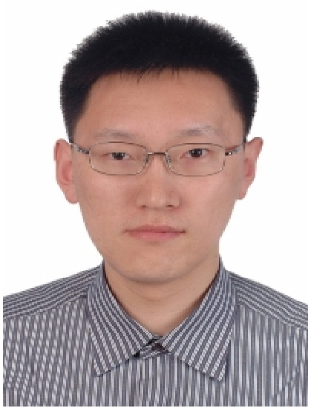
Special Session 1: Biometric Spoofing and Anti-Spoofing

Biometrics is the science of establishing the identity of a person based on physical or behavioral attributes such as fingerprint, face, iris, and gait. A biometric spoofing attack occurs as a person tries to masquerade as a valid user by presenting this user's counterfeit biometric trait to the sensor. In recent years, we have witnessed large-scale deployments of biometrics in personal and governmental identity management applications. With such wide applications, biometric spoofing has become a serious threat and a number of cases have been reported in news. Researchers have made a great deal of effort to develop biometric anti-spoofing techniques to differentiate between a real biometric trait and a fake one forged by the attacker. Despite of many published papers on this topic, biometric anti-spoofing is still an unsolved problem, especially when a number of factors (cost, size, convenience) have to be considered in developing anti-spoofing techniques for real applications. In this special session, topics of interest include, but are not limited to, spoofing, synthesis, anti-spoofing of various biometric traits, and novel biometric technologies which are robust to spoofing.

Organizers:

Jianjiang Feng
Tsinghua University, China

Arun Ross
Michigan State University, USA



Ran He
Institute of Automation, Chinese Academy of Sciences, China