Human Recognition Using Biometrics

Arun Ross
Associate Professor
Michigan State University
rossarun@cse.msu.edu

http://www.cse.msu.edu/~rossarun/i-probe
Currently: 6 PhD students, 3 Post-docs

Collaboration with several biometric research groups

Extensive research through CITeR: NSF Center for Identification Technology Research

VP of Education, IEEE Biometrics Council

Vice-Chair, IAPR TC-4 (Biometrics)
Biometrics is the science of recognizing humans.

Recognition is based on the anatomical and behavioral traits of an individual.
Ocular Biometrics

- The **eye** and its immediate surroundings
- Consists of **iris**, sclera, eyelids, eyelashes, eyebrow, skin texture
Combining multiple biometric traits

The identity of an individual is reinforced through multiple traits

Especially significant in scenarios where partial biometric data is available
Methods to quickly retrieve the correct identity from a large database, based on input biometric data.
Spoofing: When a person spoofs or mimics the biometric trait of an authorized individual in order to circumvent a biometric system

Obfuscation: When a person attempts to alter or obscure their own biometric trait in order to evade recognition by a biometric system

Methods to detect such attacks are being developed
Detecting attempts to alter identity using facial cosmetics or masks

Images selected for illustration purposes only
Friction ridge patterns on fingertips can be turned into unnatural ridge patterns by plastic surgery or mutilation.

Methods to detect such alterations are being developed.
Protecting Biometric Data

- Methods to impart security and privacy to stored biometric data
  - Biometric cryptosystems
  - Data encryption
  - “Cancellable” biometrics
  - Visual cryptography
  - etc.
Example: Protecting Biometric Data

- The input image is **split** and **stored** in two separate servers: either server will be unable to deduce original identity.
Example: De-identifying Face Images

Input Face

Images selected for illustration purposes only
Combining multiple traits can improve recognition accuracy.

Methods are being developed to detect altered or spoofed biometric traits in order to improve system security.

Protecting biometric data to improve system integrity and impart privacy.