

Basics II

COMP 388-002/488-002 Biometrics

Daniel Moreira
Fall 2023



LOYOLA
UNIVERSITY CHICAGO

Today you will...

Discuss

Biometric systems and their errors.

Metrics to compare Biometric systems.

Today's attendance

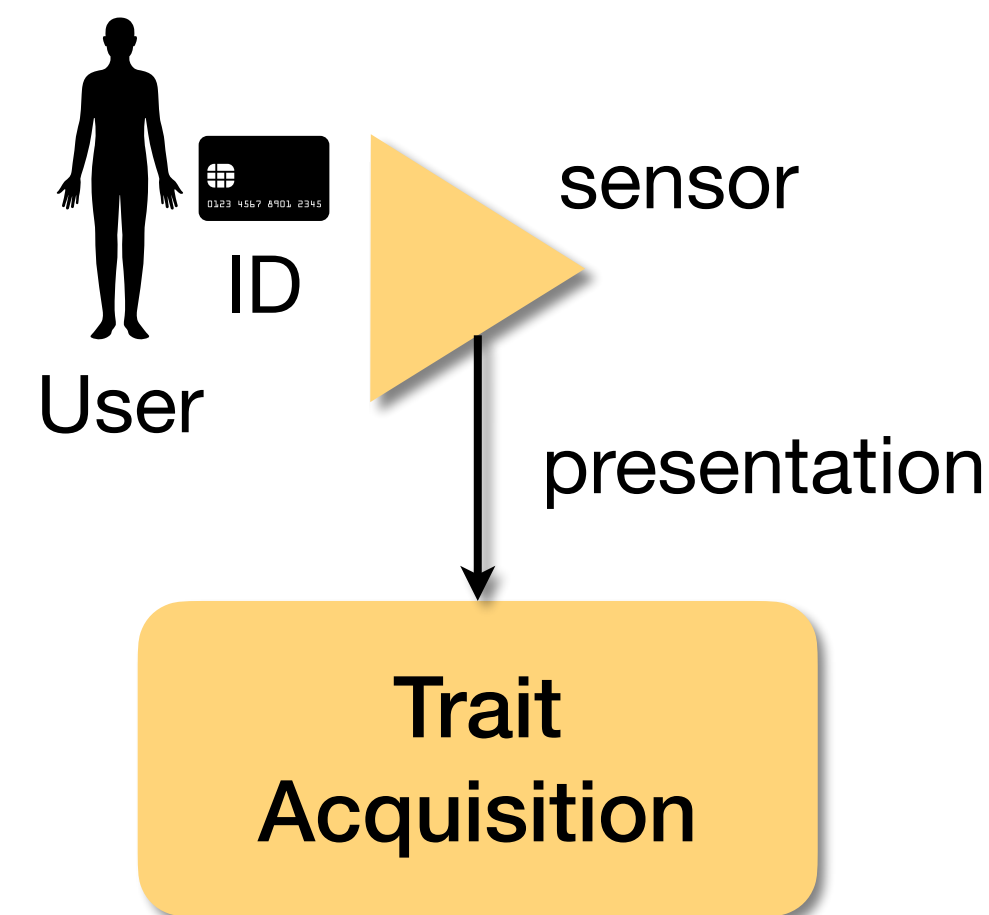
Please fill out the form

<https://forms.gle/11MHC4i3BMoL1aGs7>



Biometric Systems

Enrollment



Trait Acquisition

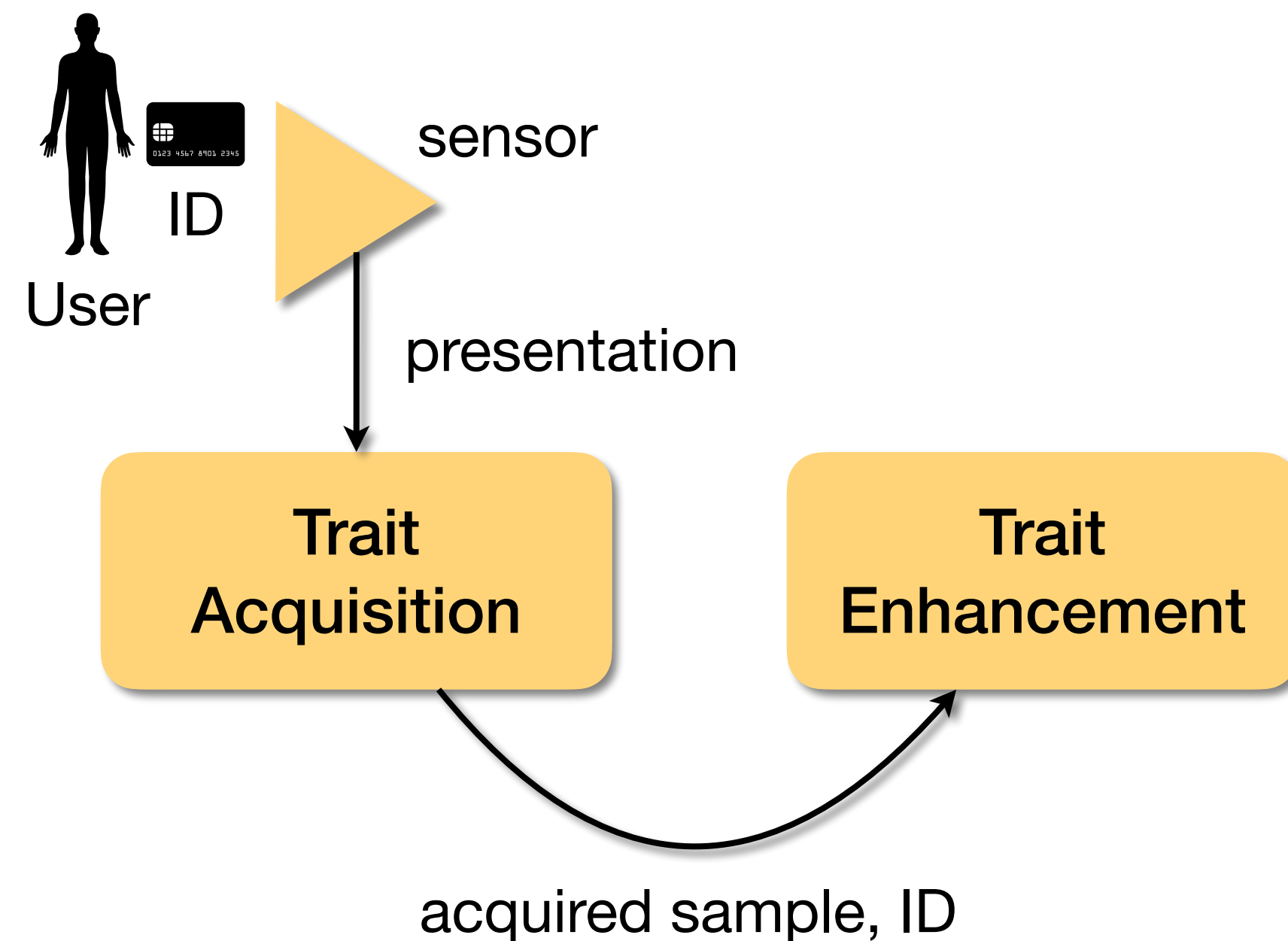
We'll have data-collection classes.
We'll use real-world sensors.

What to observe?

Sensors have different **quality**
(in terms of precision, resolution,
presence of noise, and usability)

Biometric Systems

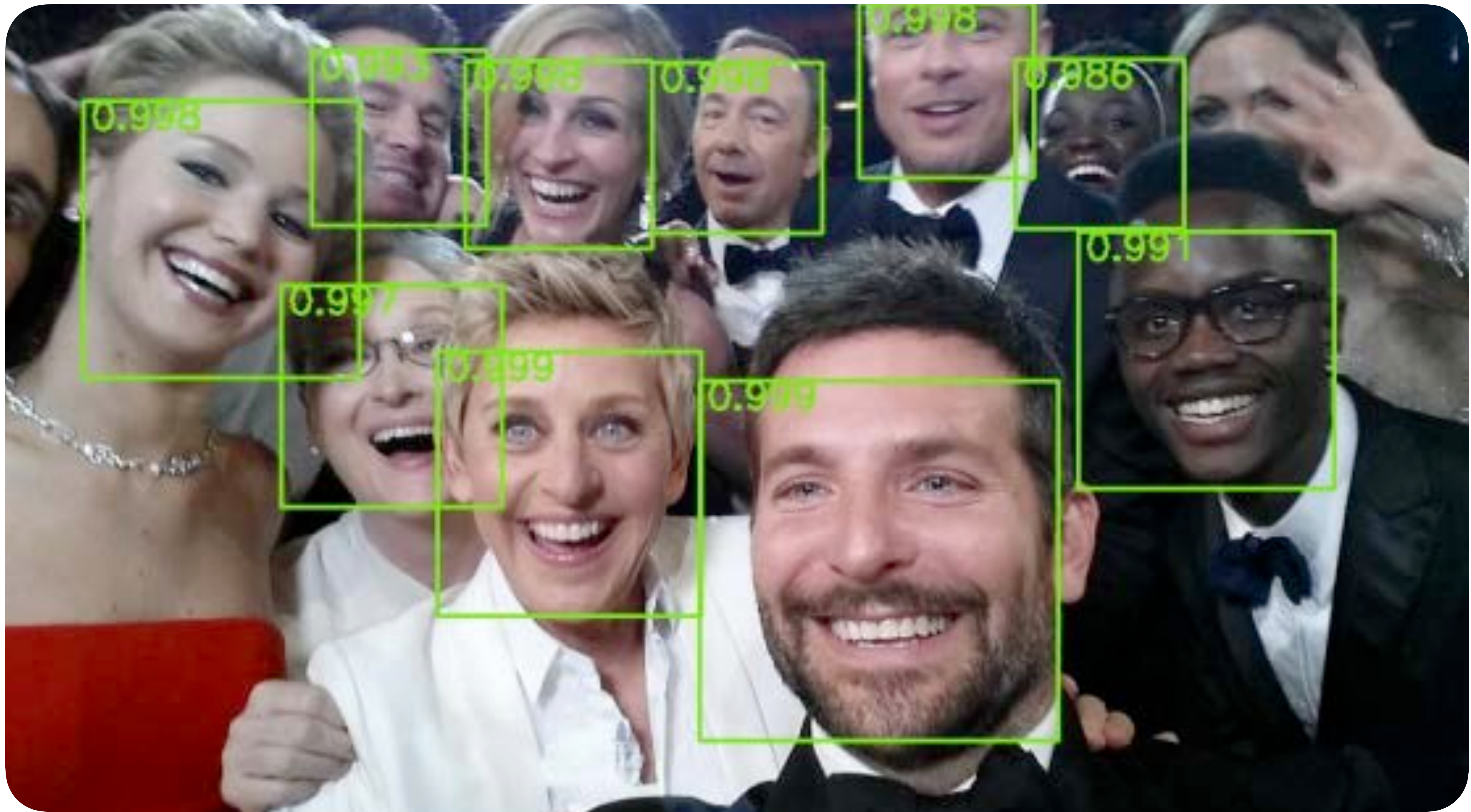
Enrollment



Trait Enhancement

Noise removal.

Operations to keep only **essential** information (consider universality, uniqueness, permanence, circumvention, explainability, and performance).



Load irises

Load examination

Save examination

Save report

Quit program

Brightness



Contrast



Sharpening



Segment iris

Brightness



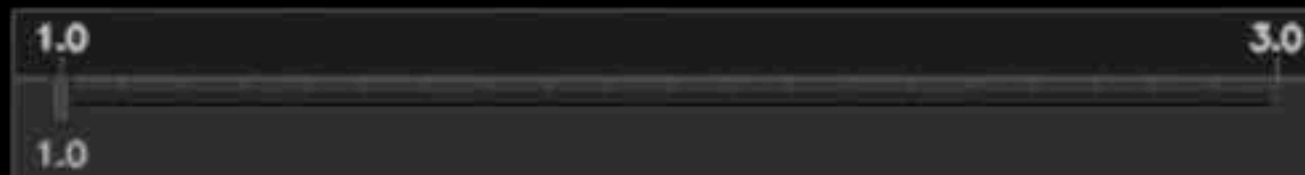
Contrast



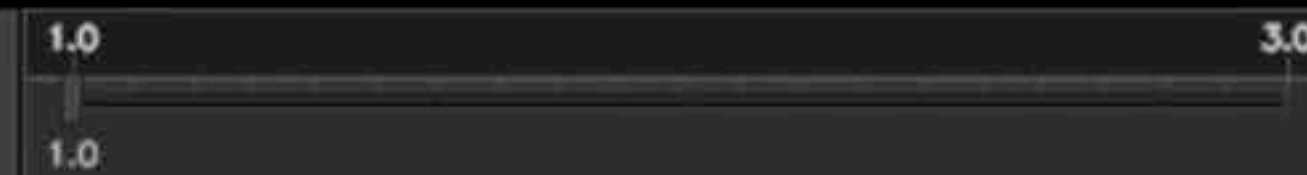
Sharpening



Segment iris



1x



Human-Interpretable Features

<input checked="" type="checkbox"/> TSHEPII	<input type="checkbox"/> Show Matched	-	0	+	out of 0
	<input type="checkbox"/> Show Unmatched	-	1	+	out of 0
<input checked="" type="checkbox"/> SURF	<input type="checkbox"/> Show Matched	-	0	+	out of 0
	<input type="checkbox"/> Show Unmatched	-	1	+	out of 0
<input checked="" type="checkbox"/> Crypts	<input type="checkbox"/> Show Matched	-	0	+	out of 0

<input checked="" type="checkbox"/> MSER	<input type="checkbox"/> Show Matched	-	0	+	out of 0
	<input type="checkbox"/> Show Unmatched	-	1	+	out of 0
<input checked="" type="checkbox"/> SIFT	<input type="checkbox"/> Show Matched	-	0	+	out of 0
	<input type="checkbox"/> Show Unmatched	-	1	+	out of 0

Undo last removal

Manual Annotation

Annotate...

☒ Matching Regions ☒ Non-Matching Regions☒ Show Matching Regions
☒ Show Non-Matching Regions

Non-Human-Interpretable Features

Gabor Filters

thr: 0.4461

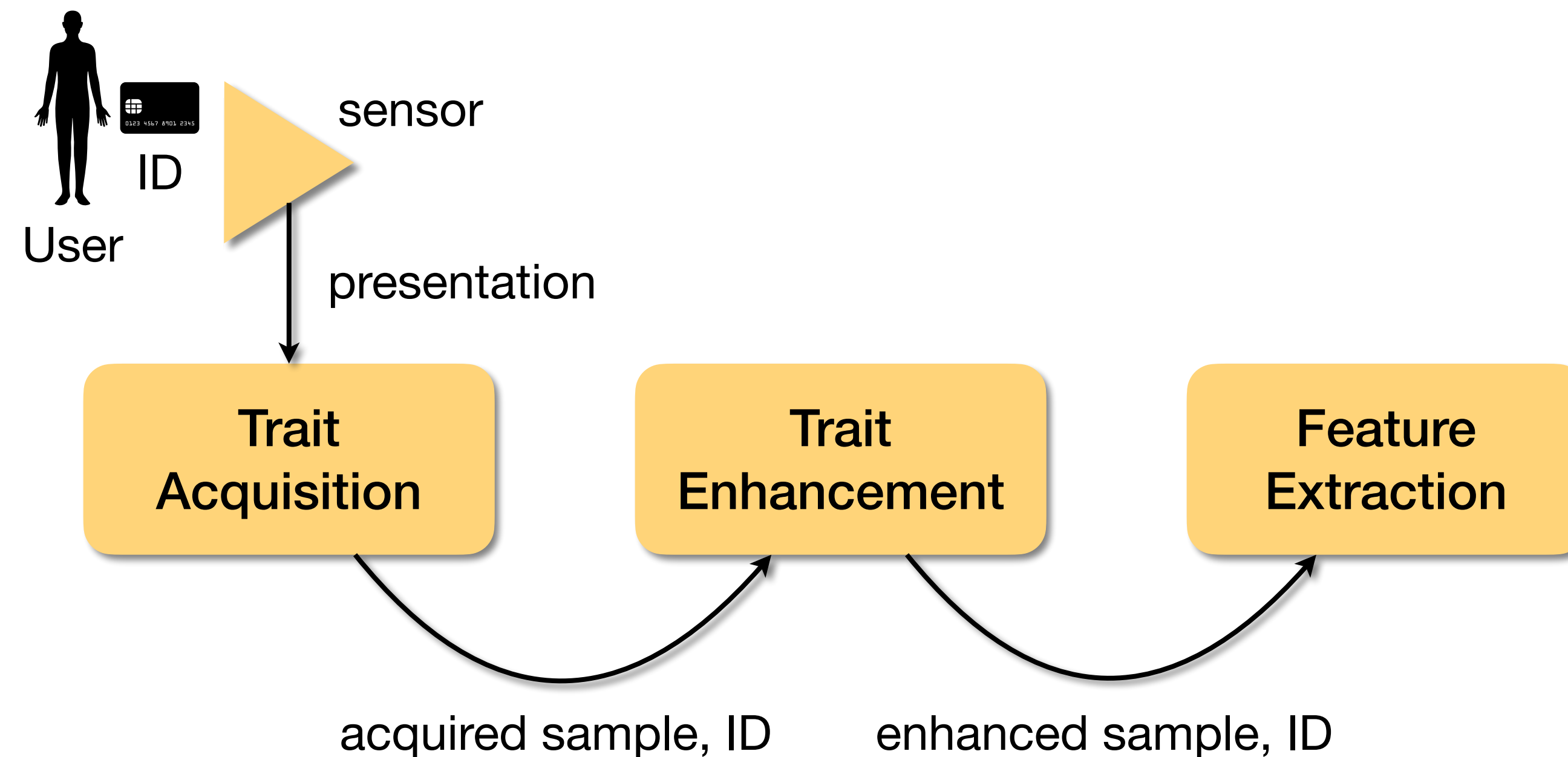
BSIF Filters

thr: 0.4216

Global match score

Biometric Systems

Enrollment Modules



Feature Extraction

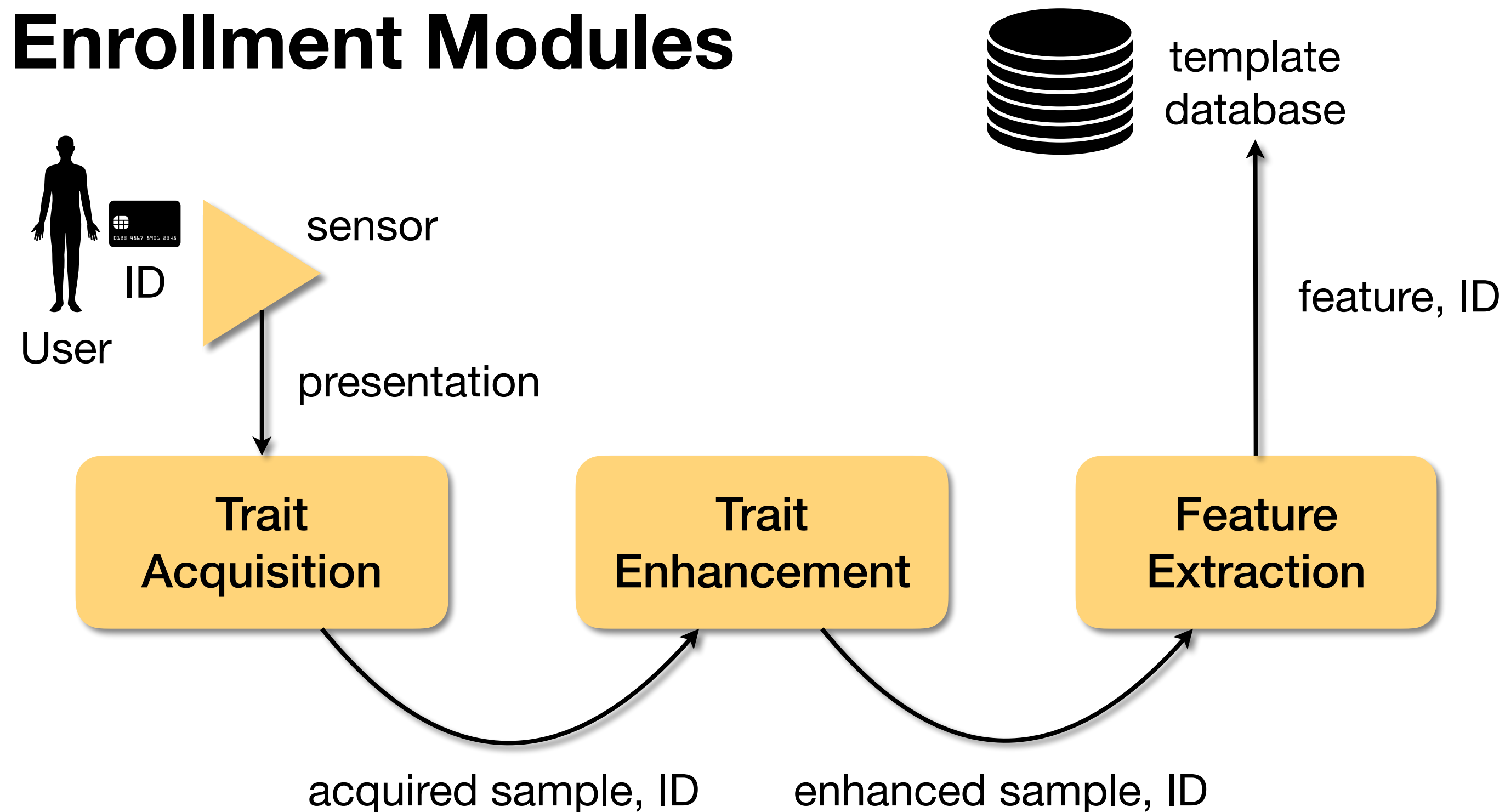
Compact but expressive digital representation of the trait.

Types

Handcrafted or **learned** with machine learning.
We'll see both cases.

Biometric Systems

Enrollment Modules

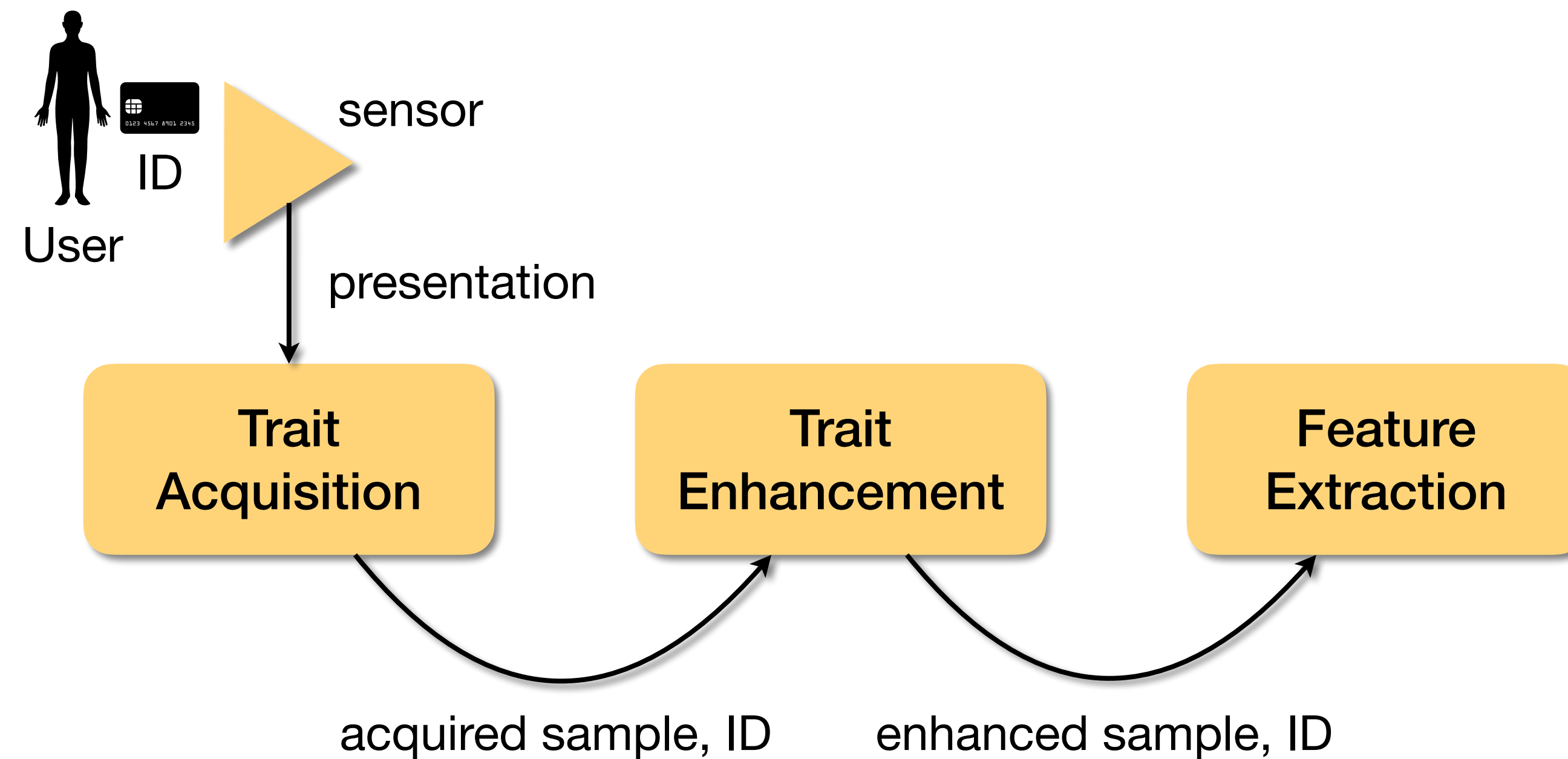


Template Database

It inherits all the security and privacy issues from database systems. Be careful with invasions, leaks, etc.

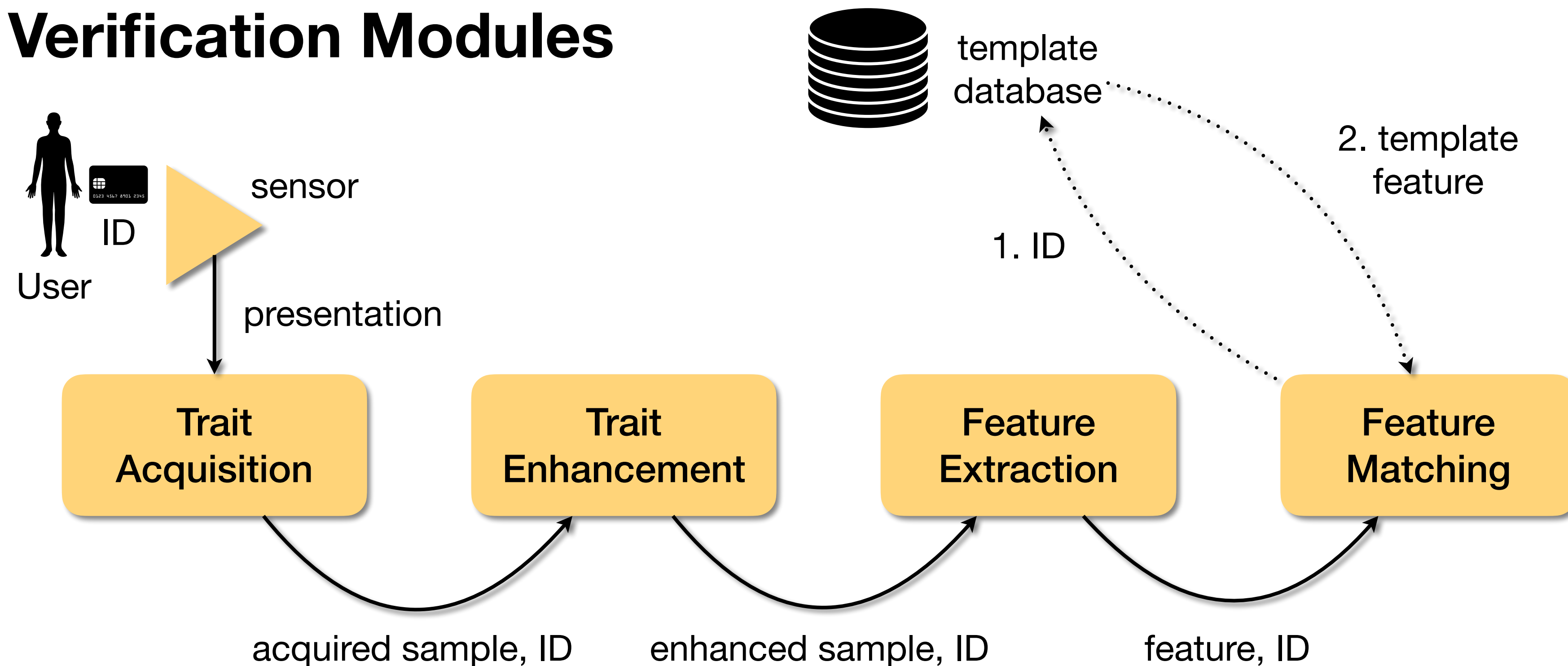
Biometric Systems

Verification Modules



Biometric Systems

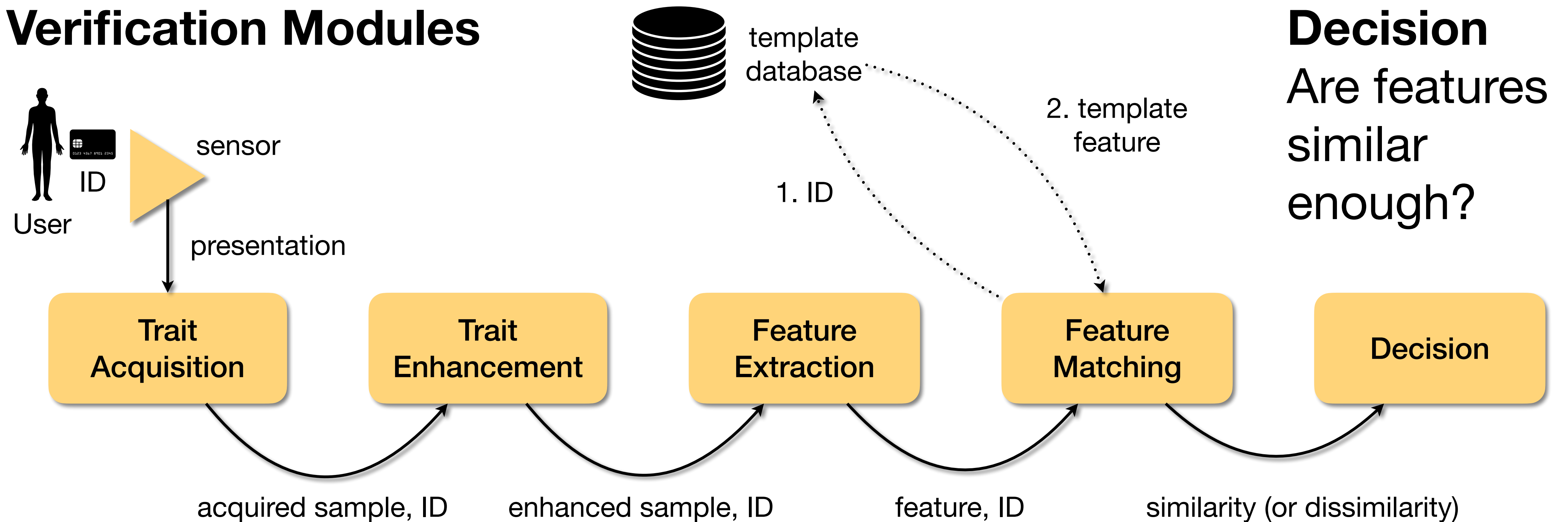
Verification Modules



Feature Matching
Comparison of **acquired** and **template** features.

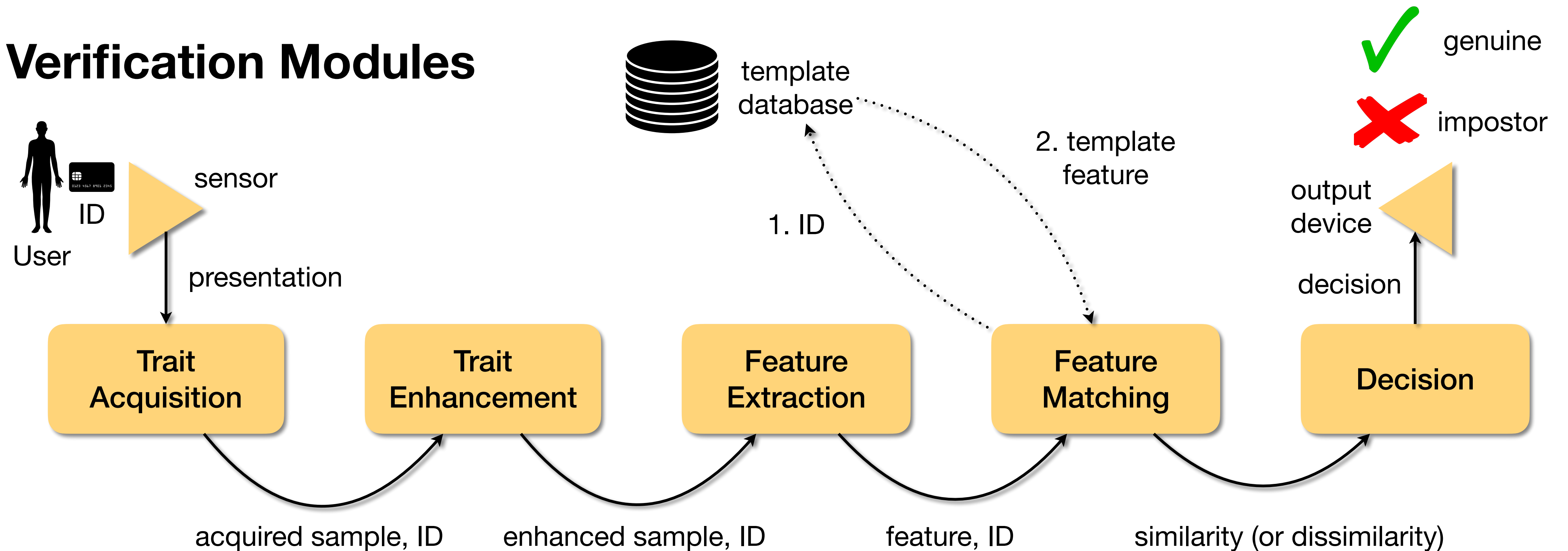
Biometric Systems

Verification Modules



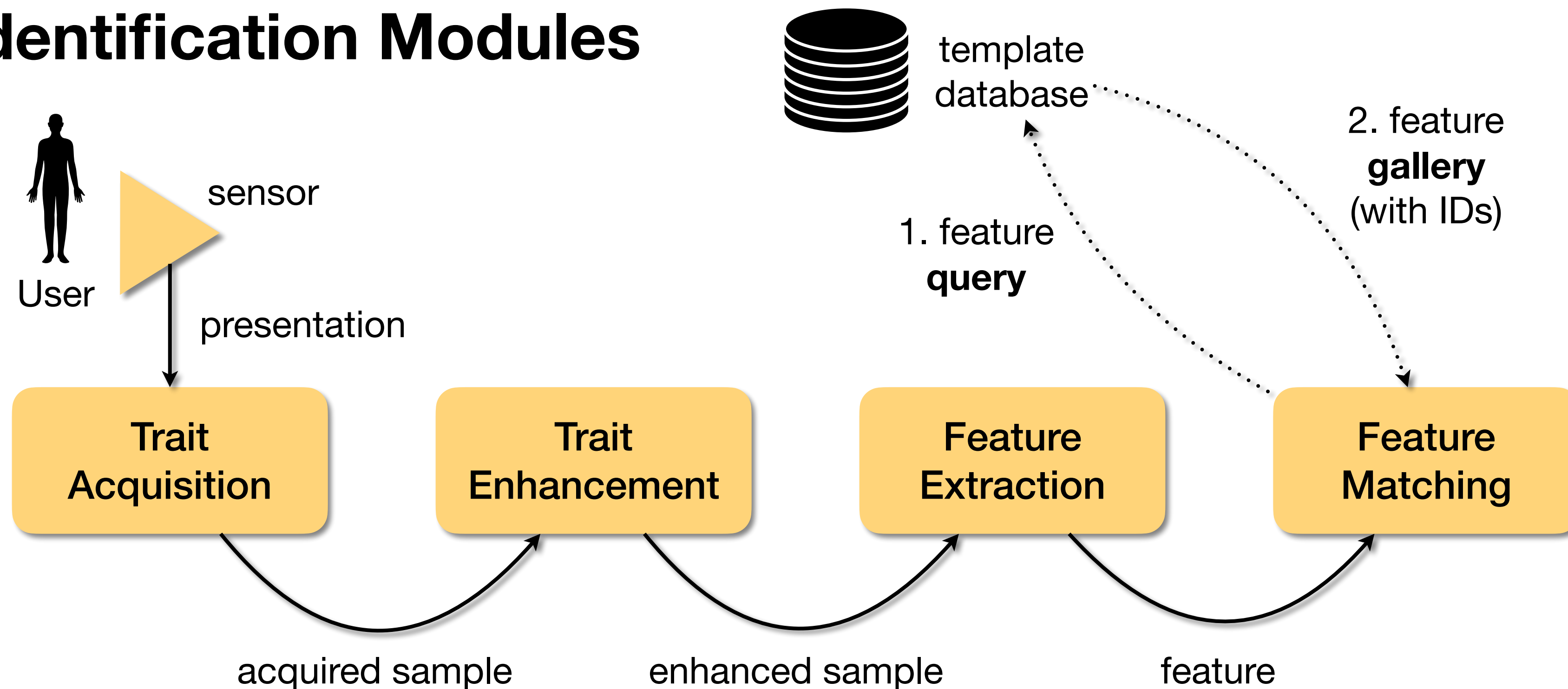
Biometric Systems

Verification Modules



Biometric Systems

Identification Modules



Gallery
Closest
template
features to
query.

Biometric Systems

Query and Gallery Example



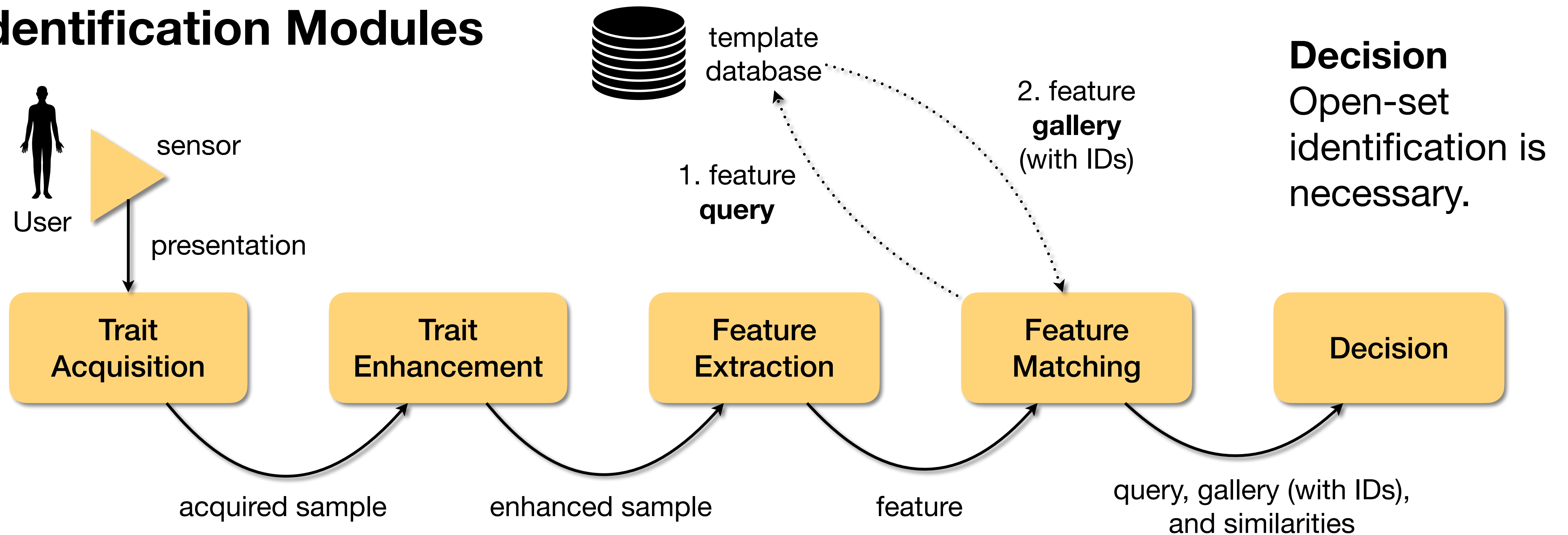
query



gallery

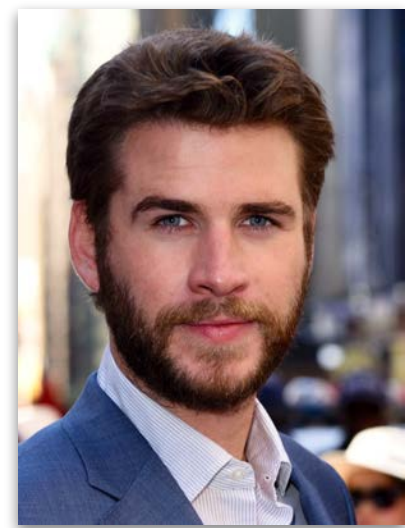
Biometric Systems

Identification Modules



Biometric Systems

Open-set vs. Closed-set Identification



Query
(Liam Hemsworth)

Dataset



Robert
Downey Jr.



Scarlet
Johansson



Chris
Evans



Mark
Ruffalo

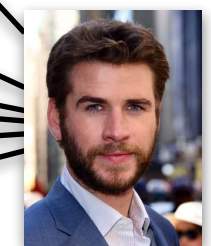


Chris
Hemsworth



Jeremy
Renner

Feature Space



Closed Set

Output
This is
Chris Hemsworth!



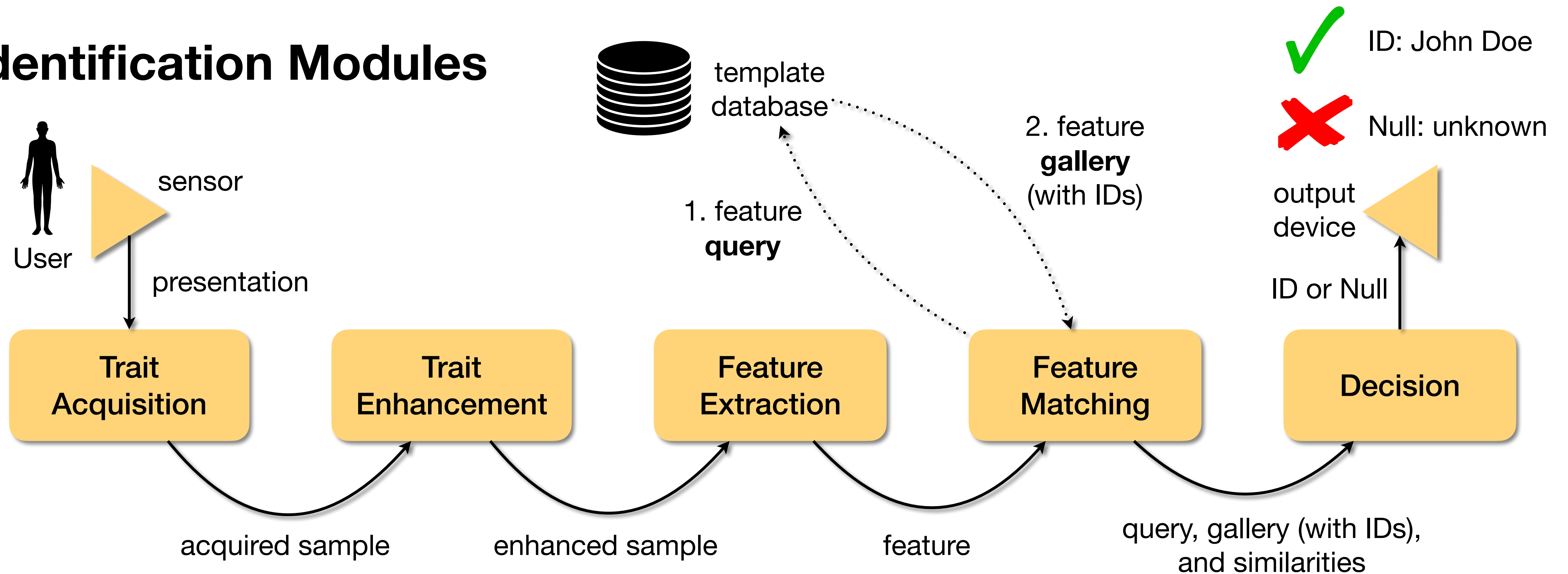
Open Set

Output
I don't know
this person!



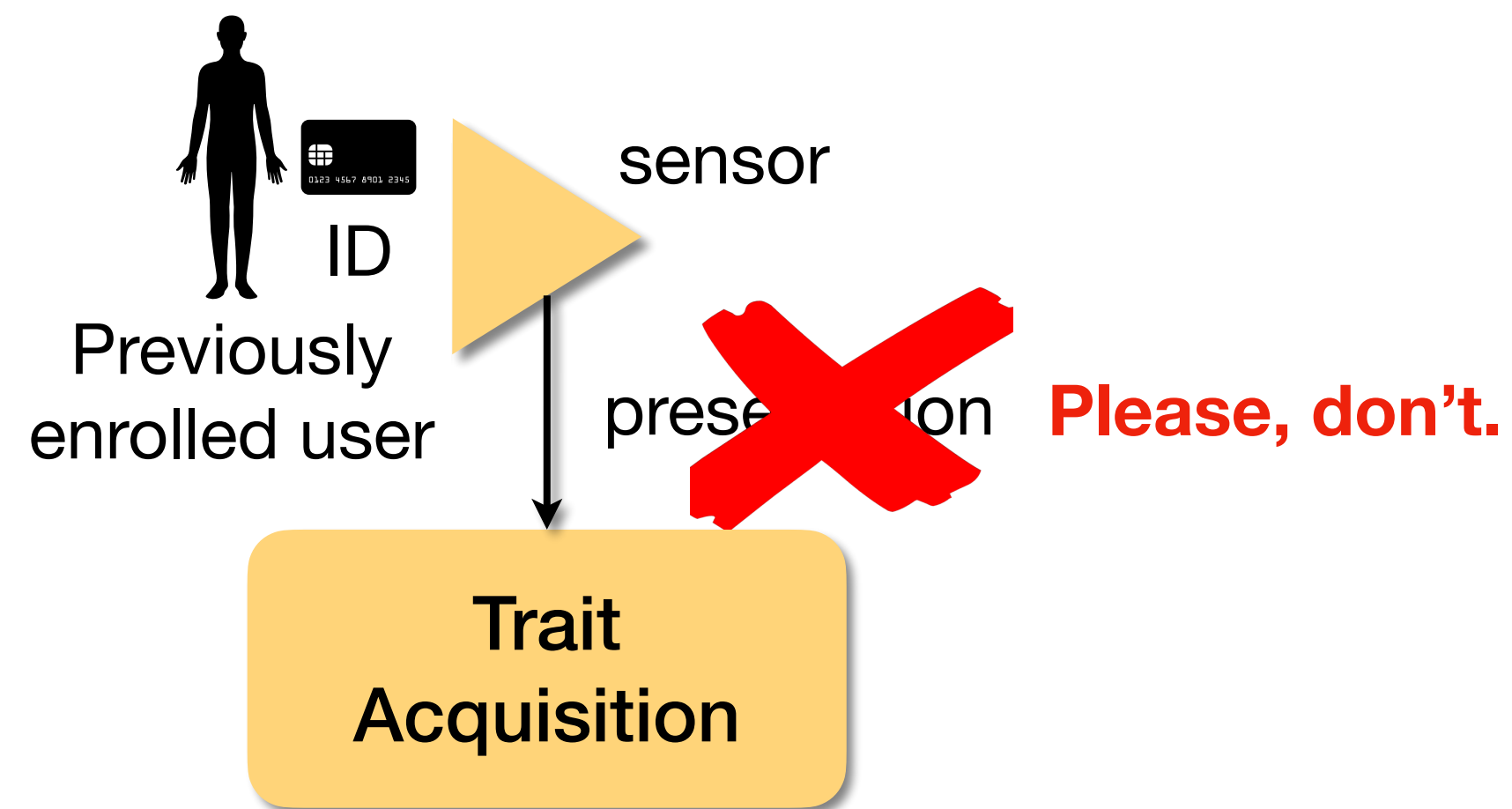
Biometric Systems

Identification Modules



Biometric Systems

Enrollment Revision

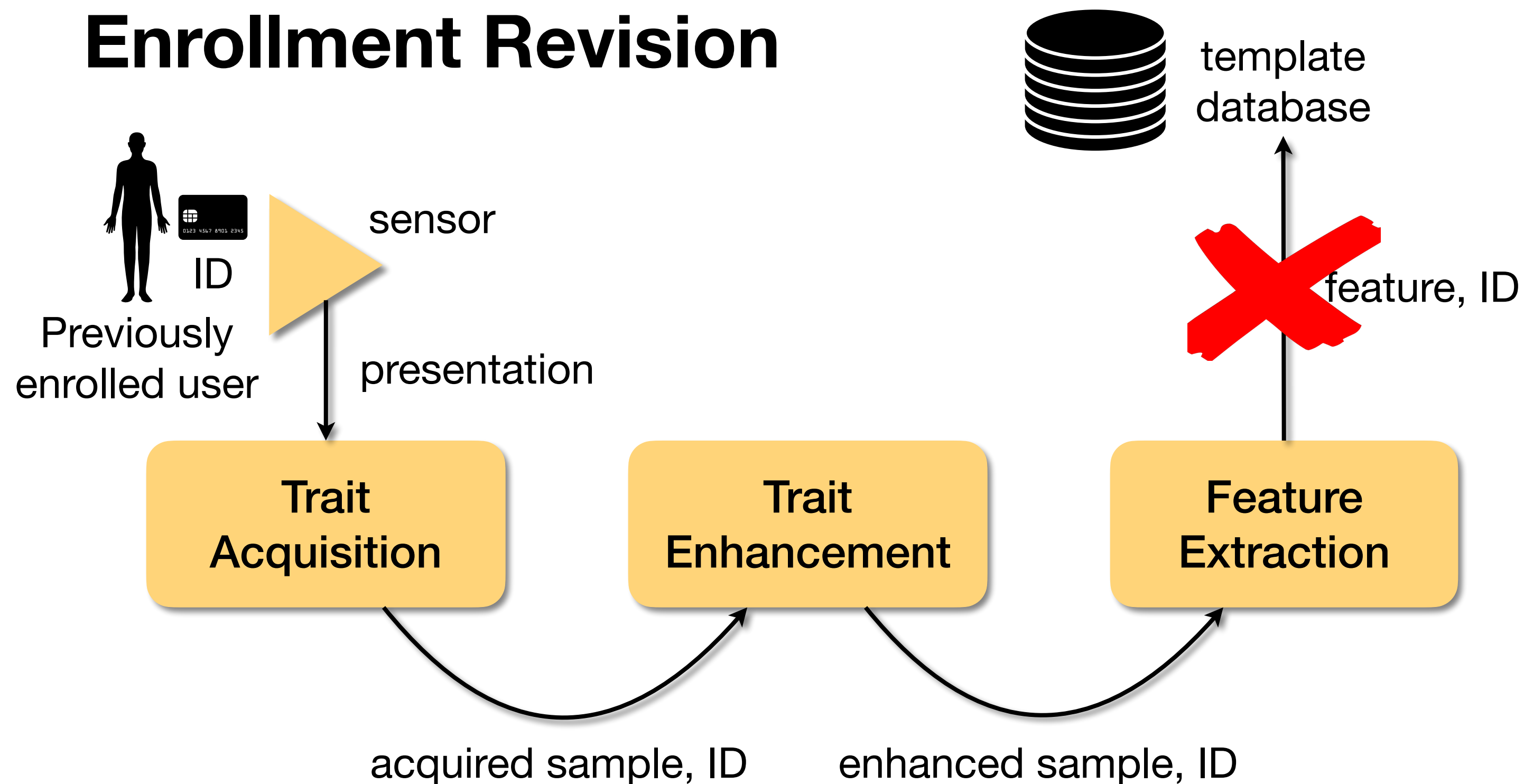


Attended operation?

“I’m seeing here in my notes that you are already enrolled.”

Biometric Systems

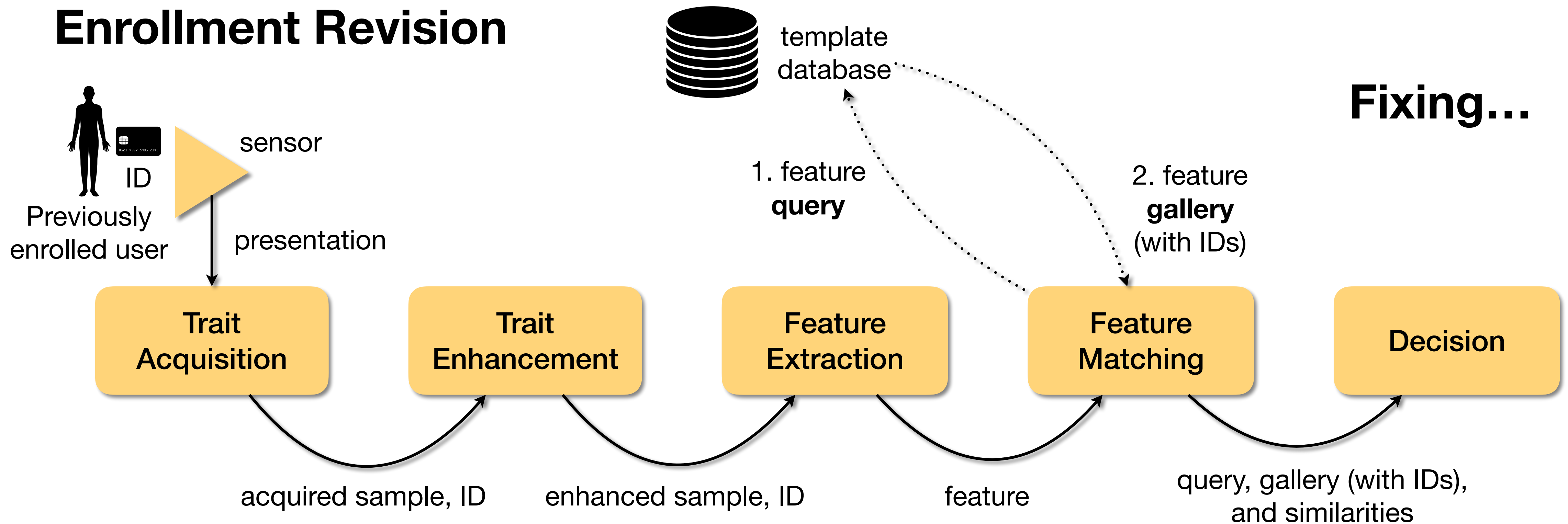
Enrollment Revision



Unattended operation?
The system must deal with re-enrollment attempts.

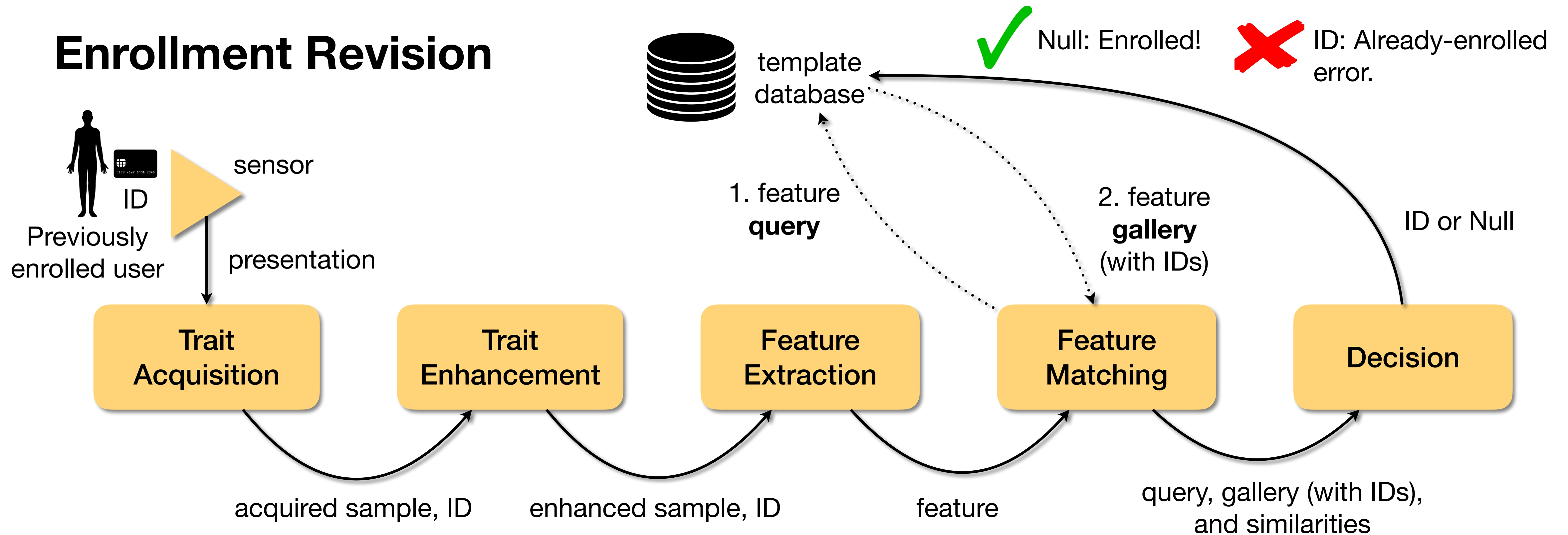
Biometric Systems

Enrollment Revision



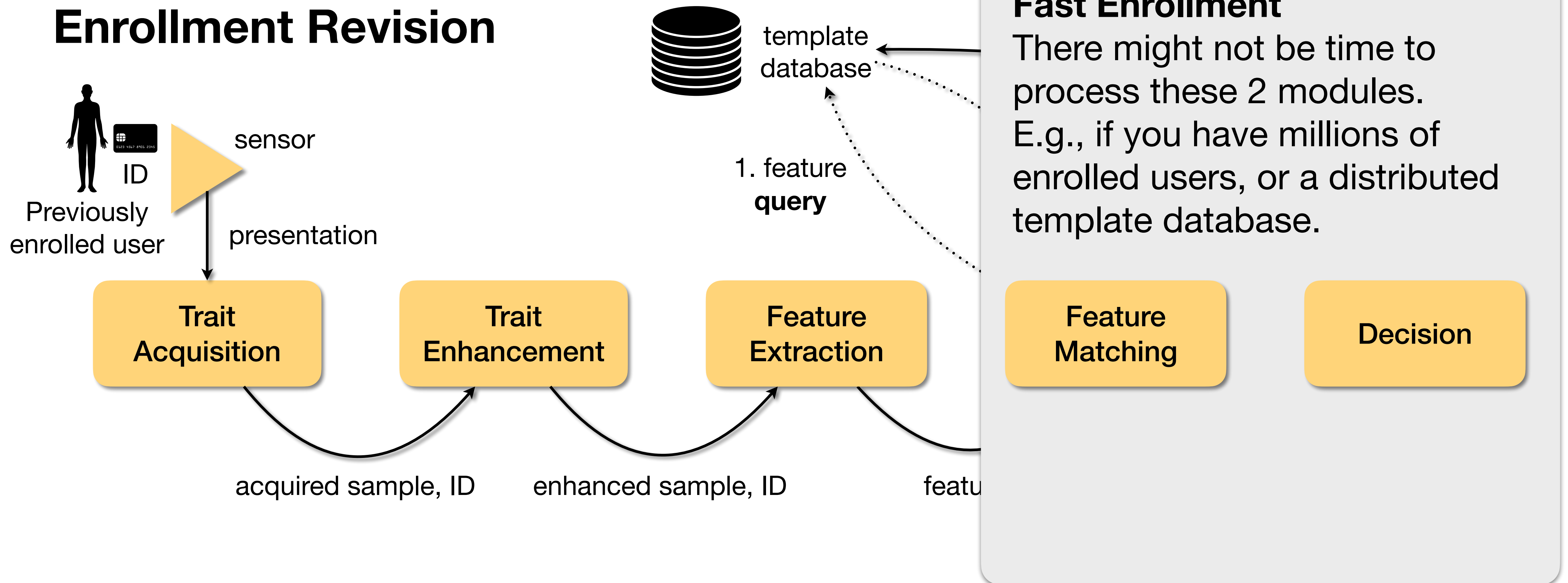
Biometric Systems

Enrollment Revision



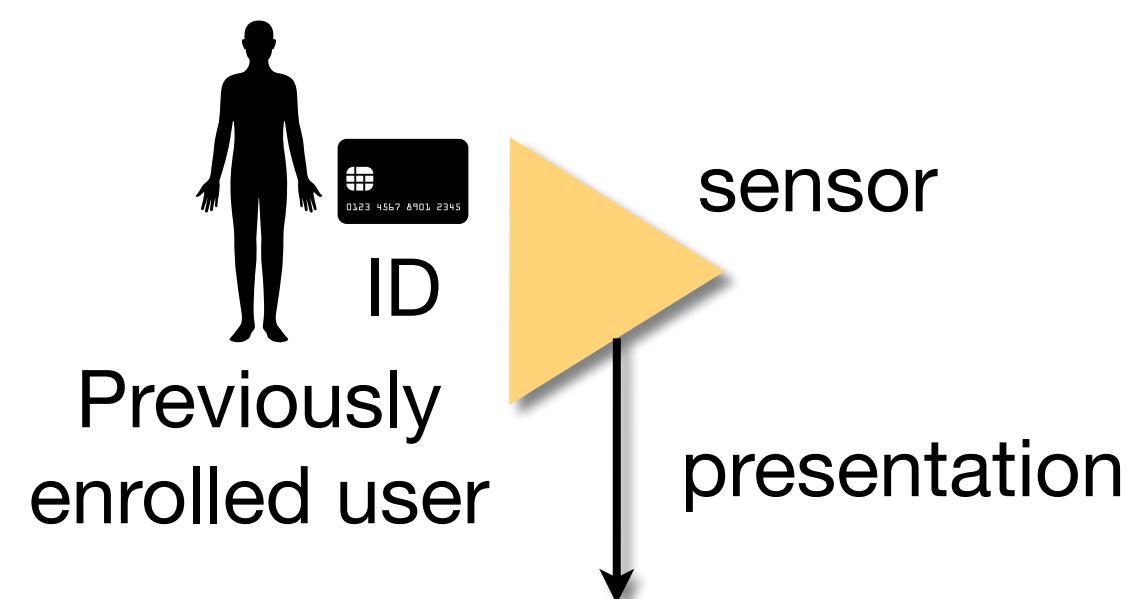
Biometric Systems

Enrollment Revision



Biometric Systems

Enrollment Revision

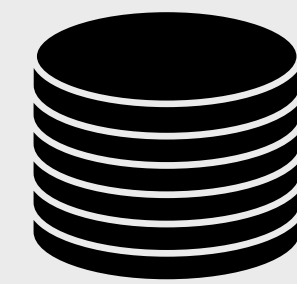


Trait
Acquisition

acquired sample, ID

Trait
Enhancement

enhanced sample, ID



template
database

feature, ID

Feature
Extraction

Fast Enrollment

Possible solution: conclude enrollment after *Feature Extraction*.

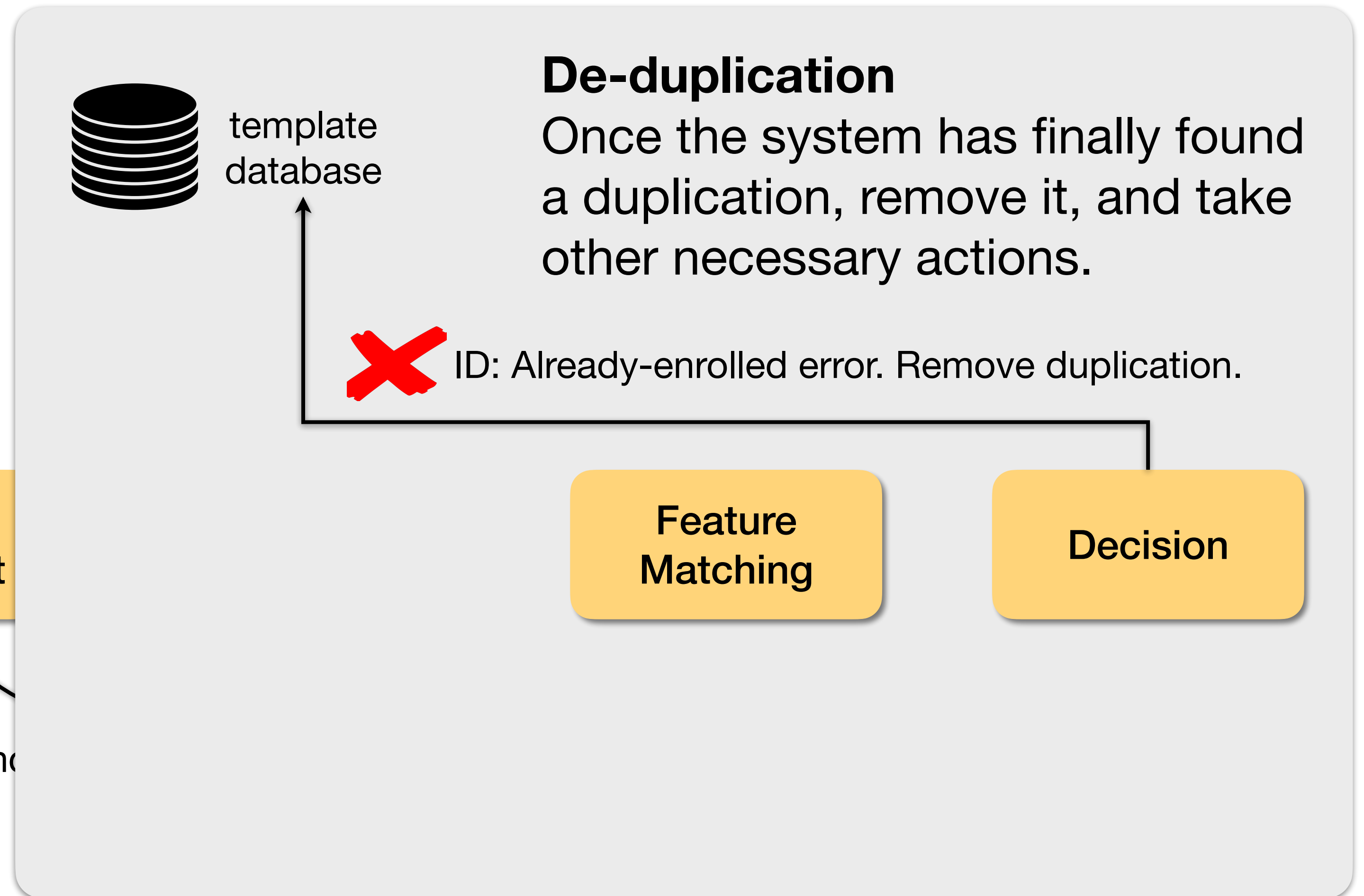
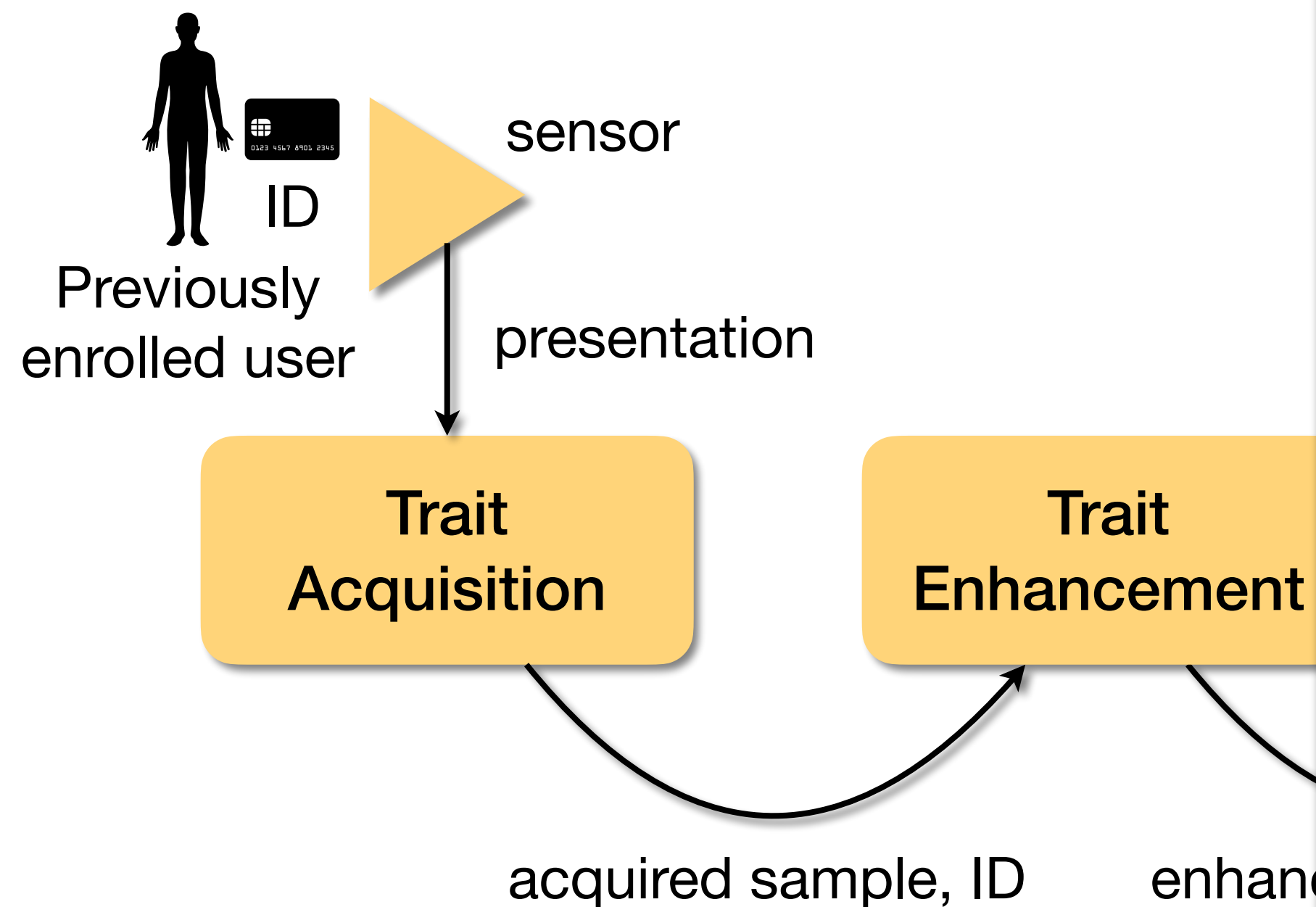
Feature
Matching

Decision

Proceed to *Feature Matching* and *Decision* and take the needed time.

Biometric Systems

Enrollment Revision



Biometric Systems

Deployment



From all modules integrated within single chips...



To disperse modules independently deployed in diverse platforms.



Biometric Systems

What do we want to consider?

Things to consider when designing a Biometrics system, besides trait.

Cooperative or non-cooperative users? (1/5)

Do users want to be identified?

Don't appeal to covert deployment.



Biometric Systems

What do we want to consider?

Things to consider when designing a Biometrics system, besides trait.

Habituated or non-habituated users? (2/5)

Do users interact with the system frequently or sporadically?



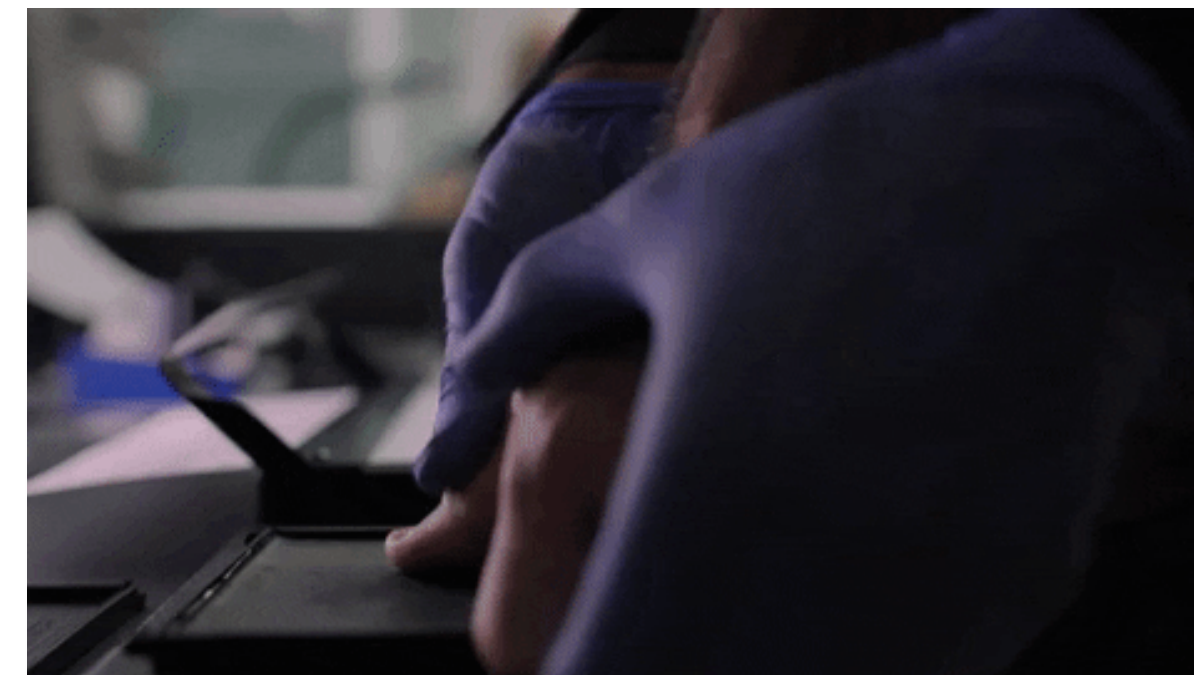
Biometric Systems

What do we want to consider?

Things to consider when designing a Biometrics system, besides trait.

**Attended or
unattended operation? (3/5)**

Will somebody be helping users?



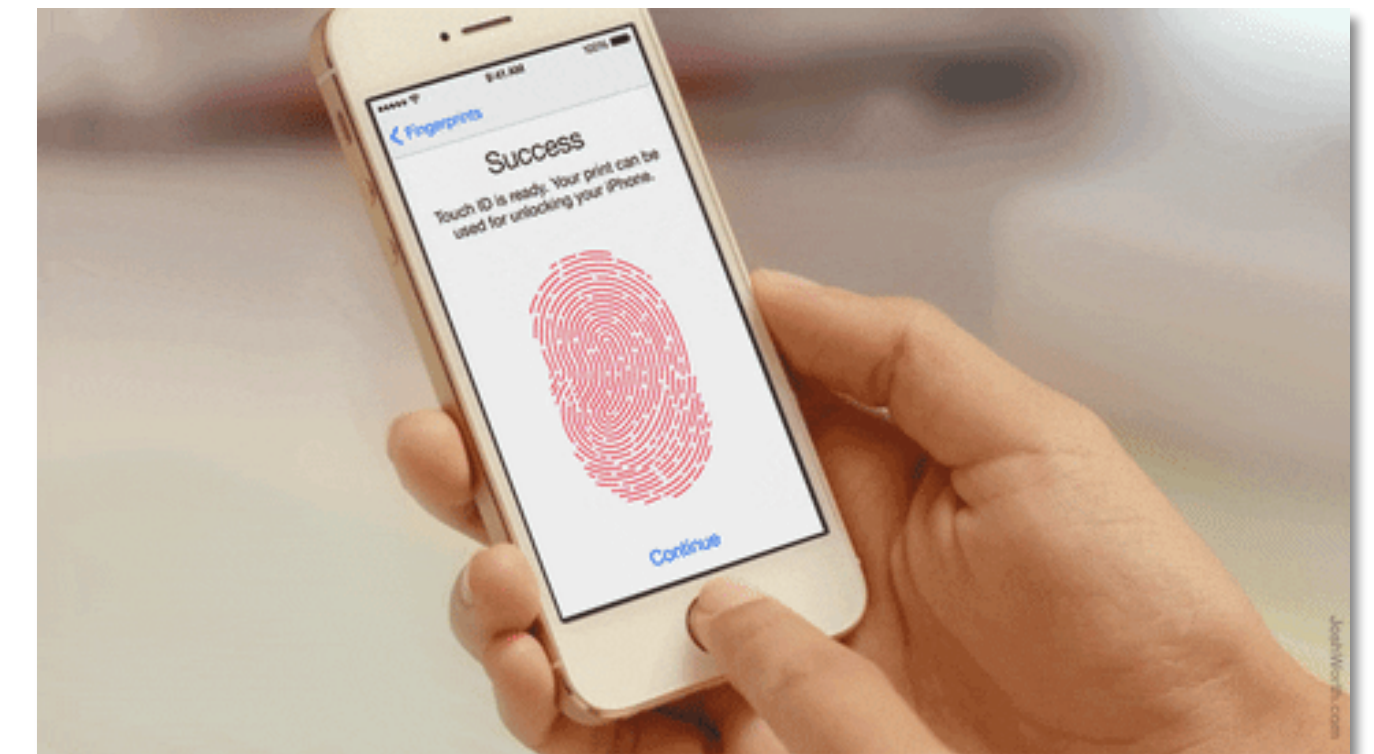
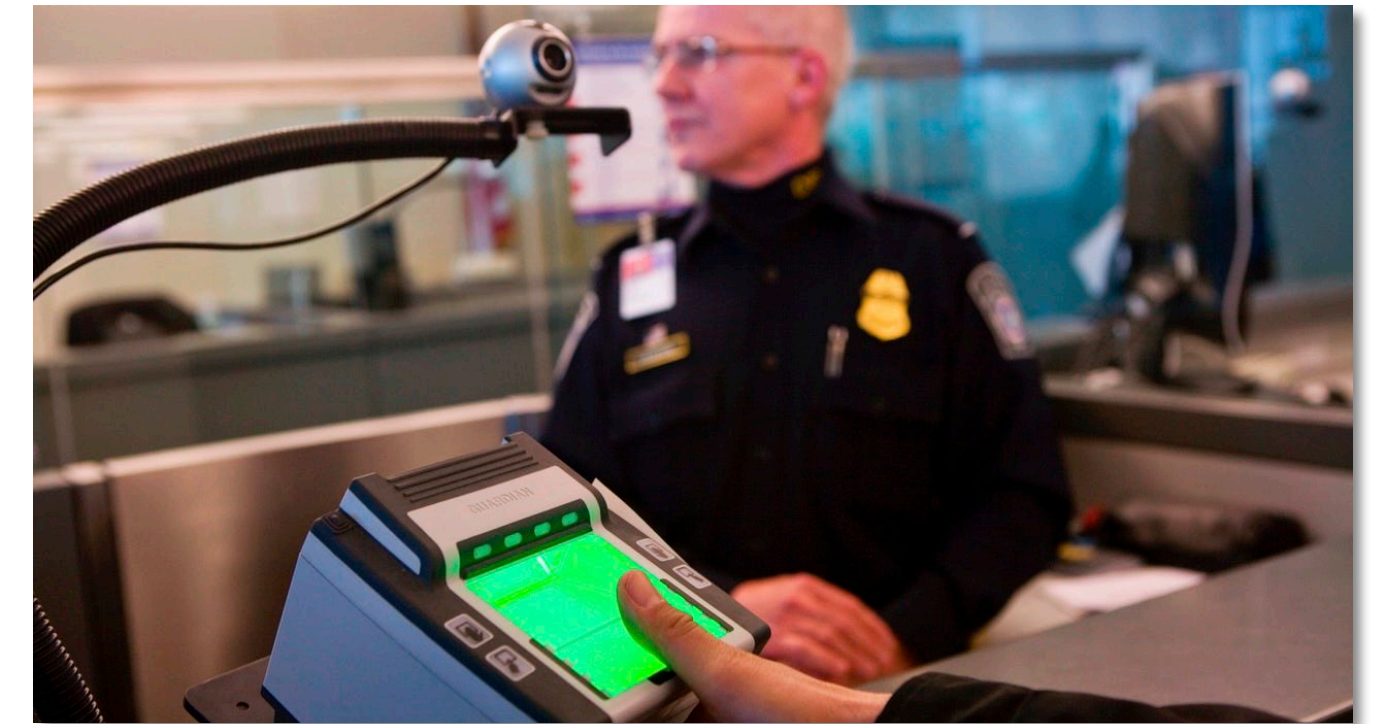
Biometric Systems

What do we want to consider?

Things to consider when designing a Biometrics system, besides trait.

Controlled or uncontrolled environment? (4/5)

How do the environmental conditions change?
(temperature, illumination, etc.)



Biometric Systems

What do we want to consider?

Things to consider when designing a Biometrics system, besides trait.

What are the computational requirements? (5/5)

Consider memory footprint, processing time, response time, and system availability.



Biometric Systems

What do we want to avoid?

✗ Covert deployment

Users must be aware of the Biometric system collecting their data.
Respect their privacy.



✗ No data confidentiality

Collected data must be confidential. Avoid function creep.

✗ Unsafe system

We will get to know threats (attacks) that may harm a system's integrity.

Biometric System Errors

Denial of Access (1/3)

Verification

Jane Doe: Here, I'm Jane Doe.

System: No, you're not.

Identification

Jane Doe: Here, my fingerprints.

System: I don't know you.



Biometric System Errors

Denial of Access (1/3)

Possible Causes

Intrinsic failure: intra-user trait variation, due to different sensors, hardware malfunction, pose, illumination, make-up, aging, illness, cosmetic surgeries, etc.

Adversarial attack: malicious alteration of template database, etc.

Biometric System Errors

Intrusion (2/3)

Verification

Jane Doe: Here, I'm Jane Fonda.

System: Welcome, Jane Fonda!

Identification

Jane Doe: Here, my fingerprints.

System: Welcome, Jane Fonda!



<https://www.wired.com/story/10-year-old-face-id-unlocks-mothers-iphone-x/>

Biometric System Errors

Intrusion (2/3)

Possible Causes

Intrinsic failure: inter-user high similarity, due to low trait uniqueness, poor trait capture, etc.

Adversarial attack: impersonation, spoofing, etc.



impersonation



spoofing

Biometric System Errors

Repudiation (3/3)

Verification

Jane Doe: See, I'm not Jane Doe.

System: Yeah, you're right.

Identification

Jane Doe: Here, my fingerprints.

System: Yeah, I don't know you.



Biometric System Errors

Repudiation (3/3)

Possible Causes

Intrinsic failure: hardware malfunction, intra-user trait variation.

Adversarial attack: obfuscation.



obfuscation

Biometric System Errors

Math Model

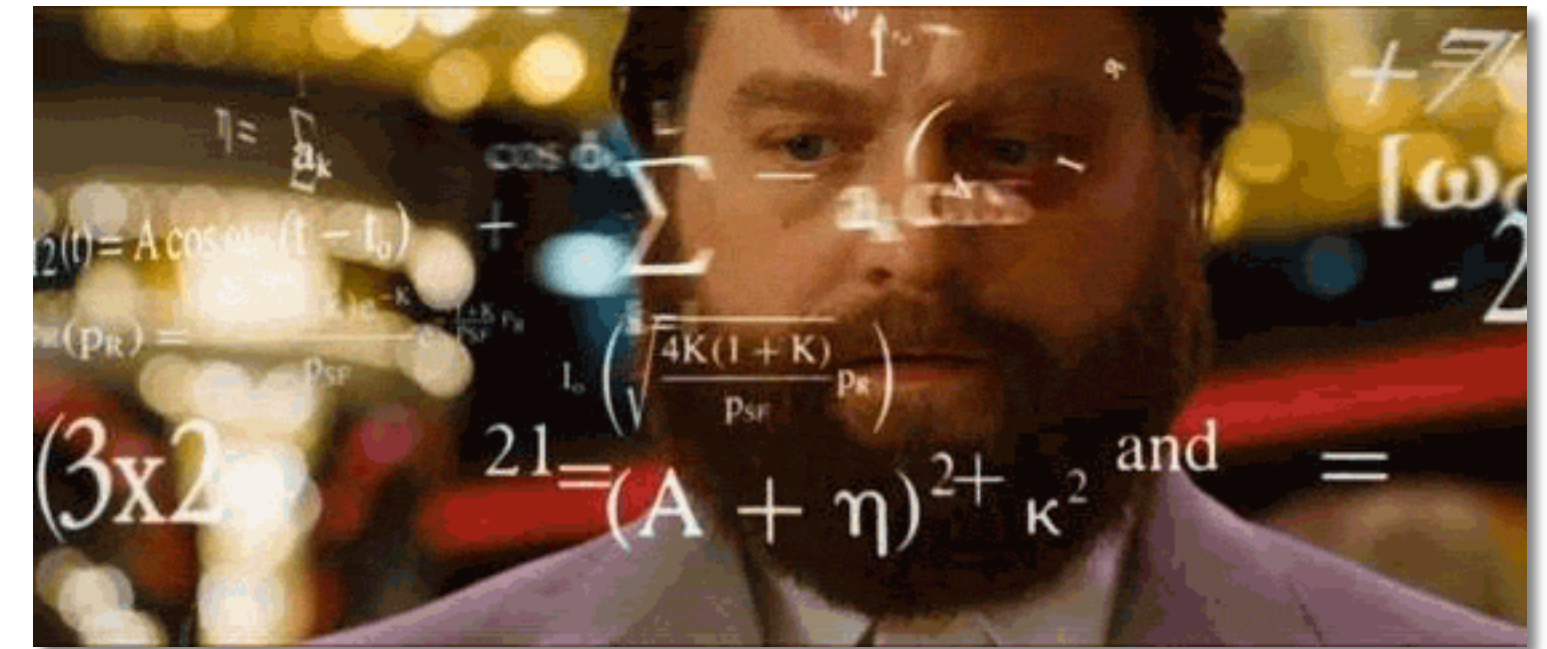
Objective definition of 2 events:

1. False Non-Match (FNM)

A comparison of two features of the same individual should lead to a match, but it led to a non-match.
It causes either a denial of access or helps repudiation.

2. False Match (FM)

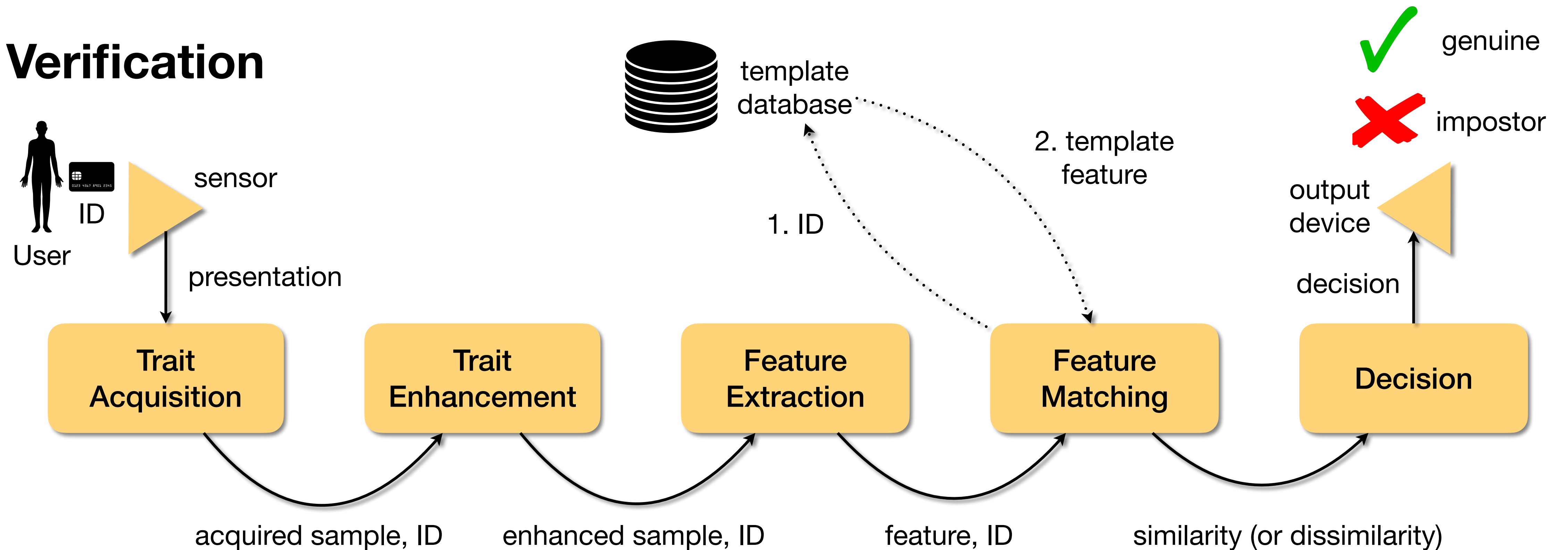
A comparison of two features from different individuals should lead to a non-match, but it led to a match.
It helps an intrusion.



Let's see how to compute them!

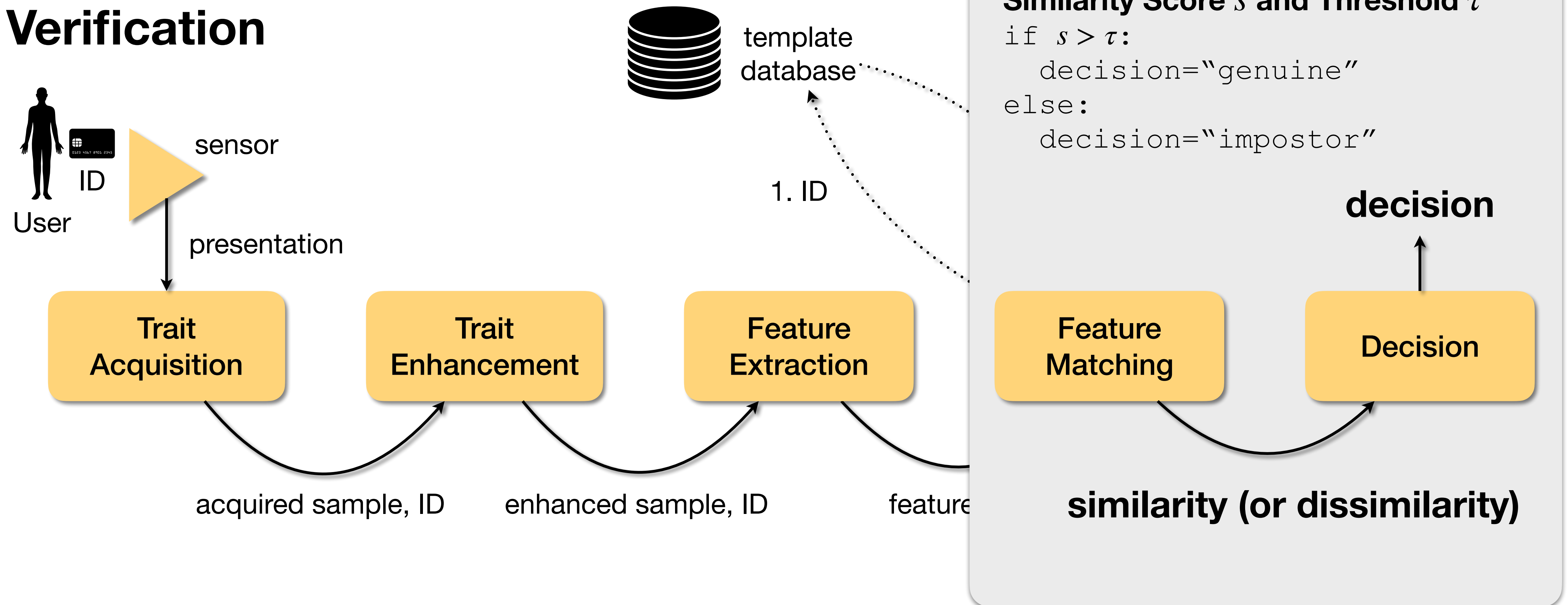
Metrics

Verification



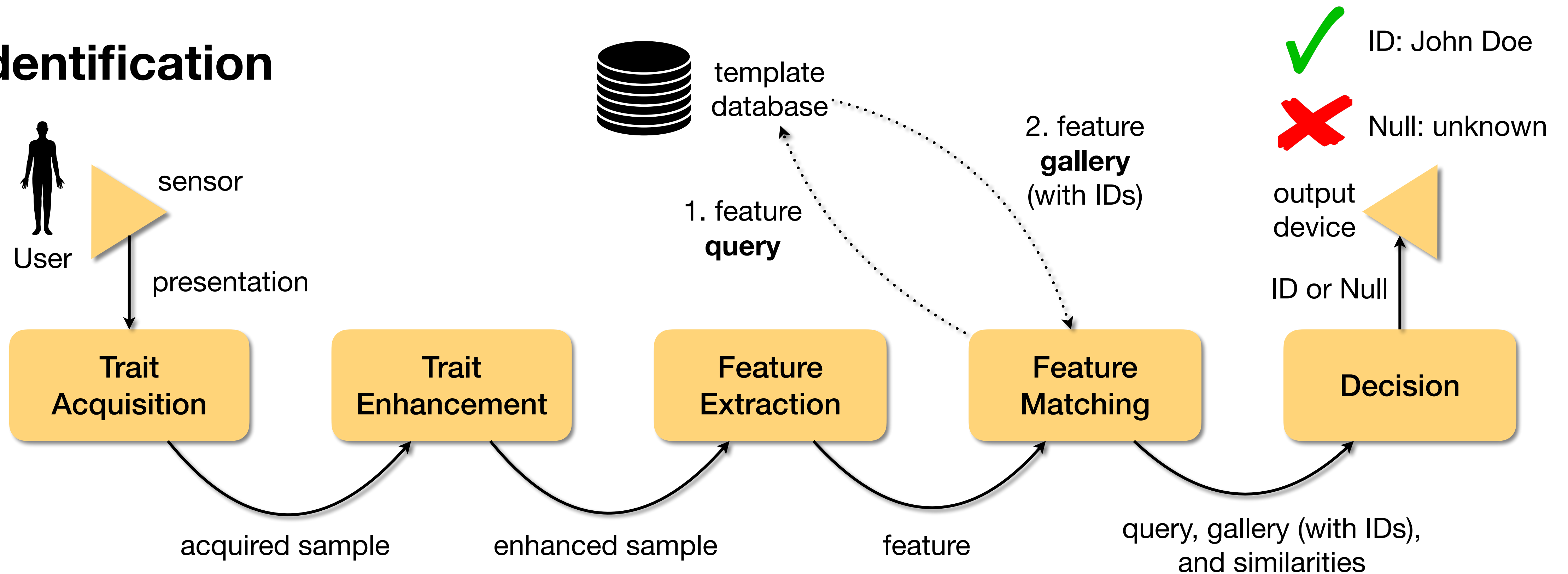
Metrics

Verification



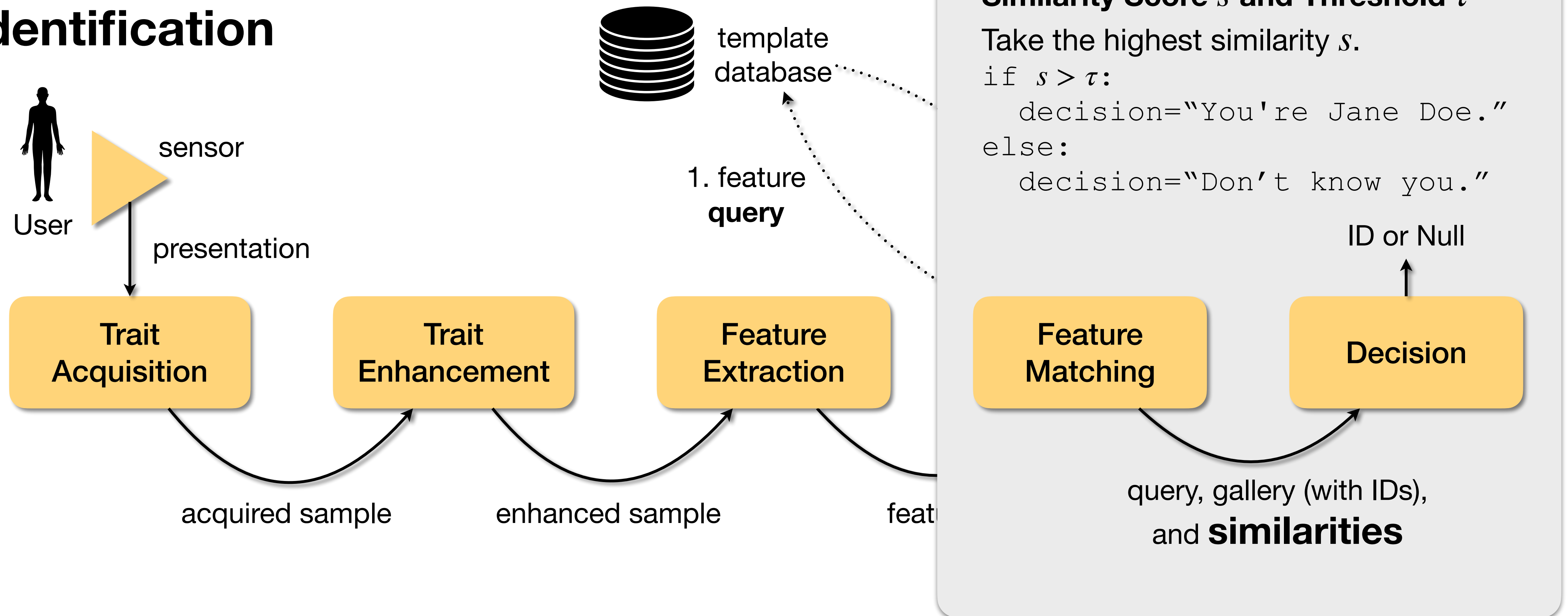
Metrics

Identification

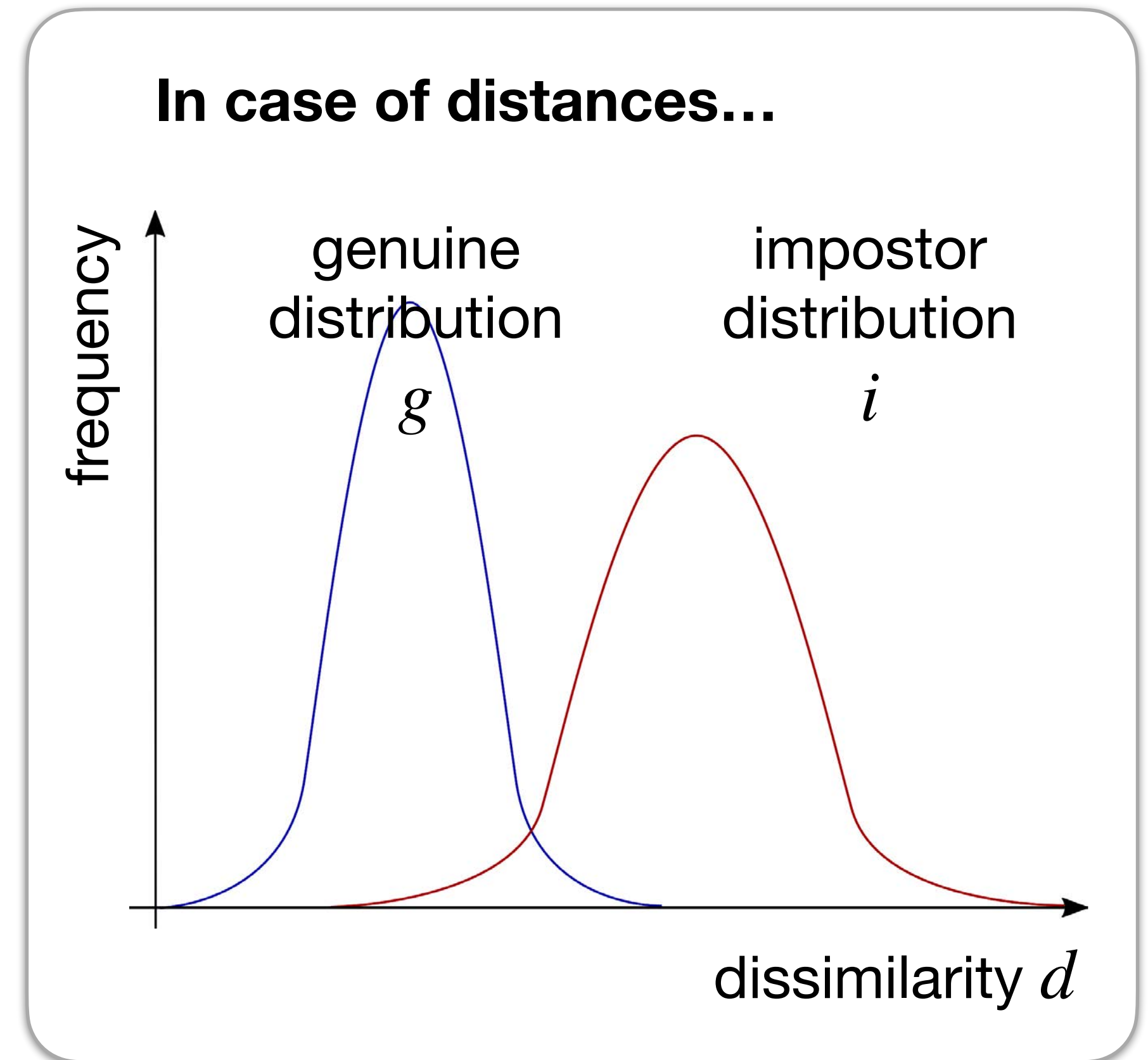
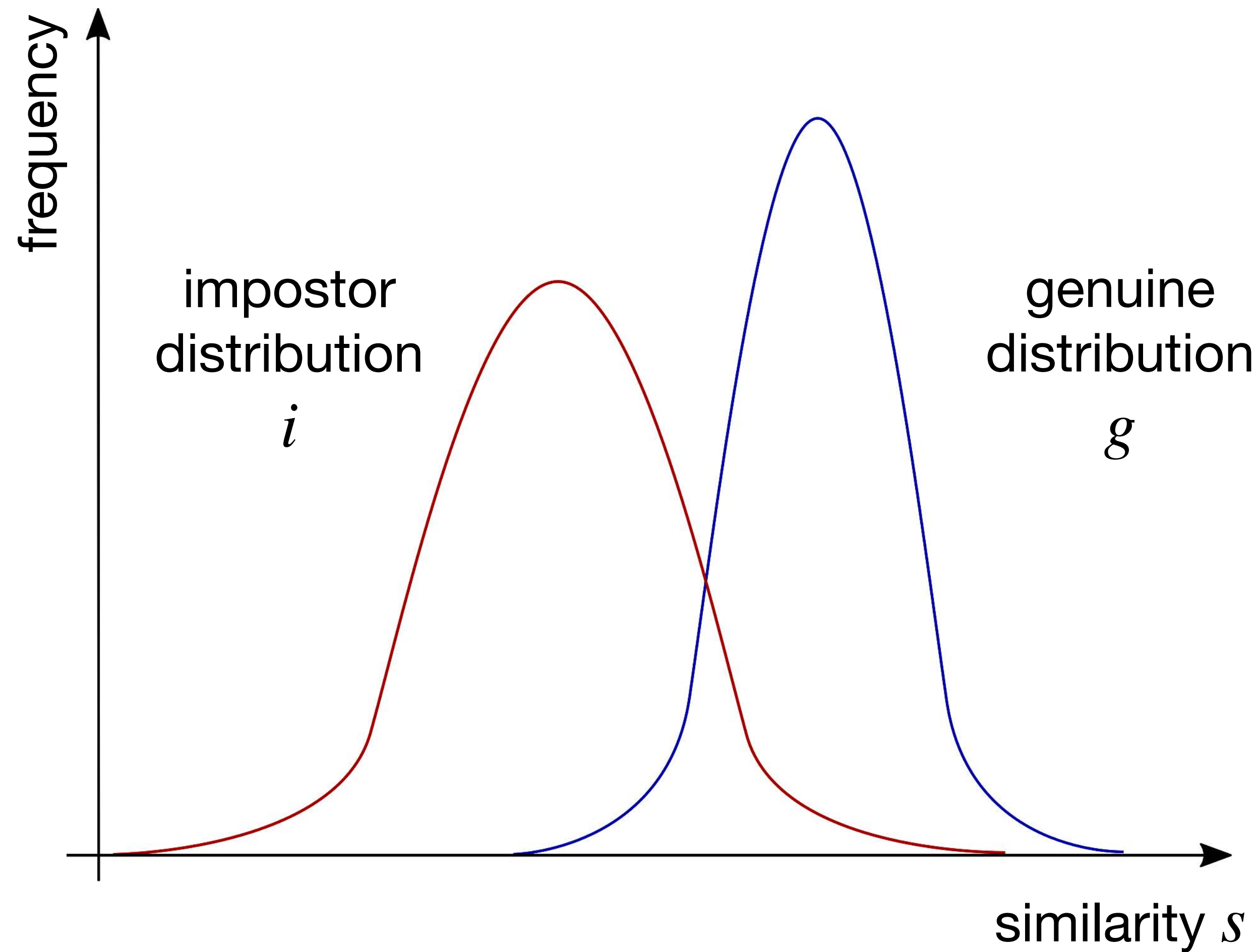


Metrics

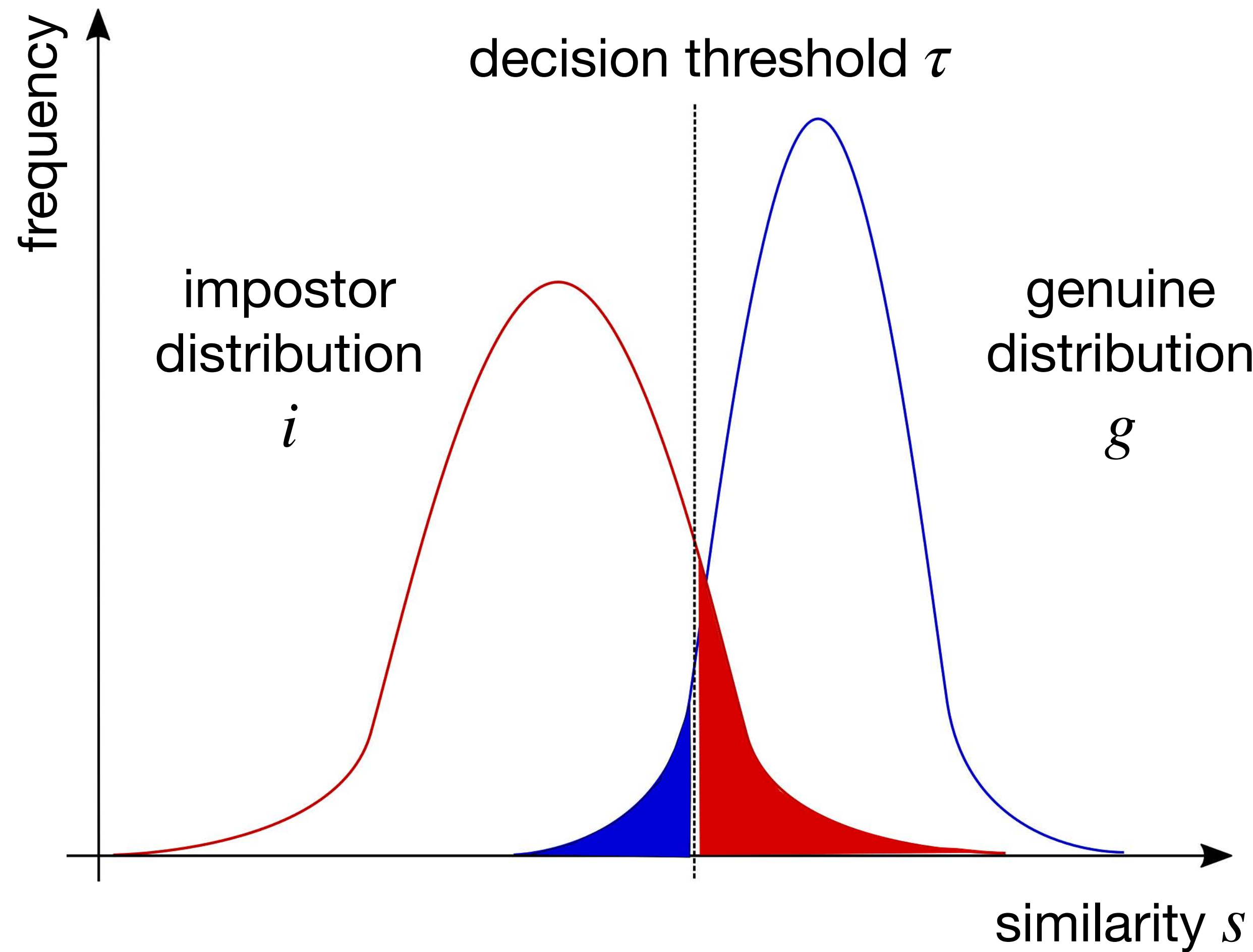
Identification




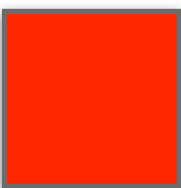
Metrics



Metrics



 $FNM(\tau) = \int_{-\infty}^{\tau} g(s) \, ds$

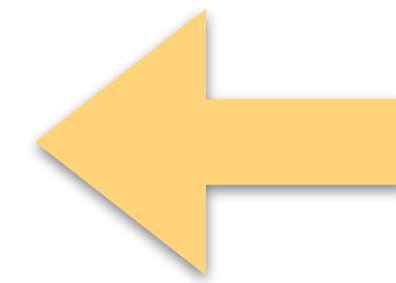
 $FM(\tau) = \int_{\tau}^{\infty} i(s) \, ds$

Metrics

In Practice

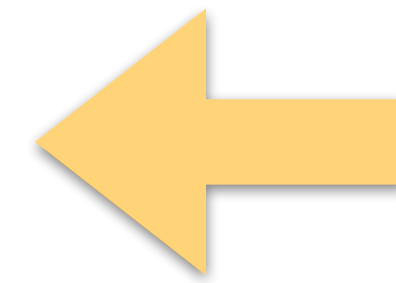
False Non-Match Rate (FNMR) and False Match Rate (FMR)

$$FNMR(\tau) = \frac{\#(\text{false nonmatches for } \tau)}{\#(\text{genuine comparisons})}$$



$$\blacksquare FNM(\tau) = \int_{-\infty}^{\tau} g(s) \, ds$$

$$FMR(\tau) = \frac{\#(\text{false matches for } \tau)}{\#(\text{impostor comparisons})}$$



$$\blacksquare FM(\tau) = \int_{\tau}^{\infty} i(s) \, ds$$

Metrics

In Practice

False Non-Match Rate (FNMR) and False Match Rate (FMR)

$$FNMR(\tau) = \frac{\#(\text{false nonmatches for } \tau)}{\#(\text{genuine comparisons})}$$

How many of the genuine comparisons are wrongly computed by the system?

$$FMR(\tau) = \frac{\#(\text{false matches for } \tau)}{\#(\text{impostor comparisons})}$$

How many of the impostor comparisons are wrongly computed by the system?

Metrics

In Practice

Interpretation of *R values.

Suppose a face recognition system with FMR=0.1%

FMR=0.001, one error in every 1K comparisons.

Is it good?



Suppose the Newark airport

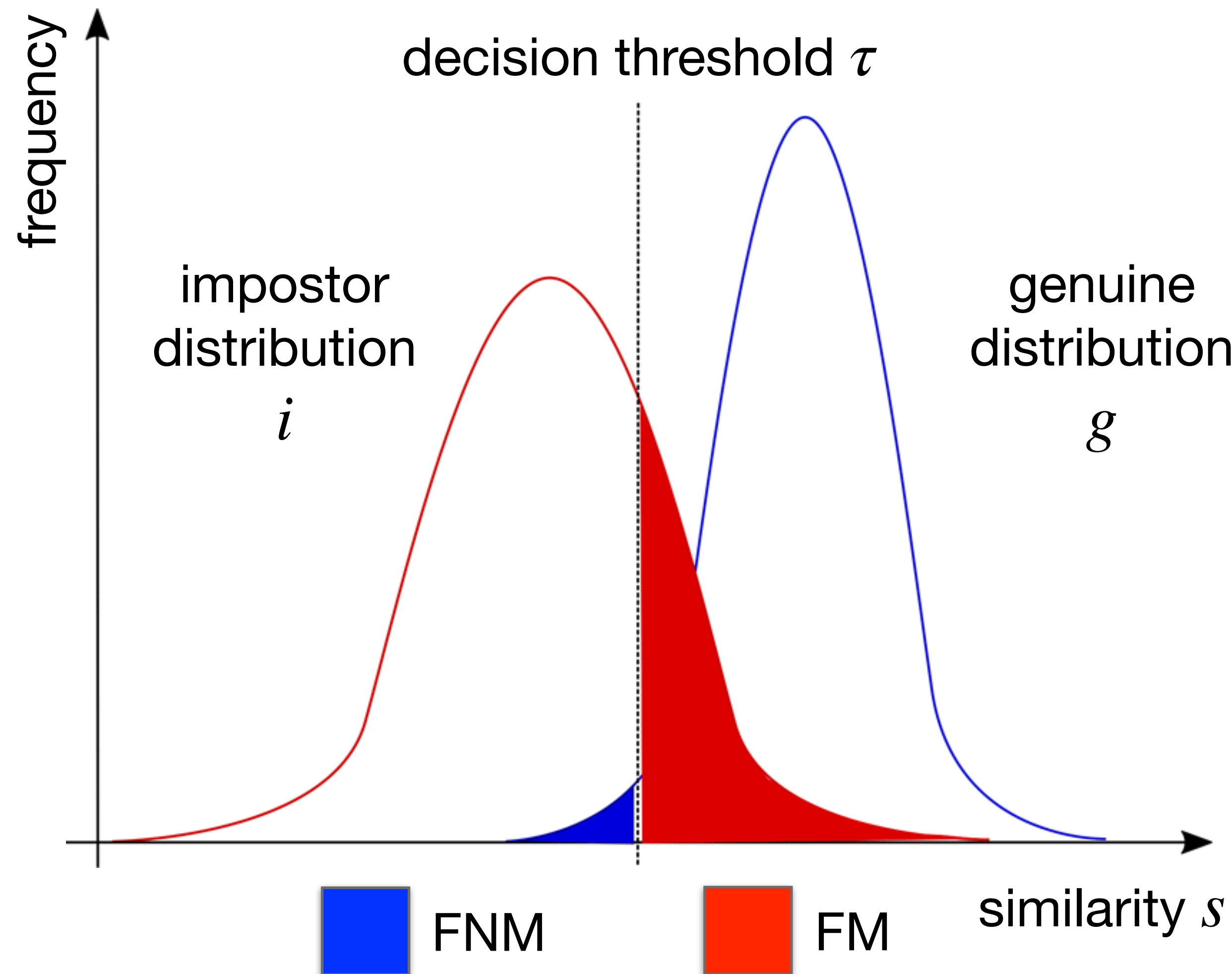
5K people per hour, 14h per day (70K people per day)

Suppose a suspect watch list with 100K people: 7 billion comparisons per day.

Average number of false matches per day: 7 million people to double check every day.

Terrorist watch list in 2016: 1,8 million people

Metrics



What is the impact of changing the decision threshold?

The larger the value of τ :
The larger the value of FNM;
The smaller the value of FM.

FNM and FM are inversely proportional.

Metrics

What to choose?

Small FNMR

Suitable to avoid denial of access and repudiation.

Increases intrusion probability, though.

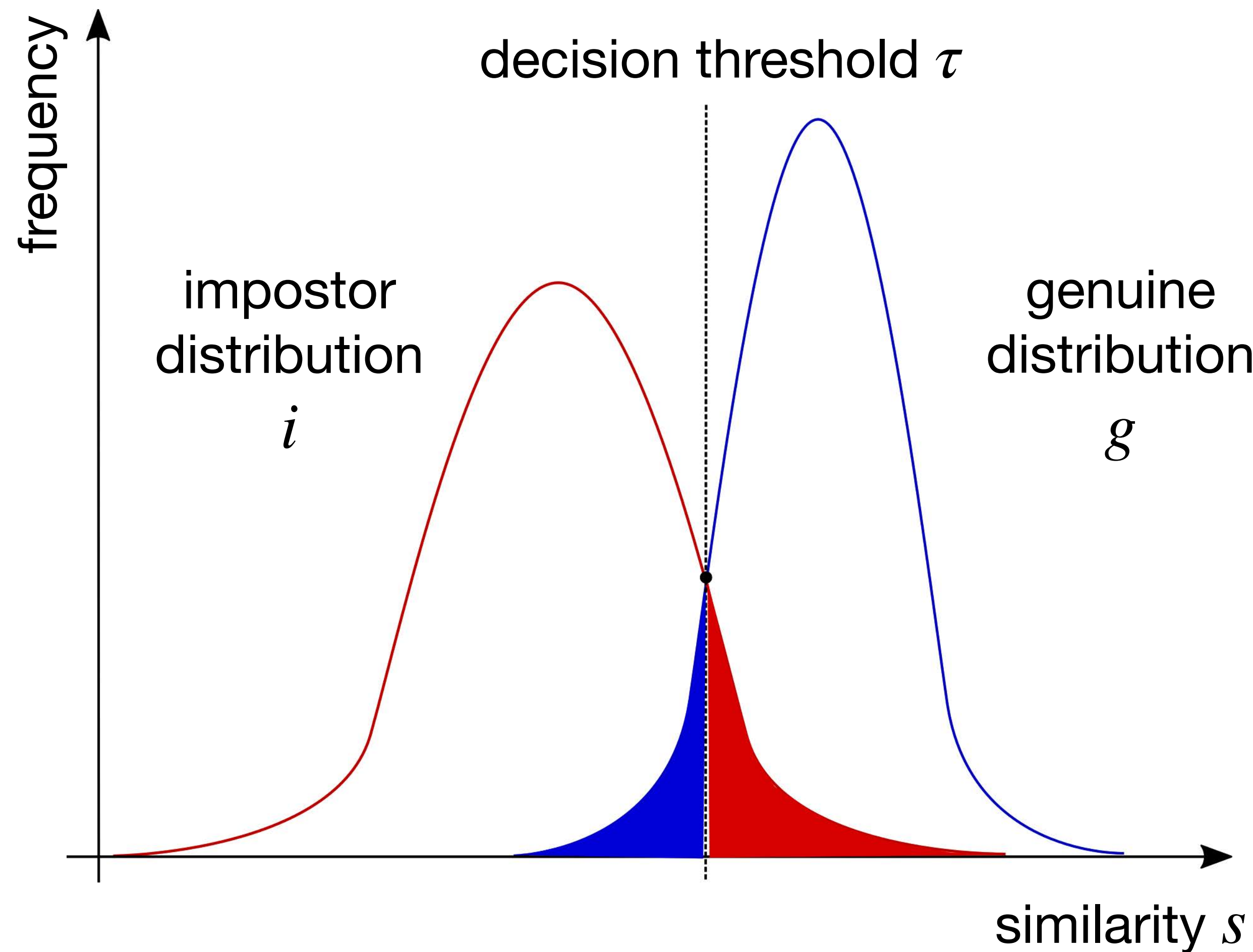
Small FMR

Suitable to avoid intrusion.

Increases denial of service and repudiation probability, though.



Metrics



What to choose?

Equal Error Rate (EER)

Common practice.

Pick the threshold where
 $\text{FNMR} = \text{FMR}$.

Metrics

How to compare two different systems?

Biometric systems *A* and *B*.

**Compare both systems' FNMR and FMR
at EER (1/3)**

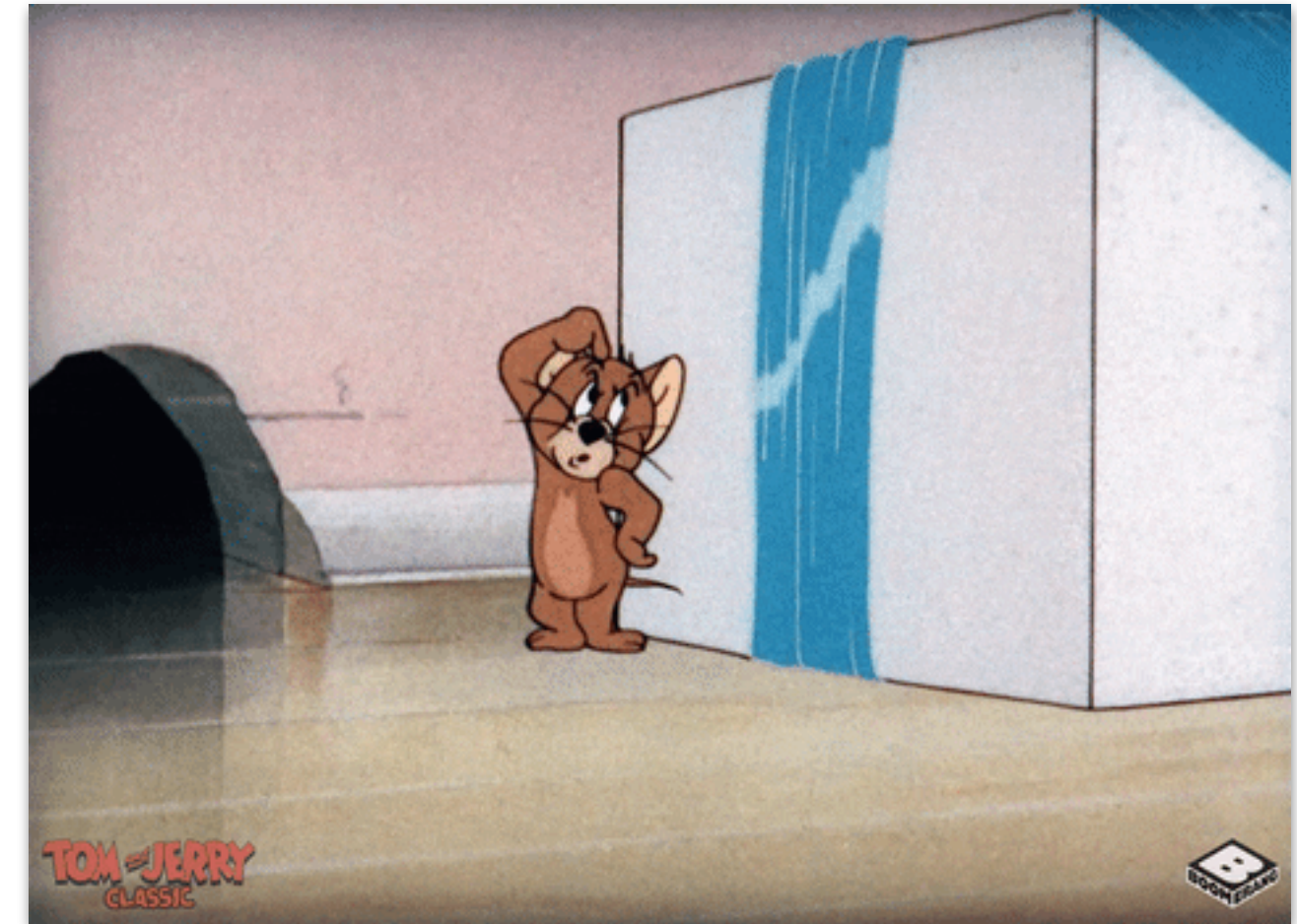
Take the one with smaller FNMR and FMR values.



Metrics

How to compare two different systems?
Biometric systems *A* and *B*.

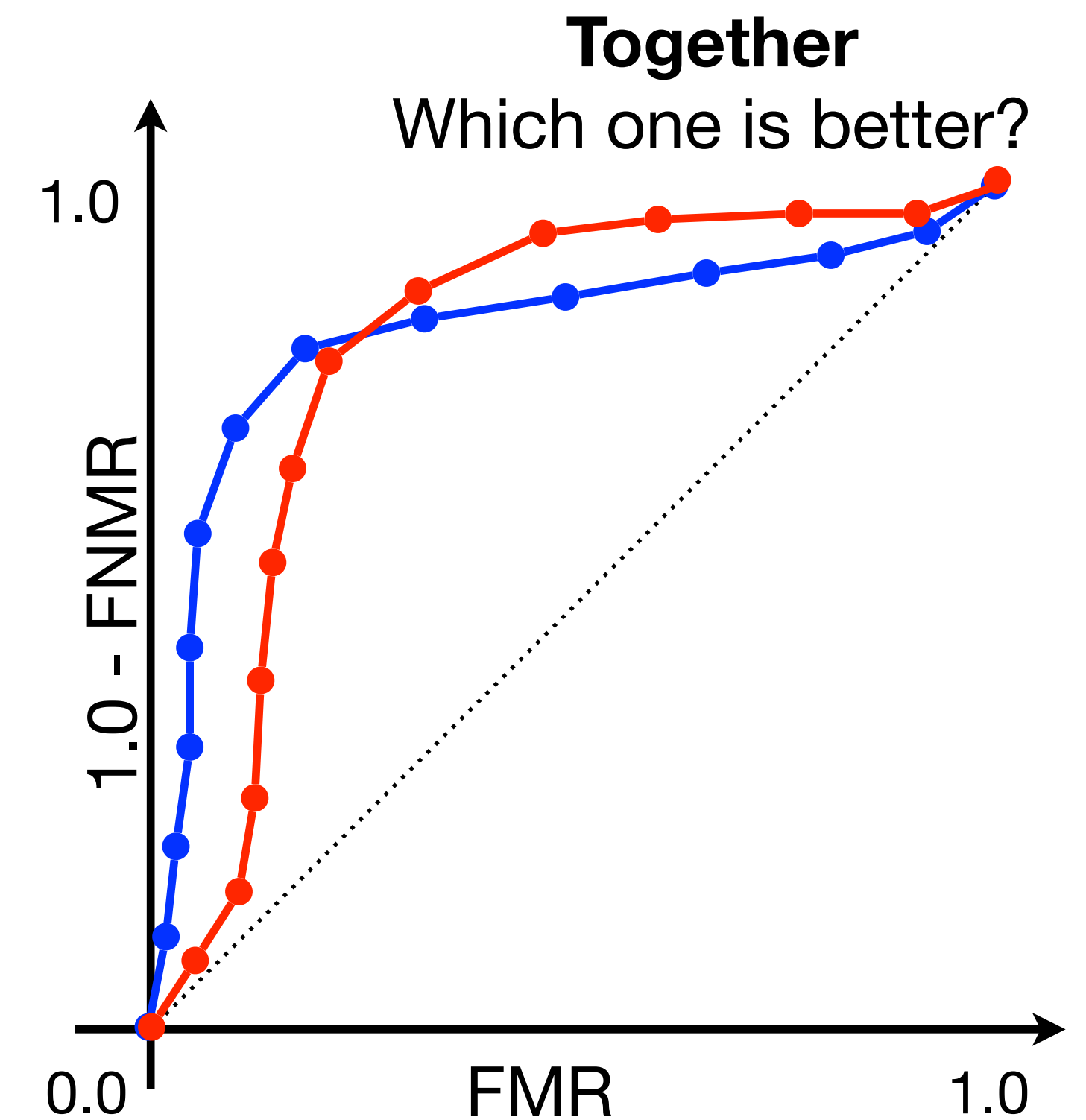
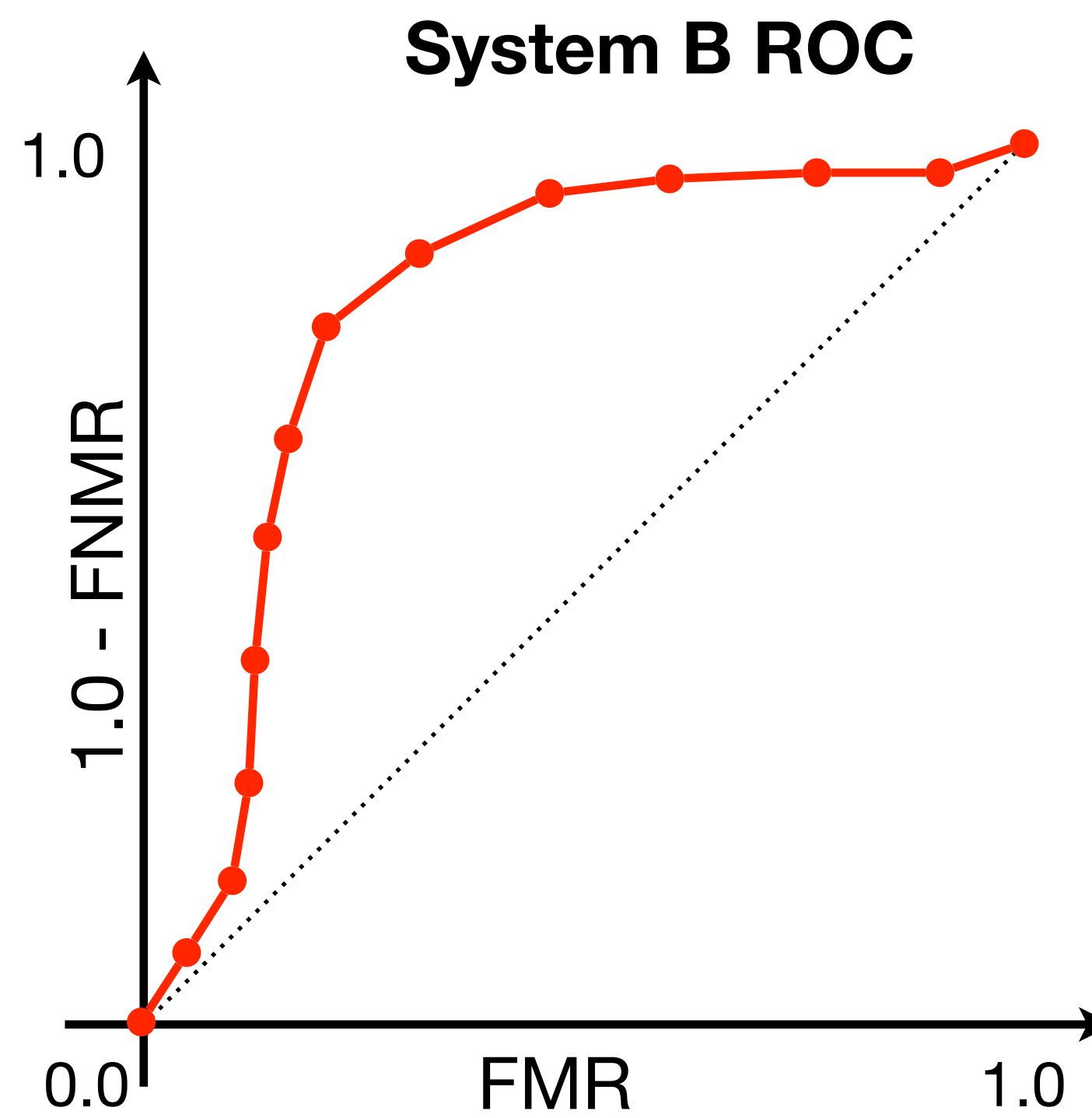
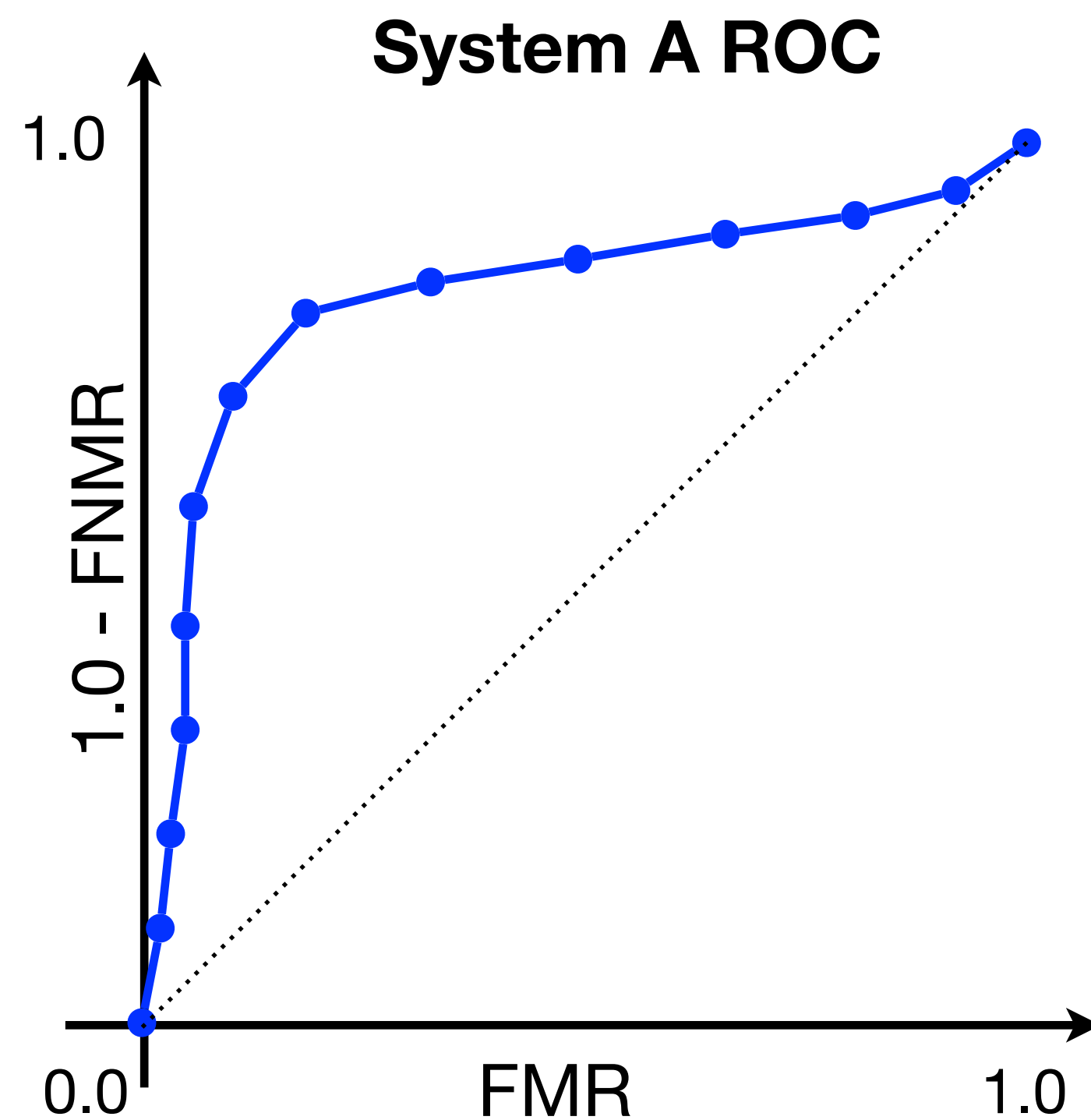
Use a Receiver Operating Characteristic (ROC) curve (2/3)



Metrics

How to compare two different systems?
Biometric systems *A* and *B*.

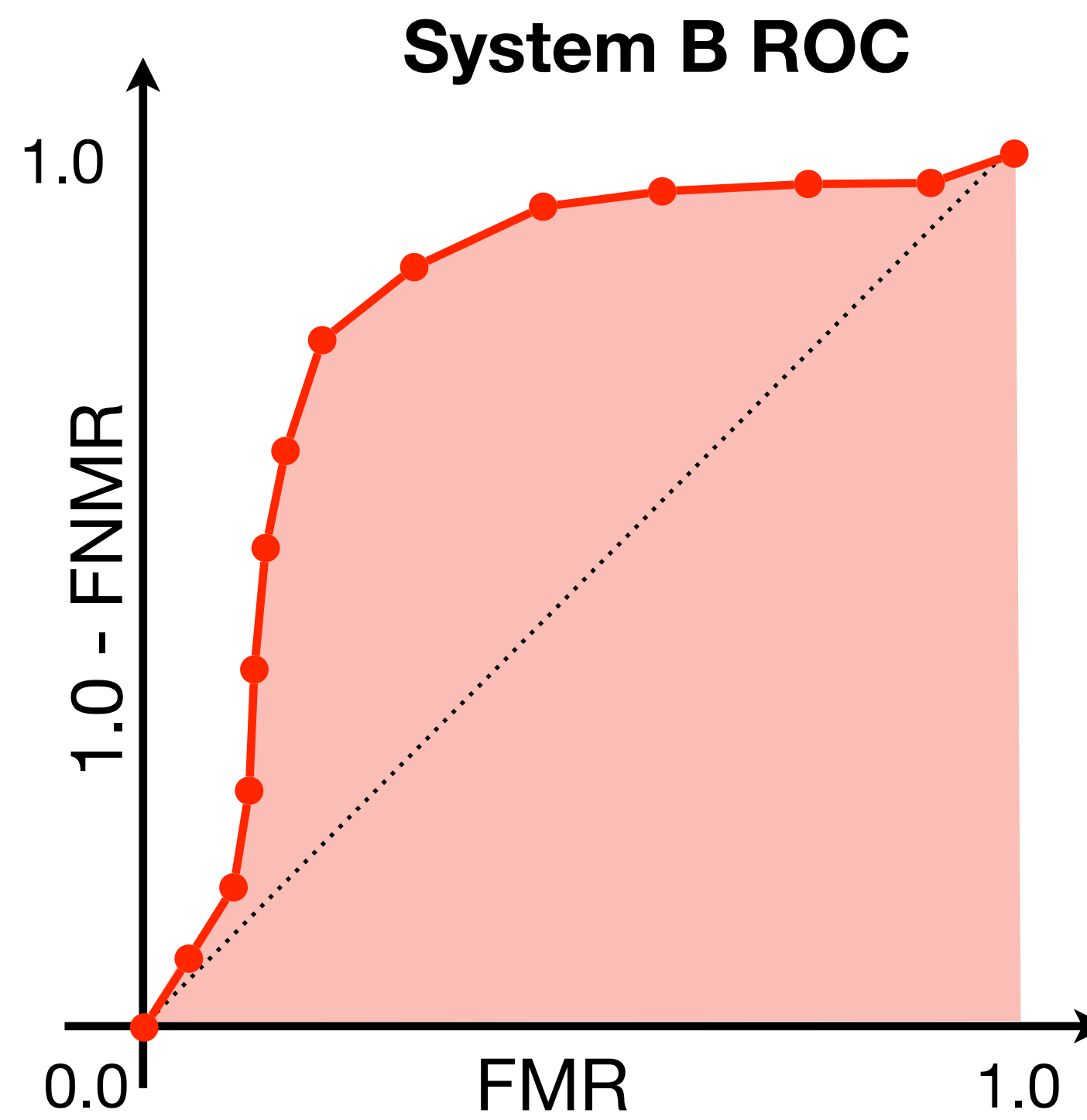
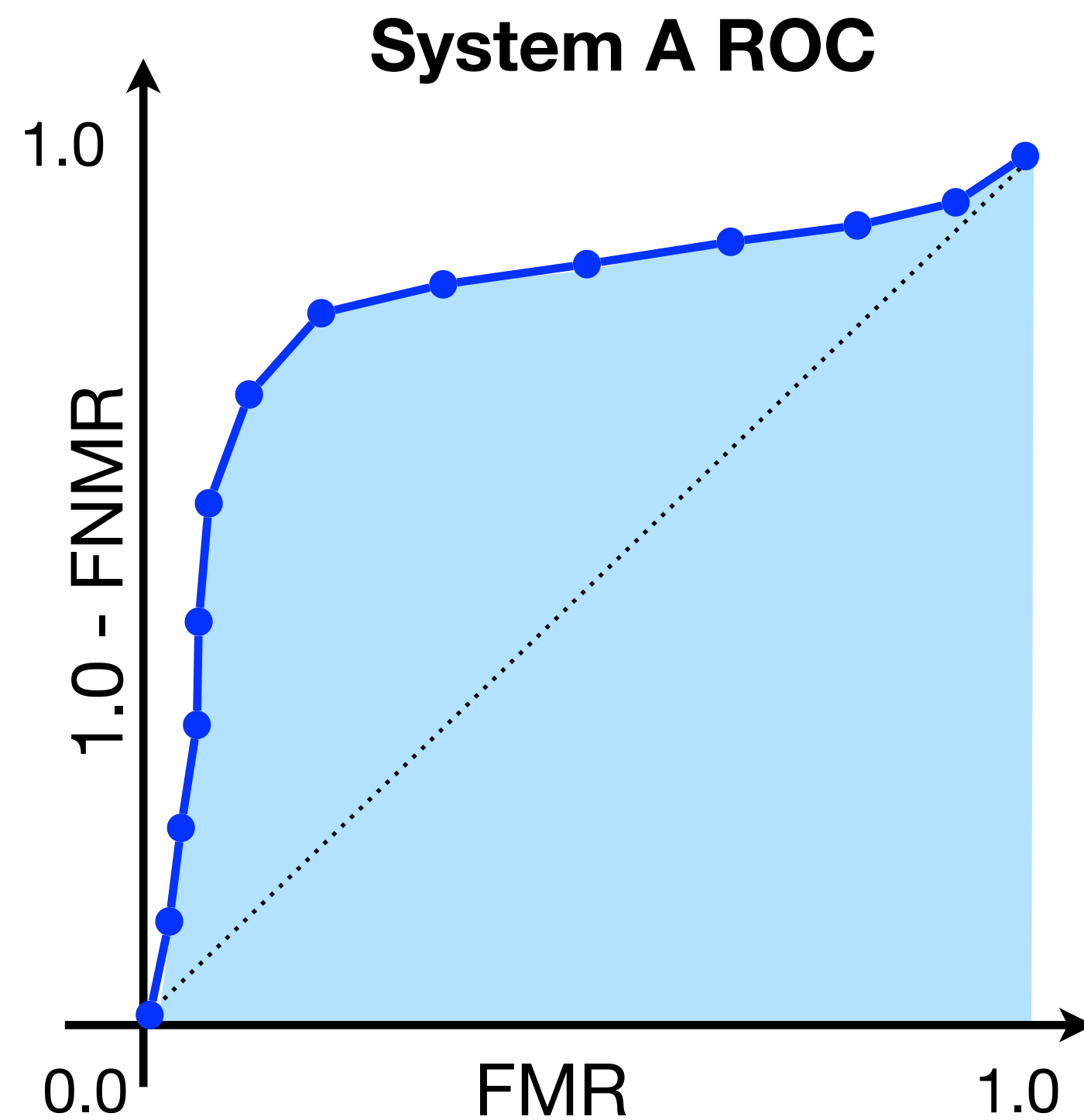
Compute FMR and FNMR for a variety of thresholds.



Metrics

How to compare two different systems?

Biometric systems *A* and *B*.



Which one is better?

Compute the Area Under The Curve (AUC).

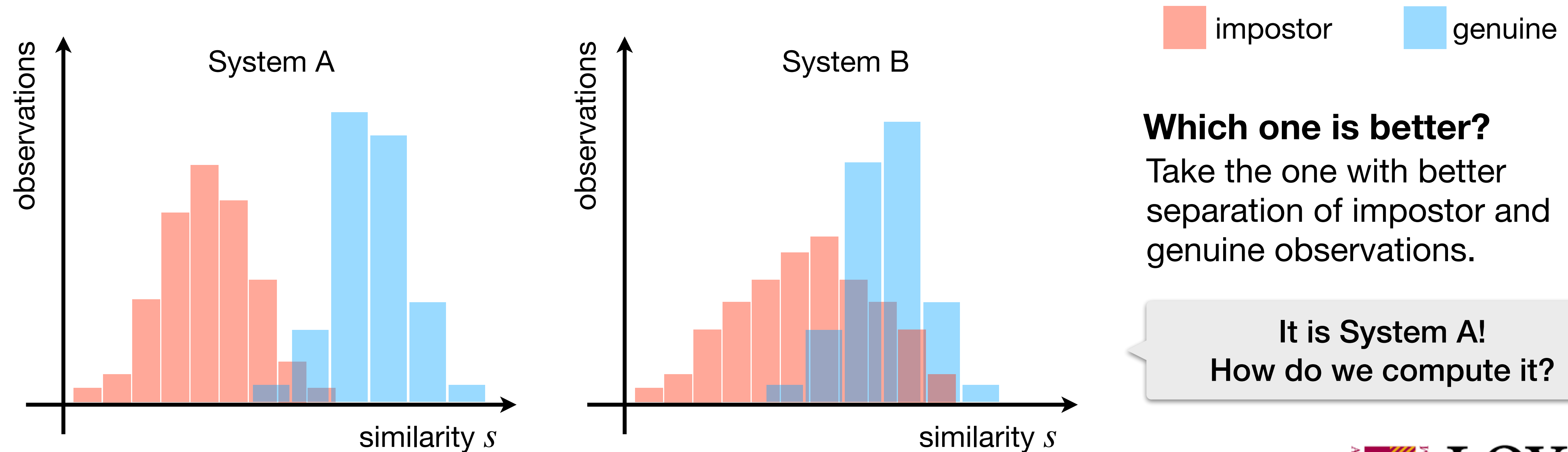
The best solution presents larger AUC.

Metrics

How to compare two different systems?

Biometric systems A and B .

Compute the difference between impostor and genuine distributions for each system (3/3)



Metrics

How to compare two different systems?

Biometric systems A and B .

Compute the difference between impostor and genuine distributions for each system (3/3)

Which one is better?

Take the system with larger **d-prime**:

$$d' = \frac{\sqrt{2} \times |\mu_{\text{genuine}} - \mu_{\text{impostor}}|}{\sqrt{\sigma_{\text{genuine}}^2 + \sigma_{\text{impostor}}^2}}$$

Hypothesis: the distributions are Gaussians
(with mean μ and standard deviation σ).

The larger the separation between the distributions,
the larger the value of d-prime.

Metrics

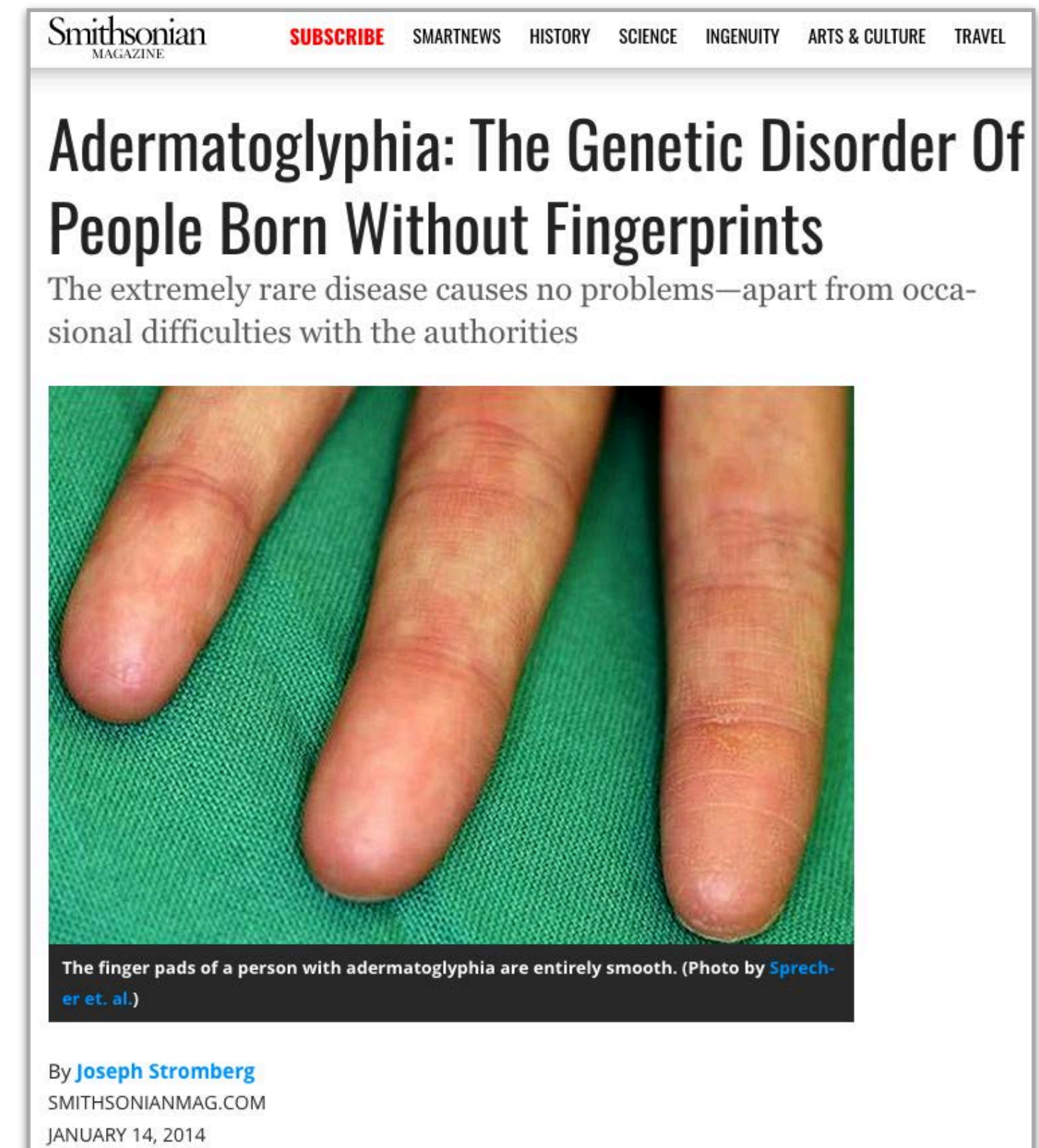
Other Metrics (1/4, 2/4)

Failure to Acquire (FTA)

Rate of falsely rejected biometric samples due to problems in acquisition.

Failure to Enroll (FTE)

The same as FTA, but during enrollment.



<https://www.smithsonianmag.com/science-nature/adermatoglyphia-genetic-disorder-people-born-without-fingerprints-180949338/>

Metrics

Other Metrics (3/4, 4/4)

Positive Metrics

True Non-Match Rate (TNMR)

$$\text{TNMR} = 1.0 - \text{FMR}$$

True Match Rate (TMR)

$$\text{TMR} = 1.0 - \text{FNMR}$$

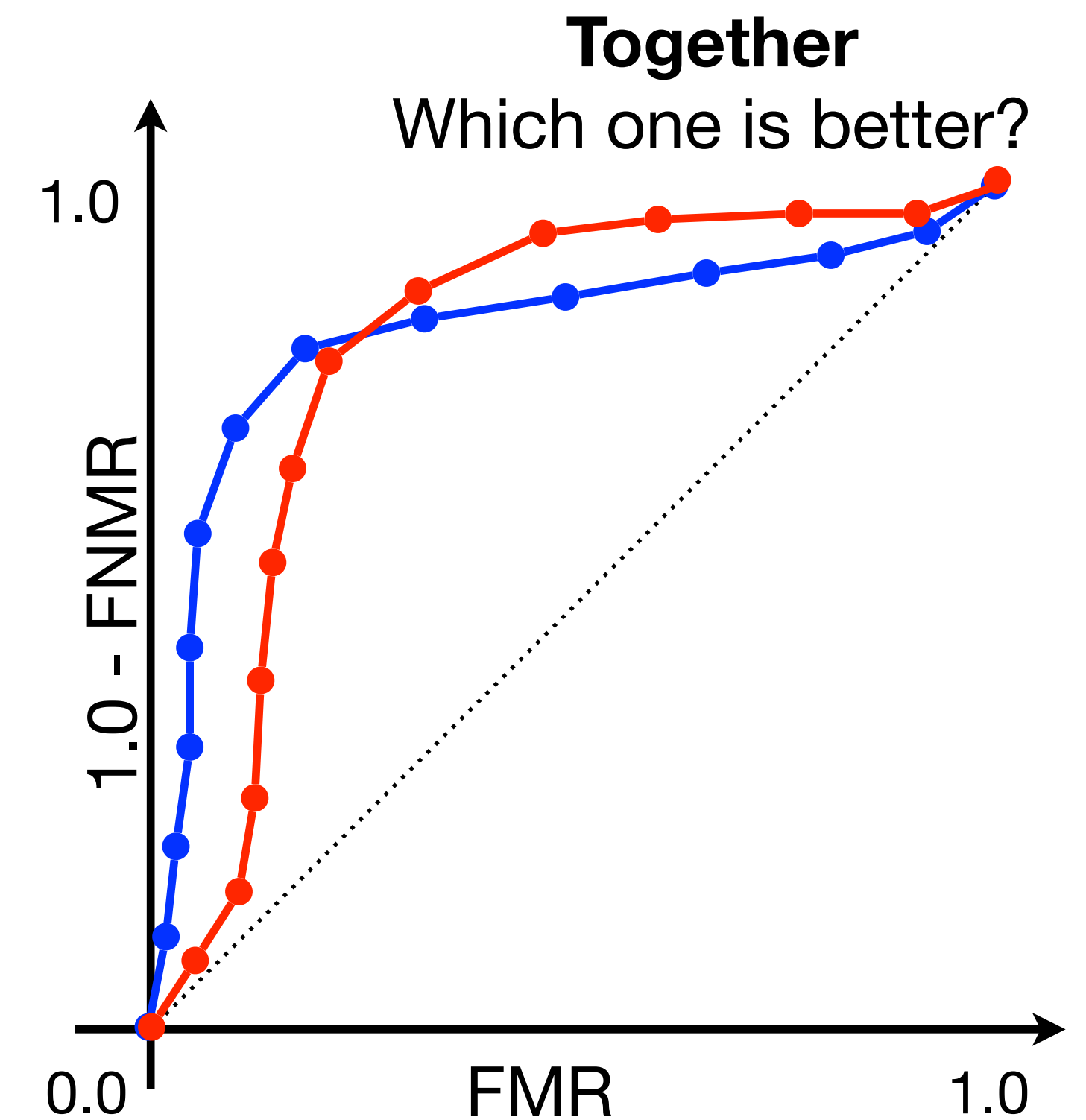
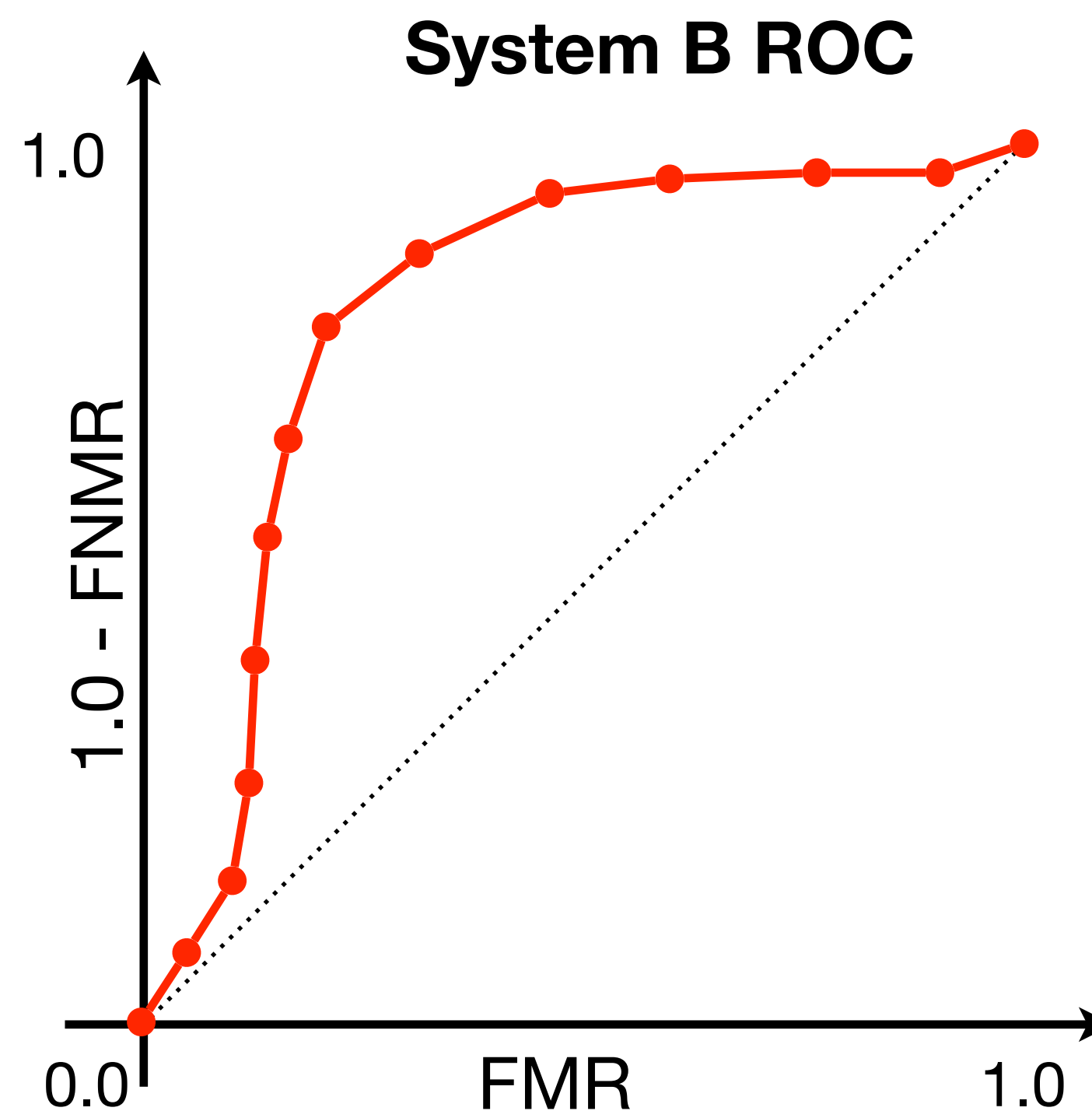
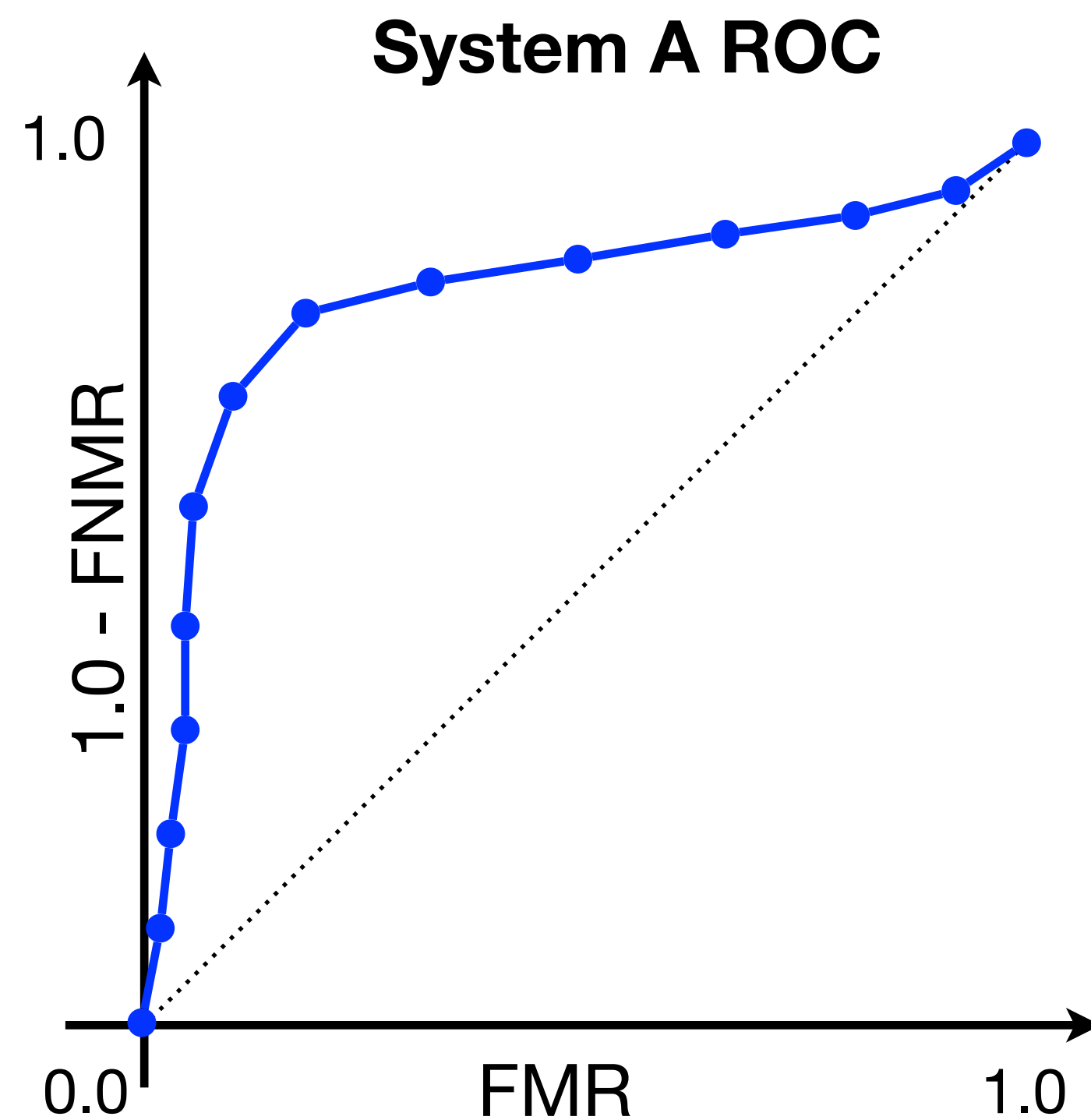
You want to maximize these instead of minimizing.



Metrics

How to compare two different systems?
Biometric systems *A* and *B*.

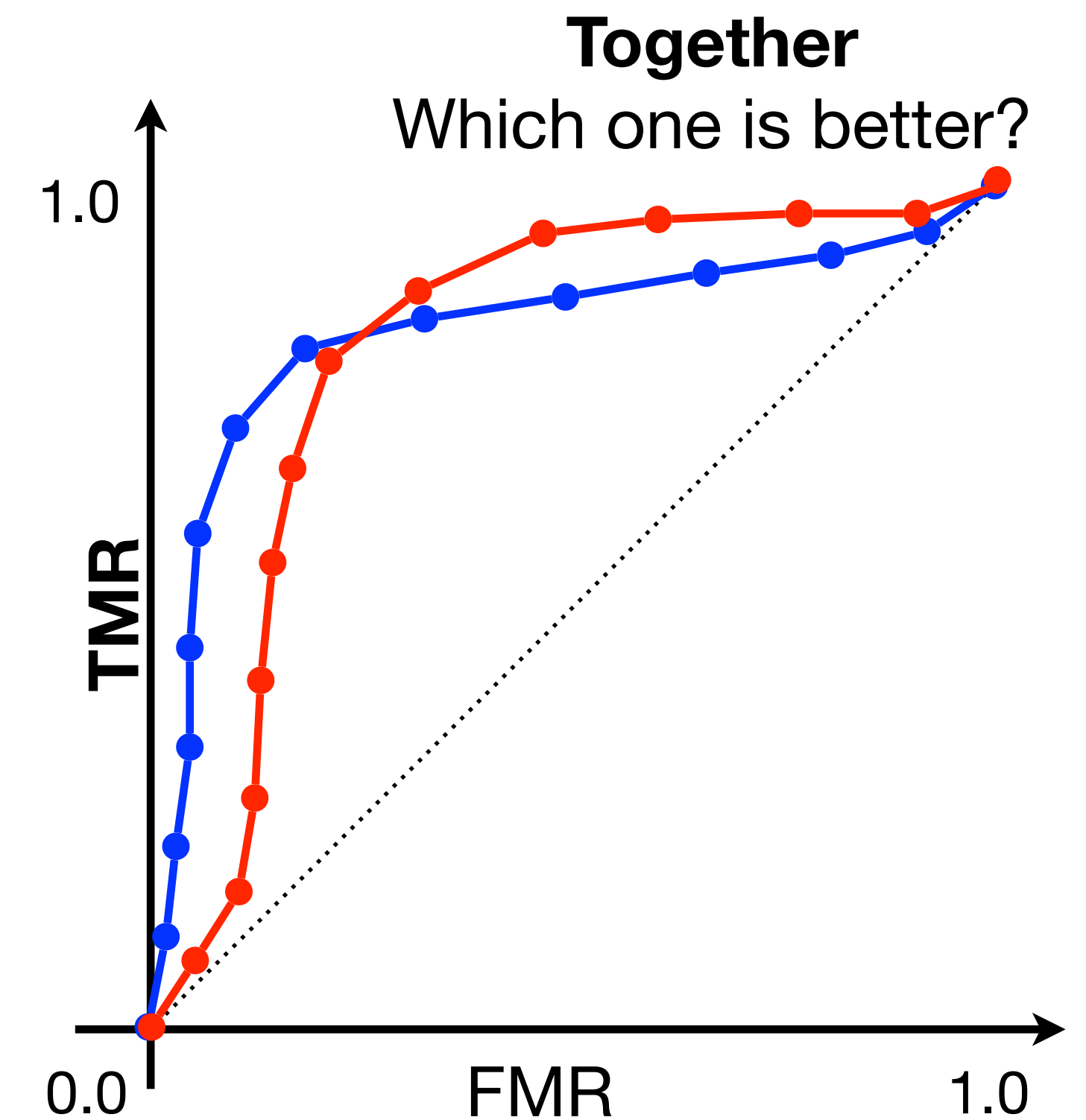
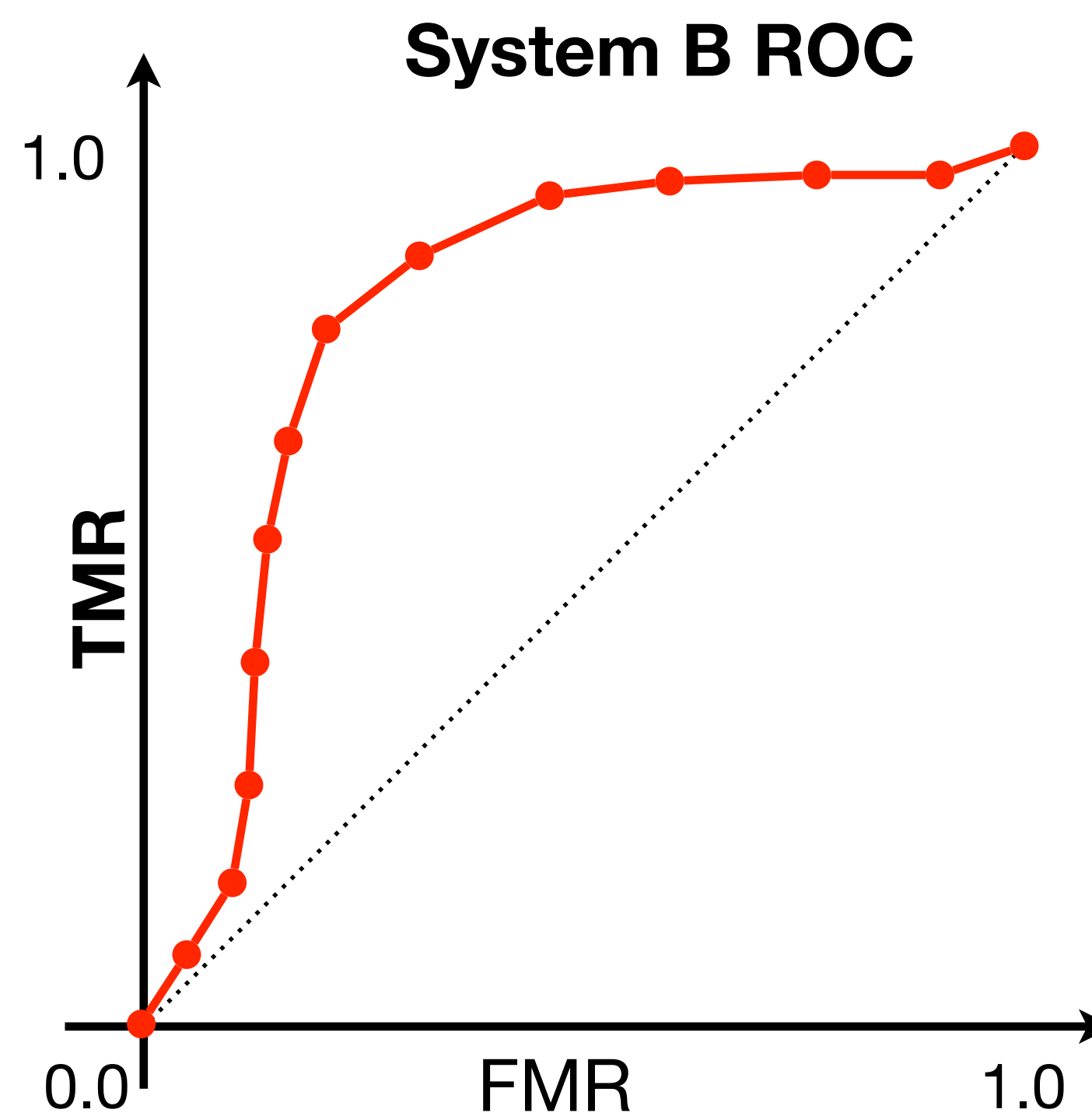
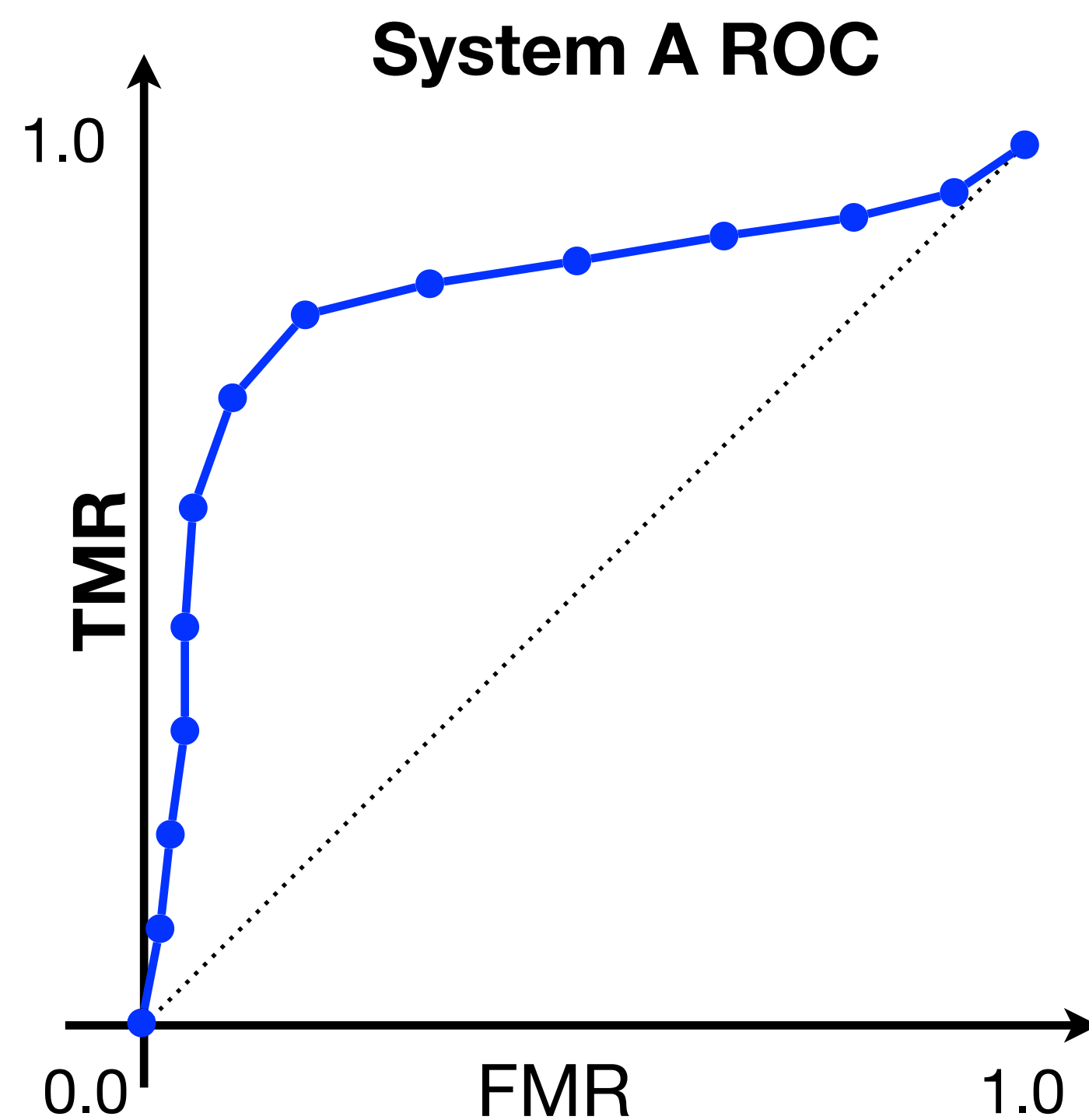
Compute FMR and FNMR for a variety of thresholds.



Metrics

How to compare two different systems?
Biometric systems *A* and *B*.

Compute FMR and FNMR for a variety of thresholds.



What's Next?

First Coding Day

Implementation of metrics.

Bring your computers

Don't have one?

Please let me know ASAP.

Be ready! :)

Tools: Google Colab.

