drôle de frimousse

La reconnaissance faciale POUR LES NULS

On entend toutes sortes de choses sur la reconnaissance faciale. Tel logiciel étasunien identifie un visage à tous les coups, la Chine suit la trombine de ses citoyens à la trace, Big Brother est parmi nous, mais il suffit d'un maquillage géométrique pour le tromper... Vous êtes un peu perdu ? C'est normal. On va remettre les pendules à l'heure.

Pour une reconnaissance faciale réussie, il vous faut trois choses. D'abord, un visage. Bon. Mais vous n'irez pas bien loin. «La reconnaissance faciale, c'est reconnaître un visage qui a déjà été vu», explique Jean-Luc Dugelay, professeur à l'école d'ingénieurs EURECOM de Sophia Antipolis. Il faut donc une autre image avec laquelle le comparer, une image qui peut être stockée dans une base de données. Cette base de données, c'est le nerf de la guerre.

Ensuite, il faut un logiciel approprié. Il ne va pas comparer ces deux images directement, mais en extraire les éléments marquants (l'écartement des yeux par exemple) pour en faire un «résumé» mathématique, un gabarit, qui sera comparé à d'autres «résumés de visages» qui sont dans des bases.

Enfin, il faut décider d'un «niveau d'exigence» car ce n'est pas le logiciel qui va dire si c'est bien la même personne sur ces deux images. Il va juste donner un taux de correspondance, comme «ces visages sont similaires à 85%». Après, à l'utilisateur de décider où il met la barre. Ou il choisit un pourcentage un peu bas, sachant qu'il risque d'identifier par erreur des «innocents», mais qu'il ne ratera pas le «suspect» s'il tombe dessus. Ou il choisit un pourcentage élevé: pas de fausse identification, mais il risque de rater sa cible. Connaître le «niveau d'exigence» établi permet de savoir si on risque d'être identifié sans rien avoir à se reprocher.

Quand on connaît ces ingrédients, on peut se poser les bonnes questions: qui a le contrôle de la base de données? Est-elle cryptée? Est-ce que les visages archivés dans cette base de données sont stockés sous leur forme d'image ou de gabarit? Est-ce que des logiciels permettent de ravoir un visage à partir d'un gabarit? Où a été mis le curseur pour dire que «ces visages sont les mêmes»? Voici les points à vérifier si vous vous trouvez confronté à un type de reconnaissance faciale.

La reconnaissance faciale, pour quoi faire? Elle peut servir à vous authentifier ou à vous identifier. Dans le premier cas, vous déclinez votre identité et le logiciel vérifie si c'est vrai. Êtes-vous bien Jean Dupond, comme vous le prétendez? Il tentera d'y répondre par oui ou non. Si c'est non, votre vraie identité ne l'intéresse pas. C'est ce qui sert par exemple pour déverrouiller des iPhone ou pour gagner du temps au passage des frontières dans certains aéroports, comme Roissy-CDG, où le logiciel vérifie que vous êtes bien la même personne que celle figurant sur le passeport que vous présentez.

"À LA VOLÉE"

Dans le second cas, l'identification: on ne sait pas qui vous êtes, et le logiciel va essayer de mettre un nom sur votre tronche en la comparant aux visages de sa base de données. En France, l'identification peut être utilisée sur décision de justice dans le cadre d'enquêtes judiciaires et administratives. A posteriori, l'image des suspects pourra être comparée avec celles contenues dans le TAJ (Traitement d'antécédents judiciaires).

Mais le type de reconnaissance faciale qui inquiète aujourd'hui ses détracteurs, c'est l'identification de citoyens «à la volée», en direct dans la rue. «Elle n'est pas autorisée en France, précise Jean-Luc Dugelay, mais il y a des expérimentations.» Par exemple à Nice, à l'occasion du carnaval de février 2019, des volontaires se sont mêlés à la foule pour savoir si le système de reconnaissance faciale arrivait à les identifier. «La Cnil [Commission nationale de l'informatique et des libertés] a demandé un rapport... or il ne tient pas la route. On ne peut rien en déduire.»

Car il y a les résultats en labo... et ceux sur le terrain. «En labo, on a une efficacité quasi parfaite. Sur le terrain, avec des images de vidéosurveillance, ça peut vite se dégrader. Pour vous donner une idée, si vous n'avez pas le même âge, c'est dramatique. Ensuite, si vous avez une nouvelle barbe, du maquillage, des lunettes, si l'éclairage change, si l'expression faciale n'est pas la même, si la résolution de la caméra est mauvaise...»

Cette question de l'efficacité se pose par exemple pour la Chine, où l'identification par reconnaissance faciale est utilisée dans la rue pour relever les infractions. Ce pays dispose de la puissance informatique, des caméras et de bases de données pour le faire. La seule chose qui manque, ce sont... les performances de ses logiciels. «On n'a aucune statistique, on ne sait pas combien de personnes ils arrivent effectivement à identifier... Une sur cent, une sur cinq, on ne sait pas», s'inquiète notre professeur. Impossible de savoir si leur système arrive à reconnaître, mais le doute suffit à faire tenir tranquille la population.

Efficacité du logiciel, base de données... il y a une troisième chose sur laquelle il faut garder un œil: savoir comment le logiciel a été «entraîné». «Pour apprendre au réseau de neurones ce que c'est qu'un visage, il faut beaucoup de visages. Et là, ils vont les pomper sur Internet, sur vos photos Facebook, vos images», conclut Jean-Luc Dugelay. Illégal certes, mais difficile à contrôler. À l'heure où l'on partage nos frimousses à tout-va, voilà des raisons supplémentaires d'y réfléchir à deux fois.

CAMILLE VAN BELLE