SCIENCES ET AVENIR
33 RUE VIVIENNE
75002 PARIS - 01 44 76 92 31

OCT 14
Mensuel
OJD : 262622

Surface approx. (cm²) : 601

Visualiser l'article

Page 1/2

HIGH-TECH Bio-identification

Les nouvelles frontières de la reconnaissance faciale

Le logiciel DeepFace de Facebook serait en mesure de reconnaître un visage avec une fiabilité exceptionnelle de 97,95 %. Mais les parades restent très nombreuses.

« SURPUISSANT », « haute performance », « ultraperfectionné », « aussi fiable que le cerveau humain»... Une salve de commentaires dithyrambiques a accueilli la dernière annonce de la société Facebook: DeepFace, un algorithme de reconnaissance faciale d'abord présenté en mars dans un article scientifique publié en ligne, puis lors de la conférence IEEE de Columbus dans l'Ohio (Etats-Unis), en juin. Mis au point par une équipe « maison » de spécialistes en intelligence artificielle et un chercheur en informatique de l'université de Tel Aviv (Israël), ce programme serait capable de reconnaître un visage avec une fabilité de 97,35 %... Contre 97,53 % pour l'être humain. Du jamais vu!

Le programme est plus performant que la biométrie

Le réseau social de Mark Zuckerberg disposait déjà de PhotoTagger depuis juillet 2009. Cette option de reconnaissance incitait les membres à indiquer l'identité des personnes présentes sur les photos qu'ils mettaient en ligne, en fournissant automatiquement une liste de noms possibles après analyse de la base de données. Mais la performance n'était pas toujours au rendez -vous. Le logiciel se fondait en effet, comme beaucoup de programmes similaires, sur des comparaisons biométriques et le repérage de critères prédéfinis comme l'écartement des yeux, la distance yeux-nez, nez -bouche, etc. Dans le cadre d'un contrôle d'accès, certains y ajoutent la détection de vivacité (clignements d'yeux, micro-mouvements faciaux...) pour distinguer un vrai visage d'une photo. « Mais la biométrie reste très limitée, statique, et produit beaucoup de faux positifs », estime néanmoins Roger Cozien, docteur en informatique et fondateur de la société d'analyse d'images Exo Makina. DeepFace va beaucoup plus loin. L'algorithme, qui relève davantage de la vérification que de la reconnaissance (lire lexique p. 80), repose sur la topologie, une branche des mathématiques. Le programme choisit lui-même les éléments les plus saillants d'un visage, plutôt que d'utiliser des critères préprogrammés, et ne retient que ceux-ci, sous forme de points. Ces derniers sont reliés pour produire un modèle 3D utilisé pour retrouver un visage sur une photo ou une vidéo (voir Sciences et Avenir n° 809, p. 89). Ce n'est pas tout.

Simulant un réseau de neurones, la technologie DeepFace apprend à partir de ce qu'elle a déjà « vu » et se constitue une mémoire. C'est ce que l'on appelle le « deep learning », l'apprentissage profond. Cette approche n'est pas nouvelle mais elle a longtemps peiné à s'imposer car elle nécessite de la puissance de calcul et surtout de vastes bases de données pour que le programme puisse « s'entraîner ». Or, Facebook dispose de ce stock massif: l'équipe de recherche a, en effet, travaillé non seulement sur des stocks d'images disponibles en ligne (Labeled Faces in the Wild, de l'université du Massachusetts et YouTube Faces, de celle de Tel Aviv) mais elle a aussi exercé DeepFace avec 4,4 millions de photos de 4 030 internautes issus du plus de 1,2 milliard de profils du réseau social! Personne d'autre ne dispose d'un tel volume sous la main.

Le défi reste de reconnaître un visage maquillé

Alors, une révolution, DeepFace? Pas sûr. « Ce taux de réussite n'apporte rien, tempère Sébastien Marcel, responsable du groupe Biométrie à l'institut de recherche Idiap, à Martigny, en Suisse. DeepFace est simplement une technique de reconnaissance de visage de plus, décrite dans un article d'une conférence prestigieuse, mais dont il serait extrêmement difficile de reproduire les résultats. » Et, donc, de vérifier les performances. En raison du stock monumental de photos que cela exige, seul Facebook peut refaire ce que Facebook a fait... Sans compter quelques soucis de transparence. « L'article détaille une étape préalable de normalisation des images: les visages sont recalculés pour être orientés de face, ajoute Jean-Luc Dugelay, chercheur à l'école d'ingénieurs Eurecom à Sophia Antipolis. Pourquoi le réseau de neurones artificiel ne peut-il pas s'en passer, s'il est si performant? De même, Facebook ne dit pas ce qui se passerait si l'on n'alignait pas les visages de face. »

Quant au comportement de l'algorithme face à des visages maquillés ou modifié par chirurgie esthétique, mystère. En fait, l'effet d'annonce cache une réalité plus complexe.

« Pour un logiciel, reconnaître des formes ne pose pas de problème aujourd'hui. En revanche, il a encore beaucoup de mal à interpréter ce qu'il «voit» », rappelle Roger Cozien. Là où le cerveau humain sait reconnaître une personne malgré une mèche lui barrant le visage, des lunettes de soleil, une mauvaise lumière ou du maquillage, un programme est facilement dépassé. C'est tout l'enjeu de la recherche que de traiter ces « variabilités ». Sébastien Marcel coordonnait ainsi jusqu'en avril dernier le projet européen Tabula Rasa d'étude de vulnérabilité des systèmes de contrôle biométrique et de recherche de contre-mesures aux attaques (le spoofing).

Ce consortium d'entreprises et de centres de recherche a, par exemple, pu leurrer des logiciels avec des masques achetés en ligne. « Nous avons alors construit des bases de données pour entraîner le système à repérer ces subterfuges et le rendre capable de séparer les caractéristiques de vrais visages de celles des faux en

DD7A958B5600C30762D646C4720C45532DB5466B31BE45F3726403A

mesurant la texture de la peau et la carte de disparité des images [des données de profondeur] », détaille Sébastien Marcel.

Actuellement chercheuse à l'Inria Méditerranée, Antitza Dantcheva a remporté en juin 2013 un concours de spoofing organisé par Tabula Rasa. Elle a trompé le logiciel de la société KeyLemon en se faisant passer pour un homme en usant de simples produits cosmétiques. Depuis, elle travaille aux contre-mesures. Utilisant une base de données de 600 photos de 151 visages féminins avant et après maquillage, la chercheuse a entraîné son algorithme à repérer les effets de la cosmétique: changement de lumière, configuration des traits, expression, couleur, etc. Avec un taux de détection de 93,5 %, les premiers résultats sont encourageants. « Nos travaux sont toujours en cours, relativise Antitza Dantcheva, et nous étudions désormais quels paramètres retenir pour qu'un algorithme reconnaisse un visage avec et sans maquillage. »

En septembre 2013, Amy Webb, une spécialiste américaine en stratégie numérique, publiait sur Slate.com une chronique en forme d'avertissement: bientôt, des technologies de « bio-identification » sauront reconnaître, sur Facebook ou ailleurs, un adulte à partir d'une photo prise lorsqu'il était enfant. La technique en est à ses balbutiements mais à l'université du Kent (Royaume-Uni), Stuart Gibson a déjà conçu un programme qui vieillit des visages d'enfants en modélisant l'évolution de divers critères (structure osseuse, texture de peau...). A l'université de Chicago, un biodémographe américain travaille sur le même sujet (lire l'encadré ci-contre).

Les caméras vidéo restent souvent trop médiocres

Si tant de perspectives s'ouvrent, c'est aussi qu'au-delà des algorithmes, la recherche profite de la diffusion de plus en plus large de capteurs de qualité: webcam, appareils photo numériques, smartphones à cellules optiques, etc. Récemment, Intel ou SoftKinetic ont aussi lancé des caméras capables de percevoir la profondeur. Mais il reste du chemin à parcourir. « La plupart des caméras de vidéosurveillance ont une résolution médiocre, ce qui pose problème pour ne serait-ce que détecter un visage! », prévient Naoufal El Ouali, président de la société Axone spécialisée dans les technologies de sécurité. A l'automne 2013, les images de vidéosurveillance du « tireur fou » Abdelhakim Dekhar n'avaient ainsi pas pu être analysées par les logiciels de la police française.

Mais la surveillance ou la lutte contre le crime ne sont pas les seules vocations de la reconnaissance faciale. Si Facebook affirme ne pas savoir ce qu'il fera de DeepFace, on imagine qu'il pourra améliorer, encore et toujours, le ciblage publicitaire. Embarquées en application sur des appareils mobiles, ces technologies peuvent aussi servir d'aide médicale pour établir un diagnostic d'urgence, d'outils d'assistance aux personnes identifiées comme âgées ou handicapées pour leur indiquer des itinéraires adaptés de repérage dans une foule de gens avec qui on a rendez-vous, etc. « Il existe autant d'usages de la reconnaissance faciale qu'il en existe pour nos yeux », souligne Roger Cozien. Autant dire que ces technologies n'en sont qu'à leurs débuts.

POUR EN SAVOIR PLUS

Le projet Tabula Rasa: www.tabularasa-euproject.org

Le site Face My Age: www.facemyage.com

CV Dazzle: http://cvdazzle.com

L'article de recherche de Facebook sur DeepFace: www.facebook.com/publications/546316888800776

DETECTION

Repérage de la présence d'une forme spécifique, comme celle d'un visage humain, caractérisée par certains critères (biométrie, lumière, textures, contrastes).

VERIFICATION

Capacité d'un programme à signaler que deux visages appartiennent à la même personne.

RECONNAISSANCE

Capacité d'une machine à identifier une personne à partir de son visage.

Devillard Arnaud