Biometric Recognition:
Some Challenges in Forensics

Anil K. Jain
Michigan State University
http://biometrics.cse.msu.edu

If you are like many people, navigating the complexities of everyday life depends on an array of cards and passwords that confirm your identity. But lose a card, and your ATM will refuse to give you money. Forget a password, and your own computer may balk at your command. Allow your card or passwords to fall into the wrong hands, and what were intended to be security measures can become the tools of fraud or identity theft. Biometrics—the automated recognition of people via distinctive anatomical and behavioral traits—has the potential to overcome many of these problems.

Biometrics is not a new idea. Pioneering work by several British scholars, including Fauld, Galton and Henry in the late 19th century established that fingerprints exhibit a unique pattern that persists over time. This set the stage for the development of Automatic Fingerprint Identification Systems that are now used by law enforcement agencies worldwide. The success of fingerprints in law enforcement coupled with growing concerns related to homeland security, financial fraud and identity theft has generated renewed interest in research and development in biometrics. It is, therefore, not surprising to see biometrics-based authentication permeating our society (laptops and mobile phones, border crossing, civil registration, and access to secure facilities). Despite these successful deployments, there are challenges related to biometric data acquisition, image quality, robust matching, system security and user privacy. This talk will introduce four challenging problems of particular interest in law enforcement and forensics: (i) face sketch to photo matching, (ii) latent fingerprint matching, (iii) fingerprint obfuscation and (iv) scars, marks & tattoos (SMT).