

CALL FOR PAPERS

IEEE Signal Processing Society

Special Issue
IEEE SIGNAL PROCESSING MAGAZINE

Special Issue on Biometric Security and Privacy

Aims and Scope

Biometrics is the science of recognising individuals based on their physical and behavioural traits such as face, fingerprints, iris, voice, gait and signature. A typical biometric system may be viewed as a pattern recognition system which utilises advanced signal processing schemes to compare and match biometric data. The past decade has seen a rapid increase in biometrics research as well as the deployment of large-scale biometric solutions in civilian and law enforcement applications. Since the biometric data of an individual can be viewed as being personal and sensitive, issues related to biometric security and privacy have been raised. These include (a) spoofing, where an adversary presents a falsified biometric trait to the system with the intention of masquerading as another person; (b) evasion, where a person attempts to obfuscate or modify a biometric trait in order to avoid being detected by the system; (c) database alteration, where the templates stored in a database are modified in order to undermine system integrity; and (d) template compromise, where the stored biometric data is perused or stolen and exploited for illegitimate means. The goal of this special issue is to highlight recent advances made in the field of biometrics security and privacy protection. A number of signal processing methods have been developed to analyse the vulnerability of biometric systems and design solutions to mitigate their impact. At the same time, privacy-preserving constructs have been developed by signal processing researchers in order to ensure that stored and/or transmitted biometric data is adequately protected so as to prevent their use for purposes beyond those intended. The special issue will bring together the latest work in biometric security and privacy protection, with an emphasis on tutorial and review-style articles.

Topics of interest include (but are not limited to):

- **Biometric system vulnerability assessment**
 - Protocols and evaluation metrics
 - Information theoretic approaches to threat assessment
 - Novel risk-based evaluation methodologies
 - White papers for formal, competitive evaluations and standards
- **Attacks and countermeasures**
 - Biometric sensors with inherent resistance to spoofing and evasion
 - New spoofing and evasion attacks
 - Advanced signal processing countermeasures
 - Adversarial machine learning and pattern recognition
 - Information forensic approaches to detection
 - Challenge-response and hardware-based solutions
- **Social, ethical and privacy dimensions**
 - Biometric crypto-systems
 - Template protection
 - Cancellable biometrics
 - Privacy Enhancing Technology (PET)
 - Privacy aware computing
 - De-identification of biometric data
 - Data anonymity
- **Application domains**
 - Distributed, mobile-cloud architectures
 - Smartphones
 - Surveillance systems
 - Forensic biometrics
 - Automated border control

Submission Process

Articles submitted to this special issue must contain significant relevance to signal processing. All submissions will be peer reviewed according to the IEEE and Signal Processing Society guidelines for both publications. Submitted articles should not have been published or under review elsewhere. Manuscripts should be submitted online at <http://mc.manuscriptcentral.com/sps-ieee> using the Manuscript Central interface. Submissions to this special issue of the IEEE SIGNAL PROCESSING MAGAZINE should have significant tutorial value. Prospective authors should consult the site <http://www.signalprocessingsociety.org/publications/periodicals/spm/> for guidelines and information on paper submission.

Important Dates: Expected publication date for this special issue is **September 2015**.

IEEE Signal Processing Magazine	Time Schedule
White paper due	September 1, 2014
Invitation notification	October 1, 2014
Manuscript due	December 15, 2014
Review results and decision notification	March 1, 2015
Revised manuscript due	April 1, 2015
Final acceptance notification	May 1, 2015
Camera-ready paper due	May 9, 2015
Publication date	September 2015

Guest Editors

Nicholas Evans, evans@eurecom.fr, Dept. of Multimedia Communications, EURECOM, France
Andrew Teoh Beng Jin, biteoh@yonsei.ac.kr, Yonsei University, Seoul, South Korea
Sébastien Marcel, marcel@idiap.ch, Idiap Research University, Switzerland
Arun Ross, rossarun@cse.msu.edu, Michigan State University, USA