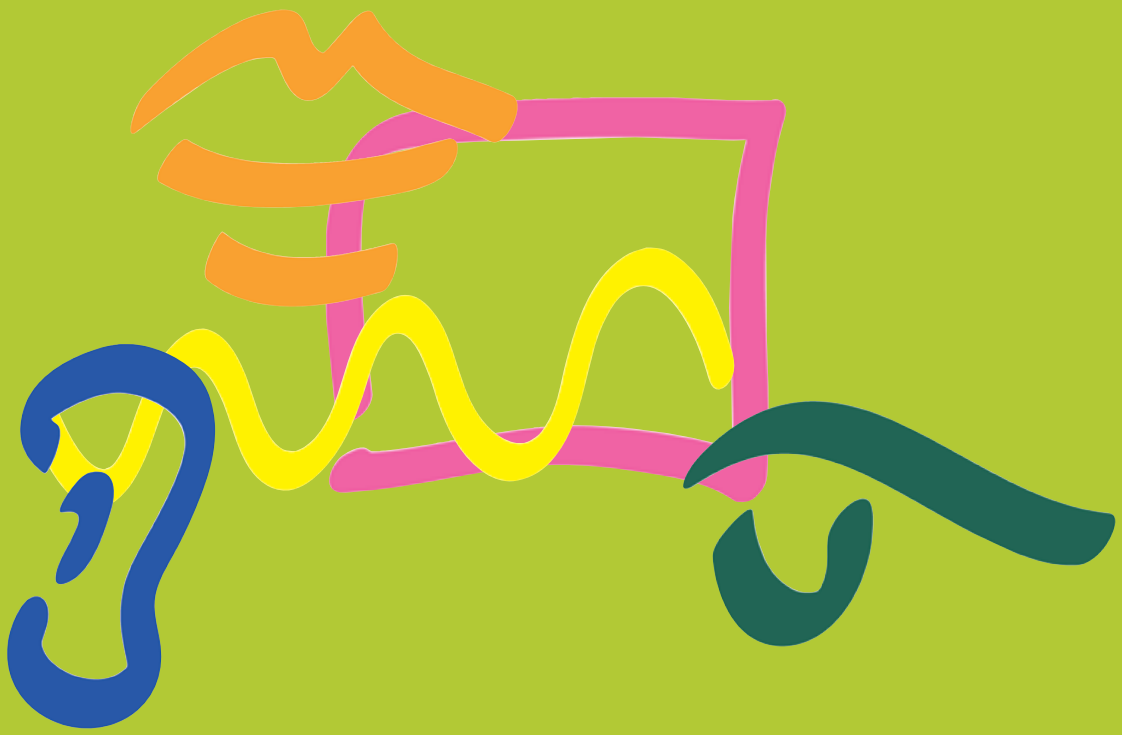
Biométrie : au doigt, à l'œil et à la voix



Trois équipes du GET, à Télécom Paris, à l'INT et à Eurécom, participent à un ensemble de projets de recherche sur les techniques et les usages de la biométrie, coordonné par l'INT et dont l'objectif est l'authentification en temps réel d'une personne à partir de ses caractéristiques physiques. La biométrie peut remplacer les codes d'accès et s'appliquer aux environnements physiques ou virtuels dans lesquels la sécurité est fondamentale.

Chaque individu possède des caractéristiques qui lui sont propres : sa voix, ses empreintes digitales, les traits de son visage, la forme de sa main, sa signature… et jusqu'à son ADN. Ces données dites « biométriques » peuvent ainsi être utilisées pour l'identifier.

Si autrefois ces méthodes étaient surtout utilisées par la police, aujourd'hui un individu a besoin d'être identifié dans une multitude de contextes : pour pénétrer dans son immeuble ou ouvrir la porte de son appartement, pour retirer de l'argent à un distributeur, pour pénétrer dans des bâtiments et y circuler librement, pour accéder à son poste de travail, à sa messagerie, à Internet et plus généralement, partout où la sécurité est essentielle.

Actuellement, pour vérifier l'identité, on utilise surtout des codes, mots de passe et autres numéros d'identification personnels, qui présentent un double inconvénient :

– il faut les mémoriser ;

– il y a un risque qu'ils soient utilisés par des personnes non autorisées.

Alors pourquoi ne pas les remplacer par des données biométriques?

La clé de la fiabilité : associer plusieurs données biométriques ou « modalités »

Aucune modalité biométrique n'est en elle-même fiable à 100 %.

Il existe des situations, liées aux dispositifs de capture des données, à l'utilisateur lui-même ou à l'environnement lors de la capture, dans lesquelles une modalité quelconque peut s'avérer défaillante.

– les empreintes digitales d'un travailleur manuel le rendent réfractaire à toute identification ;

– une extinction de voix d'un utilisateur ou le bruit ambiant trop important au moment de la capture de sa voix vont pénaliser la vérification de ce locuteur.

D'autre part, pour une personne donnée, une modalité peut être trop variable, ce qui empêche de l'identifier ainsi. C'est le cas de la signature, que certaines personnes font rarement deux fois de la même façon.

Cet état de fait conduit les chercheurs à associer différentes modalités biométriques afin de fiabiliser les résultats et rendre les systèmes de vérification plus adaptés, face à toute une panoplie de situations d'usage.

Au-delà des raisons techniques évoquées, de nombreux facteurs humains liés à la perception de ces systèmes de vérification de l'identité par le public interviennent en phase d'utilisation réelle :

– une prise d'empreintes digitales peut avoir une connotation policière ;

– une modalité donnée peut être perçue comme une intrusion dans la vie privée ;

– un capteur précis peut être rejeté par le public pour des raisons d'hygiène, etc.

Face à ces multiples écueils, d'ordre technique et humain, la multimodalité apparaît comme une solution à fort potentiel. Elle est un des objectifs majeurs de la recherche menée actuellement au sein du GET.

Ainsi, l'équipe de Gérard Chollet à Télécom Paris poursuit des recherches sur la vérification d'identité par la parole (reconnaissance vocale du locuteur) et participe à ce titre à des projets européens et internationaux.

L'équipe Intermedia, à l'INT, dirigée par Bernadette Dorizzi, s'appuie sur son expérience dans le domaine de l'écriture manuscrite en ligne pour étudier la fusion de données biométriques et la vérification de l'identité par la modalité signature en ligne.

L'équipe d'Eurécom, avec Christian Wellekens et Jean-Luc Dugelay, réunit également de fortes compétences en combinant trois des modalités étudiées : la voix, le visage et les empreintes digitales.

Constituer une base multimodale de données biométriques

La biométrie multimodale nécessite de réaliser la fusion entre les différentes modalités biométriques.

La vérification multimodale peut être effectuée, par exemple, sur une séquence vidéo d'une personne en train de parler ; dans ce cas, les modalités utilisées peuvent être la reconnaissance du visage (face et profil) et la vérification du locuteur.

« Alors qu'en reconnaissance vocale on a un taux de l'ordre de 1 % d'erreur en mode "dépendant du texte" (mot de passe) et de 10 % d'erreur en mode "indépendant du texte", le multimodal peut atteindre 0 % d'erreur, à condition qu'il n'y ait pas d'imposture délibérée », estime Gérard Chollet.

Mais le multimodal nécessite une pondération des différentes modalités. *« La pondération doit être très fine en fonction de la situation.*

Acquisition des modalités.

Les travaux issus du projet BIOMET sont valorisés au niveau de la France et de l'Europe au travers des collaborations industrielles (Thalès, ST-Microelectronics…) : dans le projet européen MÉDÉA Trust-ES, coordonné par Gemplus, l'INT gère l'étude de la faisabilité de la biométrie multimodale sur carte à puce.
Le projet européen SECUREPHONE, coordonné par Schlumberger, s'intéresse plus particulièrement aux aspects mobilité (PDA, téléphone mobile…).

Différentes techniques d'apprentissage statistique sont utilisées à ces fins », précise Sonia Salicetti.

La base de données multimodale constituée dans le cadre du projet BIOMET stocke cinq modalités pour chaque personne dont il faudra vérifier l'identité.

« Notre objectif est de créer une base de données pour cinq modalités : les empreintes digitales, la forme du visage, la voix, la signature en ligne et la forme de la main », indique Sonia Salicetti.

« Nous évaluons les systèmes de vérification en les combinant et en montrant l'apport du multimodal en termes de robustesse et de fiabilité, par rapport à un seul mode. »

À des fins applicatives, et dans le but de sécuriser l'approche biométrique par rapport à la protection de la vie privée, on ne retient que certaines caractéristiques extraites sur les données brutes capturées dans la base BIOMET : par exemple, les points caractéristiques des sillons cutanés ou « minuties » pour les empreintes digitales, les fréquences et harmoniques pour la voix, au lieu d'une image complète ou une séquence audio ou vidéo. Le volume est de l'ordre de 100 bits par mode.
« Tout cela tient largement dans une carte à puce, et peut donc s'appliquer à un terminal point de vente ou à distance », ajoute Gérard Chollet.

Le GET étudie aussi la faisabilité de ces systèmes par rapport aux usages (notamment dans le projet sur crédits incitatifs BIOLAB) et aux moyens de capture des données biométriques.

Il s'agit enfin de sécuriser ces données, en les cryptant.

Scanner : forme de la main.

Le GET est chef de file du réseau d'excellence européen BIOSECURE, conduit par Bernadette Dorizzi de l'INT, qui rassemble plus de trente partenaires. Ce réseau d'excellence permettra de concentrer les approches multidisciplinaires des équipes de recherche, pour faire émerger des méthodes innovantes d'authentification biométrique.

Les principales modalités biométriques

La voix
Analyse des caractéristiques quantitatives : fréquences, harmoniques, puissance sonore, etc.

Les empreintes digitales
Analyse des détails caractéristiques des sillons cutanés, ou « minuties » : terminaison des sillons, croisements, bifurcations, etc.

L'œil (rétine ou iris)
Analyse de la disposition des muscles circulaires et radiaux qui ouvrent et ferment la pupille.

La main
Analyse de la longueur, largeur, forme des phalanges, des articulations, des lignes de la main, etc.

Le visage (en lumière visible ou infrarouge)
Analyse de la géométrie du visage de face et profil, ou en trois dimensions : forme des yeux, de la bouche, du nez, position des pommettes, etc.) à partir d'une photographie numérique ou d'une caméra infrarouge (thermographie pour utilisation dans le noir) ; celle-ci permet l'analyse des vaisseaux sanguins du visage.

L'oreille
Analyse de la forme de l'oreille.

La signature (reconnaissance statique ou dynamique)
Analyse de la forme (statique) et/ou de la vitesse et de la trajectoire de la signature (dynamique).

L'ADN
La méthode la plus fiable pour identifier une personne, mais actuellement pas adaptée à la reconnaissance en temps réel.