Authentification biométrique

31 août 2005

1 Introduction

Dans ce chapitre, il est question d'une méthode d'authentification qui tend à se répandre dans la vie quotidienne : l'authentification biométrique. Authentifier une identité, dans le cadre d'un contrôle d'accès, consiste à certifier à une instance (un ordinateur, un terminal bancaire, une autre personne) que l'identité de l'interlocuteur est bien celle qu'il prétend avoir.

L'authentification ou la vérification de l'identité d'un utilisateur peut se faire de différentes façons [7], détaillées ci-dessous par ordre croissant de sécurité.

1. En utilisant un objet spécifique en possession de l'utilisateur. Par exemple un utilisateur aura accès à certaines ressources grâce à une clé physique ou une carte d'accès. S'il perd l'objet authentifiant, l'utilisateur n'aura plus accès aux ressources. Si l'objet est volé sans que l'utilisateur ne s'en rende compte, l'identité de l'utilisateur pourra être usurpée avec toutes les nuisances que cela peut entraîner.
2. En utilisant un savoir spécifique connu de l'utilisateur. Ceci peut être un mot de passe ou un numéro d'identification (*personal identification number* ou PIN). L'inconvénient est que les mots de passe peuvent être oubliés, devinés ou révélés. Dans le cas d'un oubli l'utilisateur n'aura plus accès au ressources. Si le mot de passe est deviné par un attaquant, celui-ci pourra usurper l'identité de l'utilisateur. Il arrive aussi que l'utilisateur révèle son mot de passe (pour diverses raisons) à un tiers. Dans ce cas, l'authentification n'est plus fiable puisqu'on ne peut certifier qu'il s'agit bien de l'utilisateur
3. En utilisant une caractéristique physique ou comportementale intrinsèque à l'utilisateur. Un trait particulier de la personne tel que son empreinte digitale, la géométrie de sa main, le motif de son iris, etc., permet d'authentifier *physiquement* son identité. Cette méthode d'authentification est appelée authentification biométrique.

Contrairement aux clés et mots de passe, la caractéristique biométrique ne peut être perdue ou oubliée. De plus, l'authentification biométrique est plus pratique à utiliser. En effet, le nombre de mots de passe que l'on doit retenir grandit chaque jour. Un oubli est dans ces conditions inévitable ce qui peut conduire à beaucoup de soucis. Bien que l'authentification biométrique ne résolve pas tous les problèmes de sécurité et qu'elle ne soit pas adaptée à toutes les applications, elle offre une méthode puissante de vérification d'identité. Aussi, elle peut être utilisée en complément aux deux autres méthodes plutôt qu'en remplacement.

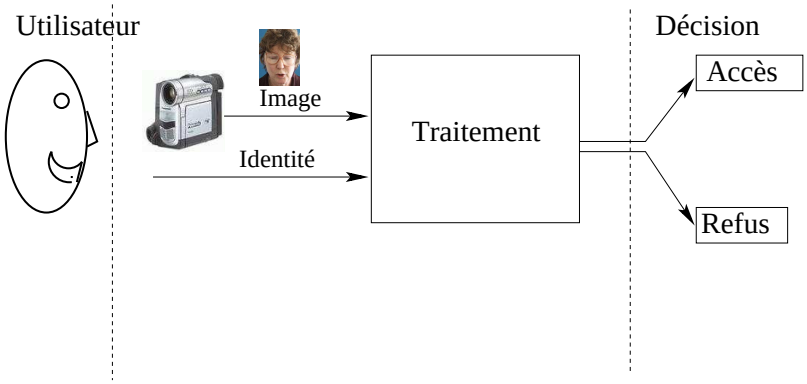

FIG. 1 – Système biométrique classique.

1.1 Vue d'ensemble

Un système d'authentification biométrique comporte en général plusieurs éléments qu'il est utile de définir précisément :

- A l'origine on trouve un *capteur* qui mesure le trait biométrique. Caméra, capteur tactile, microphone en sont des exemples classiques.
- *l'utilisateur* ou *client* est la personne qui se soumet (volontairement) à l'authentification.
- Pour pouvoir authentifier un utilisateur on doit disposer d'un *gabarit* (template en anglais), c'est-à-dire un exemple de caractéristiques biométriques de l'utilisateur en question. En outre, le système biométrique doit prévoir une procédure d'inscription au cours de laquelle le gabarit d'un utilisateur est créé.
- L'*unité de pré-traitement* a pour but d'extraire du signal qui vient d'être enregistré un vecteur de caractéristiques qui puisse être comparé au gabarit. En d'autre termes les deux vecteurs doivent avoir la même dimension.
- Le *signal biométrique test* est le signal qui va être enregistré par le capteur et comparé au gabarit après pré-traitement.
- Le système d'authentification doit comporter un espace de stockage appelé *base de données client* qui regroupe et gère les gabarits des différents utilisateurs. Notons que le gabarit peut être stocké de façon complètement décentralisée sur une carte à puce, à la disposition de l'utilisateur.

La figure 1 montre les différents modules du système biométrique pendant la phase opérationnelle. L'utilisateur fournit au système une identité présumée. Le capteur enregistre le signal biométrique test spécifique à l'utilisateur. Le gabarit associé à l'identité présumée est récupéré dans la base de données client. Après traitement, le gabarit est comparé au signal biométrique qui vient d'être enregistré. Il en résulte une décision binaire : soit l'utilisateur est accepté, soit il est rejeté. Certains systèmes offre une troisième possibilité "appel à une instance supérieure" en cas de doute sur la décision. On peut aussi imaginer que le système sort une décision souple (par exemple une probabilité) qui pourrait être utilisée à un autre niveau, par exemple en complément à une autre méthode de vérification.

La phase d'enrôlement (*enrolment phase* en anglais) est une étape nécessairement antérieure à la phase opérationnelle du système et pendant laquelle le gabarit de l'utilisateur sera créé. L'utilisateur doit volontairement permettre que la caractéristique biométrique soit enregistrée au moins une fois. Un gabarit sera forgé à partir de cet (ou ces) enregistrement(s) et sera stocké dans la base de données client. La procédure de pré-traitement qui extrait le gabarit du signal est rigoureusement identitique à celle utilisée pendant la phase opérationelle. Lorsque plusieurs enregistrements du même trait biométrique sont disponibles, on peut soit créer un seul gabarit à partir des vecteurs de caractéristiques, ou alors créer et stocker plusieurs gabarits par utilisateur. Une méthode simple mais efficace consiste à créer le gabarit en prenant la moyenne des vecteurs caractéristique extraits

Contrairement à un mot de passe classique, l'information biométrique est bruitée. Ce bruit peut provenir de l'acquisition par le capteur (bruit de fond, distorsion due au canal, bruit introduit par le capteur, conditions d'éclairage,) ou de la modalité biométrique elle-même qui varie au cours du temps (état de santé, vieillissement) ou des deux. Nous distinguerons les deux en parlant de variabilité due à l'aquisition et de variabilité intrinsèque de la modalité.

1.2 Authentification et identification

Un système biométrique peut fonctionner en mode authentification et identification. Le mode authentification est celui qui vient d'être décrit : il s'agit de certifier que l'identité présumée est correcte. Le mode identification a pour but de déterminer l'identité d'une personne inconnue. La différence avec le mode authentification est qu'on ne dispose pas de l'identité présumée. Le signal biométrique test doit donc être comparé à tous les gabarits de la base de données client.

Le mode identification est utilisé principalement dans les applications judiciaires, (exemple : déterminer l'identité d'un criminel à partir d'empreintes digitales). Dans ce chapitre, nous supposerons que l'utilisateur demande volontairement une authentification pour accéder à certaines ressources et que donc l'utilisateur fournit une identité. Nous nous concentrerons de ce fait uniquement sur l'authentification d'identité et nous n'aborderons pas l'identification. Cependant, on peut aussi envisager un contrôle d'accès qui utilise le mode d'identification lorsque le nombre d'utilisateurs est très faible, de l'ordre de 5 à 10. Par exemple l'accès au domicile familial peut être contrôlé par identification biométrique puisque dans ce cas le nombre d'utilisateurs se limite aux membres de la famille.

1.3 Biométrie et sécurité

Insistons sur le fait que les modules décrits au point 1.1 et les communications entre les modules doivent étre sécurisés. En effet imaginons que le lien entre capteur et unité de pré-traitement soit non-sécurisé. Un attaquant pourrait par exemple falsifier le signal biométrique test et pénétrer dans le système. De même, si la base de données est corrompue, l'attaquant peut remplacer un gabarit par le sien et déjouer le système d'accès (voir à ce propos [5]).

Une grande différence avec le mot de passe utilisé traditionnellement dans l'authentification d'identité est que celui-ci est secret. La caractéristique biométrique

est peut au contraire être facilement mesurée par un attaquant et être ensuite utilisée pour contourner le contrôle d'accès. Des mesures spécifiques doivent être prises pour vérifier que le signal biométrique mesuré n'est simplement pas la restitution d'un enregistrement mais bien "original". Ces parades peuvent s'avérer complexes et couteuses à mettre en oeuvre à la mesure de la complexité des subterfuges utilisés pour tromper le système biométrique. Il faut donc garder à l'esprit qu'aucune technique de contrôle d'accès n'est inviolable. Par contre l'utilisation d'une authentification biométrique en plus des mécanismes traditionnels rend les attaques plus difficiles.

2 Survol des principales modalités

Deux critères entrent en compte pour le choix d'une caractéristique ou *modalité* biométrique à des fins d'authentification : la facilité d'utilisation et la capacité de discrimination. Pour qu'une caractéristique physiologique ou comportementale ait une grande capacité de discrimination, il faut qu'elle soit distribuée dans la population avec une grande variance. En même temps, lorsqu'on mesure plusieurs fois cette caractéristique chez un même individu, on doit observer le moins de variations possibles. Pour ce qui est de la facilité d'utilisation, l'utilisateur devrait idéalement interagir aussi peu que possible avec le système d'authentification. L'enregistrement du signal biométrique test doit se faire sans contrainte pour l'utilisateur. Ces deux conditions sont inévitablement contradictoires, puisque l'absence de contraintes pour l'utilisateur engendre de la variabilité dans le signal enregistré. Ceci a comme conséquence un nombre faible de modalités viables. Nous décrivons les principales modalités ci-dessous. D'autres modalités existent mais n'ont pas, à ce jour, le même attrait que celles décrites ici. Parmi celles-ci citons la forme de la main (empreintes palmaires), la forme de l'oreille, la rétine, l'ADN, la dynamique de la signature ou de la frappe au clavier, l'odeur, etc.

2.1 La parole

Bien que la capacité à former des sons et des mots soit à la fois liée à la physiologie et au comportement, la parole est en général classée parmi les modalités comportementales. Un simple microphone peut faire office de capteur. La parole est très bien acceptée par les utilisateurs grâce à sa facilité d'utilisation. Pour être authentifié, l'utilisateur prononce quelques mots qui forment le signal biométrique test. On distingue les techniques d'authentification du locuteur qui dépendent du contenu à prononcer (*text dependent speaker verification*) et les techniques indépendantes du contenu (*text independent speaker verification*). Ces dernières sont considérées comme plus difficiles. Pour procéder à l'authentification, on décompose le signal vocal en plusieurs bandes de fréquences desquelles sont extraites des caractéristiques telles que les coefficients cepstraux (logarithme de la transformée de Fourier). Ces caractéristiques distriminantes sont alors comparées au gabarit.

Le taux d'erreur (qui sera défini précisément au paragraphe 4) pour un système d'authentification du locuteur avoisine quelques pourcents dans des conditions favorables. Ce taux d'erreur est fortement influencé par le bruit de fond, la longueur du texte à prononcer ainsi que la largeur de bande du canal de

transmission (dans le cas d'une authentification à distance par téléphone portable par exemple). On atteint alors des taux de 10 % et plus si plusieurs conditions défavorables sont réunies. Le lecteur est invité à consulter les évaluations annuelles du NIST [14] pour plus de détails sur les performances de l'authentification vocale.

2.2 Le visage

Le visage fait partie des modalités les plus facilement acceptées par le public, probablement parce que c'est principalement grâce au visage que nous nous identifions au quotidien. De plus, les capteurs utilisés pour cette technique peuvent être de simples caméras (du type *web cam* par exemple) ce qui rend le coût des systèmes très compétitif. Cependant la modalité visage souffre d'un bruit d'aquisition élevé. En effet, le visage étant une surface tri-dimensionelle, son image prise par une caméra varie fortement avec les conditions ambiantes telles que l'éclairage et l'angle de vue. L'expression du visage fait également varier son apparence de façon importante. Dans un système automatique, le visage doit être détecté et recalé par rapport à un modèle. Cette étape s'avère délicate dès que l'arrière plan n'est pas complètement uniforme.

Il existe deux approches principales pour l'authentification grâce au visage : Une approche locale dans laquelle des propriétés (de préférence invariantes) sont extraites en des points précis du visage (par exemple des réponses de filtres de Gabor [9]) et une approche holistique dans laquelle l'entièreté des pixels de l'image du visage est prise en compte (par exemple l'approche *eigenface* [18]). Dans l'approche *eigenface*, l'image du visage est exprimée comme une somme pondérée d'images constitutives appelées *visages propres*. Ces images constitutives sont obtenues par une analyse en composante principales. La figure 2 montre des exemples de visages propres obtenus à partir de la base de données XM2VTS [11].

En ce qui concerne la variabilité intrinsèque, la modalité visage est assez peu fiable. Prenons le cas de vrais jumeaux, c'est-à-dire de jumeaux qui partagent le même code génétique. Il est clair qu'un système automatique de vérification du visage qui doit tenir compte de la variabilité d'acquisition, ne pourra percevoir les différences subtiles entre les jumeaux.

Les taux d'erreur des systèmes actuels entièrement automatiques, c'est-à-dire les systèmes qui localisent et authentifient automatiquement le visage, se situent entre 10 et 20% (Voir [10] pour une évaluation de méthode d'authentification du visage récente).

2.3 L'iris

Bien que la couleur de l'iris soit liée au phénotype de l'individu, (l'expression de son génotype), les motifs de l'iris sont considérés comme uniques pour chaque individu et pour chaque oeil. Ils ne dépendent pas du code génétique de l'individu. Ceci permet donc en théorie de distinguer les vrais jumeaux à l'aide du motif leur iris.

Une caméra CCD (*Charge-Coupled Device* ou dispositif à transfert de charges) ordinaire permet l'acquisition d'une image de haute résolution. Il faut noter que cette acquisition est relativement contraignante pour l'utilisateur puisqu'il doit

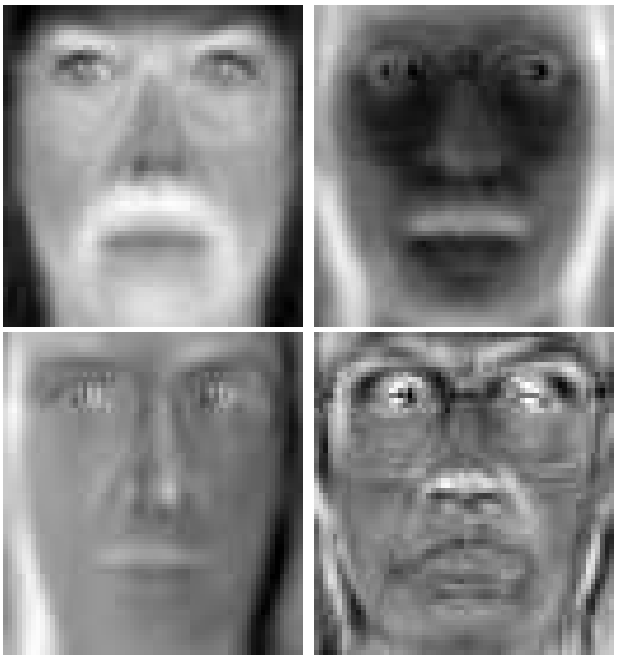

FIG. 2 – Les "visages propres" sont utilisés dans la technique *eigenface* pour extraire un vecteur de caractéristiques biométriques.

se positionner précisément par rapport à l'objectif, tant du point de vue de la distance à l'objectif, que de sa position transversale (pour que l'image de l'iris soit bien au centre de la surface du capteur CCD). D'un autre côté il résulte de cette acquisition une image, et donc un vecteur de caractéristiques, peu bruités, ce qui permet de réduire les erreurs. L'iris fait donc partie des modalités biométriques les plus fiables.

Le vecteur de caractéristiques se calcule à partir de la réponse de filtres appliqués à la texture (ou au motif) de l'iris et est défini en coordonnées polaires dont l'origine est le centre de la pupille. Il semble les taux d'erreur qu'offre ce type de systèmes soient très bas. [2]

2.4 Les empreintes digitales

L'authentification (et l'identification) à partir d'empreintes digitales est sans doute la plus ancienne technique biométrique. Elle est aussi l'une des plus mûres et probablement la plus répandue actuellement. Les empreintes sont utilisées depuis longtemps dans les enquêtes policières ce qui donne un caractère "carcéral" à la technique. De plus un contact physique est nécessaire pour acquérir le signal biométrique [1].

Les empreintes digitales, présentent sur nos doigts, forment un réseau complexe de crêtes. Il semble que ce réseau soit unique pour chaque individu. Comme pour le visage, l'image globale de l'empreinte en niveau de gris est

[1] Des capteurs qui ne nécessitent pas de contact avec le doigt existent mais il semble qu'ils soient beaucoup moins performants.

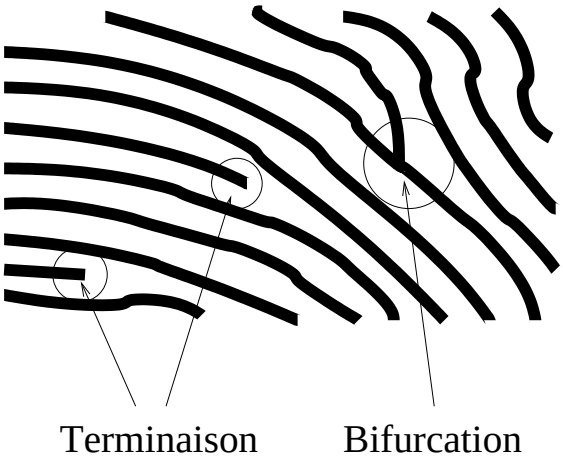

FIG. 3 – Les crêtes d'une empreinte digitale peuvent se terminer (terminaison), ou se diviser (bifurcation).

utilisée pour représenter l'empreinte. Pour contourner le problème d'alignement de l'empreinte test et de l'empreinte gabarit, on effectue une correlation spatiale des deux signaux. De nombreuse variantes de cette technique existent (voir [12] pour plus de détails).

La spécificité d'une empreinte digitale peut aussi être déterminée à partir de la configuration de *minuties*. Les minuties sont des crêtes qui apparaissent soit en tant que terminaison soit en bifurcation comme l'illustre la figure 3. Une empreinte digitale complète se compose d'environ une centaine de minuties, mais seule une partie (entre 10 et 30) pourra être extraite de façon automatique avec une fiabilité suffisante. Le vecteur de caractéristiques sera dans ce cas la liste des positions des minuties et leur orientations. La mise en correspondance des vecteurs de minuties s'apparente à la mise en correspondance de graphes. Il s'agit principalement de déterminer si les voisinages autour d'une minutie sont similaires. Deux empreintes seront considérées comme provenant du même doigt lorsqu'on trouve suffisamment de voisinages similaires (voir [12] pour plus de détails).

Il existe plusieurs types de capteurs capables d'acquérir une image de l'empreinte digitale. On distingue principalement des capteurs optiques, les capteurs intégrés et les capteurs à ultra-sons. Le principe des capteurs optiques consiste à éclairer l"empreinte placé contre une surface transparente (par exemple du verre) à l'aide d'une diode laser. Un capteur CCD mesure l'intensité de la lumière réflechie. Les crêtes, en contact avec la surface transparente réflechissent la lumière différemment des vallées, ce qui permet de reconstituer une image du relief de l'empreinte. Les capteurs intégrés sont formés de "micro-puces" électroniques qui capturent une image de l'empreinte via une mesure de capacité. Ces capteurs se présentent sous la forme d'une surface sensible constituée d'un grand nombre de micro-plaques conductives recouvertes d'une couche isolante. Lorsque le doigt de l'utilisateur est posé sur le capteur, la peau joue le rôle d'une autre plaque conductrice formant ainsi un réseau de condensateurs. Comme la tension au bornes d'un condensateur dépend de la distance entre les

plaque (dans ce cas-ci la distance entre les vallées ou crêtes et les micro-plaques) le réseau de condensateurs permet de récupérer une image du relief de l'empreinte digitale. Pour les capteurs à ultra-sons, le principe est similaire à celui des capteurs optiques, la lumière étant remplacées par un faisceau ultra-son qui balaie la surface de l'empreinte. Une image des vallées et crêtes de l'empreinte peut être reconstituée à partir de l'écho mesuré.

2.5 Biométrie multi-modale

Au lieu de considérer une seule modalité pour l'authentification de l'identité, une approche alternative consiste à utiliser plusieurs modalité *en même temps* afin de réaliser l'authentification de l'utilisateur. Un exemple de système biométrique multi-modal est un système qui utilise à la fois l'empreinte digitale et l'image du visage pour l'authentification. Si les caractéristiques extraites pour les modalités utilisées sont statistiquement indépendantes, on peut montrer que le système multi-modal offre des taux d'erreur inférieurs au meilleur système qui n'utilise qu'une seule des modalités disponibles. Plusieurs arguments théoriques et expérimentaux permettent même d'étendre cette propriété au cas où les caractéristiques sont corrélées [8]. Il en découle que les système multi-modaux peuvent atteindre un niveau de performance supérieure et donc être utile dans une vaste gamme d'applications.

La *fusion* ou l'intégration de l'information concernant l'identité de l'utilisateur peut se faire à plusieurs niveaux [17]. On peut opérer la fusion au niveau des caractéristiques extraites de chacun des signaux. Par exemple, les vecteurs de caractéristiques correspondant aux différentes modalités peuvent être simplement mis à la suite l'un de l'autre. Le problème revient alors à chercher une règle de décision globale pour les differentes modalités. D'autre part, la fusion peut être opérée au niveau des décisions souples. Dans ce cas, chaque modalité est utilisée séparément par un algorithme d'authentification à une seule modalité. Il en résulte un *score* par modalité qui reflète la probabilité que le signal soit authentique (voir point 3.2). Le problème revient cette fois à trouver la meilleur façon de combiner les scores issus des différent algorithmes. Enfin, la fusion peut être opérée au niveau des décisions "dures". Dans ce cas, chaque algorithme à une seule modalité fournit une décision binaire (utilisateur accepté ou rejeté). Le problème revient alors à concilier les differentes décisions.

3 Eléments de la théorie de la décision

Le problème de l'authentification d'identité s'inscrit dans le cadre de la théorie de la décision : étant donnés une identité prétendue et un signal biométrique test qui vient d'être mesuré, on souhaite déterminer si ce signal provient bien de l'identité prétendue. Dans l'affirmative, la requête est acceptée et l'utilisateur a accès aux ressources qu'il demande. Dans le cas contraire, l'accès est refusé. Nous supposons que le signal fourni par le capteur est sous forme numérique (il a été echantillonné si le capteur est analogique) et se présente sous la forme d'un vecteur réel de dimension n, c'est-à-dire $\mathbf{x} \in R^n$. La dimension de $\mathbf{x}$ est en général très grande puisque le signal est un signal du type séquence d'images ou enregistrement audio. Par exemple si le signal à traiter est une séquence de 10 images d'une taille de 640 par 480 pixels, la dimension de $\mathbf{x}$ equivaut à $n = 640$

x 480 x 10 = 3072000.

Le problème revient donc à classer $\mathbf{x}$ dans la classe *authentique* ω_a et la classe *imposteur* ω_b, ce qui est un problème classique de reconnaissance des formes à deux classes [4]. Une erreur se produit lorsque le signal test est mal classé. Le problème revient donc à trouver une fonction de R^n dans $\{\omega_a, \omega_b\}$ qui minimise un critère d'erreur. Plusieurs règles de décision, détaillées ci-dessous, peuvent être dérivées suivant le critère d'erreur choisi.

3.1 Règle de décision pour l'erreur minimale

La règle de décision qui minimise la probabilité d'erreur $P(\text{erreur})$ (aussi appelée règle de décision de Bayes) est décrite ici. Ayant mesuré un signal test $\mathbf{x}$, si l'on décide que le signal $\mathbf{x}$ est authentique, la probabilité de faire la mauvaise décision $P(\text{erreur}|\mathbf{x})$ est simplement la probabilité que $\mathbf{x}$ soit en réalité un imposteur, c'est-à-dire $P(\omega_b|\mathbf{x})$. De même, si l'on décide que $\mathbf{x}$ est de type imposteur, la probabilité de se tromper est donné par $P(\omega_a|\mathbf{x})$. Pour un signal biométrique test $\mathbf{x}$ donné, la probabilité d'erreur $P(\text{erreur}|\mathbf{x})$ est donc minimale si l'on décide ω_a lorsque $P(\omega_a|\mathbf{x}) > P(\omega_b|\mathbf{z})$ et si l'on décide ω_b dans le cas contraire. La probabilité d'erreur totale s'écrit dans ce cas

$$P(\text{erreur}) = \int P(\text{erreur}|\mathbf{x})p(\mathbf{x})d\mathbf{x}$$

où $p(\mathbf{x})$ est la densité de probabilité de $\mathbf{x}$. Puisque la règle de decision évoquée ci-dessus minimise $P(\text{erreur}|\mathbf{x})$ pour chaque $\mathbf{x}$, l'intégrale est aussi minimisée. La règle de décision qui assigne à $\mathbf{x}$ la classe qui a la probabilité *a posteriori* maximale est appelé la loi de Bayes :

$$P(\omega_a|\mathbf{x}) \underset{\omega_a}{\overset{\omega_b}{\lessgtr}} P(\omega_b|\mathbf{x}).$$

Ces deux inégalités résument la règle de décision de Bayes : la classe de $\mathbf{x}$ est ω_a si la probabilité de cette classe conditionnée à la mesure $P(\omega_a|\mathbf{x})$ est supérieure à la probabilité de la classe ω_b conditionnée à la même mesure. Cette règle est optimale, dans le sens où toute autre règle mène à une plus grande probabilité d'erreur. Autrement dit, en moyenne sur un grand nombre de décisions, le plus petit nombre d'erreurs possible est atteint lorsqu'on emploie la règle de Bayes. Les probabilités *a posteriori* peuvent être exprimées en fonction des densités de probabilité conditionnelles $p(\mathbf{x}|\omega_c)$ $(c \in \{a, b\})$

$$P(\omega_c|\mathbf{x}) = \frac{p(\mathbf{x}|\omega_c)P(\omega_c)}{p(\mathbf{x})},$$

où $P(\omega_c)$ est la probabilité *a priori* et $c \in \{a, b\}$. La règle de décision devient

$$\frac{p(\mathbf{x}|\omega_a)}{p(\mathbf{x}|\omega_b)} \lessgtr \frac{P(\omega_b)}{P(\omega_a)}. \tag{1}$$

Le terme de droite de ces inégalités ne dépend pas du signal mesuré $\mathbf{x}$ et reflète notre connaissance *a priori* sur l'occurence des classe ω_a et ω_b.

Le rapport des deux densités (termes de gauche) est le *rapport de vraisemblance* $l(\mathbf{x})$ [19]. La règle de décision s'écrit

$$l(\mathbf{x}) \lessgtr \eta,$$

où η est un *seuil* fixé par le concepteur du système. Ces dernières inégalités definissent une frontière de décision qui sépare l'espace des $\mathbf{x}$ en un domaine authentique Ω_a et un domaine imposteur Ω_b. Lorsqu'un $\mathbf{x}$ particulier est observé, il prend le label "authentique" ou "imposteur" suivant qu'il appartient à Ω_a ou Ω_b.

On peut distinguer à ce stade deux catégories de modèles qui vont être mis en oeuvre pour résoudre le problème de classification :

- Les modèle génératifs : dans cette catégorie, on estime les densités de probabilités conditionnelles $p(\mathbf{x}|\omega_c)$ ($c \in \{a, b\}$), et on classe $\mathbf{x}$ en utilisant l'equation (1).
- Les modèles discriminants : la frontière de décision ou de façon équivalente le rapport de vraisemblance $l(\mathbf{x})$ est estimé directement.

3.2 Le score

L'equation (1) est difficile à utiliser en pratique, car les lois de probabilité qui engendrent les signaux $\mathbf{x}$ sont inconnues et doivent être estimées. En raison de la dimension élevée de l'espace de $\mathbf{x}$ ($n = 1.000$ voire plus), cette estimation requiert un grand nombre d'échantillons, même dans le cas où on fait l'hypothèse de distributions paramétriques, par exemple gaussiennes. C'est pourquoi les algorithmes de classification au coeur des systèmes biométriques suivent plutôt les modèles discriminants (par exemple réseaux de neurones). Cependant, les modèles génératifs sont supérieurs dans certains cas par exemple le mélange de gaussienne pour l'authentification de locuteur introduite dans [16].

En pratique on cherchera donc une fonction $s(\mathbf{x})$, appelé *score*, qui est calculée à partir du signal biométrique mesuré $\mathbf{x}$. La fonction score doit idéalement s'approcher le plus possible du rapport de vraisemblance $l(\mathbf{x})$ qui n'est pas connu. La décision sur l'identité résulte de la comparaison du score avec un seuil prédéfini η

$$s(\mathbf{x}) \lessgtr \eta. \tag{2}$$

La fonction score $s(\mathbf{x})$ associée au signal $\mathbf{x}$ est souvent calculée en deux étapes.

La première étape est consiste à extraire du signal $\mathbf{x}$ le vecteur de caractéristiques $\mathbf{y}$

$$\mathbf{y} = f(\mathbf{x}).$$

Le but de cette opération est de se débarrasser de composante variable et garder la composante fixe. Le vecteur $\mathbf{y}$ est de dimension bien plus faible que le signal original.

La seconde étape consiste à mettre ce vecteur en correpondance avec le gabarit $\boldsymbol{\mu}$ au travers d'une fonction de similarité $S(\mathbf{y}, \boldsymbol{\mu})$. Le score est le résultat de cette mise en correspondance, c'est-à-dire

$$s = S(\mathbf{y}, \boldsymbol{\mu}),$$

Le score s dépend implicitement de $\mathbf{x}$ puisque $\mathbf{y}$ dépend de $\mathbf{x}$.

3.3 Règle de décision du risque minimum

Dans un problème d'authentification, et plus généralement de classification à deux classes, on distingue deux types d'erreurs :

– Une tentative d'accès est rejetée bien que le signal $\mathbf{x}$ soit authentique. On parle d'erreur de *faux rejet*.
– Une tentative d'accès est acceptée bien que le signal $\mathbf{x}$ soit de la classe imposteur. On parle d'erreur de *fausse acceptation*.

En complément à ces deux types d'erreur, on définit la probabilité de fausse acceptation e_A et la probabilité de faux rejet e_R

$$e_R = \int_{\Omega_b} p(\mathbf{x}|\omega_a)d\mathbf{x}, \qquad \text{probabilité de faux rejet et} \tag{3}$$

$$e_A = \int_{\Omega_a} p(\mathbf{x}|\omega_b)d\mathbf{x}, \qquad \text{probabilité de fausse acceptation.} \tag{4}$$

Comme le montrent ces deux équations, la probabilité d'erreur est la probabilité d'observer des imposteurs dans le domaine authentique Ω_a et des échantillons authentiques dans le domaine imposteur Ω_b. La probabilité d'erreur qui est minimisée par la règle de décision de Bayes devient

$$P(\text{erreur}) = P(\omega_a)e_A + P(\omega_b)e_R. \tag{5}$$

Il est important de déterminer quel type d'erreur est le plus dommageable dans l'application visée. Dans certains cas, la facilité d'accès prime et c'est l'erreur de faux rejet qui est inacceptable. Dans d'autres, c'est l'erreur de fausse acceptation qui doit être minimale. Pour cette raison, plutôt que de minimiser la probabilité d'erreur, on tente de minimiser *le risque*.

Un risque, associé à chaque type d'erreur, est défini comme étant proportionnel à la probabilité d'erreur. Le facteur de proportionnalité indique la gravité du type d'erreur. Soit $\mathbf{x}$ une mesure, le risque $r_a(x)$ associé avec la décision de choisir la classe ω_a est

$$r_a(\mathbf{x}) = c_{ab}P(\omega_b|\mathbf{x}), \tag{6}$$

où c_{ab} est le facteur de proportionnalité c'est-à-dire le coût imputé au fait d'accepter un imposteur. De même, le risque $r_b(x)$ associé à la classe ω_b est

$$r_b(\mathbf{x}) = c_{ba}P(\omega_a|\mathbf{x}), \tag{7}$$

où c_{ba} est le coût imputé au fait de rejeter un accès authentique. La règle de décision du risque minimal est celle qui consiste à choisir la classe pour laquelle le risque est minimal, c'est-à-dire

$$r_a(\mathbf{x}) \underset{\omega_a}{\overset{\omega_b}{\lessgtr}} r_b(\mathbf{x}), \tag{8}$$

ce qui devient, en explicitant,

$$l(\mathbf{x}) \underset{\omega_a}{\overset{\omega_b}{\lessgtr}} \frac{c_{ab}}{c_{ba}} \frac{P(\omega_b)}{P(\omega_a)}. \tag{9}$$

Par rapport à la règle de décision de Bayes, l'introduction du risque ne change que l'expression du seuil, la fonction dépendant de $\mathbf{x}$ restant égale au rapport de vraisemblance $l(\mathbf{x})$. Ceci est important car cela montre que pour adapter un système à une l'application qui impose un risque différent (au moyen de c_{ab} et c_{ba}) , il suffit d'adapter le seuil et non la fonction score.

3.4 Règle de décision du minimax

Les règles de décision (1) et (9) font apparaître explicitement les probabilités *a priori* $P(\omega_a)$ et $P(\omega_b)$, qui reflètent la connaissance que l'on a sur l'apparition d'un signal authentique ou imposteur. Malheureusement ces probabilités sont très difficiles à évaluer. Comment estimer la probabilité d'apparition d'un imposteur ? Pour résoudre ce problème une approche consiste à concevoir une règle de décision pour laquelle le risque total est constant quelle que soit la valeur des probabilités *a priori*. Cette régle est appelée la règle de décision du *minimax*

Le risque total R est le risque cumulé sur toutes les valeurs de $\mathbf{x}$, c'est-à-dire

$$R = \int_{\Omega_a} r_a(\mathbf{x}) p(\mathbf{x}) d\mathbf{x} + \int_{\Omega_b} r_b(\mathbf{x}) p(\mathbf{x}) d\mathbf{x},$$

puisque Ω_a est le domaine où la décision ω_a est prise et que donc on court le risque r_a. De même pour le domaine Ω_b. En utilisant les définitions du risque (6) and (7) est le fait que $P(\omega_b) = 1 - P(\omega_a)$, R s'écrit

$$R = c_{ab} \int_{\Omega_a} p(\mathbf{x}|\omega_b) d\mathbf{x} + P(\omega_a) \left(c_{ba} \int_{\Omega_b} p(\mathbf{x}|\omega_b) d\mathbf{x} - c_{ab} \int_{\Omega_a} p(\mathbf{x}|\omega_b) d\mathbf{x} \right).$$

Il apparaît que le risque total est une fonction linéaire de $P(\omega_a)$, une fois que la règle de décision est fixée – c'est-à-dire lorsque les domaines d'intégration Ω_a et Ω_b sont fixés. Si d'aventure les probabilités *a priori* venaient à changer, le risque suivrait cette loi linéaire et pourrait donc augmenter. Par contre, si l'on choisit Ω_a et Ω_b tels que le facteur qui multiplie $P(\omega_a)$ est nul, le risque total ne dépend plus explicitement des probabilités *a priori*. Cette condition est

$$c_{ba} \int_{\Omega_b} p(\mathbf{x}|\omega_a) d\mathbf{x} = c_{ba} \int_{\Omega_a} p(\mathbf{x}|\omega_b) d\mathbf{x}, \tag{10}$$

c'est-à-dire

$$c_{ba} e_R = c_{ab} e_A,$$

soit que les probabilités d'erreur de faux rejet et de fausse acceptation soient égales si $c_{ab} = c_{ba}$. La règle de décision devient

$$l(\mathbf{x}) \underset{\omega_a}{\overset{\omega_b}{\lessgtr}} \eta,$$

mais cette fois le seuil η est choisi tel que l'equation (10) est satisfaite. Notons que la règle du minimax ne minimise ni l'erreur totale comme la règle (1) ni le risque comme la règle (9). La règle du minimax garantit que quelle que soit la valeur des probabilités *a priori*, le risque total est constant. Ceci a l'avantage que le risque encouru est toujours le même si les probabilités *a priori* sont modifiées.

4 Evaluation des performances d'un système d'authentification

Les performances d'un système d'authentification biométrique se mesurent avec les probabilités d'erreur e_A et e_R définies aux equations (3) et (4). Rappelons que e_A est la probabilité qu'un imposteur soit accepté et e_R la probabilité

qu'un utilisateur soit rejeté. Dans un système réel, on utilise la règle de décision du score (equation (2)) pour décider de la classe d'un signal test. Les régions Ω_a et Ω_b sont donc définies par cette règle de décision. Il en résulte que l'on peut exprimer e_A et e_B en fonction des densités de probabilité conditionnelles du score $s(\mathbf{x})$ plutôt que des densités conditionnelles de $\mathbf{x}$, de Ω_a et Ω_b. On a donc

$$e_R(\eta) = \int_{\eta}^{\infty} p(s(\mathbf{x})|\omega_a)ds, \qquad e_A(\eta) = \int_{0}^{\eta} p(s(\mathbf{x})|\omega_b)ds, \tag{11}$$

l'avantage étant qu'une densité de probabilité uni-dimensionnelle est bien plus facile à estimer qu'une densité définie sur un espace de grande dimension. Le nombre d'erreurs de faux rejet et de fausse acceptation doit évidemment être le plus faible possible. La difficulté est que ces deux nombres soient petits en même temps.

En effet, on peut rendre la probabilité de faux rejet e_A (respectivement la probabilité de fausse acceptation) aussi faible que l'on veut en faisant tendre le seuil η de l'equation (11) vers l'infini (respectivement vers 0). En contrepartie la probabilité de fausse acceptation (la probabilité de faux rejet) tendra vers 1.

4.1 Taux de faux rejet et fausse acceptation

Pour calculer les probabilités d'erreur e_A et e_B, il faut estimer les densités de probabilité conditionnelles des scores $p(s(\mathbf{x})|\omega_c)$ $(c \in \{a, b\})$ à partir de données biométriques réelles. Pour ce faire, il faut obtenir un nombre N_a de scores authentiques (c'est-à-dire qui résultent de tentatives d'accès authentiques) et N_b scores imposteurs (qui résultent d'une tentatives d'accès frauduleuses). Nous donnons plus bas davantage de détails sur les données d'évaluation. Nous introduisons le Taux de Faux Acceptation (False Acceptance Rate ou FAR) T_A et le Taux de Faux Rejet (False Rejection Rate) T_R qui sont des estimations des erreurs e_A et e_B

$$T_A(\eta) = \frac{1}{N_b}\sum_{i=1}^{N_b} u(\eta - s(\mathbf{x}_i)) \qquad x_i \in \omega_b, \tag{12}$$

$$T_R(\eta) = \frac{1}{N_a}\sum_{i=1}^{N_a} u(s(\mathbf{x}_i) - \eta) \qquad x_i \in \omega_a, , \tag{13}$$

où $u(.)$ est la fonction indicatrice.

4.2 Courbe caractéristique

On voit que la difficulté est bien entendu de trouver le bon compromis entre le taux d'erreur de fausse acceptation T_A et le taux de faux rejet T_R. C'est pourquoi on introduit la courbe caractéristique (Receiver Operating Characteristic ou ROC curve en anglais [19]). Cette courbe donne pour chaque valeur de T_F la valeur de T_A qui lui est associée. Un exemple de courbe caractérisque est représenté à la figure 4. La courbe est obtenue en faisant varier le seuil η et en traçant la valeur de T_F en fonction de T_A. La courbe caractéristique fournit de façon graphique un aperçu de tous les compromis T_A-T_R. Un système

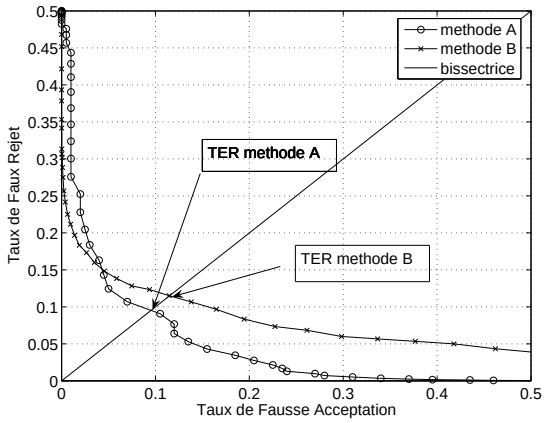

FIG. 4 – Exemples de courbes caractéristiques. Deux courbes correspondant à deux methodes d'authentification sont représentées. La méthode A est globalement plus performante que la méthode B, car sa courbe caractéristique est plus proches des axes. Elle offre par ailleurs un TER inférieur à la méthode B. Cependant, la méthode B est plus performante pour des taux de faux acceptation très faibles (inférieurs à 0,03). Cet exemple montre la nécessité de considérer les courbes dans leur totalité lors d'une comparaison de performances.

biométrique est d'autant meilleur que sa courbe caractéristique est proche de l'origine.

Un seuil η donné définit un point de travail sur la courbe caractéristique. Ce point, choisi par le concepteur, dépend de l'application visée, c'est-à-dire si un faible T_A ou un faible T_R est plus critique. On peut toujours trouver un seuil pour lequel les valeurs de T_A et T_R sont égales. On appelle ce taux le *Taux d'Egale Erreur* ou TER (*Equal Error Rate* ou EER en anglais). Ce taux correspond à l'intersection de la courbe caractéristique avec la bissectrice des axes (si les échelles des deux axes sont égales). Lorsque le TER est proche de 0, le point correspondant sur la courbe caractéristique est proche de l'origine, et le système biométrique est performant, c'est-à-dire qu'il est capable de distinguer les accès authentiques des accès imposteurs. Bien souvent, on se limite au TER pour caractériser les performances d'un système biométrique. Cependant, lorque l'on compare les performances de deux systèmes, il est important de ne pas comparer uniquement deux TER ou deux couples (T_A, T_R) mais d'étudier tous les points de la courbe caractéristique. En effet, il n'est pas rare que deux systèmes aient des performances fort différentes dans des régions différentes de la courbe caractéristique (voir figure 4). Cependant le TER offre, sous la forme d'un nombre unique, une estimation grossière des performances du système biométrique qui s'avère très utile dans la pratique.

Insistons sur le fait que les taux T_A et T_F (et donc la courbe caractéristique et le TER) sont obtenus à partir de scores sur des données biométriques réelles. Il en résulte que ces valeurs, qui sont critiques pour le choix d'un système, dépendent de la difficulté des données biométriques. Un système biométrique, aux performances médiocres dans le cas général, obtient un TER proche de zéro

si le signal biométrique test et le gabarit sont très similaires pour les scores authentiques, et très différents pour les scores imposteurs. Il est donc toujours utile, lorsque l'on consulte les performances d'un système, de prendre en considération la qualité et quantité de données utilisées pour les estimer.

Il est intéressant de remarquer que des estimations des densités conditionnelles des scores $p(\mathbf{x}|\omega_i)$ peuvent être obtenues en dérivant les taux T_A et T_R de l'equation (11) par rapport à η. On a donc

$$\hat{p}(s(\mathbf{x})|\omega_a) = -\frac{d}{d\eta}T_R(\eta), \tag{14}$$

et

$$\hat{p}(s(\mathbf{x})|\omega_b) = \frac{d}{d\eta}T_A(\eta) \tag{15}$$

4.3 Données et protocole de validation

Le paramètre principal qui influence la conception d'un système biométrique est la probabilité d'erreur du système. Cette probabilité ne peut pratiquement jamais être calculée analytiquement et doit être estimée à partir de simulations sur des données réelles.

Les données réelles sont des signaux biométriques tests que l'on s'attend à avoir dans la phase opérationnelle du système biométrique. Il s'agit donc par exemple d'enregistrements de la voix, d'images du visage, d'images de l'iris, de signatures, etc.

Ces données doivent avoir été obtenues dans les mêmes conditions d'enregistrement que dans l'application visée. En d'autres termes, les échantillons doivent représenter la population. Ceci inclut la qualité du capteur (si l'application visée on utilise un type de microphones à bas prix et à forte variabilité, il faut que les données reflètent cette variabilité) le bruit ambiant (par exemple l'arrière-plan que l'on s'attend à avoir dans l'application) et les changements liés à la durée entre deux enregistrements (par exemple les changements de coiffure, de maquillage, le vieillissement, le bronzage, la maladie, etc.). Aussi, la durée entre l'enregistrement dont sera issu le gabarit et l'enregistrement qui forme le signal biométrique test doit être suffisamment longue de façon à ce que les variations liée à la durée soient bien présentes.

L'estimation des probabilités d'erreur d'un système biométrique dépend directement des données sur lesquelles elle a été estimée. C'est pourquoi une comparaison équitable entre deux approches ne peut se faire que si les taux d'erreur ont été estimés sur le même ensemble de données, ou sur deux ensembles très proches.

La conception du système requiert également des données : pour créer les gabarits et pour mettre au point une fonction d'extraction de vecteurs de caractéristiques et de mise en correspondance performantes. Les données sont souvent fastidieuses et coûteuse à rassembler, traiter et stocker. Il faut donc veiller à les utiliser de façon efficace et éviter les erreurs de méthodologie (par exemple utiliser les mêmes données pour estimer les probabilités d'erreur et dans la conception des fonctions d'extraction).

Pour ce faire on définit un protocole de test qui stipule rigoureusement la manière dont les données doivent être utilisées. En général les données sont divisées en trois ensembles distinct : l'ensemble d'entraînement, l'ensemble de

validation et l'ensemble de test. On utilise l'ensemble d'entraînement pour créer les gabarits. Les données de l'ensemble de validation permettent de calculer les taux d'erreur et de fixer le seuil. Une fois le seuil fixé, on utilise l'ensemble de test pour obtenir le taux de fausse acceptation et de faux rejet avec les équations (12) et (13).

4.4 Intervalles de confiance

Les taux d'erreur, qui reflètent les performances d'un système biométrique, sont des estimations de probabilités obtenues sur des ensembles de données nécessairement finis. L'estimation sera donc toujours entâchée d'une incertitude. Il est donc important de connaître cette incertitude sur les performances du système. Cette connaissance, qui se fait au travers du calcul d'intervalles de confiance, aide à prédire les performances réelles à partir de performance simulées. Cependant, il faut garder à l'esprit que les intervalles de confiance donneront l'incertitude sur les taux d'erreur uniquement pour le même type de données que celui qui a été utilisé pour les obtenir. En d'autres termes, les taux d'erreur effectivement obtenus dans application réelle peuvent être beaucoup plus élevés si les conditions d'acquisition ou les conditions ambiantes sont fort différentes. Les intervalles de confiance ne représente que l'incertitude liée au fait que l'ensemble de données disponibles est fini [20].

Par définition, le taux de fausse acceptation T_A est le rapport du nombre d'imposteurs qui ont été acceptés et du nombre total de tentatives d'accès imposteurs N_b, c'est-à-dire

$$T_A = \frac{n_b}{N_b},$$

et de même pour le taux de faux rejet

$$T_R = \frac{n_a}{N_a}.$$

où n_a et N_a sont respectivement le nombre d'accès authentiques rejetés et N_b le nombre total d'accès authentiques. Ces nombres sont des estimées des probabilité de fausse acceptation e_A et de faux rejet e_R. Comme le raisonnement est identique pour les deux probabilités, nous continuons la discussion que dans le cas de la fausse acceptation. On peut montrer que le taux de fausse acceptation est distribué suivant une loi de probabilité binomiale $B(N_b, e_A)$ puisque chaque accès imposteur peut réussir avec une probabilité e_A [13]. La probabilité que le taux de fausse acceptation T_A prenne la valeur $\frac{k}{N_b}$ est donc donné par

$$\text{Prob}(T_A = \frac{k}{N_b}) = \left(\begin{array}{c} N_b \\ k \end{array} \right) e_A^k (1 - e_A)^{N_b - k}.$$

En utilisant les propriétés de la loi binomiale la moyenne du taux de fausse acceptation est

$$\text{E}[T_A] = e_A,$$

et la variance

$$\text{Var}[T_A] = \frac{e_A(1 - e_A)}{N_b},$$

ce qui montre que T_A converge vers e_A lorsque N_b tendvers l'infini.

Un intervalle de confiance est un intervalle $[a_\alpha,b_\alpha]$, calculé à partir du taux T_A estimé, qui comprend la valeur inconnue e_A avec une probabilité α, c'est-à-dire

$$\text{Prob}(a_\alpha < e_A < b_\alpha) = \alpha.$$

Lorsque N_b est suffisamment grand la loi binomiale peut être approchée par une distribution normale. On a donc

$$\frac{T_A - e_A}{\sqrt{(1-e_A)e_A/N_b}} \sim \mathcal{N}(0,1),$$

les bornes de l'intervalle sont donc [15]

$$\frac{1}{1+\epsilon^2/N_b}\left(T_A + \epsilon^2/2N_b \pm \epsilon\sqrt{T_A(1-T_A)/N_b + \epsilon/4N_b^2}\right). \tag{16}$$

Le paramètre ϵ satisfait la relation

$$\phi(\epsilon) = \int_{-\infty}^{\epsilon} \mathcal{N}(x;0,1)dx = \frac{\alpha+1}{2}.$$

où $\phi(x)$ est la fonction de répartition d'une variable normale. Pour un intervalle de confiance à 95%, on prend $\alpha = 0,95$ ce qui correspond à $\epsilon = 1,96$.

4.4.1 Hypothèses

Il faut noter que l'approche décrite ci-dessus ne fait pas d'hypothèse sur les distributions de scores. Par contre les accès imposteurs doivent être indépendants [15]. Si plusieurs signaux biométriques tests (empreintes digitales, images du visage, etc.) qui émanent de la même personne sont utilisés pour générer les scores imposteurs, ces scores ne reflèteront pas les variations liés à l'identité. Bien que souvent utilisés dans la pratique, ces scores ne seront pas indépendants, et il ne peuvent être pris en compte dans le calcul de l'intervalle de confiance ci-dessus. De même pour les scores authentiques : on obtient une meilleure estimée du taux de faux rejet si on utilise une seule mise en correspondance par paires de signaux biométriques tests emanant d'un grand nombre de personnes, plutôt qu'un grand nombre de mises en correspondance émanant d'un petit nombre de personnes.

Pour pouvoir utiliser la méthode ci-dessus, il faut aussi que les probabilités e_A et e_R soient constantes au sein de la population. Il semble que ceci ne soit pas toujours verifié. En effet il a été montré [3] que ces probabilités ne sont pas constantes dans le cas de la verification du locuteur. Certaines personnes sont systématiquement rejetés par le système, d'autres sont fréquemment acceptés alors qu'ils sont imposteurs.

Notons qu'une autre méthode d'estimation de l'intervalle de confiance est applicable aux taux d'erreur biométriques. Il s'agit de la méthode du *bootstrap* décrite dans [1].

5 Conclusion

Dans notre société où la place du virtuel est de plus en plus grande, il devient indispensable d'avoir des méthodes d'authentification d'identité qui soient à la

fois fiable, commode d'utilisation et qui respecte le principe de la protection de la vie privée. Bien que d'immenses progrès aient été faits ces dernières années, l'authentification biométrique est encore en pleine phase de développement. Plusieurs points cruciaux qui ne sont pas résolus freinent l'extension de la biométrie. Ces points ont été soulevés récemment lors d'un colloque sur l'authentification biométrique [6].

Premièrement, les performances actuelles des systèmes biométriques, en termes de taux d'erreur, sont insuffisantes pour qu'ils parviennent à remplacer dans tous les cas les moyens traditionnels d'authentification. En effet, dans une authentification biométrique il n'y a jamais de correspondance parfaite entre le gabarit et le signal mesuré comme dans le cas du mot de passe. Le signal biométrique est *toujours* bruité.

Deuxièmement, les tests effectués sur le terrain ont presque toujours été faits à petite échelle. Il est très difficile de prévoir le comportement des systèmes biométriques à l'echelle nationale, voire même trans-nationale comme dans le cas de l'Union Européenne, où il est question de millions de signaux biométriques à gérer.

Enfin, il existe une réticence chez les utilisateurs concernant la protection de la vie privée. En effet, puisque la biométrie offre une preuve irréfutable d'identité, comment être sûr et comment persuader l'utilisateur que cette information n'est pas utilisée à des fins qui transgressent les règles de la protection de la vie privée. Une direction prometteuse de recherche, qui tend à résoudre ce type de problème, concerne les systèmes cryptographiques biométriques où des clés cryptographiques sont crées à partir de données biométriques.

Références

[1] R. Bolle, S. Pankanti, and N. Ratha. Evaluation techniques for biometrics-based authentication systems. In *Proceeding of the International Conference on Pattern Recognition (ICPR)*, 2000.

[2] J. Daugman. High confidence visual recognition of statistical independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 15(11) :1148–1161, 1993.

[3] G. Doddington, W. Liggett, A. Martin, M. Przybocki, and D. Reynolds. 'sheep, goats, lambs and wolves' : a statistical analysis of speaker performance in the NIST 1998 speaker recognition evaluation. In *Proceedings of the International Conference on Spoken Language Processing*, 1998.

[4] R. Duda, P. Hart, and D. Stork. *Pattern classification, second edition.* Wiley-Interscience, 2001.

[5] G. Hachez, F. Koeune, and J.-J. Quisquater. Biometrics, access control, smart cards : a not so simple combination. In *Conference on Smart Card Research and Advanced Applications (CARDIS 2000)*, pages 273–288, September 2000.

[6] A. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross, and J. Wayman. Biometrics : a grand challenge. In *Proc. of the International Conference on Pattern Recognition*, 2004.

[7] A. K. Jain, R. Bolle, and R. Pankanti. Introduction to biometrics. In A. K. Jain, R. Bolle, and R. Pankanti, editors, *Biometrics : personal identification in a networked society*, pages 1–43. Kluwer academic publisher, 1999.

[8] J. Kittler, M. Hatef, R. P. W. Duin, and J. Matas. On combining classifiers. *IEEE Trans. on Pattern Recognition and Machine Intelligence*, 20(3) :226–239, 1998.

[9] M. Lades, J. C. Vorbrüggen, J. Buhmann, J. Lange, C. von der Malsburg, R. P. Würtz, and W. Konen. Distortion invariant object recognition in the dynamic link architecture. *IEEE Transactions on Computers*, 42(3) :300–311, Mar. 1993.

[10] K. Messer, J. Kittler, M. Sadeghi, M. Hamouz, A. Kostin, F. Cardinaux, S. Marcel, S. Bengio, C. Sanderson, J. Czyz, L. Vandendorpe, C. McCool, S. Lowther, S. Sridharan, V. C. andRoberto Parades Palacios, E. V. andLi Bai, L. Shen, Y. Wang, C. Yueh-Hsuan, L. Hsien-Chang, Y.-P. Hung, A. Heinrichs, M. Muller, A. Tewes, C. von der Malsburg, R. P. Wurtz, Z. Wang, F. Xue, Y. Ma, Q. Yang, C. Fang, X. Ding, S. Lucey, R. Goss, H. Schneiderman, N. Poh, and Y. Rodriguez. Face authentication test on the banca database. In *Proceedings of International Conference on Pattern Recognition*, 2004.

[11] K. Messer, J. Matas, J. Kittler, J. Luettin, and G. Maitre. XM2VTSDB : the extended M2VTS database. In *Proc. of Int. Conf. on Audio- and Video-based Person Authentication*, pages 72–77, March 1999.

[12] L. O'Gorman. Fingerprint verification. In A. K. Jain, R. Bolle, and R. Pankanti, editors, *Biometrics : personal identification in a networked society*, pages 43–64. Kluwer academic publisher, 1999.

[13] A. Papoulis. *Probability, Random Variables and Stochastics Processes*. McGraw-Hill, 1965.

[14] M. Przybocki and A. Martin. NIST's assessment of text independent speaker recognition performance. In *The Advent of Biometircs on the Internet, A COST 275 Workshop in Rome, Italy*, 2002.

[15] V. Pugachev. *Théorie des probabilités et statistique mathématique*. Editions de Moscou, 1982.

[16] D. A. Reynolds and R. C. Rose. Robust text-independent speaker identification using gaussian mixture speaker models. *IEEE trans. on Speech and Audio Processing*, 3(1) :72–83, 1995.

[17] A. Ross, A. K. Jain, and J.-Z. Qian. Information fusion in Biometrics. In *Proc. Int. Conf. on Audio- and Video-based Person Authentication*, pages 355–359, 2001.

[18] M. Turk and A. Pentland. Eigenfaces for recognition. *Journal of cognitive neuroscience*, 3(1), 1991.

[19] H. VanTrees. *Detection, Estimation and Modulation Theory*. Wiley, 1968.

[20] J. Wayman. Confidence interval and test size estimation for biometric data. In *Proceedings of IEEE AutoID conference*, 1999.