
# L'air de rien
# N° 8

L'aléastriel du **L**aboratoire de **R**echerche et de **D**éveloppement de l'**E**PITA[1] Numéro 8, Mars 2007

# Édito

par *Réda Dehak*

Ce premier numéro de l'année 2007 est consacré à la biométrie, un domaine qui connaît un grand succès en ce moment. On vous donne un aperçu des activités du laboratoire dans ce domaine, et un avant-goût de ce que vous pourrez suivre durant les prochains séminaires du LRDE.

En espérant que ce domaine vous intéresse, bonne lecture…

# Biométrie — Introduction

par *Réda Dehak*

Il suffit de regarder le nombre important et croissant de fraudes dans le domaine bancaire (chèques, carte bleue, ...) et dans les transactions commerciales sur Internet ainsi que les vols de téléphones portables pour connaître l'importance des applications d'authentification de l'identité d'une personne. Il existe plusieurs possibilités pour identifier une personne, on peut citer la possibilité d'utiliser des badges ou cartes magnétiques, des mots de passe et tout particulièrement l'information biométrique (empreinte digitale, iris, visage, main, parole, signature, ...). Du fait des performances obtenues par certaines modalités biométriques (iris, empreinte digitale) et la difficulté de falsifier ces informations, on a remarqué une nette augmentation des systèmes de sécurité basés sur l'identité biométrique durant ces dernières années.

Les caractéristiques biométriques peuvent être regroupées selon leur variabilité dans le temps en deux groupes :

**Statique ou morphologique** Cette classe regroupe les biométries invariantes au cours du temps pour un individu, elle représente essentiellement les caractéristiques morphologiques du corps humain. On peut citer par exemple l'iris, les empreintes digitales, les empreintes palmaires, le visage…

**Dynamique ou comportementale** Cette classe regroupe les biométries qui présentent une grande variation avec le temps, on peut citer par exemple : signature, frappe au clavier, démarche, voix…

# Biométrie I — « Parle, je te dirai qui tu es »

par *Réda Dehak*

Aujourd'hui l'authentification par la voix joue un rôle primordial dans toutes les transactions téléphoniques et les applications de renseignements comme les écoutes téléphoniques. À l'heure actuelle, les systèmes d'authentification par la voix n'ont pas encore atteint les performances des systèmes à base d'empreinte digitale et de l'iris. Pour cette raison, l'authentification vocale ne constitue pas une preuve tangible dans le système judiciaire.

## NIST-SRE

Dans le but de dynamiser les groupes de recherche sur la vérification du locuteur, le National Institute of Standards and Technology (NIST[2]) organise régulièrement des campagnes d'évaluation des systèmes de vérification du locuteur (NIST-SRE). Cet organisme s'occupe de la collecte des données (des écoutes téléphoniques en plusieurs langues) et les

[1] L'air de rien, http://publis.lrde.epita.fr/LrdeBulletin.
[2] NIST, http://www.nist.gov.

fournit gratuitement aux participants.

L'évaluation des systèmes est effectuée sur différentes tâches, dont une est obligatoire pour l'ensemble des participants. Ces tâches diffèrent au niveau de la durée de temps de parole pour le segment d'apprentissage (modèle client) et le segment de test. Chaque système doit fournir un score de confiance associé au fait que l'enregistrement test correspond bien au modèle client. Plus le score est élevé, plus le système est sûr de la correspondance des deux segments. Les systèmes doivent aussi prendre une décision, accepter ou refuser l'hypothèse que le segment test correspond à l'identité du segment client. Cette décision est prise en appliquant un seuil au score obtenu auparavant. Chaque tâche est décomposée en deux parties, la première concerne les voix d'homme et l'autre les voix de femme.

Les performances du système sont estimées à partir des erreurs commises, à savoir le taux de Fausse Acceptation ($P_{FA}$), correspondant à l'acceptation à tort d'un imposteur, et le taux de Faux Rejet ($P_{FR}$), correspondant au rejet à tort du locuteur correspondant à l'identité proclamée (client).

$$P_{FA} = \frac{\text{Nombre d'imposteurs acceptés}}{\text{Nombre d'accès imposteurs}}$$

$$P_{FR} = \frac{\text{Nombre de clients rejetés}}{\text{Nombre d'accès client}}$$

On calcule ces deux taux d'erreurs pour chaque valeur du seuil. Ce seuil permet de régler les performances de chaque système. Le taux de faux rejet est proportionnel au seuil appliqué, plus le seuil est élevé plus le taux de faux rejet sera important. Concernant le taux de fausse acceptation, il est inversement proportionnel au seuil, plus le seuil est élevé, plus le taux de fausse acceptation est faible. En conséquence, il est impossible de réduire les deux taux en même temps en jouant uniquement sur la valeur du seuil.

Dans le cadre d'une application réelle, cette valeur sera fixée pour une valeur minimale d'une fonction coût (DCF, *Decision Cost Function*). Du fait des conséquences liées aux fausses acceptations, on préfère, en général, rejeter un client qu'accepter un imposteur. Le coût associé au taux de fausse acceptation $C_{FA}$ sera donc plus élevé que le coût associé au taux de faux rejet $C_{FR}$. La fonction coût s'exprime sous la forme suivante :

$$DCF = C_{FR}\, P(Client)\, P_{FR} + C_{FA}\, P(Imposteur)\, P_{FA}$$

où : $P(Client)$ et $P(Imposteur)$ représente respectivement la probabilité des clients et imposteurs.

Une autre mesure de performance largement utilisée dans ce domaine est l'*Equal Error Rate* (EER), où les deux taux d'erreurs sont identiques $P_{FA} = P_{FR}$.

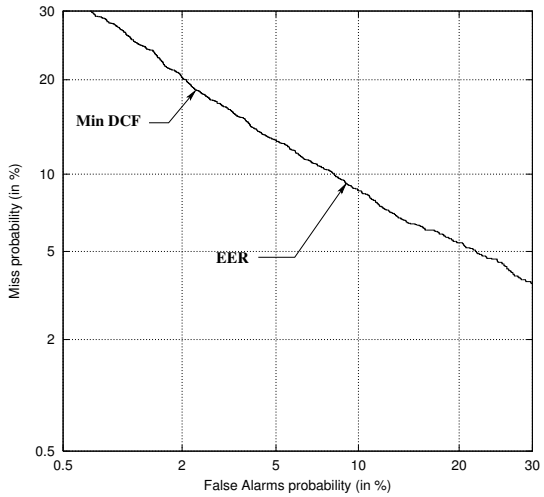


FIG. 1 – Courbe DET ; DCF, EER

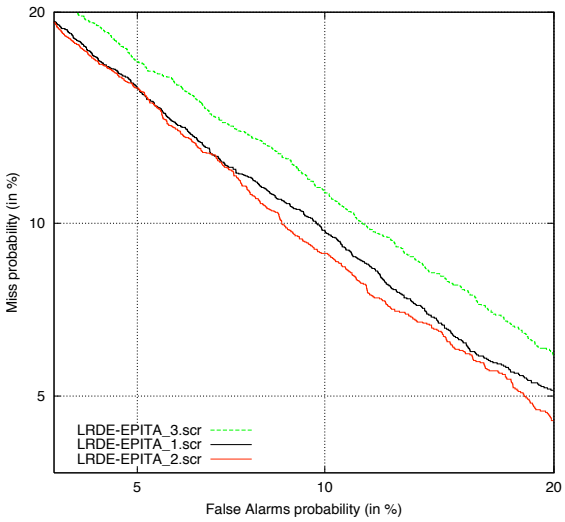


FIG. 2 – La courbe DET des trois systèmes soumis par le LRDE à la campagne NIST-SRE 2006

La courbe DET (*Detection Error Tradeoff curve*) représentant le taux de faux rejet en fonction du taux de fausse acceptation permet d'avoir une comparaison globale des systèmes pour chaque valeur du seuil (voir figure 1).

## LRDE – NIST-SRE 2006

*Avant tout, je tiens à remercier au nom du* LRDE, *l'école et tout particulièrement le bocal de nous avoir prêté dix machines pour participer à cette campagne NIST-SRE06*

Le LRDE a participé pour la première fois et en collaboration avec l'ENST et l'Université de Fribourg à la campagne NIST-SRE 2006. Nous avons soumis trois systèmes différents. Le premier (système de base) est basé sur les méthodes de l'état de l'art en matière de vérification du locuteur. Ces systèmes utilisent des modèles de mélange de gaussiennes

(GMM) pour représenter la distribution des paramètres acoustiques. La procédure de test consiste en une mesure de vraisemblance entre le signal test et le modèle (GMM) du client. Les deux autres systèmes sont fondés sur les classifieurs SVM (*Support Vector Machine*) (cf. *L'air de rien 1.0*) pour distinguer les modèles clients des modèles imposteurs. Les courbes DET des trois systèmes sont données dans la figure 2.

Pour ne pas occuper le reste des pages de ce numéro, je vous invite à lire les prochaines publications du bulletin pour connaître les détails de ces systèmes et comment construire un système de vérification du locuteur.

# Biométrie II — Identification grâce à la géométrie de la main ; Le système de référence BIOSECURE

par *Geoffroy Fouquier*

Depuis 2004, le réseau d'excellence européen BIOSECURE (pour « Biometrics for secure authentication » ; http://biosecure.info) vise à fédérer les efforts européens de recherche sur le thème de la biométrie : états de l'art des méthodes et des données, dissémination de l'information, création de nouvelles bases de données biométriques, écriture de logiciels de référence libres et des protocoles permettant la comparaison des différentes approches, organisation d'ateliers de travail.

En collaboration avec Telecom Paris, l'Université Bogaziçi d'Istanbul, l'EPITA a pris part aux activités de la modalité « main ». Le système de référence GET-EPITA de vérification et d'identification par la géométrie de la main est issu de cette collaboration. Ce système compose, avec le système de Bogaziçi portant sur l'apparence de la main, le système complet de la modalité « main ».

*Pourquoi utiliser la main alors que d'autres modalités peuvent donner de meilleures résultats, tel que l'iris ou les empreintes digitales ?* Les systèmes de reconnaissance de la main sont très simples à utiliser ; il suffit en général de poser sa main quelques secondes, au contraire des systèmes à empreintes digitales ou le positionnement peut-être difficile à obtenir. De plus, les méthodes utilisées sont non intrusives, ce qui n'est pas le cas de la reconnaissance de l'iris qui utilise souvent un laser pour photographier l'iris. Enfin, ces systèmes ne sont pas chers ni difficiles à mettre en place (un scanner suffit) et les informations à conserver sont légères par rapport à d'autres modalités comme la vidéo. Mais surtout, les systèmes de reconnaissance de la main ont montré qu'ils pouvaient obtenir des très bons taux de reconnaissance.

*La géométrie de la main, c'est quoi en pratique ?* Comme dans toutes les modalités, nous devons trouver des caractéristiques qui nous permettent de décrire au mieux un utilisateur (et donc de reconnaître toutes les images de sa main) et de le discriminer au mieux des autres utilisateurs. De multiples mesures sont possibles ; le positionnement et les écarts entre les points situés sur les articulations ou le bout des doigts sont souvent utilisés par exemple. Dans notre système, nous avons choisi une mesure un peu plus complexe : sur chaque doigt, nous parcourons le contour du doigt et nous mesurons l'écart du point du contour par rapport à un axe médian du doigt, ce qui nous fournit une série de valeurs dont nous calculons l'histogramme, qui est ensuite normalisé afin de produire une densité de probabilité.

*Et c'est suffisant ?* Cette mesure a des avantages et des inconvénients, et sa stabilité dans le temps peut être sujette à caution (les doigts peuvent grossir ou inversement). Mais la difficulté majeure n'est pas là : pour obtenir cette mesure, ou une autre, il est d'abord nécessaire de segmenter la main du fond de l'image afin d'obtenir sa silhouette, or cette tâche n'est pas triviale. Tout d'abord, aucune contrainte n'est imposée à l'utilisateur : il peut tourner sa main à 180 degrés par exemple. Ensuite, il est possible qu'un utilisateur porte des bijoux (ce qui, après binarisation, peut « couper » un doigt), ou encore la manche de son vêtement peut remonter sur son poignet. De plus, avec un scanner, la main peut-être plus ou moins appuyée, ce qui modifie le contour. Les conditions d'illumination peuvent également être variables.

*La base de données de test.* Celle du consortium biosecure, composée par les trois équipes de la modalité, comporte plus de 4500 images de mains droites et gauches pour 750 utilisateurs. Elle comporte un sous-ensemble avec de la variabilité temporelle ainsi qu'un sous-ensemble d'images à haute résolution. Les protocoles de test permettent de tester l'influence de chacun des paramètres du système : influence de la taille de la base considérée, du nombre d'images utilisées pour l'enregistrement des utilisateurs, de la résolution des images, que ce soit en réduisant (de 150ppp vers 30ppp), ou en augmentant (400ppp et 600ppp). Nous pouvons également tester la reconnaissance en utilisant la main droite et la main gauche (l'utilisateur doit alors enregistrer deux images).

*Les critères d'évaluation.* Il existe deux tâches distinctes possibles dans tout système biométrique : **la**

**vérification** (je prétends être untel, le système doit confirmer ou non) et **l'identification** (le système doit trouver qui je suis parmi sa base d'utilisateurs enregistrés). Pour la vérification, vous pouvez vous reporter à l'article de Réda Dehak sur NIST-SRE. Pour l'identification, la mesure est plus intuitive, car il s'agit tout simplement du taux de reconnaissance, c'est à dire le nombre d'utilisateurs reconnus par rapport au nombre d'utilisateurs testés.

Avec ce système de reconnaissance, le système de Bogaziçi, la base de données biosecure et les protocoles mis en place, tout ceci étant librement accessible, il est aujourd'hui possible d'effectuer des comparaisons de différentes méthodes utilisant la reconnaissance par la géométrie de la main. C'est ce que nous allons présenter en avril à la conférence ICASSP, l'une des plus importantes conférences dans le domaine du traitement du signal et des images. La méthode détaillée et les résultats par protocole seront disponibles dans l'article associé[3].

# OLENA 0.11

par *Roland Levillain (Enseignant-Chercheur)*

OLENA 0.11[4], la bibliothèque de traitement d'images générique et performante développée au LRDE, est sortie le 21 février 2007. OLENA s'inscrit dans la thématique « Calcul Scientifique et Langages » du LRDE. Ce projet est issu du besoin d'un outil générique et performant pour écrire des algorithmes de traitement d'images. En effet, il existe de nombreuses bibliothèques dans ce domaine, mais elles réussissent rarement à concilier abstraction, généricité et performances.

Le degré d'*abstraction* que fournit un outil de calcul scientifique est sa capacité à exprimer des concepts de haut niveau, souvent théoriques. Notamment, on souhaite pouvoir écrire ses programmes en utilisant un style proche d'une écriture mathématique/algorithmique, dépouillée des détails d'implémentation.

Une bibliothèque *générique* fournit des algorithmes, écrits une fois, et applicables à des types de données divers. Ainsi, les algorithmes d'OLENA peuvent fonctionner sur des images à 1, 2 ou 3 dimensions, binaires, en niveaux de gris, en couleurs, etc. Mieux : l'utilisateur peut définir des variantes d'un algorithme pour une catégorie d'images données (ex : les images binaires), connues pour être plus efficaces, sans perturber le comportement général vis-à-vis des autres types d'images.

La généricité *statique* offerte par le C++ permet à l'utilisateur de bénéficier d'abstractions ne nécessitant pas un support à l'exécution (ex. : fonction virtuelles). Ainsi, le compilateur dispose de plus d'informations, et peut réaliser de nombreuses optimisations résultant en un code *performant* à l'exécution.

L'équipe OLENA travaille actuellement sur Olena 1.0, qui étend les concepts d'OLENA 0.11 pour proposer une approche radicalement nouvelle de la programmation générique, utilisant des objets-transformations appelés *morphers génériques*.

# En bref

**Les nouvelles publications** (disponibles sur publis.lrde.epita.fr)

- **DARBON, J.**. A note on the discrete binary mumford-shah model.. In *Proceedings of the international Computer Vision / Computer Graphics Collaboration Techniques and Applications (MIRAGE 2007)*, Paris France
- **FOUQUIER, G., ATIF, J., AND BLOCH, I.**. Local reasoning in fuzzy attributes graphs for optimizing sequential segmentation. In *Proceedings of the 6th IAPR TC-15 Workshop on Graph-based Representations in Pattern Recognition (GBR)*, Alicante, Spain
- **FOUQUIER, G., LIKFORMAN, L., DARBON, J., AND SANKUR, B.**. The biosecure geometry-based system for hand modality. In *Proceedings of the 32nd IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Honolulu, Hawaii, USA
- **QUOC, C. L., BELLOT, P., AND DEMAILLE, A.**. Stochastic routing in large grid-shaped quantum networks. In *Proceedings of the Fifth International Conference on Computer Sciences, Research, Innovation and Vision for the Future (RIVF'07)*, Hanoi, Vietnam
- **VERNA, D.**. CLOS solutions to binary methods. In *Proceedings of the International MultiConference of Engineers and Computer Scientists*, Hong Kong. International Association of Engineers

**Les logiciels** OLENA 0.11 est sortie le 21 février 2007 (cf. supra).

[3] The Biosecure Geometry-based System for Hand Modality (ICASSP 2007), http://publis.lrde.epita.fr/200704-ICASSP.
[4] OLENA 0.11, http://olena.lrde.epita.fr/Olena011.