La biométrie par reconnaissance faciale

Wéry Benoît
ECAM - 1e Master Informatique
1200 Bruxelles, Belgique
20 décembre 2017

ABSTRACT

A travers cet article seront passés en revue le concept de biométrie et l'une de ses techniques les plus courante : la reconnaissance de visage.
Les notions élémentaires de biométrie seront expliquées pour mieux comprendre le contexte dans lequel s'inscrit le processus de reconnaissance et différentes méthodes seront ensuite brièvement présentées pour mettre en avant les nombreuses possibilités de traitement d'une image contenant un visage ainsi que l'usage de la reconnaissance faciale dans notre quotidien.

1. INTRODUCTION

Si la reconnaissance de visages est une tâche complètement anodine pour le cerveau humain, il n'en va pas de même pour les systèmes informatiques. Bien au contraire, ce processus s'avère être un réel défi technologique mélangeant techniques de captures d'images et algorithmes de traitements.
Pourtant, la reconnaissance faciale automatique est un très appréciée en tant que technique biométrique et utilisée dans de nombreuses applications. C'est pourquoi, depuis la fin des années 1970, les travaux de recherches ont permis de mettre au point de nouvelles méthodes qui se sont succédées et améliorées avec le temps pour passer de simples processus de traitement 2D à des systèmes capables d'analyser un visage en 3D et en temps réel, le tout dans des sysètmes de plus en plus miniaturisés.

.

Alors, quelle est la place de la reconnaissance faciale par rapport aux différentes techniques biométriques existantes ? Quelles sont les méthodes les plus connues et quelles applications futures peut-on envisager ?
C'est ce que nous tenterons de dévourir à travers cet article.

.

Dans un premier, la notion de biométrie sera expliquée ainsi que le fonctionnement général des systèmes biométriques. On verra également pourquoi l'utilisation des caractéristiques de l'être humain est interressante pour améliorer les aspects de sécurité d'un système.
Ensuite, la reconnaissance faciale sera présentée en suivant la logique de ses trois étapes caractéristiques : la *détection*, la *normalisation* et la *reconnaissance 2D et 3D*.
Enfin, deux exemples seront présentés pour mettre en avant des cas d'utilisation différents des systèmes biométriques par reconnaissance de visage, à savoir : la détection et l'authentification.

2. LA BIOMÉTRIE

La biométrie, qui signifie "mesure du vivant", désigne dans notre contexte *"l'ensemble des procédés de reconnaissance d'une personne par certaines de ses caractéristiques physiques ou comportementales"*.[1]. Il s'agit donc d'utiliser des informations, telles que : l'empreinte digitale, l'iris, le visage, la démarche, ... afin de pouvoir identifier ou confirmer l'identité d'un sujet humain.

2.1 Systèmes biométriques

Un système biométrique fonctionne sur la comparaison de deux fichiers, issus de données biométriques, afin de déterminer leur taux de similitude.
Dans un tel système, une première phase dite d'*enrôlement* permet de récupérer la donnée et de l'enregistrer de façon numérique en BDD sous forme d'un modèle mathématique, que l'on appelle *"signature"* ou *"gabarit"*. On distingue ensuite deux modes de comparaison des modèles (voir 3.5) :

- l'AUTHENTIFICATION - comparaison 1 :1
- l'IDENTIFICATION - comparaison 1 :N

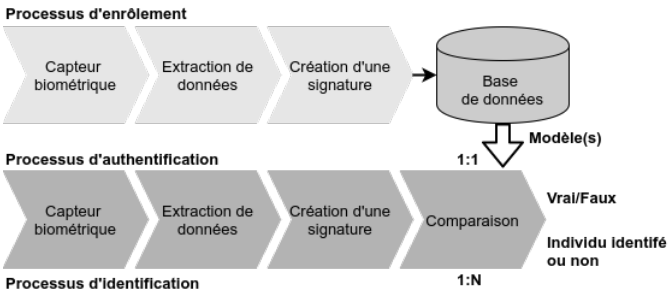

Figure 1: Modules d'un système biométrique

2.2 Aspects sécurité

Les systèmes biométriques sont particulièrement appréciés pour augmenter la sécurité des processus de vérification.
En effet, un code PIN ou un mot de passe peuvent être facilement trouvés selon leur niveau de complexité. Les données biométriques, quant à elles, présentent les avantages suivants, elles sont : universelles, uniques, invariables, enregistrables et mesurables.
Ainsi, leur utilisation complique le piratage ainsi que l'usurpation d'identité. De plus, un système biométrique ne né-

cessite plus de retenir un code. Pour ces raisons, ils sont de plus en plus utilisés dans les processus qui nécessitent la vérification de l'utilisateur.

2.3 Critères de performances et comparaison des technologies

Les éléments essentiels qui déterminent la qualité d'un tel système sont : la *donnée*, le *capteur* - nécessité d'obtenir un modèle analysable de bonne résolution - et les *algorithmes* (détection, analyse, comparaison).

.

Toutes les caractéristiques biométriques exploitables ne se valent pas mais elles peuvent être comparées selon différents critères tels que : l'*intrusivité*, la *fiabilité*, le *coût* ou encore l'*effort* (contribution du sujet lors de son analyse).

.

Ainsi, par exemple, si les empreintes digitales et l'iris sont meilleures que la reconnaissance du visage en termes de performances, cette dernière technique, quant à elle, est jugée moins intrusive et moins contraignante pour l'utilisateur. En effet, elle ne nécessite pas la coopération du sujet car il peut être identifié à distance. De plus les capteurs utilisés peuvent être relativement bons marché, puisqu'il s'agit dans le plus simple des cas d'un appareil photo ou d'une caméra.
Néanmoins, comme nous allons le voir, la reconnaissance faciale est sujette à diverses contraintes qui compliquent l'obtention d'une information de qualité et son analyse.

2.4 Evaluation de la fiabilité

Comme cela a été dit, un système biométrique évalue le taux de similitude entre deux modèles pour authentifer un individu. Or, il est impossible d'obtenir une coïncidence de 100% entre deux signatures. Dès lors, il faut fixer des seuils d'acception, qui permettent de quantifier les performances d'un système selon les facteurs suivants [2] :

- TFR - Taux de Faux Rejets : pourcentage d'individus rejetés alors qu'ils devraient être acceptés
- TFA - Taux de Fausses Acceptation : pourcentage d'individus acceptés alors qu'ils devraient être rejetés
- TEE - Taux d'Egale Erreur : point d'équivalence des erreurs. Il s'agit de l'intersection des deux autres courbes, qui est utilisée pour mesurer la performance de l'algorithme.

(voir annexe A pour les courbes)

3. LA RECONNAISSANCE FACIALE

La reconnaissance faciale est une des techniques utilisables dans les systèmes biométriques d'authentification *(ex : contrôle d'accès)* ou d'identification *(ex : surveillance d'un lieu)*.
Plusieurs méthodes peuvent être appréhendées pour la capture de l'image, cela va dépendre principalement du contexte : il peut s'agir d'un système statique ou bien dynamique, d'une reconnaissance 2D ou 3D, ... Les capteurs de l'information et les algorithmes doivent être choisis en conséquence.

3.1 Détection de visage

Après avoir capturé la donnée à analyser, dans ce cas-ci une image ou une vidéo, la première étape consiste à en extraire l'information utile. Plusieurs méthodes permettent de détecter des visages dans une image, elles peuvent être regroupées en quatre catégories [3]

1. *Knowledge-based methods* : basées sur la connaissance des éléments caractéristiques d'un visage (*nez, bouche, yeux,...*) et des relations entre eux, pour déterminer si les positions relatives décrivent un visage ou non. Malheureusement, ces techniques ont un faible taux de détection.
2. *Feature invariant approaches* : basées sur des éléments invariants tels la signature de couleur de la peau ou les caractéristiques du visages. Un algorithme classique est celui de *De Silva* qui consiste à trouver l'axe des yeux et utiliser ensuite comme référence la longueur entre le haut du visage et le plan de l'oeil.
3. *Template matching methods* : basées sur l'utilisation de templates, pour calculer la corrélation entre l'image candidate et un template. Un modèle est défini à partir d'un certains nombre de relations "essentielles" et "de confirmation". Un visage est alors localisé lorsque le nombre de relations détectées dépassent un certains seuil.
4. *Appearance-based methods* : basées sur la connaissance de modèles obtenus par apprentissage automatique. On retrouve ici un algorithme fréquemment utilisé, celui de *Viola et Jones*, qui utilise un nombre considérable de modèles exemples, représentants la variabilité de l'aspect facial. Il analyse l'image de façon itérative, en agrandissant sa fenêtre de recherche en pixels, pour y retrouver des visages.

.

Plusieurs difficultés se présentent lors de cette étape et compliquent la localisation du visage. En effet, les conditions de capture de l'image peuvent varier, les éléments suivants rentrent donc en compte :

- la *pose* : fait varier l'orientation du visage
- les *occultations* : le visage peut être partiellement ou complètement caché par certains objets
- les *expressions faciales* : engendrent la déformation du visage et donc des variations de posistions des éléments caractéristiques
- la *luminosité* : les conditions d'éclairage et les ombres qui en résultent peuvent affecter l'aspect du visage.
- la *présence ou absence de composantes structurales* : telles que la barbe, la moustache, les lunettes,...

3.2 Prétraitement ou normalisation

Une fois le visage détecté dans l'image, l'étape de prétraitement va permettre de rendre cette photo exploitable en la ramenant à un format prédéfini. Ainsi, toutes les images auront une taille, une échelle et des couleurs normalisées, ce qui est essentiel pour garantir les performances de la reconnaissance [3].
Deux processus sont importants pour préparer l'image :

1. normalisation GÉOMÉTRIQUE : permet de positionner et redimensionner la taille du visage
2. normalisation PHOTOMÉTRIQUE : consiste à jouer sur les niveaux de l'illumination du visage, par exemple, en augmentant les nuances pour améliorer le contraste.

3.3 Reconnaissance 2D

L'étape de reconnaissance permet d'extraire de l'image les informations qui serviront à la création d'une signature numérique et, par la suite, la comparaison avec les modèles

en BDD. Les techniques qui permettent la reconnaissance de données à partir d'une image 2D peuvent être regroupées en trois familles [4]

1. Approches **globales** : le visage tout entier est utilisé et représenté par un vecteur de grande dimension.
   L'avantage de ces méthodes est qu'elles permettent de conserver toutes les informations du visage et peuvent donc tenir compte des aspects de l'organisation globale de celui-ci.
   Cependant, elles utilisent uniquement des images 2D, qui sont d'autant plus sensibles au critères cités précédemment (*pose, illumination, expression,...*), et l'espace occupé par ces vecteurs est assez contraignant.

   .
   Il est alors possible d'utiliser des techniques de réduction de la dimension, telles que :
   - ***A**nalyse en **C**omposantes **P**rincipales (ACP)* : dont une des méthodes les plus connues est l'*Eigenfaces* qui calcule les propriétés du visage à partir de combinaisons de vecteurs propres issus des modèles dans différentes nuances de gris.
   - ***A**nalyse **D**iscriminante **L**inéaire (ADL)*
2. Approches **locales** : le visage est ici représenté par un ensemble de vecteurs de dimensions plus faibles. Il existe deux grandes catégories de techniques :
   - *basées sur les point d'intérêts* : consistent à identifier des points particuliers du visage pour ensuite en déterminer les caractéristiques. Une méthode reconnue est l'***E**lastic **B**unch **G**raph **M**atching (EBGM)* qui consiste à créer un réseaux pour modéliser les relations entre les points d'intérêts. On obtient ainsi un graphe topologique (fig **??**).
   - *basées sur l'apparence du visage* : le visage est divisé en plus petites régions, desquelles on extrait les caractéristiques locales.
3. Approches **hybrides** : techniques qui utilisent les caratéristiques locales et globales.

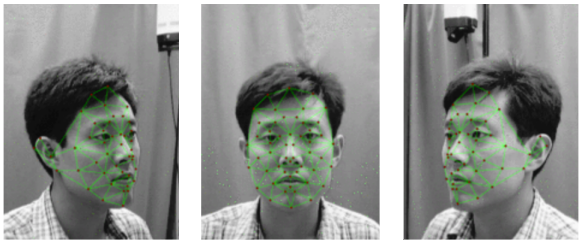

Figure 2: Graphe topologique par EBGM [5]

De manière générale, les méthodes locales sont plus performantes et surtout moins sensibles aux changements de l'environnement, qui surviennent lors de la capture d'image (voir appendice B).

3.4 Reconnaissance 3D

Contrairement aux techniques 2D qui viennent d'être présentées, les technologies de reconnaissance 3D permettent d'introduire la notion de *profondeur* dans les images analysées. De telles techniques sont en plein essors et très prometteuses quant à leurs performances.

Si les méthodes de reconnaissance sont différentes de la 2D, il en va de même pour les informations traitées et donc pour les capteurs utilisés qui ne sont plus de simples caméras.
En effet, pour reconstruire un visage en 3D (*par maillage polygonal par exemple*), un matériel spécial est nécessaire tel que des caméras à vision stéréoscopique ou des scans 3D à vision active. La première catégorie utilise plusieurs caméras qui sont positionnées à des endroits bien spécifiques par rapport à des jeux de lumières. Tandis que les scans projettent des rayons de lumière et détectent par caméra les courbes formées sur le visage.

Figure 3: Scans 3D *sans* et *avec* mapping de texture. Modèles issus de la base FRGCv2 [6]

Les principales méthodes actuelles qui permettent la reconnaissance de visages en 3D sont les suivantes [6] :

- Approches **surfaces** : la surface 3D du modèle reconstruit est alignée avec celle de la signature à comparer pour évaluer le taux de similitude par approximations.
- Approches **holistiques** ou (GLOBALES) : extensions des méthodes ACP 2D pour les représentations 3D, par exemple : *eigensurface*.
- Approches **locales** : cherches des courbes du visages ou des points caractéristiques
- Approches **3D + 2D** : combinaisons de techniques d'analyse 3D et 2D pour améliorer les performances et la robustesse

.
La reconnaissance 3D comparée à la 2D permet d'obtenir de meilleurs résultats.
De plus, les scans 3D sont beaucoup moins sensibles aux divers changements d'illumination, de variation de la pose ou encore de mise à l'échelle, autant de critères qui sont les éléments critiques de la reconnaissance automatique 2D.
Toutefois, elle est plus difficile à mettre en place, consomme plus de ressources de calcul et nécessite l'utilisation de capteurs plus onéreux.

3.5 Identification et authentification

Une fois la signature reconstruite à partir des données extraites de l'image, celle-ci va être comparée avec d'autres modèles. La validation se base sur un seuil du taux de similitudes entre les deux fichiers numériques.

.
Dans le cas de l'identification, la signature peut être comparée avec l'ensemble des gabarits de la DB pour retrouver l'individu en question ou, dans une optique de recherches, elle peut être comparée avec seulementune liste de modèles pour détecter un éventuel match.

.

Dans une utilisation d'authentification, une requête est faite vers la DB pour obtenir le modèle à comparer et vérifier si la signature reconstruite y correspond ou non.

3.6 Mesure de la performance

Afin d'évaluer les performances d'un système biométrique par reconnaissance de visage et pour aider la recherche et le développement de ces technologies, il existe des bases de données contenant de nombreux templates pouvant être utilisés. Ainsi, à titre d'exemple, il existe la base FERET, avec plusieurs centaines d'invidus collectés, ou la base XM2VTS qui contient un ensemble d'images faciales 2D et 3D avec différentes prises de vues [7].

4. EXEMPLES D'UTILISATION

Les applications de la reconnaissance faciale sont nombreuses, nous en retiendrons ici deux, chacune étant liée à un mode d'utilisation de la biométrie tel que cités précédemment : l'identification et l'authentification.

4.1 Les systèmes de surveillance en lieux publics

Depuis le mois d'août de cette année, la gare de Südkreuz à Berlin est en phase de test pour un dispositif de reconnaissance faciale. Plusieurs caméras ont été installées dans le hall principal afin de détecter la présence d'individus réguliers qui se sont prétés à l'expérience. Le but du système, à terme, s'inscrit dans la lutte antiterrorisme afin de pouvoir identifier des suspects sur base d'une liste prédéfinies.
Il s'agit donc bien ici d'un cas d'utilisation d'identification (*comparaison 1 :N*), dans lequel les capteurs cherchent sans relâche la présence des visages en mouvement et les compare avec une liste de gabarits pour détecter la présence d'une personne.

.

Le cas de videosurveillance de la gare de Südkreuz n'est qu'un exemple parmi tant d'autres. En effet, de plus en plus d'espaces publics, tel que l'aéroport de Paris à Orly, envisagent de tester des systèmes de reconnaissance faciale pour améliorer la sécurité du lieu et appréhender des suspects.
Il est à noter que, si les autorités allemandes affirment qu'aucune image des passants innoncents ne sera conservée [8], ce système reste dénoncé par certaines personnes qui voient en cela une violation de "la liberté de circulation sans être observée". Il faudra probablement encore un peu de temps avant que l'utilisation de tels systèmes soient acceptés dans les moeurs de la société.

4.2 La Face ID de Apple

L'IphoneX d'Apple embarque un nouveau système biométrique, la *Face ID*, qui utilise cette fois-ci la reconnaissance faciale.
Afin de réaliser une cartographie 3D du visage, une nouvelle technologie a été installée, la *True Depth*. Celle-ci se compose de trois éléments [9]

- un PROJECTEUR DE POINTS : projette près de 30 000 points infrarouges sur le visage
- un POINT DE LUMIÈRE : utilisé en cas de mauvaise luminosité
- une CAMÉRA INFRAROUGE : capture l'image des points projettés

La Face ID est accompagnée d'un coprocesseur dédié qui assure du *machine learning* afin reconnaître les changements d'apparence du visage ainsi que les expressions faciales.

.

Point de vue sécurité, la signature numérique (chiffrée bien entendu) du visage est stockée localement sur l'appareil de sorte qu'aucune donnée ne soit envoyée sur les serveurs d'Apple ou sur le Cloud.
D'après Apple, la probabilité d'erreur de la Face ID serait de 1 :1 000 000 contre 1 :50 000 sur son système d'empreintes digitales [10]. De plus, elle ne pourrait pas être trompée par l'utilisation d' une image 2D à cause de l'absence de profondeur détectée par les points infrarouges.
Toutefois, malgré les prouesses effectuées en matière de reconnaissance 3D et la fiabilité du système, celui-ci reste sensible, dans certains cas, à la distinction de vrais jumeaux.

.

Outre des aspects d'authentification, il est à noter qu'en parallèle à la technologie Face ID, une capture en temps réel des mouvements permet également l'animation d'*emojis* qui suivent les expressions faciales de l'utilisateur. Bien que cela puisse paraître inutile à priori, cela souligne les progrès importants réalisés. Ces capteurs permettront forcément à l'avenir de nouvelles fonctionnalités bien plus utiles.

5. CONCLUSION

Au fil de ces dernières décennies, les techniques de reconnaissance de visages se sont fortement améliorées proposant nombre de méthodes analysant des modèles 2D et 3D, avec des performances différentes et des dispositifs physiques plus ou moins onéreux. De plus, les nouvelles technologies ont permis de miniaturiser les capteurs de telle sorte que maintenant ils puissent même être embarqués dans des appareils mobiles.
Ces prouesses permettent ainsi d'obtenir des systèmes biométriques d'authentification de plus en plus performants qui améliorent la sécurité de nos appareils ou des mécanismes d'accès.
La reconnaissance de visages va également permettre à l'avenir de sécuriser des lieux publics, où circulent de nombreuses personnes, en traquant des suspects.
Toutefois, il est à noter que si les technologies biométriques représentent des solutions pratiques incontournables à l'heure du numérique et du "tout connecté", certains systèmes stockent des informations très personnelles sur les individus comme leurs empreintes digitales, leurs données faciales, leur comportement... Dès lors, cela peut soulever certaines questions quant à la protection de notre vie privée et la sécurité de ces informations. Il y a-t-il des risques potentiels à nous dévoiler autant à des "inconnus" ? Serons-nous un jour contraints par les autorités de fournir l'ensemble de nos caratéristiques biométriques pour constituer des bases de données nationales ? Dans quelle mesure peut-on accepter que des systèmes nous surveillent en public (*"pour notre bien et la sécurité"*) ? Autant de questions pour lesquelles chacun à la liberté de se faire sa propre opinion mais probablement qu'il faudra un jour tout simplement accepter d'évoluer avec son temps et de profiter avant tout des bénéfices qu'offre ces nouvelles technologies, en échange de l'intrusion quelles occasionnent.

6. REFERENCES

[1] IDEMIA (OT-Morpho). What is biometrics ? https://www.morpho.com/en/biometrics.

[2] Biometrie-online. Biometrics technologies - operating principle. http://www.biometrie-online.net/technologies/fonctionnement.

[3] Khefif Bouchra. Mise au point d'une application de reconnaissance faciale. Mémoire de fin d'études pour l'obtention du diplôme de master en informatique, Université Abou Bakr Belkaid – Tlemcen Faculté des Sciences Département d'Informatique, Novembre 2013.

[4] Souhila Guerfi Ababsa. *Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D*. Thèse de doctorat spécialité : Sciences de l'ingénieur, Université Evry Val d'Essonne, Octobre 2008.

[5] Dr. Rolf P. Würtz. Scholarpedia - elastic bunch graph matching. http://www.scholarpedia.org/article/Elastic_Bunch_Graph_Matching.

[6] Lahoucine Ballihi. *Biométrie faciale 3D par apprentissage des caractéristiques géométriques : Application à la reconnaissance des visages et à la classification du genre*. Thèse de doctorat en vu d'obtenir le grade de docteur, spécialité informatique, Université Lille 1 Sciences et Technologies - Laboratoire d'Informatique Fondamentale de Lille, Mai 2012.

[7] Anis Chaari. *Nouvelle approche d'identification dans les bases de données biométriques basée sur une classification non supervisée*. Thèse pour obtenir le diplôme du doctorat - spécialités sciences pour l'ingénieur et informatique, Université d'Evry Val d'Essonne, Octobre 2009.

[8] Euronews. Berlin teste les caméras à reconnaissance faciale. http://fr.euronews.com/2017/08/24/berlin-teste-les-cameras-a-reconnaissance-faciale, Août 2017.

[9] Kaspersky. Aspects de sécurité de la technologie face id d'apple. https://www.kaspersky.fr/blog/security-face-id-apple/9488/, Septembre 2017.

[10] Iphone.fr. Face id : tout ce qu'il faut savoir sur la reconnaissance de visage de l'iphone x. http://www.iphon.fr/post/face-id-tout-savoir-reconnaissance-faciale-iphone-x-888822, Septembre 2017.

APPENDIX

A. EVALUATION DU TAUX DE PERFORMANCE DES SYSTÈMES BIOMÉTRIQUES

Les taux d'erreurs (*Fausses Acceptations* et *Faux Rejets*) dépendent du seuil de tolérance fixé. Les deux courbes varient de façon "opposée", de telle sorte que, par exemple, en diminuant le seuil de tolérance le match des signatures comparées soit plus vite validé, au risque d'augmenter le nombre d'individu faussement reconnus. C'est l'intersection des courbes, le point TEE, qui est utilisé pour évaluer la performance d'un algorithme de reconnaissance par biométrie.

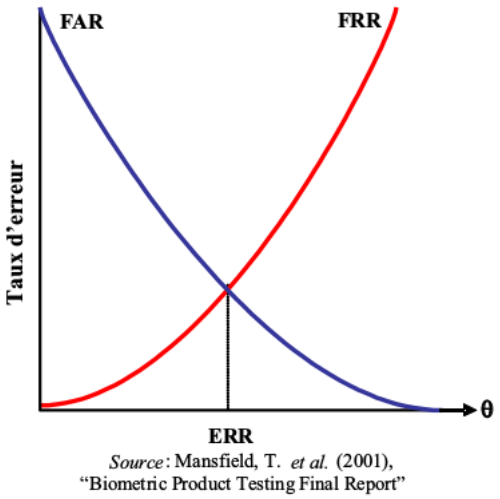

Figure 4: Source : [4]

B. COMPARAISON DES MÉTHODES LOCALES ET GLOBALES DE RECONNAISSANCE 2D

Variations	Caractéristiques locales	Caractéristiques globales
Petites variations	Pas sensible	Sensible
Grandes variations	Sensible	Très sensible
Illuminations	Pas sensible	Sensible
Expressions	Pas sensible	Sensible
Pose	Sensible	Très sensible
Bruit	Très sensible	Sensible
Occultations	Pas sensible	Très sensible

Figure 5: Tableau comparatif issu de [4]