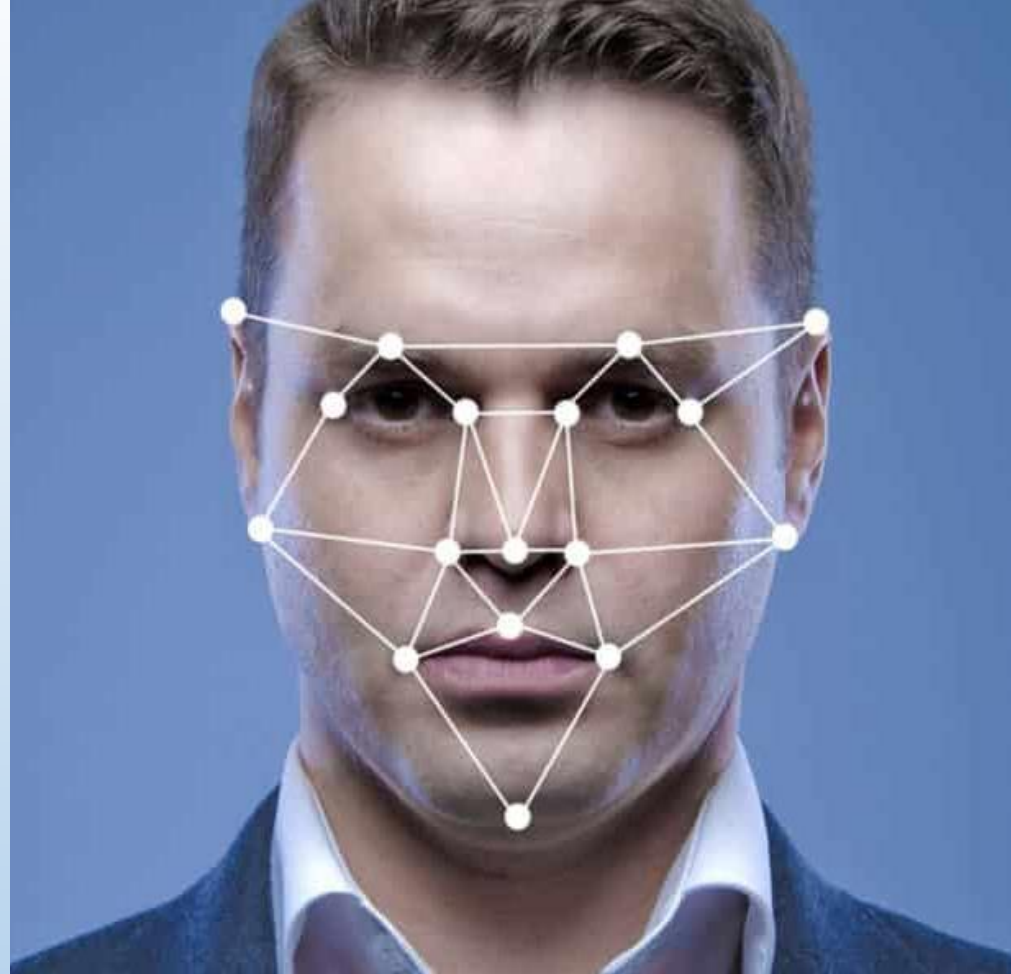


IA et Nous

Reconnaissance faciale

Reconnaissance faciale



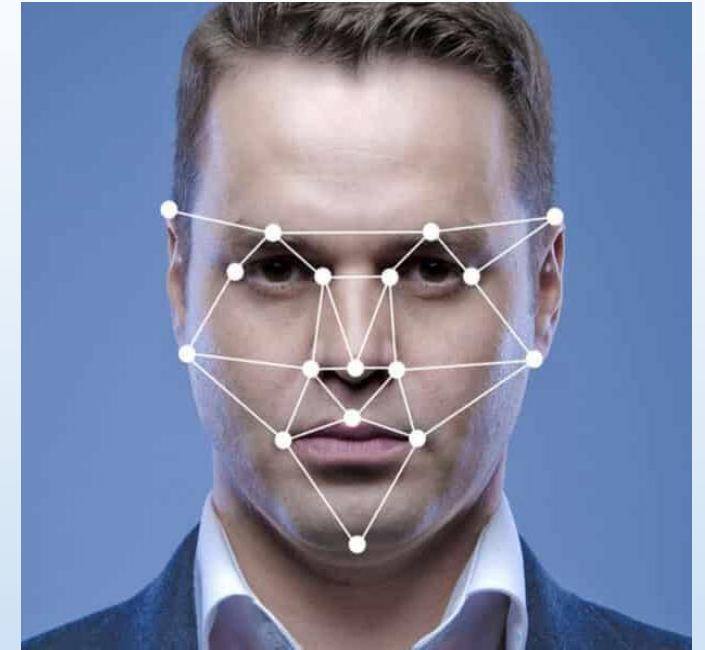
Reconnaissance faciale

Lecture de la *géométrie du visage*.

80 éléments au total → *signature faciale*.

Une signature faciale se présente sous forme mathématique. Elle sert à comparer le visage détecté aux visages contenus dans la base de données.

Principaux éléments : *la distance entre les yeux, la profondeur de l'orbite, la longueur de la mâchoire et la forme de la pommette.*



Le taux d'erreur de la reconnaissance faciale diminue au fil des ans. Ce taux est passé de 4,1% en 2014 à seulement 0,8% à l'heure actuelle.

Ce qui confirme son utilité, notamment en termes de sécurité.

Selon le NIST, l'organisation américaine des standards et normes, la précision des logiciels de reconnaissance a été multipliée par 50 en l'espace de 6 ans seulement.

Reconnaissance faciale

3 méthodes de reconnaissance faciale :

- **Système traditionnel** : identification d'une personne à partir d'une photo ou d'une image/vidéo 2D, en temps réel ou différé.
- **Système 3D** : utilisation d'un scanner 3D pour capturer la ressemblance d'un visage en temps réel.
- **Système biométrique** : analyse des contours du visage, des caractéristiques et des mesures, et d'autres caractéristiques (peau, iris,...) pour valider l'identité d'une personne.

Le système traditionnel

Étape 1 : Détection

Méthodes de détection d'objets dans une image.

Classe -Bounding Box

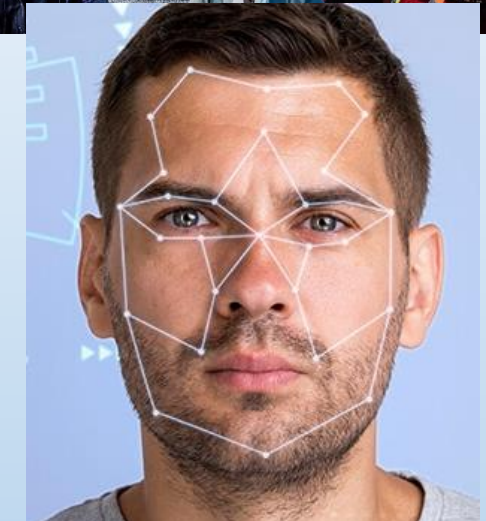


Étape 2 : Analyse

Identification caractéristiques biométriques et faciales uniques (espace entre le nez et la bouche, taille des sourcils, largeur du front, etc.

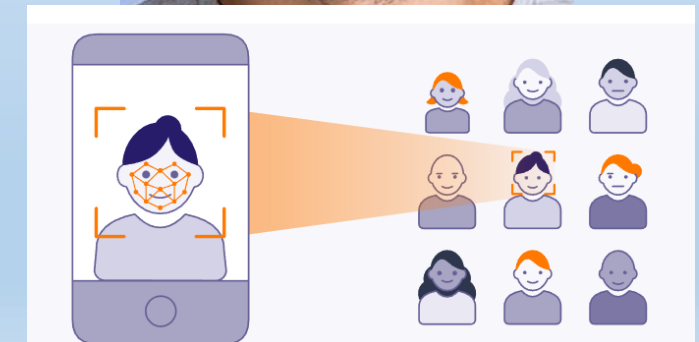
Points nodaux. En moyenne environ 80.

Conversion en numérique → empreinte faciale.



Étape 3 : Identification

Comparaison de l'empreinte faciale avec d'autres empreintes de la base de données pour trouver une correspondance.



Reconnaissance faciale 3D

Étape 1 : Détection

Capture en tant qu'image 3D par les **caméras de reconnaissance faciale** ou en scannant une photo 2D.

Étape 2 : Alignement

Le logiciel de reconnaissance faciale détermine **la position et l'angle du visage**, ainsi que sa taille..

Étape 3 : Mesure

Mesure (au millimètre près) de **la forme particulière du visage**. Création du modèle.

Étape 4 : Représentation

le système prend le modèle unique qu'il a créé à partir des caractéristiques du visage et le **convertit en code**.

Étape 5 : Correspondance

Recherche dans la base de données pour trouver une correspondance avec le modèle

Si la base de données contient des images 2D, le logiciel utilise un algorithme pour convertir l'image faciale 3D en 2D.

Étape 6 : Vérification ou identification

Pour **l'identification**, le scan est comparé à toutes les photos de la base de données

La **vérification** permet de confirmer l'identité, en faisant correspondre le scan avec une image (ex : photo)

Biométrie

*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.*

Un capteur 2D ou 3D « saisit » un visage, puis le transforme en données et le compare à la base de données.

*C'est une réplique fidèle et « augmentée » du **processus à l'œuvre dans le cerveau humain**.*

L'analyse de la texture de la peau sur une section de la peau, en utilisant un algorithme pour effectuer des mesures très minutieuses des lignes, des textures et des pores.

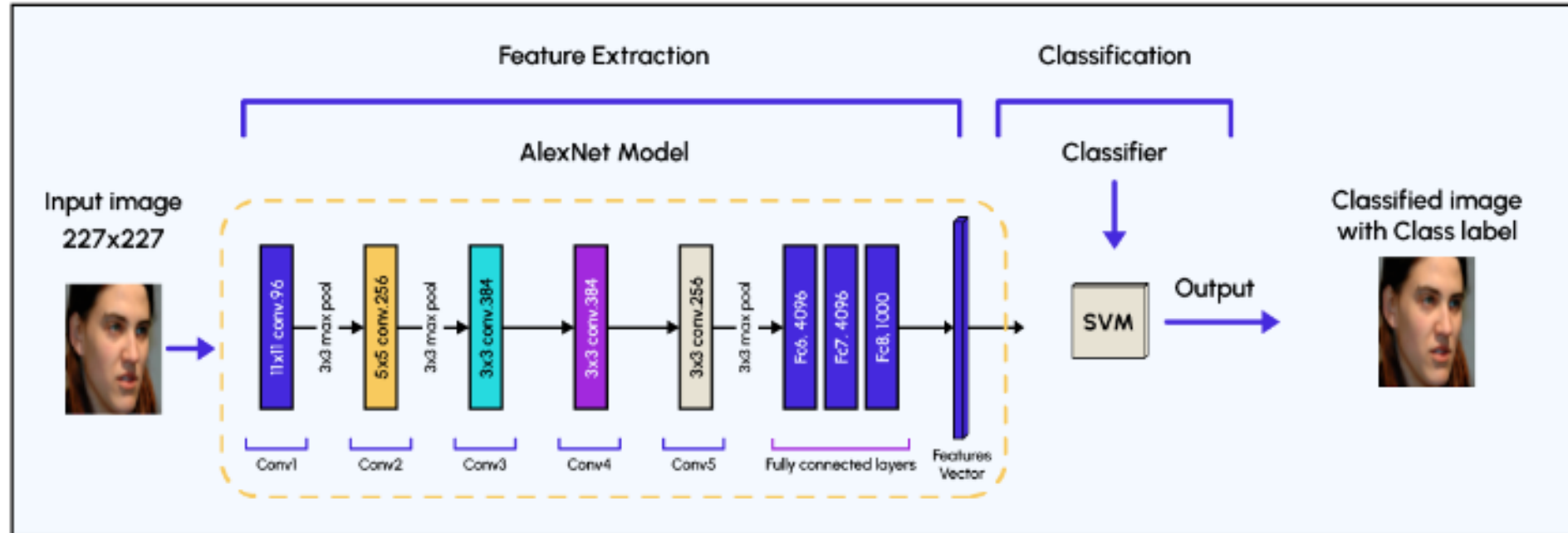
Biométrie

L'analyse biométrique de la reconnaissance faciale est si précise qu'elle peut faire la différence entre des vrais jumeaux.

D'autres signatures biométriques existent : empreintes digitales, scan de l'iris, voix, numérisation des veines de la paume ou analyse du comportement.

Elles permettent notamment de sécuriser les paiements dématérialisés .

Reconnaissance faciale



Dans un CNN pour la reconnaissance faciale, le réseau est formé sur un ensemble de données d'images de visages et d'images ne comportant pas de visages. Le CNN **apprend à identifier les caractéristiques importantes** d'un visage, telles que la forme des yeux, du nez et de la bouche, ainsi que la géométrie générale et la texture du visage. Ces caractéristiques sont ensuite utilisées pour identifier un visage dans une nouvelle image.

Protection des données biométriques

En Europe et au Royaume Uni, la Directive sur la protection des données (RGPD)

Applicable à partir du 25 mai 2018, la RGPD soutient le principe d'un cadre européen harmonisé qui défend en particulier le droit à l'oubli et exige un consentement clair et affirmé.

Cette directive a un impact international.

Elle concerne 500 millions de personnes.

Aux Etats-Unis, pas de loi fédérale unique sur la protection des données biométriques

Ce sont certains états voir des villes qui légifèrent .

Exemple :

L'état de Californie est avec New York, l'Illinois, le Texas et Washington, un des cinq états à protéger les données biométriques de façon formelle par une nouvelle loi de 2018 applicable au 1 janvier 2020.

Protection des données biométriques

En Inde, la cour suprême par un jugement du 27 août 2017 (jugement Puttaswamy) constitutionnalise le droit à la vie privée.

Il affirme le droit fondamental au respect de la vie privée des citoyens indiens.

En Chine, La reconnaissance faciale est le nouveau grand sujet techno en Chine, des banques aux aéroports mais aussi les forces de l'ordre.

Vaste réseau de vidéo-surveillance sur tout le territoire.

Plus de 200 millions de caméras de surveillance étaient utilisées à la fin de 2018 et 500 millions sont prévues d'ici à fin 2021.

Les tours de reconnaissance faciale, cibles de certains manifestants à Hong Kong sont emblématiques à cet égard.

Ce réseau est un des éléments du système de crédit ou notation sociale (社会信用体系) qui est mis en place dans le pays.

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

Reconnaissance faciale

En Russie*

Moscou. En 2017, réseau de **160 000 caméras** dans toute la ville, dont **3 000** sont connectées au système de reconnaissance faciale.

Six ans plus tard, cette technologie traque et permet d'arrêter à titre **préventif** tous ceux qui s'opposeraient, d'une manière ou d'une autre, aux décisions du Kremlin.

Nouvelle pratique pour dissuader toute personne de manifester :

À Moscou, tous les passagers sont **photographiés** lorsqu'ils franchissent les portes du métro, puis **facturés directement du prix du billet**.

Tous les visages des voyageurs sont analysés, et si le système signale un passager à arrêter, quelques secondes suffisent pour que la police intervienne.

*01Net de mars 2023 Stéphane Bascou avec source Reuters

Reconnaissance faciale

Principaux acteurs GAFAM, BATX et.... Thalès

Quelques performances

Système utilisé	Type de reconnaissance	Constitution de la base de données	Temps de reconnaissance moyen (sans échec)
Toshiba	3D	2 à 3 min	20 s
Android avec capteurs	2D	Inconnu	5s
Android 4.0	2D	2 s	< 1 s
Iphone 4S	2D	2 à 5 min	< 1s
Xbox One	Inconnu	5 s	1 à 5 s
PS4	3D	50 à 70 s	< 2 s
Iphone X, 11, 12, 13	3D	Inconnu	< 1 s

• Les porteurs d'un [iPhone X](#) sont eux déjà rompus à la technologie de la reconnaissance faciale. Même si la solution biométrique Face ID développée par Apple a fait l'objet de vives critiques en Chine fin 2017. On lui reproche son incapacité à différencier certains visages chinois.