LIVRE BLANC

Qu'est-ce que la biométrie?

AWARE

Copyright ©2014 Aware, Inc. All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means, electronic, mechanical photocopying, recording, or otherwise without the prior written permission of Aware, Inc.

This document is for information purposes only and is subject to change without notice. Aware, Inc. assumes no responsibility for the accuracy of the information. AWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. "Aware" is a registered trademark of Aware, Inc. Other company and brand, product and service names are trademarks, service marks, registered trademarks or registered service marks of their respective holders. WP_WhatareBiometrics_0114_v01

Qu'est-ce que la biométrie?

Identité et confiance

Modalités biométriques

Processus biométriques

Test de fiabilité des systèmes biométriques

Applications biométriques

Instruments et capteurs

Modes d'utilisation et architecture système

Vie privée

Sécurité

Identité et confiance

Il existe un nombre infini d'éléments nous concernant qui, pris tous ensemble, font de nous des personnes uniques. Il s'agit par exemple de nos caractéristiques physiques, de notre adresse postale, de notre date de naissance, de nos relations et de notre éducation. L'unicité de nos caractères physiques et de notre histoire personnelle s'incarne dans ce que nous appelons communément notre "identité". Dans le monde interconnecté d'aujourd'hui, baigné d'informatique, il devient plus que jamais utile 1) d'attribuer correctement des informations numériques à un individu et 2) de prouver notre identité par des moyens communicables et fiables. Notre identité peut servir à nous attribuer correctement des informations nous concernant, ceci à des fins pouvant trouver leur utilité dans le futur (ex : un registre médical ou financier). Mais ces enregistrements permettent également de mettre en évidence un historique des comportements, ceci afin d'établir un lien de confiance, et ainsi mettre chacun devant ses responsabilités. Nous exploitons cette confiance et cette responsabilisation pour obtenir des privilèges comme l'accès à une ressource, un établissement ou un pays. Dans le cadre de l'accès, l'utilité de l'identité est double : tout d'abord, il s'agit de communiquer notre crédibilité et notre responsabilité puis, lorsque nous tentons de faire valoir le "capital confiance" que nous avons gagné, de prouver que nous sommes bien la personne avec laquelle ce lien de confiance a été précédemment établi. Inversement, notre identité peut être remise en question afin de contrer de fausses déclarations, ou utilisée par quelqu'un d'autre afin de susciter la méfiance à notre égard.

"La biométrie recense nos caractères physiques (et comportementaux) les plus uniques, qui peuvent être captés par des instruments et interprétés par des ordinateurs de façon à être utilisés comme des représentants de nos personnes physiques dans le monde numérique. Ainsi, nous pouvons associer à notre identité des données numériques permanentes, régulières et dénuées de toute ambiguïté, et récupérer ces données rapidement et automatiquement à l'aide d'un ordinateur."

Nos noms et numéros personnels s'avèrent être des moyens éprouvés, relativement efficaces, pour prouver notre identité. Surtout, ils peuvent être interprétés non seulement par des personnes, mais aussi par des ordinateurs afin de nous associer des informations numériques et des attributs de confiance ou de méfiance, ce qui est évidemment très utile dans de nombreuses applications. Un dossier scolaire, une contravention pour excès de vitesse et un historique de crédit en sont de bons exemples. Cependant, nos noms et numéros ne sont efficaces que dans la mesure où ils sont 1) uniques, 2) permanents, 3) réguliers et 4) liés sans ambiguïté à nos personnes physiques. Or, nous savons qu'ils ne sont pas nécessairement uniques (ex : Jean Martin), ni permanents (ex : Jeanne Martin née Dupont), et qu'ils ne sont manifestement pas liés à nous physiquement (ex : par un tatouage sur le front). Voici où la biométrie moderne entre en jeu. La biométrie recense nos caractères physiques (et comportementaux) les plus uniques, qui peuvent être captés par des instruments et interprétés par des ordinateurs de façon à être utilisés comme des représentants de nos personnes physiques dans le monde numérique. Ainsi, nous pouvons associer à notre identité des données numériques permanentes, régulières et dénuées de toute ambiguïté, et récupérer ces données rapidement et automatiquement à l'aide d'un ordinateur.

Modalités biométriques

On parle beaucoup de l'étendue des modalités biométriques, et les recherches dans les nouveaux procédés biométriques (oreille, démarche, odeur, etc.) sont effectivement convaincantes. Toutefois, les seules modalités éprouvées à grande échelle sur le terrain sont la reconnaissance des empreintes digitales, du visage, de l'iris et de la voix. Il se trouve que ce sont les modalités biométriques qui, à ce jour, répondent le mieux à nos tests d'unicité, de permanence et de régularité, leur capture par des instruments étant par ailleurs possible de manière ergonomique et économique. Des techniques propriétaires[1] ont également vu le jour pour la géométrie vasculaire (veines de la paume et des doigts) et des mains.

La biométrie est par nature essentiellement statistique, aussi en découle-t-il que :

a) plus le nombre de données d'un échantillon biométrique (ou d'un ensemble d'échantillons) est important, plus il y a de chances qu'elles soient uniques,

b) il existe toujours un risque pour que deux individus distincts génèrent des échantillons biométriques similaires ou équivalents, et

c) il existe toujours un risque pour que des faux positifs ou des faux négatifs (erreur de type I ou II) émergent d'une comparaison biométrique.

Certaines modalités biométriques sont moins permanentes que d'autres dans le long terme, et certaines sont plus difficiles à présenter et à capturer de manière régulière. D'autres encore sont plus propices à générer des problèmes de qualité d'échantillon.

La modalité biométrique parfaite est un mythe ; chacune a ses avantages et ses inconvénients pour un cas d'utilisation donné. Par exemple, la caractéristique la plus remarquable des empreintes digitales en tant que modalité est sans doute leur capacité à laisser des preuves "latentes" sur une scène de crime (ex : empreintes de doigt sur du verre). Les iris sont probablement la modalité la plus régulière et la plus riche en informations, semblable à un code à barres. Les images faciales se distinguent dans le sens où il s'agit d'une modalité biométrique que les êtres humains savent comparer avec une grande habileté, aussi devient-il possible d'intégrer des processus de reconnaissance complémentaires entre l'homme et la machine. De plus, les images faciales sont légion dans le monde numérique, et peuvent aussi être collectées à distance en toute discrétion. La voix a ceci de notable qu'elle entre à la fois dans la catégorie comportementale et physique. Les échantillons disponibles pour un individu donné sont par conséquent abondants.

Même lorsque nos échantillons biométriques sont uniques, permanents, réguliers et physiquement liés à nous, les capteurs et les algorithmes que nous avons conçus pour les acquérir et les analyser restent, eux, imparfaits. Les capteurs induisent des distorsions optiques et électriques. Des informations sont perdues lorsque les données des échantillons sont converties du format analogique au numérique, puis à nouveau lorsque le signal numérique est compressé. Les fréquences d'échantillonnage (la résolution spatiale dans le domaine numérique) affectent de manière non négligeable la qualité des échantillons biométriques. Les algorithmes conçus pour extraire à partir d'un échantillon des "modèles" destinés aux comparaisons informatiques varient énormément en termes de précision et de performances, de même que les algorithmes et les systèmes utilisés par les ordinateurs pour évaluer rapidement leur similarité. Les machines sont douées pour le traitement automatisé, très rapide et raisonnablement fiable des signaux et pour la comparaison des modèles, mais elles ne possèdent pas la capacité humaine de percevoir, d'analyser et de caractériser visuellement la similarité entre deux échantillons. Néanmoins, nos personnes physiques fournissent une multitude de caractères très bien adaptés à la comparaison et à la recherche biométriques, et les avancées technologiques dans le domaine des capteurs et des ordinateurs améliorent sans cesse la capacité des machines à procéder à des identifications biométriques de manière extrêmement rapide et fiable.

Processus biométriques

Les systèmes biométriques s'appuient sur plusieurs processus distincts : enregistrement, capture directe, extraction de modèle et comparaison de modèle. L'objectif de l'enregistrement consiste à collecter et archiver des échantillons biométriques, et à générer des modèles numériques pour des comparaisons ultérieures. En archivant les échantillons bruts, il devient possible de générer des modèles de remplacement, au cas où de nouveaux ou de meilleurs algorithmes de comparaison seraient introduits dans le système. Il est vital de recourir à des pratiques favorisant l'enregistrement d'échantillons de grande qualité pour assurer la régularité de ces derniers, ainsi que pour améliorer les performances de recherche générales, ce qui s'avère tout particulièrement important pour la reconnaissance biométrique de type "identification".

1) Ici, "propriétaire" signifie que la capture et les logiciels et appareils de capture et de recherche sont inextricablement interdépendants.

Nous pouvons distinguer la “capture directe” de l’enregistrement en la définissant comme le processus visant à collecter des échantillons biométriques en direct lors d’une tentative d’accès ou d’identification, puis à les comparer à une “galerie” de modèles précédemment enregistrés.

L’extraction de modèle nécessite un traitement du signal des échantillons biométriques bruts (ex : images ou échantillons audio) afin d’obtenir un modèle numérique. Les modèles sont habituellement générés et stockés lors de l’enregistrement pour gagner du temps lors du traitement des comparaisons ultérieures. La comparaison de deux échantillons biométriques applique des calculs algorithmiques destinés à évaluer leur similarité. Lors de la comparaison, un score de correspondance est attribué. S’il est supérieur à un seuil donné, les modèles sont considérés comme identiques.

En règle générale, les algorithmes d’extraction de modèle biométrique et de comparaison sont propriétaires (différents et secrets), aussi ne peuvent-ils pas être utilisés au sein d’un même système avec ceux d’autres fournisseurs (ex : pour comparer des modèles générés par différents produits, ou pour utiliser un algorithme de recherche de correspondance d’une société afin de comparer des modèles générés par les algorithmes d’une autre société). Il existe cependant

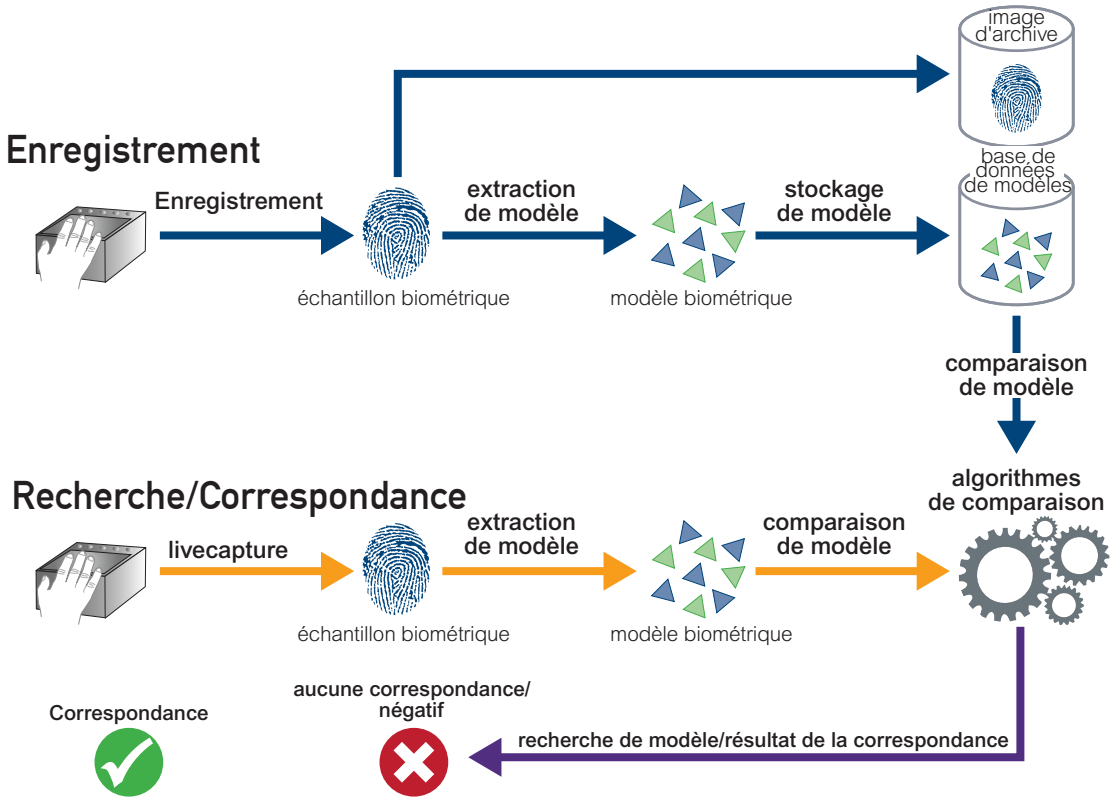

Illustration 1 – Un système biométrique

des exceptions, comme les générateurs de modèle d'empreinte digitale par point caractéristique et les algorithmes de recherche de correspondance certifiés MINEX. Les modèles et logiciels de recherche de correspondance de cette catégorie ont été conçus, testés et certifiés en toute indépendance par NIST pour être interopérables dans le cadre de vérifications biométriques, et sont donc parfaits pour un stockage compact sur des cartes à puce ou des documents de voyage.

Test de fiabilité des systèmes biométriques

La fiabilité d'un système biométrique se mesure généralement à l'aide d'une courbe "caractéristique de la performance d'un test" ou "courbe ROC" indiquant son "taux de faux positifs (FMR)" et son "taux de faux négatifs (FNMR)" par rapport à une galerie d'échantillons biométriques. Le taux de faux positifs est la fréquence à laquelle des échantillons biométriques de différentes sources sont incorrectement considérés comme originaires d'une même source. Le taux de faux négatifs est la fréquence à laquelle des échantillons d'une même source sont incorrectement considérés comme originaires de sources différentes. Un système biométrique performant se caractérise par des résultats rapides et un faible taux de faux positifs et de faux négatifs. La fiabilité d'un système est égale au point de la courbe ROC dont l'emplacement est fonction du "seuil" de correspondance appliqué. Un seuil de correspondance élevé réduit le taux de faux positifs mais augmente le taux de faux négatifs (plus de sécurité, moins de commodité). Un seuil de correspondance faible réduit le taux de faux négatifs mais augmente le taux de faux positifs (plus de commodité, moins de sécurité ; voir l'illustration 3). Un grand nombre de données (ex : plus d'empreintes digitales) et des échantillons de grande qualité (très réguliers) sont nécessaires pour les identifications, contrairement aux vérifications.

Il est important de reconnaître que la fiabilité des systèmes biométriques dépend largement de la nature des données biométriques du système. Chaque galerie de données biométriques par rapport à laquelle est effectuée une comparaison d'échantillons donnera une courbe ROC de fiabilité différente. Il existe des galeries biométriques dans le domaine public, qui servent de références afin de comparer différents algorithmes de correspondance. Cependant, les algorithmes peuvent être "entraînés" pour fonctionner plus efficacement sur des bases de données connues, ce qui revient à voir les questions d'un test avant de le passer. Leur fiabilité comparative s'en trouvera ainsi améliorée sur les bases de données connues, sans que cela indique forcément la performance du système sur des données inconnues, comme c'est le cas en situation réelle. Le meilleur moyen de prédire le comportement d'un système biométrique lors d'un déploiement en situation réelle consiste donc à tester ses performances sur des données pour lesquelles il n'a pas été expressément entraîné.

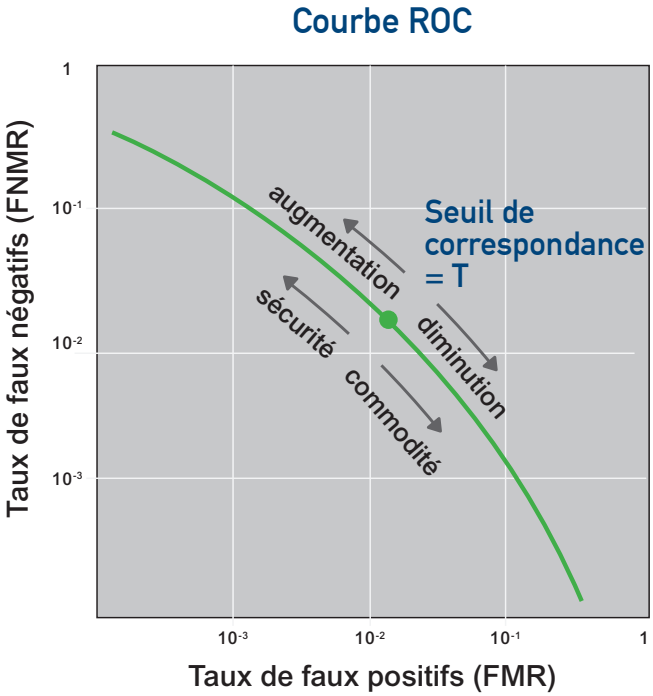

Illustration 2 - Courbe ROC pour un système de recherche de correspondance biométrique et un ensemble de données

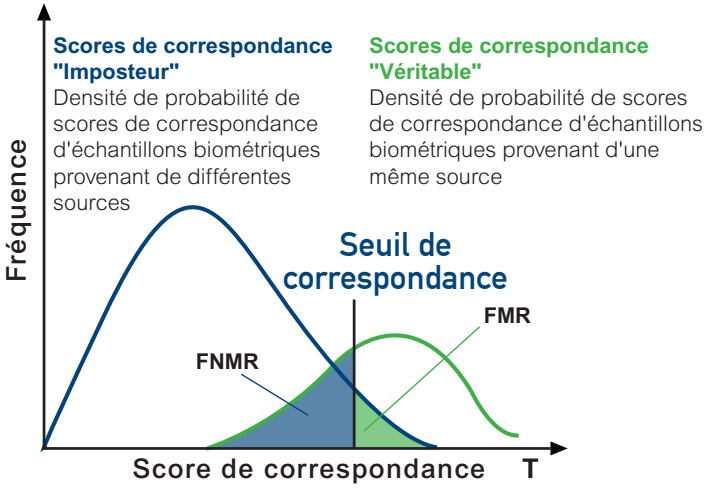

Illustration 3 – Densité de probabilité de scores de comparaison entre a) des échantillons provenant de différentes sources et b) des échantillons provenant des mêmes sources, montrant le TFP et le TFN.

Applications biométriques

Les applications biométriques peuvent se classer en trois objectifs : 1) vérification, 2) identification et 3) recherche de doublons :

La **vérification** implique d'effectuer une comparaison biométrique "un à un" pour sécuriser l'accès à une ressource physique, comme une pièce ou un bâtiment, ou à une ressource numérique, comme une application informatique ou une base de données. Pour cette application, la biométrie est utilisée un peu comme un mot de passe ou un code PIN, afin d'améliorer le contrôle de l'accès en comparant l'échantillon biométrique d'un individu à un unique échantillon fiable stocké. Cet échantillon stocké peut être hébergé dans une base de données centrale, un smartphone, ou en tant que jeton sur un identifiant comme une carte d'identité à puce. Ainsi, il est possible de vérifier la déclaration d'une personne quant à son identité, en répondant à la question : "êtes-vous la personne pour laquelle a été émis ce jeton ?" et en utilisant le résultat de la comparaison pour accorder ou refuser l'accès. L'utilisation de la biométrie afin de contrôler l'accès se révèle tout particulièrement intéressante pour les applications de sécurité commerciales ou personnelles. La vérification biométrique peut être proposée en tant qu'alternative plus pratique ou efficace à un PIN ou un mot de passe, auquel cas l'utilisateur se voit offrir la possibilité de l'utiliser, mais sans obligation s'il préfère un PIN ou un mot de passe. C'est par exemple le modèle d'utilisation de l'iPhone 5S d'Apple.

L'**identification** est un processus très différent et plus exigent (en termes d'algorithme biométrique et de performances informatiques) qui sert à déterminer si les caractéristiques biométriques d'un individu sont présentes dans une base de données, ou "galerie". Une galerie peut contenir des dizaines de millions de modèles, voire bien plus encore. Dans ce processus, les caractères biométriques d'un individu sont capturés et envoyés à un système de recherche biométrique pour une comparaison de type "un à plusieurs". Le système compare mathématiquement le modèle de l'échantillon capturé à tous les modèles de la galerie. Ainsi, les caractères biométriques permettent d'identifier un individu même s'ils ne sont pas en eux-mêmes des éléments identificateurs. C'est dans les applications du secteur public que l'identification est le plus souvent effectuée, car la fiabilité de l'identité est essentielle à la sécurité publique, notamment lors d'enquêtes criminelles et pour le maintien de l'ordre, l'émission de visas et les contrôles frontaliers, la vérification des antécédents pour le recrutement professionnel, la défense et le renseignement.

La **recherche de doublons** est un autre processus biométrique qui sert à déterminer si des individus figurent plusieurs fois dans une base de données. Elle peut être effectuée pour détecter des fraudes, par exemple dans le cas où un individu s'est enregistré plusieurs fois dans un programme de prestations sociales. Ce processus implique de comparer le modèle biométrique de chaque élément de la base de données à tous les autres, processus appelé "dédoublonnage biométrique".

Instruments et capteurs

Les instruments et les capteurs regroupent tous les systèmes mécaniques ou électroniques servant à enregistrer et capturer des échantillons biométriques bruts sous une forme pouvant être numérisée et convertie en modèle biométrique. Pour les empreintes digitales, le visage, l'iris et la voix, il s'agit respectivement des lecteurs d'empreintes digitales, des appareils photo numériques, des caméras de reconnaissance irienne et des microphones. La plupart des lecteurs d'empreintes digitales se basent sur des techniques optiques ou capacitives, mais les capteurs à luminescence et les approches multispectrales gagnent du terrain. Les lecteurs capacitifs peuvent exiger de poser le doigt ou de le faire glisser. Il est essentiel pour les performances des logiciels de comparaison que les images des empreintes digitales soient capturées à une résolution (500 ppp) et un contraste suffisants, soient correctement compressées à la norme WSQ et soient dénuées de toute distorsion. Les lecteurs optiques utilisent un prisme, une source de lumière et un capteur de lumière pour capturer l'image des empreintes digitales. Les lecteurs capacitifs comportent une puce en silicium qui détecte les courants électriques quand les crêtes digitales établissent un contact. Les lecteurs par glissement ne génèrent pas une qualité d'image suffisante pour une identification. De manière générale, la quantité et la régularité des échantillons biométriques nécessaires dépendent de la taille de la base de données qui doit être consultée.

La capture d'images faciales s'effectue à l'aide de réflex numériques, de caméras de poche et de webcams grand public. La technologie des capteurs à bas coût s'est récemment grandement améliorée, rendant possible la reconnaissance faciale biométrique à l'aide de smartphones. Les images faciales numériques nécessitent généralement une résolution interoculaire d'environ 60 pixels pour une vérification, et de 90 pixels pour une identification, plus précise. Le facteur le plus essentiel et posant le plus de difficultés concernant les

performances des logiciels de reconnaissance faciale est la régularité : obtenir une pose, un angle de tête et une expression faciale identiques du sujet, ainsi qu'une luminosité, un contraste et une netteté identiques, avec un arrière-plan dénué d'éléments indésirables.

Les capteurs biométriques de l'iris ont également bénéficié d'importantes améliorations. La reconnaissance de l'iris diffère de celle du visage dans le sens où elle nécessite une image infrarouge de l'iris afin d'optimiser le contraste de l'image et de faciliter l'analyse par la machine. C'est le degré de pureté auquel peut être capturée une image infrarouge (avec un minimum de "pollution" due à la lumière visible) qui détermine les performances de recherche de correspondance. Voilà pourquoi les appareils photo de série ne sont pas encore utilisés pour capturer des images d'iris et qu'un appareil photo spécial est nécessaire ; un système doit éclairer l'iris avec de la lumière infrarouge puis filtrer les autres longueurs d'ondes.

Les capacités audio et l'omniprésence des smartphones font de ceux-ci un moyen particulièrement efficace pour déployer des analyses biométriques vocales à grande échelle à des fins de vérification. Les analyses biométriques vocales font face aux mêmes difficultés que les analyses biométriques faciales, c'est-à-dire que l'environnement de la capture peut s'avérer aussi imprévisible et irrégulier ; comme avec les images faciales, le bruit d'arrière-plan peut interférer avec la capture et le processus de recherche de correspondance.

Modes d'utilisation et architecture système

ADans une application biométrique "à propriétaire", un seul et même individu utilise la vérification biométrique pour sécuriser l'accès à ses propres ressources, comme un smartphone. Dans un système "à autorisation", le contrôleur d'une ressource s'accorde lui-même l'accès à cette ressource (ex : une société qui utilise la biométrie pour accorder à ses employés l'accès à leurs données). Dans les applications "à opérateur", un opérateur agréé et compétent de l'instrument collecte des données biométriques auprès de l'individu fournissant l'échantillon biométrique, comme dans une application de maintien de l'ordre. Les applications "à kiosque" nécessitent que la capture soit effectuée par le sujet sans formation ni expérience et un minimum d'instructions, comme dans le contrôle frontalier automatisé.

Le ou les modèles biométriques précédemment enregistrés auxquels est comparé un échantillon capturé peuvent se trouver dans plusieurs emplacements, notamment sur un smartphone, sur un identifiant comme une puce de carte d'identité ou un code à barres imprimé, sur un instrument de capture biométrique mobile ou sur un serveur central. L'emplacement des modèles enregistrés et le lieu où est effectuée la recherche de correspondance dépendent du cas d'utilisation, des performances et de la sécurité de l'application. La vérification biométrique peut même être effectuée en totalité sur la puce d'une carte.

Vie privée

Les gouvernements collectent des informations personnelles sur leurs citoyens, généralement pour améliorer leur sécurité sociale, médicale ou physique. Tout le monde n'est pas d'accord sur la quantité d'informations personnelles qui devraient être collectées, et la biométrie tend à incarner le type d'informations personnelles que certains voudraient justement ne pas voir collectées. L'habitude qu'ont prise les autorités policières d'utiliser la biométrie comme outil de mise en détention et d'enquête criminelle renforce son association avec la privation des droits personnels. Dans certains pays, l'utilisation abusive des informations personnelles a contribué à forger une forte aversion envers leur collecte par le gouvernement. Même si, aujourd'hui, des entreprises privées possèdent, utilisent et traitent des quantités de données personnelles bien plus importantes, nous avons tendance à voir ces collectes comme plus anodines, car nous obtenons quelque chose en échange, par exemple l'utilisation de leurs produits.

Plus récemment, la prolifération d'Internet, des appareils photo numériques, des smartphones et des réseaux sociaux nous a fait entrer dans l'ère des données massives, qui apporte avec elle une disponibilité exponentielle des données personnelles et permet leur abus potentiel. Nous découvrons que, dans cette nouvelle ère, la vie privée devient un choix très personnel ; certains individus choisissent de minimiser la quantité d'informations personnelles qu'ils partagent, tandis que d'autres se "mettent à nu" avec enthousiasme. Dans tous les cas, la biométrie peut constituer un moyen plus pratique et sécurisé d'améliorer la vie privée par un meilleur contrôle de l'accès à une quantité sans cesse croissante d'informations personnelles, en particulier lorsqu'elle est utilisée en association avec d'autres mesures de sécurité traditionnelles, comme les PIN et les mots de passe.

L'abondance d'images faciales sur Internet peut inciter à en abuser en tant que données biométriques. On peut envisager que, par un processus de "résolution d'identité", les images faciales et les données qui leur sont associées (ex : nom, école, partenaires, etc.) soient liées par le biais d'une recherche de correspondance faciale biométrique à des informations d'autres sites Web et bases de données où sont stockées les images faciales. La résolution d'identité est un processus par lequel des données "cloisonnées", disparates, sont agrégées en une "identité numérique" qui présente d'une personne une vue plus complète que ce que l'on peut déduire de sources de données uniques. Dans le cas où de petites quantités éparpillées d'informations personnelles sont accessibles, chacune avec une utilisation et un public particuliers à l'esprit, l'agrégation de toutes ces données personnelles provenant de différentes sources grâce à la recherche faciale biométrique peut porter atteinte à la vie privée. Il faut noter qu'il n'existe aucune preuve claire qu'une telle opération ait jamais été mise en œuvre au point d'affecter la vie privée d'un individu. De plus, ce processus est plus traditionnellement (et peut-être plus efficacement) utilisé avec des données textuelles, aussi la menace potentielle existe-t-elle avec ou sans la présence d'images faciales. Il faut également noter que les autres modalités biométriques ne posent pas le même risque que les images faciales pour ce type de processus, car elles ne sont pas aussi abondantes dans le domaine public. Quand on évalue l'impact de la biométrie sur la vie privée, il est essentiel de la considérer dans le contexte plus vaste des données d'identification sous forme de texte et de signal ; elles comprennent les données détenues par les organismes d'État et les sociétés privées, celles accessibles sur Internet, et celles provenant d'autres sources libres.

Sécurité

Il existe très peu de cas avérés lors desquels des mesures de sécurité biométriques ont été frauduleusement contournées en situation réelle, soit pour éviter une identification, soit pour bénéficier d'un accès non autorisé. Des journalistes simulent parfois des tentatives qui sont largement médiatisées, aussi a-t-on souvent une perception disproportionnée de la menace que posent les failles de sécurité de la biométrie.

La première menace viendrait d'un individu capable de brouiller ses échantillons biométriques afin d'éviter une identification, par exemple en mutilant ses empreintes digitales ou en dilatant ses iris. Ces méthodes ne sont pas très efficaces, car elles sont facilement détectables et, dans le cas de la mutilation, irréversibles.

La deuxième menace viendrait d'un échantillon biométrique secrètement obtenu ou fabriqué par un imposteur et imité ou usurpé afin d'accéder frauduleusement aux ressources de son véritable propriétaire, de la même façon qu'avec un PIN, un mot de passe ou un identifiant volé. Cependant, si les mots de passe peuvent être modifiés et renvoyés à leur véritable utilisateur, la permanence inhérente aux caractères biométriques en empêche toute modification, aussi l'utilisation sécurisée de cette modalité biométrique dans l'avenir peut-elle se voir compromise, du moins jusqu'à ce que l'imposteur soit identifié.

L'usurpation ou le brouillage d'une donnée biométrique exige certaines compétences et un travail important, aussi ces méthodes sont-elles difficilement applicables sans être détectées. Même si cette éventualité reste possible, elle est très difficile à mettre en œuvre, peu fiable et inefficace dans les situations où la capture biométrique nécessite plusieurs échantillons, plusieurs modalités, est effectuée par un opérateur ou est associée à d'autres mécanismes de sécurité. Le développement de la "détection du caractère vivant" (ex : détection de la circulation sanguine, du clignement des yeux et des pulsations pupillaires) et d'autres techniques anti-usurpation rendent quasiment impossibles la plupart des modes de défaillance. Une autre technique consiste à émettre des données biométriques "révocables", qui sont uniquement encodés et consultées dans un domaine crypté. Elles sont sécurisées et peuvent être générées à nouveau si elles sont compromises.

Quasiment tous les mécanismes de sécurité peuvent être contournés avec certaines compétences et beaucoup de travail, et la biométrie ne fait pas exception. Il faut envisager la sécurité des mesures biométriques dans le contexte de leur application, par rapport à d'autres mécanismes de sécurité. Il est également important d'utiliser la biométrie en association avec d'autres mesures de sécurité ; aucun mécanisme de sécurité ne doit céder devant un mode de défaillance unique.

AWARE

sales@aware.com | www.aware.com