Biometric authentication

Facial, Iris and Retinal recognition

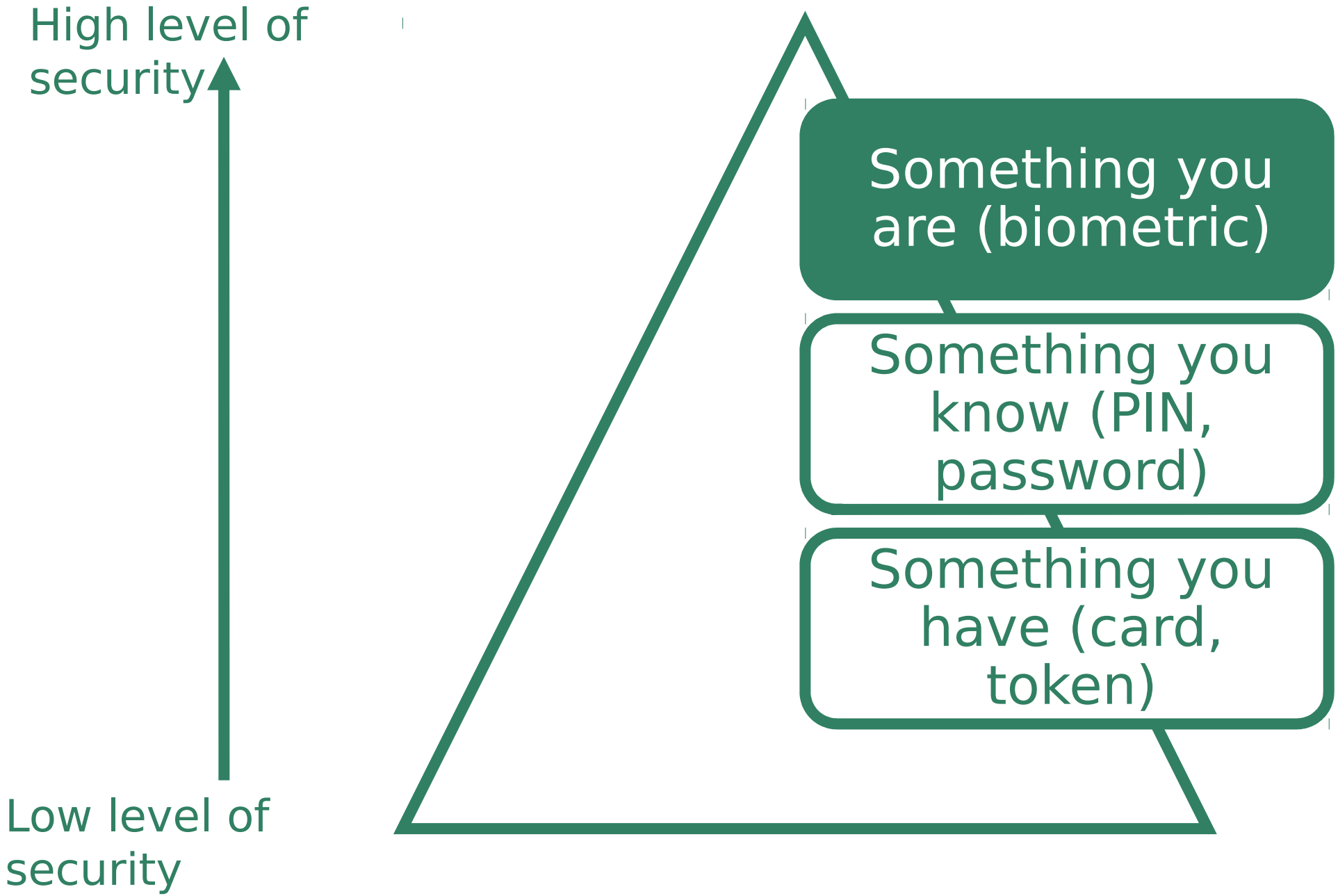
Patrick Sardinha – Adrien Razurel – Marvin Fourastié

Biometric authentication

Facial, Iris and Retinal recognition

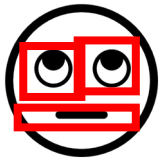
Patrick Sardinha – Adrien Razurel – Marvin Fourastié

Biometrics is the automatic recognition of a person using distinguishing traits


High level of security
Low level of security
Something you are (biometric)
Something you know (PIN, password)
Something you have (card, token)

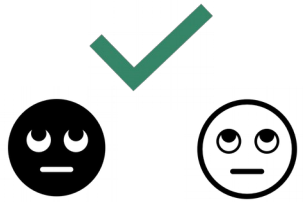
Authentication

Capture image



Extract features

Compare templates



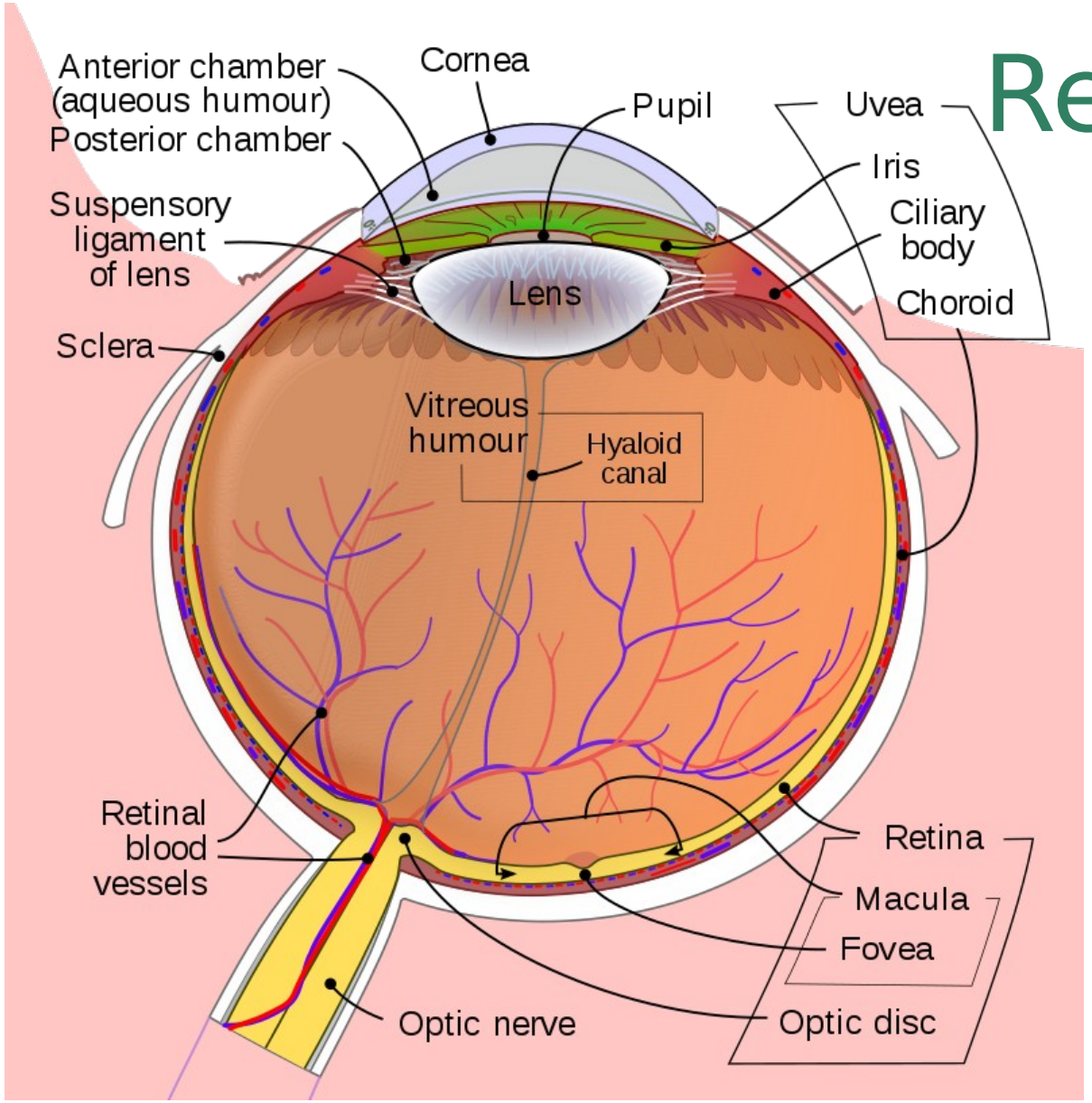
Declare matches

Retinal recognition

Iris recognition

Facial recognition

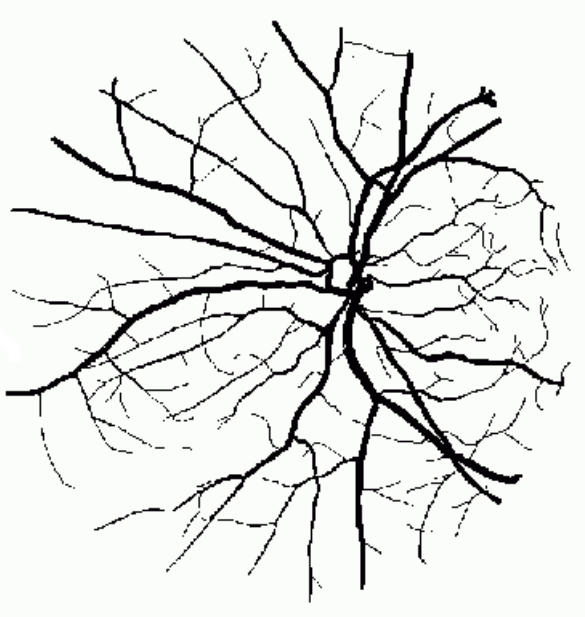
Retinal recognition

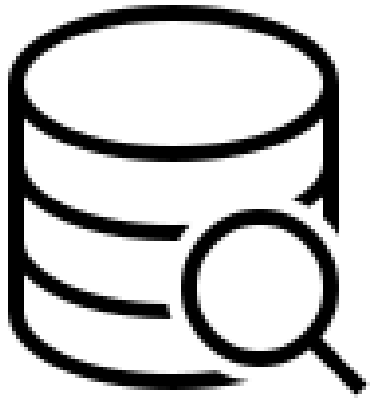


https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Schematic_diagram_of_the_human_eye_en.svg/800px-Schematic_diagram_of_the_human_eye_en.svg.png

Recall: Anatomy of the eye

How it works

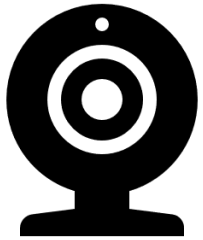




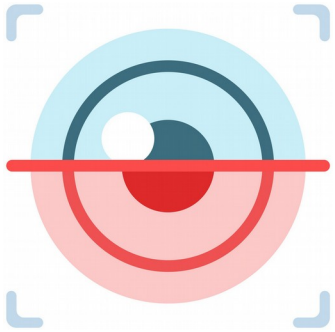
https://www.semanticscholar.org/paper/AUTOMATIC-BLOOD-VESSEL-SEGMENTATION-IN-COLOR-IMAGES-Osareh-Shadgar/ed8c54d05f1a9d37df2c0587c2ca4d4c849cb267/figure/2

Idea: Use a scanner to identify the drawing of the retinal network of a person that is to say the blood vessels and compare it with a database

Recording / Registration

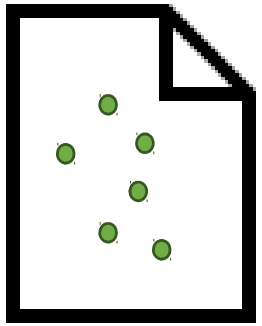


Place eye in front of a camera

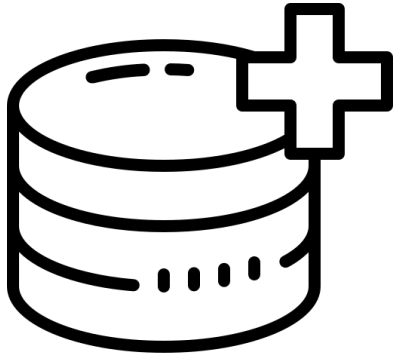


A beam of light is injected in the eye

(A few seconds)

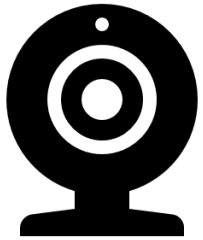


Extraction of unique features

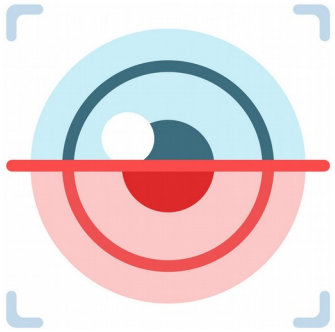


The model is added to a database.

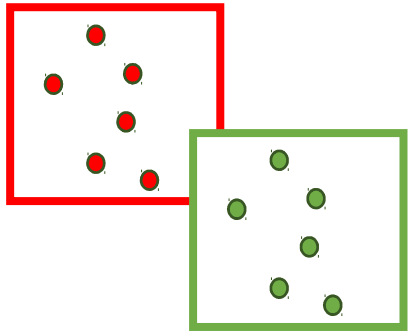
Verification



Place eye in front of a camera



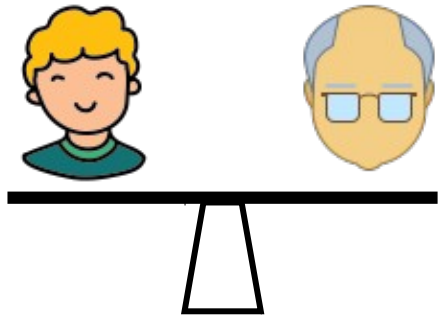
A beam of light is injected in the eye
(< 2 seconds)



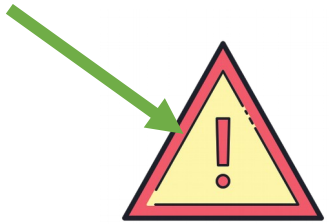
Comparison between the scanned drawing and those in the database

Verification passes or not

Advantages



Retinal is stable



Very reliable
(Error: 1 in 10 millions)

No possible counterfeiting
Attacks are difficults

Verification very fast

Disadvantages

Technique considered intrusif

To obtain quality images, the end user must be cooperative

Distances must be close

High cost

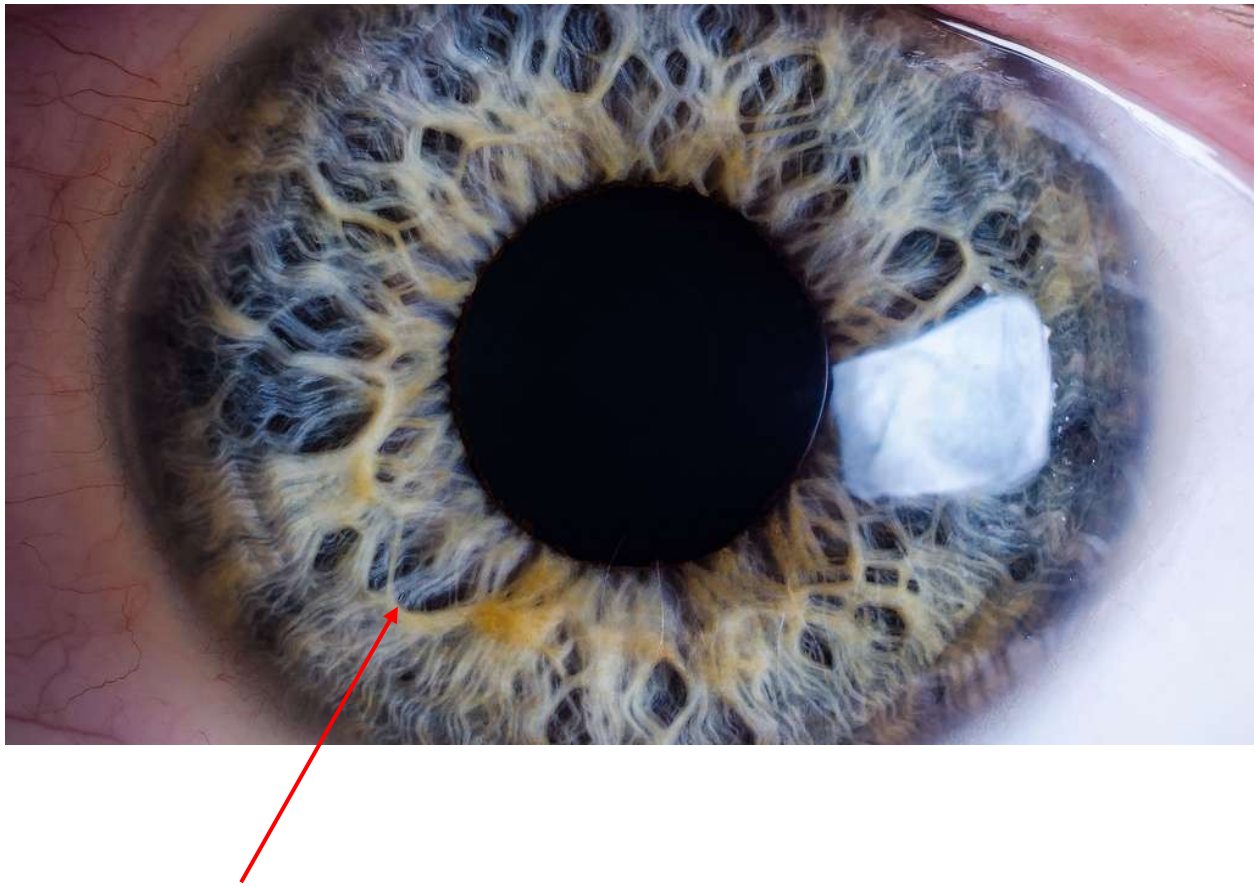
Usage

Not very used
by common people

But used in
places of high security

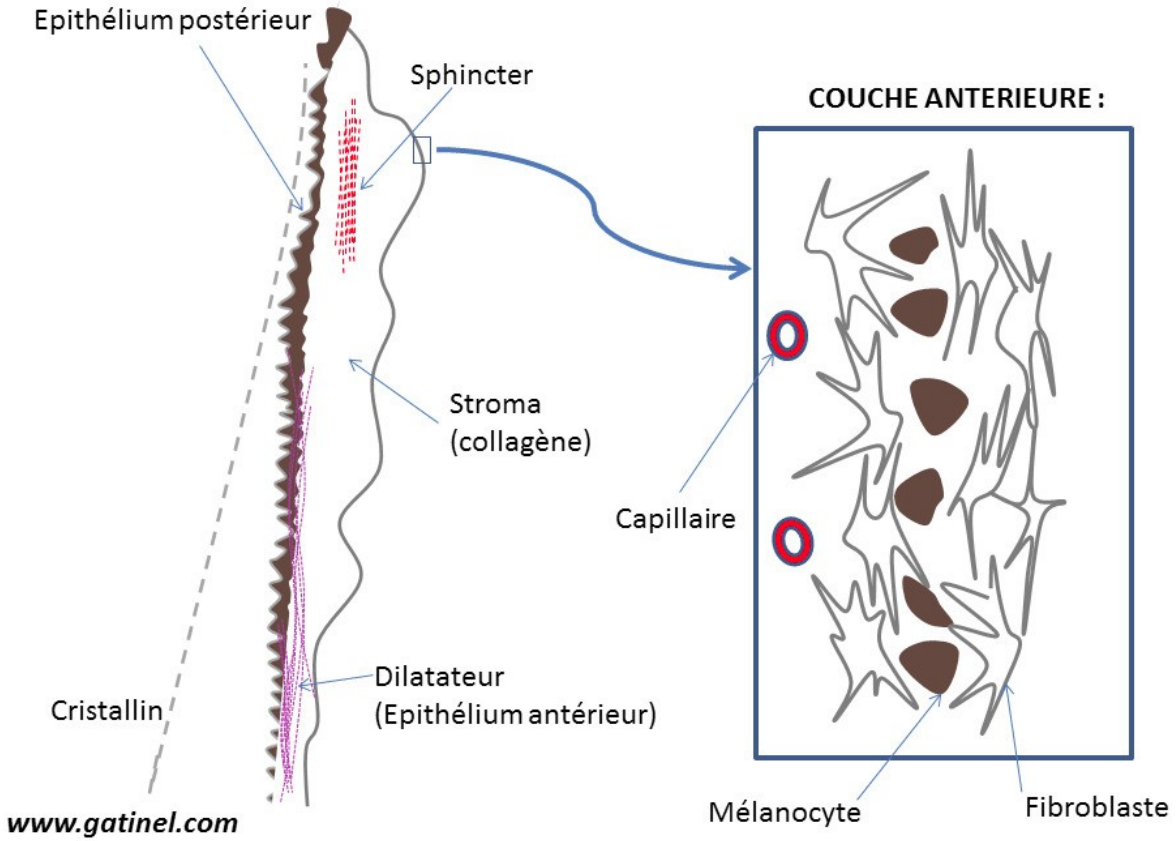
Iris recognition

Iris



Iris is the colored part of the eye

It is responsible of the dilation and contraction of the pupil



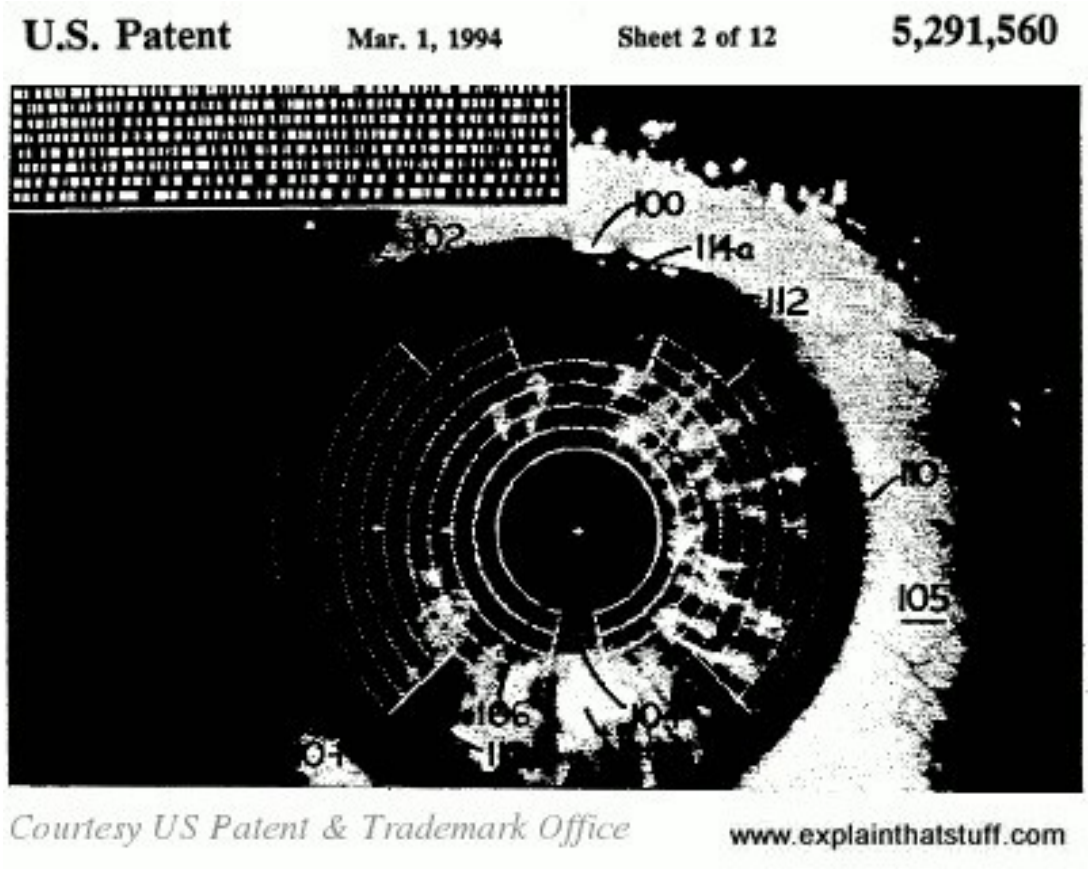
3 layers:

Posterior layer

Stomale layer that contains muscles

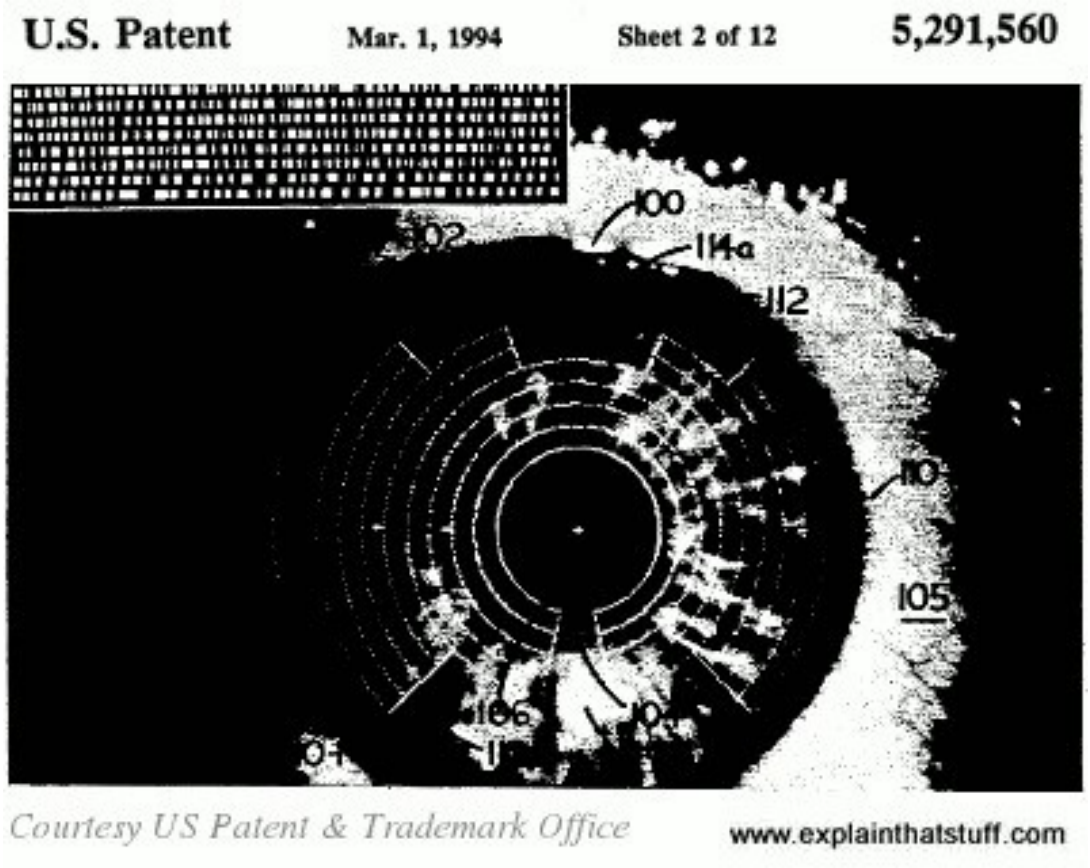
Prior layer which represent the patterns and colors of the iris. More precisely, there is 2 pigments that caracterize the color (melanine and lipofuscine) and cells (fibroblastes) that caracterize the corneal reliefs.

Iris scan pattern recognition



Enrollment:

- takes few minutes
- Photo with a normal camera + photo with infrared camera to have more precise résultats
- The system removes useless shapes (eyelashes, eyelids)
- Delimitation of the iris with circles to set the borders
- Transform all these informations to a 512 bytes data and put it on a database



Verification:

- takes few seconds
- Photo with a normal camera (not necessarily the same used for the enrollment)
- Delimitation of the iris with circles + transformation of the image using polar coordinates so that even if the pupil is contracted or dilated we can match the patterns of iris
- Pattern matching browsing all the database

Advantages

Accuracy: 1/2'000’000 chance to have false match (whereas fingerprints has 1/100’000)

Stable: iris is protected by cornea, very hard to damage + doesn’t change during person’s life

Non invasive: scan can be done remotely, no need to enlighten the eyes to do the verification, no physical contact.

Scalable: each iris is represented by 512 bytes

Disadvantages

Recognition is less precise for children (1-4 years old)

Possibility to take a photo of a person’s eye without his consent and use it against him

With a good quality image of a person, we can print the iris and use the image (Exemple of an attack on samsung S8 iris recognition). Some advanced scaners avoid these attacks by capturing eye movements or velocity of the pupil contraction/dilation.

Attack on a database that contains all the iris data is a real problem because unlike passwords, you can’t change your iris.

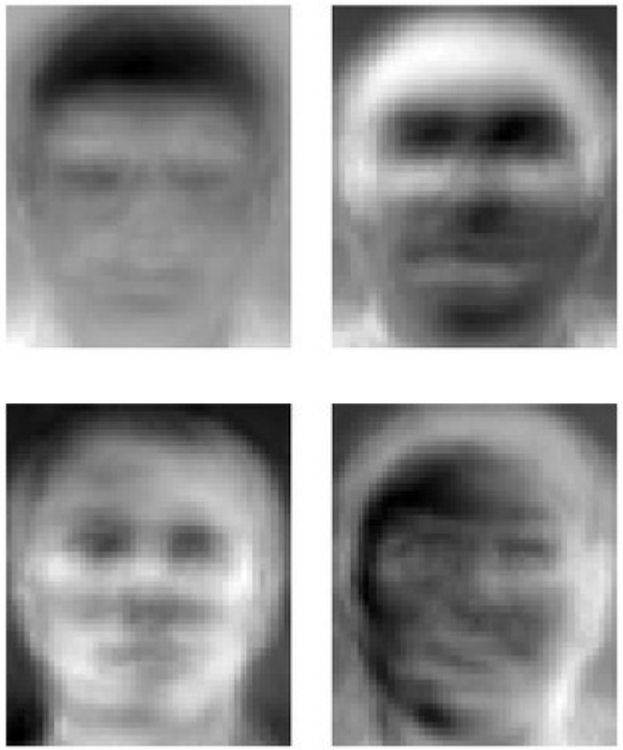
Usage

Allows law enforcement officers to compare iris images of suspects with an existing database of images in order to determine or confirm the subject’s identity.

Iris scans are quicker and more reliable than fingerprint scans since it is easier for an individual to obscure or alter their fingers than it is to alter their eyes.

Facial recognition

2D data



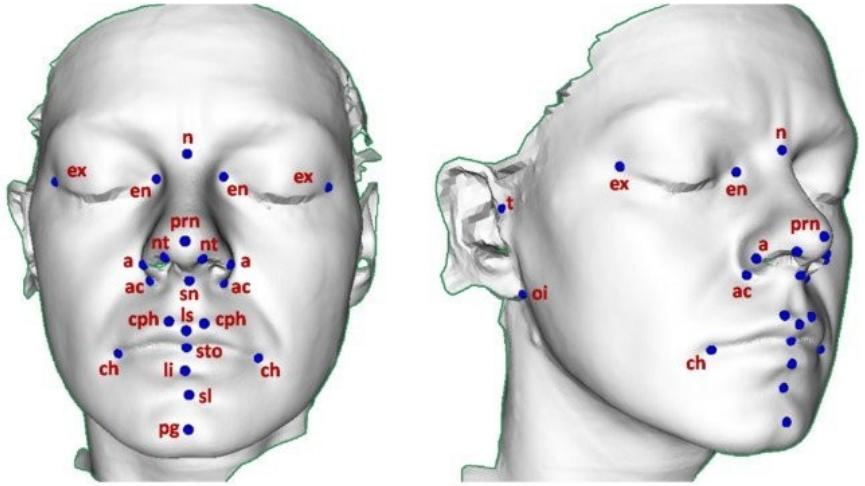
https://fr.wikipedia.org/wiki/Eigenface

→ Produce « eigenfaces » using eigenvectors of an image

→ Use JPEG / JPEG 2000 to store the images

3D data

- Take several pictures to reconstruct a 3D face
- The features stored are the reliefs of the face



https://www.researchgate.net/figure/Figure-122-Localization-of-facial-landmarks-for-3D-face-recognition-and-face-pose_fig14_310127793

Attacks

Photo (2D) :

Use a high quality photo to trick the camera

Video (2D/3D) :

Present a video like if it comes from its own camera

With a mask (3D) :

Use a printed 3D mask to trick the camera

Advantages/ Disadvantages

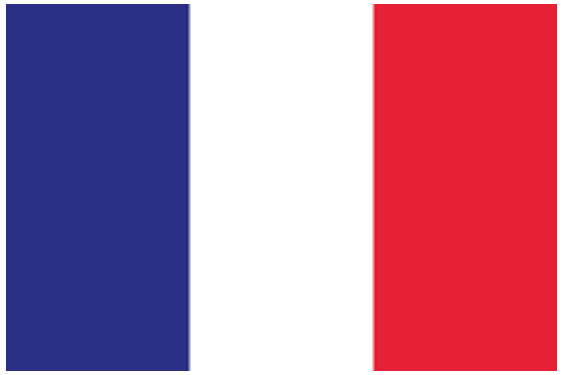
Convenience of data acquisition...

...But a lack of accuracy

Easy recognition of a person...

...But privacy issues

France wants to use facial recognition but...



→ Protect stored data

→ ~ 80% of accuracy

→ Establish database