L'identification biométrique dans le commerce électronique

Les techniques d'identification biométriques, jusqu'à récemment l'apanage des militaires ou des policiers, se retrouvent désormais dans de nombreuses applications commerciales ou bancaires. En effet, ces techniques fournissent des moyens d'identification et de fichage s'appuyant sur des propriétés biologiques ou anthropométriques et évitant les inconvénients des procédures cryptologiques, en premier lieu la gestion des clés de chiffrement. On comprend alors leur intérêt dans des applications civiles de masse telles que la téléphonie mobile, le commerce électronique ou le télétravail.

On distingue deux sortes de mesures biométriques. La première catégorie se rapporte au comportement et aux aptitudes acquises, par exemple la locution, l'écriture ou la dactylographie. En revanche, les mesures anthropométriques expriment les propriétés innées telles que le faciès, la morphologie de l'iris, la contexture de la rétine, l'anatomie de main, la forme de l'oreille ou des empreintes digitales. D'autres méthodes se basent sur la démarche, l'odeur ou le patrimoine génétique à partir de l'A.D.N (acide désoxyribonucléique) mais ne paraissent pas utilisables pour la télé-identification.

L'utilisation des systèmes biométriques se fait en trois étapes : l'acquisition de l'image pendant la phase d'inscription, le " moulage ", c'est-à-dire, l'extraction des paramètres, et l'identification ou la vérification. L'image numérique de la personne examinée provient de signaux émanant d'un capteur ou produits par un périphérique (par exemple, un microphone). Cette image est ensuite traitée pour en extraire un moule compact et univoque de l'individu en question. Ce moule - ou signature - est alors archivé dans un recueil de références centralisé ou distribué, selon l'architecture du système.

Les *systèmes d'identification* emploient un dépôt central d'images qui sera interrogé pour mettre en adéquation l'image captée d'un individu avec une des images archivées, confirmant de la sorte l'identité déclinée au moyen d'un badge ou d'un mot de passe. En revanche, les *systèmes de vérification* se basent sur une architecture distribuée : l'image recueillie étant comparée à la signature stockée sur la carte de l'usager pour vérifier le profil de l'usager et ses privilèges d'accès.

L'exactitude d'un système d'identification se mesure en fonction du taux de confusion entre deux identités et du taux de rejet d'identités autorisées. En revanche, la performance des systèmes de vérification s'exprime par le taux de faux rejets, c'est-à-dire, de rejet d'identités autorisées et le taux de fausses acceptations (acceptation d'imposteurs). Ces taux sont interdépendants et sont ajustés en fonction du niveau de sécurité souhaité.

Le choix d'un système particulier dépend de plusieurs facteurs dont :

1. la précision et la fiabilité de l'identification ou de la vérification. Le résultat ne doit surtout pas être susceptible aux conditions ambiantes ou au vieillissement
2. le coût de l'installation, du maintien et de l'opération
3. l'universalité de l'authentification par exemple, la reconnaissance par l'écriture ne convient pas aux analphabètes
4. la facilité d'emploi
5. la reproductibilité des résultats. En général, les caractéristiques physionomiques sont plus reproductibles et moins susceptibles à la contrefaçon que les caractéristiques comportementales

6. la résistance à la contrefaçon et aux attaques.

Reconnaissance de l'acquis

Reconnaissance vocale

Les techniques d'identification par reconnaissance vocale remplissent une de deux fonctions distinctes :

- L'identification du locuteur. Il s'agit de comparer un message vocal avec un ensemble de références acoustiques stockées afin de déterminer la personne qui a parlé.
- La vérification du locuteur. Là, il convient de vérifier l'adéquation du message vocal avec la référence acoustique du locuteur qu'il prétend être.

Ces deux aspects peuvent être associés dans une même application, par exemple, la vente par commandes vocales à partir d'un téléphone mobile. Le constructeur de terminaux mobile Motorola s'est ainsi associé à Trintech (http://www.trintech.com) pour faciliter ce genre de transactions.

La taille des empreintes vocales qui constituent le moule d'un individu varie entre 1 à 70 Ko, selon l'algorithme de compression et la durée de l'enregistrement.

Dans un projet pilote démarrant en juillet 2000, la Bacob, une des cinq premières banques belges (http://www.bacob.be), a choisi de tester la technologie d'identification du locuteur que fournit Keyware Technologies (http://www.keywareusa.com) pour contrôler les virements bancaires commandés par téléphone vers un autre compte que celui du client. Le réglage se fait à partir de trois mots de passe répétés trois fois pendant la phase d'inscription afin d'établir une empreinte vocale représentative de l'individu. Lors du contrôle, le client doit prononcer un de ces mots de passe afin de faire correspondre le nouvel échantillon avec l'empreinte vocale précédemment enregistrée avant d'autoriser la transaction financière.

Une mauvaise qualité sonore peut provoquer des échecs. Dans les applications à distance, cette qualité dépend de plusieurs facteurs dont la nature du combiné téléphonique, le bruit ambiant (surtout dans les consultations par téléphone mobile), le type de liaison (terrestre ou radiophonique), etc. En outre, l'emploi de bandes pré-enregistrées peut favoriser la fraude c'est pour cela que reconnaissance automatique du locuteur doit être suppléée par d'autres agents.

Reconnaissance graphologique

Les systèmes d'identification graphologique comprennent un stylet spécial et une tablette sensible reliée à un ordinateur. Le sujet utilise le stylet pour écrire sur la tablette qui capture l'écriture et la transmet au système d'analyse et de vérification. La dynamique du mouvement du stylet est décrite au moyen d'une dizaine de paramètres tels que la pression exercée, la vitesse et la direction du mouvement, les accélérations et décélérations, l'inclinaison des lettres, etc. Le principe de la reconnaissance graphologique est de distinguer les caractères permanents d'une écriture individuelle des aspects changeants afin de pouvoir identifier le scripteur. Les caractéristiques supposées permanentes sont mises en adéquation avec le spécimen préenregistré de la personne à vérifier (Voir le site de Wacom - http://www.wacom.com - producteur japonais de tablettes graphiques).

Bien entendu, ce dispositif suppose un certain niveau d'éducation. En plus, il ne semble pas avoir atteint le taux de fiabilité exigé dans les transactions financières (le taux de faux rejets est relativement élevé) [Nalwa, 1999].

Reconnaissance dactylographique

Cette technique se fonde sur les attributs de la saisie manuelle : le rythme des frappes successives sur le clavier ainsi que la durée et l'intensité de la pression sur chaque touche. En effet, le comportement humain pendant les tâches répétitives et routinières est strictement individuel. Ces mesures dactylographiques sont effectuées pour une séquence déterminée de caractères, répétée à plusieurs reprises (par exemple, l'identité login et le mot de passe associé) [Obaidat et Sadoun, 1999].

La société Net Nanny Software International, Inc. a développé un logiciel intitulé *BioPassword LogOn for NT* (http://www.biopassword.com) qui emploie la reconnaissance dactylographique pour les stations Windows NT. L'échantillon utilisé pour constituer la grille de référence doit être constitué de 8 caractères au minimum et doit être répété 8 fois. La phase de vérification emploi 15 saisies réussies.

Reconnaissance des attributs innés

Reconnaissance de la rétine

La rétine est une tunique nerveuse interne à l'oeil qui reçoit les impressions lumineuses par ses cellules visuelles pour les transmettre ensuite sous forme de décharges électriques au nerf optique. Elle est irriguée par de nombreux vaisseaux sanguins selon une configuration propre à chaque individu et qui se maintient durant toute la vie. Une carte rétinienne peut être relevée en enregistrant la réflexion d'un rayon infrarouge de faible intensité balayant la rétine au moyen d'un appareil en couplage de charge (CCD- *Charge-coupled device*) pour constituer un descripteur de 35 octets [Hill, 1999]. Cette carte permet même de distinguer entre les vrais jumeaux.

Cette technique, commercialisée dès 1975 par la société EyeDentify, Inc. (http://www.eye-dentify.com), coûte environ $5 000 par unité. Par conséquent, elle est réservée plutôt pour le contrôle d'accès aux zones confidentielles : installations militaires, nucléaires ou pénitentiaires de haute sécurité, salles de coffres-forts, centres de contrôle de réseaux de télécommunications, etc. Selon le constructeur, le temps d'enrôlement est inférieur à une minute et le temps de vérification dans une photothèque de 1,500 personnes ne dépasse pas 5 secondes. Le taux de fausses acceptations est extrêmement bas (une erreur par million). Cependant, malgré cette fiabilité, le contact direct de l'oeil avec la sonde rétinienne risque de provoquer une gêne psychologique entraînant le refus de l'usager. En outre, le taux de faux rejets semble être assez élevé. Pour le moment, cette technique n'est pas adaptée aux systèmes de télépaiement ou aux déploiement à grande échelle.

Reconnaissance de l'iris

L'iris est la zone colorée visible entre le blanc de l'oeil et la pupille. Sa texture est une caractéristique individuelle qui reste inchangée pendant de longues années. Par conséquent, la description de la texture de l'iris au moyen d'un code numérique de 256 octets (2048 bits) permet une identification extrêmement précise avec un erreur probabiliste de l'ordre de 1 pour 1,2 million. Il est même possible de distinguer entre vrais jumeaux et de séparer les deux iris d'une même personne.

Cette technique a été initiée et brevetée par la société IriScan, Inc, formée par deux ophtalmologues et un informaticien (http://www.iriscan.com). Son grand avantage est celui d'être moins invasive que l'examen de la rétine, car il suffit à la personne à identifier de fixer l'objectif d'une caméra à un mètre de distance pour capter l'image de son iris. Ainsi, muni d'un simple PC équipé d'une caméra,

l'image initiale (20 Ko) sera ensuit traitée pour produire le code numérique qui établit la correspondance avec l'iris capté sur image. La durée de l'opération est inférieure à 800 ms avec un ordinateur opérant à la cadence de 66 MHz [Daugman, 1994, 1999 Flom, Safir, 1987 Wilkes, 1997]. Ce code devient une preuve supplémentaire s'alliant au code secret du client et au numéro de sa carte bancaire pour sécuriser les transactions effectuées en ligne.

Quelques précautions doivent être respectées pendant la prise d'image. Il faudra surtout éviter les reflets en assurant éclairage uniforme. Enfin, les lentilles de contact se révèlent par la présence d'une structure régulière dans l'image traitée.

Notons que la corrélation entre l'aspect de l'iris et la santé ou l'humeur (l'iridologie) est une notion controversée (Voir le site http://www.best.com/~joyful).

Parmi les applications envisagées citons : l'identification des utilisateurs des distributeurs automatiques de banque, le contrôle d'accès physique (locaux, machines, équipements) ou logique (accès aux réseaux, aux systèmes informatiques, etc.)

Reconnaissance du faciès ou du visage

La reconnaissance du faciès ou du visage se fait à partir d'une grille (*template*) composée de 100 à 800 octets et construite à partir de quelques paramètres tels que l'écart entre les yeux, l'écartement des narines, les dimensions de la bouche, etc. Cette méthode permet de repérer une personne parmi un ensemble de 5 000 à 50 000 images. La durée de la vérification se situe entre 3 et 20 secondes selon la taille de la photothèque. Cependant, le port de lunettes de soleil, de la barbe ou des moustaches ainsi que des grimaces ou l'inclinaison de la tête d'à peine 15° provoquent des erreurs de reconnaissance. Enfin, certains algorithmes obligent l'emploi du même appareil photographique pour l'acquisition et l'identification/vérification.

Un examen approfondi des taux d'erreur a eu lien entre 1996 et 1997 avec le concours du Laboratoire de recherche de l'armée de terre étasunienne (*US Army Research Laboratory*) [Phillips et al., 2000]. L'étude s'est reportée sur 1 196 personnes dans des différentes conditions d'éclairage et pour des écarts de temps variable entre l'image de référence et celle employée pour la classification. Les résultats soulignent que le taux de faux rejets augmente avec l'intervalle entre les deux prises d'image, ainsi que l'indique le tableau suivant :

Catégorie	Taux de fausse alarmes	Taux de faux rejets
Même jour, même éclairage	2	0,4
Même jour, éclairage différent	2	9
Écart de quelques jours	2	11
Écart d'un an et demi	2	43

TrueFace™ de la société Miros est le seul produit de reconnaissance du faciès certifié par l'Association international de la sécurité informatique (*International Computer Security Association*) ICSA en 1998. Il est en cours d'évaluation dans des systèmes " liquide contre chèques " (*check cashing*) dans les distributeurs en libre service et dans les casinos. Visionics Corporation commercialise

l'algorithme FaceIt® développé à la Rockfeller University (http://www.Faceit.com). (http://www.viisage.com)

Reconnaissance de l'empreinte digitale

On sait que la forme des empreintes digitales est une caractéristique permanente de chaque individu. La méthode traditionnelle de prise d'images digitales consiste à maculer l'extrémité des doigts (ou de la paume) à l'aide d'une encre spéciale puis de les apposer sur papier pour relever en négative l'image. Cependant, de nouvelles méthodes d'imagerie permettent d'acquérir des images numérisées au moyen de capteurs optiques, optoélectroniques, électriques ou thermiques. Ces méthodes peuvent être facilement adaptées aux applications de commerce électrique en ligne ou de téléphonie mobile.

Ainsi, les fluctuations de la capacitance entre les doigts de l'usager et des capteurs aménagés dans une sourie spéciale dessinent le contour de l'empreinte. D'autre part, en appliquant un courant alternatif de faible tension aux pulpes digitales, on arrive à mesurer les variations du champ électrique entre une platine de résine sur laquelle repose le doigt et le derme. Les variations du champ électrique traduisent les détails de l'empreinte du fait que le derme en épouse la forme. Dans les techniques thermiques, le capteur mesure le gradient de température sur la surface de la sourie, localisant de la sorte les points de friction, donc de tangence avec la paume. Enfin, les méthodes opto-électroniques emploient une couche polymérique pour capter l'image de l'empreinte qu'un transducteur transforme ensuite en un courant électrique proportionnel à cet image.

Pendant la phase d'enrôlement, l'empreinte de l'utilisateur est enregistrée puis traitée pour en extraire les singularités ou *minuties*. Ces minuties constituent la " signature " qui servira de référence dans la phase de vérification. Elles doivent donc comprendre un ensemble d'indices stables, fiables et peu sensibles aux éventuels défauts d'image qu'introduisent la saleté des doigts, les déformations, les blessures, etc. Chaque minutie occupe en moyenne 16 octets. La taille des images produites varie entre 500 et 1500 octets en fonction du nombre de minuties préservées et du taux de compression employé.

Pour contrôler l'identité d'une personne, les minuties dégagées de la nouvelle empreinte seront mises en adéquation avec celles extraites de l'image de référence. Les algorithmes employés doivent être insensibles aux éventuelles translations, rotations et distorsions. Le degré de similitude entre les deux images analysées est décrit à l'aide d'un indice variant de 0 % et 100 %. Le pourcentage de faux rejets dans les systèmes commerciaux atteint 3 % environ et le taux de fausse acceptation est inférieur à une personne par million. Certains appareils utilisent l'image du doigt en entier et non pas seulement celles des extrémités [Takeda et al., 1990].

Alors que Swift avait parrainé le développement d'une sourie avec transducteur de capacitance, c'est la société Secugen qui a eu la primeur d'offrir un produit commercial pour les utilisateurs en ligne. Le tableau distinguent quelques offres commerciales selon la phénomène physique employé.

Liste de quelques offres commerciales

Phénomène utilisé	Société	Produit	Adresse URL
Capacitance	Infineon	Finger-print Security	http://www.infineon.com
	Secugen	EyeD Mouse	http://www.secugen.com
Champ électrique	Authentec	FingerLoc	http://www.authentec.com

	Veridicom	FPS110	http://www.veridicom.com
Optique	Identix	BioCard/Touchlock	http://www.identix.com
Optoélectronique	Who?Vision	TactileSense	http://www.whovision.com
Température	Thomson-CSF	FingerChip	http://www.tcs.thomson-csf.com

Reconnaissance de la géométrie tridimensionnelle de la main

La reconnaissance de la forme géométrique de la main est une des méthodes employées pour le contrôle d'accès. Cette méthode se rencontre depuis plus de deux décennies dans des applications commerciales et de grande échelle : entreprises, douanes, hôpitaux, bases militaires, prisons, etc. Aux États-Unis, par exemple, elle est utilisée par les aéroports de New York et de Newark pour accélérer le contrôle de personnes ayant fait plus de cinq entrées par an.

La prise d'un cliché numérique se fait en 1,2 seconde environ au moyen d'un appareil photographique en couplage de charge. Il suffit de faire buter les doigts écartés contre des tiges de positionnement soudées à une platine en face de l'objectif. La planche est entourée de miroirs sur trois côtés afin de capter la main en latéral et de face en même temps. La moyenne de plusieurs prises (3 à 5) est stockée en mémoire comme référentiel pour l'individu.

Les calculs emploient un modèle géométrique tridimensionnel pour examiner 90 caractéristiques et former une image de 9 octets de taille.

Parmi les compagnies actives dans ce domaine citons par ordre alphabétique :BioMet Partners (http://www.biomet.ch) et Recognition Systems (http://www.recogsys.com).

Évaluation

Le tableau suivant récapitule la taille des moules employés pour chaque méthode anthropométrique.

Caractéristique	Taille du moule en octets
Balayage de la rétine	35
Balayage de l'iris	256
Empreinte digitale	500 - 1500
Forme de la main	9
Forme du faciès	100 - 800

La richesse de l'offre montre que les méthodes d'identification biométrique méritent d'être sérieusement considérée pour les applications de commerce électronique. Il leur manque cependant quelques réquisits dont :

1. des protocoles d'évaluation normalisés afin de pouvoir comparer les performances des diverses techniques ou produits dans un environnement opérationnel et non seulement au laboratoire
2. une évaluation impartiale de la résistance de chaque système aux attaques (internes ou externes). Ces attaques peut advenir au niveau des capteurs, des liaisons entre les capteurs et l'unité de traitement, et de la connexion de cette dernière et l'administration centrale les données de référence
3. des modèles normalisés afin de faciliter les échanges de données entre deux méthodes de traitement. Sinon, chaque application dépendra d'un seul constructeur ou fournisseur. Cette lacune freine i le développement de logiciels, les développeurs n'étant pas sûr de la rentabilité de leurs efforts vu l'étroitesse du marché
4. Des formats normalisés pour le stockage des fichiers de référence.

Du point de vue des applications civiles de masse (comme pour le commerce électronique en ligne), ces systèmes présentent l'inconvénient que l'individu doit être physiquement présent pendant l'enrôlement.

Références

J. G. Daugman, " Recognizing persons by their iris patterns " U.S. Patent 5 291 560, 1994.

J. G. Daugman, " Biometric personal identification system based on iris analysis " Dans *Biometrics : Personal identification in networked society*, A. Jain, R. Bolle, S. Pankati (dir.), Kluwer Academic Publishers, 1999, p. 104-121.

L. Flom, A. Safir, " Iris recognition system ", U. S. Patent 4 641 349, 1987.

R. Hill " Retina identification ". Dans *Biometrics : Personal identification in networked society*, A. Jain, R. Bolle, S. Pankati (dir.), Kluwer Academic Publishers, 1999, p.123-124.

V. S. Nalwa " Automatic on-line signature verificatin ". Dans *Biometrics : Personal identification in networked society*, A. Jain, R. Bolle, S. Pankati (dir.), Kluwer Academic Publishers, 1999, p. 143-163.

M. S. Obaidat, N. Sadoun " Keystroke dynamics based authentication ". Dans *Biometrics : Personal identification in networked society*, A. Jain, R. Bolle, S. Pankati (dir.), Kluwer Academic Publishers, 1999, p.213-225.

P. J. Phillips, A. Martin, C. L. Wilson, M. Przybocki " An introduction to evaluating biometric systems ", *Computer* 3(2) : 56-63, Feb. 2000.

M. Takeda, S. Uchida, K. Hiramatsu, T. Matsunami, " Finger image identification method for personal verification " *Proceedings of the 10th international conference on pattern recognition*, Vol. 1 :761-766, 1990.

R. P. Wildes " Iris recognition : An emerging biometric technology " *Proceedings of the IEEE* 85(9) :1348-1363, 1997.

Sites

http://www.biometric.freeserve.co.uk
Site maintenu par Julian Ashbourn (anglais) contient des renseignements généraux sur les techniques de biométrie, les offres commerciales et les associations actives dans ce domaine.

http://www.biometricgroup.com
Site fournissant des renseignements sur les techniques biométriques et sur les différents fournisseurs avec des liens aux sites des ces vendeurs.

http://www.biometrics.org/REPORTS/BioRef.html
Une liste préparée en novembre 1995 par Roger Johnson du Los Alamos National Laboratories contenant de 544 références.

http://biometrie.online.fr
Site comprenant un dossier complet sur les techniques biométriques et des listes annotées des produits, des fournisseurs, une revue de presse de 1997 et des sujets d'actualités. Les articles publiés sont réalisés par des volontaires.

http://.www.cs.rug.nl/~peterkr
Site préparé par Peter Kruizinga, un docteur en informatique à l'Université de Groningen aux Pays-Bas et qui fournit de nombreuses pistes sur les recherches actuelles en biométrie, dont de nombreuses références universitaires sont publiées en ligne.

http://vismod.www.media.mit.edu/vismod/demos/facerec/feret_res.html
Site présentant un résumé des résultats parrainés par le laboratoire de l'armée de terre étasunienne en 1996 mettant en jeux cinq algorithmes de reconnaissance du faciès.

***Hashem Sherif*, 24 juin 2000**