THANKS TO: Nunzia,Tommaso,Elena

Questions are taken from the drive, answers are taken either directly from the answer given on the drive or are inferred from slides/summaries

Question 1

Talk about evaluation in verification systems

-To evaluate a verification systems we cannot simply count errors but we take into consideration other metrics like FAR, FRR, GA , GR, ERR, DET and ROC…

How do we calculate these rates?

$FAR = FP / (FP + TN)$ |# people accepted | / |numb of people that should have been rejected|
$FRR = FN / (FN + TP)$|# people rejected | / |numb of people that should have been accepted|
$GA = 1 - FAR$
$GR = 1 - FRR$
$ROC = True\ Positive\ Rate\ and\ False\ Positive\ Rate$
$DET = FAR\ and\ FRR$

//if asked about identification:

In the identification task we use other metrics: in open set we use
DIR (Detection and identification rate) that is |people correctly detected in rank k| / |Pg| and
FRR = 1 - DIR (t,1) and
FAR = |people recognized by mistake| / |Probe not in gallery|
In closed set we use CMS(probability of identification at rank k) and CMC that shows the DIR at different ranks.

When to privilege false acceptance rate or false rejection rate?
-depends on the application.
When we have a security application we should privilege a low FAR. This because having to repeat recognition can be tedious for the user, but being falsely accepted could constitute a serious danger.

What is the difference between open and closed set?

- Open set: the system determines if probe pi belongs to a subject in the gallery G. Some probe **might not** belong to any subject in G -> the system has a reject option.
    - *Possible errors:* reject a probe belonging to an enrolled subject **or** accept a probe non belonging to an enrolled subject **or** to return the wrong identity
- Closed set: all probes belong to enrolled subjects.

- *Possible error:* return the wrong identity.

Question 2

Talk about EER metrics

EER equal error rate is the point where the two probability errors are equal, i.e., FRR = FAR. EER is not a threshold but the reached value imposing a similarity threshold where FAR is equal to FRR.

Question 3

Talk about Fingerprint Recognition.
Talk about latent fingerprints.
What's the first problem in registering a latent fingerprint vs registering a direct one?
Talk about different types of fingerprints.
Talk about Poincaré index.

FIngerprints appear like a series of dark lines that represent reliefs and are called **ridge lines**, discontinued by bifurcations or in general micro singularities called **minuzie**. Fingerprints are a randotypic trait and that makes them a strong biometric. The most amount of differences are found between (in descending order):

- people of different ethnicities
- people of same ethnicities that aren't relatives of any kind
- parent and child
- siblings
- twins

Two modalities for fingerprints acquisitions:

- **off-line**
  - pass fingertips on ink and them transfer the image on paper
  - digitize image through high resolution camera or optical scan
    - **latent fingerprints** are a class of off-line detected fingerprints and are the prints accidentally left on surfaces due to the fat nature of our skin
      - taken with chemical reactors, of course difficult to collect and identify because maybe they are partial prints or have weird orientation
- **live-scan**
  - directly through a digital sensor
  - different kinds of scanner:
    - thermal scanner
    - capacitive scanner
    - optical scanner

Problems in **acquisition** depending on the method could be: motion on the sensor, different levels of pression (both on paper or digital sensor), too much or too little ink, dry or damaged skin, error on feature extraction (following the acquisition).
Problems in **recognition** could be: acquisitions happened in different positions, different skin conditions.

Different kind of matching:

- **correlation based:** images are overlapped (operating rotation and translation if needed) and the correlation between pixels is calculated. Sensitive to rigid and non linear transformation, high computational complexity
- **ridge characteristics based:** evaluates ridges orientation shape and texture, local frequency easy to extract not THAT distinctive, this means low discrimination power
- **minuzie based:** minuzie are represented by a set of points in a 2d environment. The alignment that guarantees the maximum number of correspondent minuzie pairs is selected and is used to measure similarity between prints. Precise but hard to collect features

N.B. **Gabor filters** can be used in feature extraction to then facilitate matching.

Feature extraction is key to recognition and there are a lot of different approaches:

- **segmentation**
  - differentiation between foreground and background by individuating patterns. useful is to detect high points on local orientations histogram and gray level variations
- **directional map**
  - a discrete matrix whose elements denote the orientation of the tangent to the ridge lines. From this map, singularities are extracted
- **frequency map:** for every point in a fingerprint, the number of ridges for length unity in an hypothetical segment centered in [x,y] and orthogonal to the local ridges orientation is studied
- **singularity:** most approaches are based on the directional image of the print. An elegant method is the calculation of the **Poicaré** index. **G** is a vector field, **C** curve immersed in **G**. **Pg,c** is the total rotation of vectors of **G** in **C**. **G** field associated to the image of orientations of **D** print and **[i,j]** position of element Θ**i,j** in the image, **Pg,c(i,j)** is calculated by summing the differences in orientation between adjacent elements in **C**
- **minuzie:** is performed through binarization, thinning and localization of pixels corresponding to minuzie. Localization examine the crossing number of points, that indicate if the point is internal, corresponds to a termination, to a bifurcation or to a more complex minuzie
- **number of ridge lines:** ridge count is an abstract measure of the distance between two points in a print. Particularly, the number of ridge lines intersected between points a and b. The two points are often chosen in particular print areas, like **core** and **delta**

N.B. to detect attacks or fake fingerprint technique is to detect the liveness of the person attached to the fingertip using pulse, temperature or other features.

Types of fingerprints are distinguished by the presence and amount of **loops**, ulnar or radial **arches** (one delta), plain or tented and **whorls** (two or more delta), plain, central pocket loop, double loop, accidental.

Question 4

What is spoofing?
Evaluate spoofing together with recognition?
What's the difference between spoofing and camouflage?
Are all biometric traits weak to spoofing?
Liveness Detection for anti-spoofing (ex.recognizing a photo or a video).
Talk about techniques.
Where can you find moiré patterns?

Biometric spoofing is the act of misleading a biometric sensor by imitating or copying a biometric trait that identifies the legitimate subject. In **camouflage** instead, the attacking subject tries to be not recognizable. It's important to consider Spoof False Acceptance Rate (SFAR) and not FAR, because the last one takes into account zero effort attacks. In this case, FRR is used but indicates the wrong classification of an authentic probe as a fake one. Spoofing can be evaluated in different ways:

- **together with recognition:** only one accepted/rejected result
- **with recognition divided in two modules:** only one accept/reject result but first the biometric system gives the answer and then the result is checked with countermeasures systems
- **separated:** to accept/reject result, one for the biometric system, one for the countermeasure system

The traits that are weak to spoofing are the ones based on appearance. Behavioral traits like gait or gestures can't be really reproduced.

When it comes to face spoofing, the two main methods are of course 2D and 3D. 2D spoofing can be done by presenting a photo or a video of another, 3D through masks for example. Liveness detection methods are various:

- **2D**
    - **photo**
        - face movement
        - lips movement
        - eyelids movement
        - intercept LPB - micro-texture analysis
        - inferior resolution
        - background
        - gaze stability
    - **video**
        - detect **moiré pattern** (stripes present when you photograph a display) appears during the recapture of video or photo replays on a screen in

different channels (R, G, B and grayscale) and regions(the whole frame, detected face, and facial component between the nose and chin).
        - through LBP and DSIFT
- **3D**
    - detect light reflection, it differs from masks to faces
    - measure bpm by looking at small color differences on the skin through rPPG

Question 5

Difference between hard and soft biometrics. Which biometrics trait is unique?

-**strong** biometric traits like iris, face, fingerprint and **soft** biometric traits like hair color, facial shapes and gait (walk).
Soft traits(or both) *lack* uniqueness (hair color) or persistence (behavioral are affected by mood) but can be used to limit research.

A biometric trait to be considered strong has to be:
- Universal
- Unique
- Permanent

in addition to that, for usability purposes, the trait should be:
- Collectable
- Acceptable

Examples of strong biometric traits are iris, face, fingerprint… Generally randotypic traits are the best.

A soft biometric trait generally lacks permanence or uniqueness, like for example hair, gait or in some ways also face, that has hereditary traits.
Usually unique biometric traits are the ones that are randotypic or the DNA:
- DNA
- fingerprint - but 46% of population has damaged fingerprints (elderly people or hard workers)
- iris

Question 6

Talk about multi-biometric approach.
How do you put together the results?
Which type of fusions exist other than the ones based on score? Feature level?
When do you use Borda count, in which method?
Can you utilize a ranking system at score fusion level?
Rank advantages and disadvantages.

Multibiometrics are systems that integrate more sources of biometric data to improve recognizement performances. It means many things:

- Multiple algorithms
    - ex Filter Bank and Minuzie
- Multiple sensors
- Multiple traits
    - ex Sign and fingerprints
- Multiple instances
    - fingerprints of index and middle finger

Different ways of combining metrics

- **before matching**
    - <u>sensor level fusion</u>
        - data taken from different sensors can be integrated and elaborated to generate new data from which features are extracted
            - ex. in face recognition you can fuse 2D and 3D to obtain a 3D model
    - <u>feature level fusion</u>
        - features extracted in different ways can be used to create a new feature vector to represent the subject
            - ex Eigenface can fuse hand and facial features
- **after matching**
    - <u>score level fusion</u>
        - different algorithms can create a new combined score
            - ex fingerprint and facial score can be combined using the sum rule, other rules can be majority or Borda count
    - <u>rank level fusion</u>
        - useful for identification, different systems combine their ranking
            - ex Borda count as final ranking
    - <u>decision level fusion</u>
        - every classifier outputs their answer and then with a rule (ex majority rule) a final answer i found

Borda count is a positional voting rule (ex. first gets 5 points, second gets 3 etc, everyone does a ranking and then fuse answer)
A confidence margin can be defined as $M(\Delta) = |FAR(\Delta) - FRR(\Delta)|$
A problem with multi-biometric can be that different matchers can be non homogenous or non reliability.

Question 7

What is the detection rate? Identification rate?

- Detection rate is correctly detected an user, meaning the user is above the threshold, on the total number of users
- identification rate is correctly identified the user, meaning that the user is the first individual detected with a score above the threshold, on the total number of users

DIR (at rank k) (Detection and Identification Rate (at rank k)): the probability of correct identification at rank k (the correct subject is returned at position k)
The rate between the number of individuals correctly recognized at rank k and the number of probes belonging to individuals in PG:
Used to evaluate the identification task.

Question 8

Doddington Zoo? What causes extension? How could you strengthen a biometric system with a gallery of subjects?

Most of the errors in a recognition system can be traced back to a class of people that has some misleading characteristics. Doddington original classification goes as it follows:

- **sheep** are easily recognized and not easily mistaken for somebody else. Low rate of false accepts and rejects -> classical users
- **goats** are not easily recognized with templates of themselves. High false rejects
- **lambs** can be easily impersonated. High false matches
- **wolves** easily impersonate others. High false acceptances

The extensions offer a different perspective and the classification is based on the genuine and impostor scores:

- **chameleons** are easily impersonated and easily mistaken for somebody else. High score both as genuine and impostor
- **ghosts** are not easily recognized and not easily mistaken for somebody else. medium-low score both as genuine and impostor
- **doves** are easily recognized and not easily mistaken for somebody else. High score as genuine and low as impostor. similar to sheep - they are the best users
- **worms** not easily recognized and easily mistaken for somebody else. Low score as genuine and high as impostor - worst users

Question 9

Verification vs identification.
todo:In how many ways can I perform an identification?
Verification happens when the user claims an identity by presenting an ID card for example. The system then makes a 1:1 matching to verify the identity and returns an accept/deny result.

- *Identification* happens when there is no claim done by the user and the system performs a 1:N matching operation with the subjects in the gallery. Possible result is recognized/not recognized.
    - Can be open set, closed set or watchlist.

Question 10

Micro-texture analysis? operator for micro-texture?

Micro texture analysis is performed as an anti-spoofing system. Analyzing light reflection or printing quality defects can be very useful for recognizing fakes. They exploit multiscale local binary patterns. Those same features could be used for recognition.
The operator is the texture-based operator: **LBP. (maybe go in detail)**

Question 11

Which are pros and cons of iris recognition particularly between image capture, near inference and visible light?
Talk about Rubber Sheet Model

Iris is a randotypic trait. The advantages:

- it's permanent and unique
- generally collectible
- you can create small dimension template

Disadvantages:

- limited surface
- a good acquisition has to be taken very near

Capture modality:

- **visible light**: layers that compose the iris are visible. In the visible light spectrum, iris has a very rich, casual, intertwined texture
- **near inference light**: La tessitura è più visibile. Più adatta in sistemi biometrici basati sul riconoscimento dell'iride. Nell'illuminazione a infrarossi anche gli occhi marrone scuro mostrano una trama ricca

Daugman

- **iris position** uses blob detection
- **eyelash position** like before but also eyelids are detected
- **iris segmentation** mask the iris
- **unwrapping of the iris** extract center of pupil, but the look can deformate everything, so it's necessary a normalization model
    - **rubber sheet model** is a normalization process that is used in iris recognition.It takes into account factors like pupil dilation and iris deformation. It takes a fixed number of points between the margin of the pupil and the iris one and it normalizes the deformed distance. Every point is made polar with the center as the pupil center. New coordinates are given by a linear combination between pupil margin and external iris margin.

Question 12

Pros and cons between 2D and 3D face recognition?

- Advantages 3D:
    - more info,
    - robustness to some distortions
    - synthesizing 2D from 3D model virtual poses and expressions
- Disadvantages 3D:
    - devices costs
    - computational costs of procedures
    - possible risks due to laser

Question 13

What's a Morphable Model?

From a generic 3D model a final 3D model can be reached. **Morphable models** are dynamic representations of the face surface that have info on the dynamic structures (muscle for example) in addition to geometry info. How to generate the final model:

1. take 2 or 3 photos from different angles
2. change a generic model to fit yours
3. generate texture combining the images

Question 14

Talk about training in face recognition: differences between Adaboost face recognition model and the ones based on specific face characteristics? Talk about Haar cascade classifier

A face recognizer is structured in this way:

- Face capture and possible image enhancement
- Localization (cropping of one or more region of interest ROIs) + normalization
- Feature extraction
- Template construction (biometric key)

Adaboosting, differently from other algorithms, is based on a sequential ensemble learning technique. AdaBoosting objective is the one of constructing a strong classifier with a series of weak ones. Adaboost is a learning technique that has to learn the best sequence of weak learners and their weights. Combining the weak classifier reduces the superior limit for classification error by limiting the areas considered as face. The positive result of one classifier will be evaluated by a slightly more complex classifier. A reject will classify the area as non-face and that portion will not be further evaluated. Every classifier is trained on the false positive of the previous one. More in depth, training is then structured this way:

1. Adjust weak classifiers threshold to try to avoid false rejection
2. Each classifier is trained with the previous one false positives
3. A 20-feature classifier achieves 100% detection rate with 10% false positive rate.

Important is to have a balanced set, with roughly the same number of positive and negative examples. In the case of face, those are respectively stereotypical elements of a face and wrong traits that could mislead the systemModels of different quality should be included Dataset has to include distorsion (PIE: Pose, Illumination, Expression).
To select the subset of features analyzed by Adaboost, it's possible to use a Haar Classifier, or Haar cascade classifier.
To start to calculate the **Haar features**, weak classifiers based on simple features are used. Those are rectangular elements that can be divided, horizontally or vertically in black and white or with mix patterns. Every feature is in a sub window and is applied modifying its dimension. The result is the sum of the values of the pixels that are in the white area minus the sum of the ones in the black area. A threshold is then set and a yes/no result is given. To speed up the process, integral images are used.

Question 15

Which is different between genotypic and randotypic characteristics

The first one is a type of mostly hereditary characteristic. This means that parents and children or siblings etc. could share the characteristic or at least have similar ones. **Randotypic** are instead characteristics that are randomly formed, for example fingerprints are probably formed based on how the fetus touches areas around it.

Question 16

If we have two characteristics, one strong but computationally slow and one soft but faster? What can we do?

It depends on the scenario, but characteristics could be combined.

Question 17

What sensors should there be to use a smartwatch for recognition in addition to the gyroscope?

For example the accelerometer or thermal sensors(?).

Question 18

In how many ways can we divide a dataset to create a model?

Three main choices on the dataset:

- how to split test vs training dataset
- which model insert in probes or gallery
- complete overlap or not of the template in probe vs subjects in gallery

For validation, an approach is k-fold cross-validation. In k-fold, data are divided in k subsets, so the model is applied k times using one subset as a validation set and the other as train. The error is estimated on all k trials. k is generally 5 or 10.