité numérique, incluant le cryptage et le RGPD, soulignant l'importance de la protection des données dans ces technologies.

CHAPITRE 2

SYSTÈME DE POINTAGE AUTOMATISÉ

"La patience est la clé du bonheur ; la pratique est la clé de la perfection. Si vous voulez comprendre quelque chose, soyez patient. Si vous voulez maîtriser quelque chose, pratiquez. Si vous voulez changer quelque chose, commencez par vous-même."

Chapitre 2. système de pointage automatisé

Après avoir examiné la littérature sur la reconnaissance faciale, nous entamons la mise en pratique des techniques étudiées dans le chapitre précédent en vue de développer notre système de pointage basé sur la reconnaissance faciale. Ce chapitre est dédié à la conception d'un tel système en utilisant la bibliothèque 'face_recognition'. Nous commençons par présenter les outils employés pour cette tâche, puis nous analysons les résultats des tests réalisés sur la base de données que nous avons constituée.

I Environnement matériel logiciel

Pour mettre en place un système de pointage basé sur la reconnaissance faciale, il est indispensable de prévoir à la fois un environnement matériel et logiciel adapté. Du côté matériel, des caméras de qualité sont essentielles pour capturer des images claires et précises des visages des utilisateurs, garantissant ainsi une reconnaissance fiable. Un dispositif informatique suffisamment puissant est également nécessaire pour le traitement en temps réel des données d'image, incluant la capacité de stockage adéquate pour gérer les informations biométriques collectées de manière sécurisée. Du point de vue logiciel, l'utilisation de bibliothèques robustes de reconnaissance faciale, comme face_recognition en Python, est cruciale. Ces bibliothèques facilitent non seulement la détection des visages, mais aussi l'encodage et la comparaison des caractéristiques faciales, assurant ainsi une identification précise et rapide des individus. En intégrant efficacement ces composants matériels et logiciels, un système de pointage de présence basé sur la reconnaissance faciale peut offrir une solution sûre, efficace et moderne pour la gestion de la présence dans divers environnements professionnels et institutionnels.

I.1 Configuration matérielle et logicielle

Pour ce qui est du côté matériel (hard), nous avons utilisé dans nos essais un PC avec la configuration suivante :

— Processeur Intel(R) Core(TM) i7-7820HQ CPU @ 2.90GHz
— Une mémoire vive d'une capacité de 16 GO.
— Une caméra « WebCam ».

Et pour ce qui est côté logiciel (Soft) :

— Système d'exploitation : Windows 10.
— Langage de programmation : Python.
— Visual studio code.

I.2 Langage de programmation

Le langage de programmation Python est reconnu pour sa simplicité et sa lisibilité, le rendant accessible tant aux débutants qu'aux experts. Conçu par Guido van Rossum et apparu en 1991, Python s'est rapidement imposé grâce à une syntaxe qui encourage un code clair et soigné. En tant que langage interprété, il permet une exécution rapide et interactive des scripts, ce qui le rend idéal pour le développement rapide de prototypes et d'applications.

Python est extrêmement polyvalent, utilisé dans divers secteurs tels que le développement web, l'analyse de données, l'intelligence artificielle et l'automatisation des tâches. Sa popularité est en grande partie due à sa bibliothèque standard étendue, qui offre une large gamme de fonctionnalités prêtes à l'emploi, et à sa vaste collection de modules tiers disponibles via des gestionnaires de paquets comme pip. Cela permet aux développeurs de créer rapidement des applications complexes sans avoir à réinventer la roue pour chaque fonctionnalité.

La communauté Python est également un atout majeur, avec des millions d'utilisateurs actifs qui contribuent à son développement et fournissent un soutien continu via des forums, des tutoriels et des ressources éducatives en ligne. Cette communauté dynamique favorise l'apprentissage collaboratif et la résolution rapide des problèmes.

Enfin, Python se distingue par sa capacité à s'intégrer facilement avec d'autres langages et outils, augmentant ainsi sa flexibilité et son efficacité dans différents contextes de développement. Des frameworks comme Django pour le développement web, des bibliothèques comme NumPy et Pandas pour l'analyse de données, et des outils d'apprentissage automatique comme TensorFlow et PyTorch témoignent de sa polyvalence et de sa robustesse dans des domaines variés de l'informatique moderne.

I.3 Environnement de programmation

Visual Studio Code, souvent appelé VS Code, est un éditeur de code source léger mais puissant créé par Microsoft. Depuis son lancement en 2015, il a rapidement acquis une grande popularité en raison de sa flexibilité et de ses nombreuses fonctionnalités.

VS Code supporte de nombreux langages de programmation grâce à ses extensions, offrant des outils pour l'écriture de code, le débogage et le contrôle de version avec Git intégré. Son interface utilisateur est extrêmement personnalisable, permettant aux développeurs de configurer l'éditeur selon leurs besoins spécifiques.

En outre, VS Code dispose d'une communauté active qui contribue régulièrement avec de nouvelles extensions et des améliorations continues. Des fonctionnalités telles qu'IntelliSense, qui propose des suggestions de code intelligentes en temps réel, et la collaboration via Live Share, qui permet de travailler ensemble sur du code en temps réel, rendent le développement plus efficace et agréable.

Un autre avantage majeur de VS Code est qu'il est gratuit et open-source, ce qui le rend accessible à tous les développeurs, indépendamment de leur plateforme ou de leurs besoins spécifiques en développement. Cela a contribué à son adoption massive dans la communauté des développeurs, aussi bien pour des projets personnels que professionnels.

I.4 Firebase Storage

Dans notre projet, nous avons opté pour Firebase afin de gérer les images et les informations de nos clients. Firebase, une plateforme de développement d'applications proposée par Google, offre une gamme complète de services pour le stockage et la gestion des données en temps réel. Voici les avantages de Firebase :

1. **Simplicité et Flexibilité :** Firebase propose une interface intuitive et des outils puissants, simplifiant ainsi le développement et la gestion des applications. Cette plateforme s'adapte à diverses exigences de projets, qu'il s'agisse d'applications web, mobiles ou autres.
2. **Stockage en Temps Réel :** Firebase permet de stocker et de récupérer des données en temps réel, garantissant ainsi que les informations des clients sont toujours à jour et facilement accessibles. Cette fonctionnalité est cruciale pour les applications nécessitant des mises à jour instantanées.
3. **Sécurité :** Firebase propose des fonctionnalités de sécurité robustes pour protéger les données sensibles des clients. Les règles de sécurité et les authentifications intégrées assurent un contrôle précis et sécurisé de l'accès aux données.

Pour gérer les images des clients, nous utilisons Firebase Storage, où les images sont téléchargées et stockées de manière sécurisée, recevant chacune une URL unique pour faciliter leur accès. Les informations des clients, telles que les noms, adresses et numéros de téléphone, sont quant à elles stockées dans Firebase Firestore ou Firebase Realtime Database. Ces données sont organisées de manière structurée, permettant une gestion et une manipulation simplifiées. Enfin, pour automatiser et gérer ces processus, nous avons développé des scripts Python qui interagissent directement avec Firebase, permettant ainsi une intégration fluide entre notre application et la plateforme Firebase.

II Face_recognition

Notre système de reconnaissance faciale repose sur le module développé par Adam Geitgey [15]. Cet algorithme suit un processus en plusieurs étapes pour identifier et authentifier les visages dans les images. Tout d'abord, il utilise des techniques avancées de détection de visage pour localiser précisément les visages dans une scène donnée. Ensuite, pour chaque visage détecté, l'algorithme extrait des caractéristiques faciales distinctives, telles que la position des yeux, du nez et de la bouche, ainsi que d'autres points clés significatifs. Ces caractéristiques sont ensuite encodées sous forme de vecteurs numériques, qui représentent de manière unique chaque visage.
Lors de la phase de reconnaissance, le système compare les vecteurs de caractéristiques extraits avec ceux stockés dans une base de données pour reconnaître les visages déjà enregistrés. Cette approche garantit une reconnaissance précise et rapide des individus, adaptée à une variété d'applications allant de la sécurité biométrique à la gestion des présences dans les organisations.

Enfin, grâce à cette technologie avancée, notre système renforce la sécurité et l'efficacité opérationnelle en permettant une gestion automatisée et précise des accès, tout en assurant la protection des données personnelles et la conformité aux normes de confidentialité.

II.1 La détection des visages dans une image

L'Histogramme des Orientations de Gradients (HOG) [17] est une technique de traitement d'image couramment utilisée pour la détection des objets, notamment dans la reconnaissance faciale. Cette méthode commence par la conversion des images en couleur en images en noir et blanc, simplifiant ainsi le processus d'analyse des gradients. Les gradients, qui représentent les variations d'intensité lumineuse dans l'image, sont calculés pour chaque pixel. Les directions et magnitudes des gradients sont alors analysées, les magnitudes étant particulièrement significatives autour des zones où l'intensité change brusquement, comme les bords et les coins. Ces régions sont riches en informations sur la forme de l'objet, en contraste avec les zones plus uniformes de l'image. Une fois les gradients calculés, ils sont regroupés en histogrammes selon leurs orientations dans de petites régions de l'image, appelées cellules. Ces histogrammes sont ensuite normalisés sur des blocs plus grands pour améliorer la robustesse aux variations d'éclairage et de contraste. La partie de l'image qui présente une distribution des directions des gradients la plus proche d'un modèle de visage HOG préalablement entraîné est alors identifiée et extraite, permettant de localiser et de reconnaître les visages avec une grande précision. Cette approche est efficace car elle met en évidence les contours et les structures principales du visage, qui sont des caractéristiques essentielles pour la reconnaissance faciale, tout en réduisant l'influence des variations locales de luminosité et des textures non pertinentes (voir Figure 2.1).

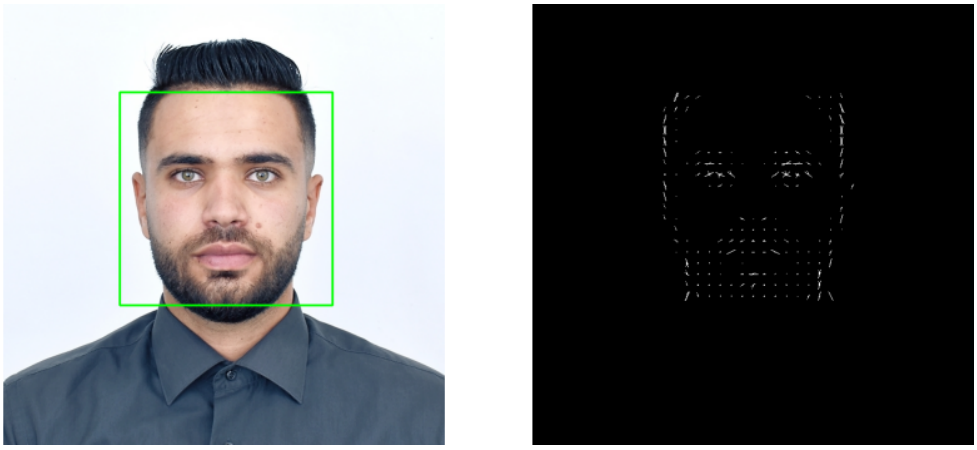

FIGURE 2.1 – Visualisation Du HOG

II.2 Positionnement du visage

Il existe 68 points de repère spécifiques sur un visage humain permettant de localiser les sourcils, les yeux, le nez, la bouche, etc. Ces repères, connus sous le nom de points de repère faciaux ou landmarks, sont essentiels dans diverses applications de traitement d'image et de vision par ordinateur. En marquant avec précision ces points sur différentes parties du visage, il devient possible de repositionner les visages dans des orientations variées. Cela permet de normaliser la position et l'alignement des visages, assurant que les traits clés, tels que les yeux et la bouche, se trouvent à peu près aux mêmes emplacements dans chaque image . Cette normalisation est cruciale pour des tâches telles que la reconnaissance faciale, où des comparaisons précises entre différentes images de visages sont nécessaires. En alignant les visages de manière cohérente, les algorithmes peuvent mieux discerner les caractéristiques distinctives de chaque individu, améliorant ainsi la précision de l'identification et de la vérification [22]. Les 68 points de repère sont également utilisés pour des applications telles que l'animation faciale, où ils permettent de créer des mouvements réalistes en suivant les expressions et les mouvements du visage humain de manière fidèle. En résumé, ces points de repère jouent un rôle fondamental dans l'analyse et la manipulation des images faciales, en facilitant des comparaisons et des transformations précises et cohérentes (voir Figure 2.2).

FIGURE 2.2 – 68 repere faciaux du visage

La technique d'alignement des visages de Kazemi et Sullivan [16] est utilisée à cette étape. Cette méthode est bien connue pour son efficacité et sa rapidité, permettant l'alignement des visages en temps réel en utilisant un ensemble d'arbres de régression pour localiser les points de repère faciaux. L'algorithme repose sur une cascade de régressions qui affine progressivement la position des points de repère, en commençant par une estimation initiale grossière et en apportant des ajustements de plus en plus précis à chaque étape. Pendant la phase d'entraînement, le modèle apprend à partir de nombreuses images annotées, et chaque arbre de régression est formé pour corriger les erreurs des prédictions précédentes. Cette approche en cascade permet de capturer les détails complexes de la structure faciale et d'assurer une localisation précise des points de repère même en présence de variations d'expression,

d'éclairage, et de position de la tête. L'efficacité de cette méthode est renforcée par la capacité des arbres de régression à effectuer des prédictions rapides avec un faible coût de calcul, permettant un traitement en temps réel souvent inférieur à une milliseconde par visage. Grâce à sa rapidité et à sa précision, la technique de Kazemi et Sullivan est largement adoptée dans diverses applications de reconnaissance faciale, de sécurité, et de réalité augmentée, où une localisation fiable et rapide des points de repère faciaux est cruciale pour le bon fonctionnement des systèmes. Cette méthode robuste offre une solution performante pour les besoins exigeants des applications modernes, assurant une grande fiabilité dans des conditions variées et imprévisibles (voir Figure 2.3).

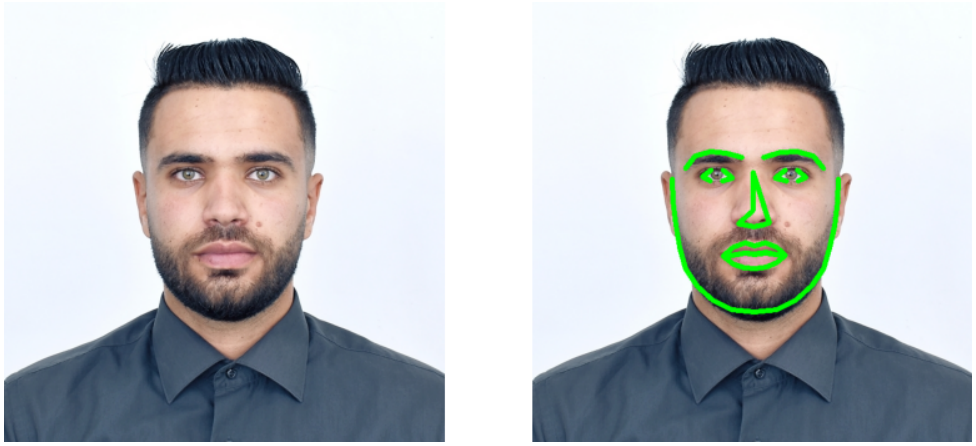

FIGURE 2.3 – Visage aligné avec la méthode Kazemi & Sullivan

II.3 Encodage du visage détecté

Après la détection des visages dans une image donnée, des caractéristiques faciales distinctives sont extraites pour identifier les visages. Il existe 128 mesures clés pour déterminer les caractéristiques faciales d'un visage [18]. Un réseau de convolution profonde a été entraîné pour optimiser directement le processus d'encodage [19]. La détection de similarité repose sur les vecteurs générés par le réseau. Deux images différentes du même visage produiront presque les mêmes vecteurs de 128 mesures clés.

Cette approche utilise des réseaux de neurones convolutifs (CNN) qui sont particulièrement efficaces pour traiter des données visuelles. Le réseau est entraîné sur une grande base de données d'images de visages, où il apprend à extraire des caractéristiques discriminatives de chaque visage, encapsulées dans un vecteur de 128 dimensions. Ce vecteur, souvent appelé "embedding", représente de manière compacte et informative les traits distinctifs d'un visage.

Lors de l'étape de comparaison, les vecteurs de deux images de visages sont comparés en utilisant une mesure de distance, telle que la distance euclidienne. Si les vecteurs sont proches l'un de l'autre, cela indique que les images proviennent probablement de la même personne. Cette méthode est non seulement précise mais aussi robuste face aux variations d'angles, d'éclairage et d'expressions faciales, ce qui

la rend très efficace pour la reconnaissance faciale dans des conditions réelles. En résumé, l'utilisation de réseaux de convolution profonde pour générer des vecteurs de 128 mesures clés permet une identification fiable et précise des visages, facilitant des applications telles que la sécurité biométrique, la gestion des identités et les interactions utilisateur personnalisées (voir Figure 2.4).

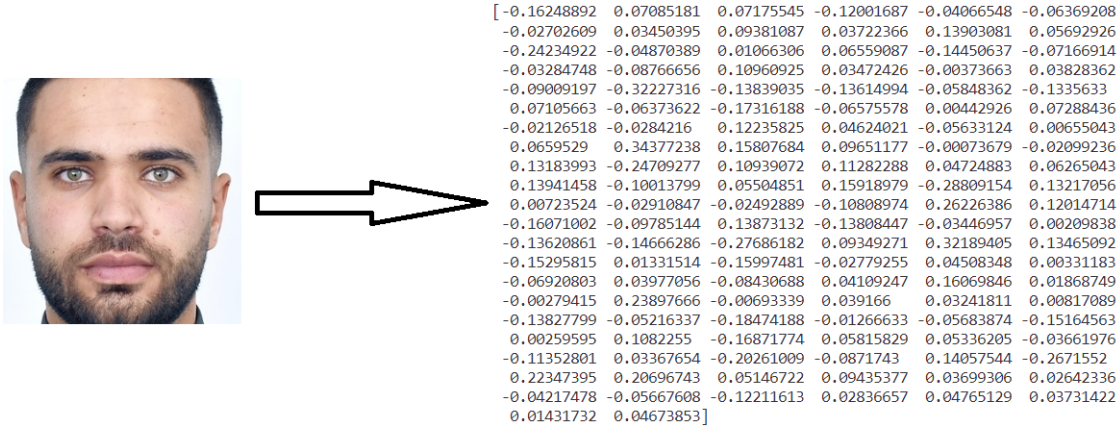

FIGURE 2.4 – Exemple de codage facial

II.4 Décision d'identification

La reconnaissance faciale est devenue une technologie cruciale dans de nombreux domaines, offrant des solutions pour la sécurité, la gestion des identités et même l'accès aux appareils électroniques. Lorsqu'il s'agit d'implémenter un système de reconnaissance faciale dans un environnement de travail, il est important de choisir la meilleure approche pour garantir des performances optimales.

Dans un lieu de travail complexe, où les conditions peuvent varier et où il peut y avoir un grand nombre de visages à traiter, le choix du bon algorithme de classification est crucial. Les classificateurs SVM linéaires sont souvent préférés pour leur rapidité dans le processus de reconnaissance faciale. Leur capacité à séparer efficacement les différentes classes de visages les rend idéaux pour des environnements où la vitesse de traitement est essentielle (voir Figure 2.5).

Cependant, dans des situations plus complexes où la reconnaissance doit être plus précise et robuste, les CNN (Réseaux de Neurones Convolutionnels) sont privilégiés. Les CNN sont capables d'apprendre des caractéristiques plus abstraites et complexes des visages, ce qui leur permet de mieux généraliser à des données plus variées et de fournir des résultats plus précis.

Ainsi, dans un environnement de travail complexe, il est souvent nécessaire de trouver un compromis entre la rapidité et la précision. Un simple classificateur SVM linéaire peut être utilisé pour les tâches de reconnaissance faciale nécessitant une réponse rapide, tandis que les CNN peuvent être déployés lorsque des performances plus précises sont requises, même si cela implique un temps de traitement plus long (voir Figure 2.6).

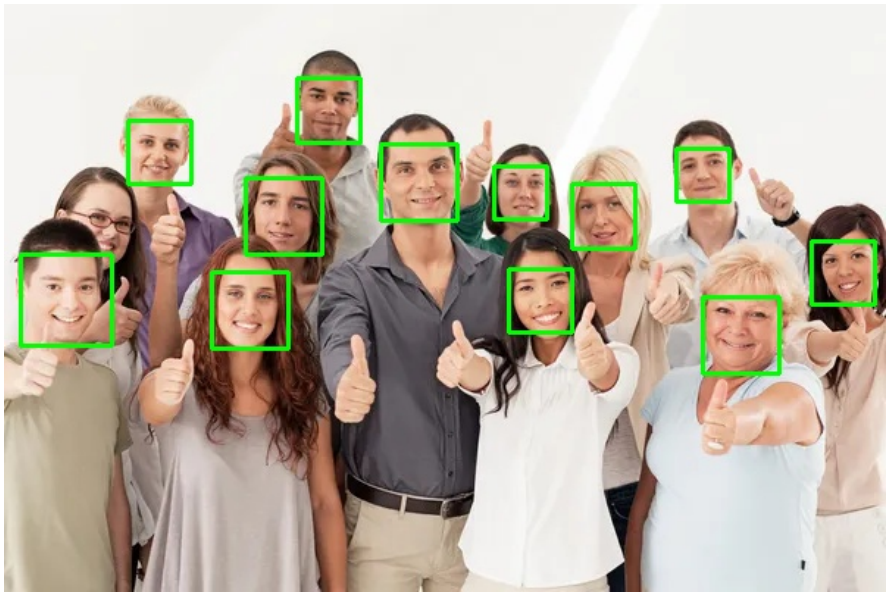

FIGURE 2.5 – Résultat avec SVM : un visage non détecté

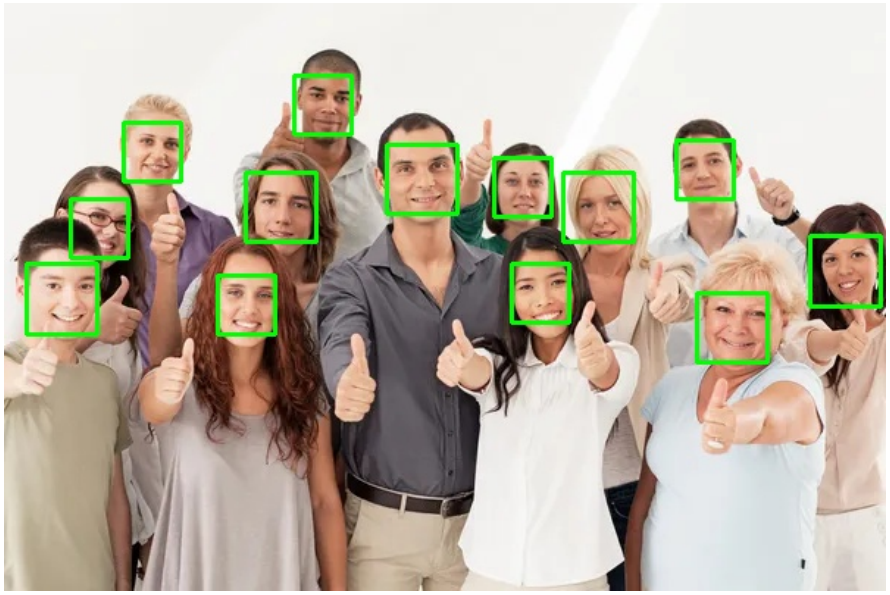

FIGURE 2.6 – Résultat avec CNN : tous les visages détectés

En fin de compte, le choix entre les classificateurs SVM linéaires et les CNN dépendra des besoins spécifiques de l'application, de la taille et de la complexité de la base de données de visages, ainsi que des contraintes de temps et de ressources du système de reconnaissance faciale. En comprenant les forces et les limites de chaque approche, il est possible de concevoir un système de reconnaissance faciale efficace et adapté aux besoins spécifiques du lieu de travail.

II.5 Enregistrement des résultats de présence

Après le processus de reconnaissance faciale, le système générera une feuille de présence au format CSV nommée par la date, qui comprendra les noms des personnes identifiées et les horaires. Cette feuille de présence servira à enregistrer de manière structurée les informations sur les personnes présentes à un moment donné, facilitant ainsi la gestion et le suivi des participants, que ce soit dans un cadre professionnel, académique ou événementiel.

Une autre feuille CSV sera également générée pour les personnes manquantes ou les visages non identifiés. Cette feuille aidera à signaler les anomalies ou les situations où la reconnaissance faciale n'a pas pu attribuer un nom à un visage détecté. Cela peut être dû à divers facteurs tels que la qualité de l'image, l'angle de la prise de vue, ou la présence de personnes non enregistrées dans la base de données.

Ces deux fichiers CSV permettent une gestion efficace de la présence et des exceptions lors de l'utilisation de systèmes de reconnaissance faciale, fournissant une traçabilité claire et un moyen de résoudre les incidents de manière rapide et précise.

III Présentation de l'application

Dans cette section, nous présenterons notre application, ses objectifs et son importance. Nous expliquerons comment la reconnaissance faciale peut être utilisée pour automatiser le pointage de présence, réduisant ainsi les erreurs et améliorant l'efficacité.

III.1 Installation

Dans le cadre de l'installation de notre système de pointage de présence basé sur la reconnaissance faciale, la bibliothèque face_recognition a été utilisée. L'installation de face_recognition a été réalisée en utilisant l'outil de gestion de paquets Python, pip. À travers la commande pip install face_recognition, la bibliothèque ainsi que ses dépendances nécessaires ont été téléchargées et installées de manière transparente. Une fois installée, face_recognition nous a fourni un ensemble d'outils puissants pour la détection et la reconnaissance faciale, simplifiant ainsi le processus de mise en place de notre système de pointage de présence. Cette étape d'installation a été cruciale pour garantir que notre système puisse fonctionner efficacement et accéder aux fonctionnalités avancées de la reconnaissance faciale offertes par la bibliothèque face_recognition.

L'utilisation de pip pour installer face_recognition a facilité l'intégration de cette technologie dans notre application, permettant une mise en œuvre rapide et efficace sans les complexités liées au développement de logiciels de reconnaissance faciale à partir de zéro. Cette approche a non seulement accéléré le déploiement de notre système, mais elle a également assuré une base solide en termes de performance et de fiabilité, essentielles pour un système de pointage de présence robuste et précis basé sur la reconnaissance faciale.

III.2 Configuration de la camera

La configuration de la caméra pour un système de pointage de présence basé sur la reconnaissance faciale est réalisée en suivant plusieurs étapes importantes, chacune utilisant la bibliothèque OpenCV.

1. **Installation de la bibliothèque OpenCV :** L'installation d'OpenCV est nécessaire pour fournir les fonctionnalités de vision par ordinateur requises.
2. **Accès à la caméra avec OpenCV :** La caméra est ouverte en utilisant OpenCV, identifiée par son ID, souvent 0 pour la caméra par défaut.
3. **Capture d'images en temps Réel :** La capture d'images ou de vidéos en temps réel est configurée via OpenCV, permettant le traitement de chaque cadre capturé par la caméra pour la reconnaissance faciale.
4. **Traitement des images :** Les images capturées sont traitées à l'aide de la bibliothèque face_recognition pour détecter les visages.
5. **Ajustement des paramètres de la caméra :** Les paramètres de la caméra tels que la résolution, la luminosité et le contraste sont ajustés pour garantir une reconnaissance faciale précise. OpenCV permet cette configuration pour améliorer la qualité des images.
6. **Gestion des erreurs et vérifications :** Des mécanismes de gestion des erreurs courantes, telles que l'incapacité d'accéder à la caméra ou des problèmes de capture d'image, sont implémentés. Cela assure un fonctionnement fluide et fiable du système.
7. **Intégration avec l'Interface Utilisateur :** Le flux vidéo capturé par la caméra est intégré dans l'interface graphique de l'application. Cela permet aux utilisateurs de visualiser le flux vidéo en temps réel et d'interagir avec le système de pointage de présence.
8. **Utilisation des caméras de surveillance :** Les caméras de surveillance peuvent remplacer l'utilisation de la caméra standard dans ce système. Les caméras de surveillance offrent généralement une couverture plus large, une meilleure qualité d'image et des capacités de capture en continu. Elles peuvent être intégrées au système de reconnaissance faciale via des flux vidéo IP, fournissant ainsi une alternative robuste et scalable à l'utilisation de caméras standard.

En suivant ces étapes, les caméras ou les caméras de surveillance sont configurées pour capturer et traiter des images en temps réel dans un système de pointage de présence basé sur la reconnaissance faciale, utilisant OpenCV. Cette configuration est essentielle pour garantir la précision et l'efficacité du système de reconnaissance faciale.

III.3 Base de données

Pour évaluer l'efficacité de notre système de pointage automatisé, nous avons constitué une base de données contenant une seule photo du visage de chaque individu parmi les 30 personnes. Chaque photo a été capturée de manière à représenter l'individu de façon claire et identifiable, sans tenir compte des différentes expressions faciales ou des angles de vue. Bien que chaque personne ait été photographiée dans des conditions d'éclairage diverses, la variété d'expressions faciales et d'angles de vue n'a pas été prise en compte dans cette base de données. Cela a été fait dans le but de simplifier la tâche d'évaluation du système de reconnaissance faciale en se concentrant sur l'identification précise des visages plutôt que sur la variabilité des expressions ou des angles.

L'objectif principal de cette base de données est de mesurer la précision du système de reconnaissance faciale. En analysant les résultats obtenus, nous pouvons identifier les points forts et les faiblesses du système. Par exemple, nous pourrions évaluer si le système est capable de distinguer les visages similaires, de gérer les variations de lumière ou de reconnaître un individu malgré des expressions faciales changeantes. Ces tests permettent également de vérifier la robustesse du système face à des perturbations mineures comme le port de lunettes ou des modifications capillaires.

Grâce à cette base de données, nous pouvons ajuster les paramètres du système pour améliorer ses performances, réduire les taux de fausses reconnaissances et minimiser les erreurs de non-reconnaissance. Cette phase de test est essentielle pour s'assurer que le système de reconnaissance faciale est fiable et efficace avant son déploiement dans des applications réelles. Les applications potentielles incluent la sécurité, l'authentification des utilisateurs et d'autres services nécessitant une identification précise et rapide des individus. En somme, cette base de données joue un rôle crucial dans le développement et l'optimisation de la technologie de reconnaissance faciale.

III.4 Générateur d'Encodage

Dans la section "Générateur d'Encodage" de notre projet de système de pointage de présence basé sur la reconnaissance faciale, nous avons développé un processus essentiel pour convertir les images des utilisateurs en encodages faciaux numériques. En utilisant la bibliothèque face_recognition, nous avons mis en place un générateur d'encodage en plusieurs étapes :

1. **Prétraitement des Images :** Les images des utilisateurs sont prétraitées pour garantir une qualité optimale, incluant redimensionnement et normalisation.
2. **Détection des Visages :** L'algorithme de détection de visages (face_recognition) localise les visages dans les images, une étape cruciale pour extraire les caractéristiques faciales pertinentes.
3. **Encodage des Visages :** Chaque visage détecté est encodé pour créer une représentation numérique de ses caractéristiques faciales uniques.

4. **Stockage des Encodages :** Les encodages faciaux sont stockés dans une base de données ou un fichier, prêts à être utilisés pour la reconnaissance faciale ultérieure.

Le générateur d'encodage assure la conversion précise des images en données numériques exploitables pour l'identification des utilisateurs dans notre système de pointage de présence. Cela garantit également la confidentialité des utilisateurs, car seules les caractéristiques faciales encodées sont stockées.

III.5 Intégration des Données Utilisateur dans notre Système de Pointage

En complément de la base de données d'images des utilisateurs, nous avons conçu un code Python permettant aux administrateurs de saisir les informations essentielles pour chaque utilisateur. Ces données sont ensuite sauvegardées dans une seconde base de données, hébergée soit sur un serveur distant tel que Firebase, soit localement, selon la préférence du client. Les champs intégrés dans ce code incluent :

1. **Nom Complet :** Le nom complet de l'utilisateur.
2. **Identifiant :** Un identifiant unique attribué à chaque utilisateur, tel qu'un numéro d'employé ou d'étudiant.
3. **Spécialité :** La discipline ou le domaine d'étude de l'utilisateur, par exemple "Informatique" ou "Biologie".
4. **Photo de l'Utilisateur :** Une image de l'utilisateur utilisée pour générer son encodage facial.
5. **État :** La situation actuelle de l'utilisateur, par exemple étudiant doublant ou non.
6. **Niveau :** Le statut ou le niveau de l'utilisateur dans le système, par exemple "2ème année" ou "Employé senior".
7. **Année de la Première Inscription :** L'année où l'utilisateur a initialement rejoint l'établissement.
8. **Nombre Total d'Assistance :** Le nombre total de fois où l'utilisateur a été détecté par la caméra.

Toutes ces données sont intégrées dans notre interface de pointage, offrant la flexibilité d'utiliser l'ensemble complet d'informations ou de sélectionner uniquement celles pertinentes en fonction des besoins spécifiques et des préférences du client.

III.6 Interfaces graphique

Dans la section "Graphiques" de notre projet de système de pointage de présence basé sur la reconnaissance faciale, nous avons introduit une interface graphique utilisateur élégante. L'objectif principal de cette étape était de fournir aux utilisateurs une expérience conviviale et intuitive lors de l'interaction avec notre système.

La création de l'interface graphique nous a permis d'intégrer plusieurs fonctionnalités clés :

1. **Visualisation du Flux Vidéo :** Nous avons intégré le flux vidéo en direct de la webcam ou de la caméra de surveillance dans l'interface utilisateur. Cela permet aux utilisateurs de voir en temps réel les visages détectés par le système.
2. **Affichage des Informations de Présence :** Des zones dédiées dans l'interface affichent les informations de présence telles que l'état (présent ou absent) et l'heure d'entrée/sortie.
3. **Interaction Utilisateur :** Des éléments interactifs tels que des boutons ont été ajoutés pour permettre aux utilisateurs de marquer leur présence, de mettre à jour leurs informations personnelles ou de télécharger des données.
4. **Notifications et Messages d'Erreur :** Des fonctionnalités sont incluses pour afficher des notifications et des messages d'erreur, assurant ainsi une expérience utilisateur transparente et informative.

De plus, pour rendre notre système plus accessible, nous avons développé une interface utilisateur multilingue. Disponible en trois langues - arabe, français et anglais - cette fonctionnalité permet aux utilisateurs de choisir la langue de leur choix, offrant ainsi une expérience personnalisée et intuitive.
L'intégration de cette fonctionnalité multilingue améliore considérablement l'accessibilité et l'expérience utilisateur pour une base d'utilisateurs diversifiée. En offrant la possibilité de sélectionner la langue préférée, nous nous assurons que chaque utilisateur peut interagir avec le système dans la langue avec laquelle il est le plus à l'aise, facilitant ainsi la compréhension et l'utilisation du système.
Nos interfaces sont disponibles en deux versions : une version basique et une version professionnelle.

III.6.1 Mode basique

Dans ce mode, le système fonctionne de manière autonome, indépendamment de toute connexion Internet active. Il s'appuie sur une base de données locale pour l'ensemble de ses opérations. Ainsi, toutes les informations d'identification et de traitement des données sont stockées directement sur le périphérique ou le serveur local où le système est déployé. Cette approche garantit la sécurité et la confidentialité des données, car toutes les informations sensibles restent à l'abri localement.
L'absence de dépendance à une connexion Internet assure la continuité du service, même en cas de panne réseau. Cette configuration est particulièrement avantageuse dans des environnements où l'accès à Internet est limité ou intermittent, ou lorsque la confidentialité des données est une priorité essentielle. En stockant les données localement, le système réduit également les risques de cyberattaques et de violations de données potentielles liées à la transmission d'informations sur le réseau. Voici comment fonctionne le mode basique :

1. **Système en état actif**

Dans cet état, notre système de pointage opère en mode de repos (voir Figure 2.7), également connu sous le nom de boucle fermée. Il surveille activement son environnement, prêt à détecter un événement ou une condition spécifique. Pendant

cette phase, le système demeure vigilant, utilisant sa caméra de surveillance pour observer en permanence l'environnement sans entreprendre d'actions visibles. Cette surveillance active lui permet de réagir instantanément dès qu'il détecte la présence d'une personne à proximité.

Ce mode est crucial pour notre système de pointage, car il nécessite une réponse rapide et précise à des stimuli spécifiques, tels que l'arrivée d'un employé ou d'un étudiant. En restant en veille mais attentif, le système garantit une efficacité énergétique tout en étant prêt à activer ses fonctionnalités principales dès qu'une condition prédéfinie, comme le passage d'une personne, est détectée.

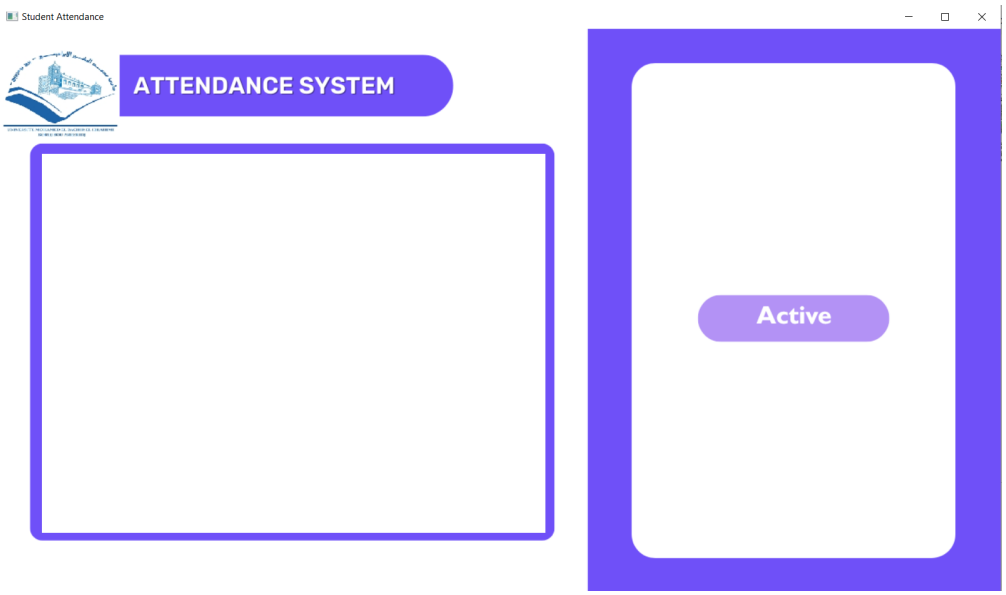

FIGURE 2.7 – Mode basique : système en état actif

2. **Système en état d'identification**

Lorsque le système est déclenché par le passage d'une personne, il entre dans un état d'identification (voir Figure 2.8). Les données capturées par la caméra de surveillance sont traitées par la bibliothèque face_recognition. Ensuite, le système compare les informations obtenues avec celles stockées dans sa base de données locale. Si une correspondance est trouvée, le système passe à l'étape suivante, indiquant que la personne est identifiée comme étant présente dans la base de données et autorisée à accéder au système ou à effectuer d'autres actions spécifiées, telles que l'ouverture d'une porte ou l'enregistrement de sa présence. En revanche, si aucune correspondance n'est trouvée, le système reste en mode veille en attendant la prochaine interaction, ou peut déclencher une alerte ou un protocole de sécurité pour gérer la présence non reconnue.

3. **Fin d'identification et marqué avec succès**

Lorsque le système est déclenché par le passage d'une personne, il entre dans un état d'identification. Les données capturées par la caméra de surveillance sont traitées

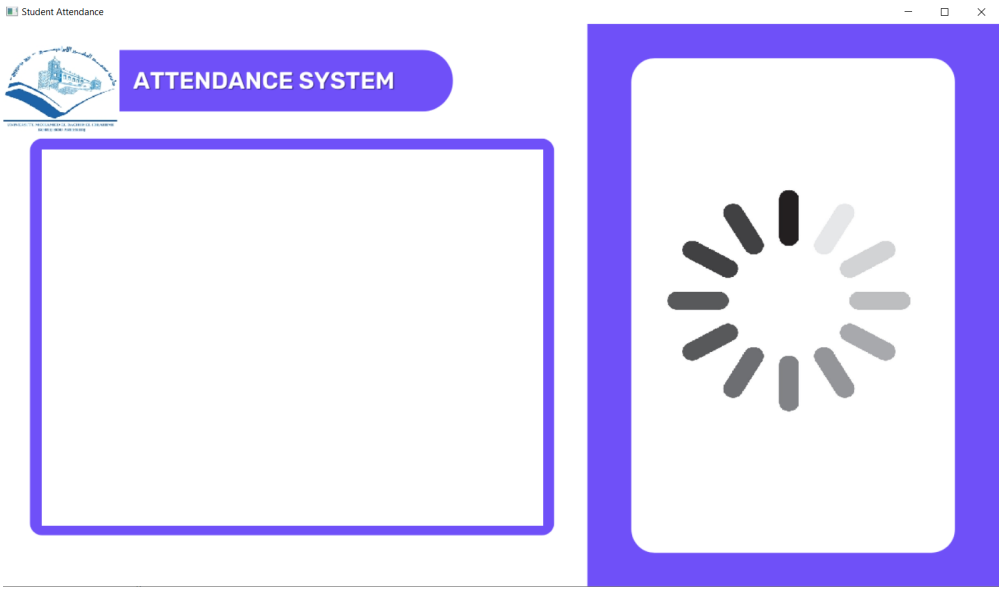

FIGURE 2.8 – Mode basique : système en état d'identification

par la bibliothèque face_recognition. Ensuite, le système compare les informations obtenues avec celles stockées dans sa base de données locale. Si une correspondance est trouvée, le système passe à l'étape suivante, indiquant que la personne est identifiée comme étant présente dans la base de données et autorisée à accéder au système ou à effectuer d'autres actions spécifiées, telles que l'ouverture d'une porte ou l'enregistrement de sa présence. En revanche, si aucune correspondance n'est trouvée, le système reste en mode veille en attendant la prochaine interaction, ou peut déclencher une alerte ou un protocole de sécurité pour gérer la présence non reconnue (voir Figure 2.9).

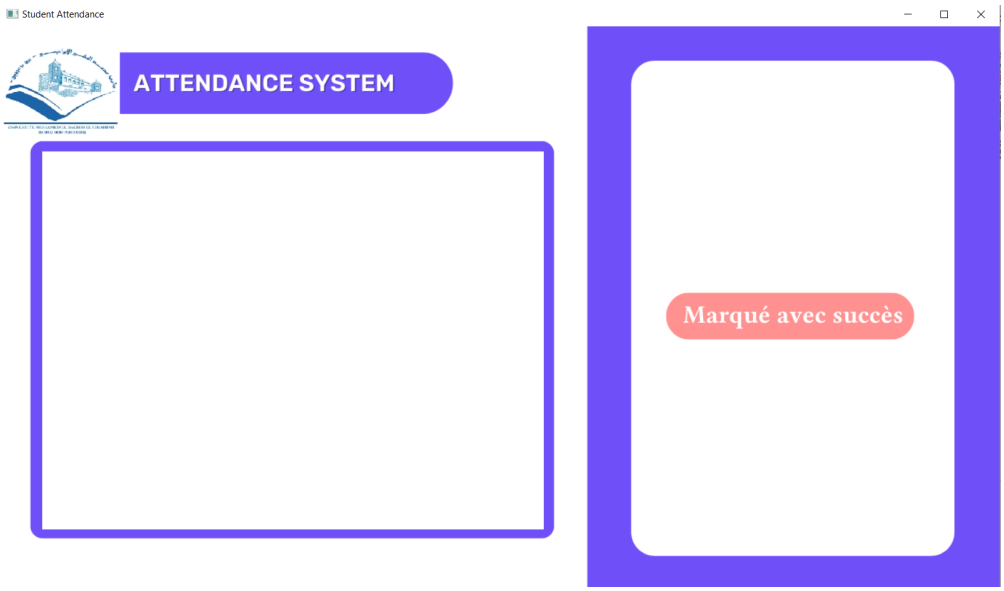

FIGURE 2.9 – Mode basique : système en phase finale d'identification

III.6.2 Mode professionnel

Dans le mode professionnel, le système utilise Firebase pour le stockage sécurisé et évolutif des données d'identification et de traitement, contrairement au stockage local du mode basique. Cette intégration permet une gestion dynamique des données en temps réel sur plusieurs appareils, avec des fonctionnalités avancées comme l'authentification des utilisateurs, la gestion des autorisations et des règles de sécurité flexibles. Idéal pour les entreprises, ce mode offre une gestion centralisée, une évolutivité facile et une sécurité renforcée, tout en exploitant les analyses en temps réel, les notifications push et l'apprentissage automatique pour des applications innovantes. Voici comment fonctionne le mode professionnel :

1. **Système en état actif**

Dans cette phase, le mode professionnel fonctionne de manière analogue au mode basique, fournissant une surveillance active et des capacités de traitement des données avancées. Grâce à cette surveillance constante, le système peut réagir rapidement et de manière adaptative à diverses situations et stimuli, ce qui en fait une solution complète adaptée aux environnements professionnels les plus exigeants. En exploitant des techniques d'analyse sophistiquées et en s'intégrant parfaitement à Firebase, le mode professionnel garantit une réactivité améliorée et une efficacité opérationnelle optimale. Il offre ainsi des fonctionnalités avancées pour une gestion de données de haut niveau et une performance optimisée dans une variété d'applications professionnelles (voir Figure 2.10).

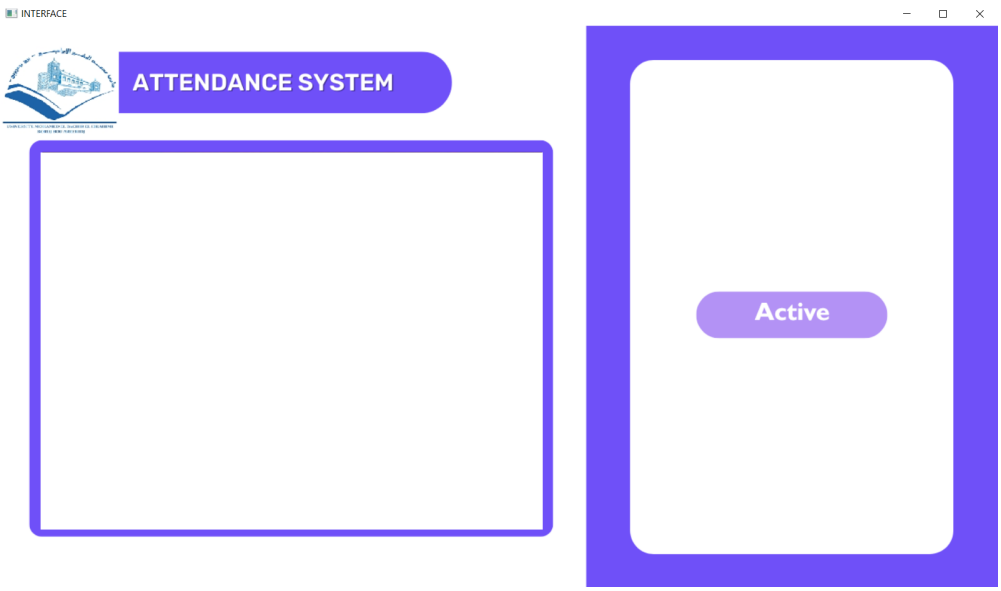

FIGURE 2.10 – Mode professionnel : système en état actif

2. **Système en état d'identification**

Lorsque le système détecte la présence d'un individu, il entre dans une phase d'identification. Les données visuelles capturées par la caméra de surveillance sont analysées à l'aide de la bibliothèque face_recognition. Par la suite, ces informations sont

comparées à celles stockées dans la base de données distante hébergée sur Firebase. Lorsqu'une correspondance est établie, le système affiche les informations de l'utilisateur sur l'interface. Les informations affichées peuvent inclure le nom de l'utilisateur, son identifiant, ainsi que d'autres données pertinentes pour assurer une identification précise et rapide (voir Figure 2.11).

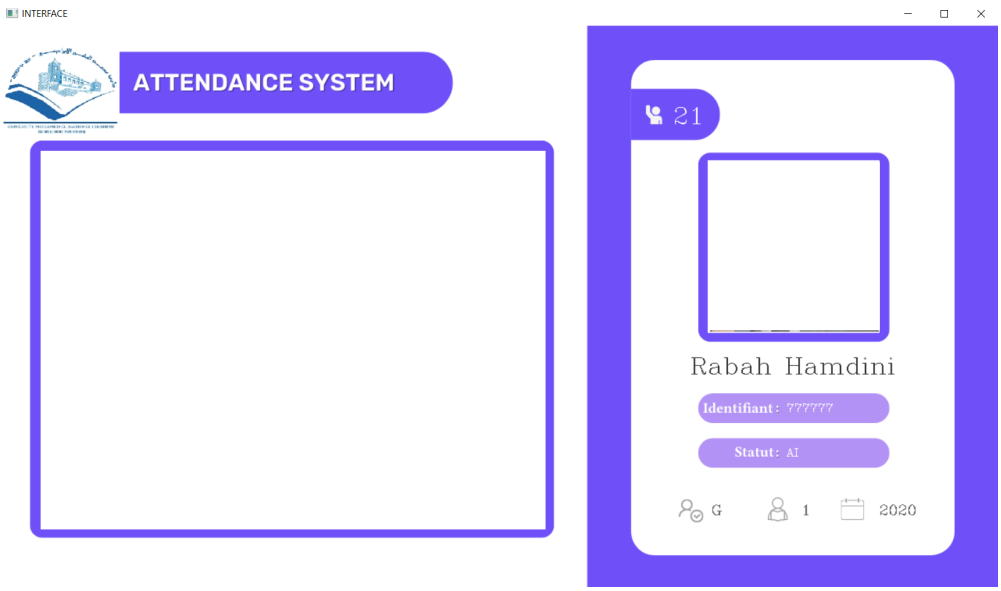

FIGURE 2.11 – Mode professionnel : système en phase d'identification

L'ensemble des informations possibles sont les suivantes (voir Figure 2.12) :

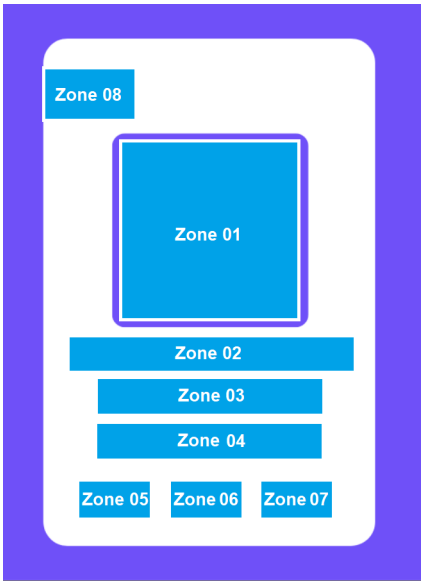

FIGURE 2.12 – Présentation des zones du mode professionnel

- **L'image (zone 01) et le nom (zone 02) et de la personne :** Lorsqu'on parle de "Nom et l'image de la personne", cela fait référence à l'affichage conjoint du nom d'une personne ainsi que de son image. Cette pratique est essentielle dans les systèmes de sécurité et d'identification pour plusieurs raisons. Tout d'abord, l'image fournit une représentation visuelle claire de l'utilisateur, ce qui permet une identification rapide et intuitive. Ensuite, le nom associé à cette image offre une identification précise et permet de confirmer l'identité de manière plus détaillée, notamment en cas de doute ou de besoin de vérification.
  Cette combinaison de nom et d'image joue un rôle crucial dans la sécurité des zones restreintes, car elle permet aux responsables de sécurité de vérifier visuellement l'identité des individus autorisés. En affichant à la fois le nom et l'image, les systèmes peuvent faciliter l'identification des personnes autorisées à accéder à des zones sécurisées, renforçant ainsi la sécurité globale du lieu. Cela permet également de suivre et de tracer plus efficacement les entrées et sorties, contribuant ainsi à la gestion efficace des accès et à la sécurité générale des installations.

- **L'identifiant (Zone 03) :** L'identifiant joue un rôle crucial dans la gestion sécurisée des accès aux zones restreintes. Il permet d'attribuer de manière unique une identification à chaque utilisateur ou dispositif autorisé. Cette attribution facilite non seulement le contrôle des accès en garantissant que seules les personnes ou les équipements autorisés entrent dans les zones sécurisées, mais elle permet également une surveillance continue et une traçabilité des activités.
  Grâce à un identifiant spécifique, les systèmes de sécurité peuvent suivre et enregistrer les mouvements des utilisateurs et des dispositifs, assurant ainsi une gestion efficace des accès. Cette traçabilité est essentielle pour les audits de sécurité, permettant de vérifier qui a accédé à quelles zones et à quel moment. De plus, l'utilisation d'identifiants aide à maintenir l'intégrité des politiques de sécurité en place, en assurant que seules les personnes autorisées interagissent avec les ressources sensibles ou restreintes.

- **Le Statut (Zone 04) :** Le "statut" d'un utilisateur se réfère au niveau d'autorisation spécifique attribué à cette personne pour accéder à une zone déterminée. Ce statut est déterminé en fonction de divers critères tels que le rôle occupé dans l'organisation, l'historique des accès précédents, et les politiques de sécurité actuellement en vigueur.
  En attribuant un statut précis à chaque utilisateur, les responsables de sécurité peuvent garantir que les accès aux zones sensibles sont strictement contrôlés et conformes aux règles établies. Par exemple, un statut peut déterminer si un utilisateur a des autorisations élevées pour accéder à des informations confidentielles ou à des équipements critiques, ou s'il est restreint à des zones spécifiques en fonction de son rôle ou de ses besoins opérationnels.
  La gestion efficace du statut d'utilisateur est essentielle pour assurer la sécurité

globale des installations et pour répondre aux exigences de conformité. Cela permet également de simplifier la surveillance et la gestion des autorisations d'accès, garantissant ainsi une utilisation sécurisée et appropriée des ressources de l'organisation.
Dans le contexte d'un système de gestion de présence universitaire, le "statut" peut effectivement se référer à la spécialité ou au domaine d'étude de l'étudiant. Par exemple, un étudiant peut être inscrit dans une spécialité comme "Informatique" ou "Biologie". Ce statut spécifie le domaine académique dans lequel l'étudiant est actif et pour lequel il suit des cours et des activités universitaires.

– **Majeur Professionnel (Zone 05) :** c'est un terme désignant différents niveaux de privilèges accordés à des utilisateurs au sein d'une organisation. Voici ce que cela pourrait signifier :
• Niveau d'accès élevé : Cela concerne les utilisateurs qui ont des droits étendus pour accéder à des informations sensibles ou à des zones restreintes, nécessitant une sécurité renforcée et des protocoles stricts.
• Responsabilités spécifiques : Ces autorisations permettent à l'utilisateur de prendre des décisions critiques ou de gérer des tâches complexes nécessitant une expertise avancée. Cela peut inclure la supervision de projets stratégiques ou l'analyse de données cruciales.
• Rôle de supervision : Ce statut indique que l'utilisateur supervise ou gère d'autres utilisateurs ou processus au sein de l'environnement sécurisé. Cela implique une responsabilité accrue dans la gestion opérationnelle et la sécurité des informations.
• Accès à des ressources critiques : Cela désigne la capacité de l'utilisateur à interagir avec des équipements ou des informations essentielles pour le bon fonctionnement sécurisé de l'organisation. Il peut s'agir notamment d'accéder à des bases de données sensibles ou à des systèmes de contrôle vitaux.
Dans le contexte d'un système de gestion de présence universitaire, la zone 05 indique la situation actuelle de l'utilisateur, par exemple s'il est étudiant régulier ou doublant.

– **Le Classement Professionnel (Zone 06) :** fait référence à la classification des individus selon leur niveau professionnel ou leur rang au sein d'une organisation. Cela englobe plusieurs aspects importants :
• Hiérarchie organisationnelle : Il désigne la position d'un individu dans la structure hiérarchique de l'entreprise, souvent en relation avec son niveau de responsabilité et d'autorité.
• Niveau de compétence : Cela peut se référer au niveau de compétence, d'expertise ou de spécialisation d'un individu dans un domaine spécifique.
• Grade ou titre professionnel : Cela inclut des titres officiels ou des grades attribués en fonction des réalisations professionnelles, de l'expérience et des qualifications.
• Autorisations et accès : Cela peut influencer les droits d'accès aux informations sensibles, aux installations sécurisées ou aux décisions stratégiques au

sein de l'organisation.

Dans le contexte d'un système de gestion de présence universitaire, la Zone 06 désigne le statut ou le niveau de l'utilisateur, faisant référence à sa position ou à son niveau dans le système. Par exemple, cela pourrait être "2ème année" pour un étudiant ou "Employé senior" pour un membre du personnel.

- **L'Année de la Première Inscription (Zone 07) :** se réfère à l'année à laquelle un utilisateur a commencé à bénéficier d'autorisations d'accès spécifiques à certaines zones. Cette information revêt une importance capitale pour plusieurs raisons essentielles :
  • Suivi de l'ancienneté : Permet de mesurer la durée pendant laquelle l'utilisateur est autorisé à accéder aux zones sécurisées, ce qui est pertinent pour les politiques de renouvellement ou de révision des autorisations.
  • Historique des accès : Fournit un contexte sur la période durant laquelle l'utilisateur a eu accès, ce qui aide à évaluer son expérience et sa familiarité avec les procédures et les protocoles de sécurité en place.
  • Gestion des autorisations : Facilite la gestion et la révision périodique des autorisations en fonction de l'ancienneté de l'utilisateur et de la continuité des besoins d'accès.
  • Analyse et rapports : Utilisée pour générer des rapports d'audit et d'analyse sur l'utilisation des installations sécurisées au fil du temps, contribuant ainsi à une gestion efficace des ressources et des infrastructures.

- **Fréquentation Totale (Zone 08) :** Cette zone désigne le nombre global de visites ou d'accès effectués par un utilisateur spécifique aux zones sécurisées sur une période donnée. Cette mesure revêt une importance cruciale pour plusieurs raisons :
  • Surveillance de l'utilisation des installations : Permet de suivre combien de fois un utilisateur accède aux zones sécurisées, offrant ainsi une indication de l'utilisation réelle des infrastructures sécurisées.
  • Analyse de la fréquence d'accès : Aide à évaluer à quelle fréquence un utilisateur a besoin d'accéder aux zones sécurisées, ce qui est essentiel pour optimiser les ressources et les procédures de sécurité.
  • Audit et conformité : Contribue à la génération de rapports d'audit précis et à la vérification de la conformité aux politiques de sécurité en enregistrant toutes les interactions de l'utilisateur avec les zones sécurisées.
  • Gestion des autorisations : Peut être utilisée pour ajuster les niveaux d'autorisation en fonction de l'utilisation réelle et des besoins de l'utilisateur, garantissant ainsi une sécurité adaptative et efficace.
  • Détection d'anomalies : Permet de repérer toute activité inhabituelle ou anormale en comparant la fréquentation attendue à celle réellement observée, renforçant ainsi la détection des tentatives d'accès non autorisées.

3. **Mode déjà marqué**

Le "mode déjà marqué" est une fonctionnalité cruciale de notre système de pointage

de présence, conçue pour adresser les potentielles lacunes et prévenir les fraudes. Lorsqu'un utilisateur tente de pointer plusieurs fois à des horaires incompatibles avec les règles établies, le système identifie cette tentative comme un marquage déjà effectué. Cette fonctionnalité vise spécifiquement à prévenir les fraudes telles que le marquage multiple pour la même période de présence.
Une fois qu'une tentative de marquage déjà effectué est détectée, le système réagit en déclenchant diverses actions. Ces actions peuvent inclure l'affichage immédiat d'une alerte pour l'administrateur, le rejet automatique de la marque supplémentaire, ou encore une action corrective automatisée comme la mise en attente du marquage jusqu'à ce qu'il soit vérifié manuellement par un administrateur (voir Figure 2.13).
En intégrant cette fonctionnalité, notre système renforce significativement sa fiabilité en réduisant les risques d'erreurs ou de fraudes associées aux données de présence. Cela permet une gestion précise et efficace des données de présence, assurant ainsi l'intégrité et la crédibilité des informations collectées et utilisées par l'organisation.

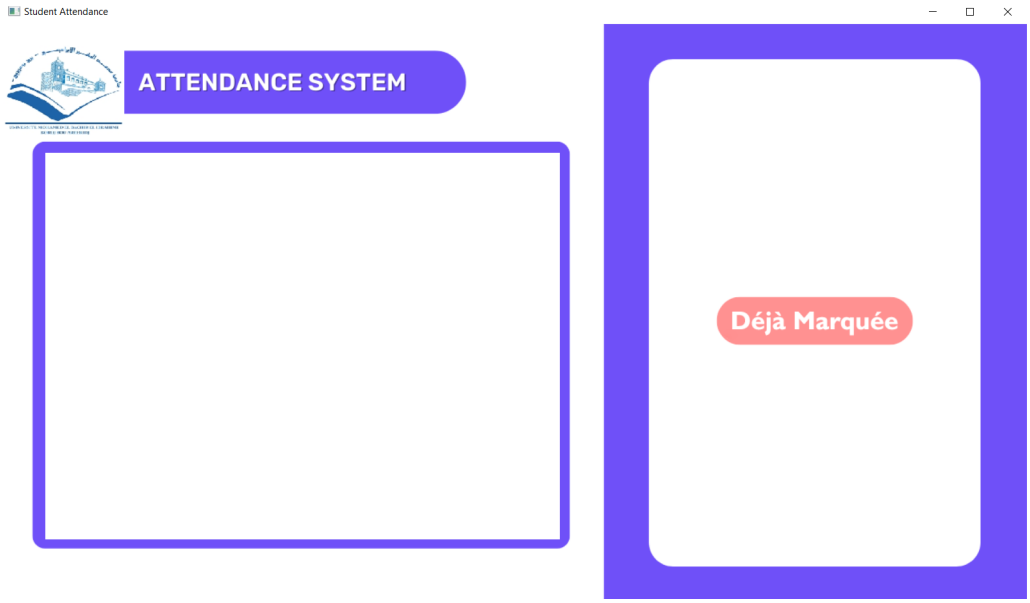

FIGURE 2.13 – Mode Professionnel : Système en Mode Déjà Marqué

IV Résultat est discutions

Le taux de reconnaissance de notre système de reconnaissance faciale atteint 99.38 %, comparable à celui de la bibliothèque face_recognition. Cette performance a été vérifiée par plusieurs ouvrages scientifiques, confirmant ainsi la fiabilité et la précision de notre technologie [23, 24, 25, 26]. Ces résultats soulignent l'efficacité de notre système dans l'identification précise des individus, ce qui en fait une solution robuste pour une variété d'applications, allant de la gestion des présences à la sécurité des accès.

Le nombre total d'assistances joue un rôle crucial dans la détection des tentatives de fraude dans le processus de pointage. En enregistrant le nombre de fois où un

individu est capté par la caméra, ce paramètre offre une mesure fiable de la fréquence à laquelle chaque utilisateur interagit avec le système. En comparant ce nombre aux attentes normales, telles que les heures de travail ou les horaires de cours, les anomalies peuvent être détectées. Par exemple, une fréquence anormalement élevée ou faible d'assistance pour un utilisateur particulier peut indiquer des comportements frauduleux, tels que la falsification des heures de travail ou le contournement du système de pointage. De même, des variations soudaines ou inhabituelles dans le nombre total d'assistances pour un groupe d'utilisateurs peuvent signaler des problèmes systémiques ou des tentatives de manipulation. Ainsi, en surveillant attentivement le nombre total d'assistances, le système de pointage peut identifier et prévenir efficacement les fraudes, garantissant ainsi l'intégrité et la fiabilité du processus de suivi de la présence.

La détection de fraude peut être réalisée soit manuellement, en vérifiant les enregistrements vidéo captés par la caméra, soit automatiquement, grâce à la génération d'alertes par le système en cas d'un nombre inhabituel d'assistances. Dans le premier cas, les administrateurs ou le personnel de sécurité peuvent examiner les enregistrements vidéo pour identifier toute activité suspecte, telle que des comportements incohérents ou des mouvements anormaux. Cette méthode nécessite une surveillance humaine régulière et peut être sujette à des erreurs ou à des retards dans la détection des fraudes. En revanche, dans le cas de la détection automatique, le système peut être configuré pour analyser en temps réel le nombre total d'assistances enregistrées pour chaque utilisateur. Lorsqu'un nombre inhabituel est détecté, dépassant un seuil prédéfini, le système déclenche automatiquement une alerte. Cette alerte peut prendre la forme d'une notification envoyée aux administrateurs du système ou d'une action automatique, telle que la suspension temporaire des privilèges d'accès de l'utilisateur concerné. Cette approche automatique permet une réponse rapide et proactive aux tentatives de fraude, minimisant ainsi les risques et garantissant l'intégrité du processus de pointage de présence.

La reconnaissance faciale présente plusieurs avantages en termes de contrôle d'accès. Elle fluidifie la circulation en permettant un flux continu et sans interruption, évitant ainsi les embouteillages aux points de contrôle. Elle permet aux utilisateurs d'accéder aux installations rapidement et efficacement, sans nécessiter de badges ou autres moyens d'identification. En éliminant les risques liés au partage ou à la perte de badges d'accès, elle renforce la sécurité. De plus, contrairement à d'autres solutions biométriques, la reconnaissance faciale ne nécessite aucun contact physique, réduisant ainsi les risques de contamination et augmentant le confort des utilisateurs.

En intégrant ces avantages, notre système de reconnaissance faciale assure non seulement une identification précise et fiable, mais il améliore également de manière significative l'expérience utilisateur. La fluidité de circulation offerte par notre système de reconnaissance faciale élimine les embouteillages aux points de contrôle, permettant aux utilisateurs de se déplacer sans interruption ni délai. Cela est particulièrement bénéfique dans des environnements à fort flux, comme les entreprises, les établissements éducatifs ou les événements publics, où chaque seconde gagnée peut contribuer à une meilleure gestion du temps et à une réduction du stress lié aux attentes.

De plus, l'accès rapide en tout temps que permet notre système de reconnaissance faciale supprime la nécessité de badges ou autres moyens d'identification physique. Les utilisateurs n'ont plus à s'inquiéter de perdre ou d'oublier leurs badges d'accès, ce qui simplifie leur quotidien et réduit les coûts et les efforts liés à la gestion des cartes d'accès. Cette automatisation et cette simplification du processus d'entrée renforcent également la sécurité, car elles empêchent le partage non autorisé de badges, une pratique courante qui peut compromettre la sécurité des installations.

Notre système de reconnaissance faciale n'exige aucun contact physique avec les dispositifs de contrôle, contrairement à d'autres solutions biométriques comme les empreintes digitales. Cela non seulement améliore l'hygiène, particulièrement important dans les contextes de santé publique et de prévention des maladies, mais aussi accroît le confort des utilisateurs en évitant le besoin de toucher des surfaces communes. Cette caractéristique sans contact est cruciale dans des lieux tels que les hôpitaux, les laboratoires, les cuisines, et toute autre installation où la propreté et l'hygiène sont prioritaires.

En termes de sécurité, notre système de reconnaissance faciale offre un niveau de protection inégalé. La technologie est capable de détecter et de prévenir les tentatives de fraude, telles que l'usurpation d'identité ou la falsification des heures de travail. Grâce à la surveillance en temps réel et aux alertes automatiques en cas de comportements suspects, les administrateurs peuvent réagir rapidement et efficacement pour maintenir la sécurité et l'intégrité des opérations. Cette capacité proactive de détection des anomalies et des comportements frauduleux garantit que les installations restent sécurisées et que seuls les individus autorisés peuvent y accéder.

En résumé, notre système de reconnaissance faciale améliore l'expérience utilisateur en facilitant l'accès rapide et sans obstacle, tout en renforçant la sécurité des installations grâce à des mécanismes de prévention de la fraude et à une gestion sans contact. Il combine efficacité, confort et sécurité, répondant ainsi aux besoins variés des utilisateurs et des administrateurs dans divers environnements.

V Conclusion

Dans ce chapitre, nous avons présenté notre système de pointage automatisé, une solution innovante qui repose sur la reconnaissance faciale. En intégrant des technologies de pointe avec une approche pratique, notre système offre une gestion efficace des présences. Grâce à sa capacité d'identification rapide et précise, ainsi qu'à ses fonctionnalités de stockage flexible et de détection des fraudes, il répond aux besoins divers des environnements professionnels et éducatifs.

CONCLUSION GÉNÉRALE

« L'expérience est une observation provoquée dans le but de faire naître une idée. »

Claude Bernard

Conclusion générale

La mise en place d'un système de pointage de présence basé sur la reconnaissance faciale représente une avancée significative dans la gestion des présences pour les environnements éducatifs, professionnels et institutionnels. Ce système intègre les technologies de la vision par ordinateur et de la reconnaissance faciale, reposant sur des algorithmes sophistiqués pour une identification précise et rapide des individus. En exploitant les caractéristiques uniques du visage de chaque personne, il garantit une détection fiable, même dans des conditions variables comme l'éclairage ou les angles de vue. Cette capacité à capturer et à traiter les données de manière précise et rapide est essentielle pour assurer l'efficacité et la fiabilité du système.

De plus, la flexibilité offerte par les options de stockage local ou distant permet une adaptation facile à diverses infrastructures et exigences de sécurité. Que ce soit via une base de données locale ou hébergée sur un service cloud comme Firebase, le système garantit la confidentialité et l'intégrité des données, tout en améliorant l'accessibilité et simplifiant la gestion. Cette polyvalence permet aux utilisateurs de choisir la solution de stockage la plus adaptée à leurs besoins spécifiques, assurant ainsi la sécurité et la confidentialité des informations collectées.

Par ailleurs, la fonctionnalité de détection des fraudes et de contrôle des tentatives d'abus renforce la fiabilité et la transparence du système, assurant ainsi une utilisation juste et équitable des données de présence. En surveillant et en analysant le nombre total d'assistances enregistrées, le système peut identifier les anomalies et les comportements suspects, ce qui permet de détecter rapidement toute tentative de fraude ou d'abus. Cette capacité à prévenir et à contrer les tentatives de manipulation renforce la crédibilité et la légitimité du système, garantissant ainsi son utilisation efficace et équitable.

En conclusion, ce système de pointage de présence basé sur la reconnaissance faciale représente une solution innovante et fiable pour la gestion efficace des présences. En combinant des technologies avancées avec une approche pratique et adaptable, il répond aux besoins variés des environnements professionnels et éducatifs d'aujourd'hui, offrant ainsi une solution complète et efficace pour le suivi des présences. Grâce à ses fonctionnalités avancées et à sa flexibilité, il constitue un outil précieux pour améliorer la gestion des présences et optimiser les processus administratifs dans une grande variété de contextes.

Nous avons l'intention, dans nos travaux futurs, d'explorer plus en profondeur les possibilités d'accroître la précision de la reconnaissance faciale en intégrant des techniques avancées d'apprentissage automatique, tout en étant attentifs à minimiser les coûts associés à cette intégration. De plus, nous nous engageons à renforcer continuellement les protocoles de sécurité et de protection des données afin de répondre aux normes réglementaires en vigueur. Cela garantira la confiance des utilisateurs et des organisations dans l'application et l'utilisation de cette technologie innovante.

BIBLIOGRAPHIE

[1] Perronnin, Florent, and Jean-Luc Dugelay. "Introduction à la biométrie authentification des individus par traitement audio-vidéo." Traitement du signal 19.4 (2002).

[2] KRICHEN, Emine. Reconnaissance des personnes par l'iris en mode dégradé. 2007. Thèse de doctorat. Evry, Institut national des télécommunications.

[3] DIB, Fouad. Identification des personnes par le réseau veineux de la main. 2018. Thèse de doctorat.

[4] Galy, Nicolas. Etude d'un système complet de reconnaissance d'empreintes digitales pour un capteur microsystème à balayage. Diss. Institut National Polytechnique de Grenoble-INPG, 2005.

[5] Rojas, Julián Zapata. Traduction dictée interactive : Intégrer la reconnaissance vocale à l'enseignement et à la pratique de la traduction professionnelle. University of Ottawa (Canada), 2012.

[6] Castelluccia, Claude, and Daniel Le Métayer. Analyse des impacts de la reconnaissance faciale-Quelques éléments de méthode. Diss. Inria Grenoble Rhône-Alpes, 2019.

[7] Casilli, Antonio A. "Quatre thèses sur la surveillance numérique de masse et la négociation de la vie privée." Etude annuelle 2014 du Conseil d'Etat" Le numérique et les droits fondamentaux" (2014) : 423-434.

[8] Besse, Thomas. "De la distinction entre le général et l'individuel dans l'authentification des actes communautaires." Dalloz Actualité (2021) : 3-p.

[9] De Spiegeleir, Sophie. "Entre soin et sécurité, entre autonomie et contrainte : enquête au sein d'unités psychiatriques médico-légales en Belgique." Les droits sous contrainte. Enfermement et contrôle au XXIè siècle : hôpitaux psychiatriques, Centres jeunesse et prisons. 2022.

[10] SIQ, Mr BENCHOHRA Mohamed Amine, Mr MAHMOUDI Sid Ali SIT, and Mme BOULKABOUL Sahar. "Mise en œuvre d'un système de contrôle d'accès pour les bâtiments intelligents basé sur la reconnaissance conjointe faciale et vocale."

[11] Beye, Pape Demba. Faisabilité technique des systèmes avancés d'aide à la conduite (ADAS) pour la sécurité routière. Diss. Université du Québec à Trois-Rivières, 2021.

[12] D'Hérouville, Xavier, Claude Gaudeau de Gerlicz, and Aurore Caulier. "Biométrie appliquée à la reconnaissance faciale de quatre portraits présumés de Leonardo da Vinci." (2018).

[13] BENSAHLA, TANI, and Mohammed Karim BEREKSI. Réalisation d'un système autonome de contrôle d'accès de véhicules par reconnaissance optique des plaques d'immatriculation. Diss. 2022.

[14] MATALLAH, Abderrazzak, Abdeldjabbar BABAHADJ, and Mohammed KADDI. SYSTÈME DE CONTROLE D'ACCES PHYSIQUE. Diss. Université Ahmed Draïa-Adrar, 2017.

[15] Geitgey, Adam. "Machine learning is fun ! part 4 : modern face recognition with deep learning." Medium. Medium Corporation 24 (2016) : 2016.

[16] Kazemi, Vahid, and Josephine Sullivan. "One millisecond face alignment with an ensemble of regression trees." Proceedings of the IEEE conference on computer vision and pattern recognition. 2014.

[17] Dalal, Navneet, and Bill Triggs. "Histograms of oriented gradients for human detection." 2005 IEEE computer society conference on computer vision and pattern recognition (CVPR'05). Vol. 1. Ieee, 2005.

[18] Schroff, Florian, Dmitry Kalenichenko, and James Philbin. "Facenet : A unified embedding for face recognition and clustering." Proceedings of the IEEE conference on computer vision and pattern recognition. 2015.

[19] Amos, Brandon, Bartosz Ludwiczuk, and Mahadev Satyanarayanan. "Openface : A general-purpose face recognition library with mobile applications." CMU School of Computer Science 6.2 (2016) : 20.

[20] Veron, Noémie. "Le contrôle de l'utilisation des données biométriques au regard du droit au respect de la vie privée." (2017) : 1-255.

[21] Jacquet 1, Maëlig, and Lionel Grossrieder. "Enjeux et perspectives de la reconnaissance faciale en sciences criminelles." Criminologie 54.1 (2021) : 135-170.

[22] Sagonas, Christos, et al. "300 faces in-the-wild challenge : The first facial landmark localization challenge." Proceedings of the IEEE international conference on computer vision workshops. 2013.

[23] Huan, Xiaoli, and Hong Zhou. "Cost-Effective Attendance Management System Using Cloud Computing and Face Recognition." Journal of Management & Engineering Integration 14.1 (2021) : 81-89.

[24] Geitgey, Adam. "face_recognition : The world's simplest facial recognition api for Python and the command line." (2018) : 64.

[25] Kutlugün, Mehmet Ali, and Yahya Şirin. "Reducing false positive rate with the help of scene change indicator in deep learning based real-time face recognition systems." Multimedia Tools and Applications 82.30 (2023) : 47517-47536.

[26] Dong, Yuxuan. "Can machine recognize a long-missed old friend ? A test to the FaceNet face recognition algorithm." Journal of Physics : Conference Series. Vol. 2634. No. 1. IOP Publishing, 2023.

[27] Toufik, Hafs. "Reconnaissance Biométrique Multimodale basée sur la fusion en score de deux modalités biométriques : l'empreinte digitale et la signature manuscrite cursive en ligne." UNIVERSITE BADJI MOKHTAR–ANNABA, Année (2016).

[28] Hili, Nefissa Khiari. Biométrie multimodale basée sur l'iris et le visage. Diss. Université Paris-Saclay ; Université de Tunis El Manar, 2016.

[29] Laadjal, Haithem, and Encadre par Saigaa. Conception et évaluation d'an système d'authentification biométrique basé sur l'empreint palmaire. Diss. 2023.

[30] Diamanka, Mouhamadou. "Système de contrôle d'accés et de planification de rendez-vous pour les sociétés externes à la plateforme logistique de distribution du Port Autonome de Dakar." (2024).