

Multibiometrics



Assoc. Prof. Dr. **DANG TRAN KHANH**

CSE/HCMUT, Vietnam

khanh@hcmut.edu.vn

Data SecuriTy Applied Research Lab

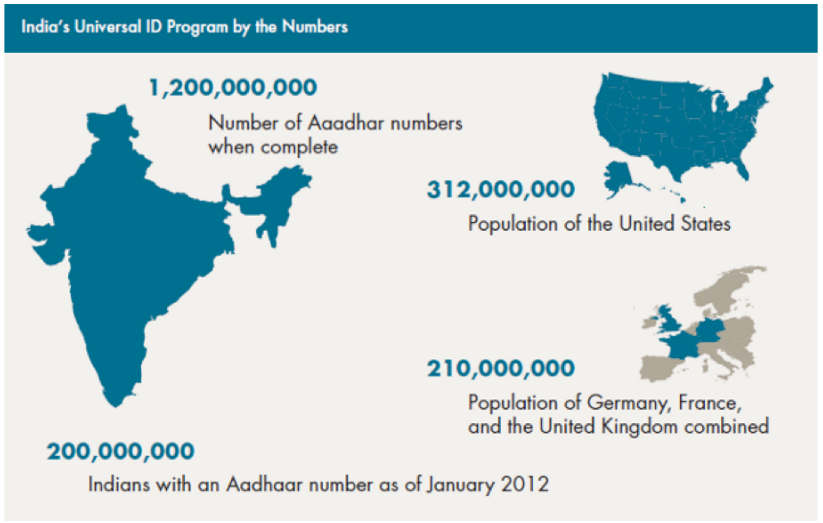
Outline

- Introduction
  - Biometric-based co-authentication systems
- Sources of multiple evidence
- Acquisition and processing architecture
- Fusion levels
- Summary
- Reading:
  - Chapter 6 [2]

Introduction

- Unibiometric systems: rely on a single biometric source for recognition
  - A source of biometric information: any piece of evidence that can be independently used to recognize a person
- Multibiometric systems: enhance the recognition accuracy by reconciling the evidence from multi-sources of information
  - High-security apps and large-scale civilian identification systems

US-VISIT
Keeping America's Doors Open and Our Nation Secure



Introduction

- Examples of biometric traits, uni/multibiometrics

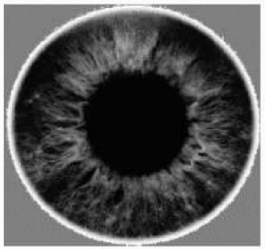

Fingerprint


Facial thermogram


Hand geometry


Face


Ear

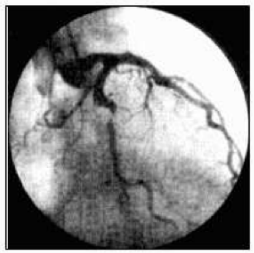

Iris


Palmprint


Voice


Gait


Signature


Retina



Unibiometric system




The *Fusion* multibiometric system (by Cogent Systems), capable of capturing fingerprint, face, and iris images

https://en.wikipedia.org/wiki/Cogent_Systems

Biometric-based Co-authentication System

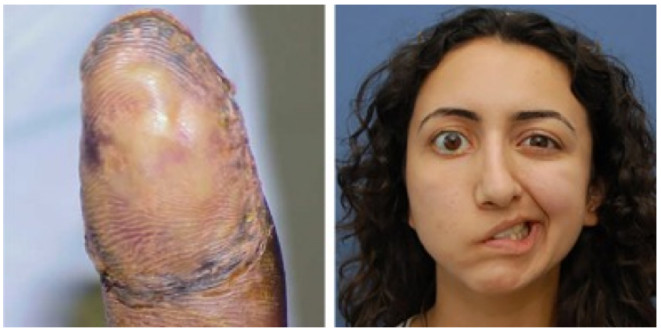
- Humans recognize one another based on the evidence presented by multiple biometric characteristics in addition to several contextual details associated with the environment
- Biometric-based co-authentication systems
  - Multibiometric sources (→ *next slides*)
    - Unimodal
    - Multimodal
  - Biometrics & other types of evidence
    - Classic evidence
    - Soft biometrics
    - Contextual details

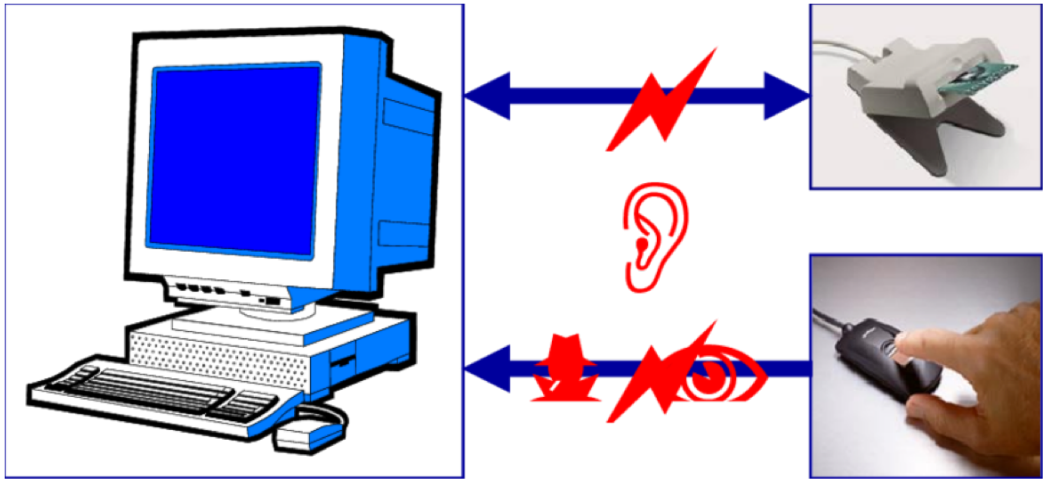
Advantages of multibiometric systems

- Improve the matching accuracy of a biometric system
- Increase the feature space available to individuals
- Address the issue of non-universality or insufficient population coverage
- Be difficult for an impostor to spoof multiple biometric traits of a legitimately enrolled individual
  - With a random subset of traits: a multibiometric system can facilitate a challenge-response mechanism that verifies the presence of a *live* user (e.g. 3 of 10 fingerprints)
- Address the problem of noisy data
- Be viewed as a fault tolerant system

and disadvantages

- Costs & benefits: the added cost and the improvement in matching performance
- Users' acceptance
- Reduced matching level: John Daugman claimed that if a stronger biometric is used with a weaker one, FAR or FRR of the weaker biometric can bring down the overall effectiveness of the system





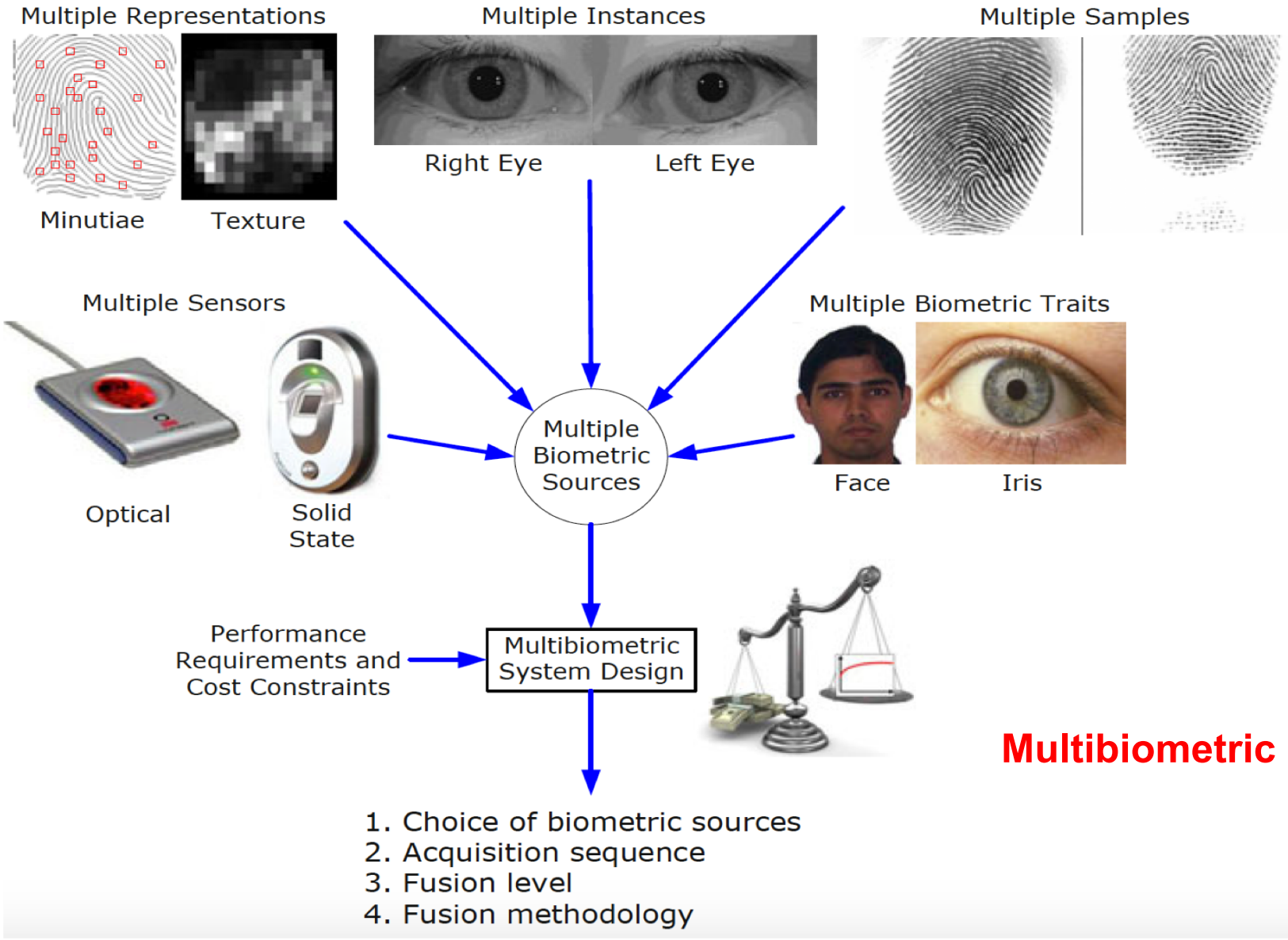
System design issues

- In designing a multibiometric system, 4 design issues must be solved:
  - Information sources: What are the various sources of biometric information that should be used in a multibiometric system?
  - Mode of operation: parallel or sequencial mode?
  - Level of fusion: will raw data, features, match scores, or decisions be fused?
  - Fusion approach: fusion scheme to combine multiple biometric sources?

Outline

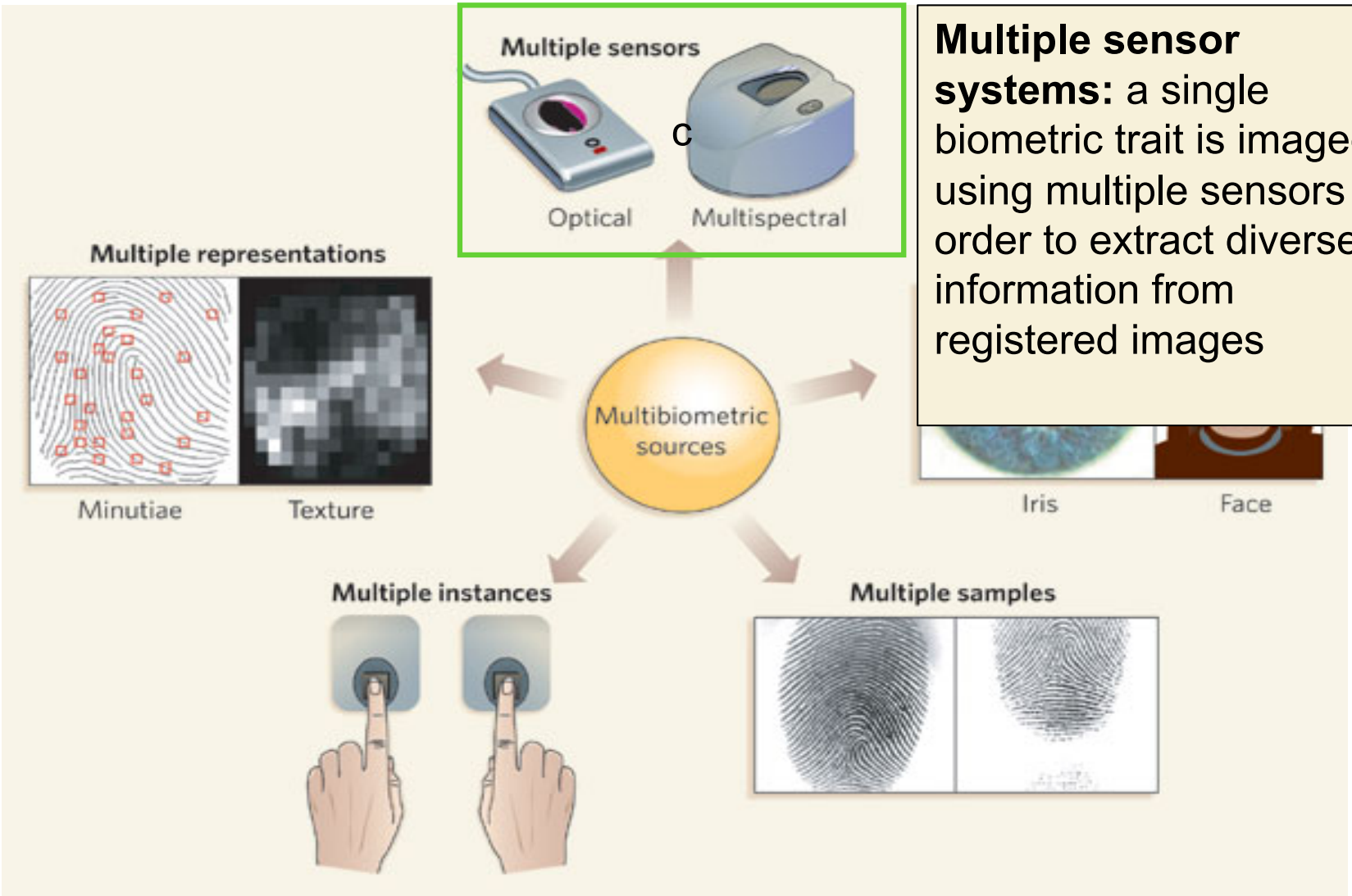
- ~~Introduction~~
  - ~~Biometric-based co-authentication systems~~
- Sources of multiple evidence
- Acquisition and processing architecture
- Fusion levels
- Summary
- Reading:
  - Chapter 6 [2]

Sources of multiple evidence



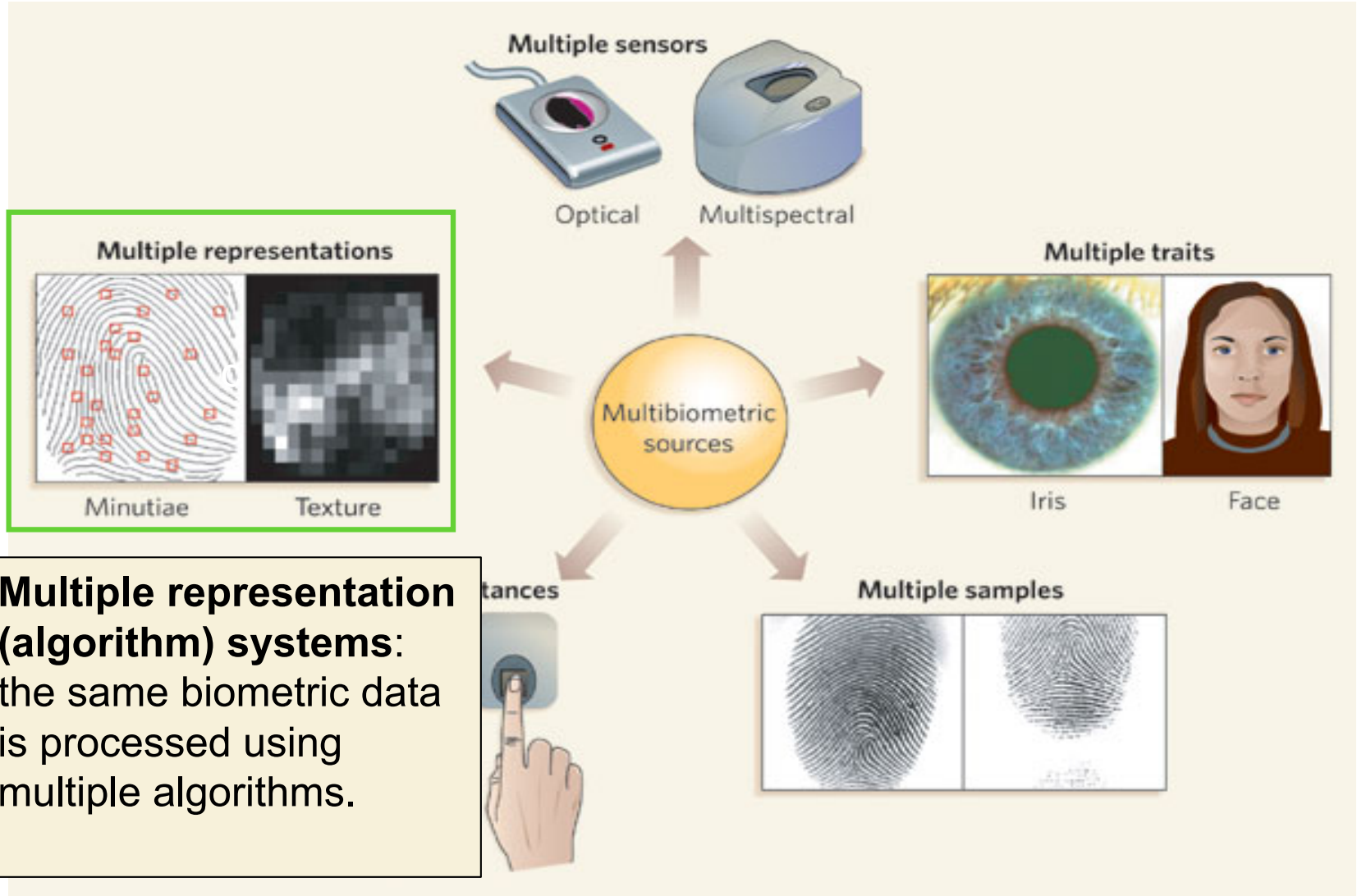
Multibiometric systems

Sources of multiple evidence



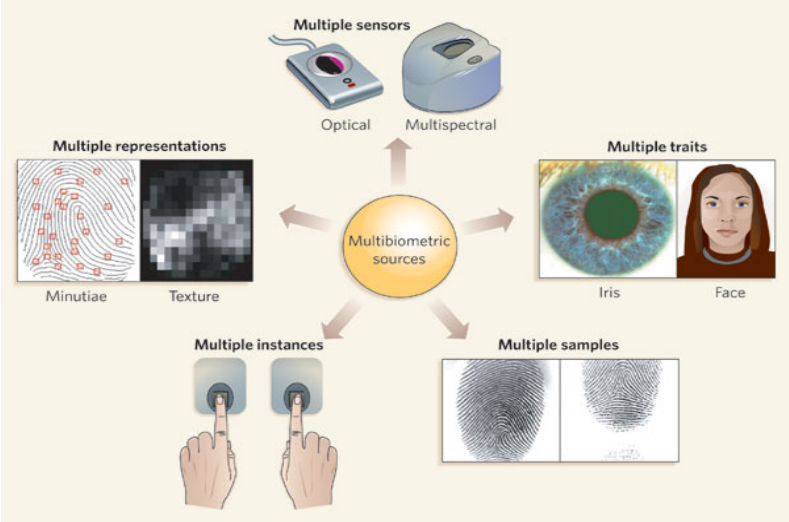
Multiple sensor systems: a single biometric trait is imaged using multiple sensors in order to extract diverse information from registered images

Sources of multiple evidence

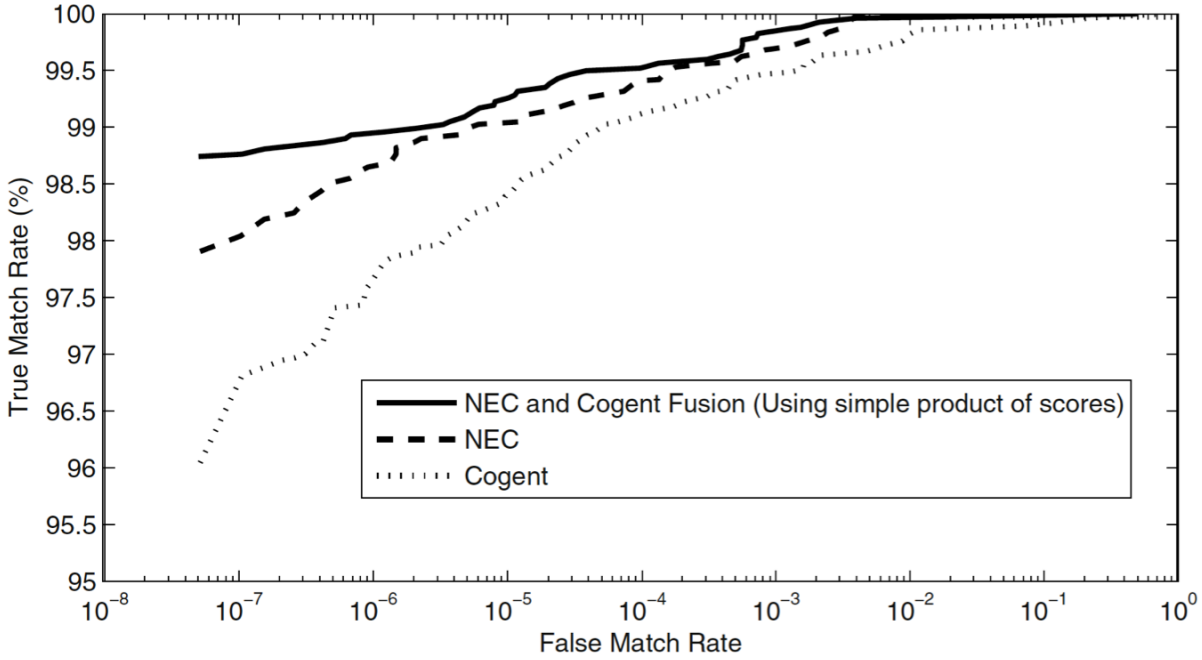


Multiple representation (algorithm) systems: the same biometric data is processed using multiple algorithms.

Sources of multiple evidence

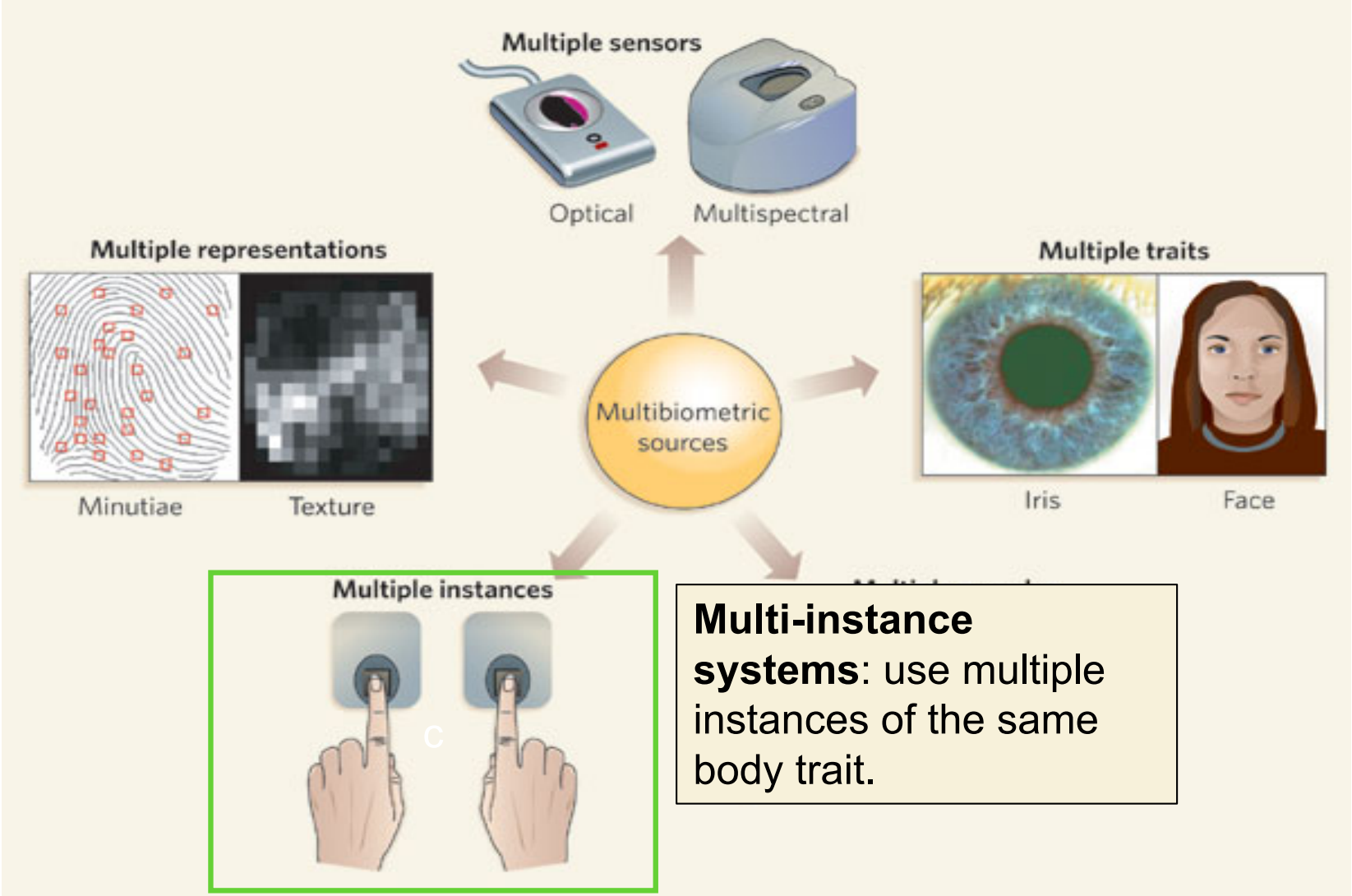


Multiple representation (algorithm) systems: the same biometric data is processed using multiple algorithms



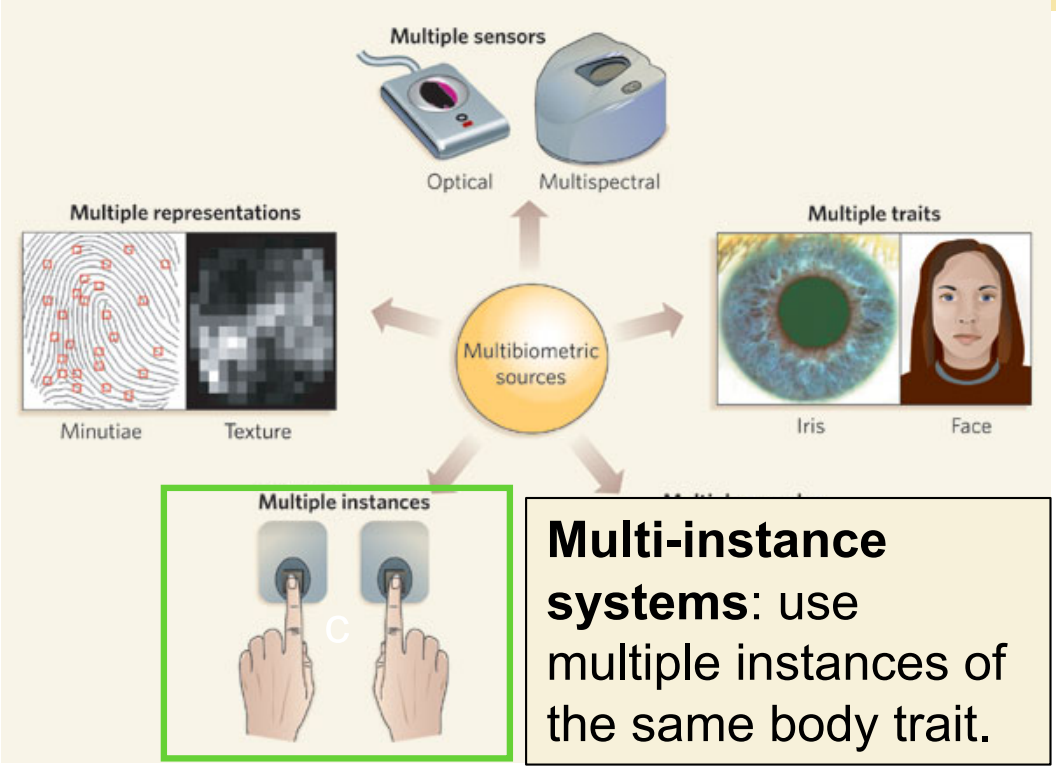
Accuracy improvement in a multi-algorithm fingerprint verification system

Sources of multiple evidence



Multi-instance systems: use multiple instances of the same body trait.

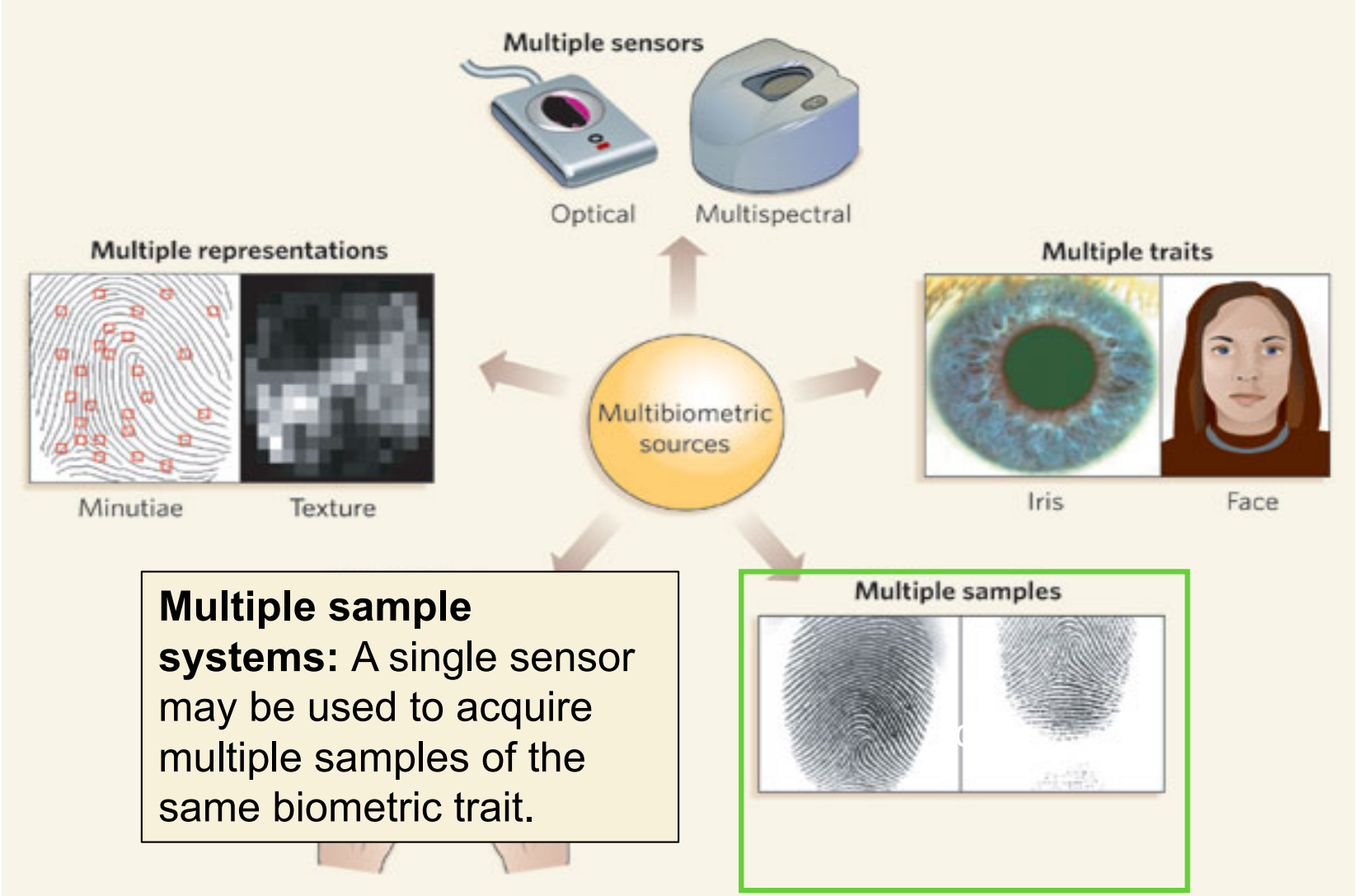
Sources of multiple evidence



Multi-instance systems: use multiple instances of the same body trait.

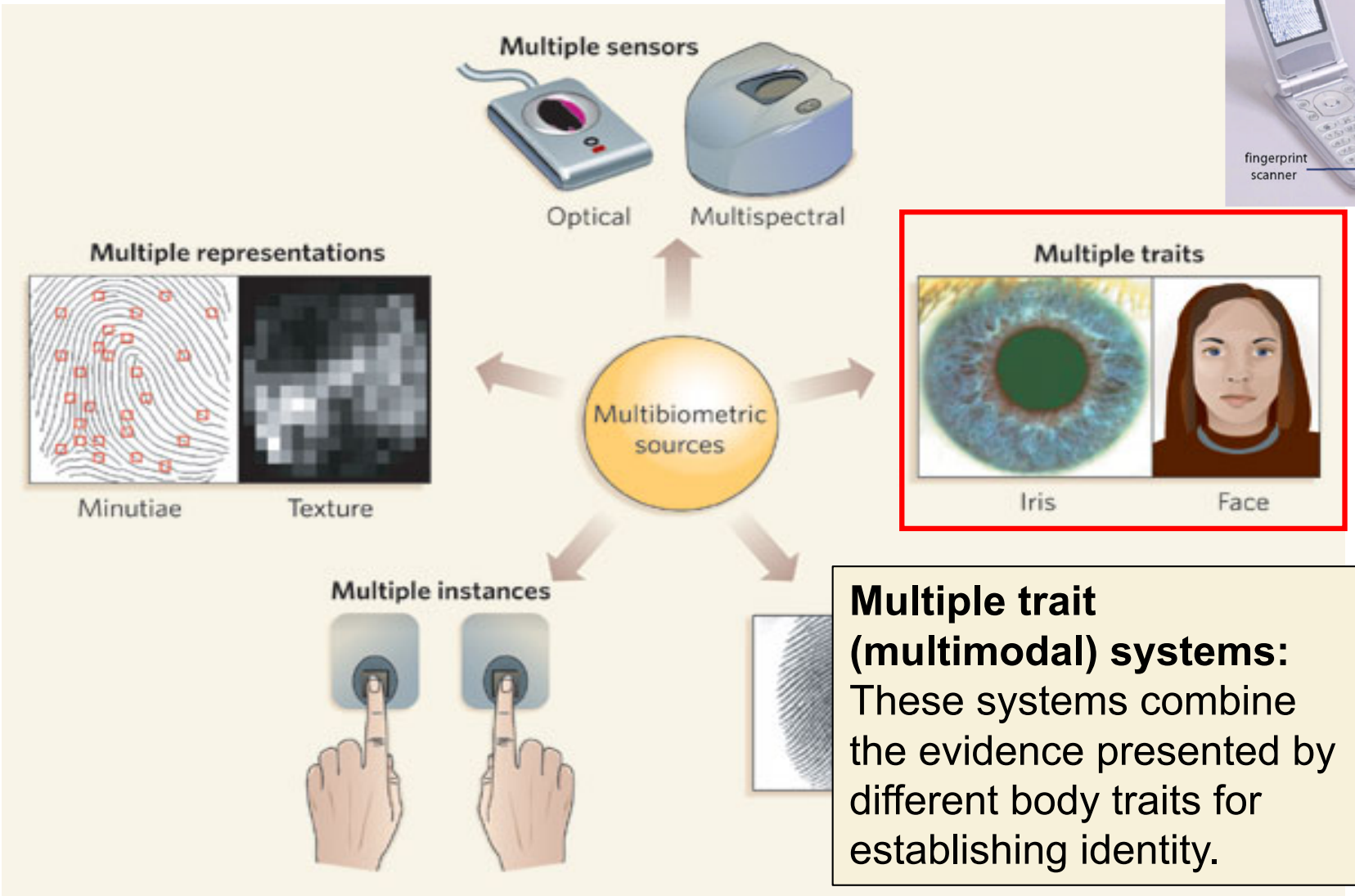
A fingerprint sensor developed by Identix that allows rapid acquisition of all ten fingers in three steps

Sources of multiple evidence



Multiple sample systems: A single sensor may be used to acquire multiple samples of the same biometric trait.

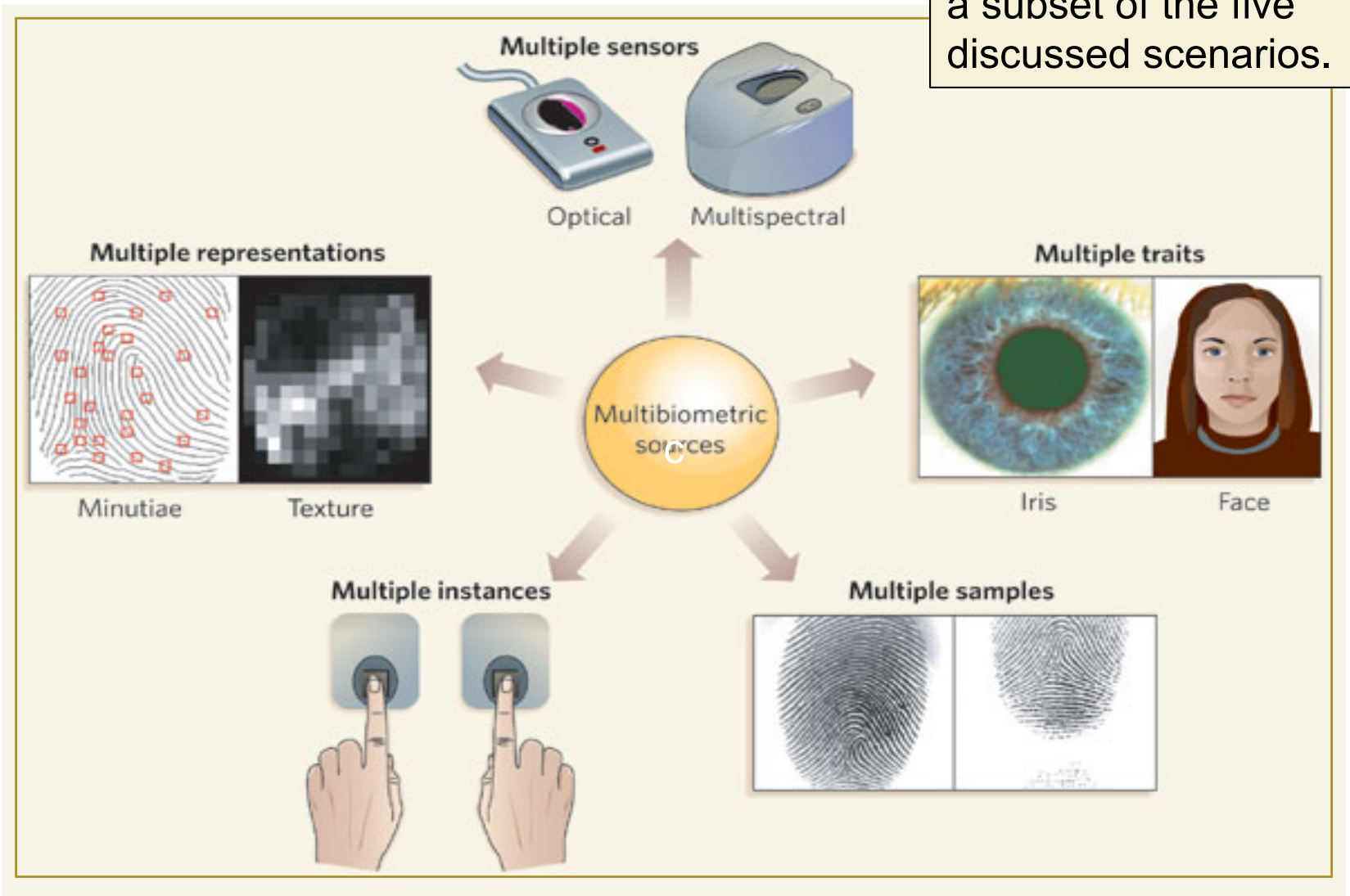
Sources of multiple evidence



Multiple trait (multimodal) systems: These systems combine the evidence presented by different body traits for establishing identity.

Sources of multiple evidence

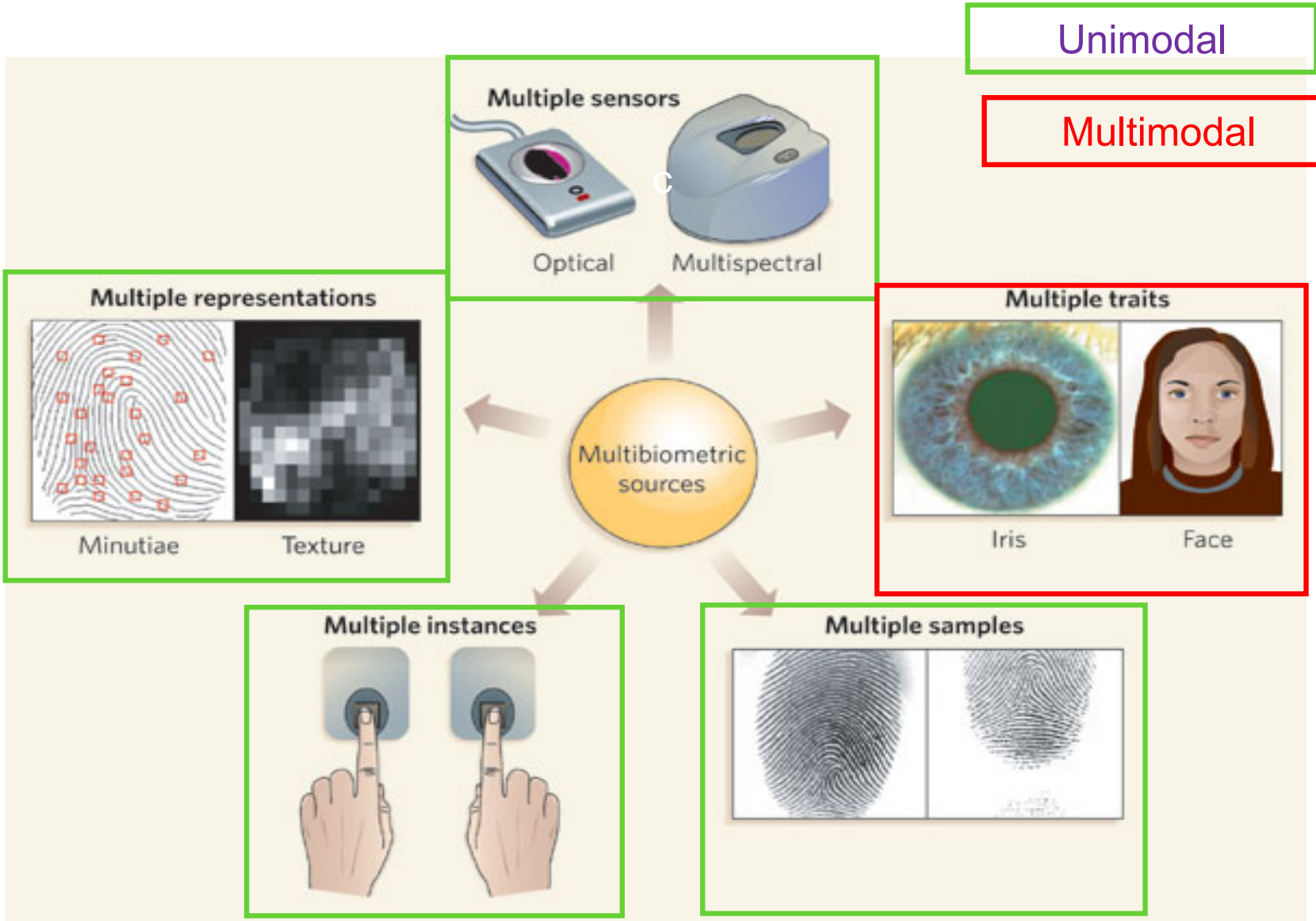
Hybrid systems: integrate a subset of the five discussed scenarios.



Sources of multiple evidence

Unimodal

Multimodal

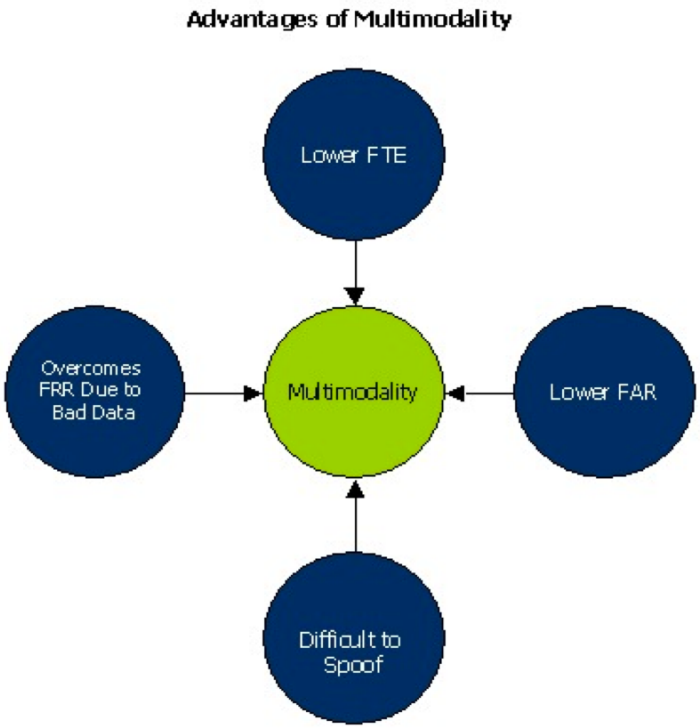


Outline

- ~~Introduction~~
  - ~~Biometric-based co-authentication systems~~
- ~~Sources of multiple evidence~~
- Acquisition and processing architecture
- Fusion levels
- Summary
- Reading:
  - Chapter 6 [2]

Acquisition and processing architecture

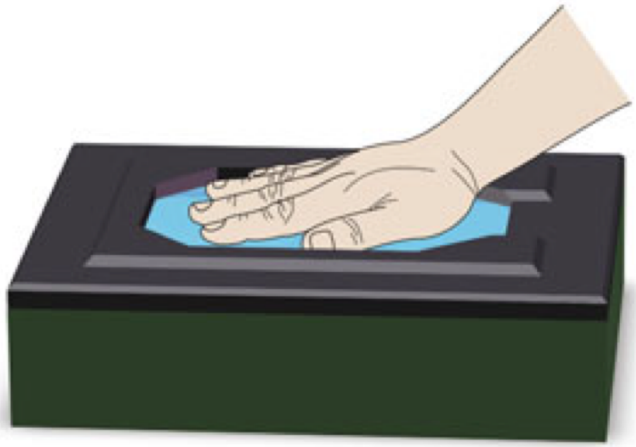
- One of the key considerations while designing a biometric system is its usability
- Important to design convenient user interfaces, efficiently capture good quality biometric images, leading to a lower failure to enroll rate (FTE)



- Sequence of biometric data acquisition has a bearing on the convenience imparted to the user
- Sequence in which the procured biometric data is processed can significantly impact the throughput time in large-scale identification systems

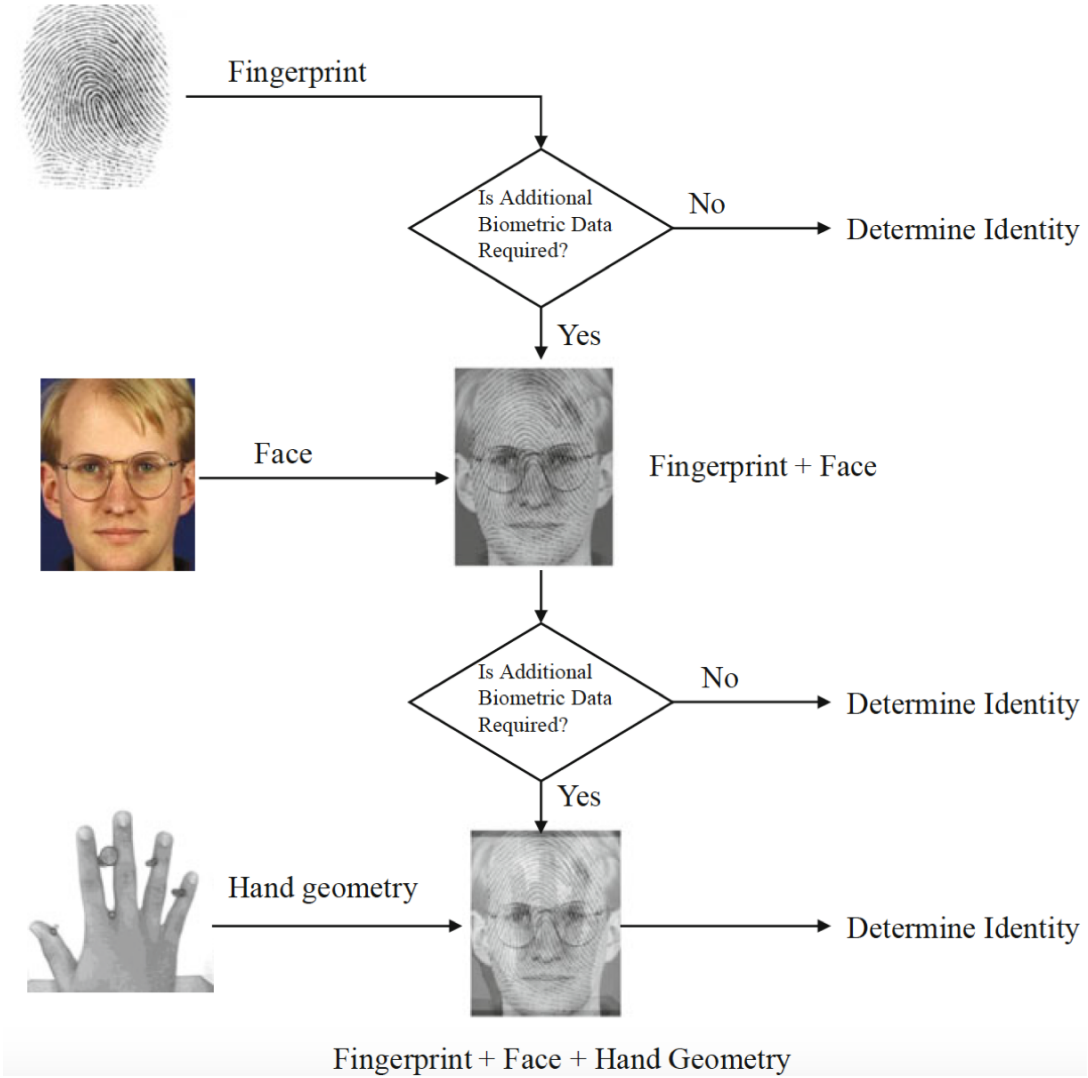
Acquisition sequence

- Serial or parallel
- In the case of multialgorithm systems, the sequence of acquisition methodology is not an issue



Processing sequence

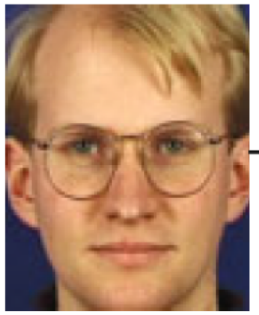
- Information may be acquired sequentially but processed simultaneously and vice versa



- Cascade (or serial) mode of operation, evidence is incrementally processed in order to establish the user's identity
- Also known as sequential pattern recognition
- It enhances user convenience while reducing the average processing time since a decision can be made without having to acquire all the biometric traits

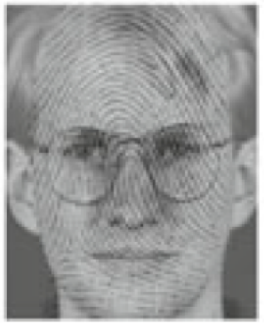
Processing sequence

Fingerprint



Face

Hand geometry



Matching Module

Determine Identity

- In the parallel mode, the evidence acquired from multiple sources is simultaneously processed in order to establish user's identity
- Note that the evidence pertaining to the multiple sources may be acquired in a sequential fashion

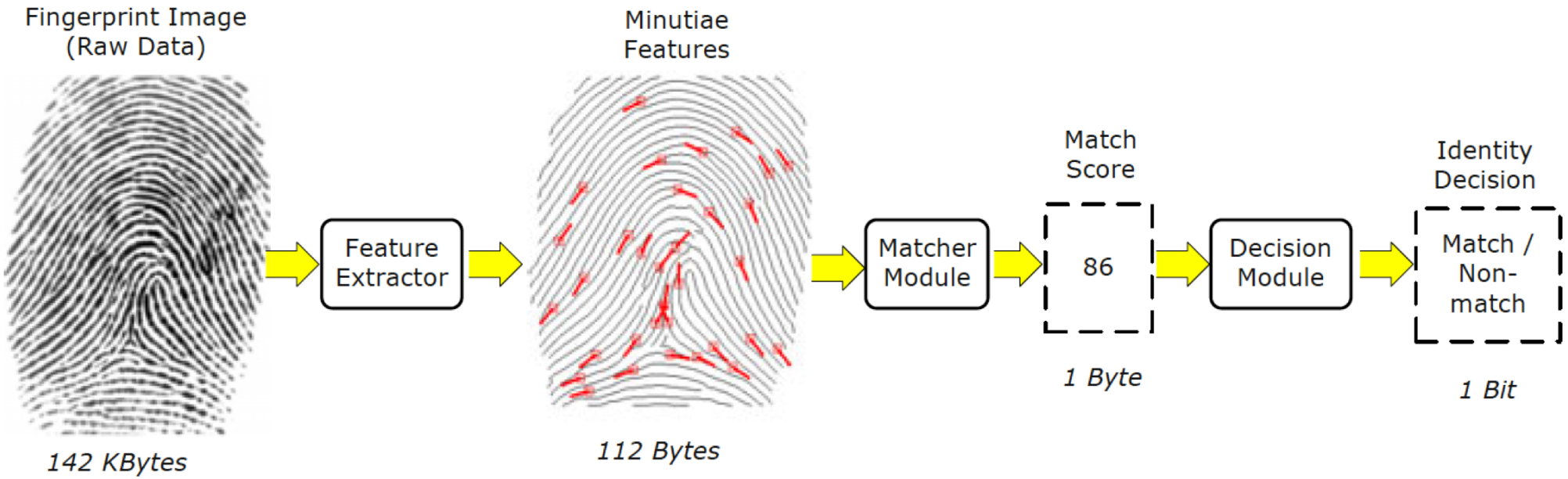
Processing sequence

- Hierarchical (tree-like) architecture to combine the advantages of both cascade and parallel architectures
- In such a scheme, a subset of the acquired modalities may be combined in parallel, while the remaining modalities may be combined in a serial fashion
- Such an architecture can be dynamically determined based on the quality of the individual biometric samples as well as when encountering missing biometric data

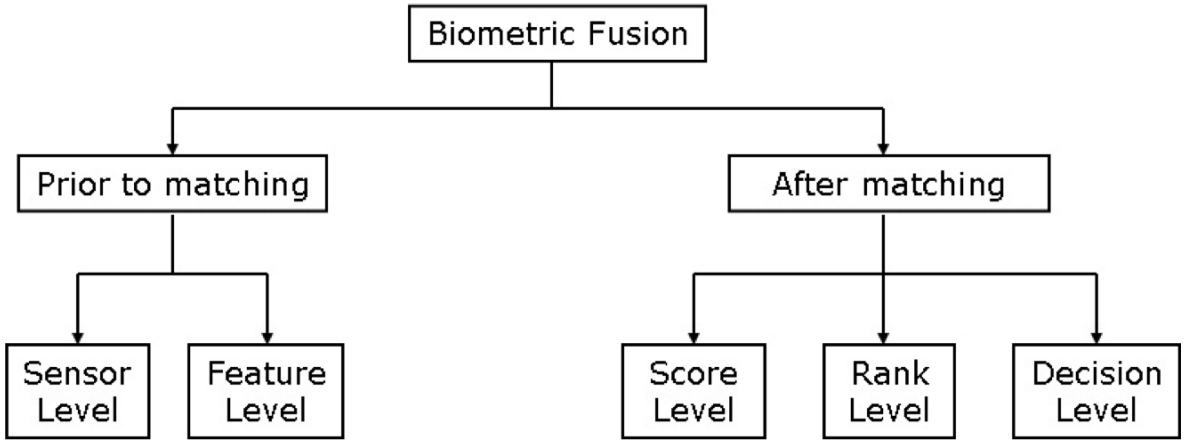
Outline

- ~~Introduction~~
  - ~~Biometric-based co-authentication systems~~
- ~~Sources of multiple evidence~~
- ~~Acquisition and processing architecture~~
- Fusion levels
- Summary
- Reading:
  - Chapter 6 [2]

Fusion levels

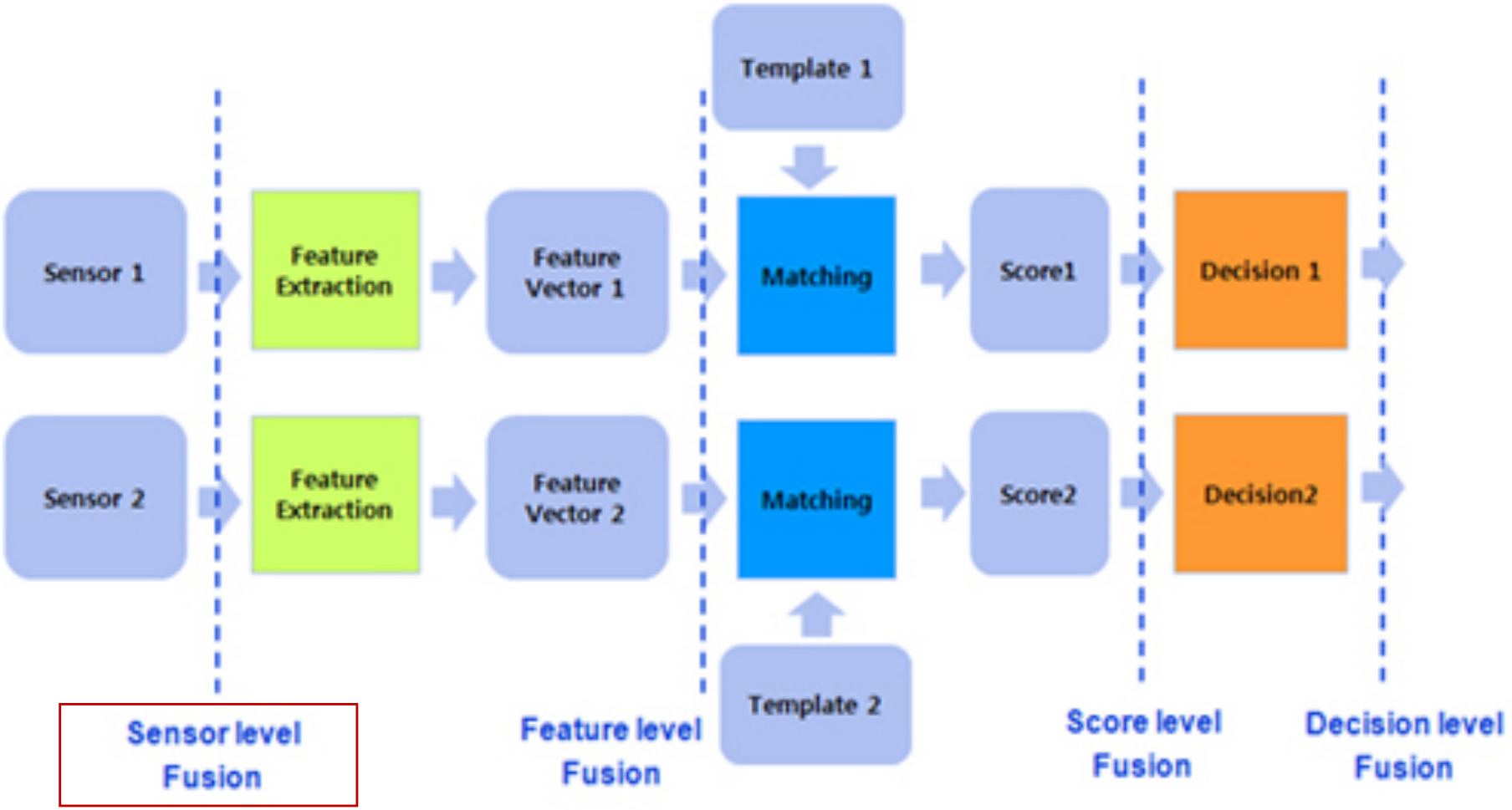


The amount of information available for fusion gets reduced as one progresses along the various processing modules of a biometric system



Fusion at the rank level is applicable only to biometric systems operating in the identification mode

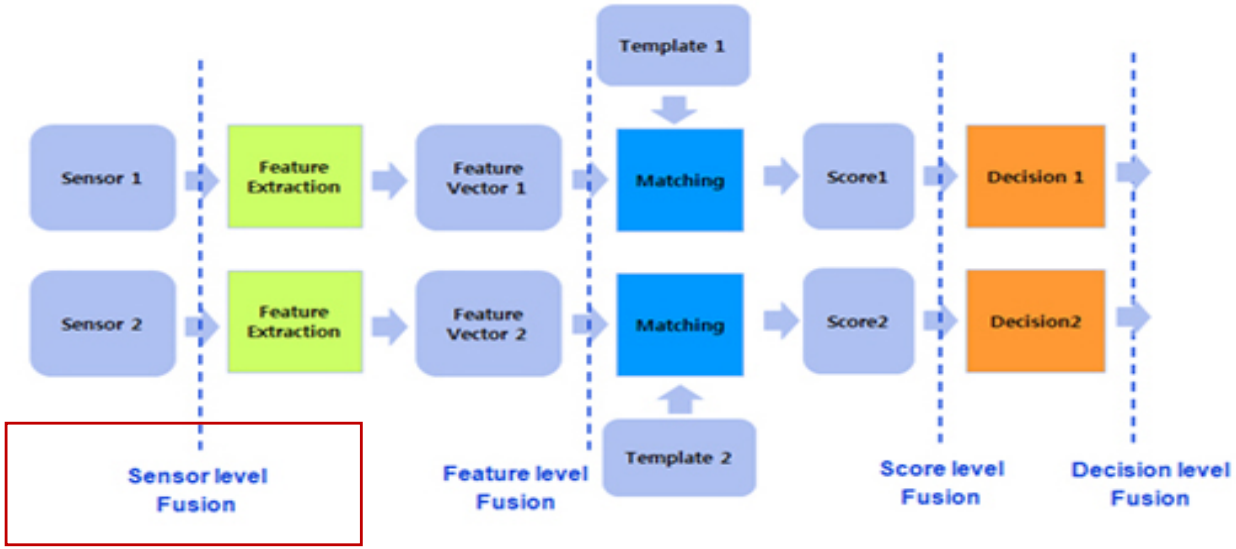
Fusion levels

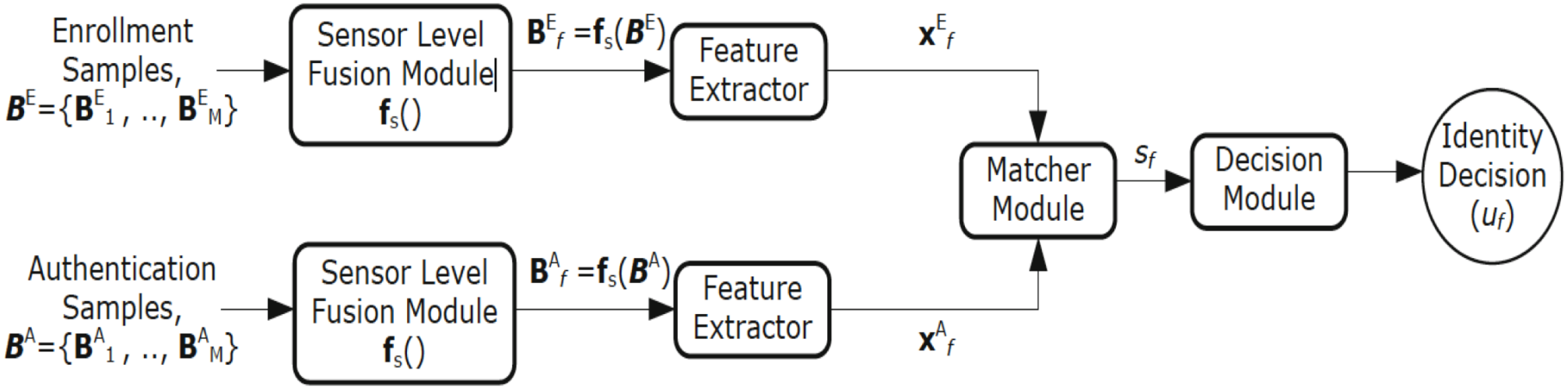


Sensor level Fusion: The raw data from the sensor(s) are combined.

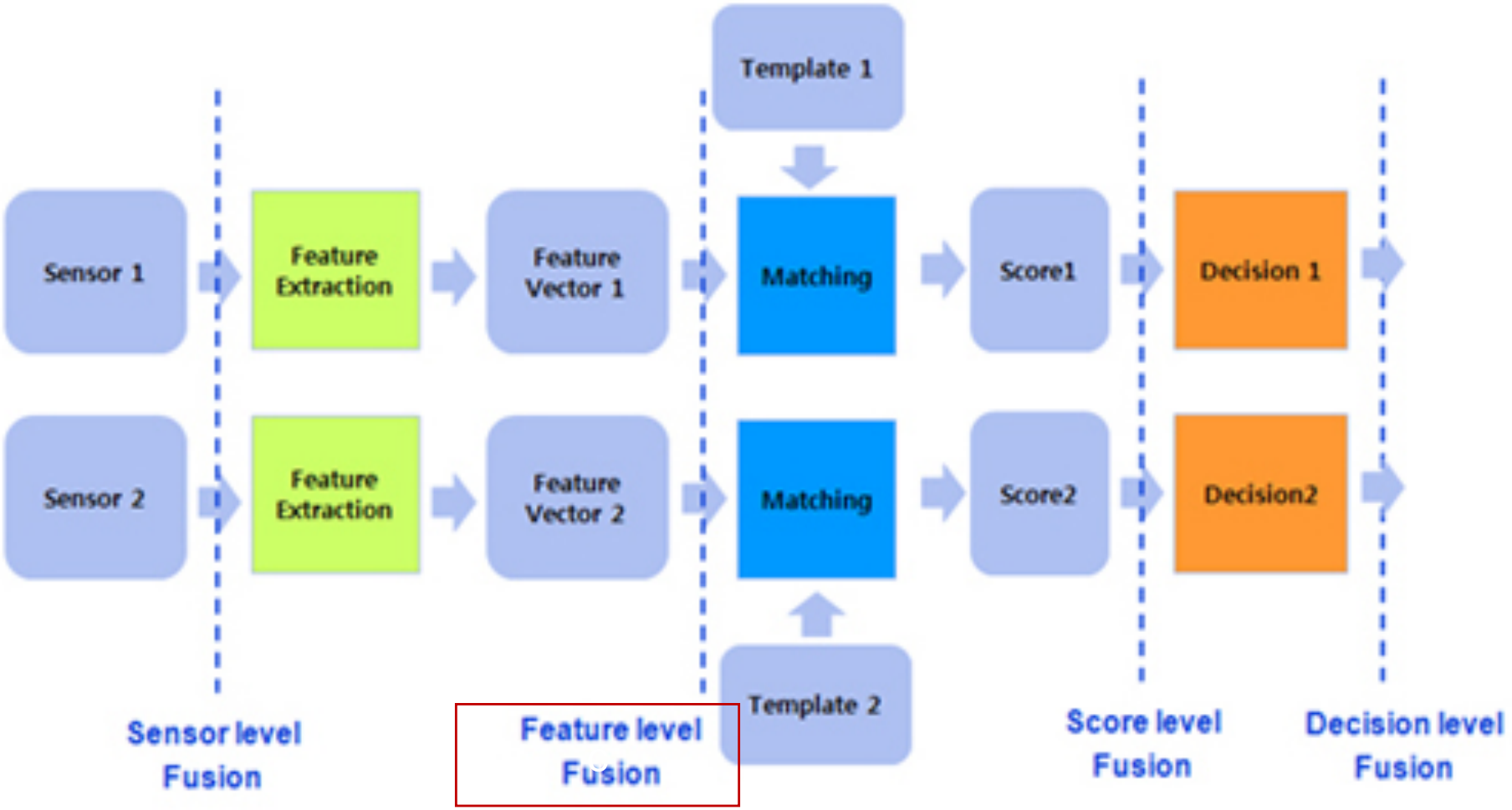
Fusion levels

Sensor level Fusion: The raw data from the sensor(s) are combined.





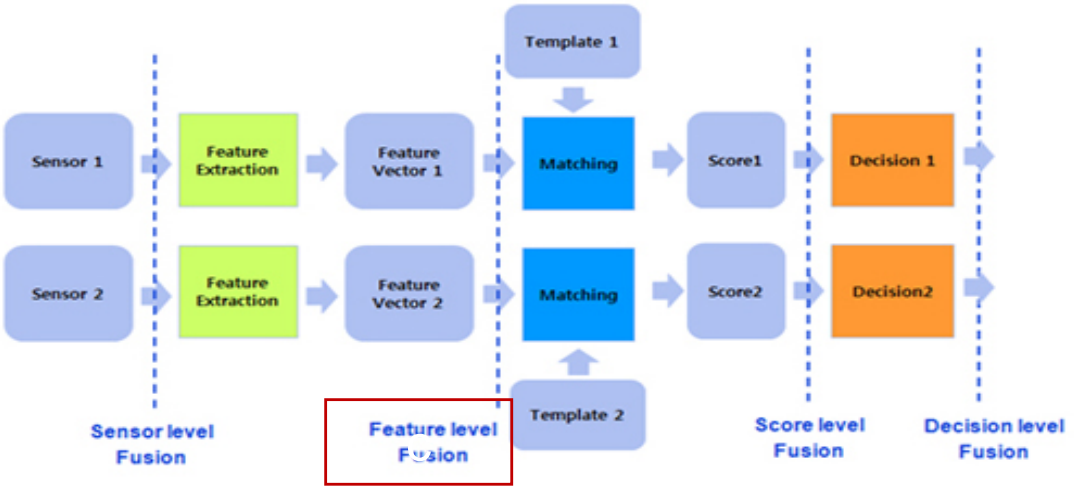
Fusion levels

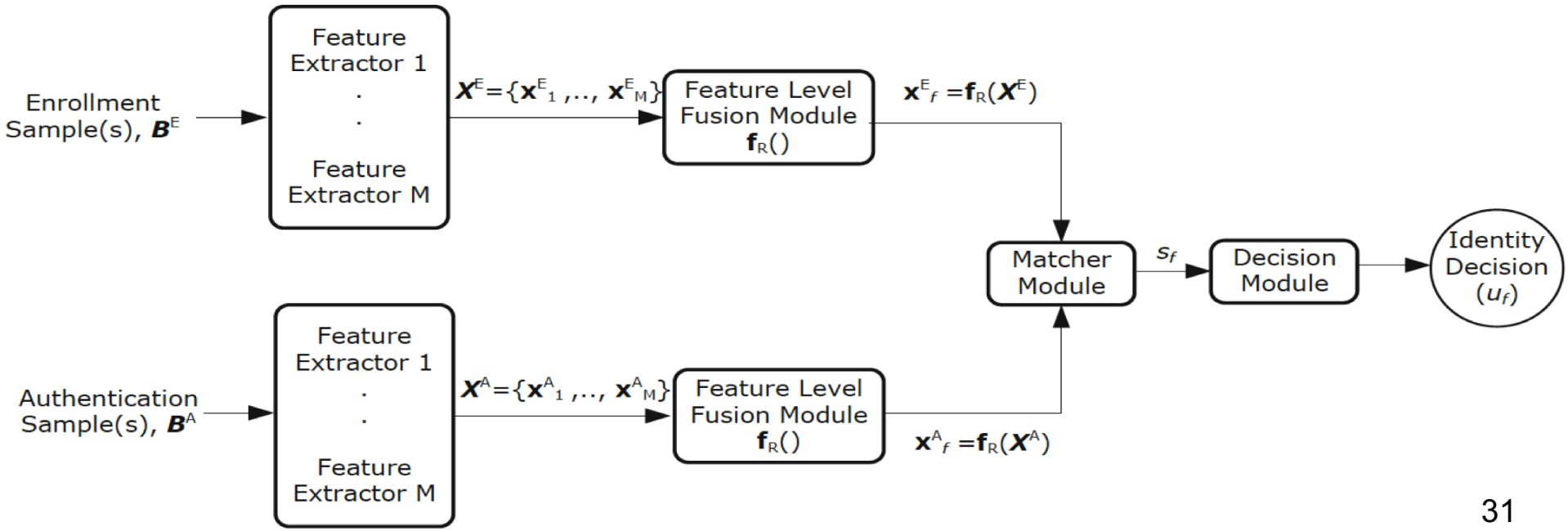


Feature level Fusion: combining different feature sets extracted from multiple biometric sources.

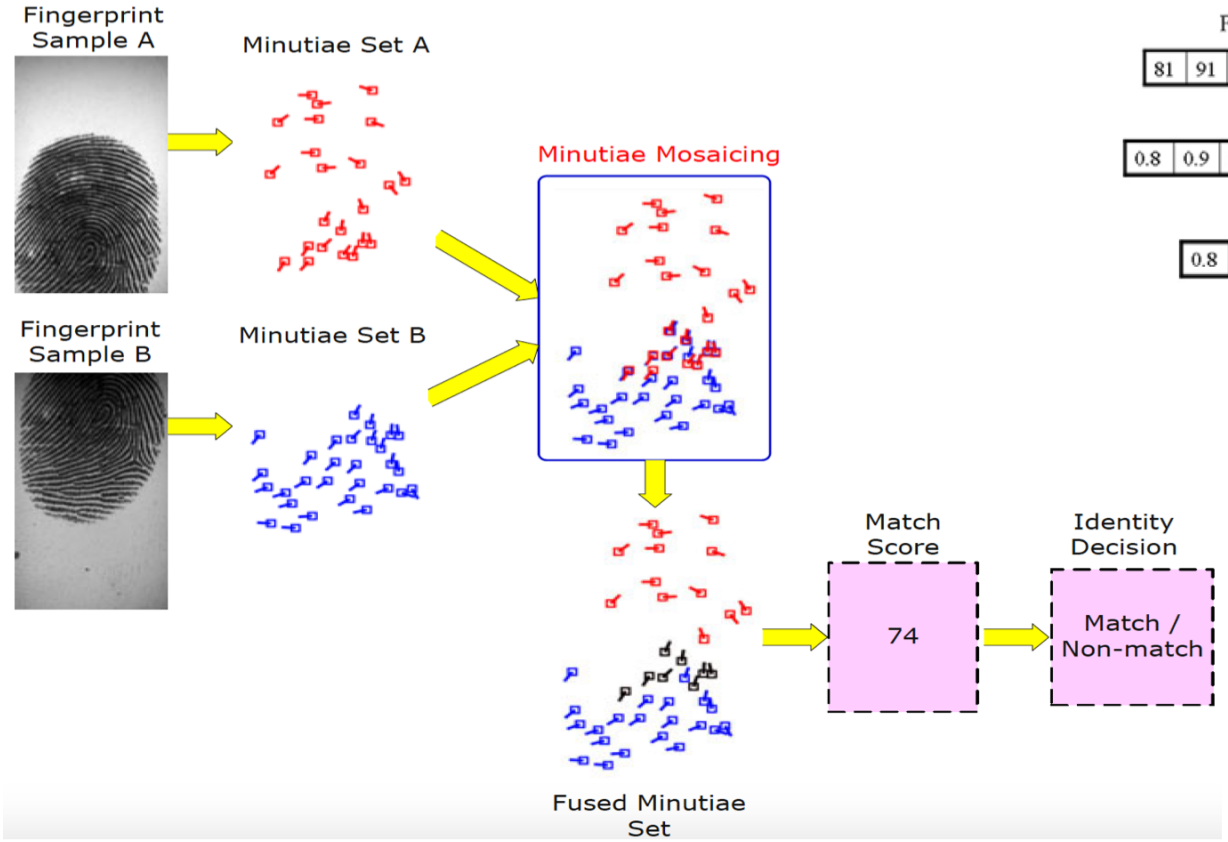
Fusion levels

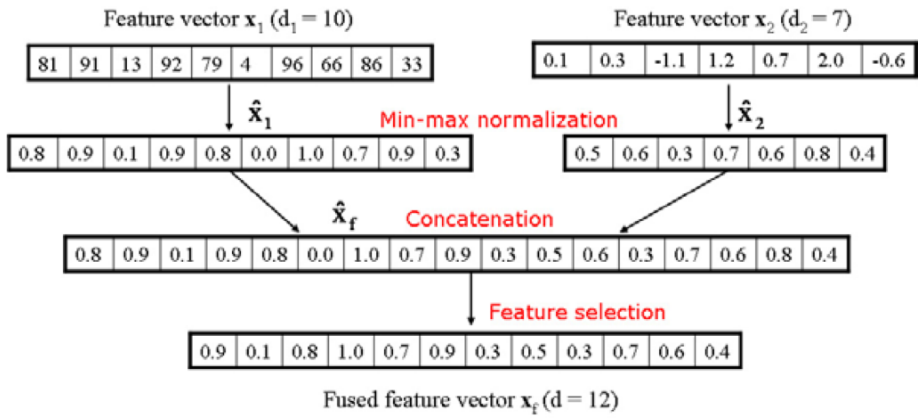
Feature level Fusion: combining different feature sets extracted from multiple biometric sources.





Fusion levels

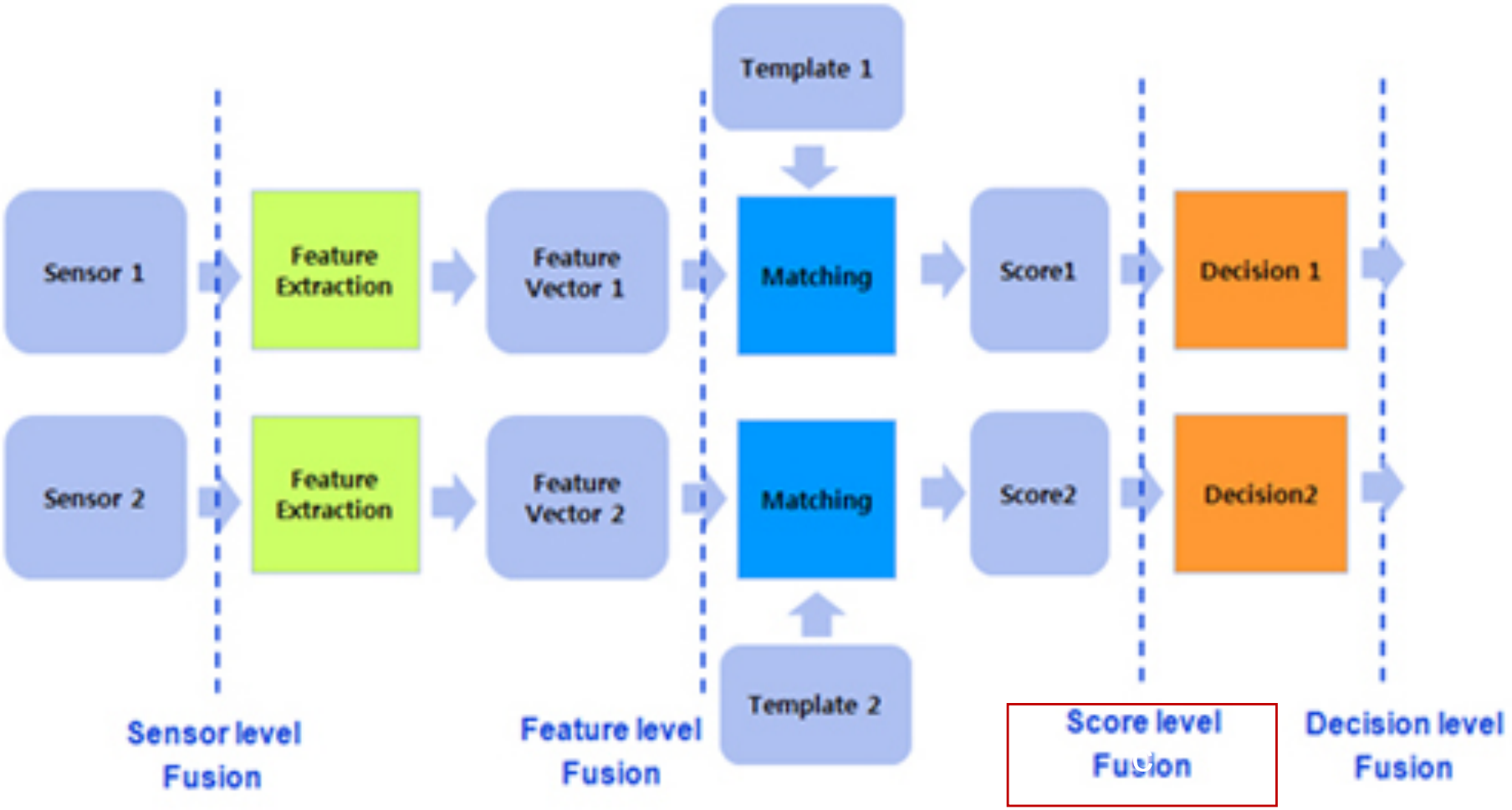




A simple scheme for the fusion of two heterogeneous feature vectors whose lengths are fixed across all users

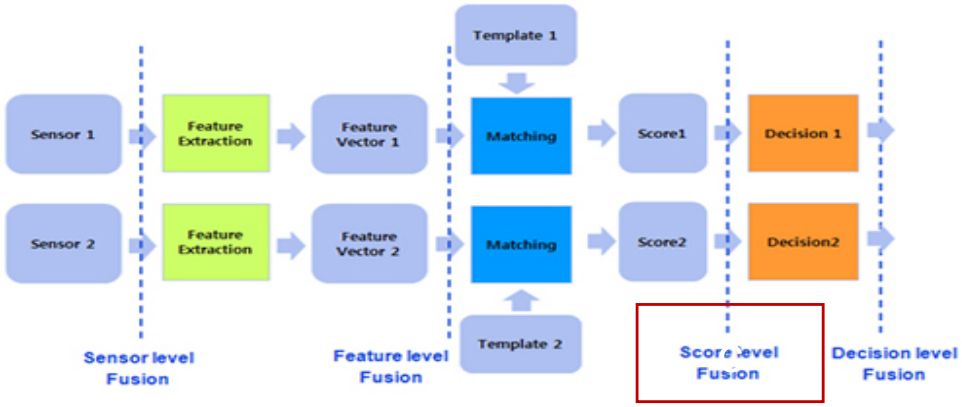
Illustration of a homogeneous feature fusion (template improvement) scheme

Fusion levels

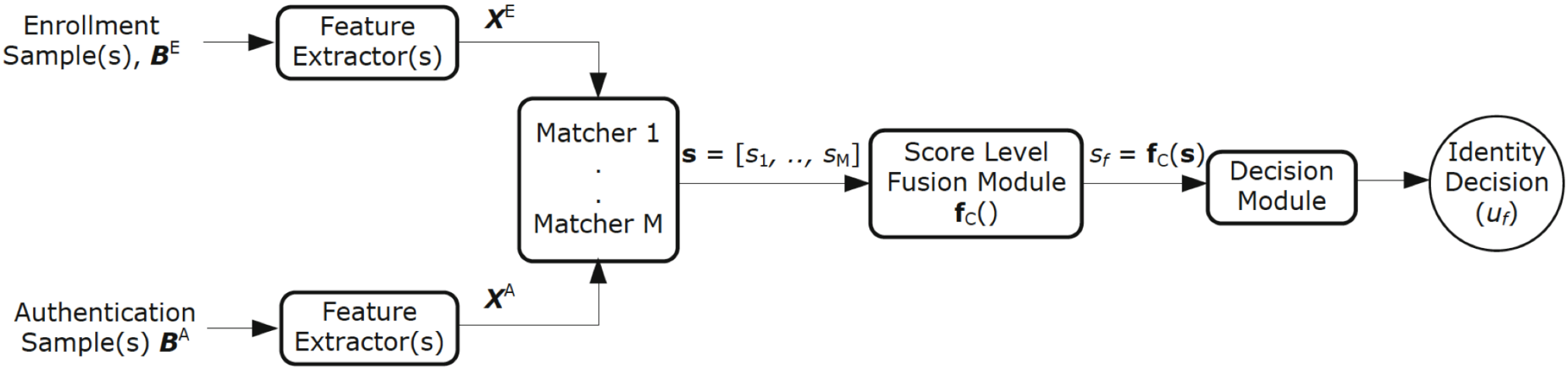


Score level Fusion: When each biometric system outputs a match score indicating the proximity of the input data to a template, integration can be done at the *match score level.*

Fusion levels

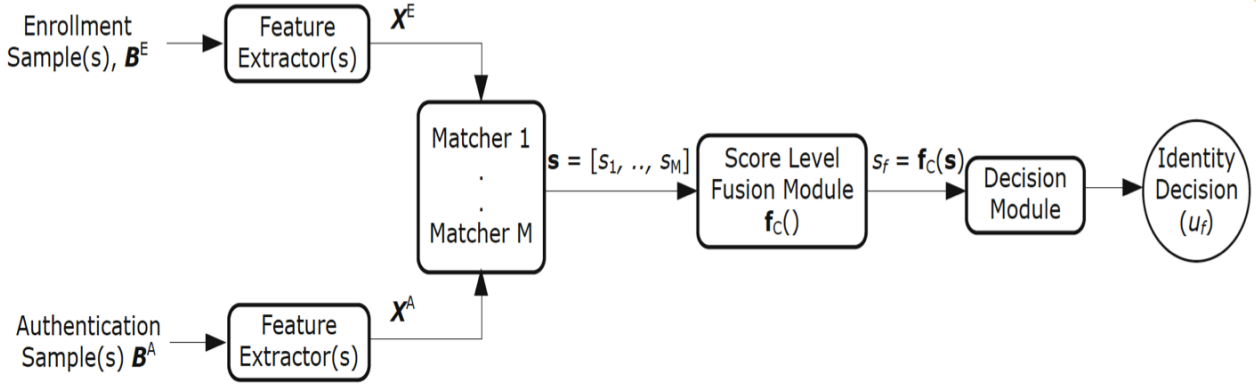


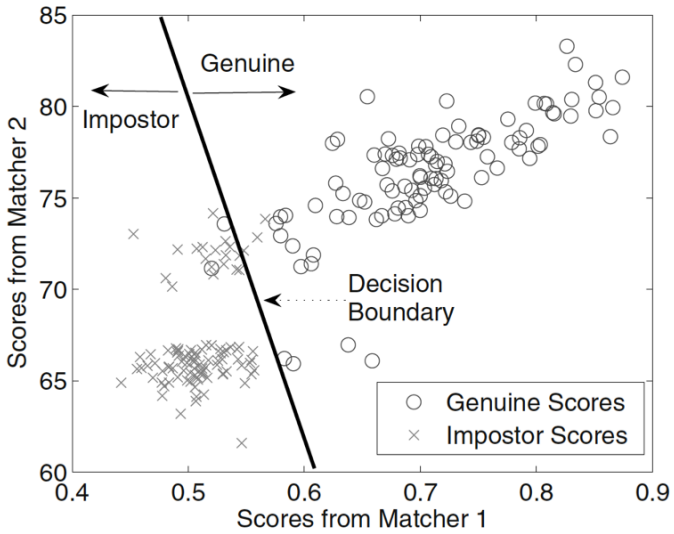
Score level Fusion: When each biometric system outputs a match score indicating the proximity of the input data to a template, integration can be done at the *match score level.*

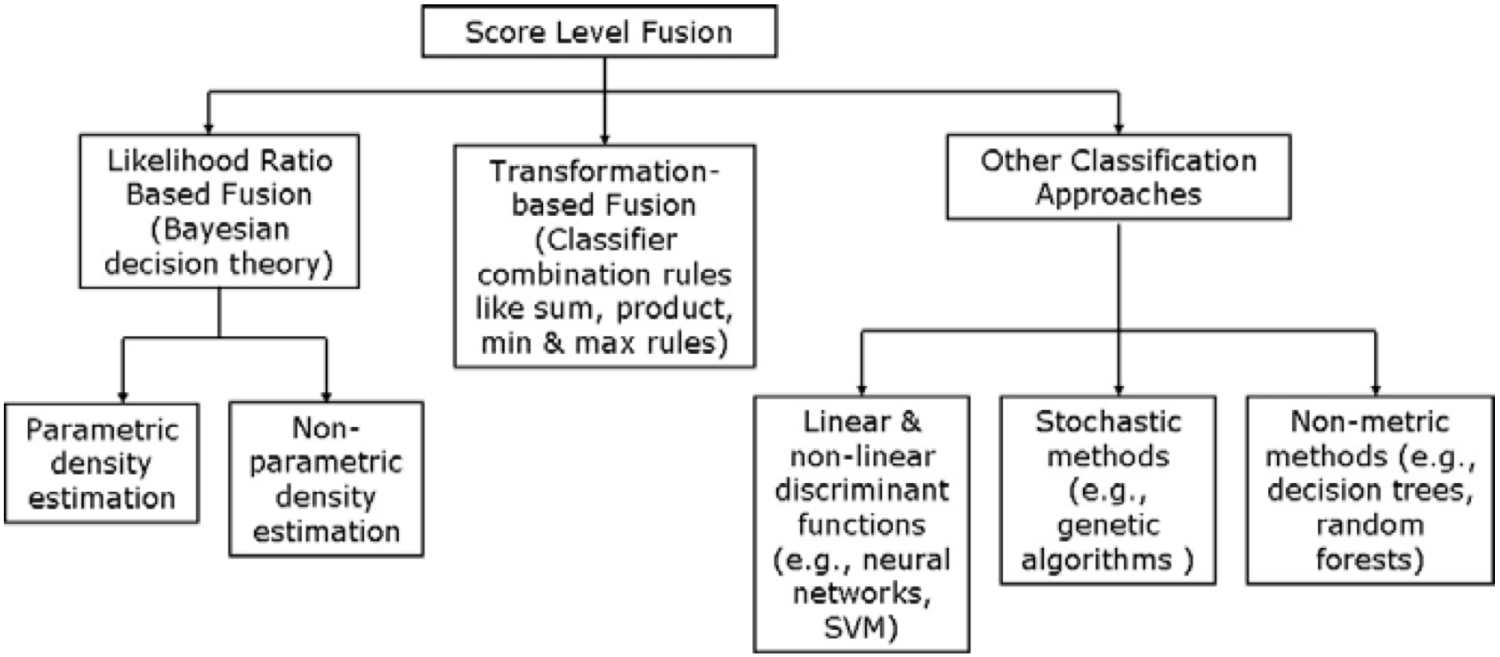


Score-level fusion is a challenging problem when the match scores generated by the individual matchers are not homogeneous

Fusion levels



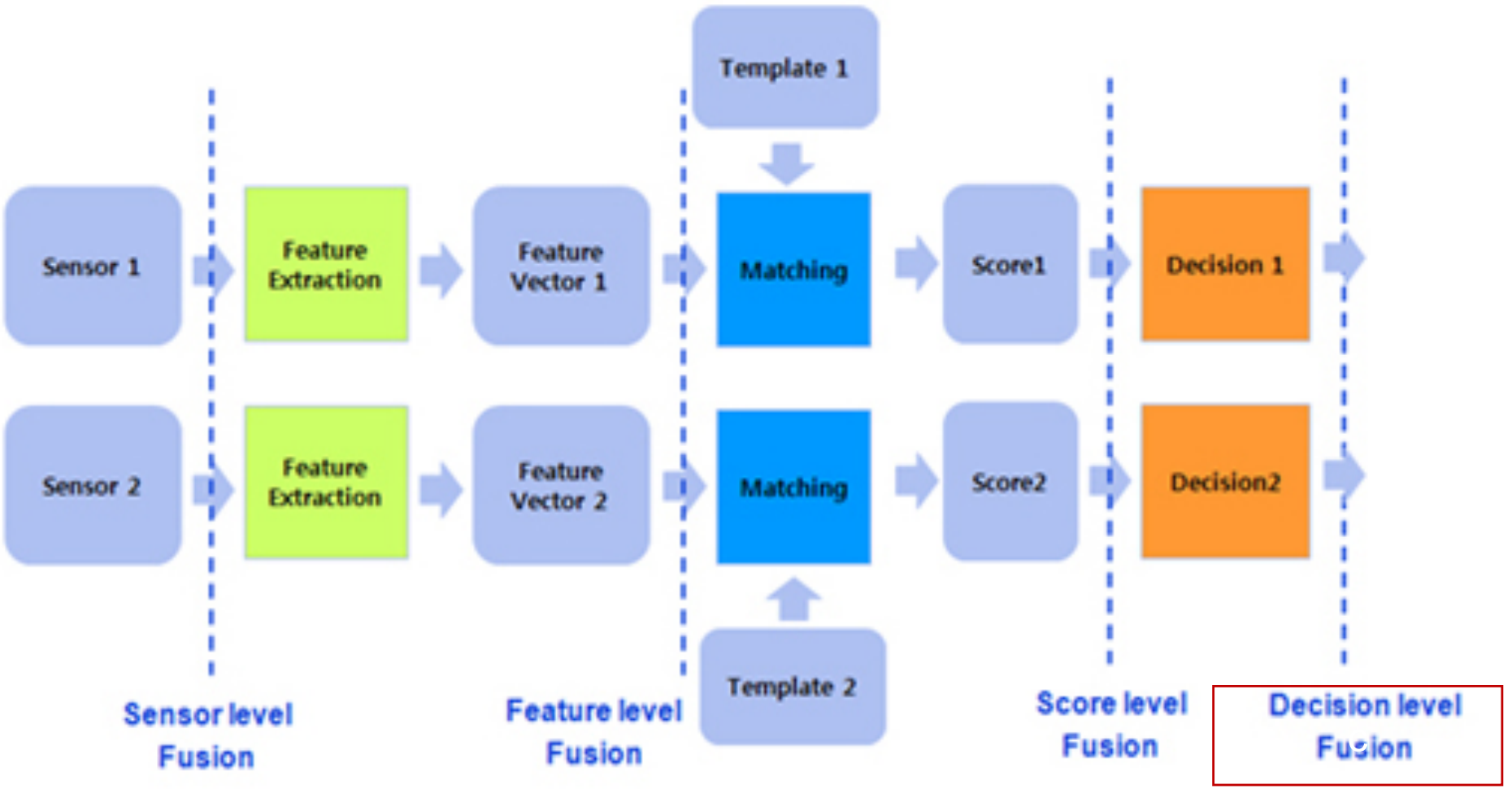




Example of a linear decision boundary

Taxonomy of classification approaches that can be used for score level fusion

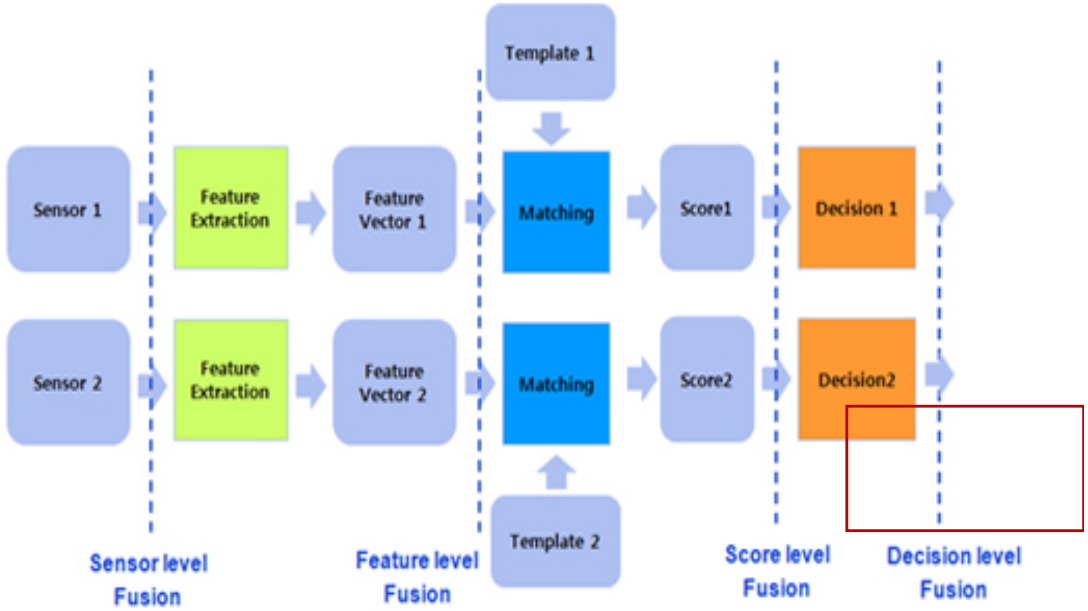
Fusion levels



Decision level Fusion: Integration of information takes place when each biometric system independently makes a decision about the identity of the user (in an identification system) or determines if the claimed identity is true or not (in a verification system)

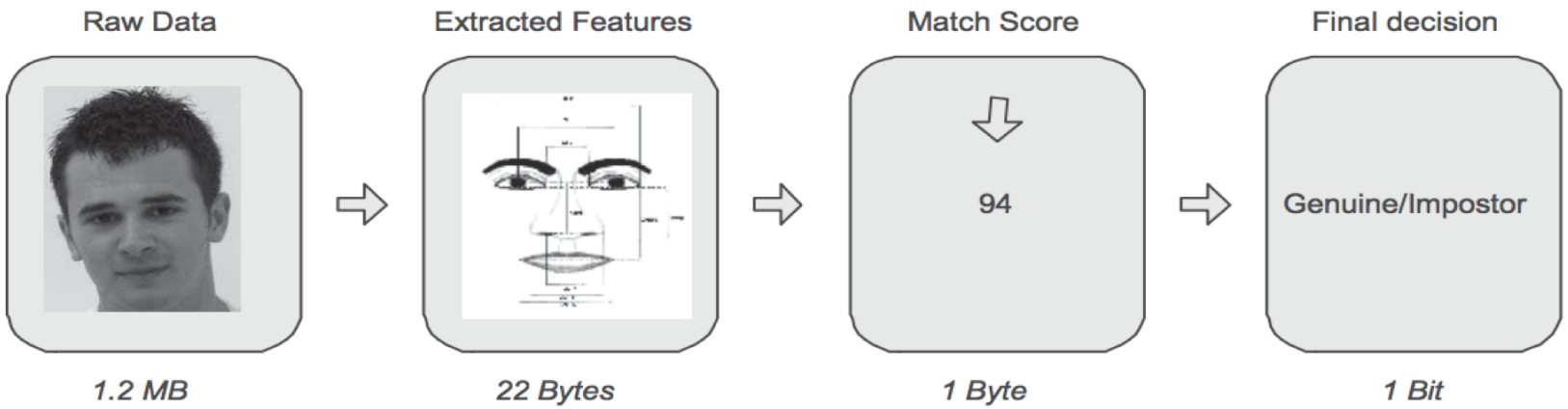
Fusion levels

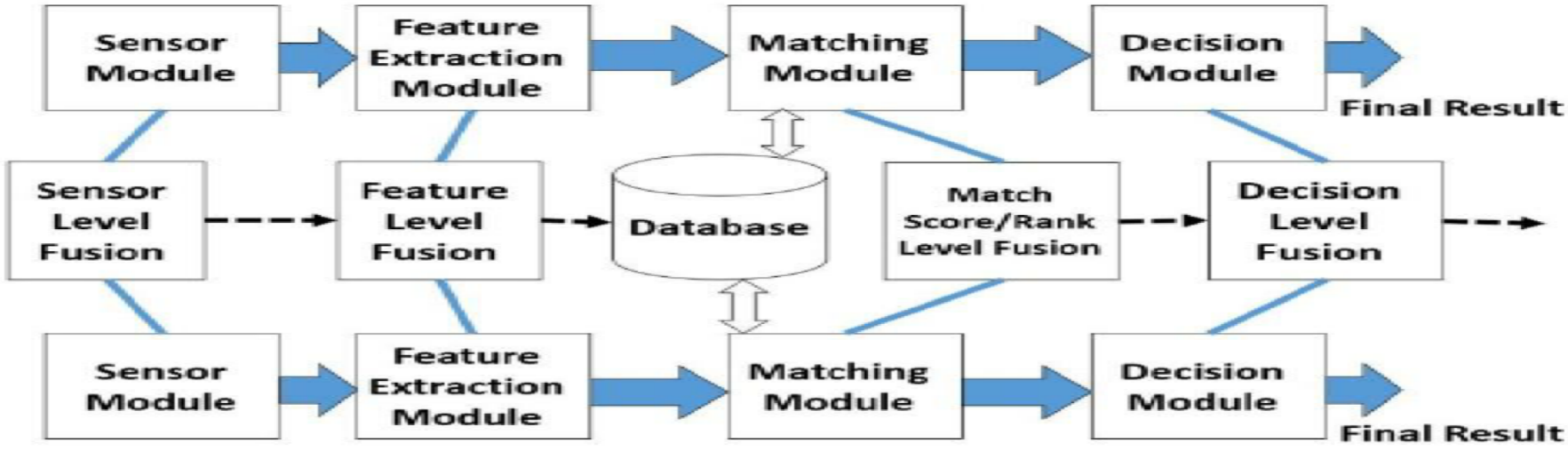
Decision level Fusion: Integration of information takes place when each biometric system independently makes a decision about the identity of the user (in an identification system) or determines if the claimed identity is true or not (in a verification system)



- AND/OR rules (note: FAR & FRR will be varied !)
- (weighted) Majority voting
- Bayesian Decision Fusion:
- …

Fusion levels



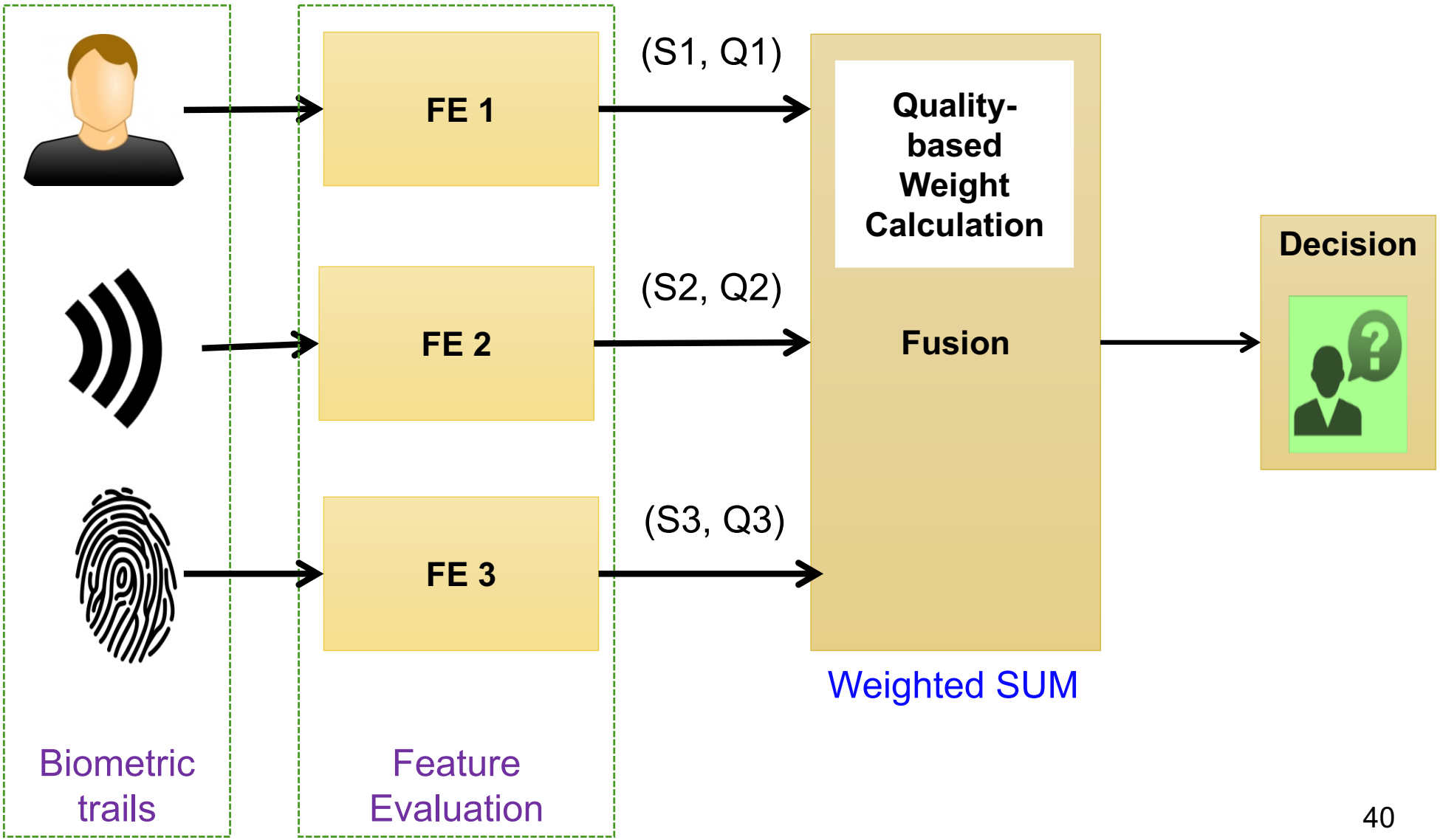


Developing efficient matching algorithms is often the most challenging aspect in the design of a biometric system and, thus, fusion at the sensor or feature levels introduces additional processing complexities

Towards a General (Intrinsic & Extrinsic) Score-level Fusion In Co-Authentication Systems

Seminar: Week 11

Biometric Co-Authentication System

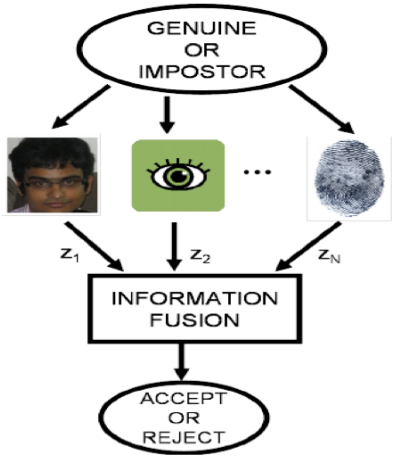


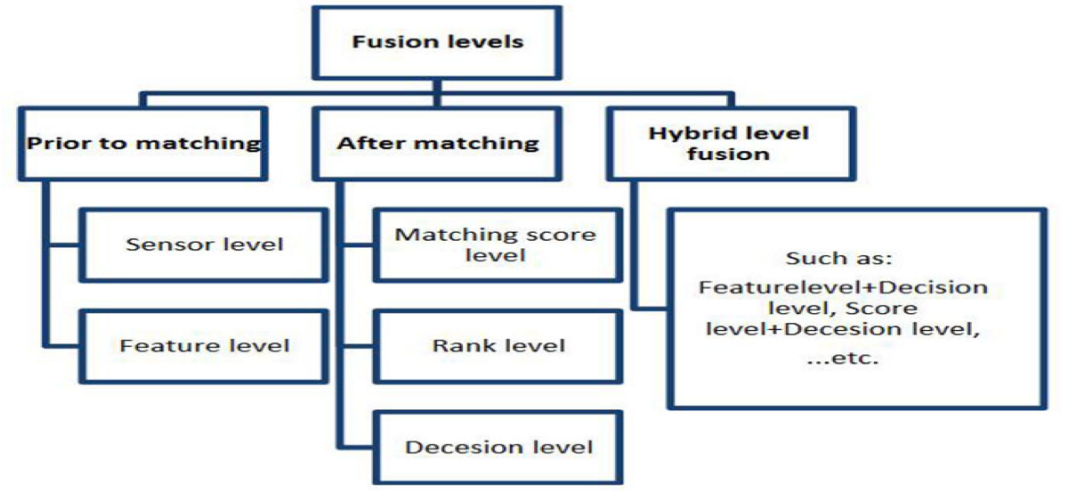
Outline

- ~~Introduction~~
  - ~~Biometric-based co-authentication systems~~
- ~~Sources of multiple evidence~~
- ~~Acquisition and processing architecture~~
- ~~Fusion levels~~
- Summary
- Reading:
  - Chapter 6 [2]

Summary

- Correlation between the biometric sources needs to be examined before determining their suitability for fusion
  - Combining uncorrelated or negatively correlated sources that make complementary errors is expected to result in a better improvement in matching performance
- Information fusion in biometrics can be accomplished at several levels
  - Hybrid level fusion is possible, too
- Multibiometric systems are expected to alleviate some of the limitations of unibiometric systems





Q&A

www.cse.hcmut.edu.vn/~khanh

khanh@hcmut.edu.vn

https://www.facebook.com/dang.ssolutions