Abstract:
Biometric systems recognize individuals based on their biological attributes such as faces and fingerprints. However, in several scenarios, additional ancillary information such as the biographic and demographic information of a user (e.g., gender, ethnicity), or the image quality of the biometric sample, anti-spoofing measurements, etc. may be available. In this dissertation, I develop a principled framework to combine multiple types of ancillary information with biometric match scores. Three major contributions are listed as: i) the design of a Bayesian Belief Network (BBN) to model the relationship between biometric scores and ancillary factors, ii) the design of a Generalized Additive Model (GAM) that uses spline functions learn transformation functions to normalize the match scores prior to fusion, and iii) the design of an ensemble of One Class Support Vector Machines (OC-SVMs) to combine multiple anti-spoofing measurements in order to mitigate the concerns associated with the issue of “imbalanced training sets” and “insufficient spoof samples”.