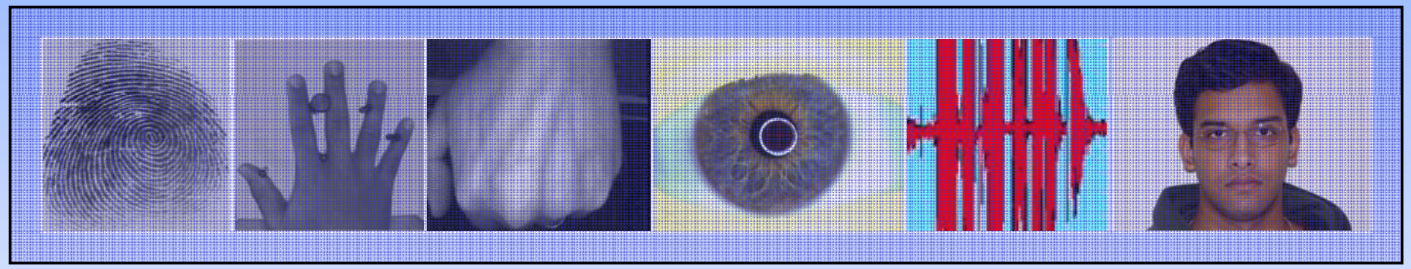
HSPD24: Data Organization, Security and Interoperability Challenges



Arun Ross

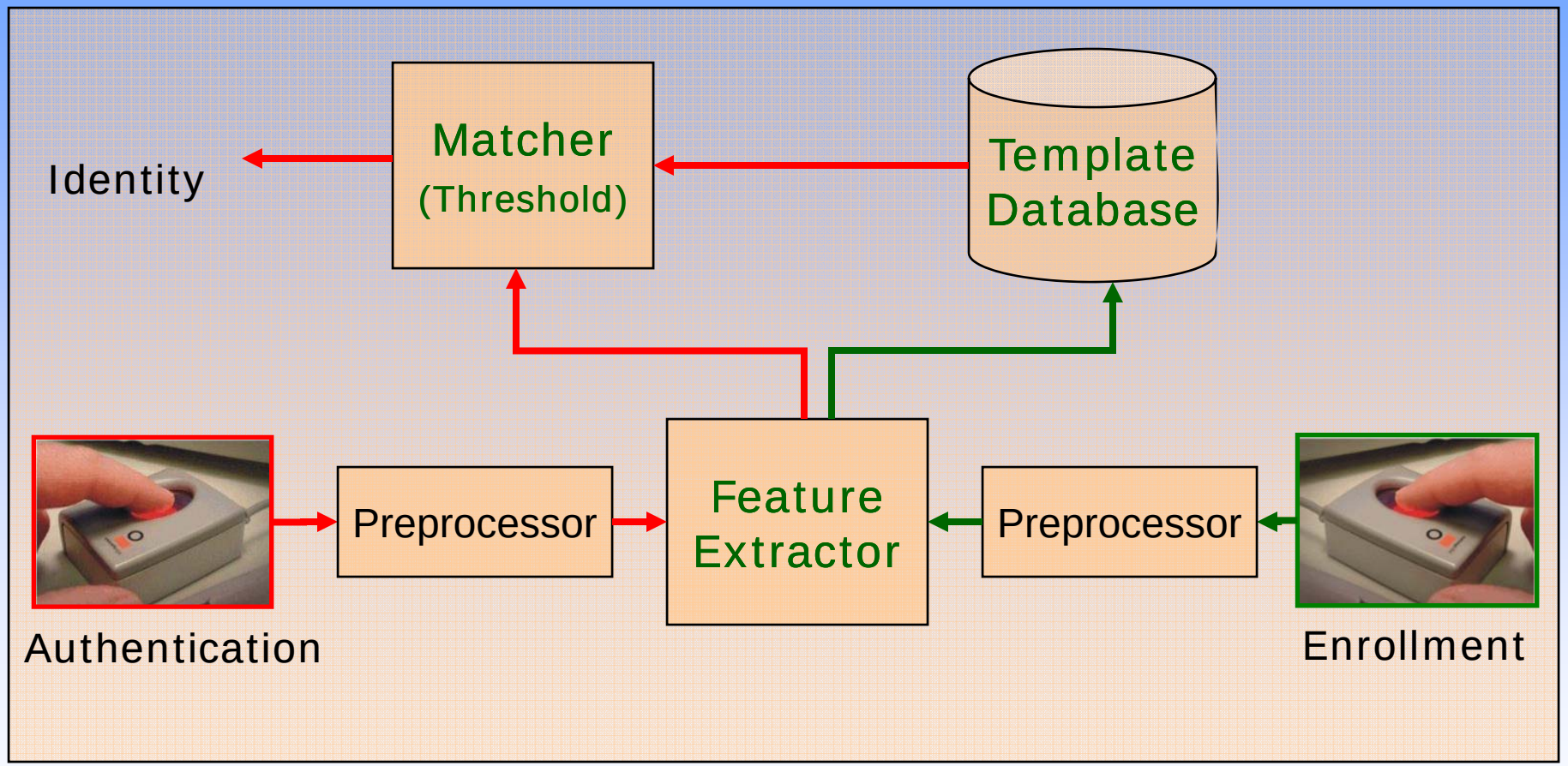
Associate Professor
West Virginia University
Morgantown, West Virginia, USA
Arun.Ross@mail.wvu.edu

http://www.csee.wvu.edu/~ross

HSPD 24

"….use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law."

Biometrics: A Pattern Recognition System



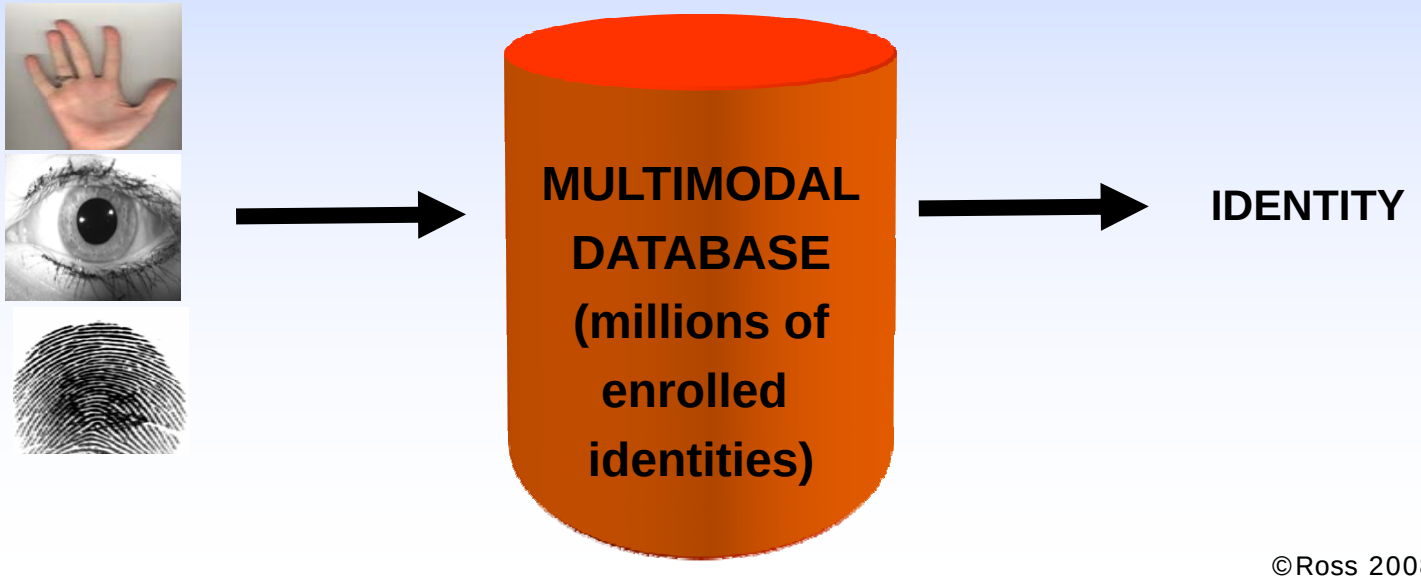
- False accept rate (FAR): Proportion of impostors accepted
- False reject rate (FRR): Proportion of genuine users rejected
- Failure to enroll (FTE) rate
- Failure to acquire (FTA) rate

Multimodal Databases

- Biometric databases are being increasingly populated by multimodal data of an individual
- This data can be categorized as:
  - Biographic/Demographic: age, gender, ethnicity, height, eye color
  - Biometric: fingerprint, face, iris
- Searching through the entire database to retrieve the correct identity is a time-consuming task that significantly impacts the system response time

Search and Retrieve Problem

- Given a suspect's multimodal biometric information (e.g., fingerprint, iris, palm), determine if his identity is present in a large multimodal database as quickly as possible
- Indexing techniques are needed to restrict the search to a subset of the database for a quick answer



Biometric Indexing

Sensor

Feature Extractor

FEATURES

INDICES

Decision

Matcher

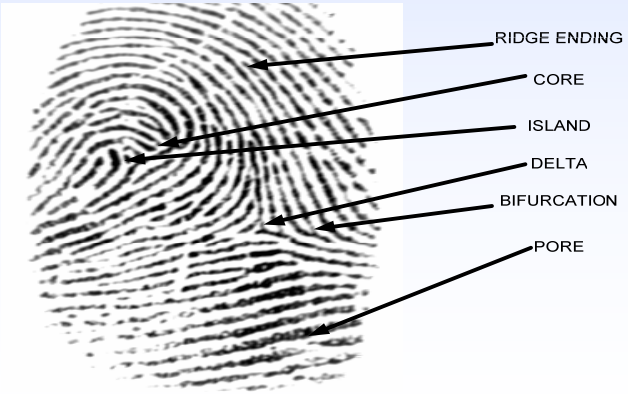
Retrieve Templates

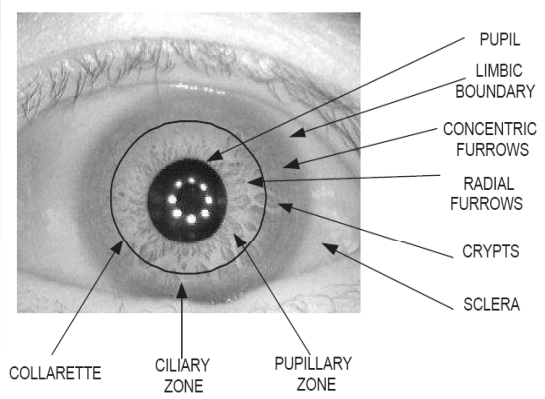
user01 001100...
user02 010011...
user03 100110...

Template Database

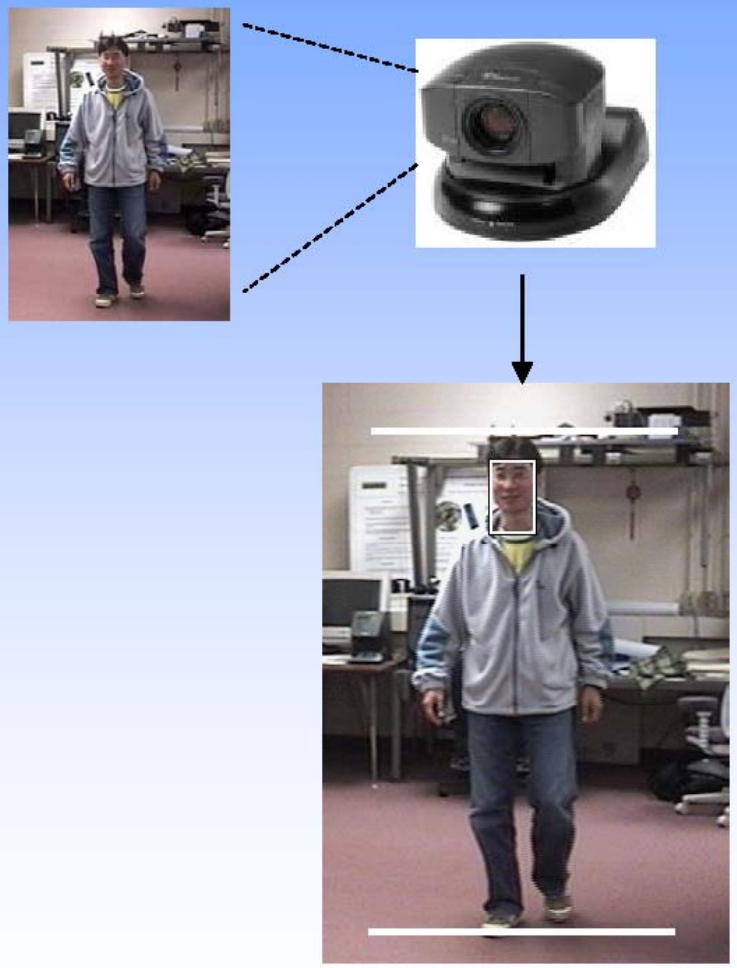
Multibiometric Indexing

- The fingerprint modality can narrow the number of possible matches and direct the query image to a particular “bin” of identities
- Then the iris modality can be used
  - to retrieve the best match from this “bin” of identities
  - cluster the “bin” of identities further in order to further prune the search space





Soft biometric traits



Height: 5.9 ft.

Eye color: black

Gender: Male

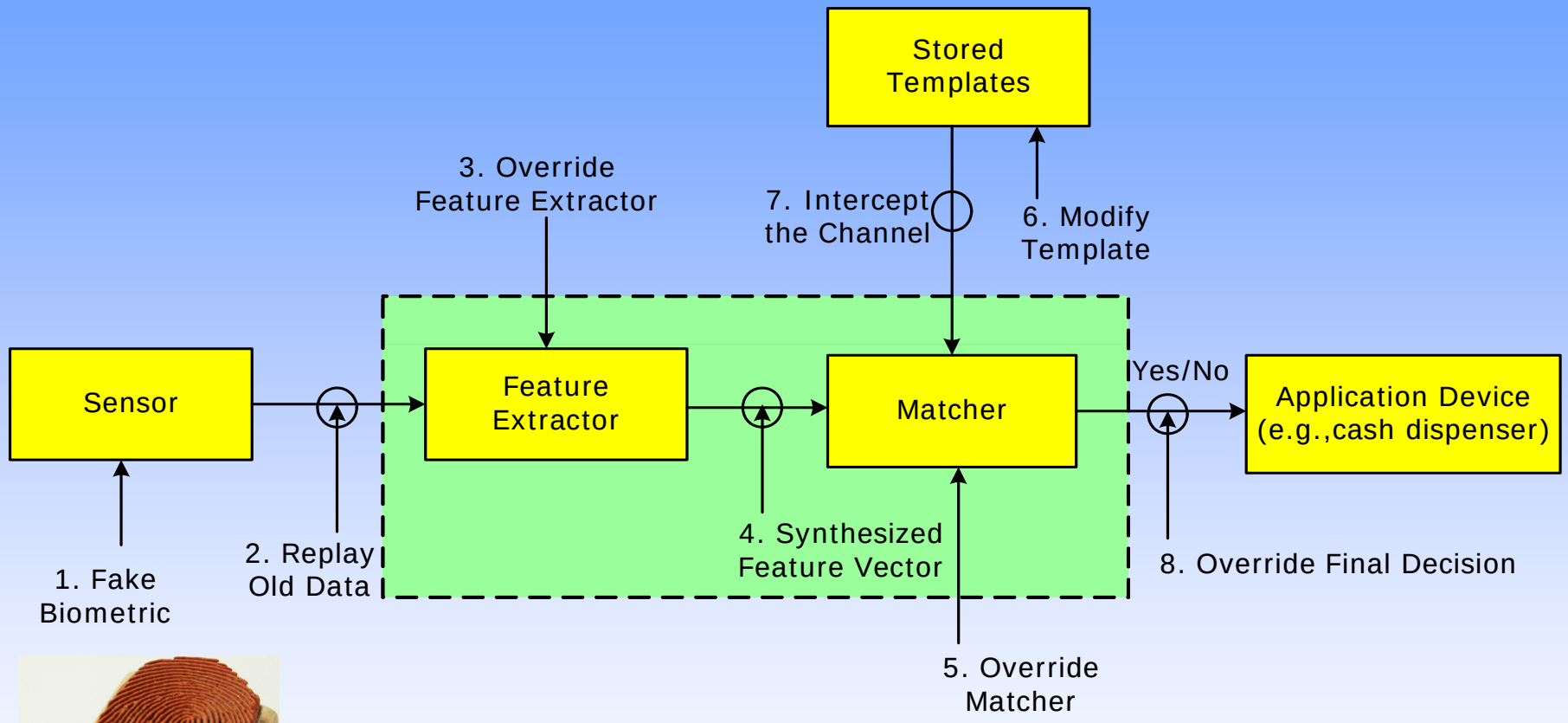
Ethnicity: Asian

Face: LDA Coefficients

Identity: Unsang

Jain et al, "Utilizing soft biometric traits for person authentication", Proc. International Conference on Biometric Authentication (ICBA), Hong Kong, July 2004

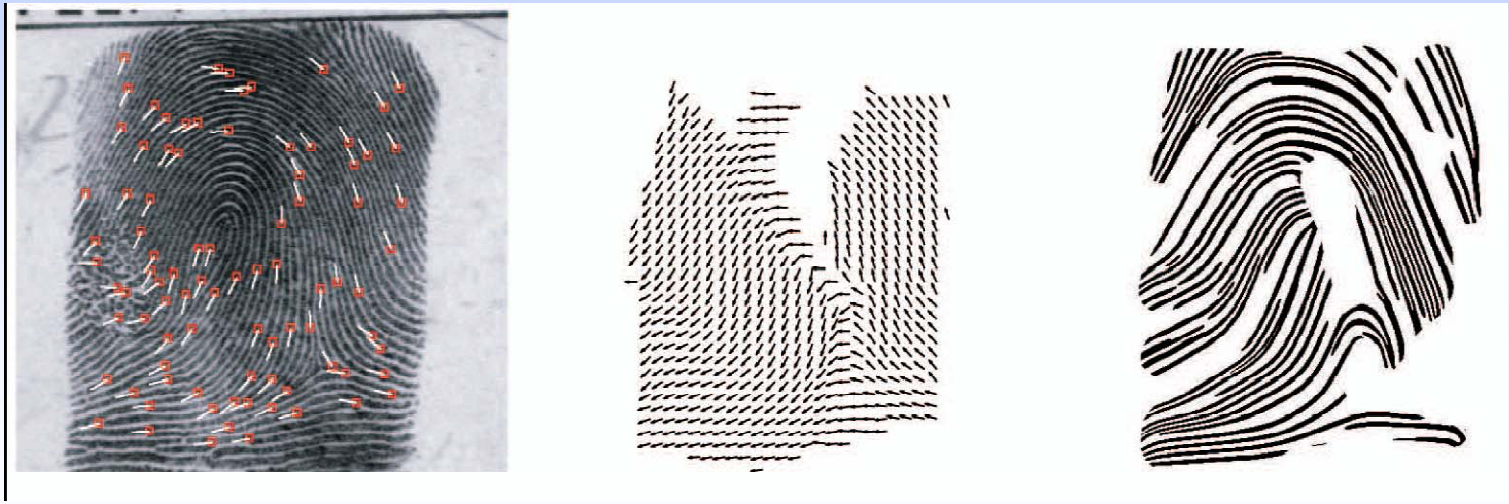
Attacks on a Biometric System



Ratha et al., An Analysis of Minutiae Strength, AVBPA 2001

Template Protection

- A prototype (template) of a user's biometric is stored in a database or a smart card
- Myth: "A true biometric image cannot be created from master template.."
- Biometric template security is critical

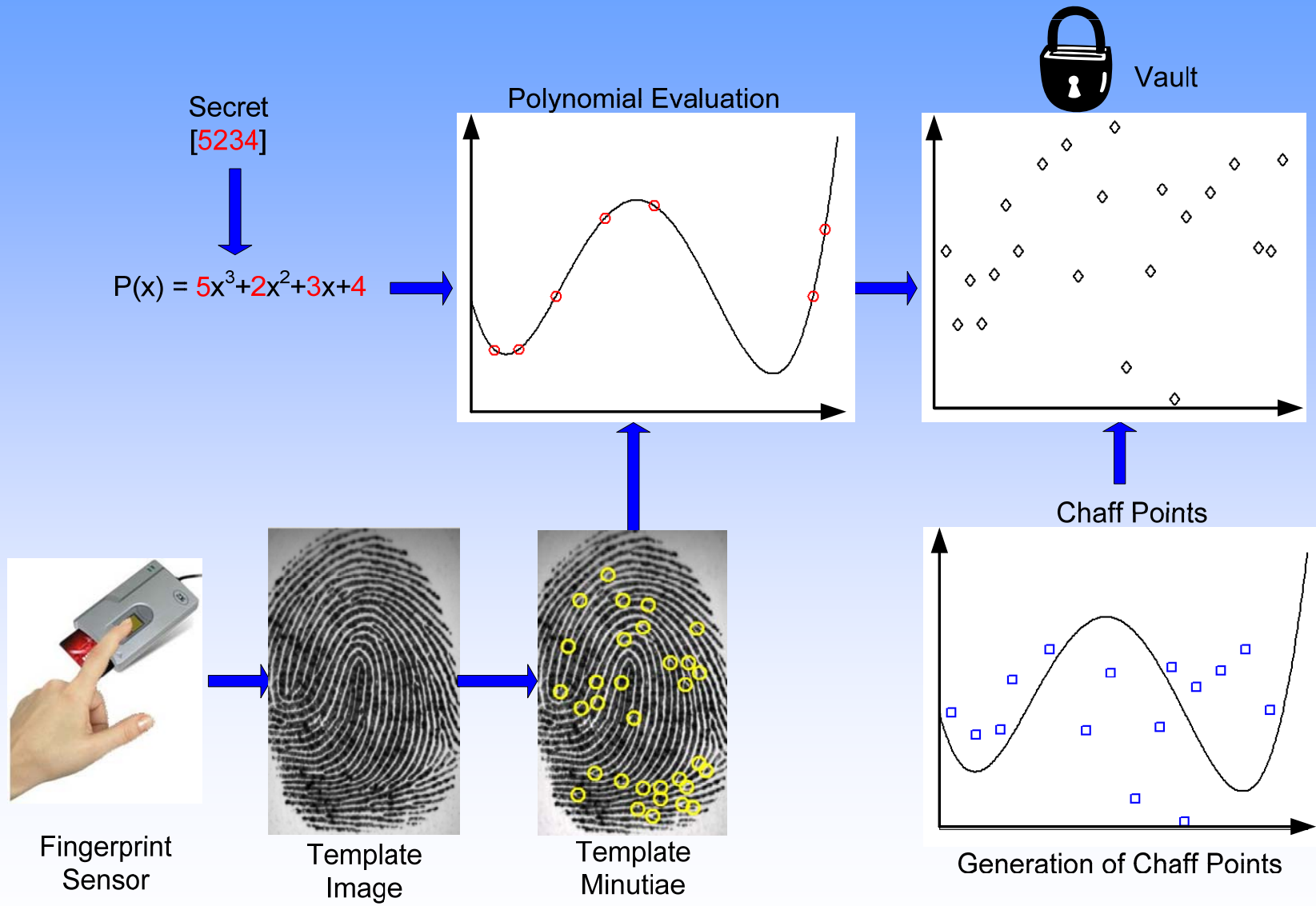


A. Ross, J. Shah and A. K. Jain, "From Template to Image: Reconstructing Fingerprints From Minutiae Points," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, No. 4, pp. 544-560, April 2007.

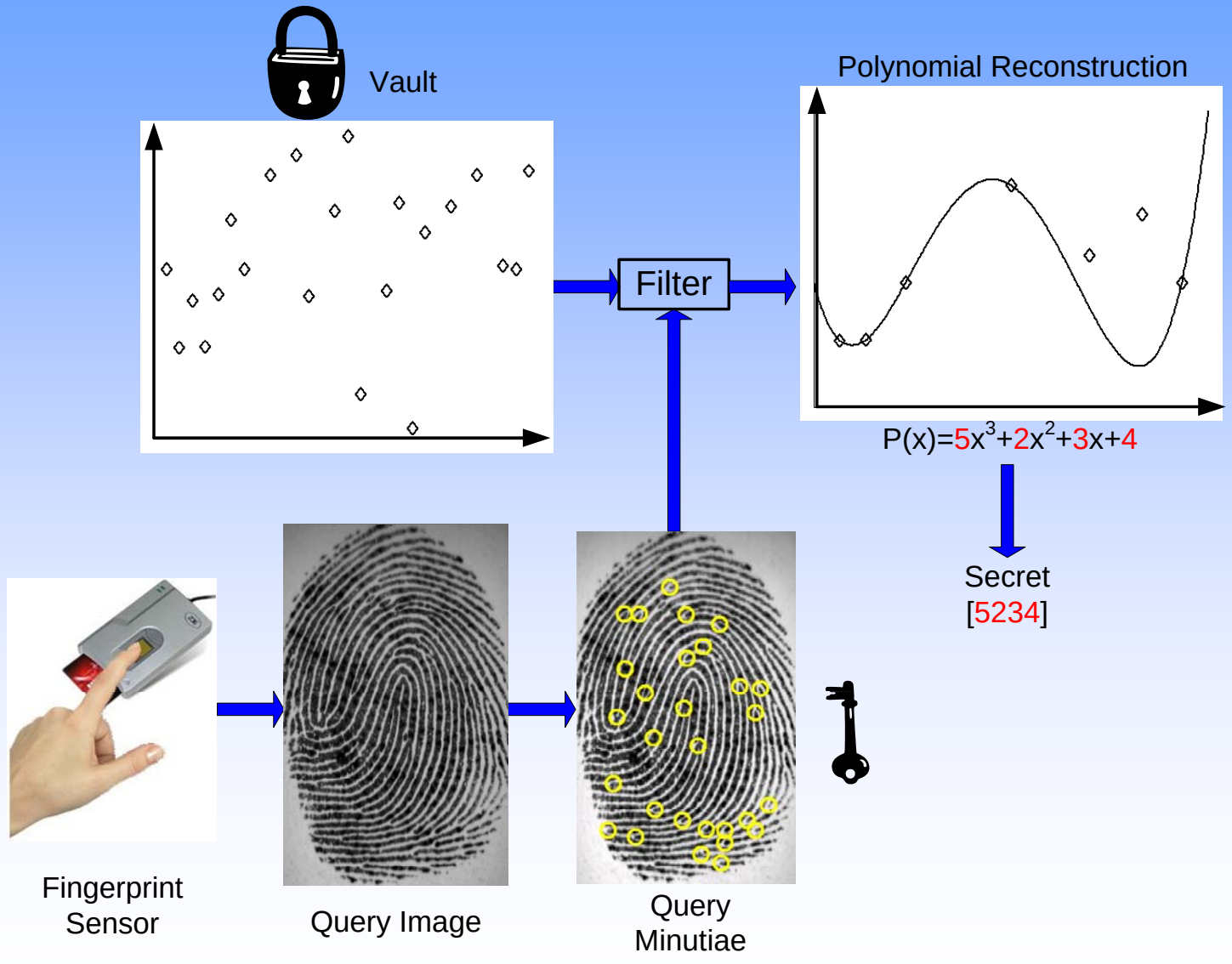
Protecting Biometric Templates

- Encryption
  - Template is encrypted using cryptographic methods
- Steganography
  - Hide the template in a carrier (cover) image
- Cancelable Template
  - Store non-invertible transform of the template
- Fuzzy Vault
  - Template is cryptographically bound to a secret; can be decoded only when matching image is available

Fuzzy Vault



Fuzzy Vault



Sensor Interoperability

Crossmatch Verifier 300

Ethenticator USB 2500

Secugen Hamster III

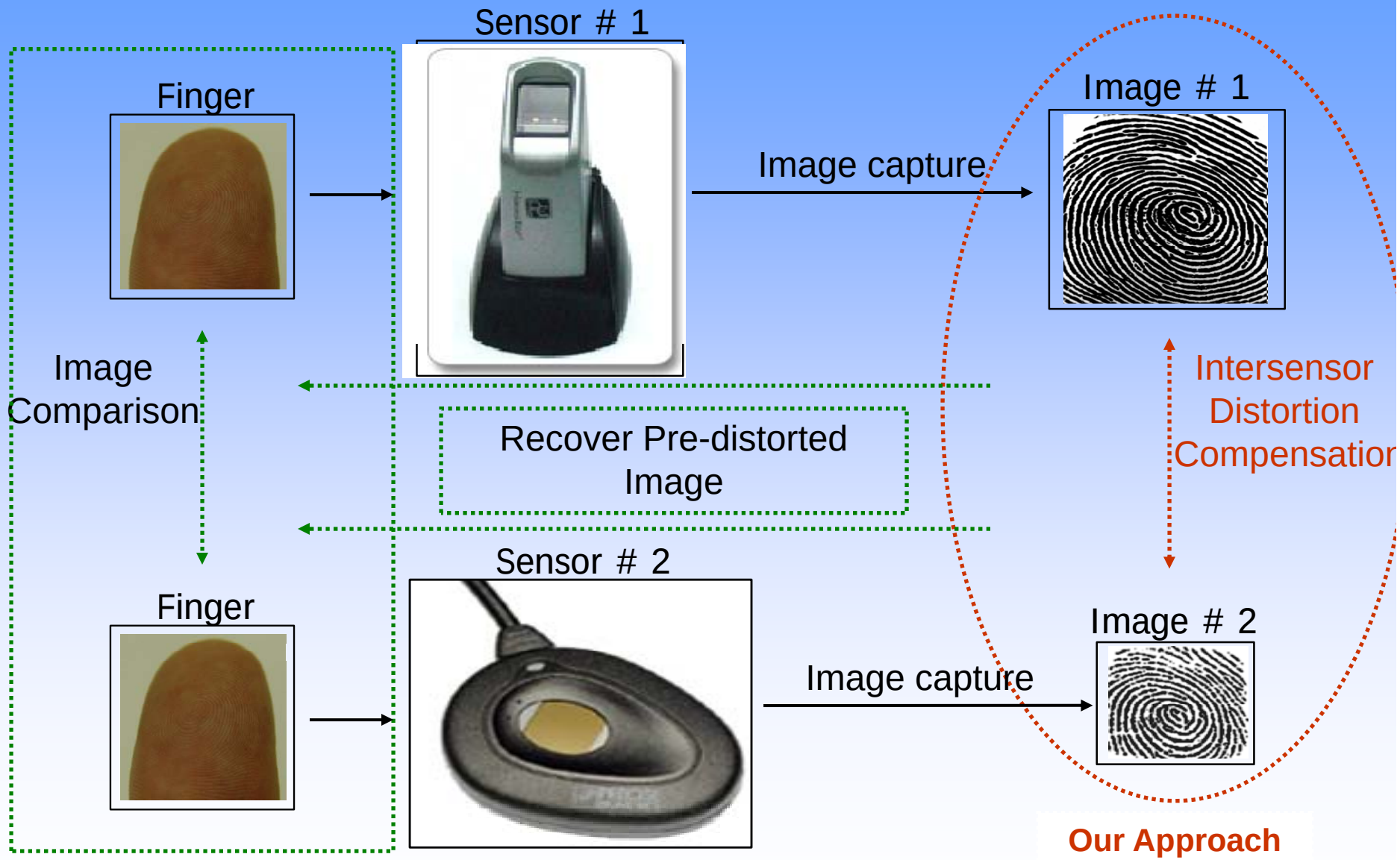
Precise 100AX

Digital Persona U.are.U 4000

Sensor Interoperability

- Can the fingerprint matcher successfully compare two minutiae templates originating from different sensors?

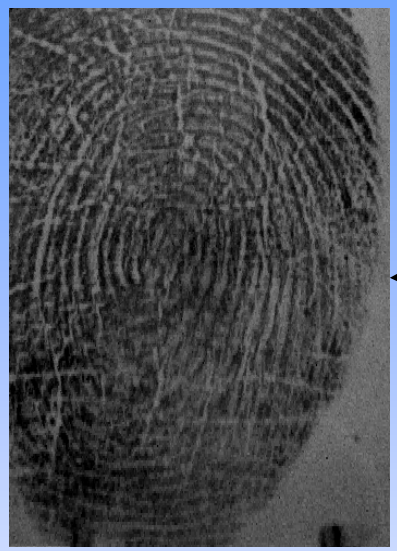
Sensor Interoperability



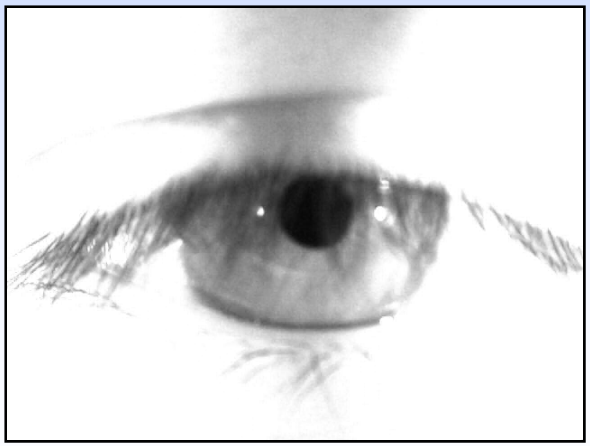
A. Ross and R. Nadgir, "A Calibration Model for Fingerprint Sensor Interoperability", *Proc. of SPIE Conference on Biometric Technology for Human Identification III*, (Orlando, USA), April 2006.

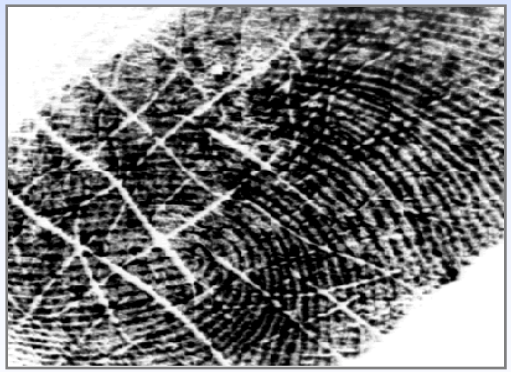
Noise in sensed data

During enrolment



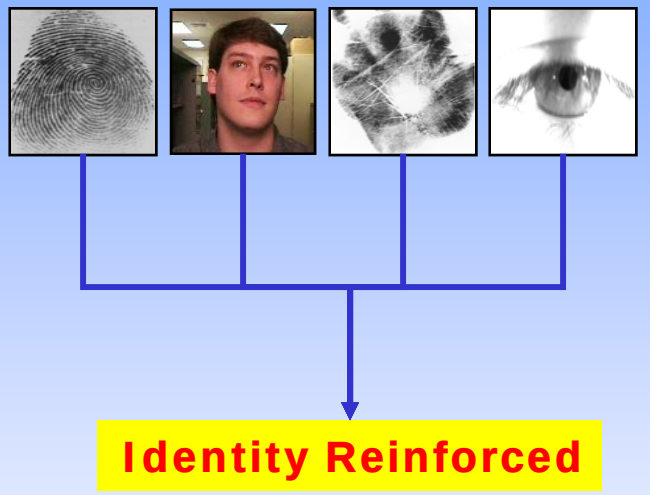
During authentication





Multibiometrics

- Information fusion in the context of biometrics
- The identity of an individual is reinforced through multiple pieces of evidence
- The use of multiple sources of evidence is especially significant in non-ideal scenarios where individual modalities can not be easily acquired



Summary

- Database Organization
  - Fast retrieval of identities
  - “Missing data” or “noisy data” problem
- Template Security
  - Protecting biometric templates
  - Matching in the encrypted domain
- Sensor Interoperability
  - Match data acquired using different sensors