SÉCURITÉ DES ACCÈS

La biométrie au Japon

La biométrie permet d'identifier des personnes à partir de données biologiques propres et de contrôler l'accès à l'entrée des bâtiments, des aéroports ou sur l'internet. Ce secteur répond ainsi aux besoins croissants en matière de sécurité. Les entreprises japonaises sont bien positionnées sur ce marché et proposent des appareils utilisant les paramètres biométriques les plus courants. Cependant, la recherche fondamentale reste peu développée, les entreprises préférant utiliser des technologies américaines sous licence. Par ailleurs, la population japonaise est assez réfractaire à l'identification biométrique et les autorités ont conduit des projets à grande échelle pour familiariser le public et tester la mise en œuvre des dispositifs.

La biométrie regroupe l'ensemble des techniques qui permettent une identification des individus à partir de caractéristiques biologiques propres : empreintes digitales, forme du visage, de l'iris ou de la main, etc. Ses applications couvrent l'authentification pour le contrôle d'accès aux bâtiments, aux réseaux informatiques, aux ordinateurs et autres appareils privés, ainsi que l'identification, notamment sur l'internet. Ces méthodes rendent obsolètes les mots de passe, codes, clés ou autres cartes à puce et renforcent la sécurité en identifiant directement les personnes.

Caractéristique majeure : la précision

Les systèmes de sécurité traditionnels sont fondés sur la reconnaissance visuelle des individus, la possession d'une clé ou d'une carte à puce, ou encore la connaissance d'un code ou d'un mot de passe. Toutes ces méthodes présentent des inconvénients, tels que le coût de l'immobilisation d'un gardien ou le risque de perte ou d'oubli. Les systèmes automatisés biométriques évitent ces écueils tout en autorisant la reconnaissance des personnes avec grande précision.

Plusieurs facteurs sont critiques pour le fonctionnement d'un système biométrique : la précision, la vitesse d'acquisition, l'acceptabilité par les usagers, l'unicité de l'organe biométrique, la résistance aux contrefaçons, la fiabilité et la nécessité de stockage des données. La précision est la caractéristique la plus importante : le système d'identification doit différencier une personne autorisée d'un imposteur. À ce titre, on distingue deux critères caractérisant un tel système : le taux d'acceptation par erreur FAR (false accept rate) et le taux de rejet par erreur FRR (false reject rate). Le CER (crossover error rate) est le seuil de sensibilité pour lequel le FAR et le FRR sont égaux. Il correspond en général au point de fonctionnement optimal de l'appareil. On peut régler la sensibilité de tous les systèmes

d'identification biométrique. Avec un seuil élevé, le système n'accepte que des données quasi identiques à celles qu'il a en mémoire et aucun indésirable n'est autorisé (FAR faible). En revanche, des personnes autorisées ne seront pas admises, par exemple à cause de doigts sales, de mouvements pendant l'acquisition, d'une voix cassée ou de verres de contact (FRR élevé). À l'inverse, avec une sensibilité plus faible, le FRR sera minime mais le FAR plus important.

La vitesse d'acquisition indique la rapidité avec laquelle la décision d'acceptation ou de rejet est annoncée. Une vitesse de 6 à 10 secondes par personne est en général admise.

Un système biométrique est d'autant mieux accepté que les utilisateurs sont persuadés qu'il y a quelque chose à protéger. En outre, il doit être inoffensif et ne pas ralentir les déplacements des individus ni entraîner des délais de production. Il ne doit pas non plus permettre à une administration ou une direction de collecter des informations personnelles ou sanitaires. Le niveau de développement technologique est surtout avancé en ce qui concerne les équipements destinés à l'utilisateur. Par contre, l'intégration de ces équipements dans des systèmes fiables et complets reste à réaliser. Ainsi, la continuité de la sécurisation tout au long de la chaîne pose encore des problèmes, notamment liés à la protection des données stockées en mémoire ou lors de la transmission de celles-ci.

Des paramètres multiples

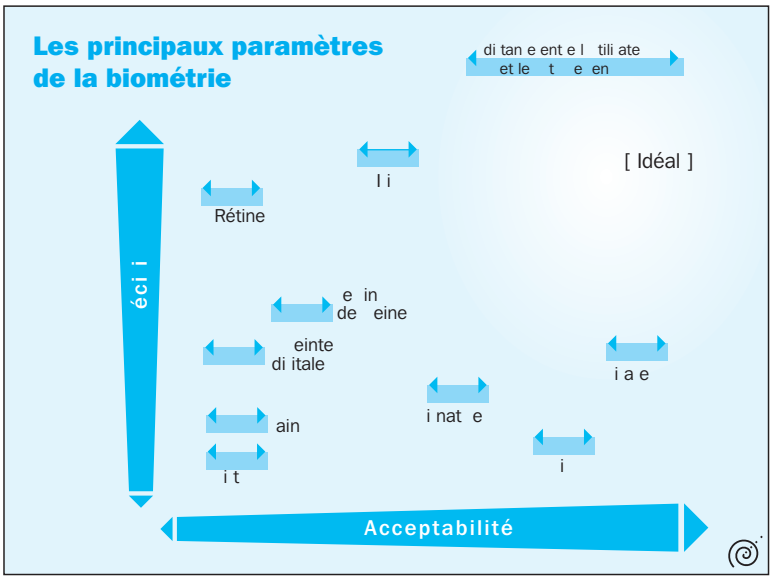
Les systèmes de reconnaissance biométrique développés jusqu'à présent portent principalement, par part de marché croissante, sur le réseau veineux, la voix, la rétine, l'iris, la main, le visage et les empreintes digitales. Ces paramètres se positionnent différemment selon leur précision et leur acceptabilité (voir encadré).

L'utilisation du réseau veineux est une technique prometteuse, qui sonde par infrarouge le dessin produit par les veines d'un doigt ou de la main. Sa mise en œuvre reste très coûteuse et les premiers produits sortent seulement sur le marché japonais. Son principal avantage est de réaliser une empreinte sans qu'aucun contact ne soit nécessaire, ne laissant aucune trace et défiant toute imposture.

La voix permet une reconnaissance à distance et cette technique est bien acceptée. Son premier défaut est la possibilité d'utiliser un enregistrement. La reconnaissance vocale nécessite par ailleurs une excellente qualité audio et l'installation d'un tel dispositif dans un lieu bruyant est difficile. Globalement, la technique est assez peu fiable. L'utilisation de l'image rétinienne l'est beaucoup plus. Très précise, cette technique s'avère toutefois contraignante, puisqu'il faut balayer la rétine avec une lumière infrarouge intense. Ce procédé invasif est également difficile à mettre en œuvre.

L'identification par l'iris est la mesure qui obtient la meilleure précision, les taux d'erreur étant de l'ordre de 10^{-4}. L'iris est en effet unique et très complexe, puisqu'on peut y distinguer près de 250 points de comparaison. Les systèmes les plus performants contrôlent le changement de taille de l'iris avec l'intensité de la lumière et ne peuvent être leurrés par une image ou une lentille reproduisant le dessin de l'iris d'une personne. Coûteuse, cette technique couvre seulement 6 % du marché de la biométrie. Obligeant à prendre une photo à haute définition de l'œil, elle rebute le public.

L'identification biométrique de la main revêt deux formes : l'empreinte palmaire, analogue à l'empreinte digitale, et l'image tridimension-



MEMS
micro-electro-mechanical systems, microsystèmes

nelle de la main. Ces deux technologies couvrent 10 % du marché. La reconnaissance par le visage a de plus en plus d'adeptes, avec 15 % de parts de marché. Pour construire une carte du faciès, cette approche s'appuie sur des caractéristiques telles que l'éloignement des yeux ou la taille de la bouche. Seule une opération chirurgicale modifiant les cartilages peut déjouer cette technique, le port d'une barbe ou la modification de la coiffure étant sans effet.

La technique utilisant les empreintes digitales est la plus ancienne et la plus répandue, avec 50 % de parts de marché. Un capteur numérise une image du doigt et un logiciel repère les coordonnées des points de fin de crêtes et de bifurcations avec un haut degré de précision. L'image ainsi acquise est comparée à l'empreinte digitale gardée en mémoire. Les systèmes haut de gamme font la différence entre un authentique doigt et un moulage de celui-ci. L'acquisition de l'empreinte peut se faire directement dans sa totalité, mais il est préférable de la scanner et de la reconstituer informatiquement : ceci évite les images résiduelles et limite les coûts, la surface active étant plus petite. Différentes méthodes sont utilisées pour l'acquisition des empreintes (optique, capacitive, ondes radio, piézoélectrique, MEMS*, thermique).

Engagement des pouvoirs publics et des entreprises

La division des passeports du ministère des Affaires étrangères, le ministère des Transports ainsi que la Police Nationale s'impliquent activement dans ce secteur. Le ministre de l'Intérieur annonçait début février que le passeport japonais pourrait contenir des données sur l'iris, les empreintes digitales, la forme de la main, du squelette et sur les caractéristiques de la voix. Le ministère des Transports a mené début 2003, en collaboration avec la compagnie aérienne JAL, une expérience utilisant la biométrie à l'aéroport de Narita. Des passagers réguliers des lignes aériennes enregistraient deux données biométriques (visage et iris) sur une carte à puce au moment de l'enregistrement. Avant d'embarquer, les données de la puce étaient lues et un appareil de reconnaissance identifiait les personnes. La police japonaise utilise déjà des appareils numériques pour la reconnaissance des empreintes digitales, dans deux applications principales : l'accès aux bâtiments et la prise d'empreintes d'individus suspects en vue de les comparer rapidement avec les fichiers centraux. L'agence de police nationale étudie également la reconnaissance par le visage, dans le but de constituer un fichier japonais des visages, au même titre qu'il existe un fichier des empreintes digitales.

Si le niveau de développement technologique est bien avancé, l'Archipel montre un déficit de recherche fondamentale en biométrie, la plupart des acteurs basant leurs produits sur des technologies brevetées

aux États-Unis. Une dizaine d'entreprises travaillent dans le domaine de la biométrie. NEC est l'entreprise japonaise qui travaille dans ce secteur depuis le plus longtemps, ses travaux sur la recherche d'un algorithme de reconnaissance des empreintes digitales ayant commencé en 1971. Aujourd'hui, NEC développe aussi des systèmes de reconnaissance de l'iris, de la voix, du visage et de la main. Hitachi joue un grand rôle, notamment par son travail de normalisation. L'entreprise propose à ses clients de développer des appareils utilisant différents caractères biométriques, mais les empreintes digitales restent sa spécialité. Le créneau de Sony est la reconnaissance d'empreintes digitales et l'entreprise propose quatre produits. Omron porte ses efforts sur l'identification par la forme du visage. Elle utilise pour cela la technologie de l'Université de Californie du Sud et a obtenu en 1997 les licences nécessaires. Oki Electric fonde ses recherches depuis 1995 sur la reconnaissance de l'iris par infrarouge. Oki détient les licences de l'entreprise américaine Iridian Technologie, qui lui ont permis de développer deux produits.

Chez Fujitsu, la recherche se concentre sur la reconnaissance des empreintes digitales avec deux produits proposés à cet effet. Un système d'identification par le réseau des veines situées sous la peau de la main a également été développé et sera commercialisé fin 2003. Les recherches chez Secom portent principalement sur l'identification par les empreintes digitales et par la voix. Toshiba, le premier fournisseur d'ordinateurs portables, a passé des accords avec la firme Identix pour fournir à ses clients une solution d'accès biométrique. NTT, le géant de la communication, a développé son propre système de lecture d'empreintes digitales et le commercialisera en décembre 2003, via sa filiale NTT Data Corporation. Matsushita-Panasonic se focalise sur la reconnaissance par l'iris, avec deux produits complémentaires, l'un destiné au contrôle d'accès aux portes et l'autre à l'identification des individus pour la connexion à un ordinateur. Enfin, SecuGen, entreprise américaine implantée depuis 2000 et numéro un de la reconnaissance par empreintes digitales au Japon, détient plus de 20 % de part de marché et propose deux gammes de produits. L'entreprise associe des détecteurs optiques à un algorithme puissant développé en interne.

Vers une standardisation de la biométrie

Au Japon, la volonté est forte d'harmoniser les méthodes d'évaluation de la précision des appareils biométriques. Un comité de standardisation existe, regroupant des acteurs publics et privés. Une association a également vu le jour en 2001, la Japan Biometric Authentication Association (JBAA). Regroupant des membres venant des grandes entreprises japonaises du domaine, son but est de promouvoir les systèmes biométriques tout en palliant les problèmes qu'ils posent. L'association a ainsi organisé avec la mairie de Kyoto une expérience utilisant la biométrie pour les services aux personnes âgées. Cinquante personnes ont bénéficié de services municipaux sans sortir de chez elles, en se connectant directement au serveur et s'identifiant grâce à une reconnaissance faciale et des empreintes digitales. Pour l'avenir, le souhait de la JBAA est une large utilisation de la biométrie, basée sur une identification multiparamètre et naturelle, à l'image de la rencontre entre individus.

Pierre Leroy

Cet article a été rédigé à partir du rapport "La biométrie au Japon ", réalisé par Arnaud Vigier, du Service pour la Science et la Technologie de l'Ambassade de France au Japon, que nous remercions pour sa collaboration.

Pour en savoir plus... :

Centres de compétences :

- *Japan Biometric Authentication Association (JBAA), www.biometrics.gr.jp/JBAA/index-en.html*
- *Biometric Consortium, www.biometrics.org*
- *Portail Biometrie Online, http://biometrie.online.fr*

À lire également :

SécuritéInfo.com, www.securiteinfo.com/conseils/biometrie.shtml

Le rapport est disponible à l'ADIT. Pour le recevoir, il suffit de compléter la page 48 de ce numéro et de nous l'envoyer par courrier ou par fax. Il est aussi possible de le télécharger gratuitement au format PDF à partir de notre site www.adit.fr (" rapports d'ambassades ").