Face Anti-Spoofing Detection with Multi-Modal CNN Enhanced by ResNet

Hala S. Mahmood[1*], **Salah Al-Darraji**[2]

[1]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq.
[2]Department of Computer Science, College of Computer Science & Information Technology, University of Basrah, Basrah, Iraq.

ARTICLE INFO

Received 09 January 2024
Accepted 19 February 2024
Published 20 June 2024

Keywords:

Face anti-spoofing, presentation attack detection, PAD, face recognition, ResNet-50, deep learning.

Citation: H.S. Mahmood, S. Al-Darraji, J. Basrah Res. (Sci.) **50**(1), 74 (2024).
DOI:https://doi.org/10.56714/bjrs.50.1.7

ABSTRACT

The growing prevalence of face recognition technology in various applications, including mobile devices, access control, and financial transactions, highlights its importance. However, the vulnerability of face recognition systems to attacks has been demonstrated, underscoring the necessity of addressing potential weaknesses that attackers may exploit. The paper delves into face presentation attack detection (PAD) within biometric systems, which is crucial for ensuring the reliability and security of face recognition algorithms. To address this issue, the paper proposes a method for face presentation attack detection using ResNet-50 in conjunction with multi-modal data, incorporating RGB, depth, infrared (IR), and thermal channels. The method explores diverse strategies to combine results from each modality, investigating various fusion techniques such as majority voting, weighted voting, average pooling, and a stacking classifier. The system has been tested on the WMCA dataset. It exhibits strong performance compared to existing methods, notably achieving an impressive ACER ratio of 0.087% with the stacking classifier. This approach proves effective by consolidating multiple modalities without requiring individual scenario-specific models, indicating promise for real-world applications.

1. Introduction

Automated authentication systems need to be protected against spoofing attacks to prevent illegal entry [1], [2]. Face anti-spoofing (FAS) is crucial for enhancing the security of face recognition systems by protecting them from presentation attacks. Face recognition has made remarkable progress, with state-of-the-art systems exceeding the performance of humans [3]. A substantial portion of this achievement may be ascribed to the accessibility of extensive annotated face datasets often gathered via the internet. In contrast, datasets for face anti-spoofing assaults need a laborious procedure of manual data acquisition, resulting in a restricted number of distinct individuals and samples.