La biométrie par reconnaissance faciale

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

ABSTRACT

1. INTRODUCTION

Bref rappel historique, motivations, utilité, ... Présentation du découpage de l'article

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 ou l'identité d'un sujet humain.
L'avantage des données biométriques est qu'elles sont : universelles, uniques, invariables, enregistrables et mesurables.

2.1 Système biométrique

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 :

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

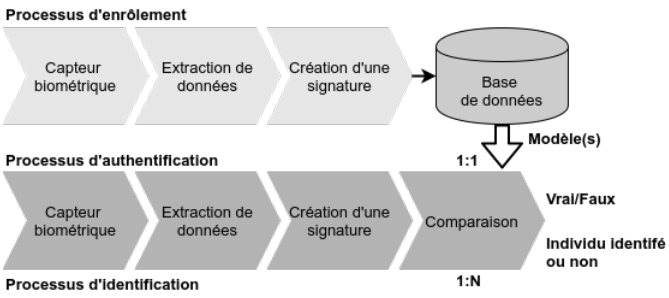

Figure 1: Modules d'un système biométrique

2.2 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.

2.3 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
- TFA - Taux de Fausses Acceptation
- TEE - Taux d'Egale Erreur

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)*.
Selon le contexte, plusieurs méthodes peuvent être appréhendées pour la capture de l'image : il peut s'agir d'un système statique ou bien dynamique, dans quel cas il faudra utiliser une caméra, spécifique ou non selon la technique de reconnaissance utilisée.

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 donc 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 avec 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 identifer 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.

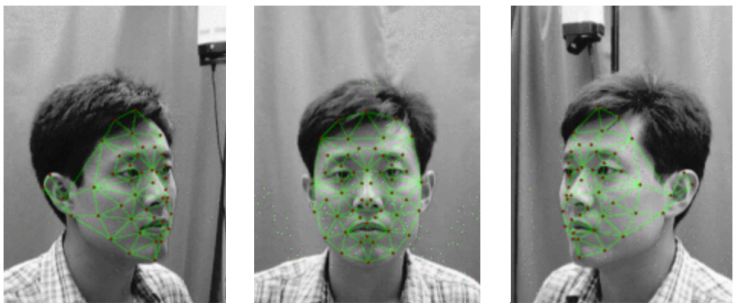

Figure 2: Graphe topologique par EBGM [5]

   - *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.

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

3.4 Reconnaissance 3D

Contrairement aux techniques 2D qui viennent d'être présentées, la reconnaissance 3D permet 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 techniques de reconnaissance sont différentes, il en va de même pour les informations traitées et donc pour les capteurs qui ne sont plus de simples caméras. En effet, pour reconstruire des visages en 3D (*par maillage polygonial par exemple*), un matériel spécial est nécessaire tels que des caméras à vision stéréoscopique ou vision active.

.

Les principales méthodes permettant 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
- Approches 3D + 2D

3.5 Mesure de la performance

Afin d'évaluer les performances d'un système biométrique par reconnaissance de visage et d'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 on 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 antiterroriste 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 identifient sans relâche la présence des visages en mouvement et les compare avec une liste de gabarits pour détecter la présence d'une personne.

.

Toutefois, si les autorités allemandes affirment qu'aucune images 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"

D'autres systèmes permettent également la lecture des émotions.

Aéroport de Paris à Orly

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 faits en matière de détection de visages et de la miniaturisation de tels systèmes. Ces capteurs permettront forcément à l'avenir de nouvelles fonctionnalités bien plus utiles.

5. CONCLUSION

Avantages et inconvénients

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] Mébarka Belahcene. *Authentification et Identification en Biométrie*. Thèse de doctorat en sciences en automatique, Université MohamedKhider – Biskra. Faculté des Sciences et de la technologie, Janvier 2013.

[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

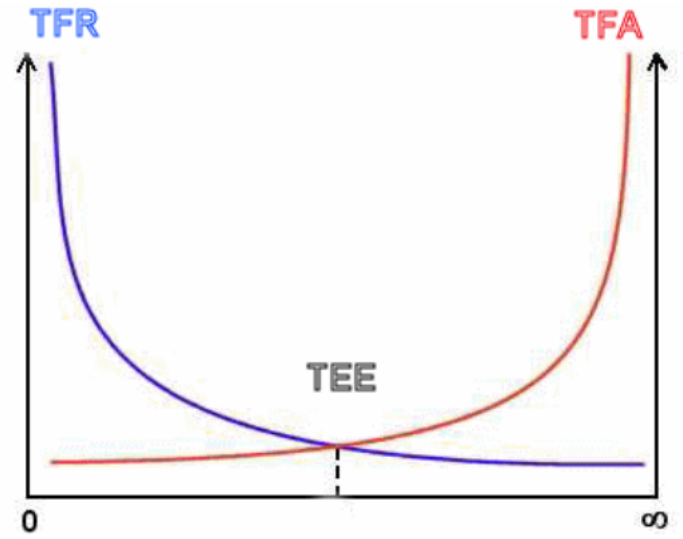

Figure 3: URL [...]

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 4: Tableau comparatif issu de [4]