Questions 2

Difference between qualitative and quantitative identity?

- Qualitative identity: things share properties so that two things can be very similar and more or less the same. An example can be: two cars are the same model, color, and year.
- Quantitative identity: things are the same thing, literally. Absolute and total identity.

What is the fundamental reason for preserving the concept of "identity"?

The concept of "identity" must be preserved primarily because it forms the basis for the notion of "identification," which is not merely abstract but represents a tangible human activity and practice.

What elements characterize recognition?

- Phisical appearance: body height, weight
- Body modification: tatoos, piercings
- Physical object: rings, necklaces
- Mental tokens: poems, musics, memories

Who where the first to introduce the concept of biometrics?

The first were the Egyptians, who used the physical characteristics of the body to identify people and the behavior.

What are anthropometric characteristics?

Anthropometric characteristics are the physical characteristics of the body that are used to identify people. For example:

- Height
- Weight
- Shape of the face
- Shape of the body
- Shape of the hands

Write down some biometric recognition mechanism

- Fingerprint
- Iris

- Voice
- Signature
- Palmprint
- Face
- Gait, the way you walk

What is the definition of Biometrics?

They are the study, design and application of characteristic of the human being given by physiological and behavioral traits. Used for identification, identity verification, authentication, recognition and medical diagnosis.

Difference between identification and verification?

- **Identification**: the process of searching inside a database for a person identity and return as result a biomeric reference for an individual.
- **Verification**: the process of comparing a biometric sample with a claimed identity.

The two phases for biometric **recognition**

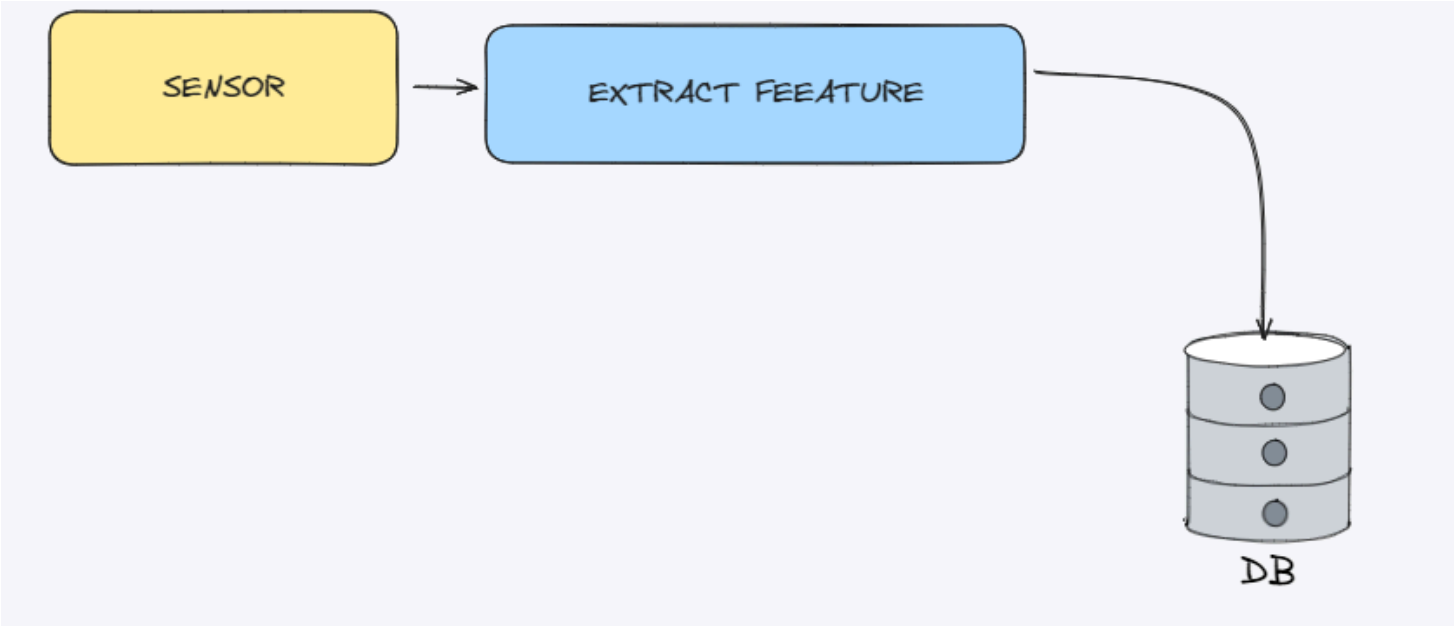
1. Enrollment: Given a person, register this to a databse of biometric references.
2. Recognition: Given a person, automatically recognize this person.

The two operation types of biometric recognition

1. **Verification**: This person is who he claims to be? This is a check 1:1.
2. **Identification**: Who is this person? This is a search 1:N.

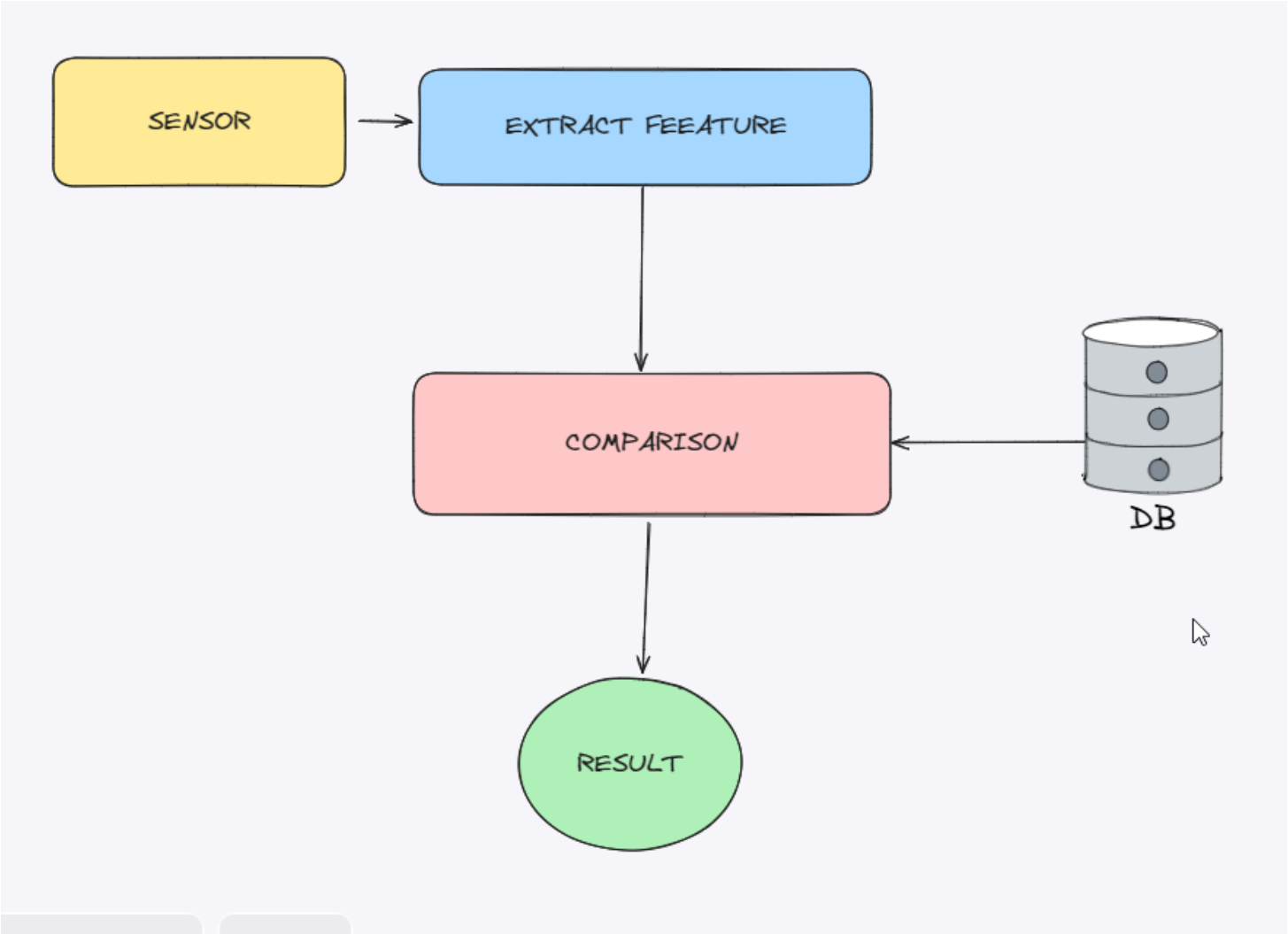
The architecture for biometric recognition - enrollment

1. Take a biometric sensor
2. Extract the biometric features
3. Put the features in a database



The architecture for biometric recognition - recognition

1. Take a biometric sensor
2. Extract the biometric features
3. Compare the features with the database
4. Return the result



What is a biometric sensor

A biometric sensor is a device that can be used to scan and read a person's unique physical characteristics. Overall, this can be multiple types of sensors, such as:

- Fingerprint sensor
- Iris sensor
- Voice sensor
- Signature sensor
- ...

What is the feature extraction process

Feature extraction is, given a biometric sample but in general any kind of data, the process of selecting and transforming the data in the correct format to be used in the recognition process. In this case, the goal is to convert into numerical feature vectors.

Why is preprocess done in the feature extraction process

The preprocess is done to remove noise and irrelevant information from the biometric sample, so that the feature extraction process can be more accurate and efficient. Not doing it can lead to problems like *failure to enroll*

Differences between deep learning and hand-crafted feature extraction

- **Hand-crafted feature extraction**: the features are manually designed by the engineer, based on the domain knowledge. This can be a problem because the features can be suboptimal.
- **Deep learning feature extraction**: the features are learned by the model itself, based on the data. This can be a problem because the model can learn irrelevant features.

How does matching work in biometric recognition

Given a biometric sample, the matching process is the process of comparing the features of the sample with the features of the database, and returning a **matching score**.

What is the matching score

The matching score is a numerical value that represents the similarity between the biometric sample and the database. The higher the score, the more similar the sample is to the database.

How isn decision made in biometric recognition

Usually, a **threshold** is selected to determine if the matching score is high enough to consider the sample as a match. If the score is higher than the threshold, the sample is considered a match.

What is a biometric template

A biometric template is a digital representation of the biometric features of a person. This template can be obtained from multiple samples of the same person, and is used in the recognition process. Usually it's nice to update the template during time, in order to keep the recognition process accurate.

What is aadhaar

Aadhaar is a technologie developed in India that uses multiple biometric feature to identify a person.

What are the Verification 1:1 evaluation metrics algorithmically speaking?

Algorithmically is referring to the fact that the error rates are calculated based on the algorithm's performance. The metrics are:

- False Non Match Rate (FNMR):
  The percentage of times that the system incorrectly fails to recognize a genuine match, meaning it

mistakenly says two biometric samples from the same person don't match. It's related to the False Reject Rate (FRR), where the system rejects the correct identity.

- False Match Rate (FMR):
  Tells us how often the system wrongly says two different people are the same based on their biometric data. It's like when the system mistakenly accepts someone who isn't supposed to be let in, especially if they didn't even try hard to pretend to be someone else. This rate is connected to the False Accept Rate (FAR), where the system wrongly lets in impostors without much effort.

What are the Verification 1:1 evaluation metrics systemically speaking?

Systemically speaking, the evaluation metrics are:

- Failure to capture rate (FTC): It's the proportion of failures due to the system not being able to capture the biometric sample. This can happen if the sensor is dirty of if the quality of the sample is poor.
- Failed to extract rate (FTX): It's the proportion of failures due to the system not being able to extract the features from the biometric sample to generate a template.
- Failure to acquire rate (FTA): Proportion of the failed acquisition of the biometric sample.

$$FTA = FTC + FTX \times (1 - FTC)$$

- Failure to enroll rate (FTE): Proportion of the failed enrollment of the biometric sample.

Evaluation metrics for verification for both algorithmically and systemically speaking

- System evaluation:
  - False Accept Rate (FAR): $FAR = FMR \times (1 - FTC)$
    The percentage of times that the system incorrectly accepts an impostor, meaning it mistakenly says two biometric samples from different people match.
  - False Reject Rate (FRR): $FRR = FTA + FNMR \times (1 - FTA)$
    The percentage of times that the system incorrectly fails to recognize a genuine match, meaning it mistakenly says two biometric samples from the same person don't match.
- Algorithm evaluation:
  - FMR = FAR
  - FNMR = FRR

What are some systems to display the performance of a biometric system

- Receiver Operating Characteristic (ROC) curve: It's the plot of the True Positive Rate (TPR) against the False Positive Rate (FPR) for different threshold values. The area under the curve

(AUC) is a measure of the system's performance. It's compared to the random classifier, which has an AUC of 0.5.
- Detection error trade off curve: Plots the FNMR vs FMR, or False Negative vs False Positive.

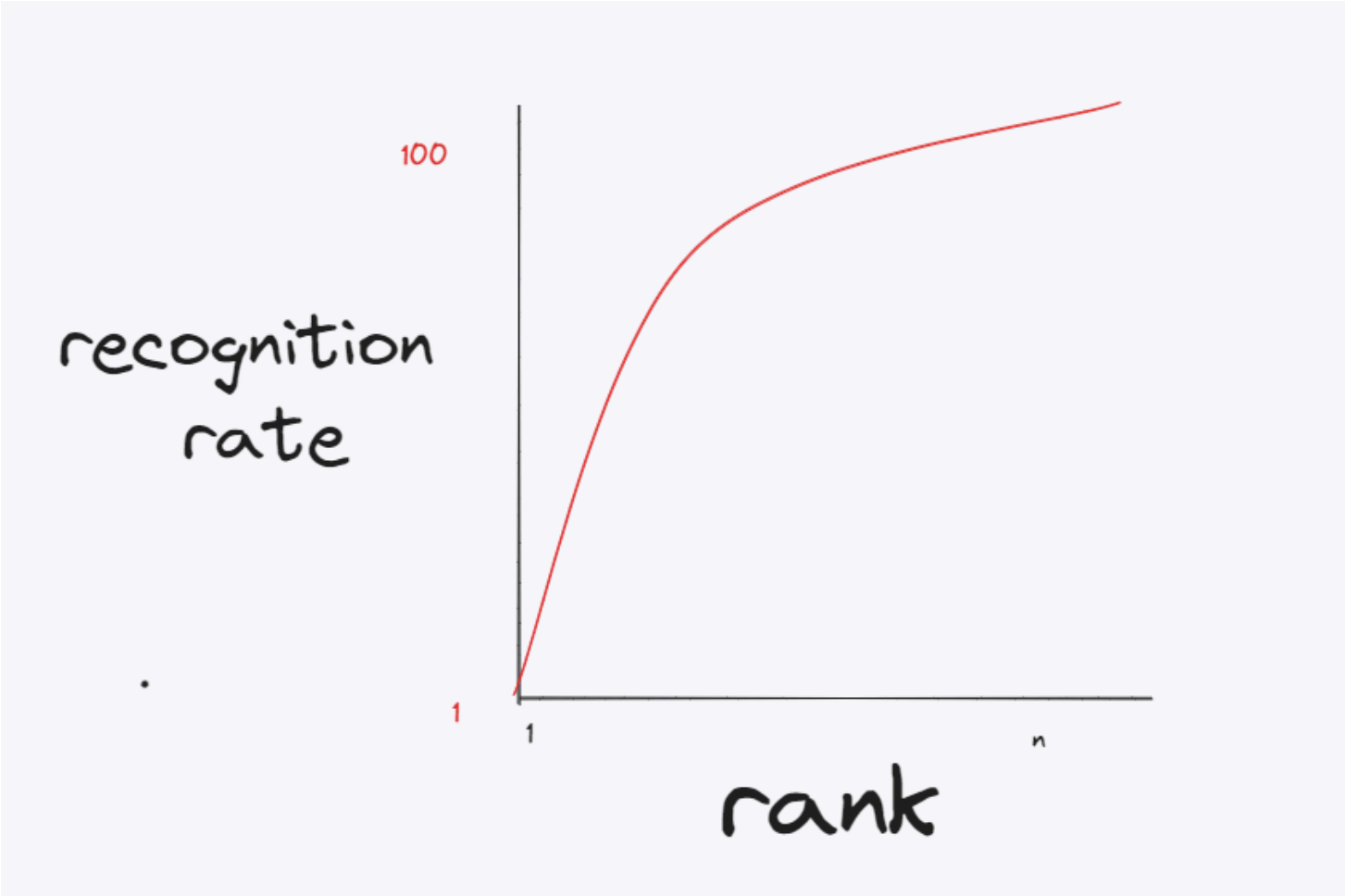
Evaluation metrics for identification 1:N

We have the concept of **rank**: A rank is the position of the true match in the list of candidates returned by the system.

- Rank 1 identification rate: The percentage of times that the system correctly identifies the person in the first position of the list.
- Rank N identification rate:
  - The TPIR (True Positive Identification Rate), is the proportion of identification trials that the system correctly identifies the person in the top N positions of the list.
  - The FPIR (False Positive Identification Rate), is the proportion of identification trials that the system doesn't put the subject in the top N positions of the list.

What can we use to plot the performance of an identification system

- Cumulative Match Characteristic (CMC) curve: It's the plot of the Rank N identification rate against the rank N. It shows how the system's performance changes as the rank increases.



Questions from the quiz 2021/2022

1: List 3 methods (of different nature), which can be employed to verify a person's identity. For each, indicate at least one advantage and one disadvantage.

Method	Advantages	Disadvantages
Fingerprints	- High accuracy	- Can be difficult to capture the fingerprint
Passwords	- Easy to use	- Can be easily forgotten
Face recognition	- Convenient	- Can be fooled by a photo

2: Biometrics recognition can operate in identification or verification modes. What is the main difference between them?

For each case, indicate one metric that is typically used for evaluation purposes.

- **Identification:** It's the process of searching inside a database for a match of a biometric sample. Usually, to evaluate this we use a metric called N-rank, that is based on checking if the true match is in the top N positions of the list. A plot can be the Cumulative Match Characteristic (CMC) curve.
- **Verification:** It's the process of comparing a biometric sample with a claimed identity. This is easier than the identification, because we only need to check if the sample matches the claimed identity so it's a 1:1 check instead of a 1:N. To evaluate this, we use the False Match Rate (FMR) and the False Non Match Rate (FNMR) and ROC.

3: In the context of biometric recognition what is understood by intra-class variation? Give an example of why this problem exists.

Intraclass variation means that a biometric sample can change during the time. An example can be the facial recognition, where the face can change due to aging, facial hair, or even the expression. To solve this problem, we can use multiple samples of the same person to create a template and acquire this more than once during the time to update the template.

4: Is there any advantage in combining the information captured by two different sensors, which acquire information of the same biometric trait? Why?

In my opinion, yes. Having more biometric recognition system is more robust than using a single one. Of course, this can be more expensive and complex, but it can increase the accuracy of the system. For example, combining the fingerprint sensor with the iris sensor can increase the accuracy of the system, because the chances of both sensors failing at the same time are lower.

5: Give 2 examples of applications where biometric recognition can be used, exemplifying how biometrics would provide an advantage.

1. Airport security: Can be used to check if a person is claiming to be who they say they are, and to check if they are on a watchlist.
2. Banking: Can be used to verify the identity of a person when they are making a transaction, to prevent fraud.

3. Building access: Can be used to control who can enter a building, and to keep track of who is inside.
4. Criminal identification: Can be used to identify criminals, and to prevent them from committing more crimes.

Questions from the quiz 2022/2023

1. To control the access to a critical system an organization may use one of the following solutions:

a) Token based PIN
b) Iris Scan
c) Identification card with photo
d) Password

Discuss the relative merits of these options, indicating the one you believe is the most effective.

a) Token Based Pin: This option is easy and fast for the user, but it can be easily lost or stolen, and it can be easily forgotten. It's not very secure.
b) Iris scan: Probably the best one since the iris is unique to each person, and it's difficult to fake. It's also fast and easy to use.
c) Identification card with photo: This is a good option, but it can be easily lost or stolen, and it can be easily faked.
d) Password: This is the worst option, because it can be easily forgotten, and it can be easily stolen.

2. What is understood by biometric verification? Indicate two metrics (explaining what they measure) which can be used for performance evaluation of a biometric verification system.

Biometric verification is a process that involves a check of a person identity. Given a person, check if biometric sample matches the claimed identity. It's a 1:1 check.

Two metrics that can be used are:

- False Match Rate (FMR): The percentage of times that the system incorrectly says two biometric samples from different people match.
- False Non Match Rate (FNMR): The percentage of times that the system incorrectly fails to recognize a genuine match, meaning it mistakenly says two biometric samples from the same

person don't match.
- ROC Curve.

3. An organization is considering implementing biometric access control for a critical system. The organization should be MOST concerned with which of the following? (Justify your answer):

a) False Match Rate (FMR)
b) False Non-Match Rate (FNMR)
c) Equal Error Rate (EER)
d) Number of staff enrolled for biometrics.

False Match rate is the most critical: If the system incorrectly says two biometric samples from different people match, it can lead to unauthorized access to the system, which can be a security risk. The other options are also important, but the FMR is the most critical.

4. Fusion of information captured from multiple biometric traits often improves biometric recognition results. Give one example to illustrate the types of information that can be considered for fusion, and an example of how the fusion of those biometric traits can be done

An example is taking more biometric data from a person. An example can be at the airport for security checks. Other than checking maybe the finger print, it's possible to check the iris scan, the face recognition, and the voice recognition. This can be done by combining the results of the different biometric recognition systems to get a more accurate result.

5. Is a biometric template always created from a single biometric sample of a given person? Why?

The answer is no. Since the biometric system needs to be reliable, a way to make this more robust is to use multiple biometric samplem to create a template. Moreover, doing it over time it's possible to update the template and make the system more accurate.