Chapter 9
Multimodal Biometric Fusion Techniques for Enhanced Identity Verification in Digital Forensics

R. N. Ravikumar
https://orcid.org/0009-0009-3705-1681
Marwadi University, Rajkot, India

S. Aarthi
https://orcid.org/0009-0006-9064-2091
Marwadi University, Rajkot, India

ABSTRACT

This chapter explores the integration of multimodal biometric fusion techniques in digital forensics to enhance identity verification accuracy and legal defensibility. Unlike unimodal systems that rely on a single trait, multimodal approaches combine fingerprints, facial recognition, voice, gait, and iris data to reduce false acceptance and rejection rates. The methodology includes deep learning-based feature extraction, score and decision-level fusion strategies, and explainable AI to ensure transparency and legal compliance. Real-world case studies demonstrate up to 29% improvement in match confidence through fusion. The chapter also addresses data governance, privacy preservation, and the necessity for adaptive, interpretable, and ethically sound systems. It concludes by highlighting the potential of AI-driven multimodal biometric frameworks to reshape forensic investigations in the digital era.

DOI: 10.4018/979-8-3373-4972-5.ch009

INTRODUCTION

This fast dynamic nature of digital forensics has increased the need to come up with a more secure and stronger identity verification system especially in those cases where the unimodal character of having single biometrics has failed to be sufficient. Biometric fusion methods (also known as multimodal biometrics) have also come to the front as a disruptive fix, with different biometric characteristics combined, like fingerprints, face characteristics, iris outline, gait, and voice, increasing accuracy, minimizing mistakes, and improving resistance to impersonation and sensor noise (Singh et al., 2019). This is specifically important in handling forensic cases in which there is a possibility that the quality along with completeness of evidence may be hindered by the environmental or circumstantial factors. Multimodal systems are much more effective in terms of improving identification performance through the application of complementary modalities, and counteracting the deficiencies of unimodal systems, which are: intra-class variance and non-universality (Meden et al., 2021). The chapter discusses design and implementation technologies, and multimodal biometric fusion forensics and its possible application to the real world and to the other subfields being developed as 2ndgeneration technologies such as Artificial Intelligence (AI) and deep learning. It also looks at questions of morality, law and interpretability that are involved in the manipulation of sensitive biometrics data that is used in the field of forensics. Finally, not only does the chapter place multimodal biometric fusion as a technological enhancement, but a driving force of justice in a more multifaceted digital environment.

FOUNDATIONS OF MULTIMODAL BIOMETRIC FUSION IN FORENSICS

Multi-modal biometric fusion refers to the fusion of two or more biometric modalities to create more capable and accurate system in regard to people recognition. This form of methodology has also been extremely useful where the field of digital forensics is concerned because of the massive variability of the quality of evidence. The unimodal systems have weaknesses including those inferred in sensor noise, non-universality, and spoof attack and intra-class variability based on fingerprints or voice (Choras, 2020). Multimodal systems have the advantage of countering each of these individual failures since combining several biometrics characteristics can counter these shortcomings, making it more stable under different contexts and individuals. There are various levels fusion can be done: sensor, feature, score or decision. There are trade-offs in every level. As an example, the feature-level fusion needs more compatible data format but leads to the more information-rich results,