IEEE TRANSACTIONS ON BIOMETRICS, BEHAVIOR, AND IDENTITY SCIENCE
Special Issue on Trustworthy Biometrics

SUMMARY

Biometrics are increasingly being used to recognize people in various applications (e.g., recognizing people through their physiological or behavioral traits such as face, fingerprint, iris, gait, signature, and voice), and are becoming an integral part of our daily life. A broad and sustainable deployment of biometric systems will rely heavily on the ability to trust the recognition process and secure handling of the output. As a result, privacy and security are also critical to the success of biometrics in addition to the high accuracy. To trust a decision made by an algorithm, we need to know that it is fair and causes no harm. Building trustworthy systems requires learning unbiased representations so that algorithms are fair to all users (i.e., are handling the imagery of everyone in the same way). Although the accuracy continues to improve, adversarial attacks have created a public concern that biometric systems can be vulnerable. As trust in biometric systems is based on our understanding of how they work, explainability and interpretability enable systems to explain their recognition process and causes of failure. Finally, human experts or users might choose to interact with the system to increase our trust.

Therefore, it is becoming essential to develop diverse approaches towards achieving fairness, robustness, explainability, transparency, and integrate them throughout the entire lifecycle of a biometric application. This special issue serves as a forum for researchers all over the world to present their works and recent advances in improving trustability of various biometrics modalities. State-of-the-art algorithm development, as well as comprehensive literature reviews, are welcomed for submission.

SCOPE

This special issue focuses on addressing multiple dimensions of trustworthy biometric systems. Broad topics of interest include but are not limited to:

- **Privacy and Security**
  - ○ Privacy preserving biometrics
  - ○ Biometrics presentation attack detection, template protection, template update, and data protection
  - ○ Forgery generation and detection
- **Bias and Fairness**
  - ○ Techniques to detect and mitigate bias in datasets and algorithms
  - ○ Unbiased representation learning
- **Adversarial Robustness**
  - ○ Adversarial attacks and defense by biometric systems
  - ○ Data poisoning and defense method
- **Explainability and interpretability**
  - ○ Optimized and directly interpretable models
  - ○ Information visualization in neural networks
  - ○ Disentangled representation learning
- **Transparency**
  - ○ Measurement of the trustworthy levels of a system
  - ○ Human-algorithm interaction in biometrics

IMPORTANT DATES

Paper submission due: May 1, 2021

First review notification: Jun 20, 2021

Revision due: Oct 1, 2021

Final notification: Dec 1, 2021

Final version due: Jan 1, 2021

Publication date: Apr, 2022

GUEST EDITORS

Weihong Deng, Beijing University of Posts and Telecommunications

Tal Hassner, Facebook AI

Xiaoming Liu, Michigan State University

Maja Pantic, Imperial College London