La biométrie par reconnaissance faciale

Wéry Benoît
ECAM - 1e Master Informatique
1200 Bruxelles, Belgique
18 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 confirmer ou identifier 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 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

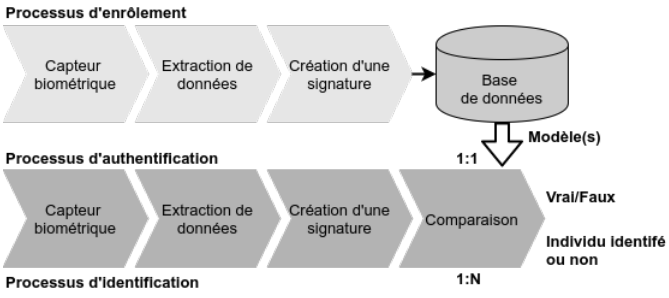

Figure 1: Modules d'un système biométrique

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 donc fixer des seuils d'acception, qui permettent de chiffrer le 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

Présentation de qqes résultats fondamentaux sur des recherches en cognition et reconnaissance faciale du visage

3.1 Détection de visage

Les difficultés rencontrées : Variations de la pose, changement d'éclairage (luminosité), expressions faciales, occultations,...

.

Les différentes méthodes : les "connaissances acquises", le "template matching", "l'apparence", les "caractéristiques invariantes"

.

Nécessité d'avoir une image de qualité -> dépend des capteurs

3.2 Prétraitement ou normalisation

Méthodes globales (ACP et ADL) vs méthodes locales (localisation de points caractéristiques et partition du visage en régions caractéristiques). Eigenface, stéréovision

3.3 Reconnaissance

Exploitation des caractéristiques extraites, création d'une signature numérique et mise en correspondance avec les modèles de la DB ou le modèle vérifié

.

Difficultés : causes inter-sujets (ressemblance entre modèles) et intra-sujet (ci-dessus)

3.4 Techniques de reconnaissance 2D et 3D

3.5 Mesure de la performance

Mise à disposition de bases de données

4. EXEMPLES D'UTILISATION

Les applications de la reconnaissance faciale sont nombreuses : depuis la sécurité des systèmes, jusqu'à la modélisation d'animation 3D en passant par la recherche de suspects. Nous retiendrons ici deux exemples, chacun étant lié à un mode d'utilisation de la biométrie tel que cité précédemment : l'identification et l'authentification.

4.1 Les portails de sécurité dans les aéroports

Ex : aéroport de Francfort - Contrôle des passagers automatisé par la reconnaissance de visages.

4.2 La FaceID de Apple

4.3 Mais encore... quel futur pour la reconnaissance faciale

Compte tenu des progrès fait en matière de reconnaissance faciale et de son intégration dans des systèmes tels que les smartphones, quelles applications pourrait-on envisager à l'avenir grâce à une telle technologie ?

.

Affichages publicitaires intelligents dont le contenu est adapté par la reconnaissance du visage.

5. LES ASPECTS LIÉS À LA SÉCURITÉ

5.1 Impact par rapport aux anciens systèmes

5.2 Les risques potentiels

5.3 Législation

En Europe, il est interdit de détcter les visages des gens sur les photos car cela peut mettre en péril leur vie privée - Exemple Facebook "DeepFace"

5.4 Questions éthiques... faut-il avoir "peur" de la reconnaissance faciale

Les technologies biométriques stockent des informations très personnelles sur les individus comme ses empreintes digitales, ses données faciales, ... dès lors, cela soulève 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 fournir tant de données à des "inconnus" , si oui lesquels ? Dans quelles mesures peut-on accepter que des systèmes (sites,) collectent autant de données sensibles à notre égard ? Quelle serait-la prochaine étape ?

6. CONCLUSION

Avantages et inconvénients

7. 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.