# Spoofing Attacks and Pathologies: In the Search for the Border between Security and Usability

Inmaculada Tomeo-Reyes, Judith Liu-Jimenez, Sara Ceballos-Burgos*, Raul Sanchez-Reillo

University Group for Identification Technologies (GUTI)
Carlos III University of Madrid
Tlf.: +34 91 624 40 35 Fax: +34 91 624 94 30
{itomeo,jliu,rsreillo}@ing.uc3m.es

*RealVision Ophthalmology Clinic, Optometry Department
sceballos@realvision.es

# Outline

# Introduction

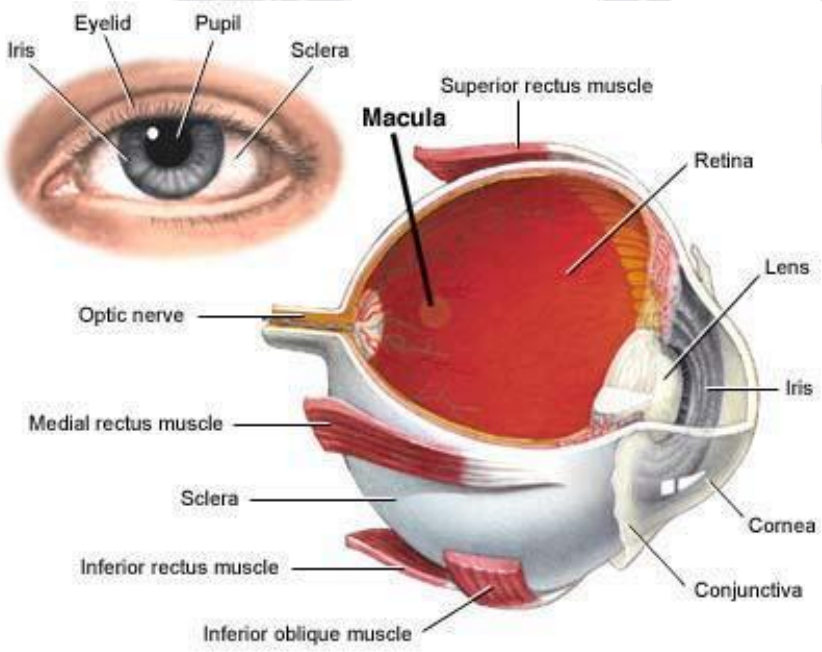


- Iris recognition
  - Iris pattern is unique, stable and non-invasive
    - Suitable for individual recognition purposes
  - It has inherent weaknesses that can compromise security
    - Susceptibility to spoofing attacks
  - It is possible that the implemented countermeasures affect users with ocular pathologies
    - A compromise between security and usability must be reached
- When a person who suffers from an ocular pathology uses an iris identification system…
  - The system should recognize the sample as anomalous
  - Unless there is a high probability that the captured sample corresponds to a fake, friendly policies shall be used with the citizen involved in order not to harm the individual integrity and user acceptance of the system by provoking unnecessary alarms
    - Examples of friendly policies could be forwarding the person to use another recognition system or seeking assistance from the supervisory agent

# Introduction



- There are several and very diverse ocular pathologies, among them, we are interested in those that directly or indirectly affect the iris
  - Iris pathologies
  - Corneal/scleral pathologies that affect iris images



# Main Target



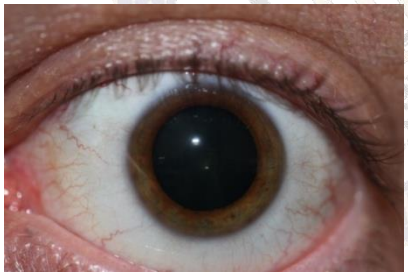
- Increase the knowledge about...
  - Iris-related pathologies influence on iris recognition systems performance
    - How and how much can an iris-related pathology affect iris recognition systems performance?
  - Relation between ocular pathologies and spoofing attacks
    - Are ocular pathologies and spoofing attacks related?
    - What should be done in each case?
  - Impact on usability
    - How can individual´s integrity and user´s acceptance be protected when an anomalous sample is detected?
- Apply later the knowledge to establish the border between security and usability

# Iris pathologies



- Miosis and mydriasis
  - Description
    - Miosis and mydriasis are, respectively, excessive constriction or dilation of the pupil
    - The cause may be disease, trauma or the use of drugs or alcohol

Miosis



Mydriasis

  - Effects on iris recognition systems
    - Samples affected by miosis/mydriasis in an advanced stage can be falsely rejected if the system is not robust enough. As both pathologies can be easily artificially provoked (miotic/mydriatic agent eyedrops, drugs,…), this fact can be easily checked
      - Experiments with OSIRIS (open source iris recognition system developed in the BioSecure Network of Excellence) demonstrated that this kind of samples can be problematic
      - Distance between the miosis/mydriasis affected sample and the corresponding normal sample is very similar to the distance between a genuine iris and a common impostor iris
      - Extra mechanisms or quality measures like iris-pupil ratio should be considered in order to avoid this

# Iris pathologies



- Miosis and mydriasis (cont.)
  - How mydriasis/miosis and, in general, pupil dilatation/constriction affects an iris recognition system is not simple to describe and quantify
  - According to certain studies*:
    - Degree of dilation enrollment ≈ Degree of dilation recognition
      - Highly dilated pupils result in worse recognition performance than comparisons involving constricted pupils
    - Matched images with similarly highly dilated pupils
      - Mean intraclass Hamming distance ↑
      - Mean interclass Hamming distance ↓

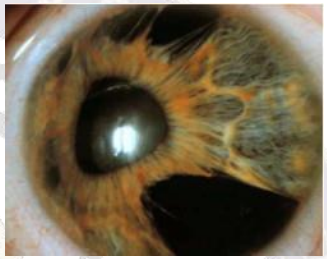
      → Probability of false rejection ↑
    - Matched images with larger differences in pupil dilation
      - Higher template dissimilarities → Probability of false rejection ↑↑
      - With less iris area visible and less data available, iris is more poorly characterized and recognition performance gets worse

* Hollingsworth, K., Bowyer, K. W. and Flynn, P. J., "Pupil dilatation degrades iris biometric performance". In *Computer Vision and Image Understanding*, vol. 113, issue 1, 2009.

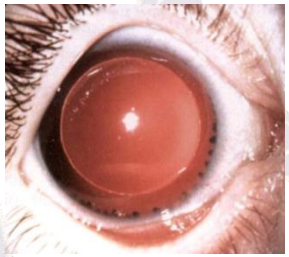
# Iris pathologies



- Aniridia
  - Description
    - Aniridia is the partial or total absence of iris. In the 2nd case, peripheral remnants of the iris are usually still present, though sometimes not directly visible
    - Aniridia can be transmitted as an autosomal-dominant trait or occur sporadically. It may also be traumatic or result from penetrating injuries



Partial aniridia



Total aniridia

  - Effects on iris recognition systems
    - In the case of total aniridia, iris recognition is not possible
    - In the case of partial aniridia, successful iris recognition depends on 2 main factors:
      - Correct segmentation and masking of the iris → a versatile segmentation method and accurate masking is required
      - Enough usable iris area → If at least the 70% of the iris area is not occluded, and thus, usable, iris recognition should be possible
        - The percentage is according to ISO/IEC 4th Working Draft 29794-6, "Biometric sample quality – Part 6: Iris image data"

# Iris pathologies



- Inflammations of the uveal tract (choroid, ciliary body and iris): Iritis, cyclitis and iridocyclitis
  - Description
    - Iritis is the inflammation of the iris. It usually occurs in combination with cyclitis or ciliary body inflammation (iridocyclitis)
    - Iridocyclitis is frequently attributable to immunologic causes (e.g. allergic reaction to bacterial toxins) or, less frequently, to infections
    - Acute iridocyclitis produces adhesions between the iris and lens (synechiae)

Synechiae

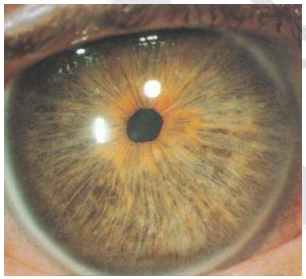
  - Effects on iris recognition systems
    - If no synechiae is produced, successful iris recognition should be possible
    - In the case of synechiaes, successful iris recognition depends on 2 main factors:
      - Correct segmentation and masking of the iris → a versatile segmentation method and accurate masking is required
      - Enough usable iris area

# Corneal pathologies



- Corneal size anomalies: microcornea and megalocornea
  - Description
    - Microcornea and megalocornea are, respectively, abnormally small or big cornea
    - Usually congenital and, in general, rare

Microcornea



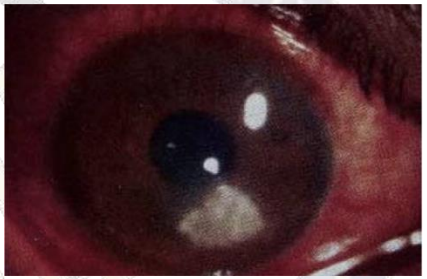
Megalocornea

  - Effects on iris recognition systems
    - It is difficult to assess to what extent can these pathologies affect iris recognition systems
      - As they are generally congenital pathologies, it is difficult and most times impossible to obtain a healthy sample of the individual iris
    - Between these two pathologies, microcornea is the most problematic in terms of successful iris automatic recognition
      - In the case of microcornea, the probability of a successful recognition decreases. Although the usable iris area would be near 100%, if the iris camera cannot capture iris texture with enough detail, not enough information is available, and no recognition is possible

# Corneal pathologies



- Corneal opacity
  - Description
    - It occurs when the usual corneal degree of transparency decreases
    - Corneal opacity causes can be very diverse. Trauma, microbial keratitis - cornea inflammation- and vitamin A deficiency are the most frequent causes. Other causes can be viral/exposure keratitis or opacity following surgery, pterygium or long-term conjunctivitis



Microbial keratitis (ulcer)

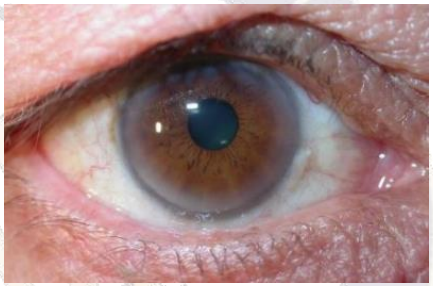
Leukoma (scarred tissue)

  - Effects on iris recognition systems
    - Successful iris recognition in this case depends on the location and extent of the opacity
      - Correct segmentation and masking of the iris → a versatile segmentation method and accurate masking is required
      - Enough usable iris area

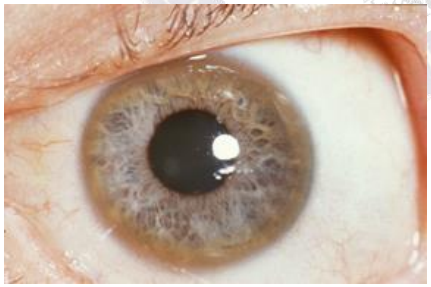
# Corneal pathologies



- Corneal deposits: Arcus senilis and Kayser–Fleischer ring
  - Description
    - Arcus senilis is a grayish-white ring-shaped fatty deposit near the limbus. It can occur at any age but it usually appears in advanced age
    - Kayser-Fleischer ring is a golden-brown to yellowish-green corneal ring caused by copper deposits. It is a sign of Wilson's disease



Arcus Senilis



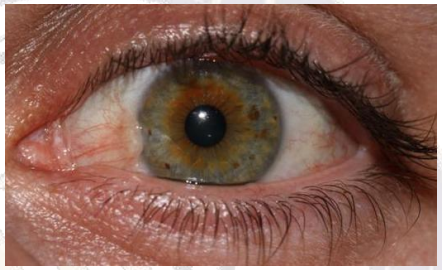
Kayser-Fleischer ring

  - Effects on iris recognition systems
    - Corneal deposits occlude the iris, particularly in the limbal ring area. Being this the situation, successful iris recognition depends on 2 main factors:
      - Correct segmentation and masking of the iris
      - Enough usable iris area

# Corneal pathologies



- Pterigyum
  - Description
    - Triangular fold of conjunctiva toward the cornea, with its apex towards the pupil. It is a very common pathology
    - It is usually caused by exposure to intense sunlight



Pterigium

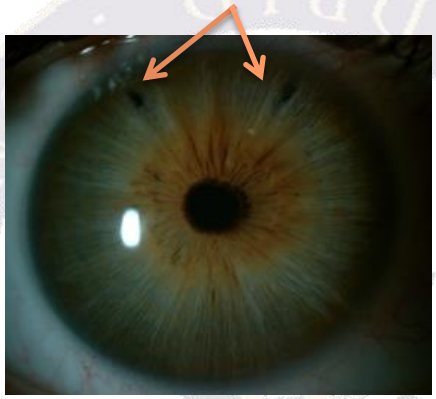
Pterigium (detail)

  - Effects on iris recognition systems
    - Pterigium occlude the iris. It usually gradually grows and can even reach the pupil. Being this the situation, successful iris recognition depends on 2 main factors:
      - Correct segmentation and masking of the iris
      - Enough usable iris area

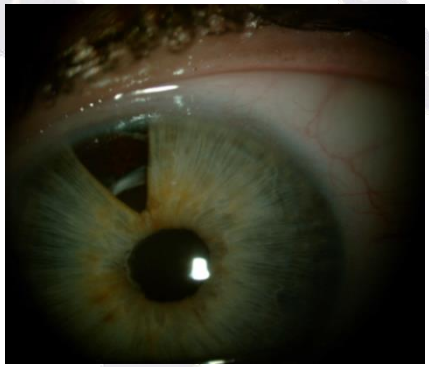
# Iris conditions due to surgical procedures or trauma



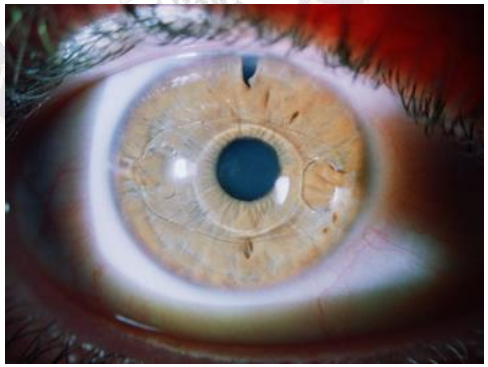
- Iridotomy and iridectomy
  - Description
    - Iridotomy and iridectomy are surgical procedures consisting on opening the peripheral iris to allow normal circulation of fluid within the eye (glaucoma treatment). In the first case, a laser is used and no incision is needed. The second case is an incisional procedure



Iridotomy



Iridectomy



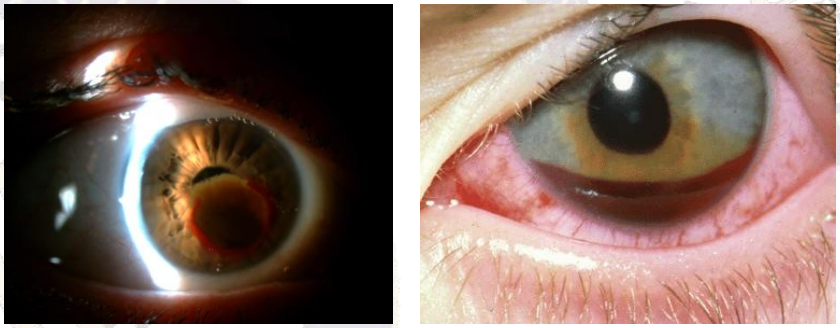
Iridectomy + lens

  - Effects on iris recognition systems
    - Iridotomies and iridectomies hardly affect iris recognition systems
      - The openings are done in the upper part of the iris, in the peripheral area, and are usually covered by the upper lid in order to avoid direct light incidence as much as possible. This way, they do not affect more than eyelids.
      - Only in the case they are as big as not enough usable iris area exist, recognition is not possible

# Iris conditions due to surgical procedures or trauma



- Hyphema
  - Description:
    - Bleeding in the eye anterior chamber
    - It can occur in rubeosis iridis (neovascularization in the iris), trauma, or, in rare cases, iridocyclitis



Hyphema

  - Effects on iris recognition systems
    - Successful iris recognition in this case depends on the location and extent of the hyphema
      - Correct segmentation and masking of the iris
      - Enough usable iris area

# Fraud-related considerations



- For security reasons, automatic iris recognition systems should recognize anomalous samples as such
- Sometimes, anomalous is understood as a synonym for fraudulent or risky. In this context, some considerations should be taken into account:
  - It is difficult to take advantage of an ocular pathology to try to *impersonate* a genuine user of an automatic iris recognition system
    - The fact that the iris is anomalous does not imply that its pattern matches another user iris pattern
    - Ocular pathologies could even help to better recognize a user (if allowed to be enrolled), because of the special characteristics of the sample. This can make impersonation even more difficult
  - It is possible to deliberately provoke some ocular pathologies to try to avoid an automatic iris recognition system (*disguise attack*)

    E.g. miosis/mydriasis can be easily artificially provoked by using a miotic/mydriatic agent in the form of eyedrops or by using drugs/alcohol
    - A single individual can try to be enrolled multiple times to use different identities
    - An enrolled user might deliberately provoke iris changes to avoid being recognized (criminal record, blacklist,...)
    - If an alternative recognition system, more easily spoofed, is used, an attacker might be successful

# Usability considerations



- Apart from recognition accuracy, *usability* and *user acceptance* are key issues when working with automatic recognition systems
- How can individual´s integrity and user´s acceptance be protected when an anomalous sample is detected?
  - Unless there is a high probability that the captured sample corresponds to a fake, *friendly policies* shall be used with the citizen involved *not to harm the individual integrity and user acceptance* of the system by provoking unnecessary alarms
    - Examples of friendly policies could be
      - Forwarding the person to use another recognition system
      - Seeking assistance from the supervisory agent
      - etc.

# Usability considerations



- How can iris image authenticity be measured?
  - Iris image authenticity can be considered as the probability (confidence value) that the iris image was captured from a real/live human eye without any alteration
    - Once an spoofing/liveness detection method is implemented, a confidence value shall be assigned to the sample. The confidence value *calculation* depends on the specific method, but its *value* should be within a *standardized range* in order to encourage recognition systems universality
      - ISO/IEC 1st Working Draft on "Anti-spoofing and liveness detection techniques" defines:
        - 4 assurance levels, being the 1st level little or no confidence in the asserted identity, and the 4th, very high confidence
        - A confidence score between 0 and 100
      - ISO/IEC 4th Working Draft 29794-6, "Biometric sample quality – Part 6: Iris image data" defines:
        - An iris image quality metric called "iris image authenticity"

# Conclusions

- Ocular pathologies are a delicate issue when working with automatic iris recognition systems
  - They can affect iris recognition systems performance
    - If the kind of pathology makes iris recognition possible, robust algorithms will be generally needed to obtain satisfactory results
      - E.g. In most cases a versatile segmentation method and accurate masking will be required
  - They can even compromise the system security
    - E.g. Disguise attacks
  - Usability and user acceptance could be also affected
- In order to minimize the impact...
  - Anomalous samples should be detected by the system
    - It is important to distinguish between a common impostor/system error and a person affected by a pathology
  - Friendly policies shall be used with a user whose sample is anomalous, unless there is a very high probability that the sample corresponds to a fake
    - Iris image authenticity can be measured by using a confidence value that defines the probability that the iris image is genuine

# Thank you for your attention
# Any question?

Inmaculada Tomeo-Reyes, Judith Liu-Jimenez, Sara Ceballos-Burgos*, Raul Sanchez-Reillo

University Group for Identification Technologies (GUTI)
Carlos III University of Madrid
Tlf.: +34 91 624 40 35 Fax: +34 91 624 94 30
{itomeo,jliu,rsreillo}@ing.uc3m.es

*RealVision Ophthalmology Clinic, Optometry Department
sceballos@realvision.es