EN DEUX MOTS Les techniques de reconnaissance des personnes par leurs caractéristiques physiques font l'objet d'un intérêt croissant de la part de nombreux États, notamment depuis que les attentats du 11 septembre 2001 ont révélé des failles dans la sécurité aérienne. La comparaison des empreintes digitales, technique centenaire, est toujours bien placée, mais d'autres systèmes sont à l'étude. Ainsi, pour améliorer la fiabilité de la reconnaissance du visage, des chercheurs travaillent sur l'analyse des mimiques faciales, et la vision en trois dimensions.

La biométrie en mouvement

Comment être sûr que vous êtes bien celui que vous prétendez être ? Qu'une foule ne dissimule pas un individu dangereux ? De nouvelles techniques biométriques, fondées sur la reconnaissance des visages, permettront bientôt de répondre à de telles questions.

Jean-Luc Dugelay
est professeur à Eurécom, Sophia-Antipolis.
jld@eurecom.fr

Dix-huit novembre 2005. Une vingtaine de lycéens font irruption dans la cantine du lycée de Gif-sur-Yvette, dans l'Essonne. Grimés en clowns, ils détruisent deux bornes d'accès à la cantine fondées sur la reconnaissance de l'empreinte de la main des élèves. Ce fait-divers, dans lequel trois lycéens ont été poursuivis et condamnés chacun à trois mois de prison avec sursis, est symptomatique de la montée en puissance des installations biométriques pour des applications de plus en plus variées, et des réticences que ces installations engendrent.

Ces réticences sont compréhensibles : la biométrie a été inventée dans le but de ficher les criminels ou supposés tels. C'est en 1880 qu'Alphonse Bertillon, embauché peu de temps auparavant à la police criminelle de Paris, proposa un système permettant d'identifier les personnes par le biais d'un ensemble de mesures opérées sur le corps (longueur des bras, de l'oreille…) et de caractéristiques physiques (couleur des yeux, cicatrices…). Ces informations étaient ensuite quantifiées, afin de définir des catégories, puis enregistrées sur une carte. On pouvait ainsi vérifier si une personne arrêtée était déjà fichée, en comparant ses données avec chacune des cartes stockées. Ce système fut adopté en France en 1882, puis en 1887 aux États-Unis, avant de se généraliser en 1900.

Mais, dès 1903, on découvrit que deux prisonniers avaient les mêmes caractéristiques anthropométriques, et donc des cartes identiques selon la méthode Bertillon. Cette même année, les prisons et l'État de New York commencèrent d'ailleurs à utiliser systématiquement les empreintes digitales : leur acquisition est plus aisée que celles des nombreuses mesures anthropométriques, et la probabilité que deux individus possèdent les mêmes est quasi nulle.

> La montée en puissance des installations biométriques engendre des réticences

Les empreintes digitales figurent toujours en bonne place parmi les techniques biométriques. Elles sont systématiquement relevées lors d'une demande de passeport, par exemple. Et elles seront parmi les premières informations à figurer, avec la photographie, dans la mémoire électronique qui équipera les futurs passeports selon les réglementations promulguées aux États-Unis après les attentats du 11 septembre 2001.

EN 1985 ***NATIONAL GEOGRAPHIC*** **publiait la photo d'une jeune Afghane aux yeux verts. Dix-huit ans plus tard, le photographe retrouva Sharbat Gula et la photographia de nouveau pour la revue américaine. Des techniques biométriques de reconnaissance de l'iris et de caractéristiques faciales furent employées pour s'assurer qu'il s'agissait bien de la même personne. L'identification fut positive.**
© PHOTOS STEVE MC CURRY/MAGNUM

La reconnaissance de ces empreintes reste le meilleur compromis entre fiabilité et simplicité. Bien que centenaire, elle connaît encore des améliorations. L'acquisition ne se fait plus en encrant son doigt et en l'appuyant sur une feuille, mais à l'aide de scanners thermiques, optiques ou à ultrasons. On commence à trouver des ordinateurs, des clés USB, et même des téléphones dont l'utilisation est sécurisée par la reconnaissance d'une empreinte digitale [1].

Toutefois, cette technique ne répond pas à tous les besoins. Depuis 2001, la demande de sécurité a fortement augmenté de la part des aéroports et des polices des frontières. La surveillance des lieux publics, rues ou stades se développe aussi fortement dans les pays occidentaux. Dans les laboratoires universitaires et industriels, les recherches se multiplient pour trouver d'autres méthodes de reconnaissance efficaces.

Les caractéristiques du corps humain sur lesquelles se fonde une technique de biométrie doivent répondre à plusieurs critères : être observables chez toute personne, mesurables, uniques, permanentes, difficilement falsifiables, et permettre de différencier deux personnes. Il n'existe pas de technique biométrique universelle : chacune est plus ou moins bien adaptée au type d'application visée. Il est matériellement impossible, par exemple, de prendre les empreintes digitales de tous les spectateurs d'un grand match de football.

Un autre aspect est la fiabilité de la technique. Dans l'idéal, on souhaite minimiser en même temps les taux de « fausses acceptations » et de « faux rejets ». En pratique, on doit faire des compromis. Dans les applications en sécurité, par exemple le contrôle dans les aéroports, une seule « fausse acceptation » peut avoir des conséquences très graves : on préfère alors risquer de refuser quelques passagers n'ayant rien à se reprocher (mais pas trop quand même). Pour d'autres applications, comme la personnalisation d'un ordinateur ou d'un téléphone, une fausse acceptation est *a priori* moins risquée, et moins gênante, qu'un faux rejet qui empêcherait l'utilisateur d'accéder à ses données. Comme aucune des techniques ne remplit parfaitement tous les critères souhaités, la tendance est à l'utilisation en parallèle de plusieurs d'entre elles.

Représentations sociales

Une dernière caractéristique à prendre en compte dans la mise au point et dans la mise en place d'une technique de biométrie est son acceptabilité : les personnes que l'on souhaite contrôler doivent s'y soumettre sans réticence. Cela dépend beaucoup des représentations sociales associées à chaque technique. Ainsi, la prise d'empreintes digitales garde une connotation criminelle peu compatible avec un usage banalisé, alors que la cartographie de l'iris de l'œil est mieux acceptée. Autre exemple, dans un aéroport aux États-Unis, les passagers étaient réticents à utiliser un système fondé sur le contour de la main, car ils ne souhaitaient pas, pour des raisons d'hygiène, poser leur main sur la vitre du système d'acquisition après de nombreuses autres personnes.

On peut classer les techniques de biométrie en trois catégories. Les plus classiques étudient les caractéristiques physiques, comme le visage, les empreintes digitales, l'iris et les veines de la main. Plus récemment, on s'est intéressé aux caractéristiques biologiques, telles que l'ADN. Enfin, les plus récentes, et les plus prometteuses, s'intéressent aux caractéristiques comportementales ou dynamiques : la voix, la démarche, le geste d'écriture. Par exemple, il est difficile, mais pas impossible, d'imiter la signature d'une personne. En revanche, il est impossible d'imiter la dynami- ⇨

[1] Gabriel Martin, « L'identification au bout du doigt », *La Recherche*, juillet-août 2005, p. 94.

⇨ que de l'écriture : notre façon d'accélérer le trait, de revenir en arrière, de mettre les points et les barres, d'appuyer plus ou moins fort selon les endroits est unique. L'alliance de la biométrie des caractéristiques physiques et de la biométrie comportementale semble une piste particulièrement intéressante.

Reconnaissance des visages

Au sein d'Eurécom, institut de recherche en systèmes de communication basé à Sophia-Antipolis, nous nous sommes intéressés à ces aspects dynamiques, appliqués à la reconnaissance des visages. Cette dernière offre en effet un potentiel plus important que la plupart des autres techniques biométriques, notamment pour la reconnaissance de grands nombres de personnes, ou encore pour la recherche et l'identification d'individus dans une foule. En effet, le visage est rapidement accessible (ce qui n'est pas le cas de l'iris), sans contact (ce qui n'est pas le cas des empreintes digitales). Son observation est bien acceptée par les utilisateurs, et elle offre un potentiel énorme dans les années à venir si on réussit à la faire fonctionner avec les systèmes de vidéosurveillance existant dans les stades, les aéroports, les rues, etc. Elle ne requiert pas une collaboration de l'utilisateur, contrairement aux empreintes digitales, qui nécessitent de poser le doigt sur une surface. Elle ne demande pas non plus de faire stopper, ni même de ralentir les personnes.

L'observation des mimiques faciales rend plus performant le système de reconnaissance

Malheureusement, c'est une technique encore peu fiable. Pour qu'elle fonctionne correctement, il faut que les conditions d'observation restent identiques dans les étapes d'apprentissage, d'enregistrement et d'authentification. Or, les sources de changements sont multiples : les conditions d'éclairage, de pose, d'expressions faciales, d'apparence, comme la présence de lunettes ou non, de maquillage, etc. Le défi consiste à faire la différence entre les variabilités dites « intraclasse » (une même personne) avec celles dites « interclasse » (deux personnes). En pratique, pour une machine, deux personnes différentes mais dans des conditions identiques sont parfois plus ressemblantes qu'une même personne prise dans des conditions radicalement différentes. À tout cela peuvent s'ajouter des variations au cours du temps liées au vieillissement.

La quasi-totalité des systèmes de reconnaissance de visages travaillent à partir d'images fixes en deux dimensions. Pour améliorer cette technique, la piste que nous privilégions est l'addition de dimensions supplémentaires : le temps, à l'aide d'enregistrements vidéo, ou l'espace, à l'aide de plusieurs caméras ou scanners, qui permettent l'ajout de relief. L'objectif est de conserver les avantages de la reconnaissance faciale tout en approchant des scores de fiabilité obtenus avec les empreintes digitales.

En vidéo, nous étudions actuellement la récupération des informations pour reconnaître les personnes en observant leurs mimiques faciales : leurs manières de bouger la tête ou les lèvres, de cligner des yeux, ou encore de sourire. On passe ainsi d'une biométrie physique (l'apparence du visage) à une biométrie comportementale. À plus long terme, le but sera de combiner les paramètres dynamiques associés au visage avec les paramètres plus classiques d'apparence pour former un système « multimodal » performant.

En pratique, le système suit d'une image à la suivante la position de quelques points et zones caractéristiques du visage, tels les yeux, le nez ou la bouche. Ensuite, image par image, plusieurs paramètres locaux sont extraits comme la largeur et l'ouverture de la bouche, la position de la rétine d'œil, l'ouverture des yeux, etc. Lors de l'apprentissage, on collecte de nombreuses fois ces données en étudiant quelques secondes de plusieurs vidéos de chaque personne à apprendre. À partir de toutes ces observations, on construit un modèle statistique de la personne. Ainsi, on a caractérisé pour chaque individu la probabilité qu'il a d'exécuter tel ou tel mouvement ou action faciale, de cligner plus ou moins des yeux, etc. Pour que ce système puisse fonctionner, il est nécessaire d'avoir accès à de nombreuses données sur les personnes. Nous nous intéressons aussi aux dissymétries dans le visage, comme le froncement différent du sourcil droit et du sourcil gauche.

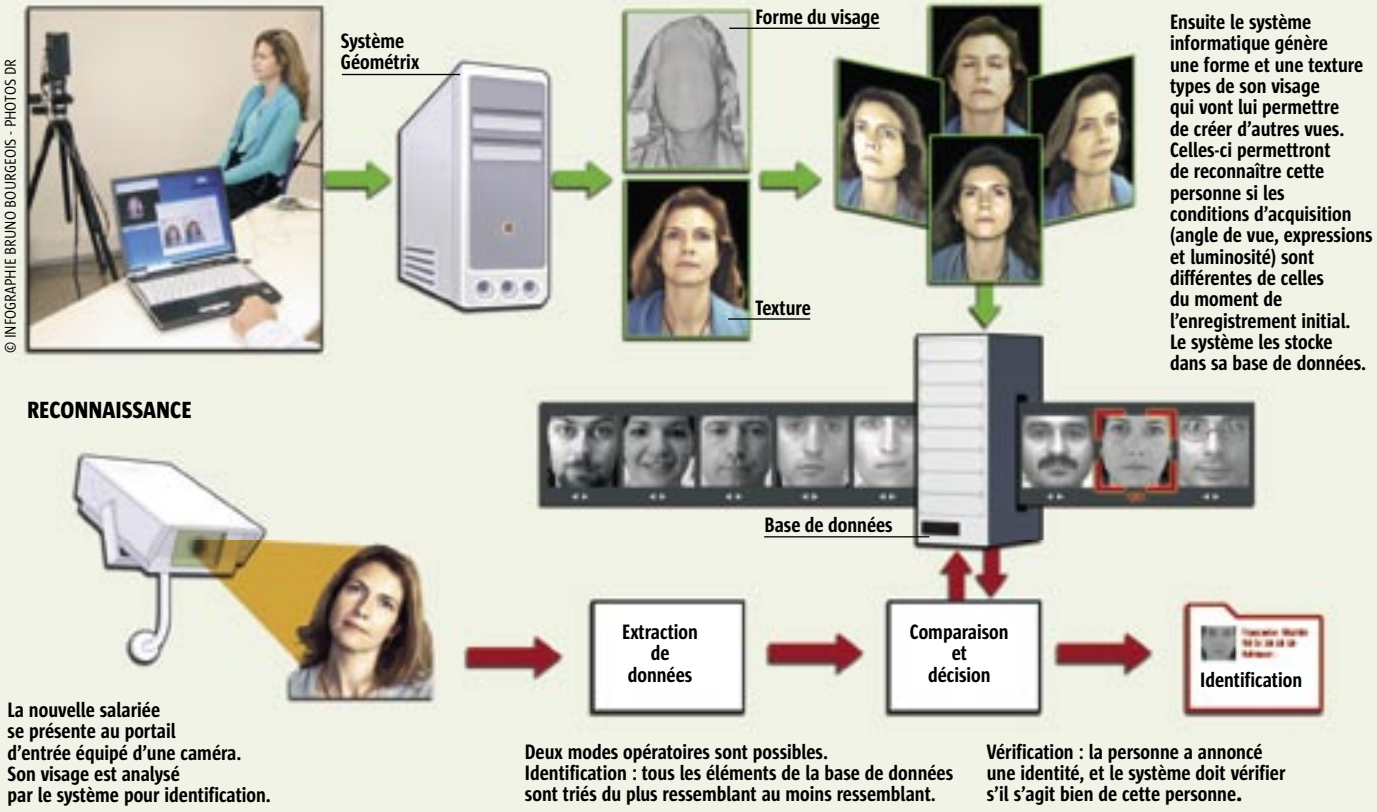
Images en trois dimensions

Reste à prouver que ces caractéristiques sont assez différentes d'une personne à une autre : ce n'est qu'à cette condition que nous pourrons les utiliser pour identifier des individus sans erreurs. Heureusement, il ne s'agit que d'affiner la reconnaissance du visage par la vidéo, et non de réaliser une biométrie uniquement fondée sur les mouvements.

L'autre piste sur laquelle nous travaillons est l'utilisation d'images en trois dimensions. Des caméras tridimensionnelles sont utilisées pour l'acquisition des données de départ, la phase d'enrôlement (lire ci-contre « Identification ou vérification ? »). Des caméras à deux dimensions, moins coûteuses, continueraient à être utilisées pour la reconnaissance. Pour bâtir une image à trois dimensions, on prend deux photos classiques à l'aide de deux caméras légèrement décalées (on parle de système stéréoscopique) un peu comme en vision humaine avec notre œil gauche et notre œil droit. Puis, sachant que la différence de position d'un point du visage dans les deux images est inversement

APPLICATIONS Identification ou vérification ?

ACQUISITION 3D. Si l'on prend l'exemple d'une nouvelle salariée dans une entreprise, son visage est d'abord photographié de face par un système de capture numérique.



© INFOGRAPHIE BRUNO BOURGEOIS - PHOTOS DR

QUELLE QUE SOIT LA TECHNIQUE DE BIOMÉTRIE, deux étapes sont incontournables : l'enrôlement (ou acquisition) et la reconnaissance. La première consiste à enregistrer les personnes dans une base de données. Seules quelques caractéristiques de la biométrie sont extraites de l'acquisition puis mémorisées. Pour reconnaître la personne, il faut alors remesurer ses caractéristiques biométriques et les comparer avec les données contenues dans la base. Cette comparaison est différente selon le but : l'identification consiste à classer une personne par rapport à une liste de personnes préenregistrées dans une base de données (contrôler par exemple qu'une personne n'est pas recensée comme terroriste). En mode vérification, on s'assure que l'identité annoncée par la personne est bien exacte et qu'il ne s'agit pas d'un imposteur.

proportionnelle à la distance qui sépare ce point du visage des caméras, il est possible de reconstruire point à point la forme en relief du visage.

L'imagerie à trois dimensions est moins sensible aux variations d'éclairage, à la modification d'apparence, volontaire ou involontaire, ou au fait que la personne ne fait pas face à la caméra. En effet, si quelqu'un se présente de biais, un logiciel fait « tourner » le modèle tridimensionnel pour le faire correspondre à l'image bidimensionnelle prise en conditions réelles. De même, ce logiciel modifie les conditions lumineuses de l'image tridimensionnelle pour les rendre plus proches de l'éclairage existant. La comparaison entre les données stockées et les images prises en temps réel est donc plus facile.

D'autres limitations de la reconnaissance faciale sont plus problématiques. C'est le cas de la variation du visage au cours du temps. Les outrages pleurés par les poètes contrarient aussi les systèmes de reconnaissance. Après un an, le taux d'erreurs augmente de 10 % ! Cette technique impose donc une remise à jour fréquente des données. Possible lorsque l'on s'attache à reconnaître les employés d'une entreprise, cette actualisation est une tout autre affaire lorsqu'il s'agit de repérer un terroriste disparu depuis cinq ans.

Ces travaux n'en sont encore qu'aux prémices. Nous devons prouver que les mouvements du visage ou les images tridimensionnelles sont discriminants, c'est-à-dire qu'on peut distinguer deux personnes avec une précision suffisante. Si nous arrivons à montrer que ces technologies améliorent la reconnaissance faciale, nous devrons ensuite étudier si elles sont utilisables en conditions réelles. Nous n'avons pas encore pu vérifier le taux de reconnaissance de ces techniques, car nous ne disposons pas des bases de données nécessaires, qui contiendraient les visages de milliers de personnes, pris à plusieurs reprises. Mais les besoins en biométrie sont tels que ces technologies seront prochainement testées à grande échelle. ■■ **J.-L. D.**

POUR EN SAVOIR PLUS

■ **www.eurecom.fr/~dugelay**
■ **http://biobimo.eurecom.fr**
Le site du projet national RNRT Biobimo.