EEE-6561 Fundamentals of Biometric Identification

January 24th, 2018

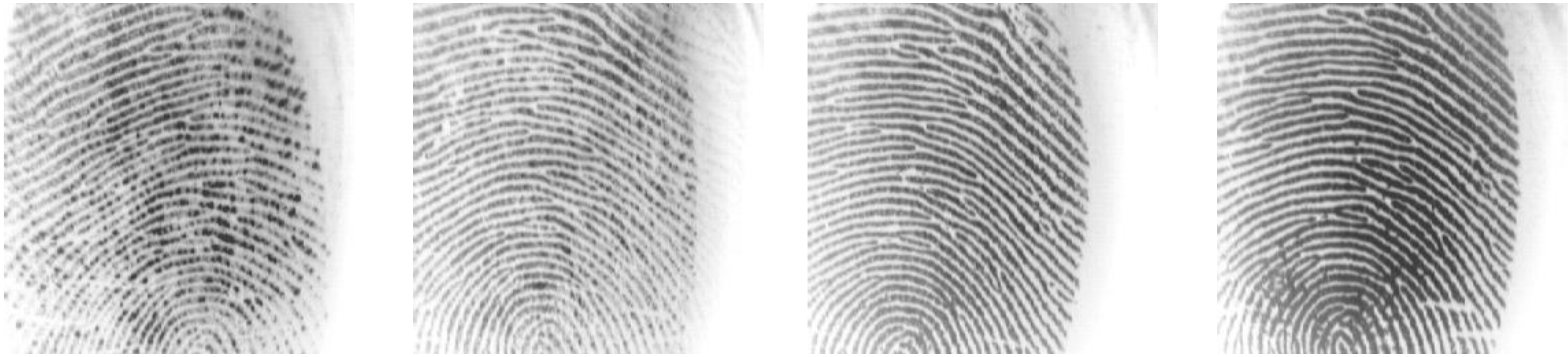
Lecture #4 Biometric System Evaluation and Design

Damon L. Woodard, Ph.D.
Dept. of Electrical and Computer Engineering
dwoodard@ece.ufl.edu

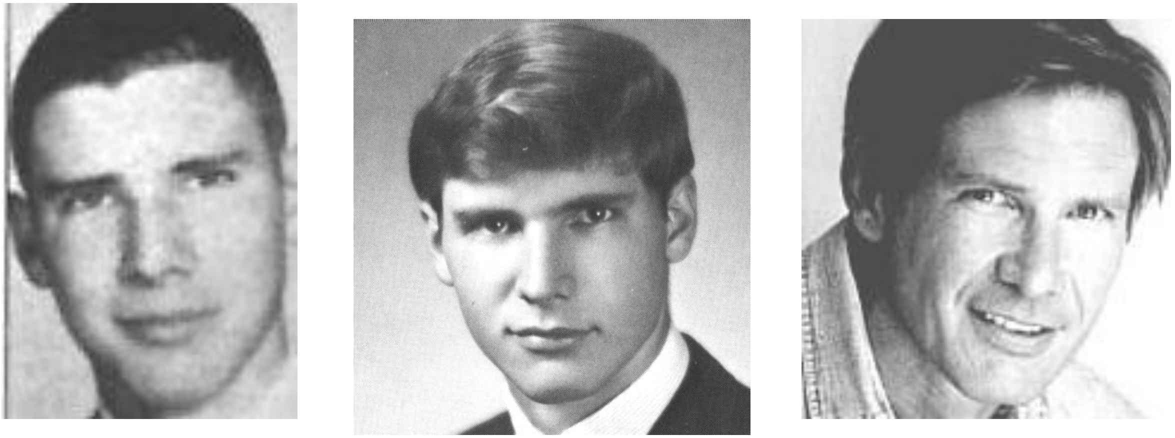
Temporal Variations

Uludag, Ross, Jain, "Biometric Template Selection and Update: A Case Study in Fingerprints", Pattern Recognition, 2004.

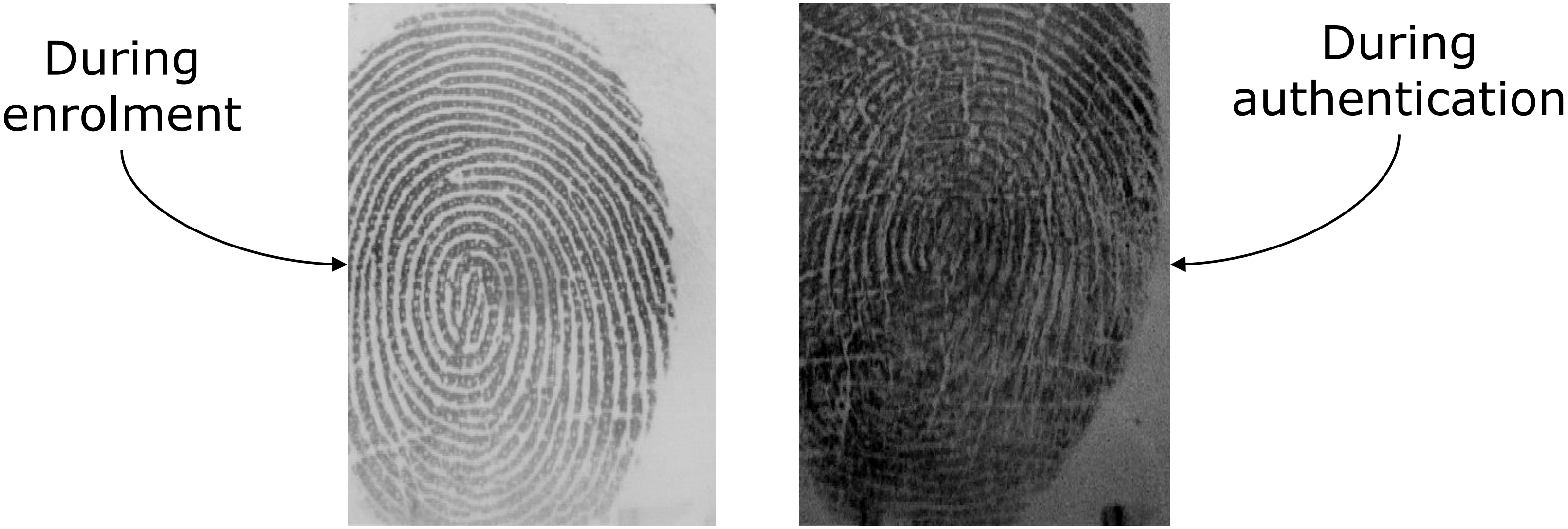
Time duration: 6 months



Time duration: several years

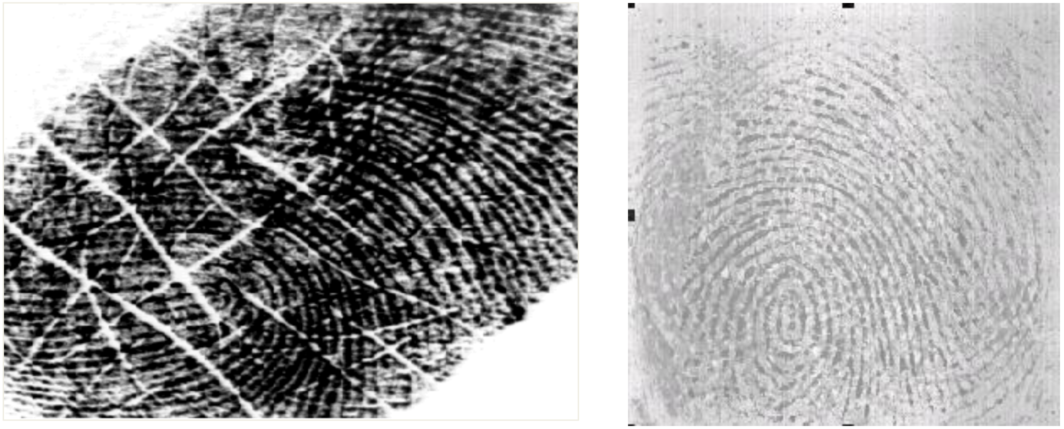


Noise in sensed data



During enrolment

During authentication



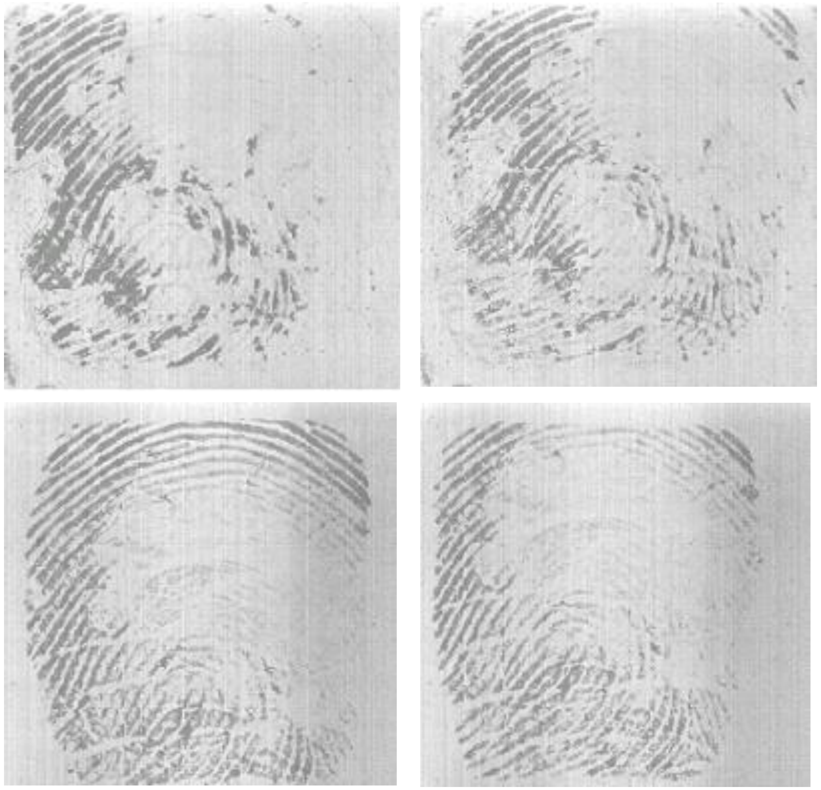
Noise due to smearing, residual deposits, cuts and folds, etc.

Rotation and Translation

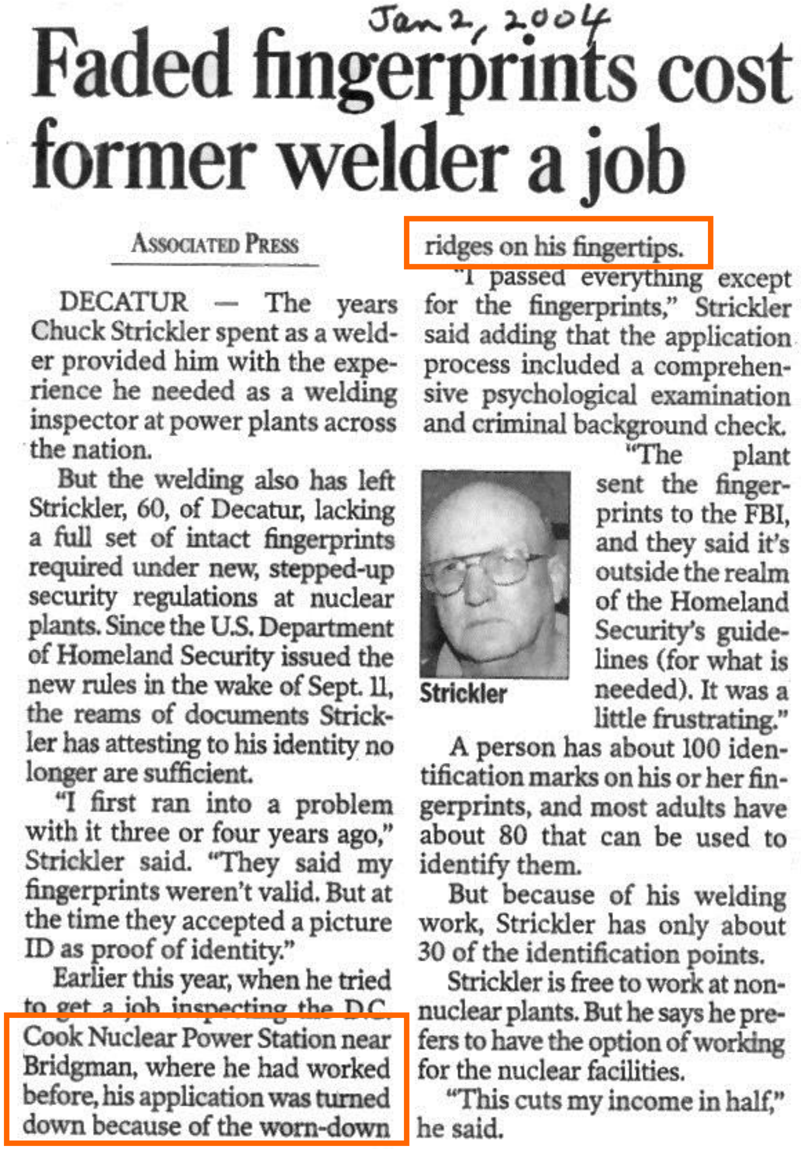
Non-linear Deformation

Failure to Enroll

A fraction of the population has poor quality fingerprint images



Four impressions of a user's fingerprint



Jan 2, 2004

Faded fingerprints cost former welder a job

Associated Press

DECATUR — The years Chuck Strickler spent as a welder provided him with the experience he needed as a welding inspector at power plants across the nation.

But the welding also has left Strickler, 60, of Decatur, lacking a full set of intact fingerprints required under new, stepped-up security regulations at nuclear plants. Since the U.S. Department of Homeland Security issued the new rules in the wake of Sept. 11, the reams of documents Strickler has attesting to his identity no longer are sufficient.

"I first ran into a problem with it three or four years ago," Strickler said. "They said my fingerprints weren't valid. But at the time they accepted a picture ID as proof of identity."

Earlier this year, when he tried to get a job inspecting the D.C. Cook Nuclear Power Station near Bridgman, where he had worked before, his application was turned down because of the worn-down ridges on his fingertips.

"I passed everything except for the fingerprints," Strickler said adding that the application process included a comprehensive psychological examination and criminal background check.

Strickler

"The plant sent the fingerprints to the FBI, and they said it's outside the realm of the Homeland Security's guidelines (for what is needed). It was a little frustrating."

A person has about 100 identification marks on his or her fingerprints, and most adults have about 80 that can be used to identify them.

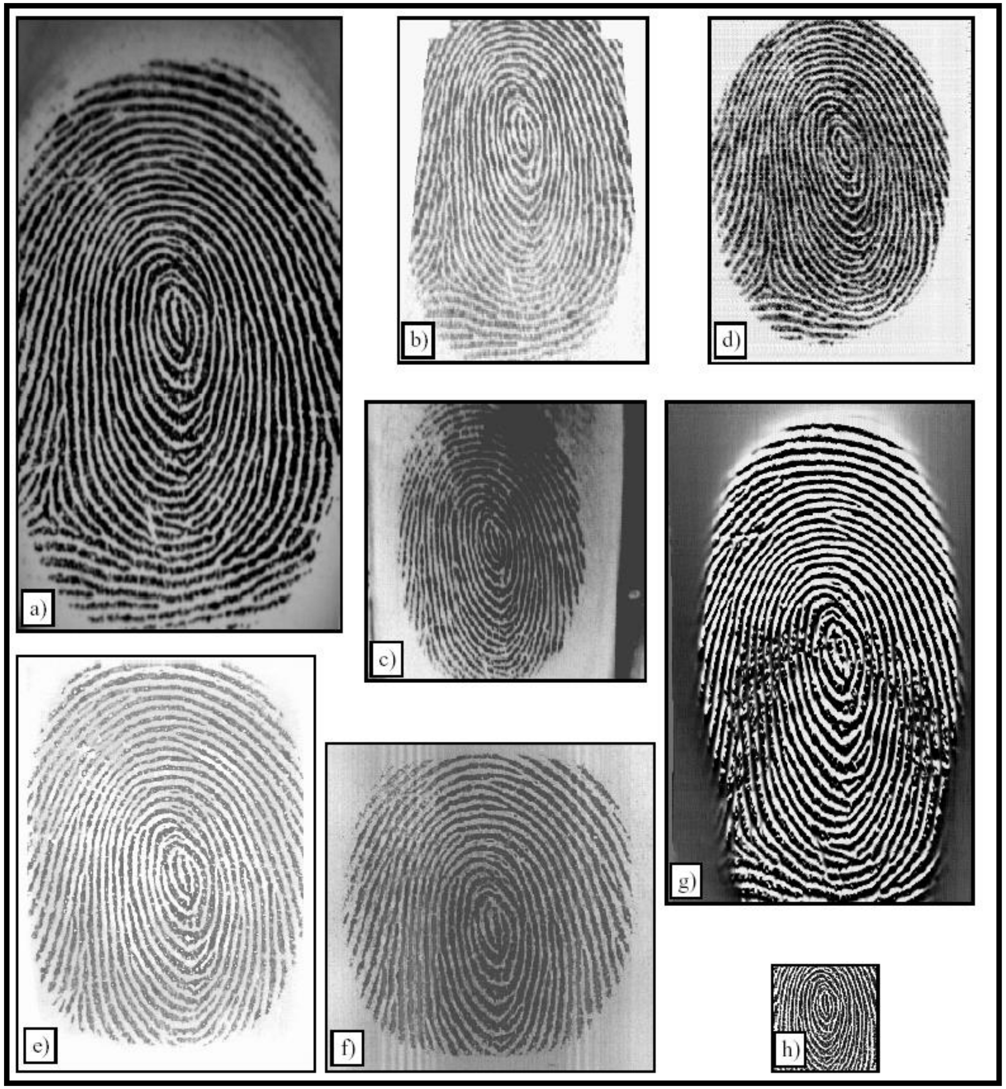
But because of his welding work, Strickler has only about 30 of the identification points.

Strickler is free to work at non-nuclear plants. But he says he prefers to have the option of working for the nuclear facilities.

"This cuts my income in half," he said.

Sensor Interoperability

- There is a degradation in matching accuracy when the sensors used for enrollment and recognition are different



- Fingerprint images of the same finger acquired by different commercial scanners:*

  a) Biometrika FX2000,

  b) Digital Persona UareU2000,

  c) Identix DFR200,

  d) Ethentica TactilSense T-FPM,

  e) STMicroelectronics TouchChip TCS1AD,

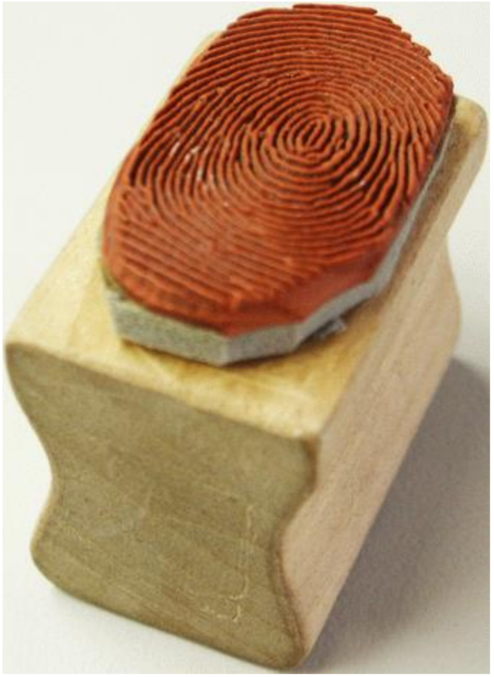
  f) Veridicom FPS110,

  g) Atmel FingerChip AT77C101B,

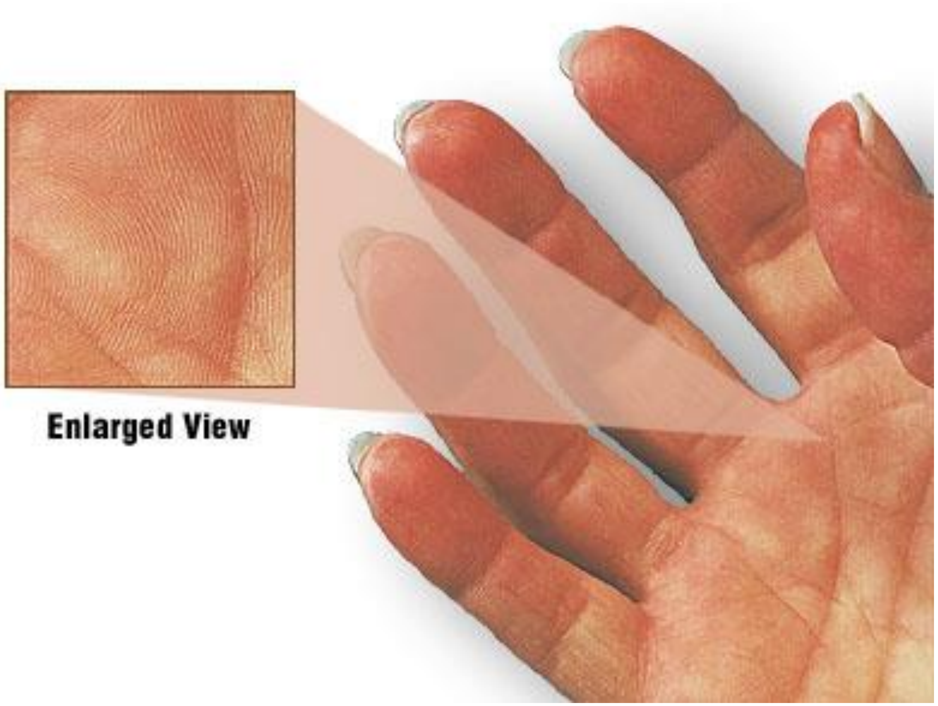
  h) Authentec AES4000

Maio, Maltoni, Jain, Prabhakar, "Handbook of fingerprint recognition", Springer 2003

Spoofing a Biometric Trait

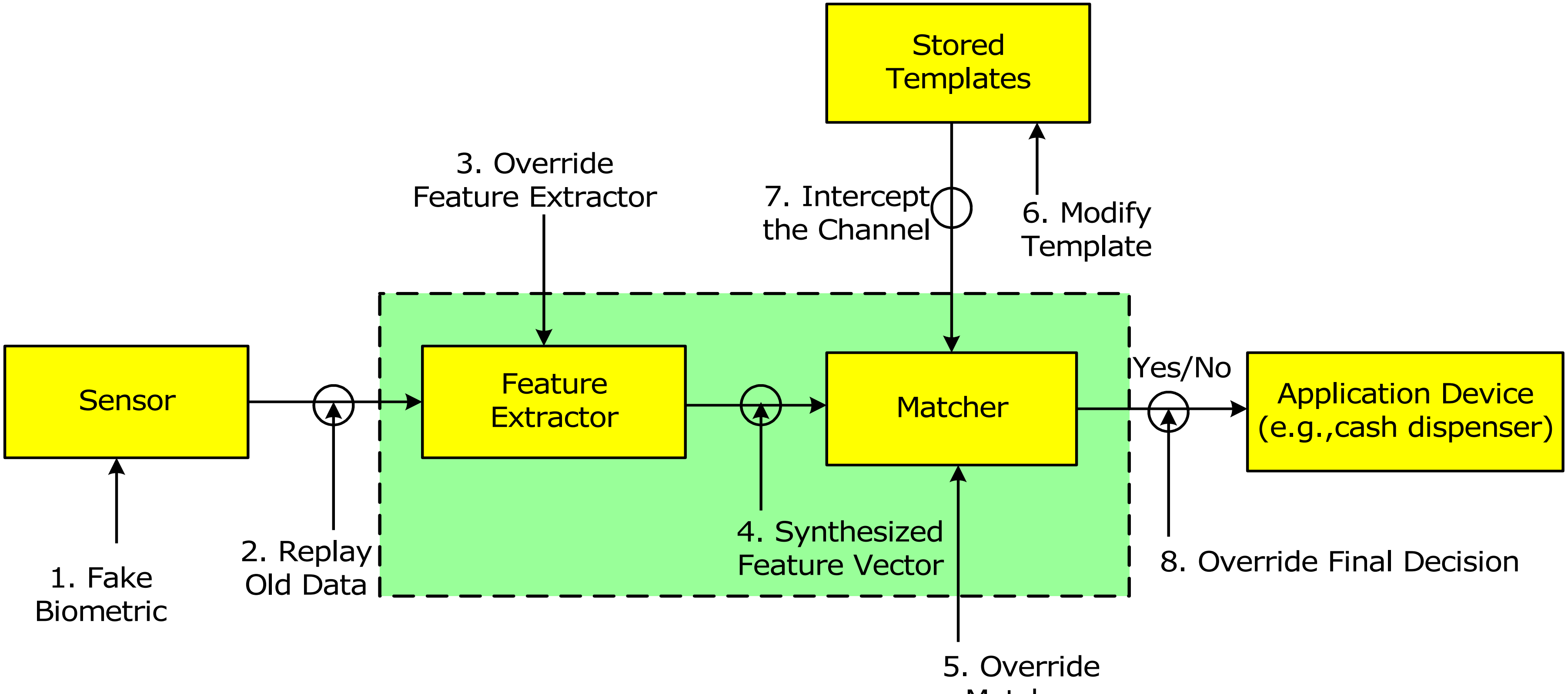


Dummy finger created from a lifted impression



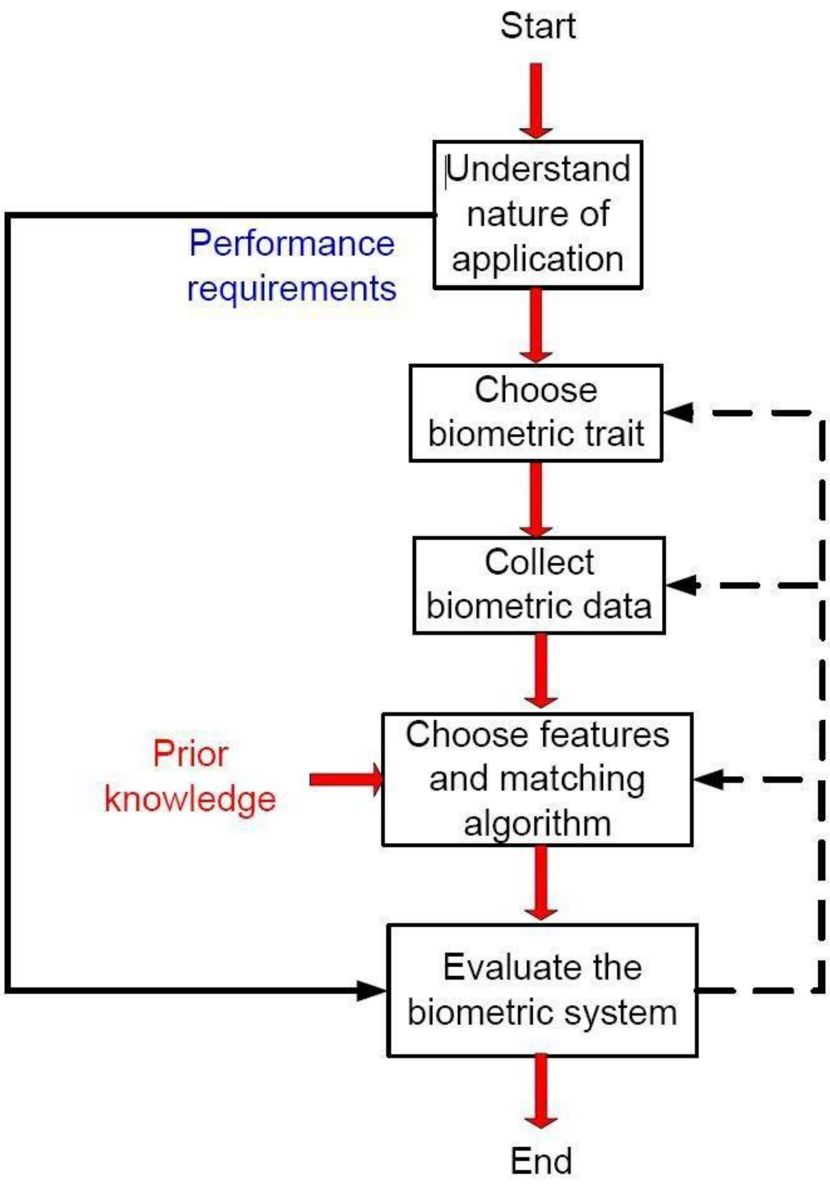
Artificial skin/fingers

Attacks on Biometric Systems



Design Cycle of Biometrics Systems

Design Cycles of Biometric Systems


Start
Understand nature of application
Performance requirements
Choose biometric trait
Collect biometric data
Prior knowledge
Choose features and matching algorithm
Evaluate the biometric system
End

Nature of the Application

- In some applications, biometrics may be used to supplement ID cards and passwords, thereby imparting an additional level of security. Such an arrangement is often called a *multi-factor authentication* scheme
- Depending on the application, we may need to choose between the verification and identification functionalities
  - This choice need not be always mutually exclusive
  - Example: In the large-scale national ID systems, one may need to perform *negative identification* during enrollment to prevent the possibility of the same user acquiring multiple identities

Nature of Application (cont.)

- Most of the commercial applications of biometrics, such as access to secure facilities, have the following attributes:
- – verification, cooperative, overt, habituated, attended enrollment and non-attended authentication, and closed

Choice of Biometric Trait

- A number of biometric traits are being used in various applications.
- Each biometric trait has its pros and cons.
- The choice of a biometric trait for a particular application depends on a variety of issues besides its recognition performance.
- The choice of traits depends on its universality, uniqueness, permanence, measurability, performance, acceptability, and circumvention.

Summary of Biometrics Traits

- No single biometric is expected to effectively meet all the requirements (e.g., accuracy, practicality, cost) imposed by all applications
  - e.g., forensics, access control, government benefits programs, etc.
- No biometric is *ideal,* but a number of them are *admissible*
- The relevance of a specific biometric to an application is established depending upon the nature and requirements of the application, and the properties of the biometric characteristic

Data Collection

- Data is required both for designing the feature extraction and matcher modules as well as for the evaluation of the designed biometric system
- Care must also be taken to ensure that the database is neither too challenging (collected under the most adverse conditions) nor too easy (collected under the most favorable conditions)
- Ideally, a database should include samples that are representative of the population and must preferably exhibit realistic intra-class variations
  - e.g., collecting data over multiple sessions, spread over a period of time, and in different environmental conditions

Choice of Features and Matching Algorithm

- Most of the research and development in the field of biometrics has been focused on this issue
- Needs some prior knowledge about the biometric trait under consideration
  - e.g., prior knowledge about the “uniqueness” of minutia points facilitated the development of minutiae-based fingerprint recognition systems
- Another important factor is the *interoperability* between biometric systems
  - e.g., the performance of face recognition algorithms is severely affected when the images used for comparison are captured using different camera types

Evaluation

- Evaluation of a complete biometric system is a complex and challenging task
- Questions to address for evaluation:
- What are the error rates of the biometric system in a given application?
  - (matching or technical performance)
- What is the reliability, availability, and maintainability of the system?
  - (engineering performance)
- What are the vulnerabilities of the biometric system?
  - What level of security does the biometric system provide to the application in which it is embedded?
  - (security of the biometric system)
- What is the user acceptability of the system?
  - How does the system address human factor issues like habituation and privacy concerns?
  - (user concerns)
- What is the cost and throughput of the biometric system and what tangible benefits can be derived from its deployment?
  - (return on investment)

Questions?

Slide Credits

Material used from Introduction to Biometrics text authors Arun Ross and Anil Jain as well as Walter Scheirer