electronics

an Open Access Journal by MDPI

IMPACT FACTOR 2.397

CITESCORE 2.7 SCOPUS

Recent Advances in Biometric Security in IoT Based on Machine Learning

Guest Editors:

Prof. Dr. Nima Karimian
Computer Engineering Department, San José State University, San Jose, CA 95192, USA

nima.karimianbahnemiri@sjsu.edu

Prof. Dr. Tempestt Neal
Department of Computer Science and Engineering, University of South Florida (USF), Tampa, FL 33620, USA

tjneal@usf.edu

Deadline for manuscript submissions:
31 May 2022

Message from the Guest Editors

Dear Colleagues,

Internet of Things (IoT) applications has been deployed in a wide variety of critical infrastructure and applications ranging from transportation, healthcare, and supply chain. While IoT brings a number of benefits including convenience and efficiency, it also introduces a number of emerging threats. With the emergence of the Internet-of-Things (IoT), there is a growing need for access control and data protection. Biometric-based authentication is promising for IoT due to its convenient nature and lower susceptibility to attacks. Additionally, machine learning and deep learning techniques are delivering a promising solution to biometric systems and to increase the accuracy and plays a decisive role for presentation attack detection.

The goal of this special issue is to solicit high quality contributions on: (i) investigating the usage of deep learning and biometric systems in the context of IoT applications; (ii) novel techniques in biometric deep fakes and digital data forensics, particularly by exploiting, but not limited to, deep learning approaches.