CALL FOR PAPERS

IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY

Special Issue on Biometric Spoofing and Countermeasures

Guest Editors

Nicholas Evans EURECOM, France (evans@eurecom.fr)
Sébastien Marcel Idiap Research Institute, Switzerland (marcel@idiap.ch)
Arun Ross Michigan State University, USA (rossarun@cse.msu.edu)
Stan Z. Li Chinese Academy of Sciences, China (szli@nlpr.ia.ac.cn)

While biometrics technology has revolutionized approaches to person authentication and has evolved to play a critical role in personal, national and global security, the potential for the technology to be fooled or 'spoofed' is widely acknowledged. Efforts to study such threats and to develop countermeasures are now well underway resulting in some promising solutions. While progress with respect to each biometric modality has attained varying degrees of maturity, there are some notable shortcomings in research methodologies. Current spoofing studies focus on specific, known attacks. Existing countermeasures designed to detect and deflect such attacks are often based on unrealistic *a priori* knowledge and typically learned using training data produced using exactly the same spoofing method that is to be detected. Current countermeasures thus have questionable application in practical scenarios where the nature of the attack can never be known. This special issue will focus on the latest research on the topic of biometric spoofing and countermeasures, with a particular emphasis on novel methodologies and generalized spoofing countermeasures that have the potential to protect biometric systems against varying or previously unseen attacks. The aim is to further the state-of-the-art in this field, to stimulate interactions between the biometrics and information forensic communities, to encourage the development of reliable methodologies in spoofing and countermeasure assessment and solutions, and to promote the development of generalized countermeasures. Papers on biometric obfuscation (e.g., fingerprint or face alteration) and relevant countermeasures will also be considered in the special issue. Novel contributions related to both traditional biometric modalities such as face, iris, fingerprint, and voice, and other modalities such as vasculature and electrophysiological signals will be considered. The focus includes, but is not limited to, the following topics related to spoofing and anti-spoofing countermeasures in biometrics:

- vulnerability analysis with an emphasis on previously unconsidered spoofing attacks;
- theoretical models for attack vectors;
- advanced machine learning and pattern recognition algorithms for anti-spoofing;
- information theoretic approaches to quantify spoofing vulnerability;
- spoofing and anti-spoofing in mobile devices;
- generalized countermeasures;
- challenge-response countermeasures;
- sensor-based solutions to spoof attacks;
- biometric obfuscation schemes;
- information forensic approaches to spoofing detection;
- new evaluation protocols, datasets, and performance metrics;
- reproducible research (public databases, open source software and experimental setups).

Submission Procedure: Manuscripts are to be submitted according to the Information for Authors at http://www.signalprocessingsociety.org/publications/periodicals/forensics/forensics-authors-info/ using the IEEE online manuscript system, Manuscript Central. Papers must not have appeared or be under review elsewhere. Manuscripts by the guest editors submitted to this SI will be handled by the EIC of IEEE-TIFS.

Schedule:

Submission deadline: 1st June 2014
First Review: 15th September 2014
Revisions Due: 1st November 2014
Final Decision: 15th December 2014
Final manuscript due: 15th January 2015
Tentative publication date: 1st April 2015