Chapter 8
Deep Learning–Based Multimodal Biometric Fusion for Forensic Person Identification in Challenging Environments

Sarâh Benziane
https://orcid.org/0000-0002-0450-6522
USTO MB, Algeria

ABSTRACT

This chapter summarizes, analyses and discusses the current maturity of deep learning technology regarding the development and use of multimodal biometric fusion for forensic identity verification. The chapter identifies several challenges in relation to the collection and processing of wild data (low quality/resolution images, noise due to environmental factors and/or partial occlusion). The chapter discusses advantages of using deep neural networks (DNNs) to replace traditional single-mode systems for the processing and recognition of wild data sets. Finally, the chapter describes three primary methods of fusion (feature-level, score-level and attention-based) that can be effectively used to combine disparate data sets; stresses the importance of cross-modal transformers for achieving accurate identification despite severe degradation caused by the use of dissimilar data sets; presents and emphasizes several advanced preprocessing methods, including the use of generative adversarial networks (GAN) for super-resolution.

DOI: 10.4018/979-8-3373-4972-5.ch008

1 INTRODUCTION

The fact that there has been, over the last couple of decades, significant advancement in the area of biometrics, but that real-world forensic applications continue to show significant limitations—and even failure—in the use of unimodal biometric systems for use in unconstrained environments. It should be noted that, while civil authentication applications (e.g., border control, access control, unlocking mobile devices, etc.) are conducted in a controlled environment, forensic identification is performed post hoc, meaning an item of evidence was not collected for the purpose of identifying the individual in question. The primary mismatch between the system's assumptions and the reality of the system's use has resulted in documented cases of failure, which illustrate the necessity for a multimodal approach that is very robust.

High-profile forensic cases have shown the vulnerabilities inherent in unimodal systems. An example is face recognition; it is likely that face recognition systems will perform very poorly if applied to low-quality CCTV footage, when subjects are captured at a low resolution, from extreme angles, or in low-light environments. The result of these scenarios is that even the best deep learning-based face recognition systems have experienced a dramatic decline in performance, which leads to false rejections and, more importantly, false identifications. Similarly, fingerprint evidence, which has historically been regarded as the gold standard in forensics, can become unusable due to smudging, partial prints, or contamination from the environment. Such failures are not isolated events but, rather, systemic failures that result from using a single biometric trait when acquiring evidence in a hostile environment (Benziane & Benyettou, 2011; Simonyan & Zisserman, 2014).

Biometric recognition is greatly hindered by the environment in which it operates. In the case of forensic artifacts, they are often collected passively (e.g. without consent) and with low-cost consumer equipment that is calibrated for monitoring not for identifying someone. Because of motion blur and sensor noise, as well as the fact that the distance from the subject to the recording device is not controlled, these aspects will create scenarios that violate the basic assumptions on which most unimodal biometric systems are designed and trained. Therefore, identity cues that would be very discriminative in a controlled environment become unreliable or completely absent in the forensic media collections.

The differences between civil and forensic identification are highlighted by the way they both operate; civil systems are closed-set (with controlled enrolment, consent from the subject, and repetition) while forensic identification is mostly an open-set (the suspect may not be in any database and may have only a single performance observation available). The legal implications of forensic conclusions also add significantly to the degree of required reliability, transparency and explainability over that of consumer biometric systems (Best-Rowden et al., 2014).