

L'ESPIONNAGE NUMERIQUE

BIOMETRIE ET SECURITE

La signature digitale

« Le XXIème siècle sera caractérisé par un bouleversement des interfaces hommes-machines, nous conduisant progressivement à cette intégration de nos cerveaux avec les réseaux de télécommunications et les ordinateurs » indiquait récemment Joël de Rosnay. Il affirmait également que « nous allons vers une troisième étape qui sera bioélectrique, où des paramètres seront captés directement sur notre corps. Nous porterons des outils quasi invisibles comme un écouteur dans l'oreille ou un capteur fixé à une montre. »

Au dernier sommet européen de la microélectronique, il a été estimé que dans 10 ans, chaque terrien utiliserait dans sa vie quotidienne près de 1 milliard de transistors intégrés, dans sa voiture, son téléphone, son PC et ses vêtements. Ce total colossal représente l'équivalent d'une centaine de microprocesseurs haut de gamme d'aujourd'hui comprenant chacun environ une dizaine de millions de transistors.

Au-delà des nouvelles technologies de l'information et de la communication, la biométrie prend une place à part, certainement prépondérante dans un futur proche car, c'est elle qui va définitivement « greffer » l'informatique et l'électronique dans le biologique, au sein même du corps humain.

Il est clair que l'évolution va obligatoirement se coupler à des dispositifs biométriques, lesquels, à partir des caractéristiques spécifiques de la personne humaine et non plus d'un simple mot de passe, donneront accès aux ordinateurs, aux automates bancaires, au paiement sur Internet et à une multitude de fonctions et d'activités privées et professionnelles.



Déjà l'ordinateur biométrique sort des laboratoires en utilisant certaines « signatures digitales » supposées uniques et quasi infaillibles comme l'iris de l'œil (il n'y a que 1 chance sur 10 puissances 50 que 2 individus présentent 2 iris identiques), le timbre de la voix, les mouvements des doigts sur le clavier ou l'empreinte digitale pour le rendre inviolable. L'objectif de la biométrie est d'offrir un maximum de sécurité dans l'identification de l'utilisateur, en faisant que lui seul devienne l'unique mot de passe. Pour la première fois dans l'histoire de l'humanité, la biométrie va lier de façon imparable une activité économique ou sociale aux caractéristiques unique de chaque individu.

LES PREMIERES APPLICATIONS BIOMETRIQUES

Actuellement, les 3 premières facettes de cette nouvelle technologie de l'identification en phase industrielle sont :

- La reconnaissance d'écriture au clavier :

Elle représente l'une des voies les plus prometteuses de la biométrie. Le principe repose sur le constat que chacun tape de façon différente sur un clavier, même si le plus souvent, ces écarts sont imperceptibles pour l'œil humain. Il suffit d'enfoncer une vingtaine de touches pour que le logiciel mémorise de façon définitive la « signature » de l'utilisateur.

- La reconnaissance du visage :

Peu contraignante pour l'utilisateur et relativement bon marché, elle suppose dans un premier temps que l'utilisateur se laisse prendre en photo, afin que le système mémorise les caractéristiques numériques du visage. Ensuite, opère « l'intelligence » du logiciel qui traite les clichés fournis par la caméra, lesquels sont comparés à ceux mémorisés dans une base de données.

- Le lecteur d'empreintes digitales :

Il existe déjà et pas seulement dans les films de science-fiction. De petites puces de la taille d'un timbre-poste permettent de lire une empreinte digitale avec une efficacité correspondant « aux critères définis par le FBI pour ses propres systèmes de protection ».



MODE D'EMPLOI DE LA BIOMETRIE

1^{ère} étape : Il s'agit de mémoriser dans l'ordinateur les informations (empreintes digitales, échantillon de voix modélisation du visage ou de l'iris de l'œil, caractéristiques de la façon de taper sur un clavier) que l'utilisateur est le seul à pouvoir fournir.

2^{ème} étape : L'informaticien paramètre son logiciel de façon à donner soit une certaine souplesse, soit une grande rigidité. Dans le premier cas, le système risque de laisser passer plus d'utilisateurs qu'il ne faut, mais il ne bloquera pas quelqu'un d'autorisé. Dans le second cas, là où la sécurité est primordiale, le système risque de refuser l'accès à quelqu'un d'autorisé afin d'être certain que personne n'entre indûment. C'est à cet échelon que la biométrie offre une véritable supériorité par rapport aux systèmes traditionnels d'autorisation.

3^{ème} étape : Une fois les caractéristiques paramétrées, celles-ci sont intégrées dans une base de données pour être utilisées ultérieurement par le logiciel, qui les comparera chaque fois à celles que l'utilisateur se présentera pour être identifié.

BIOSECURITE, 12 PROCEDES D'IDENTIFICATION

Dans le secret des laboratoires, certains procédés d'identification sont actuellement à l'essai en essayant d'exploiter des caractères morphologiques de l'homme. En ce domaine, l'avenir est certainement dans le couplage simultané de 2 ou de plusieurs systèmes de biosécurité.

Liste des principaux procédés actuellement expérimentés en matière de biométrie :

1) L'IRIS

La personne qui cherche à se faire identifier doit fixer l'objectif d'une caméra qui récupère instantanément le dessin de son iris, c'est à dire la membrane colorée de l'œil (vert, bleu, marron, noir). La durée de l'opération est de moins de 2 secondes avec un taux d'erreur estimé à 1 sur 10.000. Le système peut toutefois être trompé avec une lentille de contact qui reproduirait, à partir d'une simple photo, l'iris d'une personne habilitée.



2) LA RETINE

Ce système parmi les plus fiables, suppose qu'une caméra capture la distribution des vaisseaux sanguins de la membrane située au fond de l'œil et compare cette image avec celles contenues dans une base de données. D'une durée de 1,5 seconde, ce procédé n'est pas anodin car il suppose d'illuminer le fond de l'œil. En se fondant sur 90 points de comparaison sur les 2 yeux, le risque d'erreur est de seulement 222 sur 6 milliards d'individus.

3) LA GEOMETRIE DU VISAGE

L'écartement des narines, la forme du nez, l'écart entre les 2 yeux, la largeur de la bouche ou la hauteur de l'espace naso-labial permettent à un ordinateur d'opérer des corrélations suffisantes en une dizaine de clichés. Si la marge d'erreur est estimée à moins de 1 %, le système s'adapte toutefois assez mal aux changements de physionomie (lunettes, barbe) et se révèle incapable de différencier deux vrais jumeaux.

4) LA THERMOGRAPHIE

Très cher, ce système fonctionne avec une caméra thermique qui produit un cliché infrarouge du visage, faisant apparaître une répartition de la chaleur qui reste unique pour chaque individu. Il est ainsi possible de cartographier le réseau veineux du visage invisible à l'œil nu. La distinction entre de vrais jumeaux est possible avec ce procédé.

5) LA STEREOSCOPIE

Elle permet l'analyse en relief du visage à partir d'un examen géométrique en trois dimensions. La stéréoscopie ne concerne que le haut du visage, Afin de s'affranchir des déformations engendrées au niveau des joues par d'éventuelles grimaces, une prise de poids ou une rage de dents.

6) L'EMPREINTE VOCALE

Comme l'empreinte digitale, l'empreinte vocale est unique d'un individu à l'autre. La voix est saisie à l'aide d'un micro puis amplifiée et filtrée avant d'être numérisée selon des courbes d'intensité distinctes. Le principe de la « serrure vocale » est le moins cher des systèmes de biosécurité, bien qu'il souffre d'un taux d'erreur moyen de 5 %. La fatigue, le stress ou un simple rhume modifiant la physiologie de la voix peuvent rendre le système totalement inopérant.



7) LA DENTURE

La radiographie dentaire panoramique permet d'identifier un individu de manière imparable. Cependant ce procédé basé sur l'analyse des os de la mâchoire et de la denture oblige d'irradier faiblement chaque personne qui demande l'autorisation d'entrer.

8) L'OREILLE

Les propriétés anthropométriques des oreilles sont propres à chaque individu. Pavillon, conque, lobe, hélix, anthélix, etc.

Les différences morphologiques d'une oreille à l'autre sont assez notables pour caractériser à la fois certaines grandes lignes du profil psychologique des individus mais aussi son identification. L'institut de recherche criminelle de la gendarmerie nationale française a ainsi pu confondre un criminel à partir de la simple photo de son oreille prise dans un distributeur de billets, alors que celui-ci tentait d'utiliser la Carte Bleue de sa victime.

9) L'EMPREINTE DIGITALE

C'est la technique de biosécurité la plus courante. L'empreinte du doigt est saisie en temps réel par un capteur optique, puis « nettoyée » par un logiciel de traitement de l'image. La comparaison ne porte que sur 80 points de comparaison et non pas sur la totalité du dessin de l'empreinte digitale. Ce système est l'un des moins chers et parmi les plus fiables, surtout lorsqu'il inclut des capteurs thermiques capables de détecter le flux sanguin, ceci afin de pouvoir déjouer l'empreinte reproduite sur un tampon ou le doigt coupé.

10) LA RECONNAISSANCE DE LA MAIN

La technique la plus utilisée repose sur la géométrie de la main. Une analyse tridimensionnelle permet d'étudier certaines caractéristiques comme la largeur et l'épaisseur de la paume, les dessins des lignes de la main ou encore la longueur des doigts qui sont propres à chaque individu. Avec ce procédé, il est également possible de faire ressortir en infrarouge, les réseaux veineux pour rendre le système encore plus performant.

11) LES BATTEMENTS DU COEUR

Encore au stade expérimental, ce procédé repose sur la transformation de l'électrocardiogramme en système de biosécurité.



12) L'ODEUR

Un nez électronique doit repérer les spécificités de l'odeur humaine en reniflant la main de l'arrivant, laquelle est placée devant une rangée de capteurs. Il se charge alors d'analyser les molécules des différents composés chimiques dégagés par la peau. La commercialisation de ce procédé est en cours.

LITTLE BROTHER

« Le danger n'est pas que les technologies de l'information soient utilisées à bon ou mauvais escient, mais de façon totalement irresponsable ». C'est le sentiment partagé par de nombreux observateurs de l'évolution des technologies, qui pensent que passé le stade de l'émerveillement technique, le grand public n'en vient à ressentir l'aspect inquiétant de certaines de ces technologies. En fait, le plus grand risque est que les « signatures digitales » facilitent un suivi de chaque utilisateur à la « Big Brother ». La combinaison des informations recueillies au cas par cas, pourrait en de mauvaises mains ouvrir la porte à une sorte de « fichage » informatique systématisé.

Les dangers potentiels de la biométrie sont que bientôt les compagnies d'assurances, les banques, les grands magasins, les grandes entreprises pourront non seulement retracer l'emploi du temps de leurs abonnés, de leurs clients et de leurs personnels mais aussi connaître avec précision leur passe-temps et leurs petites manies. En fait, être capable d'anticiper avec justesse leurs habitudes, leurs besoins et les moyens pour y parvenir.

Sur Internet, il existe des « cookies », c'est à dire de petits marqueurs logiciels qui permettent de repérer l'internaute lorsque celui-ci revient sur un site qu'il a déjà visité.

Ce n'est pas la biométrie - qui relève d'une technologie neutre - qui a initié le désir d'en savoir plus sur l'individu. Des organismes privés et publics collectent depuis très longtemps des informations plus ou moins personnelles et confidentielles.

Genève, octobre 2003

Jacques GUILLET
Conseiller en sécurité
et sûreté économique



JG SECURITE

