CIS 4360
Secure Computer Systems

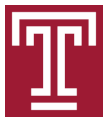
Biometrics
(Something You Are)

Professor Qiang Zeng

Spring 2017

Previous Class

- Credentials
  - Something you know (Knowledge factors)
  - Something you have (Possession factors)
  - Something you are (Inherence factors)
- How to store passwords securely?
- Multi-factor authentication
- Time-based One Time Password (OTP)
  - RSA's SecurID
  - Google Authenticator

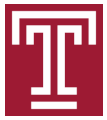


Previous class…

When you go to an ATM machine to withdraw money, is it two-factor authentication?

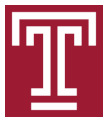
Yes.

Something you know: PIN
Something you have: Debit Card



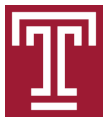
How to store user passwords

- Store hash values only (i.e., never store passwords as plaintext)
  - It will be a disaster if you store user passwords as plaintext and the server gets compromised
- Adding "salts" when hashing
  - Prevent rainbow table attack
  - Store "salt1, hash(salt1, password1); salt2, hash(salt2, password2); …"
  - Now the pre-computed rainbow table is useless
- Using a slow hash algorithm
  - Slow down Brute Force or Dictionary Attack



Outline

- What are Biometrics?
- What are Biometrics used for?
- Advantages and Disadvantages
- How to evaluate its effectiveness?
- Framework of a Biometric System
- Case studies
  - Fingerprint
  - Iris



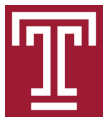
Biometrics

- Biometrics: the measurement and application of human characteristics
  - Bio-: life
  - -Metrics: to measure
- Applications:
  - Authentication: Something you are
  - Identification: To identify individuals

Identification vs. Authentication

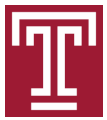
- **Identification (also known as One to Many)**
  - A sample is effectively matched against all templates in the database
  - The user only provide her biometric as input

- **Authentication (also known as Verification or One to One)**
  - The sample is matched against one pre-selected template.
  - The pre-selected template is determined by the claimed identity in the form of, e.g., username



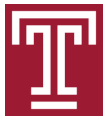
Biometrics are widely used

- Smartphones
- FBI
- US Immigration department
- Disney
- …



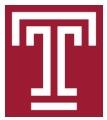
Advantages and Disadvantages

- Advantages
  - You do not need to remember sth. (as with passwords)
  - You do not need to carry sth. (as with security tokens)
  - More convenient and quicker (e.g., compared to typing)
  - Recognition can be automated (critical for police and FBI)
- Disadvantages
  - Some biometrics may be easily stolen, e.g., fingerprint
  - Accuracy
  - Users may not feel comfortable (e.g., scanning eyes)
  - Costly



Types of Biometrics

- Physiological Biometrics
  - Fingerprint
  - Hand Geometry
  - Iris
  - Face
  - DNA
- Behavioral Biometrics
  - Signature
  - Typing Rhythm
  - Gait



Market share

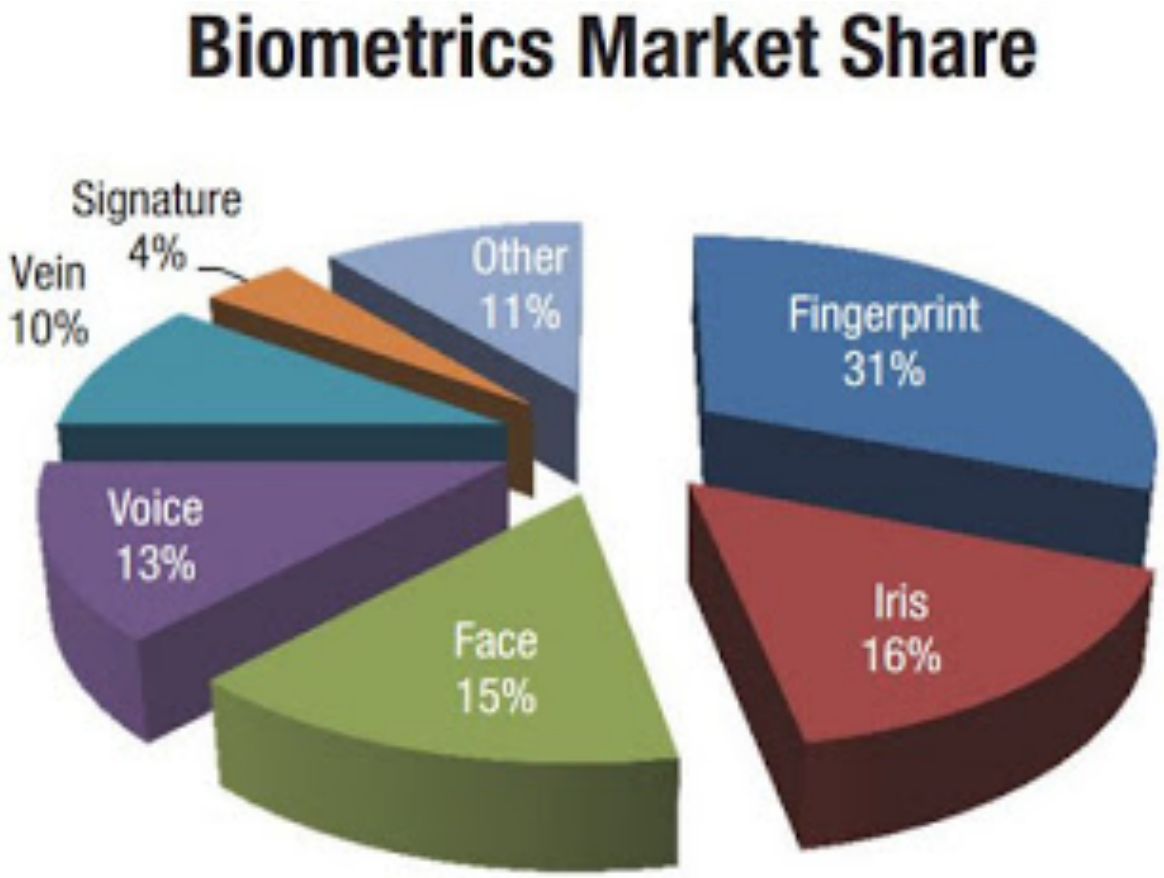
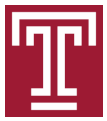
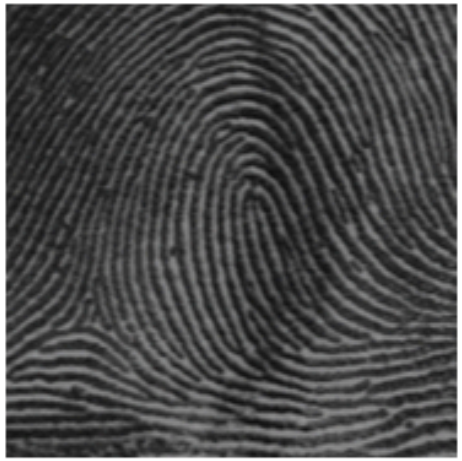


Figure 1: Biometrics market share by system type



Face



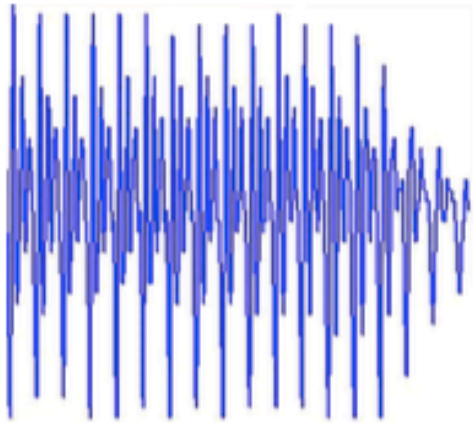
Fingerprint

Iris

Hand geometry

Palmprint

Signature

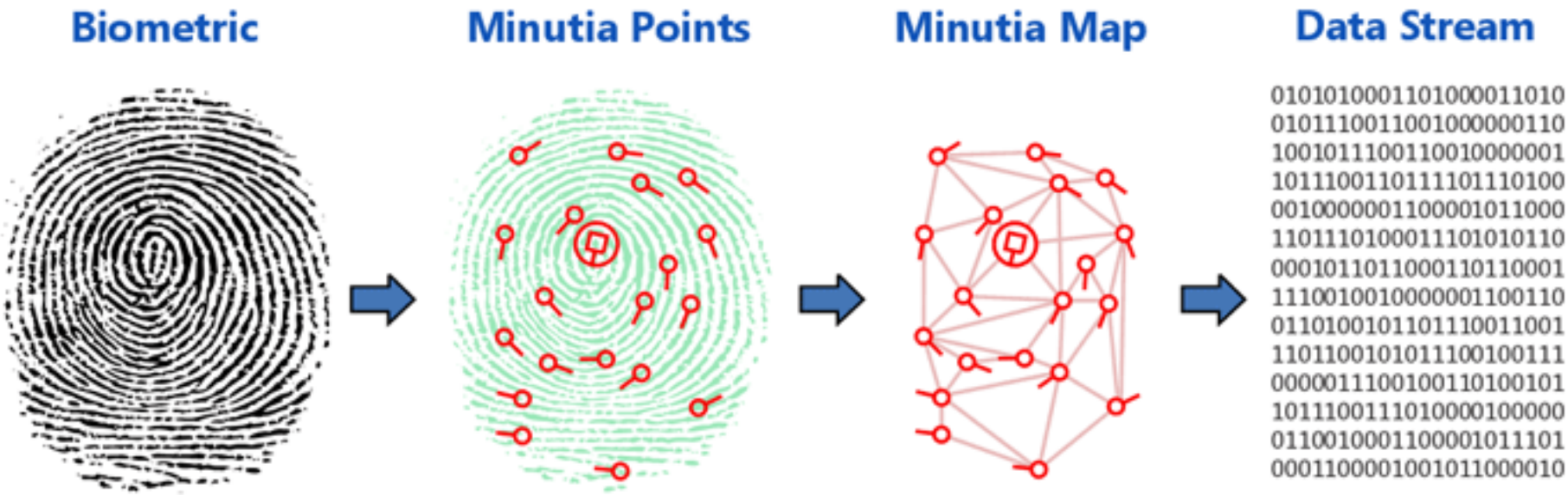


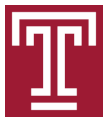
Voice

Gait

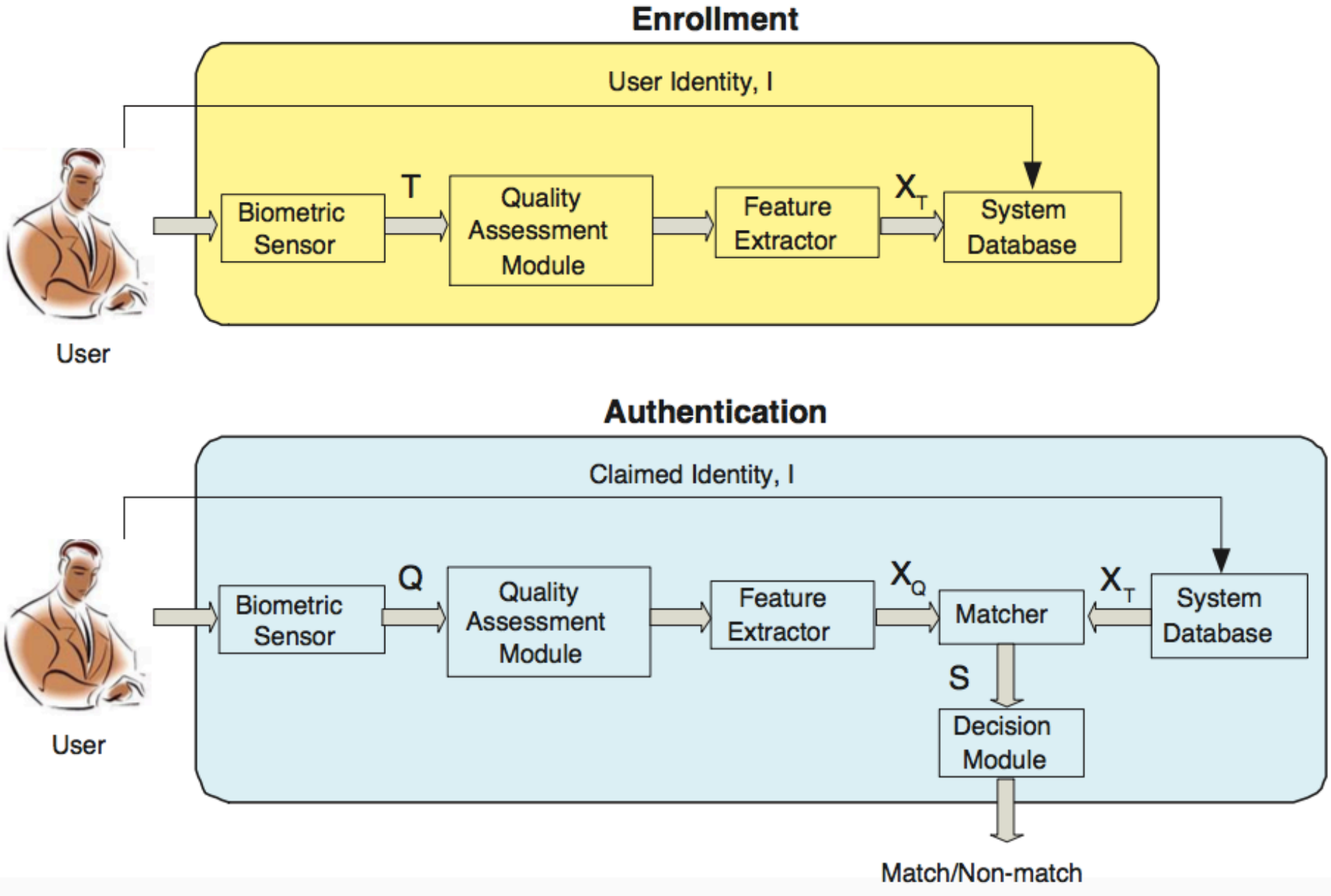
Biometric Template

- A biometric template is a digital representation of an individual's distinct characteristics



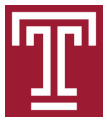


Framework of Applying Biometrics for Authentication



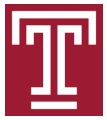
Five important components

- Sensor
  - Scans the biometric trait of the user
- Feature extractor
  - Processes the scanned biometric data to extract the template
- Template database
  - For storage
- Matcher
  - Compares two templates and outputs a similarity score
- Decision module
  - Determines “Yes” (matched) or “No” (not-matched)

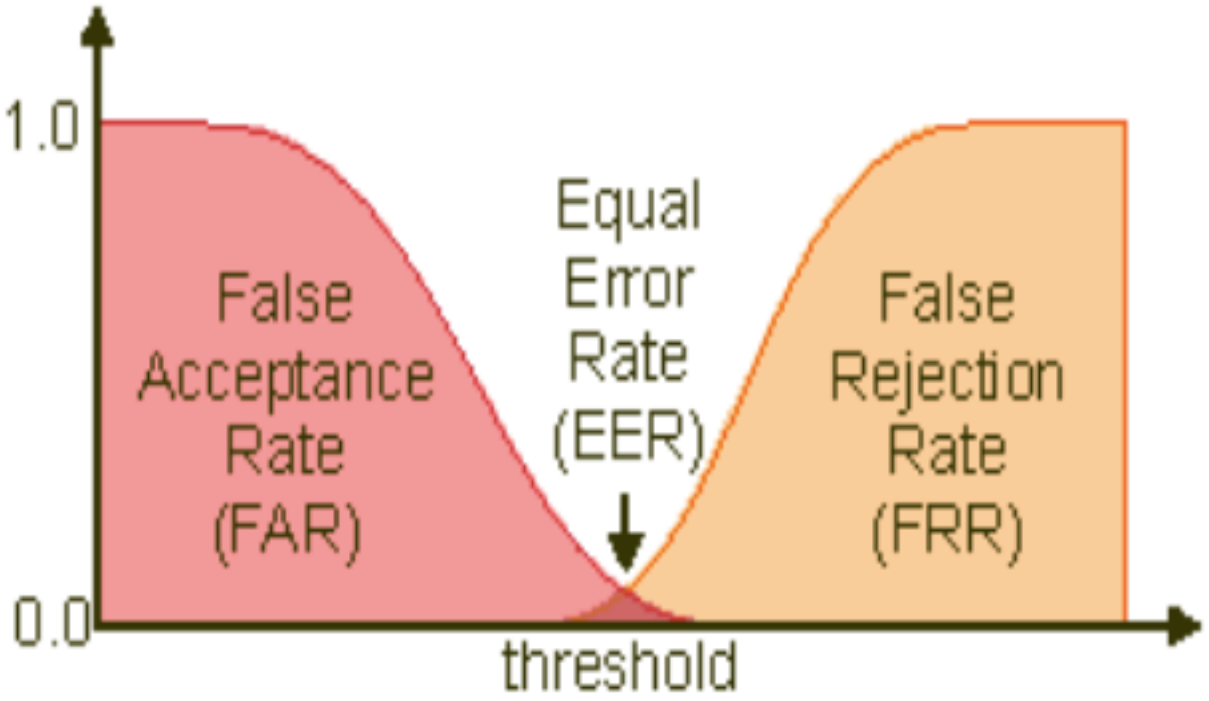


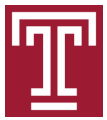
How to measure accuracy

- False Rejection Rate (FRR) as known as False Non-Match Rate (FNMR)
  - the percentage that the system fails to detect a match between a user's input template and the user's stored template
- False Acceptance Rate (FAR) also know as False Match Rate (FMR)
  - the percentage that the system incorrectly matches the input pattern to a non-matching template in the database.
  - Apple's TouchID: FAR is 1 in 50,000

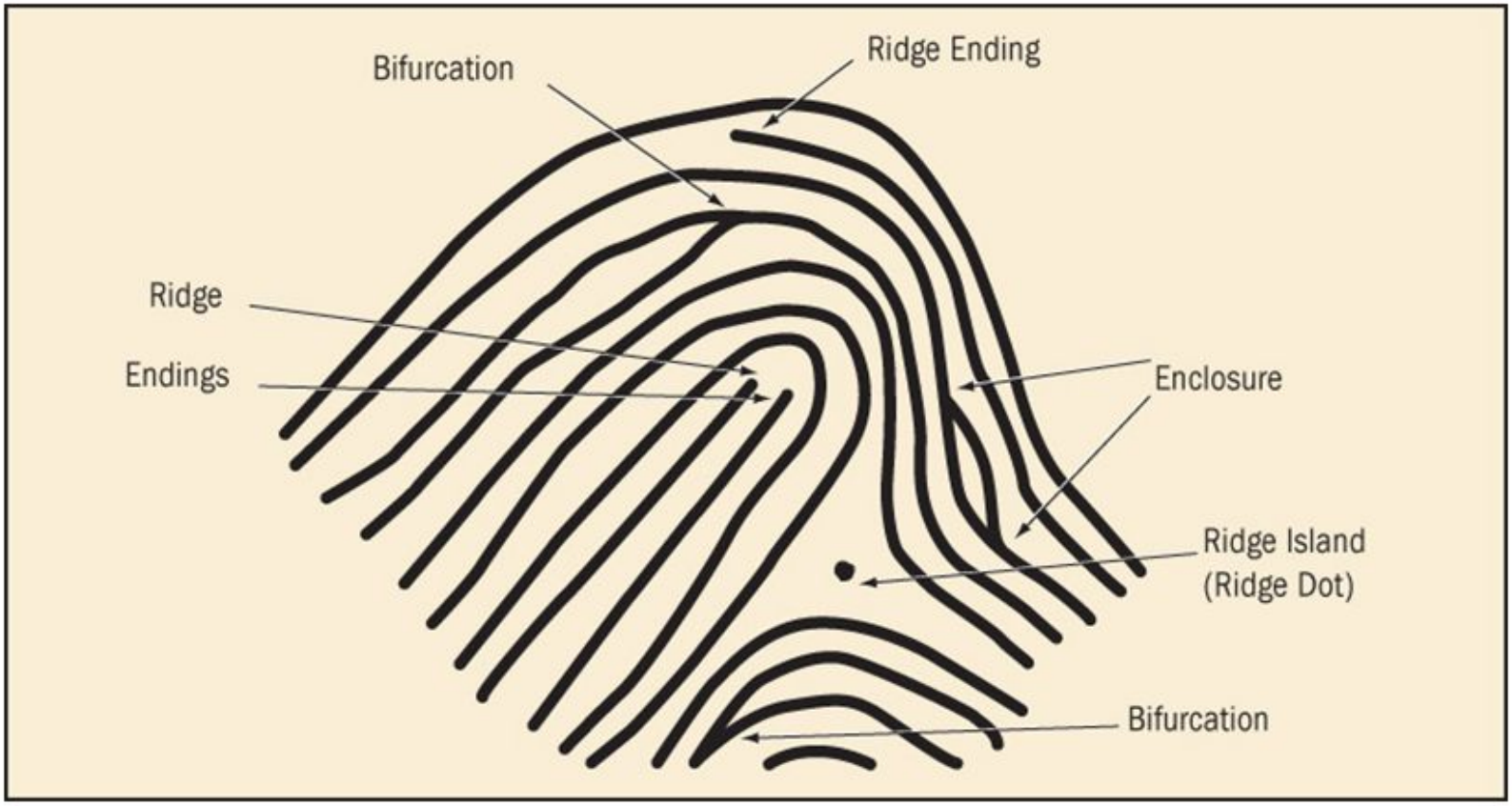


FRR and FAR


1.0
0.0
False Acceptance Rate (FAR)
Equal Error Rate (EER)
False Rejection Rate (FRR)
threshold

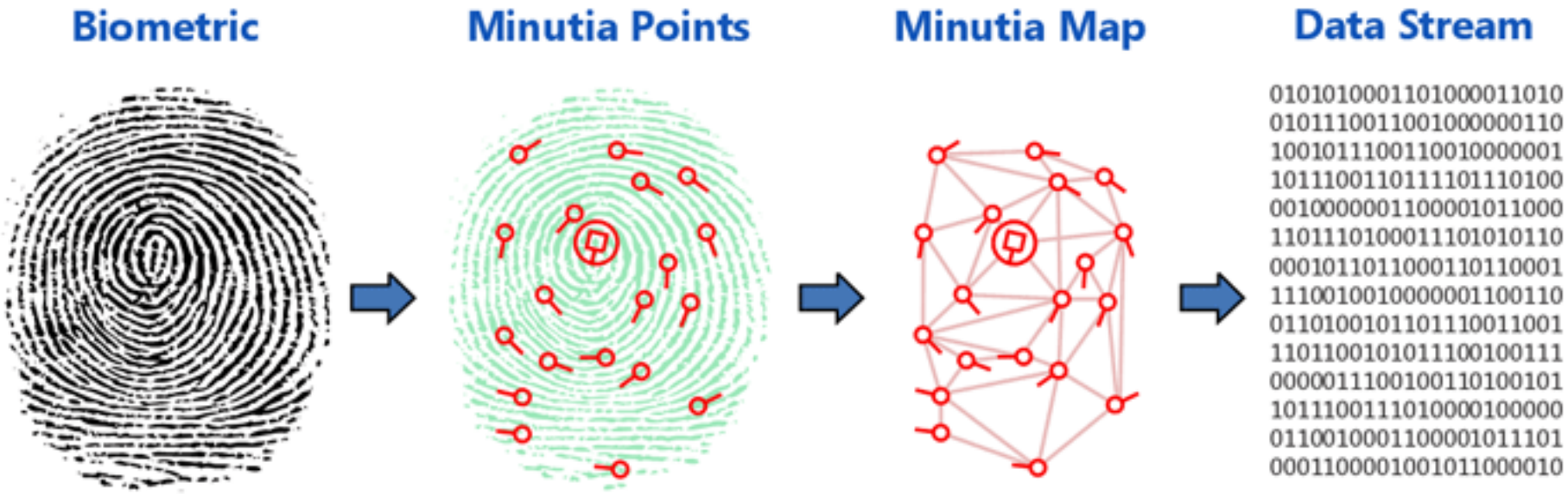


Fingerprint Characteristics

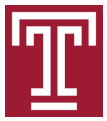


Fingerprint ridge characteristics. Courtesy Sirchie Finger Print Laboratories, Inc., Youngsville, N.C., www.sirchie.com

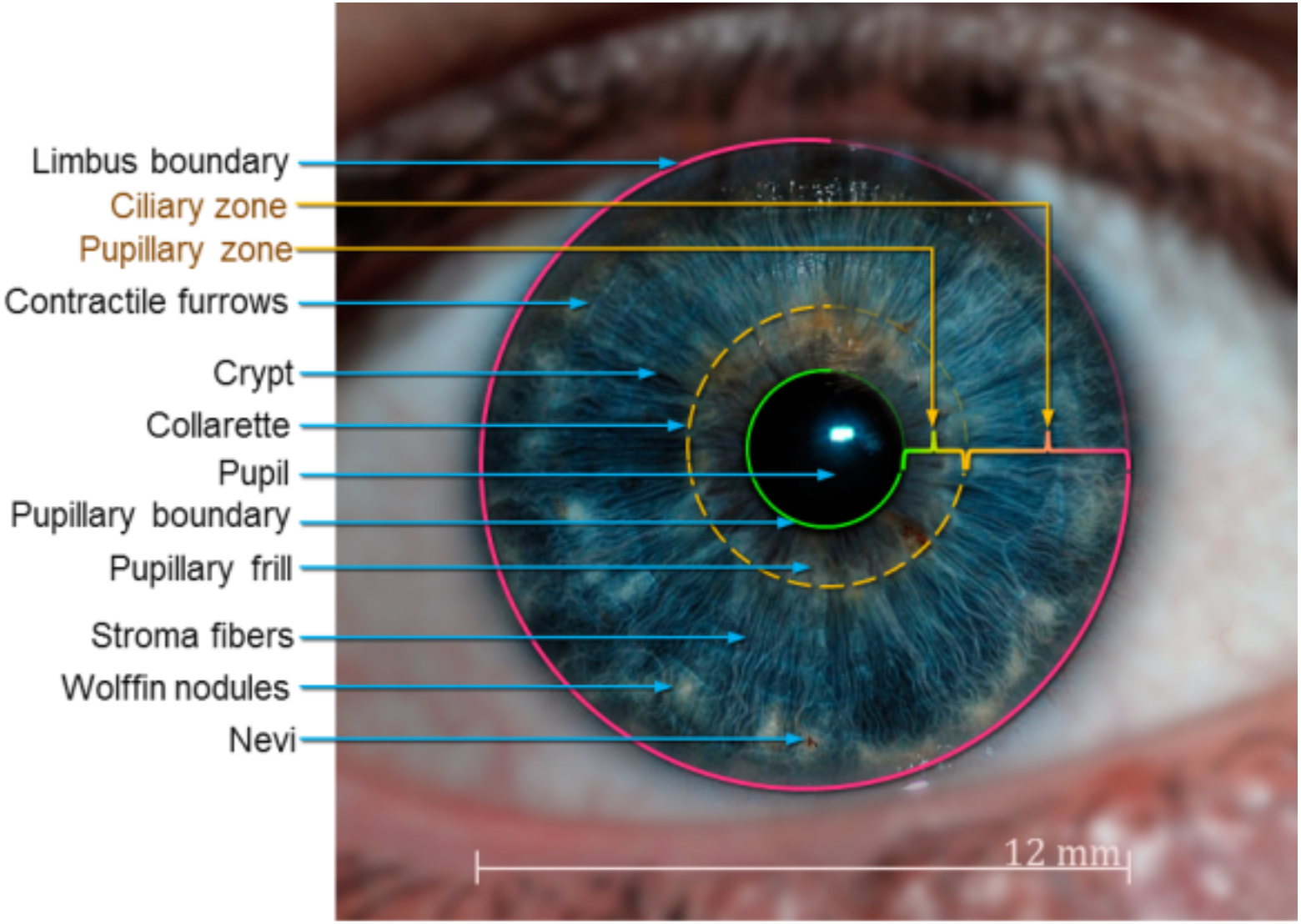
An example technology that extracts features from fingerprints



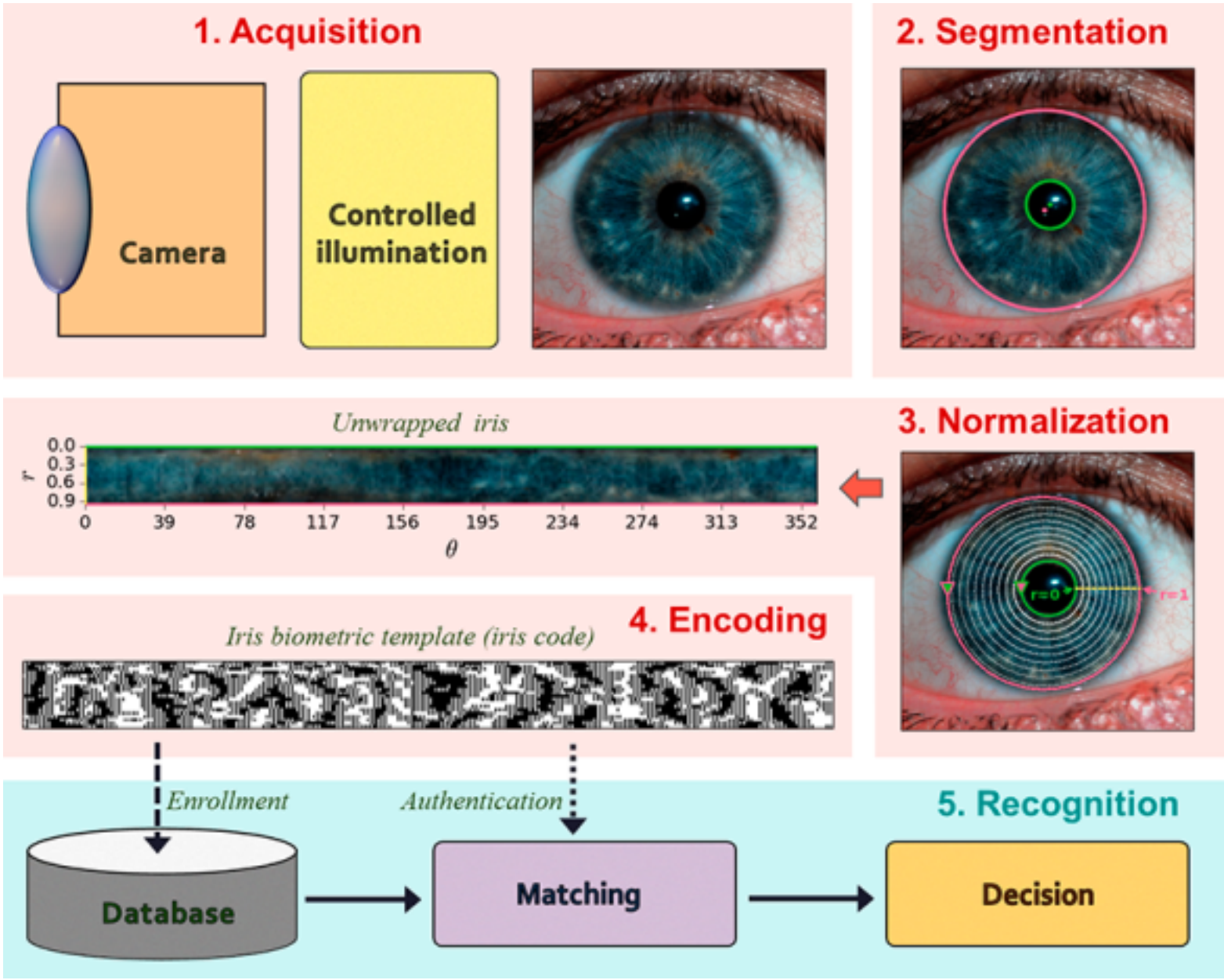
- A fingerprint is made of a series of ridges and grooves. Once a fingerprint is captured the system locates the minutia points where the lines of the ridges begin, end, branch off and merge.
- These points are then mapped and lines are drawn between points. This creates a map of how each point relates to the other points. The map is then stored as a data stream called a **minutia template**



Iris Recognition

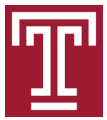


Source (eye image): Dr. Jan Drewes. www.jandrewes.de

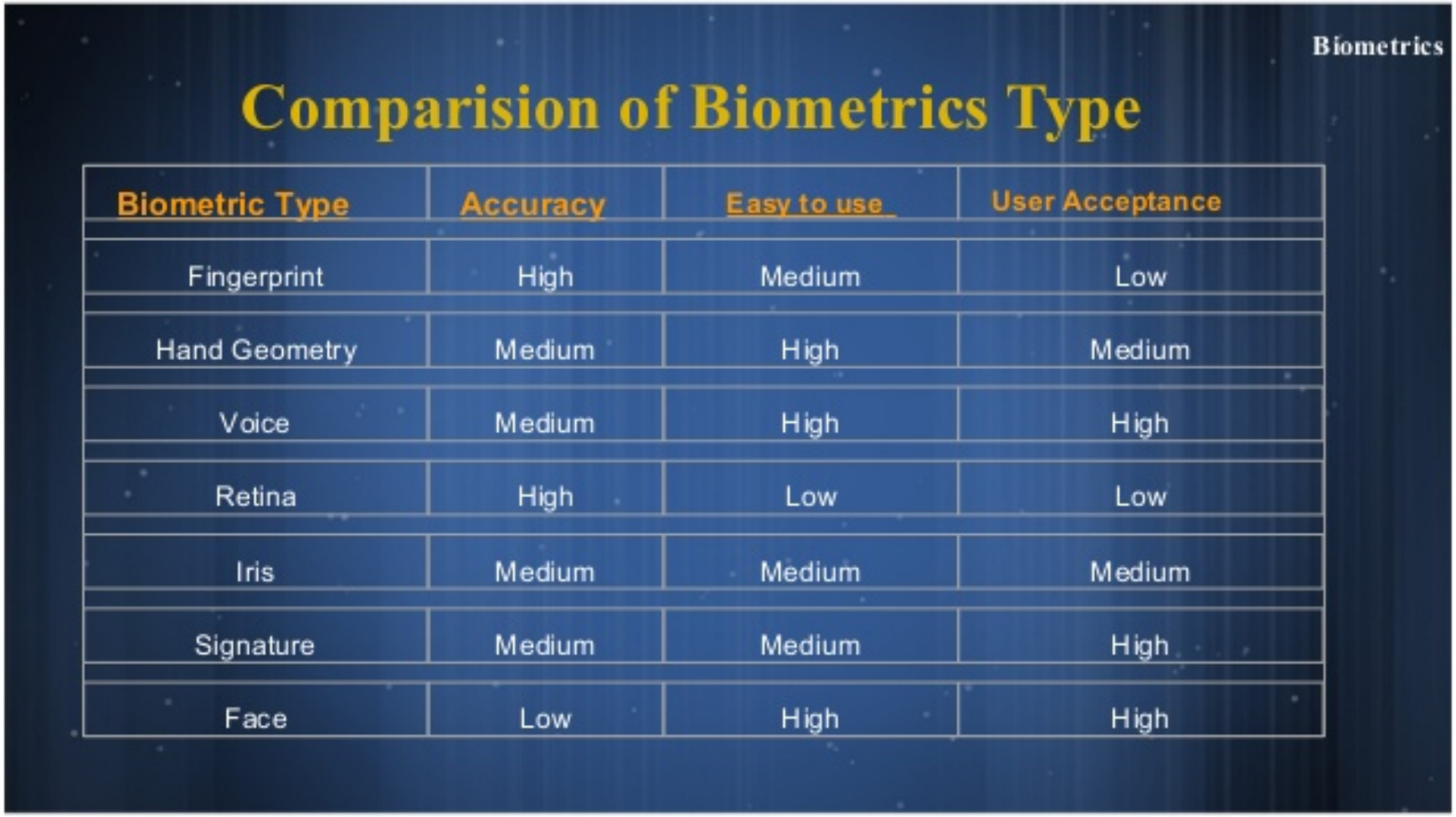

1. Acquisition
Camera
Controlled illumination
2. Segmentation
Unwrapped iris
0.0
0.3
0.6
0.9
r
0
39
78
117
156
195
234
274
313
352
θ
3. Normalization
r=0
r=1
4. Encoding
Iris biometric template (iris code)
Enrollment
Authentication
5. Recognition
Database
Matching
Decision

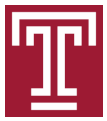
Some systems do not work well (yet)

- Voice recognition is hard because there are filters which can make a female voice seem male and makes you sound like another, etc.
- Face recognition currently has error rates that are too high.
- Typing patterns, walking patterns ("gait"), etc.



Comparison


Biometrics
Comparision of Biometrics Type
Biometric Type
Accuracy
Easy to use
User Acceptance
Fingerprint
High
Medium
Low
Hand Geometry
Medium
High
Medium
Voice
Medium
High
High
Retina
High
Low
Low
Iris
Medium
Medium
Medium
Signature
Medium
Medium
High
Face
Low
High
High



Summary

- Biometrics
  - Measurement and applications of human characteristics
- Applications
  - Identification
  - Authentication
- False rejection rate; false accept rate
- Fingerprint
- Iris