Abstract

Convolutional Neural Networks for Presentation Attack Detection in Fingerprint Biometric Systems

by

Soha Sandouka

Master of Science in the Department of Computer Engineering at the College of Computer and Information Sciences.

King Saud University, Riyadh, December 2021

Prof. Yakoub Bazi

The fingerprint-based biometric system is the oldest biometric system used for verification and identification. The proven high authentication accuracy, collectability, and uniqueness of fingerprints render this system widely used in various day-to-day personal, governmental, and sensitive tasks such as international border security and mobile payments. However, these systems suffer from several vulnerabilities, including spoofing, forgery, and presentation attacks. The process of detecting and preventing presentation attacks (PAs) in a biometric system is known as presentation attack detection (PAD).

This thesis aims to propose fingerprint PAD methods based on deep learning techniques. The aim is to improve the generalization performance of fingerprint PAD systems against spoofs acquired with unknown sensors or made from materials not seen during training. In particular, this thesis presents two main contributions through two approaches. The first approach is based on a classification backbone coupled with generative adversarial networks (GAN) for solving the problem of multi-target domain adaptation in a one-to-one mapping manner. While the second approach uses a unified GAN model for multi-domain conversion to jointly learn several mappings between all domains.

The effectiveness of the proposed approaches was tested through several experiments with different scenarios on the LivDet2015 dataset. The obtained results confirm the promising capabilities of the proposed approaches in improving the PAD classification accuracy.