REE REVUE DE L'ÉLECTRICITÉ ET DE L'ÉLECTRONIQUE

La biométrie aujourd'hui : du rêve à la réalité

Bernadette Dorizzi
Professeur Emérite, Télécom SudParis

La biométrie s'immisce dans notre quotidien suscitant intérêt pour notre sécurité et crainte pour nos libertés. Cet article propose un panorama des principales techniques ainsi que des enjeux actuels.

Introduction

Systèmes de suivi facial de la population en Chine mais aussi en Europe, téléphones portables déverrouillés par le doigt ou le visage, passeport biométrique, contrôle d'identité aux frontières, la biométrie s'immisce dans notre quotidien suscitant intérêt pour notre sécurité et crainte pour nos libertés.

C'est à la fin du 19e siècle qu'est mis en place le premier laboratoire de police d'identification criminelle basé sur «le bertillonnage» du nom de son inventeur Alphonse Bertillon. Il s'agit de repérer les individus «recherchés» grâce à la mesure d'un certain nombre de leurs caractéristiques personnelles (anthropométrie judiciaire). On y ajoute bientôt aussi les portraits de face et profil et les empreintes digitales. C'est ainsi que naît l'idée de biométrie (mesure du vivant) pour caractériser un individu.

Aujourd'hui le terme biométrie renvoie à des techniques qui veillent à vérifier l'identité d'un individu par ce qu'il est, c'est-à-dire en utilisant des caractéristiques physiques (telles les empreintes digitales, l'iris de l'œil, le visage) ou comportementales ●●●

" L'identification peut être une tâche très difficile lorsque la base de données contient des milliers d'individus. Les problèmes de temps d'accès deviennent alors cruciaux, c'est pourquoi on utilise des algorithmes d'indexation ou de hachage de la base de données. "

(signature, démarche, frappe au clavier), acquises via des capteurs. Les applications visées dépassent le seul cadre policier et sécuritaire même si celles-ci restent prégnantes [1].

L'essor actuel de la biométrie vient de l'explosion du monde numérique et des capacités de traitement rapide des données qui en découlent. Il est en effet possible aujourd'hui de numériser, stocker, traiter, comparer des données biométriques dans des temps éclair et avec des performances satisfaisantes ce qui permet de parler de déploiements biométriques à grande échelle.

Aujourd'hui divers systèmes sont déployés largement pour les modalités les plus usuelles : empreintes digitales, visages, iris, tandis que l'exploration des biométries comportementales est encore en cours d'étude et de validation (marche, frappe au clavier…).

Les défis qui se posent aujourd'hui pour ces systèmes sont nombreux : maintien d'une fiabilité importante pour une très grande population, robustesse aux attaques, sécurité globale des systèmes, assurance de la confidentialité des données personnelles.

Principes des systèmes biométriques

Fonctionnement

On distingue deux modes d'utilisation distincts d'un système biométrique. On peut vouloir identifier une personne parmi un ensemble composé de N individus. Plus N est grand, plus la tâche est difficile. C'est ainsi que fonctionne le système européen d'identification des visas qui utilise une base de données de plus de 70 millions d'empreintes digitales de tous les postulants à un visa de courte durée dans l'espace Schengen. Se développent aujourd'hui les applications de surveillance de foule, lorsque par exemple, on veut repérer un malfaiteur potentiel (à partir d'une liste de criminels identifiés) dans une foule (aéroport, terrain de football, grande surface…). Plus facile est la tâche qui consiste à vérifier l'identité d'une personne, encore appelée *authentification*. Ainsi, face à un individu qui se présente au guichet d'une banque ou à l'entrée d'un bâtiment et qui se prétend être un client répertorié, le système devra simplement prendre une décision d'acceptation ou de rejet de cette personne. Dans ce cas, il n'y a pas forcément besoin de stocker l'information relative à la personne dans une base centralisée. Celle-ci peut être enregistrée par exemple sur une carte à puce détenue par l'utilisateur, ce qui assure une meilleure confidentialité.

Architecture

En général, on répertorie deux phases dans un système biométrique, une phase d'apprentissage, appelée aussi enregistrement, et une phase de reconnaissance, ou vérification. Dans tous les cas, la modalité considérée (par exemple, l'empreinte digitale ou l'iris) est enregistrée à l'aide d'un capteur et des données numériques sont alors disponibles (un tableau de pixels, un signal numérique...). En général, on ne travaille pas directement sur ces données mais on en extrait d'abord des caractéristiques pertinentes, qui constituent un gabarit. Cela présente un double intérêt : le volume d'informations à sauvegarder est plus restreint et l'anonymat dans le stockage de ces données est favorisé. En effet, à partir de ces caractéristiques, il n'est *a priori* pas possible de revenir au signal original.

Le rôle du module d'apprentissage est de constituer un modèle d'une personne donnée à partir d'un ou de plusieurs enregistrements (références) de la modalité considérée. La plupart des modèles rencontrés sont des modèles statistiques qui permettent de prendre en compte une certaine variabilité dans les données individuelles.

Le module de reconnaissance permet de prendre une décision qui est toujours basée sur une mesure de similitude. Si l'on est en mode identification, le système compare le signal mesuré avec les différents modèles contenus dans la base de données et sélectionne le plus proche ou fournit une liste ordonnée de candidats possibles. En mode vérification, le système compare le signal mesuré avec un seul des modèles de la base de données et autorise ainsi la personne ou la rejette en fonction d'un seuil de décision.

L'identification peut être une tâche très difficile lorsque la base de données contient des milliers d'individus. Les problèmes de temps d'accès deviennent alors cruciaux, c'est pourquoi on utilise des algorithmes d'indexation ou de hachage de la base de données.

Erreur associée à un système biométrique

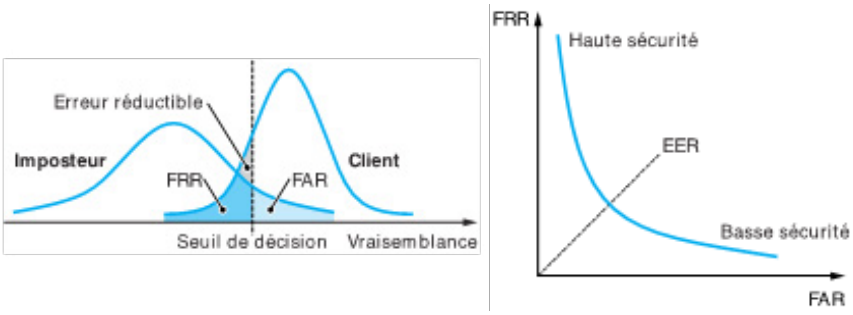
Les systèmes biométriques, contrairement aux codes pin ou mots de passe, font des erreurs. Ceci est dû à une variabilité qui vient soit de la personne elle-même ; par exemple si elle change de coiffure, de lunettes ou si elle se coupe la barbe, les images de visages sont différentes. De plus, selon l'humeur, la fatigue, l'émotion, une personne ne se comporte pas de la même manière, ce qui a un impact sur les biométries comportementales telles que la frappe au clavier, la marche, la signature. Enfin les environnements d'acquisition peuvent varier entre la prise de références et de test (effets d'éclairage sur

les visages, bruit dans la reconnaissance vocale, réflexions sur les images de l'iris) ainsi que les capteurs utilisés.

Dans le cas d'un système de vérification, on évalue deux taux d'erreur qui varient en sens contraire : le taux de faux rejet FRR (*False Rejection Rate* : taux de rejet d'un utilisateur légitime) et le taux de fausse acceptation FAR (*False Acceptation Rate* : taux d'acceptation d'un imposteur). Étant donné un système de vérification, la figure 1 (gauche) représente la distribution théorique des taux de vraisemblance (similarité) des utilisateurs légitimes et des imposteurs. Les FAR et FRR sont alors représentés en fonction d'un seuil qui devra être ajusté en fonction des caractéristiques souhaitées pour l'application considérée (haute ou basse sécurité). En effet, plus le seuil est bas, plus le système acceptera d'imposteurs. Plus il est élevé, plus le système sera robuste aux imposteurs mais il rejettera alors plus de vrais utilisateurs. Chaque application nécessite de recalculer ce seuil pour l'adapter à la population spécifique considérée.

La courbe ROC (*Receiver Operating Curve*) de la figure 1 (droite) permet de représenter la performance d'un système de vérification en termes de couples (FAR, FRR) en fonction des différentes valeurs possibles du seuil. Le taux d'erreur égale EER (*Equal Error Rate*) correspond au point FAR = FRR et est souvent utilisé pour mesurer la performance du système.

Au-delà de la performance des systèmes, d'autres facteurs interviennent lors de la mise en œuvre d'un système biométrique. Citons tout d'abord la qualité et la robustesse des capteurs utilisés. Il est assez évident que la qualité des capteurs influe sur les performances des algorithmes de reconnaissance associés. C'est pourquoi on peut être amené à évaluer la résistance d'un algorithme de reconnaissance à l'utilisation de différents types de capteurs (problème d'interopérabilité). Un autre facteur déterminant de l'acceptabilité d'une solution biométrique est la qualité de l'interface de communication



I Figure 1 : (gauche) Distribution théorique des taux de vraisemblance des utilisateurs légitimes et des imposteurs ; (droite) Courbe ROC d'un système biométrique.

associée. Outre le confort d'utilisation, la vitesse d'acquisition et la rapidité du traitement sont des facteurs déterminants, bien souvent non évalués en pratique.

Progrès récents dans l'étape d'extraction des caractéristiques

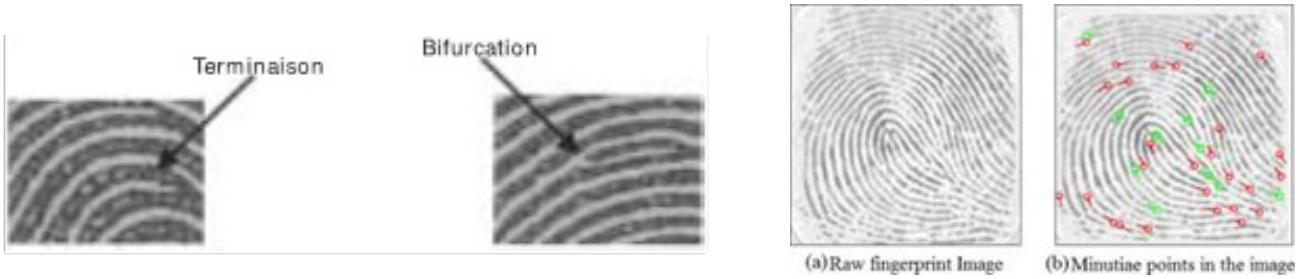
L'apparition des réseaux de neurones profonds (*deep networks*) dans le domaine de l'apprentissage machine a révolutionné la conception des systèmes de reconnaissance des formes. En effet un tel système se compose classiquement de 2 étapes distinctes : une étape d'extraction de caractéristiques suivie d'une étape de classification résultant ou pas d'un calcul de similarité. Traditionnellement la phase d'extraction des caractéristiques était réalisée grâce à une connaissance experte sur les données et leur nature, en utilisant des algorithmes d'analyse d'images qui sont déterministes et qui reposent sur des concepts mathématiques. Les architectures de réseaux de neurones profonds remettent en cause ce schéma puisqu'elles permettent en même temps d'extraire les caractéristiques et de les classer grâce à un apprentissage sur des données étiquetées en nombre important. Il est alors possible de visualiser après apprentissage les caractéristiques générées (en général sur les dernières couches du réseau de neurones).

Les systèmes biométriques n'échappent pas à cette tendance. C'est particulièrement flagrant pour la reconnaissance par le visage mais ces modèles sont aussi utilisés pour la reconnaissance et la segmentation de l'iris ou les empreintes digitales.

Dans le cas de l'identification, on utilise en général la technique de «*transfer learning*» qui permet d'utiliser les paramètres d'un réseau déjà entraîné comme point de départ pour une phase d'optimisation complémentaire réalisée à l'aide d'une base d'exemples spécifiques du problème à traiter.

Pour la vérification, les architectures de réseaux profonds servent à extraire des caractéristiques pertinentes et sont associées à des fonctions de coût particulières. Le modèle est entraîné de manière à optimiser le rapprochement des exemples d'une personne donnée et l'éloignement des exemples de personnes différentes et ceci pour l'ensemble des personnes. Finalement le système de décision utilise la dernière couche du réseau comme mesure de similarité/dissimilarité pour prendre la décision de rejet ou acceptation.

"L'apparition des réseaux de neurones profonds (*deep networks*) dans le domaine de l'apprentissage machine a révolutionné la conception des systèmes de reconnaissance des formes."



I Figure 2 : Minuties extraites d'une empreinte digitale.

Les différentes modalités

Il existe aujourd'hui une panoplie assez large de modalités biométriques et il en apparaît constamment de nouvelles. En fait, aucune modalité ne permet d'assurer à la fois une précision suffisante et un confort d'utilisation et cela dans toutes les situations d'usage. De plus, quelle que soit la modalité, il existe toujours des personnes réfractaires (mains usées de travailleurs manuels, visages voilés, voix enrouées). Jusqu'à récemment, l'empreinte digitale était considérée comme ayant le meilleur compromis en termes de performance et de coût, ce qui expliquait son déploiement dans de nombreuses applications. Aujourd'hui on voit l'essor de la vérification par le visage, modalité jusqu'alors considérée comme trop variable pour donner des performances acceptables. Les progrès récents sont dus à l'existence de grandes bases de données et à l'utilisation de techniques de «*deep networks*» qui ont permis des progrès spectaculaires dans le domaine du traitement des images en général.

Nous ne décrivons ici succinctement que les modalités les plus communes, à savoir le visage, les empreintes digitales, l'iris de l'œil, laissant de côté d'autres modalités moins classiques (veines de la main, ADN, odeur corporelle, forme de l'oreille, rythme de frappe sur le clavier, démarche...).

Empreintes digitales

L'empreinte digitale est utilisée depuis un siècle pour l'identification criminelle depuis que Francis Galton découvrit la permanence et l'inaltérabilité du dessin papillaire de la naissance à la mort. Elle correspond à l'essentiel du marché actuel même si elle a tendance à être détrônée par le visage. Elle possède un taux de fiabilité suffisant pour permettre d'identifier les individus dans de grandes bases de données. Utilisée depuis longtemps dans le contexte policier, elle n'est pas toujours très bien acceptée par les utilisateurs mais présente néanmoins un bon compromis entre les contraintes d'utilisation et la fiabilité recherchée. Elle est constituée par les dessins des crêtes et des vallées de la peau des doigts dans des orientations particulières. Le motif obtenu présente également des variations limitées permettant d'opérer une classification.

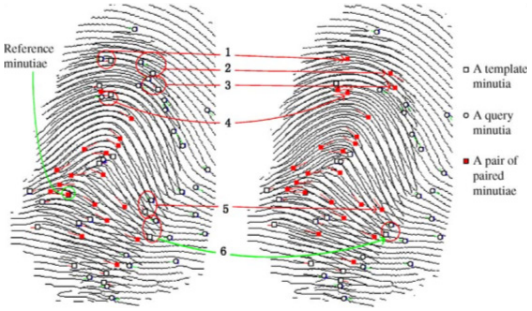
A la base, une empreinte présente des crêtes et des vallées. Pour permettre les traitements de comparaison, l'objectif est de repérer des caractéristiques particulières appelées minuties, consistant en terminaisons ou bifurcations de crêtes (figure 2).

Chaque empreinte est ainsi caractérisée par la position et le type de ses minuties. On cherche également à trouver l'orientation locale (sous la forme d'un angle) du sillon sur lequel se trouve le point. L'extraction des minuties permet non seulement de caractériser efficacement une empreinte digitale mais aussi d'obtenir un condensé de l'empreinte occupant presque mille fois moins de place que l'image initiale. Plusieurs travaux récents proposent l'utilisation d'algorithmes de réseaux de neurones profonds pour extraire ces minuties avec des modèles qui couplent la connaissance experte a priori des minuties et la capacité de généralisation induite par l'apprentissage.

La comparaison entre deux empreintes (figure 3) repose sur un score qui mesure le taux d'appariement entre les minuties détectées sur les deux empreintes. La tâche est relativement complexe pour plusieurs raisons : certaines minuties peuvent manquer, l'image de l'empreinte peut avoir tourné ou avoir été translatée, de « fausses » minuties peuvent être apparues. On cherche à obtenir que l'implémentation réalisée accepte toutes les rotations du doigt sur le capteur et toutes les translations verticales et horizontales pourvu qu'il existe une surface commune à deux empreintes.

Vérification par le visage

Depuis son enfance, tout être humain a appris à reconnaître le visage des personnes qui l'entourent. C'est pourquoi cette modalité nous apparaît comme tout à fait naturelle, d'autant plus que des photos ornent nos documents d'identité. Différents types de caméras et d'appareils photo, de qualité et de coût variables, sont apparus sur le marché, permettant d'adapter la qualité des images aux conditions d'usage. L'essor du net, des réseaux sociaux, des téléphones mobiles a vu aussi la circulation de



I Figure 3 : Mise en correspondance des minuties de deux empreintes d'un même doigt.

myriades d'images de visages sur internet. Finalement la vidéosurveillance maintenant bien installée dans beaucoup de lieux publics ou privés pose la question de l'identification automatique des visages en résultant. C'est donc aujourd'hui la modalité biométrique qui pose le plus de questions sociétales.

Pourtant, ce n'est que récemment que les systèmes de vérification par le visage ont atteint des performances impressionnantes. C'est en effet l'essor des systèmes basés sur les réseaux profonds et les algorithmes tels Deepface [2] ou Facenet[3] (figures 4 et 5) qui permettent des taux de reconnaissance similaires voire supérieurs à l'humain. La force de ces systèmes vient de leur capacité à prendre en compte les fortes variabilités des images de visages : arrières-plan texturés, illumination, pose, lunettes, résolution. Ceci résulte de la disponibilité de bases de données présentant la plupart des variabilités possibles et de puissances de calcul hors normes qui permettent d'apprendre des modèles avec un nombre très important de paramètres. Ces modèles profonds permettent d'apprendre une représentation de l'ensemble des visages possibles, représentation ensuite optimisée pour mesurer la similitude de deux visages.

Dans la lignée de ces travaux pionniers, on observe aujourd'hui un nombre très important de publications sur ce domaine que ce soit pour améliorer encore les architectures et l'entraînement des modèles ou pour générer et labelliser automatiquement des données représentatives. Les systèmes sont en effet sujet à des biais dus à la constitution des bases de données et de ce fait, la question de l'éthique de la reconnaissance faciale est largement posée [4].

Photographie de l'iris

L'identification par l'iris est une technique relativement récente qui s'est développée dans les années 1980 grâce aux travaux de J. Daugman [5]. L'iris est la zone colorée visible entre le blanc de l'œil et la pupille. Les stries apparentes ainsi que leur répartition sont stables durant la vie de l'individu. L'iris

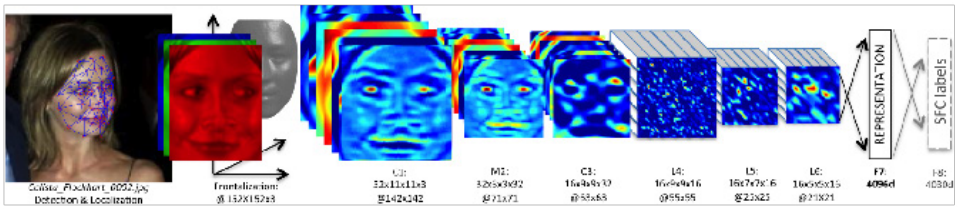


Figure 4 : Architecture du réseau Deepface (Facebook) pour reconnaître les visages. Chaque couche effectue différents filtrages sur les couches précédentes, résultant en une extraction efficace de caractéristiques pertinentes.

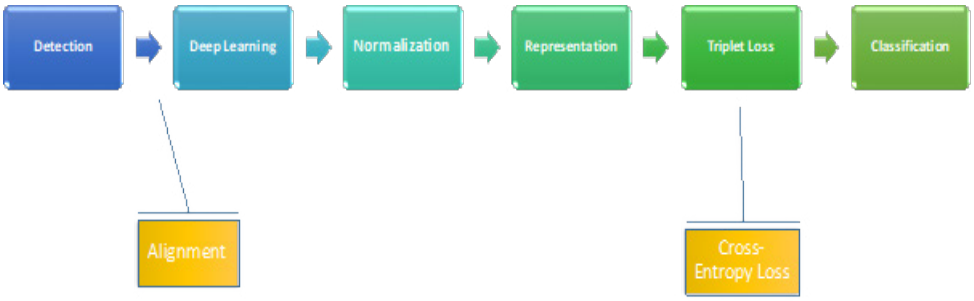


Figure 5 : Facenet (Google) utilise une fonction de coût nommée «triplet loss» pour optimiser les caractéristiques qui serviront à la classification des visages en client-imposteur.

n'est pas une modalité génétique : les deux iris d'un même individu ou de jumeaux sont différents. Bien que de dimension réduite (11 mm de diamètre), la texture de l'iris possède l'immense avantage de présenter une variabilité considérable entre tous les individus, c'est ce qui fait son intérêt pour la biométrie. Un système d'identification par l'iris comporte plusieurs étapes :

Acquisition : l'iris est de petite taille dans l'œil et caché derrière une surface réfléchissante, la cornée ; de ce fait la plupart des systèmes fonctionnent en lumière infrarouge de manière à obtenir une image de la texture de l'iris de bonne qualité ce qui est plus difficile en lumière visible.

La figure 6 présente des images d'iris acquises respectivement en lumière visible et infrarouge. On remarque la meilleure qualité de l'infrarouge (figure 6 droite).

Segmentation de l'iris dans l'image : il s'agit ici d'une étape délicate car l'iris doit être extrait du reste de l'image (pupille, cils et paupières) et du fait que d'une image à l'autre, on va devoir faire face à de fortes variabilités. Les travaux récents montrent un apport substantiel des techniques d'apprentissage profond pour cette tâche par rapport aux méthodes classiques de traitement d'image (transformée de Hough, contours actifs). ●●●

Figure 6 : Images d'un iris, à gauche caméra CCD, à droite caméra infrarouge.

Codage et normalisation : l'extraction des caractéristiques repose, après une normalisation de la zone de l'iris, sur un codage multi résolution de la texture par une transformée en ondelettes complexe. Seule l'information de phase est utilisée dans le codage de l'iris. L'information d'amplitude ne serait pas assez discriminante car trop dépendante de facteurs externes comme le contraste de l'image, l'illumination ou le gain de la caméra. Finalement l'iriscode résulte d'une quantification de la phase et correspond à une matrice de 2048 bits par exemple.

Comparaison des iriscodes : on utilise la distance de Hamming pour quantifier la différence, mesurée bit à bit, entre deux iriscodes. La simplicité des opérations booléennes à réaliser permet d'aboutir à des vitesses de traitement adaptées à la production de résultats obtenus très rapidement (quelques secondes) sur des bases de données de plusieurs centaines de milliers, voire de millions, d'individus.

Sécurité des systèmes biométriques

La détection d'attaques sur les systèmes biométriques est un sujet d'importance aujourd'hui. En effet alors que les systèmes biométriques étaient considérés comme LA solution sûre aux problèmes de falsification d'identité, un article de Matsumoto [6] en avril 2002 a fait beaucoup couler d'encre. Dans cet article, il a été montré que de fausses empreintes fabriquées à partir d'empreintes latentes récupérées sur des objets à l'insu de la personne pouvaient leurrer la plupart des systèmes de vérification de l'époque. De plus fabriquer de telles empreintes ne nécessite pas une expertise ni des matériaux rares ; de la gélatine suffit pour fabriquer un faux doigt.

Depuis les fabricants de systèmes rivalisent d'idées pour rendre leurs systèmes plus robustes à de telles attaques. Renforcer les algorithmes est difficile car détecter des faux veut dire risquer de ne pas reconnaître des vrais. L'idée est donc d'utiliser d'autres caractéristiques que celles qui servent à la vérification à proprement parler et qui ont trait par exemple à mesurer le caractère vivant du doigt (température) ou sa déformation sur une surface qui n'est pas la même pour la peau ou un doigt recouvert de latex.

Plus compliqué et plus cher est de rajouter d'autres capteurs ou d'autres modalités. IDEMIA par exemple propose un système qui analyse l'empreinte et les veines du doigt pour vérifier l'identité [7]. L'ensemble est acquis avec un seul capteur et permet de meilleures performances de reconnaissance, une meilleure résistance aux attaques mais à un coût plus important ce qui le limite à un marché de niche.

Il faut alors fabriquer des systèmes capables de distinguer une vraie empreinte d'une fausse. Aujourd'hui l'état de l'art repose sur des méthodes à base de réseaux profonds. A noter que le NIST organise régulièrement des compétitions pour qualifier les possibles systèmes en proposant des bases de données de taille conséquente. Ainsi les bases livDet dans le cas des empreintes existent depuis 2009, et sont disponibles comme benchmark de référence pour la communauté scientifique. De ces évaluations il ressort que la qualité des faux et leurs techniques de fabrication ont une très grande importance sur les performances des contre-attaques.

Nous avons déjà dit que l'usage du visage en biométrie prend une place de plus en plus importante. Or il se trouve que cette modalité est relativement facile à falsifier.

En effet, du fait de la disponibilité d'images de visage sur de larges échelles (réseaux sociaux, internet), il est très facile de se procurer des images du visage de «n'importe qui», et de se les approprier pour

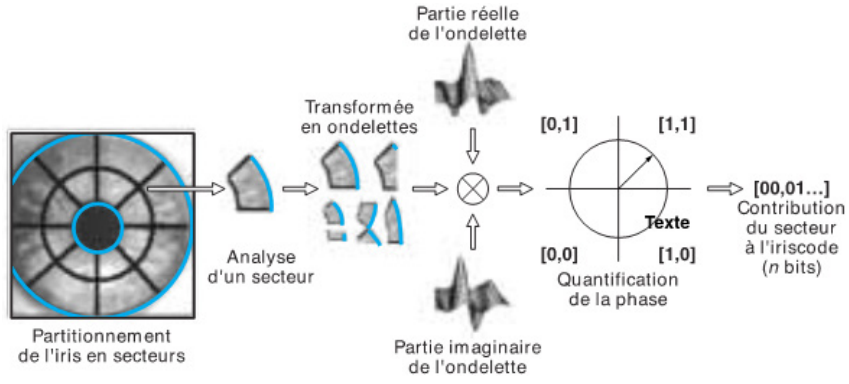


Figure 7 : Chaîne de traitement de l'iris (d'après [1]).

L'auteur

Bernadette Dorizzi est professeur émérite à Télécom SudParis, école qu'elle a rejoint en 1989 et où elle a été directrice du département Electronique et Physique puis directrice de la recherche et des formations doctorales. Diplômée de l'Ecole normale supérieure, elle a obtenu l'agrégation en mathématiques en 1978 et sa thèse d'Etat en physique théorique à l'Université Paris XI à Orsay en 1983, sur l'étude de l'intégrabilité des systèmes dynamiques. Dans le domaine de la reconnaissance des formes et de l'apprentissage automatique, elle est spécialiste de biométrie et a notamment coordonné le réseau d'excellence européen BioSecure (Biometrics for Secure Authentication). Ses recherches ont été publiées dans plus de 230 revues internationales et elle a supervisé plus de 20 doctorats.

tromper un système. Certains attaquants utilisent des masques 3D pour reproduire forme et texture.

Une attaque difficile à détecter correspond au «morphing». Il est de plus en plus facile de permuter automatiquement les visages dans les images et les vidéos ou de transformer deux visages différents en un seul, virtuel, en utilisant des techniques de réseaux de neurone profond adverses (GAN).La haute qualité de l'image générée soulève la question de la vulnérabilité des systèmes de reconnaissance faciale à de telles images et vidéos fausses. Il a été montré [8] que les systèmes récents de reconnaissance par le visage (tels VGG Net ou FaceNet) sont très vulnérables aux vidéos de morphing profond, avec des taux de fausse acceptation de l'ordre de 90 %, ce qui implique que des méthodes de détection *a priori* de ces vidéos sont nécessaires. C'est ce à quoi s'attaquent aujourd'hui les chercheurs du domaine.

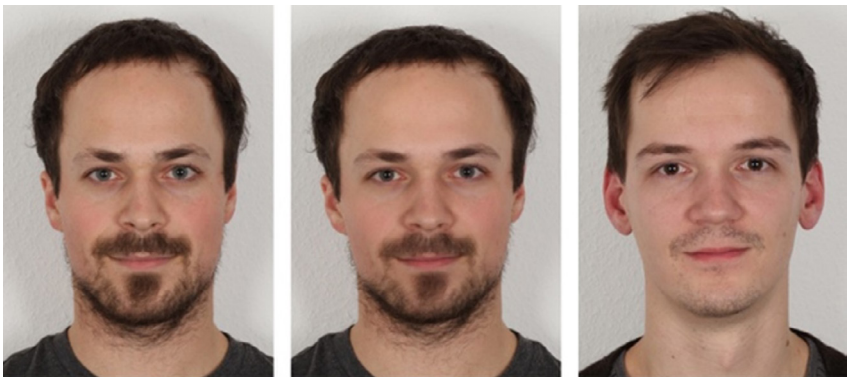


Figure 8 : Les deux visages de droite et de gauche sont transformés par algorithme de «morphing» dans l'image centrale.

Conclusion

Même si de larges déploiements de la biométrie sont en cours comme le projet Aadhaar de recensement de la population en Inde ou la délivrance de carte nationale d'identité en France ce qui dénote une maturité des technologies, l'acceptation de la biométrie en Europe passera par une meilleure sécurisation des systèmes et surtout, dans un contexte de réglementation européenne des données personnelles (RGPD), par la garantie pour chaque individu que ses données biométriques sont bien traitées. La question de la vérification par les visages et des possibles dérives associées à une large utilisation de vidéos comme moyen de sécuriser des lieux publics constitue d'ailleurs à ce jour un enjeu citoyen majeur. ■

Résumé

Dans cet article nous présentons les principes à la base de tout système de reconnaissance biométrique d'identité : architecture, mode de fonctionnement, mesures de performance, puis nous décrivons succinctement 3 modalités biométriques utilisées dans les systèmes déployés à grande échelle : empreintes digitales, visage et iris en mettant en exergue leurs avancées récentes. Finalement, nous discutons les aspects de sécurité (résistance aux attaques), qui prennent de plus en plus d'importance dans la conception et l'acceptation des systèmes. ■

Abstract

In this article we present the principles underlying any biometric identity recognition system: architecture, mode of operation, performance measurements, then we briefly describe 3 biometric modalities used in systems deployed on a large scale: fingerprints, face and iris by highlighting their recent advances. Finally, we discuss the security aspects (resistance to attacks), which are becoming increasingly important in the design and acceptance of systems. ■

Références

[1] B. Dorizzi, J. Leroux Les Jardins, Ph. Lamadelaine, C. Guerrier, «La biométrie - Techniques et usages», Techniques de l'Ingénieur, Avril 2004
[2] Y. Taigman, M. Yang, Marc'Aurelio Ranzato, L. Wolf, DeepFace: Closing the Gap to Human-Level Performance in Face Verification, 2014 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)
[3] F. Schroff, D. Kalenichenko and J. Philbin, «FaceNet: A unified embedding for face recognition and clustering,» 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, 2015, pp. 815-823, doi: 10.1109/CVPR.2015.7298682.
[4] Richard Van Noorden, «The ethical questions that haunt facial-recognition research», NATURE-NEWS FEATURE, 18 NOVEMBER 2020[5] J. Daugman, «How Iris Recognition Works», ieee transactions on circuits and systems for video technology, vol. 14, no. 1, january 2004
[6] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems," Electronic imaging, International society for optics and photonics, pp 275-289, 2002.
[7] Morphosmart : https://www.biotime-technology.com/capteurs-biometriques/morphosmart-cbm-oem/
[8] Pavel Korshunov, Sébastien Marcel, Vulnerability of Face Recognition to Deep Morphing, arXiv:1910.01933