Abstract
With ever growing public demand for remote access to government and commercial services through personal computers and mobile devices, the opportunity to fraudulently abuse such access is equally on the increase for individual hackers and international criminal gangs with skill, sophistication and ever more powerful hardware and software resources. Traditional four-digit personal identification numbers and six-character passwords are hardly serious barriers any longer against hacking attacks, and biometric authentication methods, including speaker recognition, face recognition and finger scan are being used to supplement or substitute for traditional security methods. A parallel development has taken place in recent years in the forensic science of person identification. Algorithm development in pattern recognition, the collection of large biometric databases and the wide acceptance of the likelihood-ratio paradigm have made biometrics like DNA, voice and face into reliable forensic tools and have taken much of the subjectivity out of traditional paradigms like fingerprint identification. This talk will sketch the state of the art in biometric person authentication, including pattern recognition algorithms, multimodal fusion and liveness assurance, as well as the main current and future application areas for biometric technology.