cesi

VEILLE TECHNOLOGIQUE

RECONNAISSANCE FACIALE

ANNÉE
2020/2021

MAILLOCHAUD
Laurianne

TABLE DES MATIERES

TABLE DES FIGURES

REMERCIEMENT

Je tiens tout particulièrement à remercier Monsieur Franck Bardol. Expert dans la Transformation Numérique par les Algorithmes et la Data, formateur en entreprises et enseignant dans le domaine des méthodes de l'Intelligence Artificielle pour les Grandes Écoles (École Microsoft IA, ISEP, Media School), Monsieur Bardol a vivement accepté de partager ses connaissances dans le domaine de la Reconnaissance Faciale afin de contribuer au présent rapport.

INTRODUCTION A LA VEILLE TECHNOLOGIQUE

OBJECTIFS DE LA VEILLE TECHNOLOGIQUE

Cette veille technologique vise à synthétiser les diverses informations collectées et analysées sur plusieurs mois. Différentes sources sont exploitées afin d'apporter un maximum de précisions et d'informations. Ainsi ce travail se base sur des articles issus de médias journalistiques, des interviews, des témoignages d'expert, des sondages mais aussi des vidéos explicatives. Dans ce rapport l'objectif est de communiquer sur les possibilités d'évolutions et les besoins de la technologie de Reconnaissance Faciale sur le marché.

CORRELATION AVEC LA THEMATIQUE CHOISIE

La Reconnaissance Faciale est une technologie omniprésente dans notre société. Elle se déploie sous différentes formes et attire de plus en plus de chercheurs faisant d'elle une technologie en perpétuel évolution. Sujet de recherche et d'expérimentation faisant partie des plus important de la décennie, son développement nécessite un encadrement strict et révèle de nombreuses failles.

Pour un être humain, reconnaître un visage est le résultat d'un processus cognitif par lequel le cerveau analyse une image pour y détecter et identifier un visage parmi un ensemble de visage connus. Le système de Reconnaissance Faciale essaie de reproduire cette forme d'intelligence humaine par des processus automatisés aussi appelés Intelligence Artificielle.

Depuis une soixantaine d'années, l'usage de la biométrie par Reconnaissance Faciale est de plus en plus sollicité par les entreprises mais aussi par les gouvernements. À la suite des attentats du 11 septembre, les gouvernements de nombreux pays ont investi activement dans la biométrie par Reconnaissance Faciale, technologie jugée comme prometteuse pour accroître la sécurité et le contrôle de la population. Parmi les diverses méthodes biométriques, la Reconnaissance Faciale ne requiert pas le consentement des individus étudiés, ce qui apparaît être très utile pour les gouvernements. De plus, avec l'avancée et le développement des services informatisés il est devenu primordial d'identifier les individus pour lutter contre les fraudes. Utilisation à caractère ludique (filtres), sécuritaire (authentification d'accès) ou préventif (surveillance militaire), une majorité de la population mondiale a déjà expérimenté ce système de manière passive ou active. Les possibilités d'intégration de la Reconnaissance Faciale se multiplient chaque jour.

En France les entreprises Thales et Idemia se positionne dans le top 10 des leaders mondiaux de la reconnaissance faciale. Mordor Intelligence prévoit que le marché mondial de la Reconnaissance Faciale devrait atteindre les 9 milliards d'euros d'ici 2024. Ils spécifient que ce marché se tourne majoritairement aux forces de l'ordre.

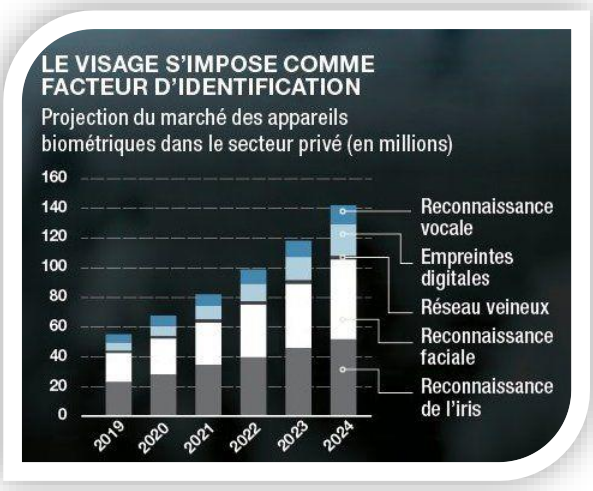


Figure 1 : SOURCE TRACTICA

ETAT DE L'ART

NOTION DE BIOMETRIE

Selon la CNIL la biométrie est « l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales, etc.). » La Reconnaissance Faciale est donc un système biométrique.

EVOLUTION DES TENDANCES

SCANNERS 2D

Cette tendance est la plus utilisée à l'heure actuelle. Elle consiste à identifier des caractéristiques faciales à l'aide d'algorithmes performants capable d'extraire des points de repères (appelés Landmark en anglais). Ces points repères sont nombreux et permettent d'identifier de manière unique un individu, ils peuvent être des repères positionnés au niveau des yeux, du nez, de la bouche, etc. Une fois que la géométrie du visage est établie par les algorithmes, l'empreinte du visage est transférée à la base de données et est enregistrée avec les informations personnelles relatives à l'individu. La plupart des algorithmes utilisent eigenfaces, Linear Discriminate Analysis, Elastic Bunch Graph Matching, Hidden Markov model, Multilinear Subspace Learning, et dynamic link matching.

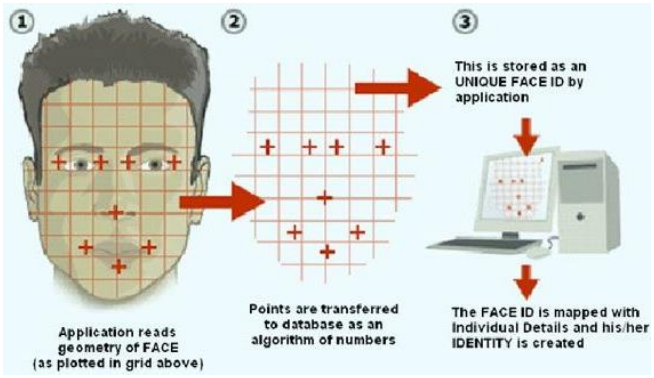


Figure 2 : engineersgarage

UTILISATION DE LA 3D

Les chercheurs ont mis au point une technologie de Reconnaissance Faciale en utilisant des capteurs 3D. Dans un premier temps la forme du visage est capturée, puis vont être identifiées des caractéristiques distinctives sur la surface d'un visage, comme le contour de l'orbite, le nez et le menton. La 3D offre de nombreux avantages que la 2D ne présente pas, par exemple l'identification d'un visage sous différents angles et éclairage, une meilleure précision et adaptable aux expressions faciales. Il y a maintenant plusieurs bases de données publiques de référence 3D du visage. Dans le marché l'entreprise Bioscrypt propose une interface de sécurité basée sur l'authentification 3D par Reconnaissance Faciale.

Figure 3 : Source StudioRed-Technologie Bioscrypt

METHODES GLOBALES / LOCALES / HYBRIDES

Les méthodes globales effectuent des analyses statistiques sur des images de visage. Tout d'abord une matrice de pixels est générée puis va être linéarisée par des vecteurs. Cette méthode ne nécessite pas l'utilisation de points de repère.

On distingue deux types de techniques : les techniques linéaires visant à projeter linéairement l'espace d'entrée, l'image de visage, en un autre espace de plus faible dimension, et à ne conserver que les données considérées comme significatives. Et les techniques non linéaires ayant pour but de trouver des espaces de séparation capables de représenter les données sous forme de classes indépendantes.

Les méthodes locales détectent les points caractéristiques du visage, mesure chaque position de ces points dans l'espace du visage et les comparer avec les paramètres extraits d'autres visages.

Les méthodes hybrides combinent les caractéristiques globales et locales afin d'améliorer les performances de la reconnaissance de visages.

METHODES	PERFORMANCES	LIMITES
GLOBALES	Rapides à mettre en œuvre Opérations matricielles simples	Très sensibles aux variations d'éclairage, de pose et d'expression faciale
LOCALES	Performantes face aux variations d'éclairage, d'expression faciale etc.	Méthode longue et difficile
HYBRIDES	Combinent la détection de caractéristiques géométriques avec l'extraction de caractéristiques d'apparence locales.	

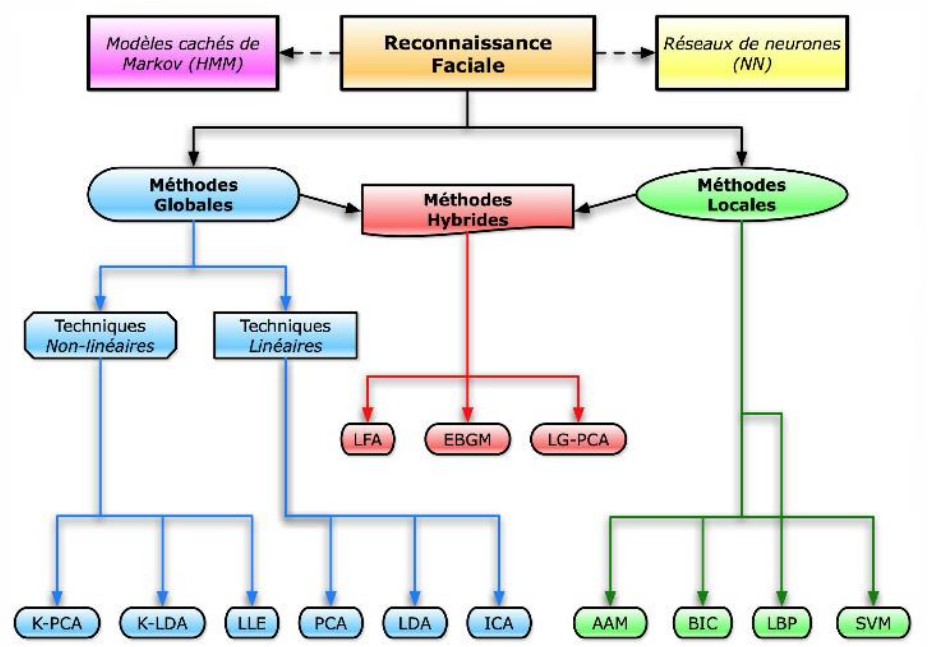


Figure 4 : Source Serge KOMANDA BASEMA

INTELLIGENCE ARTIFICIELLE ET RECONNAISSANCE FACIALE

Le système de Reconnaissance Faciale repose sur l'Intelligence Artificielle.

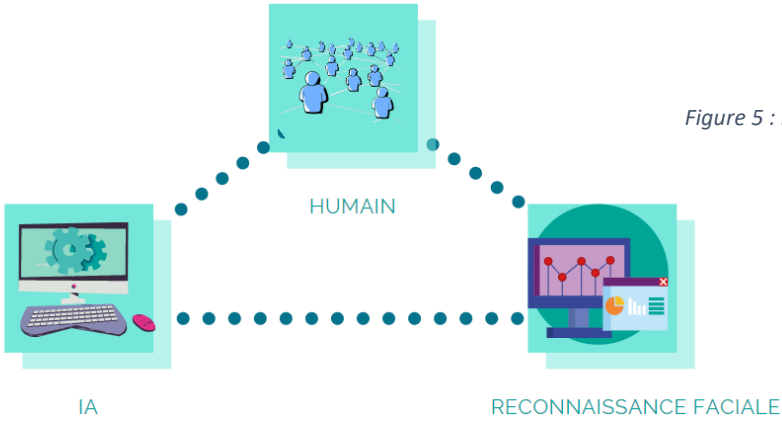


Figure 5 : Diagramme réalisé sur Canva

QU'EST-CE QUE L'INTELLIGENCE ARTIFICIELLE ?

Le conseil de l'Europe définit l'Intelligence Artificielle comme « un ensemble de connaissances, théories et techniques mises en œuvre en vue de réaliser des machines capables de simuler les capacités cognitives d'un être humain. En l'état de l'art, l'IA vise par exemple à confier à des machines des tâches complexes auparavant prises en charge par des êtres humains. » En d'autres termes, l'Intelligence Artificielle vise à reproduire des processus cognitifs humain qui, suite à de nombreux entraînements acquiert une logique et une intelligence propre capable d'apprendre en autonomie de nouvelles compétences. L'Intelligence Artificielle est donc en mesure de reconnaitre plusieurs caractéristiques telles que :

- L'âge
- Le sexe
- L'ethnicité
- Le vieillissement
- Les étirements du visages causés par les émotions (sourire, colère…)
- Un comportement

PARRALELISME ENTRE INTELLIGENCE ARTIFICIELLE ET RECONNAISSANCE FACIALE

Le système de Reconnaissance Faciale analyse les images ou vidéos avec un algorithme d'Intelligence Artificielle. Dans un premier temps le logiciel doit capturer un média, ce dernier peut être sous format image ou vidéo, ensuite c'est au tour des algorithmes d'Intelligence Artificielle d'établir de nombreux calculs et mesures dans le but d'analyser et extraire des informations, et c'est grâce à ces analyses que la Reconnaissance Faciale peut s'établir en comparant les analyses avec sa base de données.

AUTHENTIFICATION ET IDENTIFICATION

La Reconnaissance Faciale doit répondre à deux fonctions principales :

- Authentifier une personne : cela revient à vérifier qu'une personne est bien celle qu'elle prétend être, c'est-à-dire de certifier son identité.
- Identifier une personne : cela revient à reconnaître et identifier une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données. Le système compare le visage et cherche le modèle le plus similaire enregistré dans sa base de données.

POINTS HISTORIQUES

1964 : Début de la Reconnaissance Faciale.

Des chercheurs américains, Woodrow Bledsoe, Helen Chan et Charles Bisson, travaillent sur une méthode de détection de visage. Sur un ordinateur, l'utilisateur doit entrer manuellement plusieurs informations sur les caractéristiques du visage étudié afin d'avoir une mesure de ce dernier. Cependant ces vingtaines de mesures restent insuffisantes pour garantir l'efficacité de leur travail.

1991 : Eigenfaces.

Sirovich et Kirby développe la première technologie de Reconnaissance Faciale : Eigenfaces. *« Cette technique de reconnaissance utilise la méthode d'analyse en composantes principales (PCA) ou la méthode de décomposition en valeurs singulières (SVD). De manière simple, elle vise à diminuer la dimension de l'espace de travail pour simplifier les données et leur interprétation. Le but est ainsi de prendre en compte les informations importantes qui permettront de reconnaître un visage parmi d'autres avec un bon taux de réussite. »* Selon silanus.fr

2003 : Programme FERET.

La DARPA estime que la Reconnaissance Faciale doit être développée, pour cela elle met en place le programme FERET en 2003 qui contient 850 portraits de personnes.

2011 : Le deep learning.

Il permet à la Reconnaissance Faciale de s'améliorer, cette fois-ci la machine est en mesure de sélectionner automatiquement les points à comparer.

2014 : Deepface

Facebook dévoile Deepface, un système de Reconnaissance Faciale promettant 97 % d'efficacité.

2018 : Lunette de Reconnaissance Faciale.

Mises au point en 2017, ces lunettes ont aidé à l'interpellation de sept personnes recherchées. Vingt-six individus voyageant sous une fausse identité ont également été repérés par ces lunettes.

Face ID : Dévérouiller son smartphone

Sécurité et contrôle de la population

Santé et Cosmétique

Nous avons vu que la Reconnaissance Faciale est une technologie combinant les techniques biométriques, l'Intelligence Artificielle, la cartographie 3D et le Deep Learning pour comparer et analyser le visage d'une personne afin de l'identifier.

Aujourd'hui cette technologie est déployée sous diverses formes. Dans cette partie nous allons exposer les trois principales déclinaisons de la Reconnaissance Faciale.

LA RECONNAISSANCE FACIALE A USAGE PERSONNEL

Etude de cas : Face ID

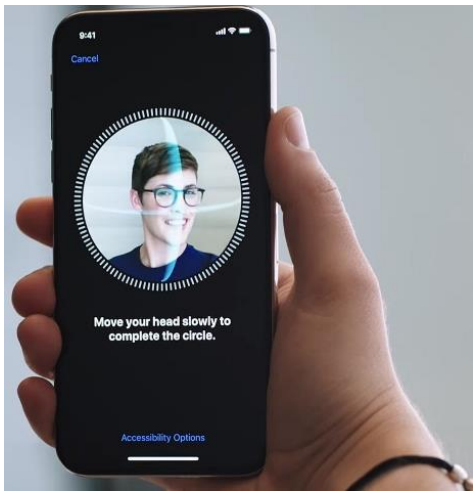


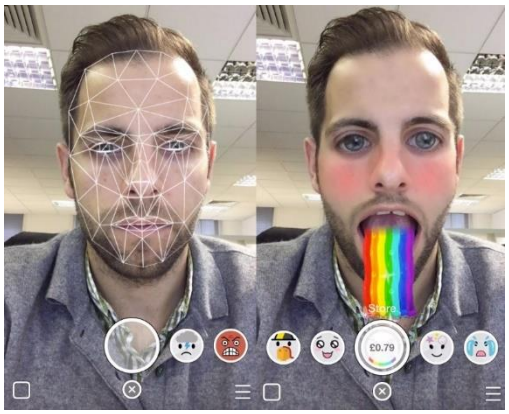
Figure 6 : Source nexter.org

La biométrie est la méthode la plus utilisée pour déverrouiller nos appareils électroniques car elle est jugée plus fiable que les techniques qui la précèdent tel que le mot de passe.

Aujourd'hui une quantité importante d'informations de notre identité est stockée sur nos appareils électroniques (smartphone, tablettes etc.). Pour assurer notre sécurité ces données numériques doivent être protégées. Par exemple Apple révolutionne le marcher avec Face ID qui permet une authentification par Reconnaissance Faciale grâce au système de caméra TrueDepth. Apple décrit que ce système permet de *« cartographier avec précision la géométrie d'un visage en projetant et en analysant plus de 30 000 points invisibles, afin de créer une carte de profondeur et de capturer une image infrarouge du visage ».*

La technologie Face ID s'adapte automatiquement aux changements de l'apparence physique. Elle est en mesure de s'adapter au maquillage, à la pilosité faciale, aux couvre-chefs, aux lunettes, ou encore aux lentilles de contact. Face ID vise aussi à simplifier les démarches de l'utilisateur en proposant une authentification par Reconnaissance Faciale pour payer sur certaines plateformes comme Apple Pay, iTunes Store, App Store et la libraire d'Apple Books. Enfin il est aussi possible avec Face ID de remplir automatiquement les champs du nom d'utilisateur et du mot de passe sur des sites web dans Safari.

Etude de cas : filtre Snapchat



Snapchat est le premier réseau social à révolutionner l'utilisation de la Reconnaissance Faciale à travers des filtres. L'analyse par Reconnaissance Faciale se fait en temps réel avec la caméra du smartphone. Une fois que le visage est analysé une empreinte virtuelle est créé et est superposée au visage.

La technologie est en mesure de s'adapter même si le sujet est en mouvement. Et c'est à partir de cette empreinte virtuelle que la technologie va pouvoir superposer au visage différents filtres.

L'utilisation ludique de la Reconnaissance Faciale à travers l'usage de filtres émerge de plus en plus. En 2017 Instagram aussi ajoute l'option filtre à son application.

LA RECONNAISSANCE FACIALE AU SERVICE DES GOUVERNEMENTS

La Reconnaissance Faciale s'avère également utile pour contrôler les déplacements de la population.

Par exemple, cette technologie est très présente au contrôle des frontières. Son but est de comparer la photographie du visage de l'individu figurant sur un passeport biométrique à un portrait numérisé en direct.

Cas d'étude : Aéroports parisiens

Depuis le 22 juin 2018 une collaboration entre le groupe Aéroports de Paris, le ministère de l'intérieur et la société Gemalto à permit la création et la mise en place d'infrastructure de Reconnaissance Faciale au niveau des postes de frontière des aéroports de Roissy et Orly. On compte quinze systèmes de Reconnaissance Faciale en service à Orly, et une vingtaine à Roissy Charles-de-Gaulle.

Cependant cette infrastructure présente trois failles.

1. Erreur de planimétrie ou « Le bug du T-shirt Johnny Hallyday »

La machine peut scanner par erreur un visage plat sur un vêtement, cette erreur est arrivée de nombreuses fois sur des individus portant un haut avec un imprimé du visage de Johnny Halliday.

2. Délinquance

La technologie n'empêche pas un individu de forcer la porte du sas, elle peut donc s'avérer inutile si l'individu ne collabore pas.

3. Eclairage

Une forte intensité de lumière peut empêcher le fonctionnement de la Reconnaissance Faciale.

La Reconnaissance Faciale permet aussi de retrouver des individus portés disparus.

Etude de cas : TrackChild en Inde

Figure 7 : Source up-magazine.info

En Inde la Reconnaissance Faciale s'associe à une base de données nommée TrackChild qui répertorie les photos des enfants recherchés. En l'espace de 4 jours le logiciel a permis à la police de retrouver 2 930 enfants

Depuis les attentats du 11 septembre les gouvernements de différents pays investissent dans la Reconnaissance Faciale pour déjouer la menace terroriste.

Etude de cas : Carnaval de Nice

Figure 8:Source 20minute.fr

Nice a été victime de nombreux attentats terroristes. Pour veiller à la sécurité de la population le maire de Nice a fait installer des infrastructures de Reconnaissance Faciale, on compte près de 3 000 caméras dans la ville ce qui fait d'elle la ville la plus surveillée de France.

Du 16 février au 2 mars 2019, 50 personnes volontaires ont fourni des photographies d'eux permettant ainsi de tester l'efficacité du système. Postée à une entrée du carnaval, elle a réussi à détecter et identifier ces 50 individus parmi 5000, différenciant même des jumeaux.

Etude de cas : La Chine

Figure 9: Source LeBigData.fr

Comment parler de la Reconnaissance Faciale sans citer la Chine ?

Avec près de 20 millions de caméras en service, le gouvernement chinois contrôle en temps réel et sur l'ensemble du territoire, le déplacement et le comportement de ses habitants. C'est le pays qui comptabilise le plus de caméra de Reconnaissance Faciale au monde. En 2018 la Chine a passé un nouveau cap pur imposer la Reconnaissance faciale sur son territoire, en effet pour acheter un smartphone les chinois doivent se soumettre à la technologie. Il existe un autre exemple montrant que cette technologie s'est imposée : Si le feu est rouge et qu'un piéton décide tout de même de traverser la route il se peut que son visage, son nom, et d'autres informations personnelles peuvent s'afficher sur les écrans de la ville. Avec l'apparition du covid-19 certains chinois se sont fait interpellés par des drones leur demandant de mettre leur masque.

Dans le domaine de la santé l'association de la performance du Deep Learning au système de Reconnaissance Faciale permet de :

- Suivre plus précisément la consommation de médicaments d'un patient ;
- Détecter une maladie génétique telle que le syndrome de DiGeorge avec un taux de réussite de 96,6%

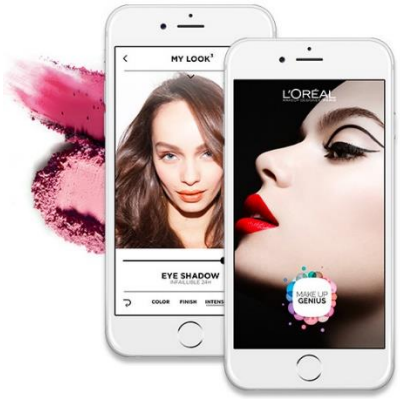
Cas d'étude : Face2Gene

L'application Face2Gene est le produit de recherches menées au sein du FNDA de Boston. Cette application identifie des centaines de maladies différentes. Pour que cette technologie soit opérationnelle, les chercheurs ont rentré une multitude de visage de patients dans une base de données tout en mentionnant leur maladie.

Enfin, la Reconnaissance Faciale fait ses preuves dans le secteur de la cosmétique. Que ce soit pour un usage dermo-cosmétique comme avec Poséidon, ou simplement esthétique comme avec L'Oréal.

Cas d'étude : Poséidon

Poséidon est un miroir connecté élaboré par la société Care Os. En sa possession l'utilisateur peut accéder à de nombreux services. Poséidon analyse sa peau et fournit des recommandations de produits en fonction des imperfections qu'il détecte.



Cas d'étude : L'Oréal

La filiale dévoile une application qui se révèle être un franc succès car elle comptabilise près de 20 millions de téléchargement.

En utilisant la Reconnaissance Faciale l'application permet à l'utilisateur de tester leur gamme de maquillages virtuellement.

FONCTIONNEMENT DE LA RECONNAISSANCE FACIALE

Dans un premier temps le logiciel va capturer une image de visage en utilisant l'Intelligence Artificielle pour détecter automatiquement la scène et d'optimiser automatiquement des paramètres pour améliorer la capacité de détection des images de la vidéo.

Example of iA effect

Figure 10 : Source business.panasonic.fr

Ensuite c'est au tour d'un algorithme d'Intelligence Artificielle de capturer les points caractéristiques du visage. Grâce à ces points elle va créer ce que l'on appelle une emprunte faciale. Les cheveux et les vêtements ne sont pas pris en compte. Cette empreinte faciale va être comparée à d'autres empreintes déjà référencée dans une base donnée. Et l'empreinte avec le plus haut taux de similitude sera retenue par le logiciel.

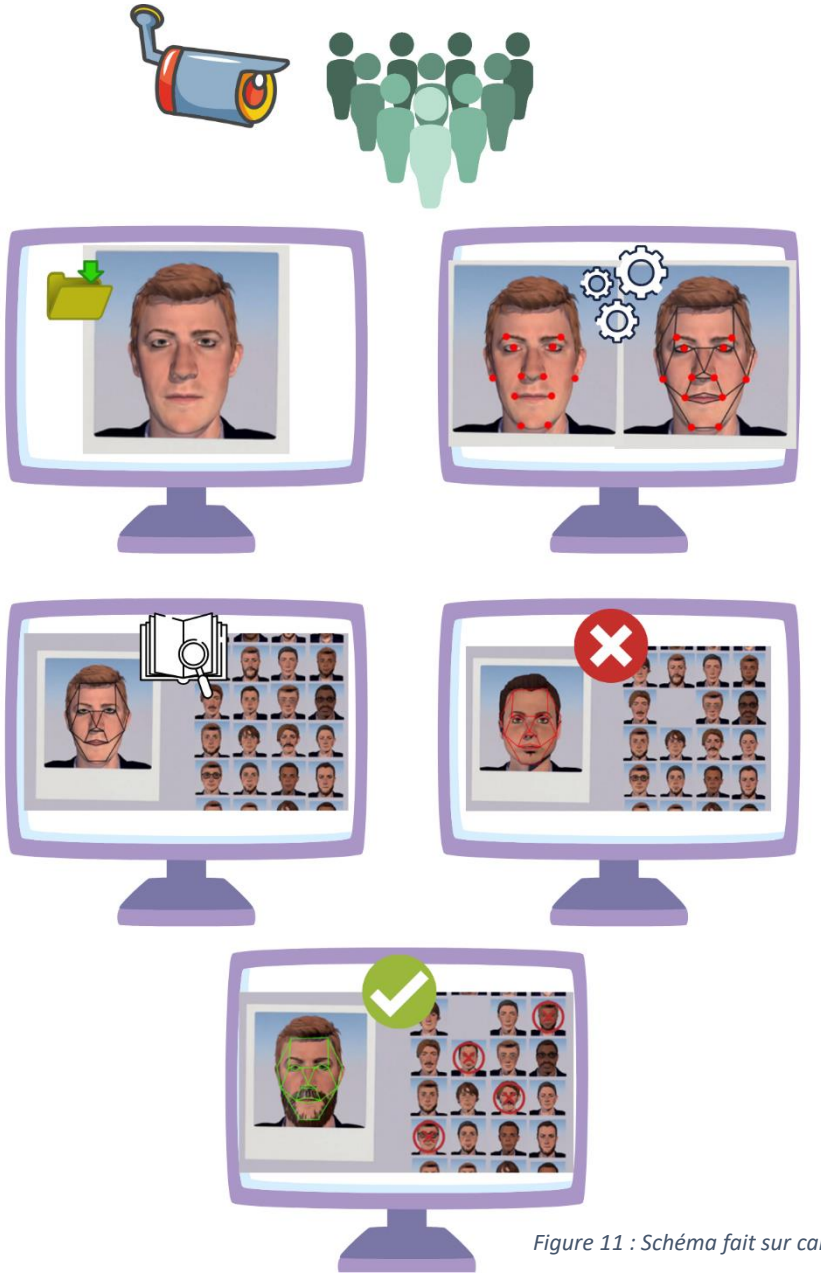


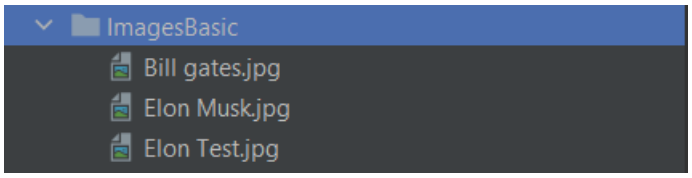
Figure 11 : Schéma fait sur canva

Il est possible de programmer un système de Reconnaissance Faciale en langage python.

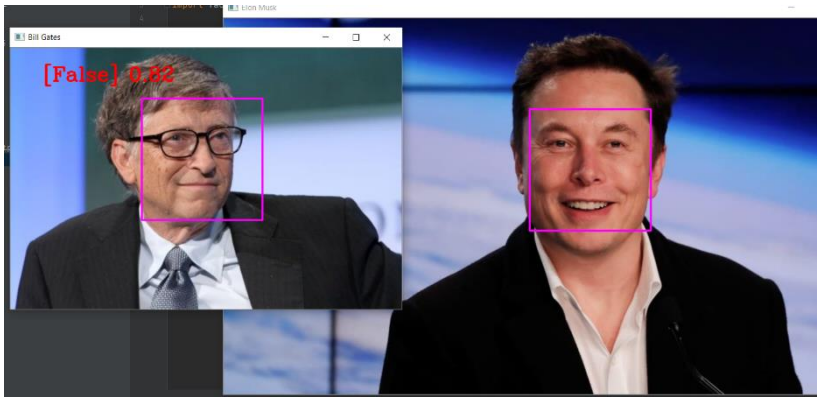
Dans cette partie je me suis inspirée du code de monsieur Murtaza Hassan qui a publié sa version de programmation d'une Reconnaissance Faciale sur la plateforme GitHub. Le code utilisé est mis en annexe.

SIMULATION DU CODE NUMERO 1

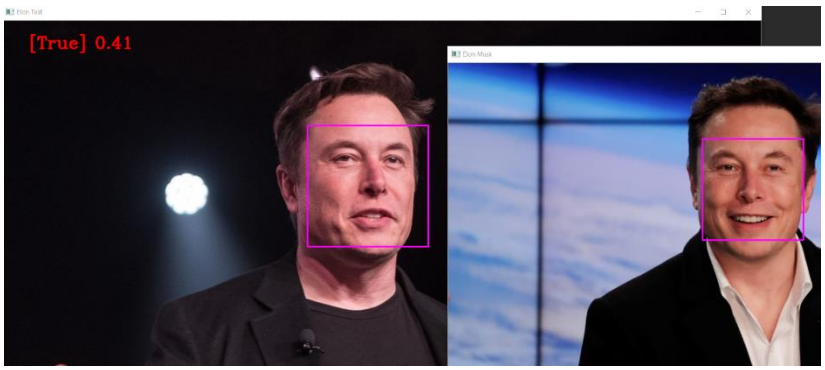
Ce premier projet consiste à comparer des images en utilisant la Reconnaissance Faciale. Tout d'abord il faut créer un dossier dans lequel nous déposons les images à comparer. Ceci correspond à notre base de données. Pour cet exemple nous avons renseigné 2 individus : Bill Gates et Elon Musk, puis Elon Test qui nous servira à faire les comparaisons. C'est-à-dire que le programme doit être en mesure d'identifier que Elon Test et Elon Musk sont la même personne, et que Elon Musk et Bill Gates sont deux individus différents.



Observons les résultats :



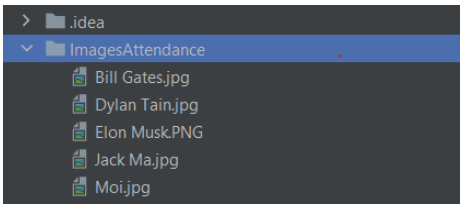
Le système fonctionne, il différencie Bill Gates de Elon Musk.



A nouveau le système fonctionne, il reconnaît Elon Musk dans les deux images.

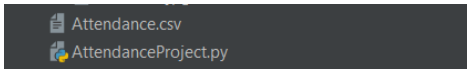
SIMULATION DU CODE NUMERO 2

Ce deuxième code est plus intéressant car il identifie en temps réel un individu en utilisant la caméra de notre ordinateur.



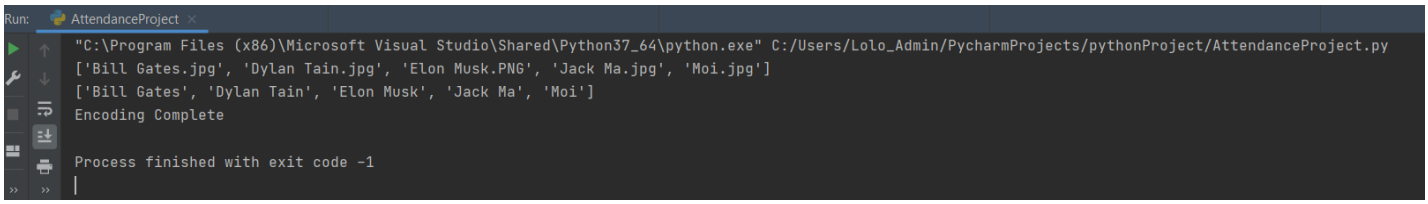
Tout d'abord nous devons créer une base de données servant de référence au système.

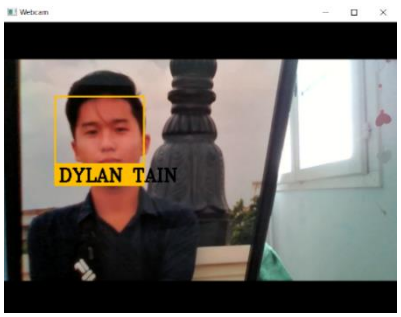
Ensuite il y a un fichier .csv, celui-là est utilisé pour enregistrer chaque individu que le système reconnaîtra et l'heure à laquelle l'individu a été capturé par la caméra.



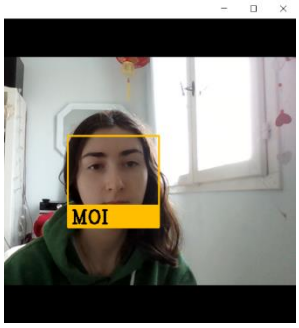
Le fichier .py est notre fichier principal contenant le code python du système de Reconnaissance Faciale.

Lorsqu'on exécute le programme un message apparaît dans le terminal. Ce message affiche le nom des individus qu'il connaît puis le nom qu'il affichera dans le cadre si cet individu est capté par la caméra. Une fois que le message Encoding Complete apparaît, la caméra s'allume.

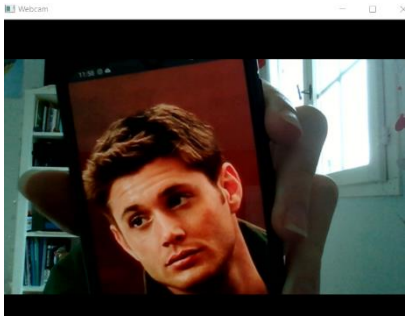




1er essai concluant, le système reconnaît Dylan Tain sur une image.



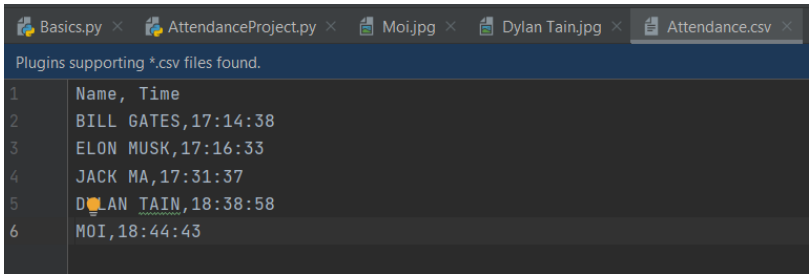
2eme essai concluant, en temps réel et en mouvement le système à réussi à me reconnaître.



3eme essai, si on place un individu non enregistré dans la base de données le système ne reconnaît pas le visage et l'ignore.

J'ai réalisé les mêmes tests sur les 3 personnages connus et le résultat était concluant.

Regardons maintenant le fichier .csv



Comme vous pouvez le constater chaque individu reconnu à été enregistré dans ce document en renseignant son nom et l'heure à laquelle il a été capturé par la caméra.

Ainsi à travers ces deux simulations nous avons pu tester la Reconnaissance Faciale par image statique et dynamique et temps réel.

EVOLUTION DE LA RECONNAISSANCE FACIALE

En 1949 l'auteur George Orwell publie un roman appelé 1984.

Dans ce livre l'écrivain décrit une société dans laquelle les citoyens sont surveillés en permanence par l'oeil de Big Brother.

Dans cette œuvre la population britannique est encadrée par un régime totalitaire où la liberté d'expression n'existe plus, et où chaque faits et gestes est surveillé.

Petit à petit nous pouvons observer le monde converger vers un modèle similaire. Avec l'arrivée et l'avancée de la technologie de Reconnaissance Faciale de nombreux gouvernement l'utilisent à des fins de surveillance de la population.

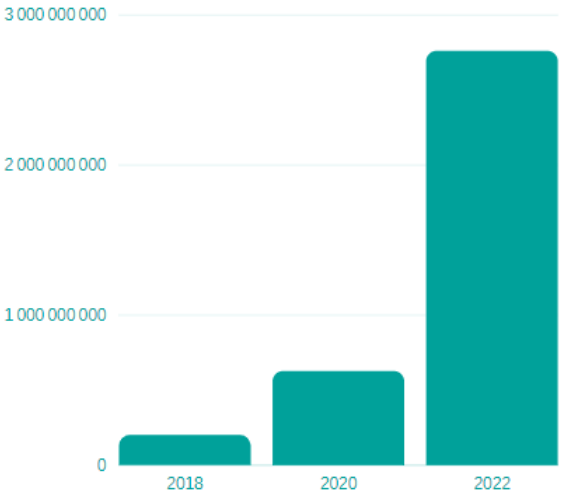
Cette partie vise à approfondir les possibilités d'avenir de la Reconnaissance Faciale et ses potentiels dangers pour l'humanité.

AVENIR DE LA RECONNAISSANCE FACIALE

REVOLUTION DES METHODE PAIEMENT

La Reconnaissance Faciale va être déployer dans de nombreux domaines tel que le commerce. Dans une société où chaque action doit être accélérée, certaines enseignes se dirige vers la Reconnaissance Faciale pour effectuer des paiements. Ce système éviterait les fraudes, serait un gain de temps considérable et allègerai les consommateurs qui n'auront plus besoin de transporter avec eux une carte bleue ou du liquide.

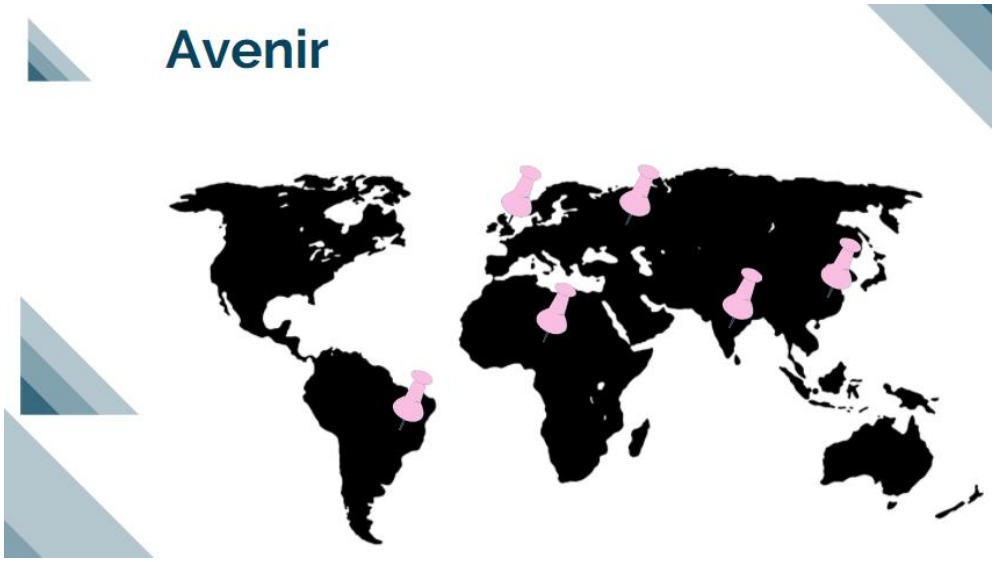
Nous avons vu précédemment qu'Apple aussi se tournait vers la Reconnaissance Faciale pour accéder à de nombreux services de paiement.



La Chine a également une ambition très forte en matière d'Intelligence Artificielle puisque le pays cible la première place pour 2030.

En 2018 la Chine avait installé 200 000 000 caméras, en 2020 on en observe 626 000 000, soit plus du triple du nombre de caméra présentent en 2018. Enfin la Chine a pour objectif de déployer 2,76 milliards de système de vidéosurveillance.

Le Brésil, a pour ambition de tenir une base de données qui devrait recenser environ 140 millions de citoyens pour 2020.



Un projet de loi a été rédigé contre ce projet car la centralisation de ces données présente une vulnérabilité d'être divulguée.

En Afrique, Huawei met en place de nombreuses caméras de vidéosurveillance.

En Russie, de nombreuses données biométriques sont collectées (scan visage, iris, empreinte digitale et voix) par la Banque Centrale.

L'Inde possède la plus grande base de données biométriques au monde avec plusieurs milliards d'individus recensés.

« Créer une Intelligence Artificielle serait le plus grand événement de l'histoire humaine. Malheureusement, ce pourrait être le dernier, à moins que nous découvrions comment éviter les risques. » Stephen Hawking

LA RECONNAISSANCE FACIALE, UN SYSTEME NE NECESSITANT PAS DE CONSENTEMENT POUR FONCTIONNER

Nous l'avons vu au début de ce rapport, la Reconnaissance Faciale et une méthode biométrique qui peut fonctionner sans avoir le consentement d'un individu. N'importe qui peut être surveillé sans en être conscient et sans avoir consentit d'être observé. Cette absence de consentement pose des problèmes à la liberté d'un individu. En effet la Reconnaissance Faciale est une entrave à la liberté de pouvoir se déplacer anonymement. Certains gouvernements respectent cette liberté comme en Europe et au Royaume Uni ou la Directive sur la protection des données (RGPD) encadre cette technologie. Elle interdit que la Reconnaissance Faciale soit déployée dans le but d'enquêter sur la vie privée de l'individu ou ses déplacements sous peine d'amendes. Cependant d'autres gouvernements comme aux états unis ne respectent pas cette liberté. C'est le cas dans 45 états ou la technologie fonctionne sans consentement explicite. « En France, la CNIL (Commission Nationale de l'Informatique et des Libertés) confirme que leur accord préalable n'est pas nécessaire lorsque l'intérêt public est en jeu. Cependant elle se veut prudente et propose d'étudier l'utilisation de ce dispositif biométrique au cas par cas, pour décider de sa légitimité ou non ». *Source leblogduherisson.com*

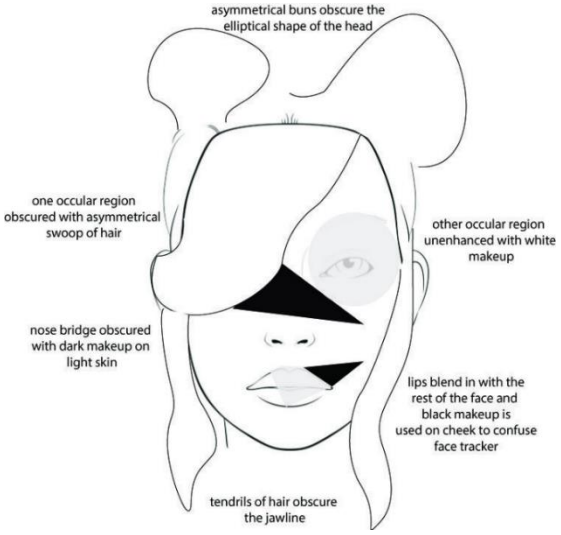
DES ACTIVISTES DEJOUENT LE SYSTEME DE RECONNAISSANCE FACIALE

L'usage de la Reconnaissance Faciale amène de nombreuses craintes sur sa fiabilité. Ces dernières années des militants ont mis au point des parades pour déjouer la surveillance des caméras.

En Russie, un militant a mis au point un algorithme dont l'objectif est de créer un maquillage particulier. En effet, le maquillage peut modifier certains points repères du visage aux yeux des logiciels de Reconnaissance faciale et donc rendre impossible l'identification.

En Allemagne un maquillage similaire à été mis au point, et sont allés plus loin avec la création de vêtements dont les motifs brouillent la détection.

D'autres solutions comme le logiciel Fawkes permet de modifier très légèrement les pixels d'une image, invisible à l'œil humain mais faisant une grande différence aux yeux d'un ordinateur.



CONFIDENTIALITE EN PERIL

La Reconnaissance Faciale soulève aussi de nombreuses craintes et inquiétudes concernant la sécurité et la confidentialité. Dans une société où les attaques d'hacker se multiplient, cette technologie engendre le risque qu'une personne mal intentionnée accède aux données collectées par cette technologie. Cette crainte est fondée, en 2017, une société vietnamienne a réussi à hacker Face ID d'Apple en utilisant un masque.

Une autre crainte serait que les autorités et les entreprises privées utilise la Reconnaissance Faciale pour pister des individus. Grâce à ces données ces entreprises seraient en mesure d'établir un " profil "précis pour chaque individu étudié. Le fait d'établir ce profil est un danger à l'individu d'être manipulé car il serait possible par la suite de prédire le comportement à des fins de prévention du crime ou de ciblage publicitaire.

LA RECONNAISSANCE FACIALE PEUT VOUS CONFONDRE AVEC UN CRIMINEL

La Reconnaissance Faciale manque de fiabilité. En se développant les ingénieurs ont réussi à améliorer les performances du système, en effet le taux d'erreur est passé de 4% à 0,2% mais certaines erreurs persistent.

Ces erreurs peuvent être dues à une capture d'images trop floues, un éclairage trop ou peu intense, des visages maquillés ou accessoirisés. Il existe aussi le risque de vieillissement qui impacte l'identification et le fait que l'algorithme est entraîné majoritairement sur des hommes blancs ce qui implique que le logiciel peut avoir du mal à identifier les femmes ou les personnes de couleur. Toutes ces erreurs peuvent mener le logiciel à confondre des individus, ce qui peut être extrêmement dangereux dans certains cas.

« *En 2018, lors d'un test mené par ses soins, l'ACLU a découvert que le logiciel Amazon Rekognition a confondu 28 membres du Congrès américain avec des criminels. Les concernés étaient principalement des personnes afro-américaines ou d'origine latine. Ce manque de précision à l'égard des minorités amplifie le risque que des innocents soient accusés à tort.* » Source : LeBigData

TEMOIGNAGE

Dans l'objectif d'apporter un complément et d'éclaircir certains points sur la Reconnaissance Faciale j'ai contacté Franck Bardol pour répondre à quelques questions.

Profil LinkedIn :

« Je suis expert dans la Transformation Numérique par les Algorithmes et la Data. Je suis formateur en entreprises et j'enseigne en Grandes Écoles (École Microsoft IA, ISEP, Media School) les méthodes de l'Intelligence Artificielle. Je suis diplômé en Intelligence Artificielle, en Gestion d'entreprises et en Éthique philosophique. »

RETRANSCRIPTION DU TEMOIGNAGE DE MONSIEUR FRANCK BARDOL.

Monsieur Franck Bardol incite les étudiants à sortir de la technique et à se pencher sur les enjeux qu'elle représente.

« Les élèves ingénieurs sont bombardés par la technique : programmation, mathématiques etc. A mon sens ils ne passent pas assez de temps à réfléchir à toutes ces techniques qui maintenant émergent et qui modifient notre quotidien. Et pour réfléchir à ses techniques il faut pouvoir sortir de la technique. »

Comment définiriez-vous la Reconnaissance Faciale ?

« Pour ma part, je définis la Reconnaissance Faciale comme l'ensemble des procédés techniques destinés à identifier une personne à partir de l'analyse de son visage par un programme informatique. Pour ce faire, en premier lieu, le programme informatique élabore et réalise une cartographie du visage ou aussi appelé gabarit. On parle alors de signature numérique. »

Quelles sont les utilisations de cette technologie ?

« A partir de la réalisation de ce gabarit on va voir qu'il y a deux utilisations de Reconnaissance Faciale qui ont chacune une portée différente. La première utilisation est l'authentification. La deuxième utilisation du gabarit est l'identification.

Qu'est-ce que l'authentification ?

« Authentifier : il s'agit tout simplement de prouver que l'on est bien la personne que l'on prétend être. Comme un acte notarié où l'on doit apporter des documents pour prouver son identité. L'important dans l'authentification est que notre consentement est présupposé parce que si je cherche à prouver mon identité cela dit bien que je suis dans une démarche volontaire et donc mon consentement est réalisé. On fournit un élément de preuve qui est notre visage on parle donc de Reconnaissance Faciale afin d'accéder à un service. C'est donc mon visage qui va m'authentifier. Notre participation est active et notre consentement est explicite. Des exemples classiques : le portique d'aéroport qui s'ouvre après lecture et analyse du visage du voyageur, ça peut être aussi un déverrouillage du téléphone mobile avec une caméra, un paiement en ligne sécurisé etc. Concernant l'authentification le questionnement de l'aspect éthique est questionné à la marge mais est moins important que l'aspect éthique de l'identification. Dans l'authentification on parle plus de fracture numérique par exemple : comment feront ceux qui ne disposent pas de téléphone mobile pour accéder à ces services ? Si vous avez un entourage jeune, tout le monde est connecté vous avez l'impression que tout le monde a un téléphone portable mais dans la réalité ce n'est pas le cas. Beaucoup de gens n'ont pas de téléphone mobile, d'ordinateur ou de

caméra et ne pourraient pas accéder aux services. Donc on peut aussi se demander s'il est raisonnable de généraliser ces dispositifs dans les services publiques ? »

Qu'est-ce que l'identification ?

« Identifier : ici on parle d'une chaîne de traitement qui vise tout d'abord à détecter un visage parmi d'autres, le plus généralement dans une foule. Puis à l'issu de cette phase de détection, identifier le visage afin de lui réserver un traitement adéquat. Donc un traitement adéquat ça peut être : déclencher une alerte, un dispositif de sécurité etc. Ici le plus souvent on ne donne pas son consentement explicite, on ne nous donne pas le choix. Cela peut arriver par exemple lorsque l'on rentre dans une zone où il y a un panneau avec écrit zone sous vidéosurveillance, mais notre consentement est forcé car si on souhaite rentrer dans la zone nous n'avons d'autres choix que de se soumettre aux cameras. Donc la lecture et l'analyse de notre visage est faite à notre insu.
On comprend donc que les enjeux de ces deux fonctions ne sont pas les mêmes. Il faut donc bien distinguer la reconnaissance active de la reconnaissance passive, donc entre l'identification et l'authentification »

Quel est votre avis général concernant la Reconnaissance Faciale ?

« Moi ce que j'observe, on nous la présente comme un pinacle de technologies abouties, modernes, fiables, indolores, neutres, or il n'en est rien. On va passer en revue quelques expérimentations et observer les résultats. Pour commencer, le carnaval de Notting Hill à Londres a vu se dérouler une expérimentation en 2018 de Reconnaissance Faciale active en grandeur réelle. Imaginez un énorme carnaval, où vous n'avez pas le choix car si vous voulez vous soustraire au système de reconnaissance il faut contourner la zone d'au moins 1km. Seul une centaine de personnes l'ont contourné parce qu'ils n'étaient pas d'accord avec cette expérimentation. Cependant à l'issus de ce détour il y avait un cordon de policier qui les attendait car ceux qui faisaient ce détour étaient considérés comme étant suspect. Ce qui en dit long sur le procédé. Donc bien entendu le but était d'identifier les personnes recherchées par la police anglaise. Ils ont procédé à plusieurs dizaines d'arrestations en croyant appréhender les individus recherchés, ensuite ils se sont livrés à une vérification de leurs identités. Le résultat de cette expérimentation est que tous les individus ont été relâchés. L'identification a échoué pour chacun d'entre eux. Le seul qui a été retenu plus longtemps avait déjà eu des problèmes avec la justice mais avait été disculpé mais son profil était toujours conservé par la police.

Donc la Reconnaissance Faciale échoue ?

« Oui, ce que l'on peut dire c'est que cette technologie échoue, mais encore plus pour certaines populations. On parle des gens de couleur et des femmes. Pour les femmes, la raison est que le maquillage influence la Reconnaissance Faciale, toutes modifications (cheveux attachés, détachés, accessoires) fragilisent la Reconnaissance Faciale, un autre facteur est qu'il y a moins de femmes dans les bases de données donc leurs algorithmes ont été moins entrainé à reconnaitre des femmes. Pour la même raison, les algorithmes échouent avec les gens de couleur car il y en a moins dans les bases de données. Il y a majoritairement des hommes blancs entre 20 et 40 ans.

Est-ce qu'il y a des solutions misent en place pour palier à ces problèmes de diversité dans les bases de données ?

« Pour palier à ces failles, la Chine qui est un grand pourvoyeur de Reconnaissance Faciale, acquiert des gigantesques bases de données de populations africaines entières. En échange de ces bases de données les gouvernements africains bénéficient des infrastructures de Reconnaissance Faciale. Par exemple la firme Cloud Walk a procédé à ce genre d'échange avec le Zimbabwe et le Ouganda. De nombreuses associations contestent ces procédés parce qu'on parle de dizaine de millions de visages d'individus qui n'ont a aucun moment donné leur consentement.

Dans une autre expérience, des chercheurs se sont amusés à comparer les membres du Congrès, en utilisant les technologies les plus récentes, avec des fichiers de 25 000 délinquants. A priori le programme ne devrait faire aucune correspondance avec les membres et les délinquants. Pourtant le programme Amazon Rekognition a reconnu 28 membres du Congrès comme délinquants notoires. On parle donc de faux positif : les gens que le système reconnait mais qu'il ne devrait pas, et de faux négatifs, les gens qui devraient être reconnu mais qui ne le sont pas. On a donc des résultats toujours questionnables. »

Mais alors si ça ne fonctionne pas, pourquoi on en parle-t 'on ?

« En fait si, il y a de très bons résultats mais il faut des conditions idéales en matière de lumière d'ambiance, de pixélisation, d'angle de prise etc. Le cadre doit être parfaitement contrôlé. Le vieillissement du visage n'est pas pris en compte par l'algorithme. Il y a des études avec deux photos d'un même individu avec 1 an d'écart, le programme échoue. Pour conclure sur cette question, ce qui me frappe dans cette technologie de reconnaissance active c'est cette disproportion entre le traitement de masse que l'on applique et le résultat finalement assez médiocre. Sans compter la suspicion et les bavures à venir si on adopte de manière massive cette technologie. »

Selon vous quels sont les dangers si le gouvernement venait à implanter cette technologie dans notre quotidien ? (Tel que la Chine)

« Selon moi les usages les plus problématiques concernent donc ceux de la reconnaissance active. En ce moment on assiste à des expérimentations sauvages qui se multiplient un peu partout en France. Il y a eu des expérimentations à Lille, à Nice, à Marseille etc. A l'issu de ces expérimentations, le premier risque est de banaliser la technologie. La stratégie des industriels est de créer un usage. Le besoin va découler alors naturellement. De ce fait la technologie va se fondre dans le paysage de nos villes sans qu'on y prenne garde. Il faut donc bien comprendre que l'outils créé l'usage, l'usage créé le besoin. Il faut aussi prendre en compte qu'on utilise le mot outil mais il faut plutôt utiliser infrastructure, avec des caméras, de portiques de détections, des centres de contrôle, des ordinateurs, des programmes de reconnaissances etc.
Ensuite autre danger, la conformité avec la réglementation n'est pas acquise par ce système, principalement ils sont en infraction avec le RGPD, Règlement générale de protection des données. Le tribunal administratif de Marseille affirme que l'usage de portique dans les lycées n'est pas conforme à la politique de RGPD. Des associations de parents d'élèves ont refusé, le tribunal a dit non. Ils ont dû désinstaller les portiques. »

Pour quelles raisons ?

« Les disproportions entre la taille de l'infrastructure vis à vis de ses faibles résultats, et le manque de consentement font que le système à été retiré. Ce dispositif portait aussi atteinte a des libertés fondamentales : intimité, vie privé, droit à l'anonymat. »

Ces libertés sont aussi bafouées en Chine ?

« Effectivement, la vice-présidente de la commission européenne en charge du numérique, Margrethe Vestager a visité Hongkong et a dit « ce que j'ai vu à Hongkong m'a véritablement effrayée ». Lorsqu'un manifestant pro-démocratique passait par les portiques il recevait un sms disant : Nous savons que vous êtes là vous devriez rentrer chez vous. ». On assiste donc à la fin d'une liberté fondamentale. Avec tous ces éléments le contrôleur européen pour la protection des données a pris position dans un arrêt pour une interdiction temporaire de la reconnaissance active dans les lieux publics. Mais après discussion avec de industriels ils ont remis en cause ce moratoire. »

En tant qu'expert quelles seraient vos recommandations pour limiter les risques qu'engendre la reconnaissance faciale ?

« J'ai repris ce que dit la CNIL qui met en garde contre la reconnaissance active. Dans un rapport elle parle d'« un glissement progressive qui aboutit à un changement de société » la commission conclue également que le politique devrait évaluer les risques et interdire certains usages. En ce qui me concerne, le risque est que si on autorise la reconnaissance passive (authentification) même si on le fait dans un cadre précis et réglementer, cela va en banaliser l'usage. Les gens vont s'habituer à ce que l'on scanne leur visage et ce sera la porte ouverte pour la reconnaissance active qui compte plus de danger. On pourrait autoriser cette authentification dans un usage militaire mais je reste dubitatif. Concernant le grand public avec Alicem par exemple le glissement intervient. »

Que pensent les ingénieurs de la Reconnaissance Faciale ?

« En ce qui concerne l'aspect technique, Microsoft demande la régulation par le législateur européen. Il ne faut surtout pas selon moi dire que la technologie est neutre et que ce sont les usages qui doivent être régulé, parce que contrôler les usages ne suffit pas. La technologie n'est pas neutre, ce sont des infrastructures et une fois qu'elles sont là on ne peut plus les débrancher. Dernier exemple, l'Inde collecte la plus grande quantité de données biométriques au monde. Le programme s'appelle Aadhaar. On parle du plus gros programme au monde qui a débuté en 2010. Ils ont collecté les données de milliard d'individus. Pour justifier ces expérimentations le gouvernement indiens disait qu'il voulait retrouver les enfants perdus. Il faut savoir que maintenant il permet de traquer des opposants politiques. Pour conclure selon moi il faut interdire tous les usages de reconnaissance active. Une fois stabilisées, ces technologies permettront de contrôler indistinctement une population, ce sont des technologies liberticides by design. »

Il y a des bases de données pour faire fonctionner la Reconnaissance Faciale, certaines sont plus complètes que d'autres en termes d'informations. N'était-ce pas dangereux de réunir autant d'information surtout dans une aire ou le hacking se développe ?

« Absolument c'est extrêmement problématique il y a le danger de se faire dérober toutes ces informations biométriques. »

On peut voir sur nos téléphones plusieurs moyens de déverrouillages, le mot de passe traditionnel, le schéma, les méthodes biométriques avec l'empreinte digitale. Pensez-vous que la Reconnaissance Faciale est la méthode la plus sécurisée ?

« Je pense que le verrouillage par Reconnaissance Faciale ne devrait pas être utilisé, personnellement je ne l'utilise pas même si j'ai un appareil Samsung qui est équipé de cette technologie pour les raisons dont on a parlé même si ce sont des reconnaissances passives. Moins je l'utilise, moins de gens l'utilisent moins ça donne d'arguments pour ceux qui veulent nous imposer le Reconnaissance Faciale active. On a bien vu que la Reconnaissance Faciale passive est le cheval de trois vers Reconnaissance Faciale active. En ce qui me concerne la double vérification mot de passe plus sms devrait faire l'affaire. »

CONCLUSION

L'objectif de cette veille technologie est d'étudier la technologie de Reconnaissance Faciale sous ses diverses formes. Nous avons vu ces deux déclinaisons avec l'usage par authentification et par identification qui soulèvent déjà de nombreuses questions sur la place de cette technologie au sein de la société. Tout d'abord par ses nombreuses failles de système : technologie non neutre, des bases de données très peu diversifiées, infrastructures coûteuses mais aussi ses failles portant atteintes aux libertés fondamentales comme le consentement ou le droit à l'anonymat.

La Reconnaissance Faciale est présentée comme une technologie qui se veut rassurante et comme étant un pilier de sécurité à l'échelle personnelle (déverrouillage de nos smartphones) et à l'échelle d'une population (contrôle des accès pour limiter la menace terroriste). Les gouvernements la présentent aussi comme une technologie qui se veut bienveillante et nécessaire comme en Inde où elle est présentée pour retrouver des enfants disparus. Cependant au long de cette veille nous avons pu voir que les industriels et les gouvernements utilisent aussi cette même technologie pour encadrer et surveiller les agissements de ses habitants et pister les opposants. Le cas de la Chine nous permet de visualiser les conséquences d'une forte utilisation de Reconnaissance Faciale, libertés inexistantes, contrôle totale de la population, consentement aucunement spécifié.

Malgré toutes ses failles, la Reconnaissance Faciale peut s'avérer d'une grande utilité dans certains domaines. Nous avons pu exposer le cas de Face2Genes qui permet de détecter des maladies plus rapidement.

Ainsi selon moi, avec tout ce que nous avons pu apprendre au long de ce rapport, je rejoins l'avis des ingénieurs et de Franck Bardol qui consiste à limiter et réglementer la technologie. A mes yeux cette technologie n'est pas suffisamment fiable pour être déployée massivement et le fait que seulement 3.8 milliards d'individus aient accès à internet prouve qu'il y aurait des soucis de discriminations quant à l'accès au service par Reconnaissance Faciale comme la France qui souhaite mettre en place Alicem. De plus, la population n'aura aucun contrôle sur la gestion de ces données numérique et biométriques, le France pourrait très bien échanger ses bases de données avec d'autres pays comme le fait déjà la Chine. A mon avis la Reconnaissance Faciale doit être employée sur des actions précises comme pour la médecine où cette technologie peut venir en aide à l'humain. Pour ma part la solution serait une destruction instantanée des données biométriques une fois que l'authentification est établie comme le propose l'entreprise Thales avec son application où la vérification se fait de manière instantanée au niveau locale et détruit la photographie une fois que la comparaison est établie.

ANNEXE

Code de Monsieur Murtaza Hassan, en ligne sur GitHub.

1er projet

Basics.py | AttendanceProject.py | Moi.jpg | Dylan Tain.jpg | Attendance.csv | Elon Musk.PNG | Bill gates.jpg | Bill Gates.jpg | Jac

```python
import cv2
import numpy as np
import face_recognition

imgElon = face_recognition.load_image_file('ImagesBasic/Elon Musk.jpg')
imgElon = cv2.cvtColor(imgElon, cv2.COLOR_BGR2RGB)
imgTest = face_recognition.load_image_file('ImagesBasic/Bill gates.jpg')
imgTest = cv2.cvtColor(imgTest, cv2.COLOR_BGR2RGB)

faceLoc = face_recognition.face_locations(imgElon)[0]
encodeElon = face_recognition.face_encodings(imgElon)[0]
cv2.rectangle(imgElon, (faceLoc[3], faceLoc[0]), (faceLoc[1], faceLoc[2]), (255, 0, 255), 2)

faceLocTest = face_recognition.face_locations(imgTest)[0]
encodeTest = face_recognition.face_encodings(imgTest)[0]
cv2.rectangle(imgTest, (faceLocTest[3], faceLocTest[0]), (faceLocTest[1], faceLocTest[2]), (255, 0, 255), 2)

results = face_recognition.compare_faces([encodeElon], encodeTest)
faceDis = face_recognition.face_distance([encodeElon], encodeTest)
print(results, faceDis)
cv2.putText(imgTest, f'{results} {round(faceDis[0], 2)}', (50, 50), cv2.FONT_HERSHEY_COMPLEX, 1, (0, 0, 255), 2)

cv2.imshow('Elon Musk', imgElon)
cv2.imshow('Elon Test', imgTest)
cv2.waitKey(0)
```

2eme projet

```python
import cv2
import numpy as np
import face_recognition
import os
from datetime import datetime #bibliotheque

# from PIL import ImageGrab

path = 'ImagesAttendance'
images = []
classNames = []
myList = os.listdir(path)
print(myList)
for cl in myList:
    curImg = cv2.imread(f'{path}/{cl}')
    images.append(curImg)
    classNames.append(os.path.splitext(cl)[0])
print(classNames)


def findEncodings(images):
    encodeList = []
    for img in images:
        img = cv2.cvtColor(img, cv2.COLOR_BGR2RGB)
        encode = face_recognition.face_encodings(img)[0]
        encodeList.append(encode)
    return encodeList
```

```
def markAttendance(name):
    with open('Attendance.csv', 'r+') as f:
        myDataList = f.readlines()
        nameList = []
        for line in myDataList:
            entry = line.split(',')
            nameList.append(entry[0])
        if name not in nameList:
            now = datetime.now()
            dtString = now.strftime('%H:%M:%S')
            f.writelines(f'\n{name},{dtString}')

#### FOR CAPTURING SCREEN RATHER THAN WEBCAM
# def captureScreen(bbox=(300,300,690+300,530+300)):
#     capScr = np.array(ImageGrab.grab(bbox))
#     capScr = cv2.cvtColor(capScr, cv2.COLOR_RGB2BGR)
#     return capScr

encodeListKnown = findEncodings(images)
print('Encoding Complete')

cap = cv2.VideoCapture(0)

while True:
    success, img = cap.read()
# img = captureScreen()
    imgS = cv2.resize(img, (0, 0), None, 0.25, 0.25)
    imgS = cv2.cvtColor(imgS, cv2.COLOR_BGR2RGB)

    facesCurFrame = face_recognition.face_locations(imgS)
    encodesCurFrame = face_recognition.face_encodings(imgS, facesCurFrame)

    for encodeFace, faceLoc in zip(encodesCurFrame, facesCurFrame):
        matches = face_recognition.compare_faces(encodeListKnown, encodeFace)
        faceDis = face_recognition.face_distance(encodeListKnown, encodeFace)
# print(faceDis)
        matchIndex = np.argmin(faceDis)

        if matches[matchIndex]:
            name = classNames[matchIndex].upper()
            # print(name)
            y1, x2, y2, x1 = faceLoc
            y1, x2, y2, x1 = y1 * 4, x2 * 4, y2 * 4, x1 * 4
            cv2.rectangle(img, (x1, y1), (x2, y2), (0, 191, 255), 2) #couleur du cadre
autour du prenom
            cv2.rectangle(img, (x1, y2 - 35), (x2, y2), (0, 191, 255), cv2.FILLED)
#couleur du cadre autour du visage
            cv2.putText(img, name, (x1 + 6, y2 - 6), cv2.FONT_HERSHEY_COMPLEX, 1, (0, 0,
0), 2) #couleur du texte
            markAttendance(name)

    cv2.imshow('Webcam', img) #afficher sur l'écran la webcam
    cv2.waitKey(1)
```

BIBLIOGRAPHIE

Points historiques

- https://www.wedemain.fr/inventer/9-dates-qui-ont-marque-l-essor-de-la-reconnaissance-faciale_a4568-html/
- https://www.coe.int/fr/web/artificial-intelligence/history-of-ai
- https://penseeartificielle.fr/focus-comment-marche-la-reconnaissance-faciale/
- https://web2day.co/event/etat-de-lart-de-la-reconnaissance-faciale/

Intelligence Artificielle et Reconnaissance Faciale

- https://www.lebigdata.fr/reconnaissance-faciale-tout-savoir
- https://www.lebigdata.fr/reconnaissance-faciale-tout-savoir#:~:text=La%20reconnaissance%20faciale%20est%20une,dans%20une%20base%20de%20donn%C3%A9es.
- https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/biometrie/reconnaissance-faciale

Reconnaissance Faciale et son implantation dans notre quotidien

- https://techtomed.com/usages-de-la-reconnaissance-faciale-en-sante/
- https://www.rtl.fr/actu/international/chine-la-reconnaissance-faciale-une-arme-politique-et-industrielle-7799652259
- https://www.youtube.com/watch?v=AuxgoNMqLFU
- https://business.panasonic.fr/solutions-de-securite/technologies-de-securite/reconnaissance-faciale
- https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/biometrie/reconnaissance-faciale
- https://www.latribune.fr/technos-medias/innovation-et-start-up/comment-la-reconnaissance-faciale-transforme-deja-notre-quotidien-836660.html
- https://www.mazarine.com/fr/loreal-realite-virtuelle-innovation-beaute
- https://www.leparisien.fr/economie/aeroports-de-roissy-et-d-orly-des-controles-par-reconnaissance-faciale-pour-embarquer-29-06-2018-7799964.php

Reconnaissance Faciale fonctionnement

- https://www.youtube.com/watch?v=189Y7u6moT8
- https://www.cnil.fr/fr/definition/reconnaissance-faciale
- https://business.panasonic.fr/solutions-de-securite/technologies-de-securite/reconnaissance-faciale
- https://www.youtube.com/watch?v=acYXeFSGYuA
- https://business.panasonic.fr/solutions-de-securite/technologies-de-securite/reconnaissance-faciale

Code python d'un programme de Reconnaissance Faciale

- https://www.youtube.com/watch?v=54WmrwVWu1w
- https://www.youtube.com/watch?v=pfDmUDPD7UQ

Avenir

- https://www.lesnumeriques.com/vie-du-net/en-chine-kfc-suggere-menus-grace-a-reconnaissance-faciale-n58739.html
- https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/biometrie/reconnaissance-faciale
- https://www.bfmtv.com/economie/entreprises/services/la-chaine-de-fast-food-kfc-teste-les-menus-a-la-tete-du-client_AN-201701040152.html
- https://www.rtl.fr/actu/international/chine-la-reconnaissance-faciale-une-arme-politique-et-industrielle-7799652259
- https://www.youtube.com/watch?v=AuxgoNMqLFU
- https://www.usinenouvelle.com/editorial/la-reconnaissance-faciale-progresse-en-france.N1025999
- https://siecledigital.fr/2018/04/25/inde-reconnaissance-faciale-retrouver-3000-enfants-disparus-4-jours/#:~:text=Selon%20la%20cha%C3%AEne%20d'information,grand%20nombre%20d'enfants%20disparus.&text=De%20fait%2C%20le%20minist%C3%A8re%20en,les%20photos%20des%20enfants%20recherch%C3%A9s.

Danger

- https://www.youtube.com/watch?v=x1JInKKbSq8
- https://www.laquadrature.net/2019/11/18/la-reconnaissance-faciale-des-manifestants-est-deja-autorisee/
- https://www.lci.fr/high-tech/reconnaissance-faciale-peut-on-y-echapper-2136346.html
- https://usbeketrica.com/fr/article/un-maquillage-pour-contrer-la-reconnaissance-faciale
- https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse220-FR.pdf
- https://www.francetvinfo.fr/replay-radio/le-monde-est-a-nous/en-chine-difficile-dechapper-a-la-video-surveillance_4194301.html