digital

an Open Access Journal by MDPI

CITESCORE 3.1

Biometric Presentation Attack Detection in Mobile Devices

Guest Editors:

Dr. Emanuela Marasco
Center for Secure Information Systems, George Mason University, Fairfax, VA 22030, USA

Dr. Gian Luca Marcialis
Associate Professor, Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy

Dr. Maria De Marsico
Department of Computer Science, Sapienza University, Rome, Italy

Deadline for manuscript submissions:
closed (1 May 2021)

Message from the Guest Editors

Dear Colleague,

Biometric authentication mechanisms in mobile phone applications come with vulnerabilities to presentation attacks (PAs), challenging the effectiveness of this technology. PAs refer to techniques that inhibit the intended operation of a biometric capture system, interfering with the acquisition of the true identity. An impersonation attack can occur when a malicious individual tries to unlock the phone of someone else. Biometric spoofs can be detected through accurate and robust presentation attack detection (PAD) algorithms. PAD modules classify biometric samples as either live (non-spoof) or fake (spoof). The specificity of the sensor in determining a live biometric—as opposed to a recording, picture, or another non-living spoof—is commonly known as liveness detection. The latest development is therefore a subset of the potential attacks that might be detected through PAD. Despite the significant attention given to the problem of face spoofing and fingerprint recognition, PAD systems still produce poor results, through either false alarms or poor usability, lacking generalized PAD methods performing robustly in a practical environment.