# Analyse d'images biométriques en contexte forensique

Sujet de thèse DGA en partenariat ESIEE-IRCGN

Laurent Najman, Hugues Talbot (ESIEE) – Commandant Patrick Perrot (IRCGN)

## 1 Introduction

Le concept d'analyse « forensique », mot dérivé de l'anglais *forensic* désigne dans le contexte de cette proposition de sujet de thèse thèse une analyse réalisée suite à un évènement. Dans la situation générale des études conduites à l'Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN), les évènements en questions sont des crimes, par exemple crimes sur des personnes (aggressions, meurtres), ou sur des biens (vols à main armées). Dans le cadre de cette thèse, nous nous positionnons dans la classe des évènements pour lesquels des données biométriques sous forme d'images fixes ou de vidéos existent. Ces données peuvent être par exemple des enregistrements de systèmes de surveillance, des vidéos de téléphones portables ou d'appareils de photo numériques.

L'objectif de cette thèse est de développer des méthodes et algorithmes d'identification *ou de non-identification* de personnes basés sur ces données dans le contexte d'une enquête judiciaire. Dans la suite du document, nous explicitons en quoi le problème est similaire en surface mais différent en profondeur du contexte d'identification biométrique habituel, pourquoi une telle recherche est nécessaire, quel est le plan de la thèse, quels sont les résultats attendus et les retombées possibles.

## 2 Etat de l'art

### 2.1 Identification biométrique dans un contexte de sécurité

L'identification biométrique automatique pour des applications de sécurité est un champ applicatif vaste et daté historiquement des années 1970 [**?**] avec l'identification de visages. La première méthode considérée comme utilisable pratiquement dans ce domaine a été l'analyse en composantes principales connue sous le nom d'*eigenfaces* [**?**]. Depuis d'autres méthodes ont été proposées avec des performances au moins équivalentes, soit utilisant des charactéristiques globales de l'image du visage [**?**], soit par extraction de caractéristiques mesurables (écartement des yeux, longueur du nez, facteurs de symétrie, etc) [**?**].

Ces méthodes ont été déployées avec succès par exemple en Australie pour l'entrée dans le pays conditionnée aux données biométriques des passeports récents, aux États-unis pour l'identification liée au permis de conduire (afin d'éviter les doubles permis), et dans certains casinos pour reconnaître les tricheurs interdits de jeu. Les succès de ces méthodes dans le domaine de la sécurité sont indissociables d'une une acquisition d'image contrôlée. Les auteurs de la méthode *eigenfaces* reconnaissent par exemple dans leur article original que leur méthodologie est sensible à l'illumination, à l'orientation du visage et à la résolution. Ainsi, la coopération des sujets est indispensable malgré les progrès réalisés.

Lorsque la coopération des sujets n'est pas assurée, on trouve que les méthodes sus-décrites ne produisent pas de suffisamment bons résultats. Un essai grandeur nature de détection et reconnaissance des personnes soupçonnées de terrorisme, organisé avec des moyens considérables à l'aéroport Logan de Boston s'est par exemple soldé par un échec [**?**].

### 2.2 Identification biométrique dans un contexte forensique

Le contexte forensique, c'est à dire l'identification de suspects après un crime est différent de plusieurs points de vue :

- Compte tenu de la diversité des sources, on ne peut pas garantir un certain degré de qualité de l'image, ni d'illumination, de pose, etc ;
- Il est peu probable d'obtenir la collaboration des sujets.

La tâche paraît donc bien plus difficile que le contexte de sécurité sus-décrit, et donc presque impossible, mais des éléments viennent mitiger ce bilan :

1. On ne cherche pas nécessairement à établir une identification positive, c'est-à-dire reconnaître quelqu'un. On peut vouloir au contraire disculper un suspect, ce qui peut se faire sur des critères bien plus variés que l'apparence du visage : on peut estimer la taille et la corpulence, la démarche, etc.
2. D'une manière générale l'objectif est de proposer à un juge ou un jury des données objectives permettant d'inculper ou de disculper un suspect, mais l'analyse biométrique n'est qu'un outil parmi d'autres. Une méthode d'identification avec un taux de succès faible peut néanmoins se révéler occasionnellent utile.
3. On dispose de plus de temps pour une analyse non temps-réel, et donc on peut exploiter des techniques plus sophistiquées de reconnaissances qui ne seraient pas utilisables en sécurité. On peut aussi chaîner plus d'une méthode.
4. L'utilisation de techniques de reconnaissances peut s'opérer interactivement avec un expert ce qui augmente les chances de succès. Nous avons montré par exemple que présenter à l'utilisateur non pas un seul mais les trois plus proches résultats lors de la reconnaissance faciale permettait d'augmenter significativement les taux de succès [**?**].
5. L'objectif premier d'un système de surveillance automatique est d'éliminer les faux négatifs : on souhaite surtout que les terroristes ne montent pas dans l'avion. L'objectif premier d'un système de forensique est d'éviter les faux positifs : on veut éviter les erreurs judiciaires et donc que l'outil ne donne pas confiance aux jury et aux juges.

## 3 Objectifs de la thèse

Le projet de thèse est donc d'exploiter les différentes modalités biométriques à disposition pour identifier un individu. Ces modalités sont en par exemple le visage et la démarche. La thèse s'articulera autour de trois parties. Tout d'abord il conviendra de définir un état de l'art de l'exploitation de données biométriques dans un contexte forensique, afin d'en connaître la robustesse, les limites, le niveau de performance attendu. Ensuite la thèse consistera à développer de nouvelles méthodes adaptées à la problématique définie fondée par exemple sur des pré-traitement spécifiques (techniques de segmentation, suivi sur vidéo, super résolution...), mais aussi sur l'exploitation de paramètres et de méthodes de classification pertinentes. Enfin, étape indispensable à un tel projet, nous nous attacherons à l'étape de

validation. Celle-ci devra permettre d'évaluer les performances du système en terme de fausses acceptations et de faux rejet sur des données opérationnelles.

## 4 Résultats attendus

## 5 Synergies et retombées annexes

## Bibliographie