UNIVERSITÉ DE BOURGOGNE

ESIREM

RAPPORT

Option : Informatique et Electronique

Réalisé par :
Primous **POMALEGNI**
Etudiant en 4ème année IT / ILC

Système de contrôle d'accès basé sur la vidéo-surveillance et l'utilisation de l'intelligence artificielle : cas particulier du pointage dans les entreprises.

Sous la supervision de :
-

Année Académique : **2019-2020**

Table des matières

Table des figures

Introduction

0.1 Contexte

L'ère des nouvelles technologies de l'information contribue beaucoup à simplifier la vie de ses nombreux utilisateurs. Que ce soit dans les domaines de l'éducation, de la santé, de l'économie et même des transports, elle apporte sa contribution afin de soulager le quotidien des utilisateurs avec des outils ou applications simples d'emploi.

La gestion de la présence dans les entreprises et dans les écoles est un problème qui préoccupe beaucoup les dirigeants de ces structures. Même possèdant des outils comme le pointage et la signature, ils cherchent toujours à s'améliorer afin d'offrir de meilleures conditions de travail à leurs employés en ce qui concerne les entreprises et d'études et ce qui concerne les universités et les écoles.

Ainsi, avec le développement des nouvelles technologies d'information et de communication et notamment de l'intelligence artificielle, on peut se demander si ces derniers ne peuvent pas servir et aider à atteiendre ce objectif de gestion optimale des présences au sein des entreprises et également des écoles ou université.

0.2 Problématique

La problématique abordée dans le cadre de ce projet est de resoudre de façon optimale la gestion des présences dans les entreprises et ceci afin de simplifier la vie des employés qui oublient soit leur badge, soit de pointer dans le cadre des entreprises utilisant de système de pointage. Il ne sera guère question d'utiliser notre système pour être intrusif ou malveillant.

0.3 Objectifs

Notre projet a pour objectif principal de mettre à la disposition des entreprises qui le souhaitent un système complet de gestion de présence au sein de leur entreprise en se basant sur les ressources dont ils disposent. Pour atteindre cet objectif, nous orientons notre réflexion sur la mise en place d'un logiciel qui sera capable de faire les traitements suivants :

- reconnaissance faciale des employés prenant service à l'entrée en utilisant le sytème existant de vidéo-surveillance
- enregistrement des données (nom, prénom et de l'heure d'arrivée) dans la base de données de notre logiciel
- reconnaissance faciale des employés finissant leur service à la sortie
- enregistrement des données
- calcul des horaires de présences sur une période donnée

0.4 Contribution

Notre travail permettra d'orienter le processus de pointage de façon automatisée et sans ingérance humaine. Notre système se chargera d'enregistrer ces données pour l'entreprise qui pourra s'en servir pour suivre la présence de ses employés.

Bien qu'en utilisant les caméras de vidéo-surveillance et de la reconnaissance faciale, il ne sera pas question d'être intrusif dans la vie de ses employés ou d'utliser leur image à des fins autres que l'objectif défini. On respectera donc les règles liées au droit à l'image.

Chapitre 1

Revue de littérature

Introduction

Ce travail n'est pas exploratoire. Beaucoup de travaux qui pourraient inspirer ont porté sur des thématiques proches. Cette revue de littérature est un récapitulatif d'œuvres basées sur des systèmes utilisant la reconnaissance faciale et l'intelligence artificielle pour simplifier la vie des utilisateurs.

1.1 Présentation de quelques solutions existantes

1.1.1 Le projet Alicem

1.1.2 C'est quoi Alicem ?

Alicem est une application mobile qui permet de se connecter à des services publics en ligne grâce à des technologies de reconnaissance faciale. Testée depuis le mois de juin 2019, elle a été annoncée en juillet 2019 par le ministère de l'Intérieur. Comme FranceConnect, qui donne accès au site des impôts, de la sécurité sociale ou encore de la poste avec un identifiant unique, Alicem est censée permettre d'éviter d'avoir à jongler entre plusieurs identifiants. L'application permettra également de se passer de présence physique à un guichet ou de l'envoi de multiples documents pour accéder à des services qui requièrent une identification sécurisée. Dans ce cas-là, Alicem sera le seul moyen d'effectuer ces procédures de façon dématérialisée. Ce projet s'inscrit donc dans l'objectif du gouvernement de permettre un accès en ligne à la totalité des services publics d'ici à 2022.

FIGURE 1.1 – Alicem

1.1.3 Comment ça marche ?

Alicem atteste l'identité de manière sécurisée au moyen d'un processus rigoureux. L'utilisateur s'inscrit depuis son smartphone avec son titre d'identité (passeport ou titre de séjour) dont la puce est lue par lecture sans contact NFC (communication en champ proche) et dont l'authenticité et la validité sont vérifiées auprès des services de l'État. Grâce à une technologie de reconnaissance faciale, l'utilisateur prouve qu'il est le titulaire légitime du titre d'identité.

Après cette phase d'inscription, Alicem permet d'accéder de manière simplifiée, mais toujours sécurisée, à l'ensemble des services partenaires de FranceConnect. Pour ce faire, l'utilisateur s'authentifie depuis son smartphone avec son code de sécurité. Pour certains usages, une lecture NFC de la puce du titre est également nécessaire.

Ce haut niveau de sécurité est un moyen de lutter contre les usurpations d'identité qui causent de nombreux préjudices à de nombreuses personnes.

1.1.4 Protection des données

- Les données extraites du titre d'identité sont vérifiées lors de l'inscription mais ces dernières ne sont stockées que sur le smartphone de l'utilisateur sous son contrôle exclusif et protégées par un chiffrement.
- Alicem n'a pas accès aux historiques de transactions grâce à la séparation garantie par la plateforme « FranceConnect », qui anonymise les fournisseurs de service auxquelles sont transmises les données.
- Le décret qui réglemente Alicem contient des dispositions très strictes sur la gestion des données.
- Les données ne font l'objet d'aucune utilisation pour d'autres objectifs que l'authentification électronique et l'accès à des services en ligne par Alicem. Elles ne sont pas transmises à des tiers.

Mais malgré toutes les mesures de sécurité et les règles de protection que l'application applique, elle est sujette à de fortes interrogations sur la gestion des données notamment sur ce qui est fait de la reconnaissance faciale sur laquelle elle a été construite afin de garantir la non ursurpation d'identité dans les services publics.

1.2 ClearView

ClearView est une application créée par Hoan Ton-That qui en échange d'une simple photo de vous, est capable de retrouver votre nom, mais aussi dans la plupart des cas votre âge, le quartier où vous habitez, des photos de vos proches, de vos compétitions sportives, tout comme celles de la fête de famille qu'avait immortalisée votre grand-oncle il y a cinq ans. Et même des photos anciennes.

L'application est en effet capable de puiser dans les contenus que vous postez sur les réseaux sociaux, et ce, sans avoir votre autorisation. Extrêmement efficace, donc, mais également redoutable puisque ClearView est utilisée par pas moins de 600 agences gouvernementales, selon le New York Times, qui a révélé l'existence de cette application au grand public.

1.3 LFIS, le système de reconnaissance faciale en temps réel

Le système d'identification de visages en direct Gemalto Cogent est un système de reconnaissance faciale vidéo qui reconnaît automatiquement les visages dans une foule, même dans des environnements dynamiques et incontrôlés.

Il envoie des alertes en temps réel pour pouvoir agir rapidement.

Le système peut être intégré dans une large gamme d'équipements vidéo, et des algorithmes avancés augmentent la précision des correspondances.

Le système d'identification de visage en direct de Gemalto Cogent (LFIS) inclut 2 composants principaux

- Core LFIS et LFIS Check SDK (Kit de développement logiciel). Core LFIS fournit une reconnaissance faciale basée sur de la vidéo, conçue pour la détection de visages dans une foule en temps réel ou après un événement et recherchée par rapport à une liste intégrée de personnes.
- LFIS Check SDK est un kit de développement logiciel robuste qui permet aux développeurs de créer des applications utilisant le visage en tant qu'identifiant biométrique.

  Le SDK est livré avec une application de démonstration qui montre comment le SDK peut être intégré avec un lecteur de documents Gemalto pour faire correspondre les visages réels avec les visages des documents. Cette solution de reconnaissance de visage en temps réel a été conçue pour être évolutive et est construite sur une configuration de technologies stables.

Traditionnellement, les systèmes biométriques distribués à grande échelle nécessitent des spécialistes du produit très expérimentés pour les configurer. LFIS dispose d'un système de configuration pratique et d'un riche ensemble de services Web RESTful (transfert d'état représentatif).

Chapitre 2

Analyse, choix technique et conception

2.1 Analyse

La phase d'analyse d'un projet consiste à déterminer la description du besoin pour élaborer la solution technique. Elle doit donc décrire les futures applications avec une double préoccupation : bien traduire les besoins en vue d'une préparation optimale du futur développement. L'analyse vise aussi à définir et à justifier la solution optimale qui répondra aux exigences du projet et qui tiendra compte de toutes les contraintes du contexte projet. Dans le cadre de notre analyse, nous avons choisi de montrer le fonctionnement de notre logiciel.

Comme tout projet utilisant les données biométriques, il est composé de plusieurs étapes avant utilisation.

En effet la biométrie permet d'identifier et d'authentifier une personne sur la base d'un ensemble de données reconnaissables et vérifiables, uniques et spécifiques à celles-ci.

2.1.1 L'identification répond à la question « qui êtes-vous ? ».

Dans ce cas, la personne est identifiée parmi d'autres (vérification 1 :N). Ses données personnelles sont comparées aux données d'autres personnes contenues dans la même base de données ou dans d'éventuelles bases de données reliées.

2.1.2 L'authentification répond à la question : « Etes-vous bien celui que vous prétendez être ? ».

La biométrie permet ici de certifier l'identité d'une personne en comparant les données qu'elle va présenter avec les données préenregistrées de la personne qu'elle prétend être (vérification 1 :1).

En voici quelques exemples :

- Dans le cas de la biométrie faciale, un capteur 2D ou 3D « saisit » un visage, puis le transforme en données numériques par l'opération d'un algorithme et le compare à une base de données. C'est en quelques sortes une réplique fidèle et « augmentée » du processus à l'œuvre dans le cerveau humain.

- Ces systèmes automatisés permettent d'identifier ou de vérifier l'identité d'individus en quelques secondes seulement à partir des caractéristiques de leur visage : écartement des yeux, des arêtes du nez, des commissures des lèvres, des oreilles, du menton, etc., y compris au milieu d'une foule, au sein d'environnements dynamiques et instables.

2.2 Choix technique

Dans le cadre de notre projet, nous nous sommes renseignés sur les différentes posssibilités que nous avions pour le développement. En effet, plusieurs langages de développement offrent des outils assez spécifiques dans le traitement d'images et sur la reconnaissance faciale. C'est notamment, le cas de la librairie **openCV** developpée dans le langage C++ mais également utilisable en python pour ce qui est de la reconnaissance faciale. Cette librairie dispose de plusieurs fonctions permettant d'analyser les flux d'images et de vidéos afin de mettre en place un dataset (jeu de données) qui pourra au moyen de l'intelligence artificielle nous aider à atteindre notre objectif qui est d'arriver à faire du pointage en entreprise et ceci bien sûr en respectant les règles du droit à l'image de chaque personne.

2.2.1 Présentation d'openCV

OpenCV (Open Source Computer Vision) est une bibliothèque proposant un ensemble de plus de 2500 algorithmes de vision par ordinateur, accessibles au travers d'API pour les langages C, C++, et Python. Elle est distribuée sous une licence BSD (libre) pour les plate-formes Windows, GNU/Linux, Android et MacOS.

Initialement écrite en C il y a 10 ans par des chercheurs de la société Intel, OpenCV est aujourd'hui développée, maintenue, documentée et utilisée par une communauté de plus de 40 000 membres actifs. C'est la bibliothèque de référence pour la vision par ordinateur, aussi bien dans le monde de la recherche que celui de l'industrie.

Elle dispose de nombreux modules dont les principaux modules sont :

- core : les fonctionnalités de base. Cette bibliothèque permet de manipuler les structures de base, réaliser des opérations sur des matrices, dessiner sur des images, sauvegarder et charger des données dans des fichiers XML…
- imgproc : traitement d'image. Les fonctions et structures de ce module ont trait aux transformations d'images, au filtrage, à la détection de contours, de points d'intérêt…
- features2d : descripteurs. Ce module concerne principalement l'extraction de descripteurs selon deux approches courantes (SURF et StarDetector)
- objdetect : détection d'objets. Cette bibliothèque permet de faire de la reconnaissance d'objets dans une image au moyen de l'algorithme Adaboost (Viola et Jones, 2001).
- video : traitement de flux vidéo. Ces fonctions servent à segmenter et suivre les objets en mouvement dans une vidéo.

- highgui : entrées-sorties et interface utilisateur. OpenCV intègre sa propre bibliothèque haut-niveau pour ouvrir, enregistrer et afficher des images et des flux vidéo. Celle-ci contient aussi un certain nombre de fonctions permettant de réaliser des interfaces graphiques très simples.
- calib3d : calibration, estimation de pose et stéréovision. Ce module contient des fonctions permettant de reconstruire une scène en 3D à partir d'images acquises avec plusieurs caméras simultanément.

Elle offre donc de plusieurs possibilités pour faire du computeur vision ce qui justifie notre choix de ce langage.

2.3 Conception et Réalisation

La mise en place du pointage par vidéo-surveillance dans notre projet a éte faite sur plusieurs étapes qui sont :

- une première étape d'acquisition de données et d'étiquetage.
- une seconde phase d'apprentissage
- et une dernière phase de mise en situation et d'écriture des données reçues.

2.3.1 Acquisition des données et étiquetage

2.3.1.1 Acquisition des données

L'acquisition des données pour l'apprentissage consiste à recuperer des images de personnes en utilisant un flux vidéo ou des photos qui nous sont données. Dans le cadre du flux vidéo, il s'agira de faire passer ce flux vidéo dans notre programme qui s'occupera de détecter les visages des personnes présentes dans la vidéo en utilisant la fonction detectMultiscale d'openCV et ceci en utilisant un modèle xml dans lequel les caractérisques générales d'un visage de face ont été décrites. Ces visages détectés sont ensuite recadrés et enregistrés sous formes de fichiers png qui seront utilisés au cours de l'apprentissage.

2.3.1.2 Etiquetage

L'etiquetage est le classement manuel des images de visage prises au cours de la phase précédente et ceci en se basant sur les identitées des personnes (nom, prenom ...).

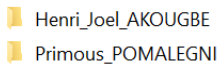

FIGURE 2.1 – Jeu de données étiqueté

2.3.2 Apprentissage

Cette phase est l'une des plus importantes. Grâce à l'intelligence artificielle, on peut amener un programme à apprendre en utilisant un jeu de données. Et le jeu de données utilisé dans notre projet

est l'ensemble de nos images de visages etiqueté à l'étape précédente. Il est ensuite passé au programme qui se charge de lier les caractéristiques de chaque dossier etiqueté à l'identité associée. Ce qui permettra de procéder à l'identification par la suite.

2.4 Mise en situation et écriture des données

Dans cette phase qui intervient apres l'apprentissage, notre logiciel est capable d'identifier les personnes qui passent devant une caméra de vidéo-surveillance dont on lui fournit le flux. Il peut ainsi associer une identité à chaque personne qui passe et ainsi écrire dans la base de données son l'heure d'arrivée et son heure de départ ce qui permettra de justifier de la présence ou non d'un employé au sein d'une entreprise pendant une période donnée. Elle pourrait aussi utile dans le cadre de l'accès à des endroits cas des badges utilisés pour l'accès à l'université par exemple pour l'ouverture des portes.

Elle peut être aussi utilisée dans le cadre des présences des étudiants à l'université et ceci en étudiant avec minutie le cadre juridique afin d'avoir les autorisations requises avant l'utilisation d'un tel système.

2.5 Présentation de résultat

Dans cette partie nous nous sommes inspiré d'un flux de vidéo test sur lequel nous reconnaissons deux personnes et nous procédons à la sauvegarde de ces informations (nom, prénom et heure de passage) dans notre base de données.

Notons que ce flux vidéo a été pris avec l'accord des personnes qui y sont présentes et son usage dans le cadre de notre projet leur a été précisé.

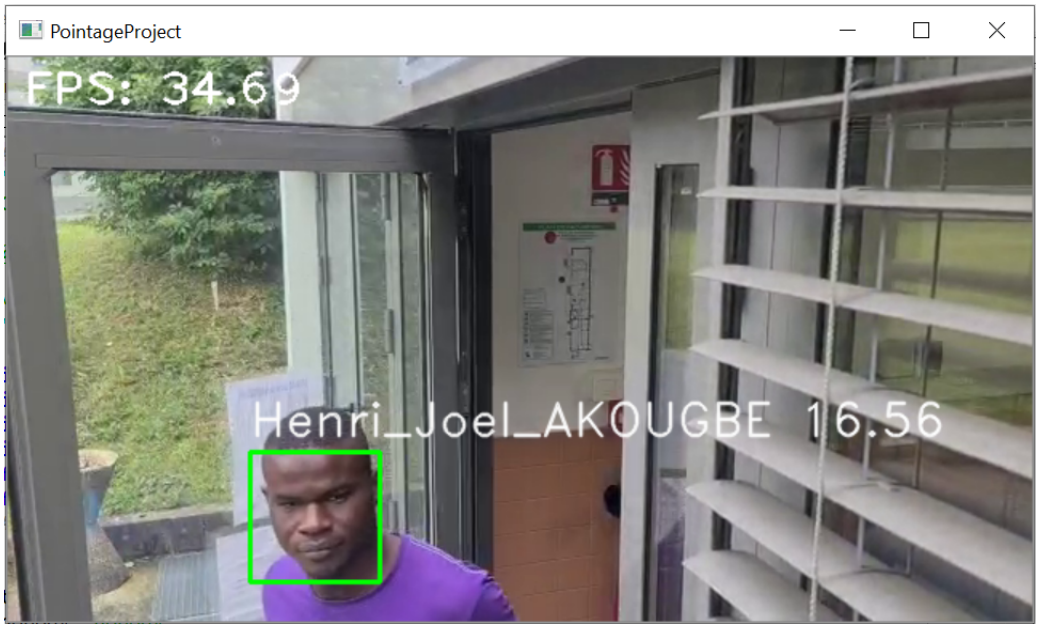

FIGURE 2.2 – Reconnaissance d'un employé sortant du bureau

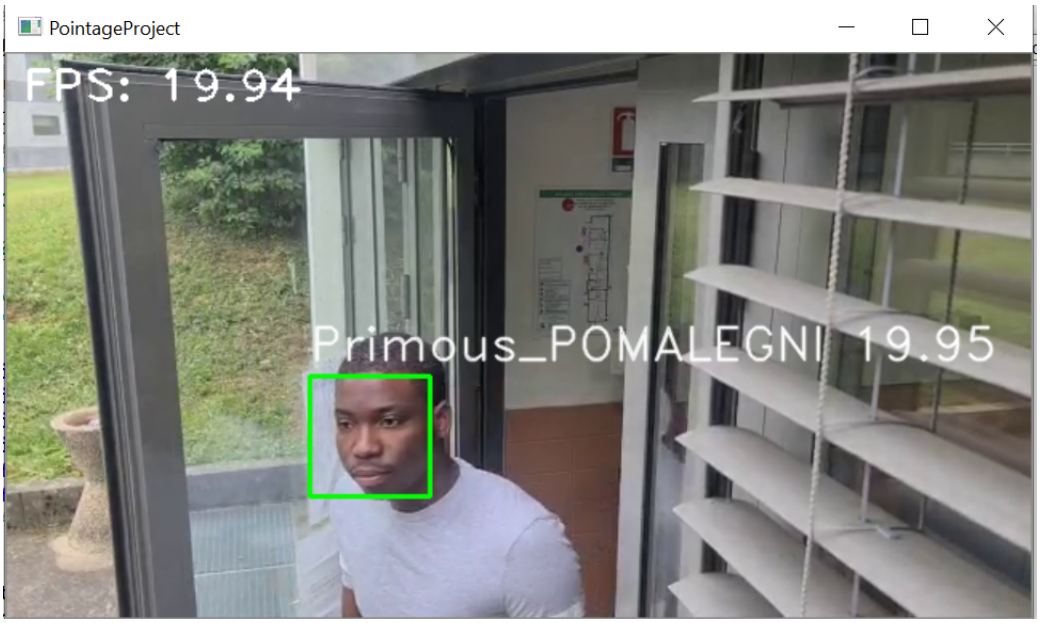

FIGURE 2.3 – Reconnaissance d'un autre employé sortant du bureau

On peut voir sur les figures précédentes, que les personnes présentes sont identifiées (reconnaissance du visage et identifiacation avec nom à l'appui). Ces données sont ensuite enregistrées dans la base de données pour constituer l'ensemble de données nécessaires pour justifier de la présence de quelqu'un. Base de données qu'on peut voir sur la figure suivante.

```
('Inconnu', ('2020-06-30 18:25:46.783532', False))
('Henri_Joel_AKOUGBE', ('2020-06-30 18:26:07.932163', False))
('Inconnu', ('2020-06-30 18:26:07.944503', False))
('Henri_Joel_AKOUGBE', ('2020-06-30 18:26:08.040231', False))
('Inconnu', ('2020-06-30 18:26:09.005910', False))
('Primous_POMALEGNI', ('2020-06-30 18:26:15.175464', False))
('Inconnu', ('2020-06-30 18:26:16.054627', False))
('Henri_Joel_AKOUGBE', ('2020-06-30 18:26:23.783576', False))
```

FIGURE 2.4 – Vue sur la base de données

2.6 Problème d'ursurpation

L'un des grands problèmes de l'utilisation d'un tel système est l'utisation par un tierce de photo de quelqu'un pour passer inaperçu par le système ou se faire passer pour quelqu'un d'autre.

Afin de résoudre ce problème, il est possible d'ajouter à notre programme une partie qui se charge de vérifier que ce n'est pas une photo qui est utilisée. En effet ce programme se charge de vérifier si la personne à des clignotements des yeux ce qui n'est pas le cas quand on se sert d'une photo d'autrui pour passer inaperçu.

Chapitre 3

Cadre juridique

Dans le cadre de la mise en place d'un projet de reconnaissance il est important de respecter les droits qui protègent l'utilisation de l'image de quelqu'un et voir dans quelles mesures on pourrait utiliser une image pas pour l'utiliser à des fins commerciales mais dans le but de s'en servir comme au cours de l'apprentissage qui est une phase importante de notre projet. L'un de ces droits principaux est le droit à l'image.

3.1 Le droit à l'image

3.1.1 Définition

Le droit à l'image vous permet de faire respecter votre droit à la vie privée. Ainsi, il est nécessaire d'avoir votre accord écrit pour utiliser votre image. Des exceptions existent, par exemple la photo d'un événement d'actualité. Vous pouvez demander le retrait d'une image au responsable de sa diffusion. En cas de refus, vous pouvez saisir le juge et/ou la Cnil si l'image est diffusée en ligne. Vous pouvez porter plainte en cas d'atteinte à votre vie privée.

3.1.2 Dans quels cas pouvons-nous utiliser l'image de quelqu'un ?

Le droit à l'image est lié à votre droit au respect de la vie privée.

Ainsi, il est nécessaire d'avoir un accord écrit pour utiliser l'image d'une personne (diffusion, publication, reproduction ou commercialisation).

L'image peut être une photo ou une vidéo sur laquelle la personne est identifiable, dans un lieu privé ou dans un lieu public : vacances, événement familial, manifestation sportive, culturelle, religieuse...

L'image peut être diffusée via la presse, la télévision, un site internet, un réseau social...

Toutefois, la diffusion de certaines images ne nécessite pas l'accord de la personne photographiée ou filmée, sous réserve du respect de sa dignité.

3.1.3 Cas d'une personne majeure

Le photographe/vidéaste doit obtenir l'accord écrit de la personne avant de diffuser son image.

Par exemple pour diffuser son image sur Internet.

Le consentement à être photographié ou filmé n'est pas suffisant.

L'accord doit être précis : sur quel support est diffusé l'image ? Dans quel objectif ? Pour quelle durée ?

Votre accord est également nécessaire si votre image est réutilisée dans un but différent de la 1ère diffusion.

Dans le cas d'une image prise dans un lieu public, son autorisation est nécessaire uniquement si elle est isolée et reconnaissable.

3.1.4 Cas d'une personne mineure

Avant d'utiliser l'image d'un mineur, l'autorisation des parents (ou du responsable légal) doit obligatoirement être obtenue par écrit.

Il n'y a pas d'exception, y compris pour le journal et l'intranet d'une école.

Pour un groupe d'enfants, l'autorisation écrite des parents de chaque enfant est obligatoire.

Conclusion

A la fin de ce travail, nous sommes satisfaits à titre personnel du résultat obtenu même s'il peut être encore amélioré. En effet, n'ayant aucune notion en reconnaissance avant de nous lancer dans ce projet, on peut avouer que le thème que nous avons choisi nous a permis d'en apprendre beaucoup sur la vision par ordinateur et des nombreuses possibiltés qu'elle offre. Ainsi, nous avons pu avoir une idée sur les projets actuels se basant sur la reconnaissance et des difficultés dont ils font face dans leur mise en déploiement. Aussi cela nous a permis de voir le cadre juridique lié à l'utilisation de l'image d'une personne ce qui est une problématique importante à cette époque où grâce au smartphone on peut tout filmer. Nous pensons que ce cadre juridique doit être fortement partagé et connu de tous afin d'éviter des problèmes juridiques qui pourraient venir suite à son nom respect.

Ce projet nous a permis également d'augmenter nos compétences personnelles sur plusieurs plans que ce soit dans le domaine informatique ou transversal notomment les compétences d'organisation et d'autonomie.

https ://www.service-public.fr/particuliers/vosdroits/F32103

https ://www.lefigaro.fr/secteur/high-tech/qu-est-ce-qu-alicem-le-projet-d-identification-par-reconnaissan
faciale-de-l-etat-francais-20191009

https ://www.interieur.gouv.fr/fr/Actualites/L-actu-du-Ministere/Alicem-la-premiere-solution-
d-identite-numerique-regalienne-securisee

https ://www.thalesgroup.com/fr/europe/france/dis/gouvernement/biometrie/reconnaissance-
faciale

https ://www.thalesgroup.com/fr/europe/france/dis/gouvernement/biometrie/identification-
biometrique/reconnaissance-faciale