Biometrics for Information Security

Dr. Natarajan Meghanathan
Associate Professor of Computer Science
Jackson State University, Jackson, MS, USA
E-mail: natarajan.meghanathan@jsums.edu

Motivation for using Biometrics

- People are normally verified or identified using one or more of the following three means:
  - With something they have (e.g., ID card, ATM card)
  - With something they know (e.g., Passwords)
  - With something they are (e.g., Biometrics)
- Authentication schemes using something people have or know do not really distinguish between authorized users and persons who are in unauthorized possession (e.g., say the ID card or the password).

Introduction to Biometrics

- Biometrics: Comprises of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits or identifiers
  - Used to authenticate users and grant or deny access control rights to data and system resources.
- Biometric identifiers can be divided into two main classes:
  - Physiological: related to the body – often unique and can be used for identification as well as verification
    - Examples: Fingerprint, Face recognition, DNA, Palm print, Iris recognition and etc.
  - Behavioral: related to the behavior of a person – may not be unique for each person and can be used mainly for verification
    - Examples: Typing rhythm, body mechanics (gait), voice and etc.

Strength of Biometrics

- Biometric identifiers are difficult to be lost or forgotten, difficult to be copied/shared, and require the person to be authenticated to be present at the time and point of authentication (a user cannot claim his password was stolen and misused!!)

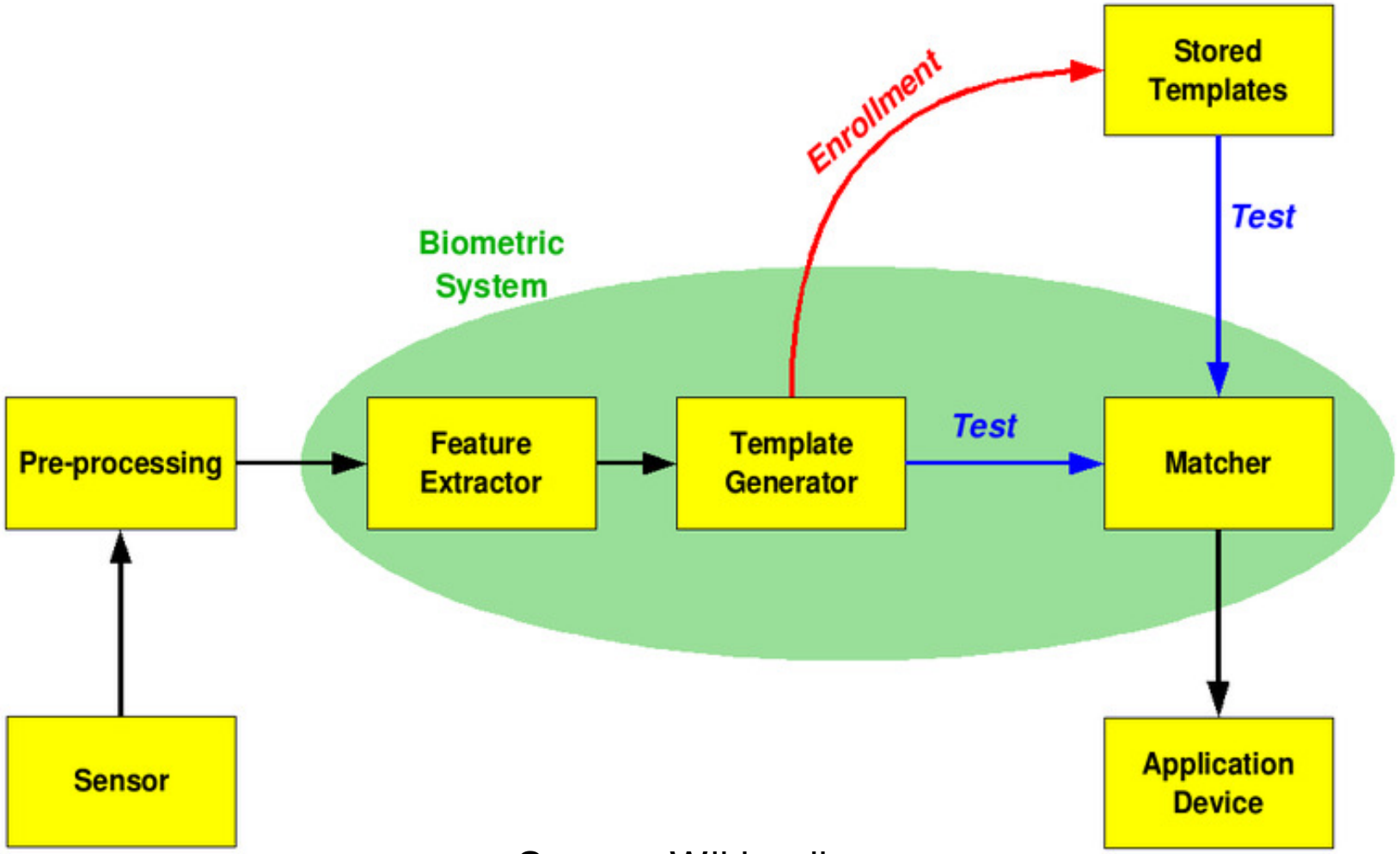
- Instead of passwords, biometric systems could be used to protect the strong cryptographic keys.

- For a given biometric identifier, all users have a relatively equal security level – One user's biometrics is no easier to break than another's.
  - There cannot be many users who have "easy to guess" biometrics that can be used to mount an attack against them.

Two Modes of a Biometric System

- Verification Mode: The captured biometric undergoes a “one-to-one comparison” with a stored template to verify (authenticate) that the individual is who he claims to be.
- Identification Mode: The captured biometric undergoes a “one-to-many comparison” against a biometric database to identify an unknown individual and establish the identity of the person as someone who has been enrolled in the system.
  - The comparison is considered to be successful if the biometric sample collected falls within the threshold values for the characteristic in the database.
- Verification Mode – Enrollment vs. Subsequent Uses:
  - The first time an individual uses a biometric system, it is referred to as enrollment. During the enrollment phase, biometric information from the individual is collected and securely stored in a database.
  - During the subsequent attempts, biometric information is collected from the individual and compared with the information stored at the time of enrollment. The retrieval of the information from the database must be done in a secured fashion.

Basic Block Diagram of a Biometric System



Source: Wikipedia

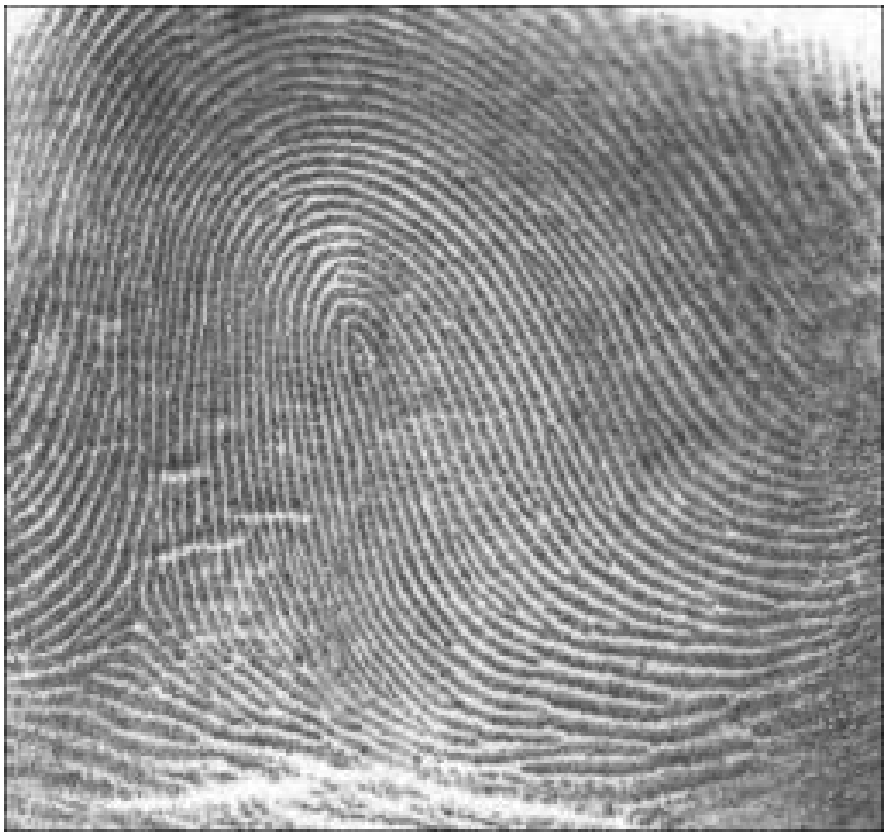
Fingerprint Ridge Patterns - Arch

- An arch is a pattern where the ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.

Source: Wikipedia

Fingerprint Ridge Patterns - Loop

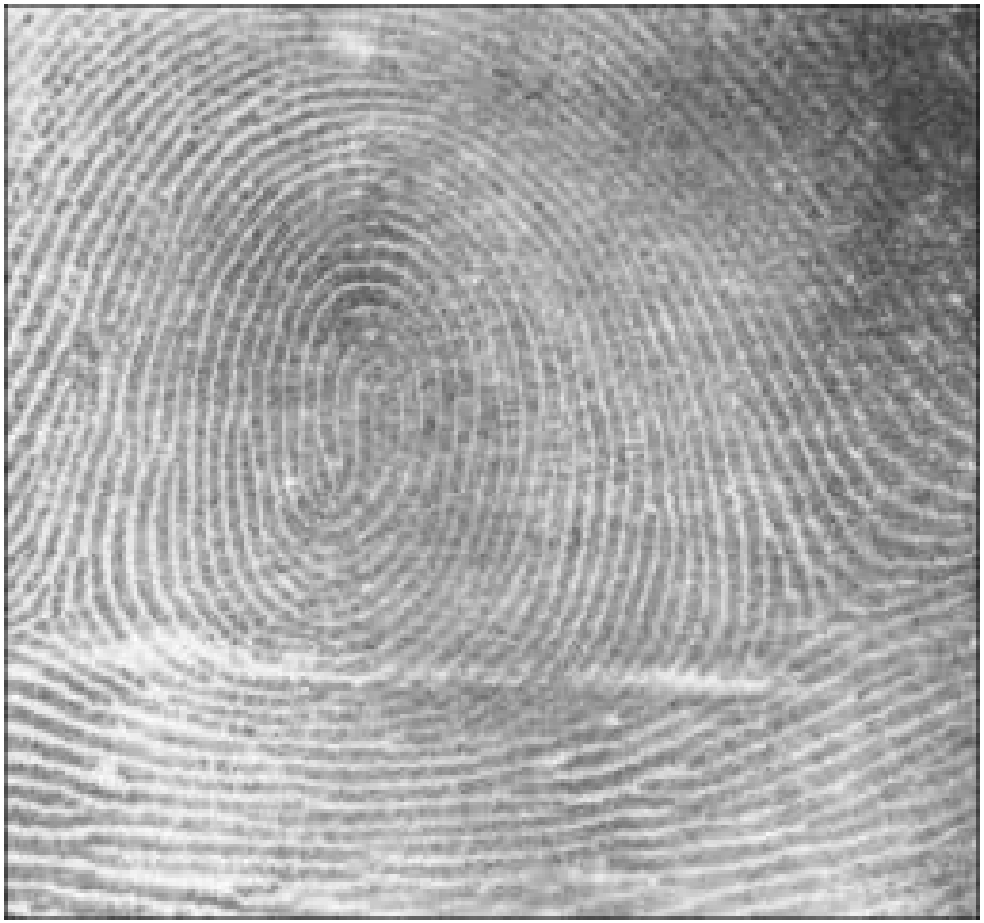
- The loop is a pattern where the ridges enter from one side of a finger, form a curve, and tend to exit from the same side they enter.



Source: Wikipedia

Fingerprint Ridge Patterns - Whorl

- Ridges form concentric circles around a central point on the finger.

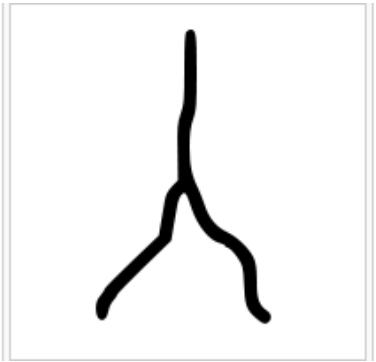


Source: Wikipedia

Fingerprint Minutia Features

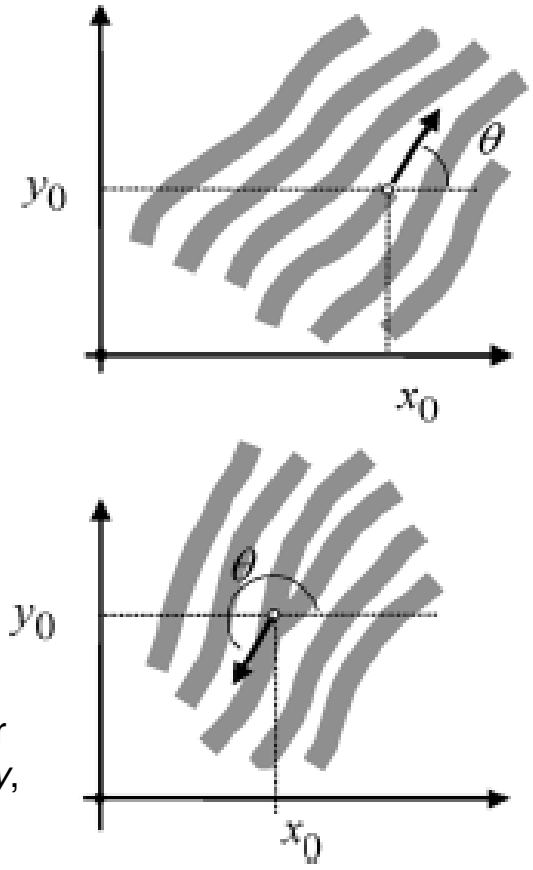
- The ridge ending is the point at which a ridge terminates.
- Bifurcations are points at which a single ridge splits into two ridges.
- Short ridges (or dots) are ridges which are significantly shorter than the average ridge length on the fingerprint.

Ridge Ending



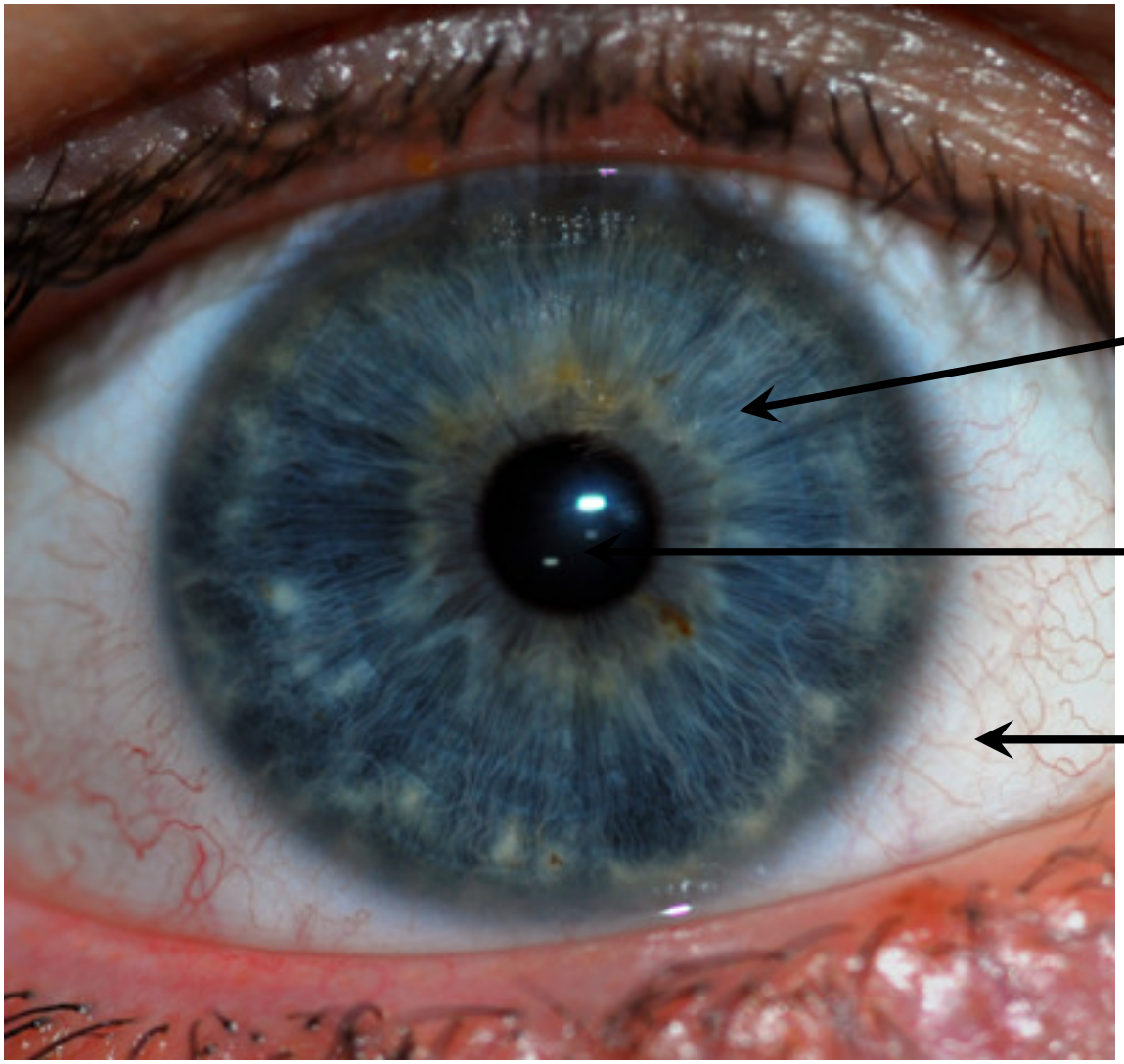
Bifurcation

Short Ridges (Dots)



Sources: Wikipedia, A. K. Jain, A. Ross and S. Pankanti, "Biometrics: A Tool for Information Security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125 – 143, June 2006.

Human Eye and the Iris



Source: Wikipedia

Iris Recognition

- The method involves capturing the detail-rich, intricate structures of the iris using near infra-red illumination (NIR, 750 nm wavelength) that would reduce the reflection (would be very noisy if visible light was used) from the cornea.
- The images captured through the infra-red camera are converted to digital templates to provide mathematical representations of the iris that yield unique positive identification of an individual.
- Iris (Plural: Irides) is a thin, circular structure in the eye, responsible for controlling the diameter and size of the pupil (the black hole) and the amount of light reaching the pupil.
- Eye color is normally classified according to the color of the iris, which can be green, blue, grey or brown.
- The muscles attached to the Iris expand or contract the pupil; the larger the pupil, the more light can enter.

Security Considerations

- Live-tissue Verification Problem: Iris recognition systems are vulnerable to the problem of live-tissue verification.
  - Any biometric identification system has to ensure that the signal acquired and compared has actually been recorded from a live body part of the person to be identified and is not a manufactured template.
  - Many commercially available Iris-recognition systems are easily fooled by presenting a high-quality photograph of a face instead of a real face. This makes Iris-recognition systems unsuitable for unsupervised applications like door access-control systems.
- The problem of live-tissue verification is of less concern in supervised applications (like immigration control), where a human operator supervises the process of taking the picture.

Face Recognition Systems

- A facial recognition system is used to automatically identify or verify a person from a digital image or a video frame from a video source.
  - One way to do this is to compare selected facial features (that are not easily altered – upper outlines of the eye sockets, the areas around the cheekbones, and the sides of the mouth) with those in the database.
- Key Advantage: One key advantage with facial recognition systems is that it does not require aid (or consent) from the rest subject.
  - Properly designed systems installed in airports, multiplexes, and other public places can identify individuals (though the correctness and effectiveness is often questionable!!) among the crowd.
  - Other biometric systems like fingerprints, iris scans, retinal scans, speech recognition and etc., cannot be used for in mass identification (surveillance).
- Weaknesses:
  - Sensitive to facial expressions (a big smile can make the system less effective) and the frontal orientation at which the photo is taken.
  - Privacy concerns as it could lead to a “total surveillance society”

Signature Recognition Systems

- Signature recognition refers to authenticating the identity of a user by measuring handwritten signatures.
- In a signature recognition system, a person signs his or her name on a digitized graphics tablet or a PDA.
- The signature is treated as a series of movements that contain unique biometric data, such as personal rhythm, acceleration, stroke order, stroke count and pressure flow.
- The signature dynamics information is encrypted and compressed into a template.

- Signature recognition systems (for hand signatures) measure how a signature is signed and are different from electronic signatures, which treat a signature as a graphic image.

Source: http://www.gao.gov/new.items/d031137t.pdf

Parameters Considered for Selecting a Human Characteristic

- Universality – each person should have the characteristic
- Uniqueness – how well the biometric separates one individual from another
- Permanence – how well the biometric resists aging and other variations over time
- Collectability – ease of acquisition for measurement
- Performance – accuracy, speed and robustness of technology used.
- Acceptability – degree of approval of a technology by the public/ users of the biometric
- Circumvention – ease of use of a substitute

Comparison of the Biometric Technologies vs. The Parameters

Biometric Identifier	Parameters/ Factors to Choose a Biometric Technology						
	Universality	Distinctiveness	Permanence	Collectable	Performance	Acceptability	No Circumvention
Face	Best	Best	Avg	Best	Poor	Best	Poor
Fingerprint	Avg	Best	Best	Avg	Best	Avg	Avg
Hand Geometry	Avg	Avg	Avg	Best	Avg	Avg	Avg
Iris	Best	Best	Best	Avg	Best	Poor	Best
Signature	Poor	Poor	Poor	Best	Poor	Best	Poor
Voice	Avg	Poor	Poor	Avg	Poor	Best	Poor