Introduction à la Biométrie

Authentification des Individus par Traitement Audio-Vidéo

An Introduction to Biometrics

Audio- and Video-Based Person Authentication

Florent Perronnin & Jean-Luc Dugelay

Institut Eurécom, Multimedia Communications Department

2229, route des Crêtes, B.P. 193, 06904 Sophia Antipolis Cedex

{perronni, dugelay}@eurecom.fr

Tél. : +33 (0)4 93 00 26 26

Fax. : +33 (0)4 93 00 26 27

URL : http://www.eurecom.fr/~image

3 juillet 2002

Résumé

La biométrie, qui consiste à identifier un individu à partir de ses caractéristiques physiques ou comportementales, connaît depuis quelques années un renouveau spectaculaire dans la communauté du traitement du signal. Elle a aussi reçu une attention accrue de la part des médias depuis les tragiques événements du 11 septembre 2001. Dans cet article nous introduisons tout d'abord la notion de biométrie. Nous décrivons l'architecture d'un système biométrique ainsi que les métriques utilisées pour évaluer leur performance. Nous donnons un bref aperçu des technologies biométriques les plus courantes et des moyens de les fusionner pour obtenir des systèmes multimodaux. Nous présentons enfin les applications possibles de la biométrie.

Mots clés: article de synthèse, biométrie, traitement du son et de l'image, sécurité, multimodalité.

Abstract

Biometrics, which refers to identifying an individual based on his/her physical or behavioral characteristics, has gained in popularity among researchers in signal processing during recent years. It has also focused the attention of medias since the tragic events of September 11th, 2001. We first introduce the notion of biometrics. Then, we describe the architecture of biometric systems and the metrics used to evaluate their performances. We briefly discuss the most common biometrics and the different ways to combine them to obtain multimodal systems. Finally, we present applications of biometrics.

Key words: overview, biometrics, audio and video processing, security, multimodality.

1 Introduction

Savoir déterminer de manière à la fois efficace et exacte l'identité d'un individu est devenu un problème critique dans notre société. En effet, bien que nous ne nous en rendions pas toujours compte, notre identité est vérifiée quotidiennement par de multiples organisations : lorsque nous utilisons notre carte bancaire, lorsque nous accédons à notre lieu de travail, lorsque nous nous connectons à un réseau informatique, etc.

Il existe traditionnellement deux manières d'identifier un individu. La première méthode est basée sur une *connaissance* (knowledge-based). Cette connaissance correspond par exemple au mot de passe utilisé au démarrage d'une session Unix ou au code qui permet d'activer un téléphone portable. La seconde méthode est basée sur une *possession* (token-based). Il peut s'agir d'une pièce d'identité, une clef, un badge, etc. Ces deux modes d'identification peuvent être utilisés de manière complémentaire afin d'obtenir une sécurité accrue comme pour la carte bleue. Cependant, elles ont leurs faiblesses respectives. Dans le premier cas, le mot de passe peut être oublié par son utilisateur ou bien deviné par une autre personne. On estime ainsi qu'une personne sur quatre écrit directement sur sa carte bleue son code secret afin de ne pas l'oublier [20]. Dans le second cas, le badge (ou la pièce d'identité ou la clef) peut être perdu ou volé.

La biométrie est une alternative aux deux précédents modes d'identification. Elle consiste à identifier une personne à partir de ses caractéristiques *physiques* ou *comportementales*. Le visage, les empreintes digitales, l'iris, etc. sont des exemples de caractéristiques physiques. La voix, l'écriture, le rythme de frappe sur un clavier, etc. sont des caractéristiques comportementales. Ces caractéristiques, qu'elles soient innées comme les empreintes digitales ou bien acquises comme la signature, sont attachées à chaque individu et ne souffrent donc pas des faiblesses des méthodes basées sur une connaissance ou une possession. En effet, un attribut physique ou

comportemental ne peut être oublié (cf. le slogan de Nuance [57] : "No PIN to remember, no PIN to forget") ou perdu. En général, ils sont très difficiles à "deviner" ou à "voler" ainsi qu'à "dupliquer" [27].

Nous décrivons maintenant les propriétés souhaitables d'une caractéristique biométrique [19]. Cette caractéristique doit être *universelle*, c'est-à-dire que toutes les personnes de la population à identifier doivent la posséder. Elle doit être à la fois facilement et quantitativement *mesurable*. Elle doit être *unique*, c'est-à-dire que deux personnes ne peuvent posséder exactement la même caractéristique. Elle doit être *permanente*, ce qui signifie qu'elle ne doit pas varier au cours du temps. Elle doit être *performante*, c'est-à-dire que l'identification doit être précise et rapide. Elle doit être bien *acceptée* par les utilisateurs du système. Enfin elle doit être *impossible à dupliquer* par un imposteur.

Le reste de l'exposé est organisé de la manière suivante. Nous décrivons tout d'abord l'architecture des systèmes biométriques (section 2) ainsi que les métriques utilisées pour évaluer leur performance (section 3). Nous donnons un bref aperçu des technologies biométriques les plus courantes (section 4) et des moyens de les fusionner pour obtenir des systèmes multimodaux (section 5). Nous présentons enfin les applications de la biométrie (section 6) avant de conclure sur son potentiel mais aussi ses dérives possibles (section 7).

2 Architecture

Il existe toujours au moins deux modules dans un système biométrique : le module d'*apprentissage* et celui de *reconnaissance* [27], [21]. Le troisième module (facultatif) est le module d'*adaptation*. Pendant l'apprentissage, le système va acquérir une ou plusieurs mesures biométriques qui serviront à construire un modèle de l'individu. Ce modèle de référence servira de point de comparaison lors de la reconnaissance. Le modèle pourra être réévalué après chaque utilisation grâce au module d'adaptation.

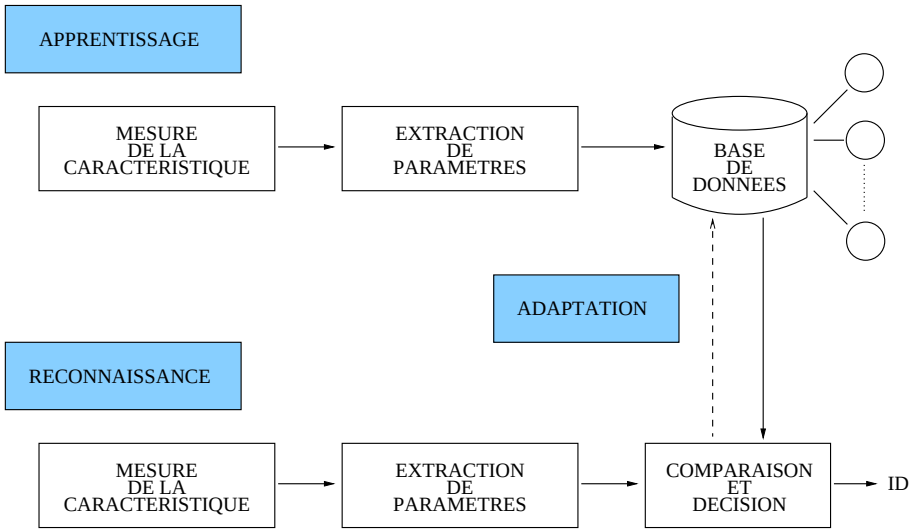

FIG. 1 – *Architecture d'un système de reconnaissance biométrique*

2.1 Module d'apprentissage

Au cours de l'apprentissage, la caractéristique biométrique est tout d'abord mesurée grâce à un capteur; on parle d'acquisition ou de *capture*. En général, cette capture n'est pas directement stockée et des transformations lui sont appliquées. En effet, le signal contient de l'information inutile à la reconnaissance et seuls les paramètres pertinents sont extraits. Le modèle est une représentation compacte du signal qui permet de faciliter la phase de reconnaissance, mais aussi de diminuer la

quantité de données à stocker. Il est à noter que la qualité du capteur peut grandement influencer les performances du système. Meilleure est la qualité du système d'acquisition, moins il y aura de pré-traitements à effectuer pour extraire les paramètres du signal. Cependant, les capteurs de qualité sont en général coûteux et leur utilisation est donc limitée à des applications de haute sécurité pour un public restreint.

Le modèle peut être stocké dans une base de données comme représenté sur la figure 1 ou sur une carte de type carte à puce.

2.2 Module de reconnaissance

Au cours de la reconnaissance, la caractéristique biométrique est mesurée et un ensemble de paramètres est extrait comme lors de l'apprentissage. Le capteur utilisé doit avoir des propriétés aussi proches que possibles du capteur utilisé durant la phase d'apprentissage. Si les deux capteurs ont des propriétés trop différentes, il faudra en général appliquer une série de pré-traitements supplémentaires pour limiter la dégradation des performances. La suite de la reconnaissance sera différente suivant le mode opératoire du système : *identification* ou *vérification*.

En mode identification, le système doit deviner l'identité de la personne. Il répond donc à une question de type : "Qui suis-je ?". Dans ce mode, le système compare le signal mesuré avec les différents modèles contenus dans la base de données (problème de type 1:n). En général, lorsque l'on parle d'identification, on suppose que le problème est *fermé*, c'est-à-dire que toute personne qui utilise le système possède un modèle dans la base de données.

En mode vérification, le système doit répondre à une question de type : "Suis-je bien la personne que je prétends être ?". L'utilisateur propose une identité au système et le système doit vérifier que l'identité de l'individu est bien celle proposée. Il suffit donc de comparer le signal avec un seul des modèles présents dans la base de

données (problème de type 1:1). En mode vérification, on parle de problème *ouvert* puisque l'on suppose qu'un individu qui n'a pas de modèle dans la base de données (*imposteur*) peut chercher à être reconnu.

Identification et vérification sont donc deux problèmes différents. L'identification peut-être une tâche redoutable lorsque la base de données contient des milliers, voire des millions d'identités, tout particulièrement lorsqu'il existe des contraintes de type "temps réel" sur le système. Ces difficultés sont analogues à celles que connaissent par exemple les systèmes d'indexation de documents multimédia.

2.3 Module d'adaptation

Pendant la phase d'apprentissage, le système biométrique ne capture souvent que quelques instances d'un même attribut afin de limiter la gêne pour l'utilisateur. Il est donc difficile de construire un modèle assez général capable de décrire toutes les variations possibles de cet attribut. De plus, les caractéristiques de cette biométrie ainsi que ses conditions d'acquisition peuvent varier. L'adaptation est donc nécessaire pour maintenir voire améliorer la performance d'un système utilisation après utilisation.

L'adaptation peut se faire en mode *supervisé* ou *non-supervisé* mais le second mode est de loin le plus utile en pratique. Si un utilisateur est identifié par le module de reconnaissance, les paramètres extraits du signal serviront alors à ré-estimer son modèle. En général, le taux d'adaptation dépend du degré de confiance du module de reconnaissance dans l'identité de l'utilisateur. Bien entendu, l'adaptation non-supervisée peut poser problème en cas d'erreurs du module de reconnaissance.

L'adaptation est quasi indispensable pour les caractéristiques non permanentes comme la voix [11] [16].

3 Evaluation de performance

La performance d'un système d'identification peut se mesurer principalement à l'aide de trois critères : sa *précision*, son *efficacité* (vitesse d'exécution) et le *volume* de données qui doit être stocké pour chaque locuteur. Nous nous concentrerons dans cette section sur le premier aspect. Comme nous l'avons vu précédemment, l'identification et la vérification sont des modes opératoires différents. Elles nécessitent donc des mesures de précision différentes que nous étudierons dans les deux sous-sections suivantes. Le lecteur pourra aussi se référer à l'article de P. Phillips et al. sur l'évaluation des systèmes biométriques [34].

3.1 Evaluation de l'identification

Le taux d'identification est la mesure la plus couramment utilisée mais il n'est pas toujours suffisant. En effet, en cas d'erreur, il peut être utile de savoir si le bon choix se trouve dans les N premiers. On trace alors le *score cumulé* (cumulative match score) qui représente la probabilité que le bon choix se trouve parmi les N premiers [35].

Dans le cas où il existe plusieurs modèles pour chaque individu dans la base de données, les mesures classiques des *système de recherche dans une base de données* (database retrieval system) peuvent être utilisées. La *précision* (precision) est le rapport entre le nombre de modèles correctement retrouvés par le système dans la base de données et le nombre total de modèles retrouvés. Le *rappel* (recall) est le rapport entre le nombre de modèles correctement retrouvés dans la base de données et le nombre total de modèles qui auraient dû être retrouvées.

3.2 Evaluation de la vérification

Lorsqu'un système fonctionne en mode vérification, celui-ci peut faire deux types d'erreurs. Il peut rejeter un utilisateur légitime et dans ce premier cas on parle de

faux rejet (false rejection). Il peut aussi accepter un imposteur et on parle dans ce second cas de *fausse acceptation* (false acceptance). La performance d'un système se mesure donc à son *taux de faux rejet* (False Rejection Rate ou FRR) et à son *taux de fausse acceptation* (False Acceptance Rate ou FAR).

La vérification est un problème de *décision* similaire à la détection d'un signal dans le bruit en *théorie de l'information* [40]. Il peut être formulé de la manière suivante. Soient H_0 l'hypothèse : "la capture C provient d'un imposteur" et H_1 l'hypothèse : "la capture C provient de l'utilisateur légitime". Il faut donc choisir l'hypothèse la plus probable. On considère que la capture C provient d'un utilisateur légitime si $P(H_1|C) > P(H_0|C)$. En appliquant la loi de Bayes on obtient :

$$\frac{P(C|H_1)P(H_1)}{P(C)} > \frac{P(C|H_0)P(H_0)}{P(C)}$$

et donc :

$$\frac{P(C|H_1)}{P(C|H_0)} > \frac{P(H_0)}{P(H_1)}$$

Le *taux de vraisemblance* (likelihood ratio) $\frac{P(C|H_1)}{P(C|H_0)}$ est comparé à un seuil θ appelé *seuil de décision*. Les valeurs $P(H_0)$ et $P(H_1)$ qui représentent respectivement la probabilité pour qu'un imposteur ou un utilisateur légitime essayent d'accéder au système sont des valeurs difficilement à estimer.

Nous avons représenté sur la figure 2 la distribution hypothétique des taux de vraisemblance qu'obtiendraient les utilisateurs légitimes et les imposteurs d'un système de vérification donné. Les FAR et FRR sont représentés en hachuré. Idéalement, le système devrait avoir des FAR et FRR égaux à zéro. Comme ce n'est jamais le cas en pratique, il faut choisir un compromis entre FAR et FRR. Plus le seuil de décision θ est bas, plus le système acceptera d'utilisateurs légitimes mais plus il acceptera aussi d'imposteurs. Inversement, plus le seuil de décision θ est élevé, plus le système rejettera d'imposteurs mais plus il rejettera aussi d'utilisateurs légitimes.

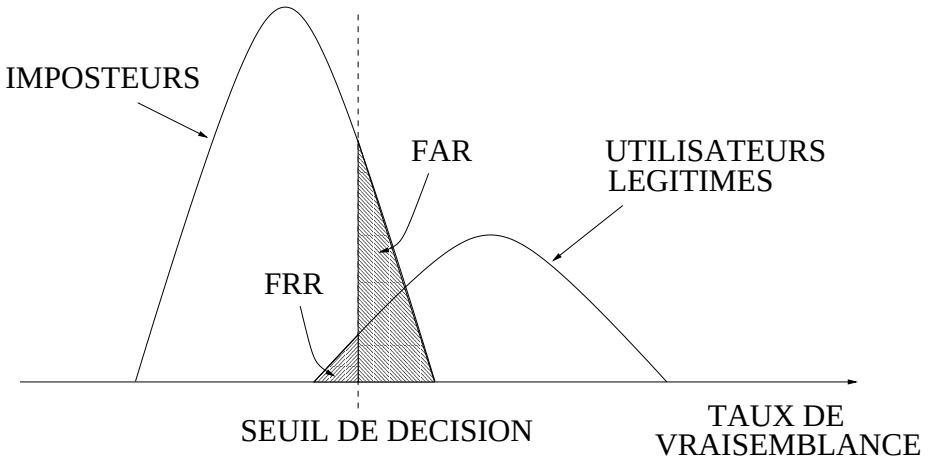

FIG. 2 – *Distributions des taux de vraisemblance des utilisateurs légitimes et des imposteurs d'un système biométrique*

Il est donc impossible en faisant varier le seuil de décision de faire diminuer les deux types d'erreurs en même temps. C'est l'une des raisons qui a motivé l'introduction de la multimodalité puisqu'il est possible de diminuer les deux types d'erreur à la fois en combinant correctement plusieurs modalités (c.f. section 5).

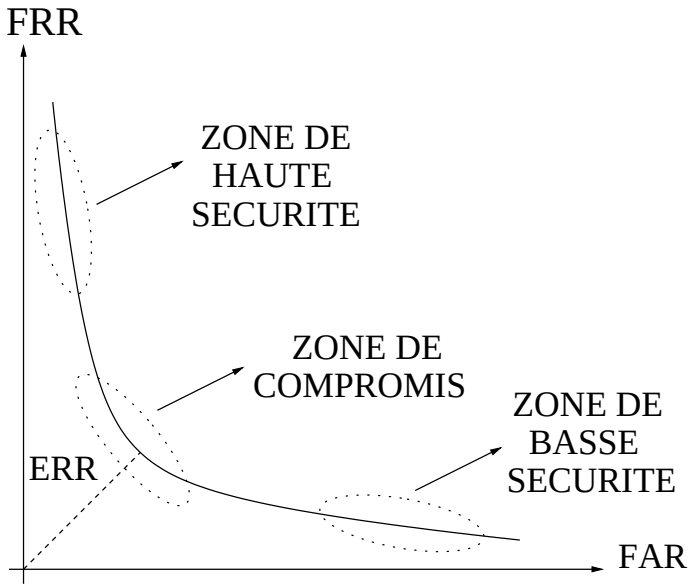

FIG. 3 – *Courbe ROC*

La courbe dite ROC (Receiver Operating Characteristic), représentée à la figure 3, permet de représenter graphiquement la performance d'un système de vérification

pour les différentes valeurs de θ [10]. Le *taux d'erreur égal* (Equal Error Rate ou EER) correspond au point $FAR = FRR$, c'est-à-dire graphiquement à l'intersection de la courbe ROC avec la première bissectrice. Il est fréquemment utilisé pour donner un aperçu de la performance d'un système. Cependant, il est important de souligner que le EER ne résume en aucun cas toutes les caractéristiques d'un système biométrique.

Le seuil θ doit donc être ajusté en fonction de l'application ciblée : haute sécurité, basse sécurité ou compromis entre les deux.

4 Panorama des différentes biométries

Nous ne donnons ici qu'un rapide aperçu des technologies biométriques les plus courantes. Pour les caractéristiques physiques, nous décrirons la reconnaissance de visage, de thermogramme facial, d'empreintes digitales, de géométrie de la main, de rétine et d'iris. Pour les caractéristiques comportementales, nous décrirons les systèmes basés sur la voix et la signature.

Il existe d'autres méthodes biométriques basées sur les veines de la main, l'A.D.N. (acide désoxyribonucléique), l'odeur corporelle, la forme de l'oreille, la forme des lèvres, le rythme de frappe sur un clavier, la démarche, etc. dont nous ne parlerons pas. Il est important de noter qu'il n'existe aucune caractéristique biométrique idéale. A chaque application correspond une ou plusieurs mesures biométriques appropriées.

4.1 Visage

Le visage est certainement la caractéristique biométrique que les humains utilisent le plus naturellement pour s'identifier entre eux, ce qui peut expliquer pourquoi elle est en général très bien acceptée par les utilisateurs. Le système d'acquisition est soit un appareil photo, soit une caméra numérique. Bien que ce ne soient pas encore des accessoires standards sur les ordinateurs personnels, de nos jours on peut acheter de petites caméras numériques de qualité correcte pour un coût raisonnable.

La difficulté de la reconnaissance de visage varie énormément suivant que l'acquisition se fait dans un environnement contrôlé ou non. Dans un environnement contrôlé, des paramètres tels que l'arrière plan, la direction et l'intensité des sources lumineuses, l'angle de la prise de vue, la distance de la caméra au sujet sont des paramètres maîtrisés par le système. Dans un environnement non-contrôlé, une série de pré-traitements sont souvent nécessaires avant de faire la reconnaissance à pro-

prement parler. Il faut tout d'abord *détecter* la présence ou l'absence de visage dans l'image (face detection). Le visage doit ensuite être segmenté (face segmentation). Enfin, si nous travaillons sur un flux vidéo, le système doit suivre le visage d'une image à l'autre (face tracking).

En 25 ans de recherche [5] [45], la performance des systèmes de reconnaissance du visage s'est grandement améliorée mais les résultats sont encore loin d'être parfaits. Les évaluations organisées par NIST (National Institute of Standards and Technology) sur la base de données FERET [33] ont montré que les systèmes sont très sensibles aux variations d'illumination et de pose. De plus, si sur une période de temps relativement courte les systèmes de reconnaissance du visage ont en général des performances acceptables, après un an, le taux de reconnaissance des mêmes systèmes peut chuter de 50%.

4.2 Thermogramme Facial

La quantité de chaleur émise par les différentes parties du visage caractérise chaque individu. Elle dépend de la localisation des veines mais aussi de l'épaisseur du squelette, la quantité de tissus, de muscles, de graisses, etc. Contrairement à la reconnaissance de visage, la chirurgie plastique n'a que peu d'influence sur les thermogrammes faciaux. Pour capturer l'image, il est possible d'utiliser un appareil photo ou une caméra numérique dans le domaine de l'infrarouge. La capture peut se faire dans n'importe quelle condition d'éclairage et même dans le noir complet ce qui est un avantage supplémentaire sur la reconnaissance de visage classique. Les thermogrammes ont certaines faiblesses communes à la reconnaissance du visage telles que la sensibilité à la pose. Elles sont aussi influencés par des facteurs tels que la température corporelle ou l'état émotionnel. Il a été avancé dans [50] que la reconnaissance des thermogrammes faciaux était la plus sûre des biométries. Cependant, dans l'état actuel de nos connaissances, aucun système n'a réussi à le

prouver.

4.3 Empreintes digitales

La reconnaissance d'empreintes digitales est la technique biométrique la plus ancienne et c'est l'une des plus matures. Cependant les empreintes digitales sont une mesure biométrique assez mal acceptée par les utilisateurs à cause de l'association qui est souvent faite avec la criminologie.

Les empreintes digitales sont formées par les *crêtes* (ridge) et les *vallées* (furrow) présentes sur la surface du bout des doigts. Les empreintes digitales ne sont pas totalement déterminées par la génétique puisque même des jumeaux monozygotes ont des empreintes différentes. Les empreintes sont différentes pour chaque doigt d'une même personne. Il existe de nombreuses méthodes d'acquisition des empreintes digitales. La plus ancienne consiste à couvrir le bout du doigt d'une fine couche d'encre et à l'imprimer sur une feuille de papier. L'empreinte ainsi imprimée peut ensuite être numérisée. Les appareils d'acquisition numériques des empreintes digitales sont basés sur la capture optique, thermique, électromagnétique ou sur les ultrasons [31].

(a) (b) (c) (d)

FIG. 4 – *(a) Arche, (b) boucle droite, (c) boucle gauche et (d) volute - Images fournies par ST Microelectronics*

Une empreinte digitale peut être caractérisée à la fois par ses propriétés *globales* et *locales*. Les crêtes dessinent au centre du doigt des motifs qui peuvent êtres classés

dans un nombre limité de catégories (4 à 6 généralement). L'information de classe représente l'information globale de l'empreinte. Quelques exemples de ces motifs sont représentés sur la figure 4. La classification n'est pas suffisante pour reconnaître une empreinte digitale. Cependant, une fois que la classe d'une empreinte a été déterminée, il suffit de la comparer avec les autres empreintes de la même classe ce qui limite le temps de recherche dans une base de données. Le lecteur pourra se référer à [6] pour un panorama des méthodes de classification.

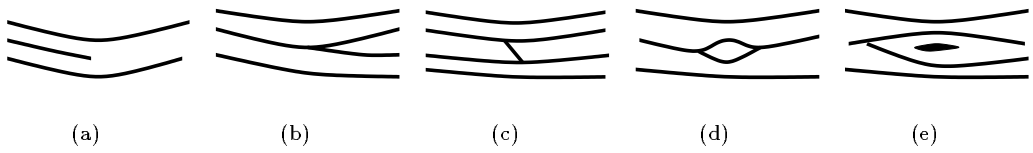

FIG. 5 – *Différents types de minuties: (a) terminaison , (b) bifurcation, (c) pont, (d) lac et (e) île*

La reconnaissance se fait à partir des propriétés locales des crêtes. Ces caractéristiques locales sont appelées *minuties* (cf. figure 5). Les deux types de minuties qui sont principalement utilisées pour la reconnaissance d'empreintes digitales sont la *terminaison* et la *bifurcation*. Les techniques de reconnaissance automatique des empreintes digitales visent en général à imiter les techniques utilisées par les experts humains. Au cours d'une première étape, les minuties et leurs caractéristiques (position, orientation) sont extraites de l'image afin de former un modèle de l'empreinte. Ce modèle est ensuite comparé aux modèles présents dans la base de données. Pour une description détaillée d'un système typique de reconnaissance d'empreintes digitales, le lecteur peut consulter [22] [23] [24].

Les variations entre deux impressions d'une même empreinte proviennent notamment de la position du doigt sur le scanner (parfois, seule une partie de l'empreinte est visible), de son orientation, de son humidité (i.e. sueur) ainsi que de la pression que l'utilisateur exerce sur le scanner et qui résulte en une déformation non

uniforme de l'empreinte. La présence de blessures temporaires ou permanentes sur les empreintes affecte aussi la performance du système. Ainsi, l'identification par empreintes digitales peut se révéler inappropriée pour certaines catégories de la population (personnes âgées, travailleurs manuels). On estime que 4% de la population n'ont pas des empreintes d'assez bonne qualité pour être correctement identifiés [39].

Comme l'a montrée l'évaluation *FVC2000* [28] [53], lorsque les systèmes de reconnaissance des empreintes digitales sont testés dans des conditions réelles, leur performance est encore loin d'être parfaite.

4.4 Rétine

La reconnaissance de la rétine est une méthode assez ancienne puisque les premières études remontent aux années 30. Les motifs formés par les veines sous la surface de la rétine sont uniques et stables dans le temps. Ils ne peuvent être affectés que par certaines maladies. Pour ces raisons, la reconnaissance de la rétine est actuellement considérée comme une des méthodes biométriques les plus sûres.

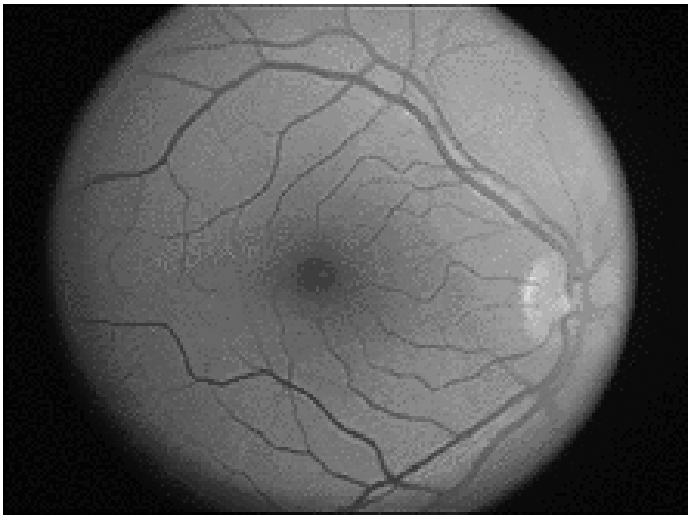

FIG. 6 – *Détail d'une rétine*

Les systèmes d'acquisition de la rétine sont coûteux. L'image est obtenue en projetant sur l'oeil un rayon lumineux de faible intensité dans les fréquences visibles

ou infrarouges. L'oeil doit être situé très près de la tête de lecture et l'utilisateur doit fixer son regard sur un point déterminé pendant plusieurs secondes ce qui demande une grande coopération de sa part. Les personnes hésitent en général à approcher un organe aussi sensible que l'oeil près de l'appareil de mesure ce qui explique pourquoi cette méthode est mal acceptée par le grand public.

4.5 Iris

La reconnaissance de l'iris est une technologie plus récente puisqu'elle ne s'est véritablement développée que dans les années 80, principalement grâce aux travaux de J. Daugman [8]. L'iris est la région annulaire située entre la pupille et le blanc de l'oeil. Les motifs de l'iris se forment au cours des deux premières années de la vie et sont stables. Les iris sont uniques et les deux iris d'un même individu sont différents. L'iris n'est pour l'instant pas modifiable par intervention chirurgicale. La reconnaissance de l'iris est donc aussi considérée comme une des méthodes biométriques les plus fiables qu'il soit.

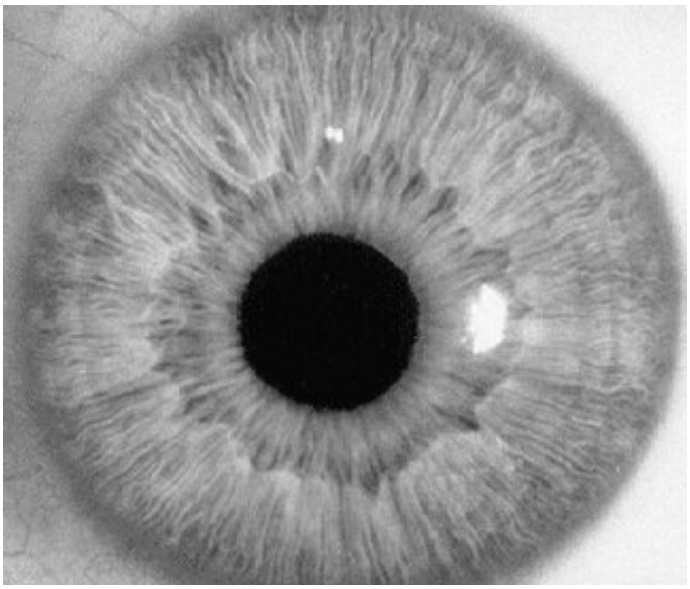

FIG. 7 – *Détail d'un iris*

La capture de l'iris se fait par une caméra standard. Du fait des contraintes sur

l'éclairage de l'oeil, le capteur doit être assez proche de celui-ci (un mètre maximum) ce qui restreint les applications d'une telle technologie. L'éclairage de l'oeil doit être uniforme et il faut éviter les reflets. Bien que la reconnaissance de l'iris soit moins contraignante que la reconnaissance de la rétine, les gens ont également du mal à accepter cette biométrie.

4.6 Géométrie de la main

Cette méthode consiste à déterminer les caractéristiques de la main d'un individu : sa forme, la longueur, la largeur, la courbure des doigts, etc. Les systèmes de reconnaissance de la géométrie de la main sont simples d'usage. L'utilisateur doit poser la paume de sa main sur une plaque qui possède des guides afin de l'aider à positionner ses doigts. Ces appareils peuvent être difficiles à utiliser pour certaines catégories de population pour lesquelles étendre la main est un problème, telles que les personnes âgées ou celles qui ont de l'arthrite. Une photo de la face de la main est ensuite prise par un appareil photo numérique. Une photo de profile peut aussi être prise pour obtenir de l'information sur l'épaisseur de la main. En raison de la taille du système de capture, ce type de technologie est limité à certaines applications. La géométrie de la main a un faible pouvoir discriminant et les systèmes peuvent être facilement trompés par de vrais jumeaux ou même par des personnes de la même famille. Le lecteur peut se rapporter à [41] pour une description détaillée d'un algorithme typique de reconnaissance de la géométrie de la main.

Il existe une alternative à la géométrie de la main : la géométrie des doigts qui s'appuie sur la forme du majeur et de l'index.

4.7 Voix

La reconnaissance du locuteur vise à déterminer les caractéristiques uniques de la voix de chaque individu. Bien que généralement classée comme caractéristique

comportementale, la voix se trouve à la frontière avec les caractéristiques physiques. En effet, un grande partie de cette caractéristique est déterminée par le conduit vocal ainsi que les cavités buccales et nasales. La voix n'est pas un attribut permanent. Elle change bien entendu avec l'âge mais peut être aussi affectée temporairement par l'état de santé ou émotionnel du locuteur. Cette biométrie est en général très bien acceptée car la voix est un signal naturel à produire. De nos jours, tous les ordinateurs sont équipés en standard d'un microphone ce qui explique la popularité de la reconnaissance du locuteur pour les applications de type "desktop".

Il existe différentes modalités de reconnaissance du locuteur :

- *texte-fixe* : le modèle du locuteur est entraîné avec un texte (un mot, une phrase) qui sera aussi utilisé au moment du test. C'est une manière indirecte de combiner reconnaissance de la voix et sécurité basée sur une connaissance car, tant qu'un imposteur ne connaît pas le mot de passe de l'utilisateur, ses chances de tromper le système sont extrêmement faibles. Cependant, si un imposteur enregistre un utilisateur, il lui suffit ensuite de repasser l'enregistrement pour tromper le système.

- *texte prompté* : ce mode évite l'écueil précédent. Pendant la phase de reconnaissance, le système prompte une ou plusieurs phrases que le locuteur doit répéter.

- *indépendant du texte* : le locuteur peut parler librement. Ce mode est utile lorsque l'on veut reconnaître un locuteur sans sa coopération. C'est ce mode que NIST a choisi pour conduire chaque année des évaluations en reconnaissance du locuteur [56] [30].

La recherche en reconnaissance du locuteur a débuté voilà plus de 20 ans et la littérature dans ce domaine est abondante. Le lecteur intéressé pourra notamment consulter [4] [12] [30] [42].

Une alternative à la reconnaissance des caractéristiques de la voix est l'analyse du choix des mots. Des travaux récents dans ce domaine [9] ont montré que les mots et expressions utilisées dépendaient fortement du locuteur.

4.8 Signature

Chaque personne possède une signature qui lui est propre et qui peut donc servir à l'identifier. Il existe deux modes de reconnaissance : le mode *statique* et le mode *dynamique*. Le mode statique n'utilise que l'information géométrique de la signature. Le mode dynamique utilise à la fois l'information géométrique et dynamique, c'est à dire les mesures de vitesse, d'accélération, etc. Le mode dynamique est plus riche en information que le mode statique et donc plus discriminant. De plus, si un imposteur veut dupliquer une signature à partir d'un exemple, il n'a pas accès à l'information dynamique. La capture se fait à l'aide d'une tablette graphique. La signature a l'avantage par rapport aux autres mesures biométriques d'être couramment utilisée pour les transactions. Pour cette raison, la signature comme moyen d'identification est en général bien acceptée. Le problème de la reconnaissance par signature provient de la très grande variabilité qui existe entre deux occurrences de la signature d'un même individu. De plus, la signature peut être affectée par l'état de santé ou émotionnel de l'individu. Pour un panorama des techniques de reconnaissance des signatures les plus classiques, le lecteur pourra se référer à [37] [38] [46].

Enfin, le lecteur trouvera des tableaux comparatifs des différentes caractéristiques biométriques précédemment décrites dans [20] et dans [27] ainsi qu'une étude comparative de divers systèmes biométriques dans [29].

5 Multimodalité

Bien que de nos jours il existe des techniques biométriques extrêmement fiables telles que la reconnaissance de la rétine ou de l'iris, elles sont coûteuses et, en général, mal acceptées par le grand public et ne peuvent donc être réservées qu'à des applications de très haute sécurité. Pour les autres applications, des techniques telles que la reconnaissance du visage ou de la voix sont très bien acceptées par les utilisateurs mais ont des performances encore trop peu satisfaisantes pour être déployées dans des conditions réelles [44].

Afin d'améliorer la sécurité des systèmes précédents, une première solution consiste à intégrer la biométrie avec l'identification basée sur une connaissance ou une possession. Cette méthode permet d'améliorer la sécurité du système, mais elle possède les faiblesses inhérentes à l'identification basée sur une connaissance ou une possession.

La multimodalité est une alternative qui permet d'améliorer de manière systématique la performance d'un système biométrique [17]. Par performance, nous entendons à la fois la précision du système mais aussi son efficacité, plus particulièrement en mode identification [26]. En effet, des classificateurs différents font en général des erreurs différentes, et il est possible de tirer parti de cette complémentarité afin d'améliorer la performance globale du système.

Nous exposerons d'abord les différentes formes de multimodalité possibles, puis les bases de données multimodales existantes, et enfin, les moyens de fusionner les informations obtenues par les différents classificateurs.

5.1 Différentes formes de multimodalité

Nous reprenons ici la classification exhaustive utilisée dans [17] et [40]. Les différentes formes de multimodalités sont les suivantes :

1. *systèmes multiples biométriques* : par exemple combiner reconnaissance du visage, reconnaissance des empreintes digitales et reconnaissance du locuteur. C'est le sens le plus classique du terme multimodal.

2. *systèmes multiples d'acquisition* : par exemple utiliser deux scanners différents (l'un optique, l'autre thermique) pour la reconnaissance d'empreintes digitales.

3. *mesures multiples d'une même unité biométrique* : par exemple faire la reconnaissance des deux iris ou des dix doigts d'un même individu.

4. *instances multiples d'une même mesure* : faire une capture répétée du même attribut biométrique avec le même système d'acquisition.

5. *algorithmes multiples* : utiliser différents algorithmes de reconnaissance sur le même signal d'entrée.

Il convient de comparer les mérites respectifs de chacune de ces formes de multimodalité. Les critères retenus sont les différences de coût, de gêne pour l'utilisateur et de quantité d'information par rapport à un système biométrique unimodal.

Le coût supplémentaire peut être séparé en coût matériel et coût logiciel. Il est clair que les deux premiers scénarios ajoutent un coût supplémentaire dans la mesure où ils nécessitent plusieurs systèmes d'acquisition. Pour le scénario (3), tout dépend si plusieurs capteurs sont utilisés pour effectuer les différentes mesures simultanément ou si un unique capteur est utilisé pour faire des mesures successives. Les scénarios (1) et (5) ont un coût logiciel supplémentaire puisqu'ils font appel à plusieurs algorithmes.

En termes de gêne pour l'utilisateur, le scénario (4) est le plus contraignant puisqu'il augmente la durée du protocole d'identification. Au contraire, le scénario (5) est le plus apprécié puisqu'il est totalement transparent pour l'utilisateur. Pour ce qui est des trois premiers scénarios, la différence sera plus ou moins importante suivant que les différentes acquisitions pourront être effectuées simultanément ou successivement.

Enfin, en termes d'apport d'information supplémentaire, le scénario (1) est le plus riche et les scénarios (4) et (5) les plus pauvres. Le scénario (3) peut aussi apporter une grande quantité d'information, car, comme nous l'avons vu, les deux iris ou les dix empreintes d'un même individu sont différents. Cependant, si l'empreinte d'un doigt d'un individu est de mauvaise qualité (parce qu'il exerce une activité manuelle par exemple), il est fort probable que les autres empreintes soient aussi de mauvaise qualité.

5.2 Bases de données multimodales

Nous n'utilisons dans ce paragraphe le terme multimodal que dans son sens le plus classique (i.e. le premier sens présenté dans 5.1). L'idée la plus simple pour créer une base de données multimodale à N modes consiste à utiliser N bases de données et à créer des individus "virtuels" en associant de manière aléatoire l'identité des différents individus des différentes bases. Par exemple, pour créer une base multimodale combinant visages et empreintes digitales, il faudra choisir une base de données $\mathcal{A}$ qui contient les visages des individus $\{A_i\}$ et une base de données $\mathcal{B}$ qui contient les empreintes digitales des individus $\{B_i\}$. Les identités "virtuelles" sont ensuite créées en associant, par exemple, le visage de A_1 avec les empreintes de B_1, le visage de A_2 avec les empreintes de B_2, etc. C'est l'idée utilisée dans [18] ou [14] par exemple.

Cependant, il n'est pas toujours possible de procéder de la sorte. Tout d'abord,

les bases de données virtuelles ne permettent pas d'étudier les éventuelles corrélations qui pourraient exister entre les différentes biométries. Ensuite, si nous voulons par exemple étudier la fusion de la reconnaissance du visage et du locuteur, nous ne pouvons pas simplement prendre une base de visages et une base de parole. En effet, si les reconnaissances du visage et du locuteur sont effectuées simultanément, l'action de parler déformera le visage. Des bases de données multimodales doivent donc être spécialement enregistrées pour prendre en compte ce type d'interactions. Les bases de données multimodales sont encore peu nombreuses dans la mesure où elles représentent un effort important pour les organismes qui les collectent. De plus, la création d'une base de données multimodales peut soulever des problèmes juridiques. Les deux principales bases à l'heure actuelle sont M2VTS [36] et XM2VTS [32]. Elles regroupent à la fois des séquences vidéos et sons synchronisées ainsi que des séquences qui permettent de voir un même visage sous plusieurs angles. La principale différence entre M2VTS et XM2VTS provient de la quantité de données collectées : dans le premier cas 37 individus avec 5 sessions par individu et dans le second 295 individus avec 8 sessions par individu.

Il est à noter qu'une nouvelle base de données multimodale est en cours de définition à l'initiative des écoles du GET [54] réunies au sein du projet Biomet.

5.3 Fusion de l'information

Comme annoncé au début de cette section, la multimodalité permet d'améliorer la performance d'un système biométrique. Dans le mot performance, nous incluons bien entendu la précision mais aussi l'efficacité du système, notamment en mode identification. Par exemple, dans [18], l'identification se fait en deux phases. La reconnaissance de visage permet d'obtenir une liste des N individus les plus probables et la reconnaissance d'empreintes digitales est ensuite restreinte à ces N individus. Dans la suite de ce paragraphe, nous nous restreindrons au premier sens du mot

performance. Notre but n'est en aucun cas de faire une présentation exhaustive des algorithmes de fusion de l'information mais de citer les plus classiques ou les plus prometteurs.

La fusion de plusieurs modalités est un problème classique de combinaison de multiples classificateurs. Elle peut se faire à trois niveaux différents : niveau *abstrait*, niveau des *rangs* ou niveau des *mesures* [3] par ordre croissant de quantité d'information disponible. Au niveau abstrait, la sortie de chaque module est une liste de labels : l'identifiant de la personne dans le cas de l'identification, la réponse binaire accepte/rejette dans le cas de la vérification. Au niveau des rangs, ces labels sont classés par ordre de confiance. Au niveau des mesures, une mesure de confiance est associée à chaque label. Ce dernier niveau permet de prendre des décisions de manière beaucoup plus fine et c'est le plus couramment utilisé. Soit $\{\omega_i\}_{i=1..N}$ l'ensemble des classes possibles entre lesquelles chaque classificateur doit faire son choix. Dans le cas de l'identification, le nombre de classes est égal au nombre d'individus présents dans la base de données (problème fermé). Dans le cas de la vérification, il n'y a que deux classes : celle des utilisateurs légitimes et celle des imposteurs. Soit $\{x_j\}_{j=1..M}$ l'ensemble des captures biométriques utilisées par les différents classificateurs.

La méthode la plus simple consiste à travailler au niveau abstrait et à fusionner les labels grâce, par exemple, à un *vote à la majorité* ou à un vote de type *K-parmi-M* [7].

Pour fusionner au niveau des rangs, les règles les plus couramment utilisées sont celles de type *maximum*, *minimum* et *médian* [26]:

$$\max_{i=1}^{N} \quad \max_{j=1}^{M} \quad P(\omega_i|x_j)$$

$$\max_{i=1}^{N} \quad \min_{j=1}^{M} \quad P(\omega_i|x_j)$$

$$\max_{i=1}^{N} \quad med_{j=1}^{M} \quad P(\omega_i|x_j)$$

Enfin, la manière la plus simple de fusionner au niveau des mesures est de moyenner les différents scores :

$$\max_{i=1}^{N} \frac{1}{M} \sum_{j=1}^{M} P(\omega_i|x_j)$$

ou bien d'utiliser une moyenne pondérée:

$$\max_{i=1}^{N} \sum_{j=1}^{M} \lambda_j P(\omega_i|x_j)$$

Les coefficients de pondération λ_i sont déterminés par minimisation de l'erreur effectuée sur la base d'apprentissage.

Une méthode extrêmement prometteuse de combinaison des classificateurs appelée *Machine à Vecteurs de Support* (Support Vector Machine ou SVM) est apparue récemment [43] et a été appliquée avec succès à la reconnaissance biométrique multimodale [2] [13] [14] [15] [25]. Cette technique d'apprentissage repose sur la minimisation du *risque structurel*, c'est-à-dire la minimisation de la borne supérieure de l'erreur en généralisation, alors que les techniques classiques visent à minimiser le *risque empirique*, c'est-à-dire le taux d'erreur sur la base d'apprentissage.

6 Applications de la biométrie

On peut distinguer quatre grands types d'applications de la biométrie : le *contrôle d'accès* (access control), l'*authentification des transactions* (transaction authentication), la *répression* (law enforcement) et la *personnalisation* (personalization).

6.1 Contrôle d'accès

Le contrôle d'accès peut être lui même subdivisé en deux sous catégories : le *contrôle d'accès physique* et le *contrôle d'accès virtuel*. On parle de contrôle d'accès physique lorsqu'un utilisateur cherche à accéder à un lieu sécurisé. On parle de contrôle d'accès virtuel dans le cas où un utilisateur cherche a accéder à une ressource ou un service.

6.1.1 Contrôle d'accès physique

Longtemps, l'accès à des lieux sécurisés (bâtiments ou salles par exemple) s'est fait à l'aide de clefs ou badges. Les badges étaient munis d'une photo et un garde était chargé de la vérification. Grâce à la biométrie, la même opération peut être effectuée automatiquement de nos jours.

L'une des utilisations les plus célèbres de la géométrie de la main pour le contrôle d'accès est le système INSPASS [55] (Immigration and Naturalization Service Passenger Accelerated Service System) déployé dans plusieurs grands aéroports américains (New-York, Washington, Los Angeles, San Francisco, etc.). Cette application permet aux passagers répertoriés dans le système d'éviter les files d'attente pour le contrôle des passeports. Ceux-ci possèdent une carte magnétique qui contient l'information sur la géométrie de leur main. Lorsqu'ils présentent leur main au système, celle-ci est comparée à l'information contenue dans la carte.

6.1.2 Contrôle d'accès virtuel

Le contrôle d'accès virtuel permet par exemple l'accès aux réseaux d'ordinateurs ou l'accès sécurisé aux sites webs. Le marché du contrôle d'accès virtuel est dominé par les systèmes basés sur une connaissance, typiquement un mot de passe. Avec la chute des prix des systèmes d'acquisition, les applications biométriques devraient connaître une popularité croissante.

Un exemple d'application est l'intégration par Apple dans son système d'exploitation MAC OS 9 d'un module de reconnaissance du locuteur [1] de manière à protéger les fichiers d'un utilisateur, tout particulièrement lorsque l'ordinateur est utilisé par plusieurs individus ce qui est de plus en plus souvent le cas.

6.2 Authentification des transactions

L'authentification des transactions représente un marché gigantesque puisqu'il englobe aussi bien le retrait d'argent au guichet des banques, les paiements par cartes bancaires, les transferts de fond, les paiements effectués à distance par téléphone ou sur internet, etc.

Mastercard estime ainsi que les utilisations frauduleuses de cartes de crédit pourraient être réduites de 80% en utilisant des cartes à puce qui incorporeraient la reconnaissance des empreintes digitales [49]. Les 20% restant seraient principalement dû aux paiements à distance pour lesquelles il existerait toujours un risque. Pour les transactions à distance, des solutions sont déjà déployées en particulier pour les transactions par téléphone. Ainsi, la technologie de reconnaissance du locuteur de *Nuance* (Nuance Verifier^{TM} [57]) est utilisée par les clients du *Home Shopping Network* et de *Charles Schwab*.

6.3 Répression

Une des applications les plus immédiates de la biométrie à la répression est la criminologie. La reconnaissance d'empreintes digitales en est l'exemple le plus connu. Elle fut acceptée dès le début du XX^e siècle comme moyen d'identifier formellement un individu et son utilisation s'est rapidement répandue.

Il existe aussi des applications dans le domaine judiciaire. T-Netix [60] propose ainsi des solutions pour le suivi des individus en liberté surveillée en combinant technologies de l'internet et de reconnaissance du locuteur.

6.4 Personnalisation

Les technologies biométriques peuvent être aussi utilisées afin de personnaliser les appareils que nous utilisons tous les jours. Cette application de la biométrie apporte un plus grand confort d'utilisation.

Afin de personnaliser les réglages de sa voiture, Siemens propose par exemple d'utiliser la reconnaissance des empreintes digitales [59]. Une fois l'utilisateur identifié, la voiture ajuste automatiquement les sièges, les rétroviseurs, la climatisation, etc.

7 Conclusion

Comme le fait remarquer Bill Spence de Recognition Systems Inc. [58] : "Chaque fois que vous utilisez votre clef, vous vous identifiez auprès de votre maison. Chaque fois que vous utilisez votre carte de crédit, chaque fois que vous vous connectez à un système, vous vous identifiez." [51]. A terme, tous les mots de passe, codes confidentiels, badges, clefs, etc. seront amenés à être remplacés par des systèmes biométriques. La recherche en biométrie est donc un domaine à très fort potentiel.

Cependant, nombreuses sont les personnes qui craignent que l'essor de la biométrie ne s'accompagne d'une atteinte généralisée à la vie privée des individus. Tout d'abord le manque de fiabilité des systèmes biométriques inquiète. Après les attentats du 11 Septembre 2001, beaucoup ont vu dans la biométrie, et plus précisément dans la reconnaissance de visages, le meilleur moyen de surveiller les lieux publics tels que les aéroports [47]. Mais supposons, par exemple, que le système FaceIt de Visionics [61], l'un des systèmes de reconnaissance du visage les plus populaires à l'heure actuelle, soit déployé dans le Hartsfield Atlanta International Airport (ATL), premier aéroport au monde en termes de passagers. Sachant que, d'une part, selon les chiffres fournis par Visionics, le EER de FaceIt est de 0.68% et que, d'autre part, le Airports Council International [52] estime à 80 millions le nombre de passagers de ATL en 2000, un rapide calcul aboutit à une moyenne de 1500 personnes "rejetées" à tort quotidiennement et à plus d'un demi million de personnes par an! Même si aujourd'hui les passagers sont prêts à faire des concessions pour garantir leur sécurité, ils accepteront sans doute très mal ces erreurs à répétition. Et bien que des progrès constants soient enregistrés séparément pour chaque modalité, la performance des systèmes à un seul mode est encore loin d'être satisfaisante ce qui plaide en faveur du développement de systèmes biométriques multimodaux.

Un problème très différent est le stockage de données personnelles dans des bases

de données biométriques et l'utilisation malveillante qui pourrait en être faite. La meilleure solution à ce problème est d'abandonner l'idée d'une base de données centralisée au profit des cartes de type carte à puce dont l'utilisateur resterait possesseur [48]. Conscient de l'enjeu que représentent les libertés individuelles, c'est d'ailleurs l'un des arguments qu'utilise Mastercard pour promouvoir sa carte à puce intelligente ("We will not have a database of fingerprints anywhere." [49]).

Quoi qu'il en soit, la biométrie peut apporter beaucoup dans la vie quotidienne en termes de sécurité mais également de confort. Comme pour d'autres "nouvelles technologies" (biotechnologie, réalité virtuelle, etc.) son essor devra s'accompagner d'une réflexion approfondie sur le respect des libertés individuelles.

Références

[1] J. BELLEGARDA, D. NAIK, M. NEERACHER, K. SILVERMAN, "Language-Independent, Short Enrollment Voice Verification over a Far-Field Microphone", ICASSP, Vo. 1, p.445-448, Salt Lake City, Utah, 7-11 Mai 2001.

[2] S. BEN-YACOUB, Y. ABDELJAOUED, E. MAYORAZ, "Fusion of Face and Speech Data for Person Identity Verification", IDIAP Research Report 99-03

[3] R. BRUNELLI, D. FALAVIGNA, "Person Identification Using Multiple Cues", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vo. 17, No. 10, p. 955-966, Octobre 1995.

[4] J. P. CAMPBELL, "Speaker Recognition: A Tutorial", Proceedings of the IEEE, Vol. 85, No. 9, p. 1437-1462, Septembre 1997

[5] R. CHELLAPPA, C. WILSON, S. SIROHEY, "Human and Machine Recognition of Faces: A Survey", Proceedings of IEEE, Vo. 83, p.705-740, Mai 1995.

[6] L. CHUNG ERN, G. SULONG, "Fingerprint Classification Approaches", International Symposiom on Signal Processing and its Applications, Vo. 1, p.347-350, Kuala Lumpur, Malaisie, 13-16 Août 2001

[7] B. V. DASARATHY, "Decision Fusion", IEEE Computer Society Press, 1994

[8] J. DAUGMAN, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vo. 15, p. 1148-1161, 1993

[9] G. DODDINGTON, "Speaker Recognition Based on Idiolectal Differences between Speakers", Eurospeech, Vo. 4, p. 2521-2524, Aalborg, Danemark, 3-7 Septembre 2001

[10] J. EGAN, "Signal Detection Theory and ROC Analysis", Academic Press, New-York, 1975

[11] C. FREDOUILLE, J. MARIETHOZ, C. JABOULET, J. HENNEBERT, J.-F. BONASTRE, C. MOKBEL, F. BIMBOT, "Behavior of a Bayesian Adaptation Method for Incremental Enrollment in Speaker Verification", International Conference on Acoustics, Speech, and Signal Processing, p. 1197-1200, Istanbul, Turquie, 5-9 Juin 2000

[12] S. FURUI, "Recent Advances in Speaker Recognition", Proceedings of the First International Conference on Audio- and Video-based Biometric Person Authentication, AVBPA-97, p237-251, 1997

[13] M. FUENTES, S. GARCIA-SALICETTI, B. DORIZZI, "On-Line Signature Verification: Fusion of a Hidden Markov model and a Neural Network via a Support Vector Machine", à paraître dans IWFHR 8, Canada, Août 2002

[14] M. FUENTES, D. MOSTEFA, J. KHARROUBI, S. GARCIA-SALICETTI, B. DORIZZI, G. CHOLLET, "Vérification de l'Identité par Fusion de Données Biométriques: Signatures En-Ligne et Parole", soumis à la Conférence Internationale Francophone sur l'Ecrit et le Document, CIFED'02, 2002

[15] B. GUTSCHOVEN, P. VERLINDE, "Multimodal Identity Verification Using Support Vector Machine", Fusion'2000, Paris

[16] L. HECK, N. MIRGHAFORI, "On-Line Unsupervised Adaptation in Speaker Verification", International Conference on Spoken Language Processing, Vo. 2, p. 454-457, Pékin, Chine, 16-20 Octobre 2000

[17] L. HONG, A. JAIN, S. PANKANTI, "Can Multibiometrics Improve Performance?", Proceedings AutoID'99, Summit, NJ, Oct 1999, p.59-64

[18] L. HONG, A. JAIN, "Integrating Faces and Fingerprints for Personal Identification", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 20, No. 12, p1295-1307, 1998

[19] L. HONG, "Automatic Personal Identification Using Fingerprints", Thèse de Doctorat, Michigan State University, 1998

[20] A. JAIN, R. BOLLE, S. PANKANTI, "Biometrics: Personal Identification in Networked Society", Kluwer, New York, 1998

[21] A. JAIN, L. HONG, S. PANKANTI, "Biometrics: Promising Frontiers for Emerging Identification Market", Communications of the ACM, Feb 2000, p. 91-98

[22] A. JAIN, S. PANKANTI, "Fingerprint Classification and Recognition", The Image and Video Processsing Handbook, Academic Press, Avril 2000

[23] A. JAIN, S. PANKANTI, "Advances in Fingerprint Technology", 2nde édition, Elsevier Science, New York, 2001

[24] A. JAIN, S. PANKANTI, "Automated Fingerprint Identification and Imaging Systems", Advances in Fingerprint Technology, 2nde édition, Elsevier Science, New-York, 2001

[25] J. KHARROUBI, D. PETROVSKA-DELACRETAZ, G. CHOLLET, *et al.*, "Combining GMMs with Support Vector Machines for Speaker Verification", Eurospeech, p. 1761-1764, 2001

[26] J. KITTLER, M. HATEF, R. DUIN, J. MATAS, "On Combining Classifiers", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vo. 20, No. 3, p. 226-239, 1998

[27] S. LIU, M. SILVERMAN, "A Practical Guide to Biometric Security Technology", IEEE Computer Society, IT Pro - Security, Janvier-Février 2001

[28] D. MAIO, D. MALTONI, R. CAPPELLI, J.L. WAYMAN A.K. JAIN, FVC2000: fingerprint verification competition, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, No. 3, p. 402-412, Mars 2002

[29] T. MANSFIELD, G. KELLY, D. CHANDLER, J. KANE, "Biometrics Product Testing: Final Report", Issue 1.0, 19 Mars 2001
http://www.cesg.gov.uk/technology/biometrics

[30] A. MARTIN, M. PRZYBOCKI, G. DODDINGTON, D. REYNOLDS, "The NIST Speaker Recognition Evaluation - Overview, Methodology, Systems, Results, Perspectives (1998)", Speech Communications 31, p. 225-254, 2000

[31] P. MEENEN, R. ADHAMI, "Fingerprinting for Security", IEEE potentials, Vol. 20, No. 3, p. 33-38, Août-Septembre 2001

[32] K. MESSER, J. MATAS, J. KITTLER, J. LUETTIN, G. MAITRE, "XM2VTSDB: The Extended M2VTS Database", 2nd International Conference on Audio- and Video-Based Person Authentication, Mars 1999

[33] P. PHILLIPS, H. WECHSLER, J. HUANG, P. RAUSS, "The FERET Database and Evaluation Procedure for Face Recognition Algorithms", Image and Vision Computing, Vo. 16, p. 295-306, 1998

[34] P. PHILIPS, A. MARTIN, C. WILSON, M. PRZYBOCKI, "An Introduction to Evaluating Biometric Systems", Computer, Vo. 33, No. 2, p. 56-63, Février 2000

[35] P. PHILLIPS, H. HYEONJOON, S. RIZVI, P. RAUSS, "The FERET Evaluation Methodology for Face-Recognition Algorithms", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vo. 22, No. 10, Octobre 2000

[36] S. PIGEON, L. VANDENDORPE, "The M2VTS multimodal Face Database", Lecture Notes in Computer Science: Audio- and Video-Based Biometrics Per-

son Authentication (J. Bigun, G. Chollet and G. Borgefors Eds.), Vo. 1206, p. 403-409, 1997

[37] R. PLAMONDON, G. LORETTE, "Automatic Signature Verification and Written Identification: The State of the Art", Pattern Recognition, Vol. 22, p. 107-131, 1989

[38] R. PLAMONDON, G. LORETTE, "Automatic Signature Verification and Written Identification: The State of the Art (1989-1993)", Progress in Automatic Signature Verification, édité par R. Plamondon, World Scientific, p. 3-19, 1994

[39] S. PRABHAKAR, "Fingerprint Classification and Matching Using a Filterbank", Thèse de Doctorat, Michigan State University, 2001

[40] S. PRABHAKAR, A. JAIN, "Decision-Level Fusion in Biometric Verification", Pattern Recognition, Vol. 35, No. 4, 2002, p. 861-874

[41] R. SANCHEZ-REILLO, C. SANCHEZ-AVILA, A. GONZALEZ-MARCOS, "Biometric Identification through Hand Geometry Measurements", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 22, No. 10, Octobre 2000, p. 1168-1171

[42] D. REYNOLDS, "An Overview of Automatic Speaker Recognition Technology", International Conference on Acoustic, Speech and Signal Processing, ICASSP 2002, Vol. 4, p. 4072-4075, 13-17 Mai 2002, Orlando, Floride

[43] V. VAPNIK, "The Nature of Statistical Learning Theory", Statistics for Engineering and Information Science, Second Edition, Springer, 1999

[44] P. VERLINDE, "Une Contribution à la Vérification Multimodale de l'Identité en Utilisant la Fusion de Décision", Ecole Nationale Supérieure des Télécommunications, Paris, France, Septembre 1999

[45] W. ZHAO, R. CHELLAPPA, A. ROSENFELD, P. PHILLIPS, "Face Recognition: A Literature Survey", UMD CAR-TR-948, 2000

[46] "A Review of Dynamic Handwritten Signature Verification", James Cook University, Computer Science Department, Technical Article, 1997

[47] "Focusing on biometrics at Comdex", CNN.com/SCI-TECH, 15 Novembre 2001, http://www.cnn.com/2001/TECH/ptech/11/15/comdex.biometric

[48] "Identifiez Vous au Doigt et à l'Oeil", Courrier Cadres, No. 1412, 20 Septembre 2001

[49] "Biometrics Comes To Life", Banking Journal, Janvier 1997
http://www.banking.com/aba/cover_0197.htm

[50] "Using Biometrics for Improved Security", Unisys, European Security Centre of Excellence, http://www.unisys.com/security/default.asp

[51] "The Price of Biometrics", USA Today, 26 Janvier 1999
http://www.usatoday.com/life/cyber/tech/ctc448.htm

[52] Airports Council International, http://www.airports.org

[53] Fingerprint Verification Competition, http://bias.csr.unibo.it/fvc2000

[54] Groupement des Ecoles des Télécommunications, http://get-telecom.fr

[55] INSPASS, http://www.ins.usdoj.gov/graphics/howdoi/inspass.htm

[56] NIST Speaker Recognition Evaluations, http://www.nist.gov/speech/tests/spk

[57] Nuance, http://www.nuance.com

[58] Recognition Systems Inc., http://www.recogsys.com

[59] Siemens Automotive, http://media.siemensauto.com

[60] T-NETIX Inc., http://www.t-netix.com

[61] Visionics, http://www.visionics.com

Florent Perronnin

Ingénieur diplômé de l'Ecole Nationale Supérieure des Télécommunications de Paris, anciennement ingénieur de recherche au Panasonic Speech Technology Laboratory (Santa Barbara, Californie) Florent Perronnin est actuellement doctorant au sein du département Communications Multimédia de l'Institut Eurécom. Son sujet de thèse porte sur l'indexation d'images appliquée à la biométrie et principalement à la reconnaissance de visages et d'empreintes digitales.

Jean-Luc Dugelay

Docteur en informatique (Rennes, 1992), Jean-Luc Dugelay est actuellement professeur à l'Institut Eurécom (Sophia-Antipolis) au sein du département Communications Multimédia et chercheur invité à l'Université de Californie, Santa Barbara. Ses domaines de recherche se concentrent en imagerie multimédia sur la sécurité (tatouage et biométrie) et la réalité virtuelle (visages parlants). Membre du comité scientifique de l'IEEE Multimédia, il est éditeur associé de plusieurs revues

nationales et internationales dont *IEEE Transactions on Image Processing*. Il a co-organisé et présidé la session spéciale de ICASSP 2002 (Orlando, Floride) intitulée "Multimodal Person Authentication".