Iris Attack Presentation

Ryan Quan, Vincent Goyette,
Tucker Mercier, Joseph Kuebler,
Dillon Coffey, Kenan Reu
Lumantas

A Brief History of Iris Recognition

- John Daugman published a paper in 1994 and patented the basis for iris recognition.
- Today at least 1.5 billion people worldwide are enrolled in iris recognition systems, with 1.2 billion being from India.
- Many countries use iris recognition for identification in addition to fingerprints and passports.

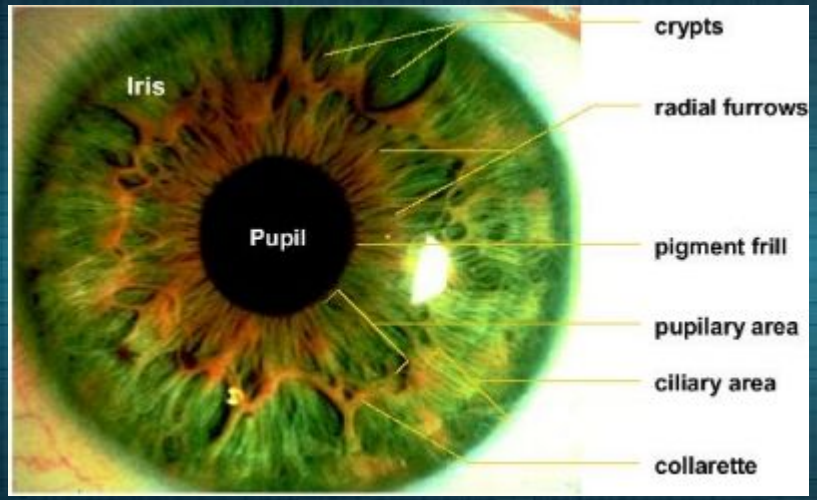
Generation of False Samples

- Paper Printouts: Use the iris scanner to capture a real iris, and then print the image. Use iris scanner to capture this "paper" iris
- Contact Lens: Scan a participant's iris while they are wearing a special textured contact lens
- Zero-Effort: Simply scan a participant's iris for comparison against a different iris that isn't theirs (or their opposite iris)
- Video Attack: Scan the subject's iris from a video (i.e. one you might be able to find on YouTube)
- Latent RGB Images: Scan a color image from an iris, like on a phone screen or laptop screen

About our System

- Device: **IriShield MK 2120U**
  - Infrared LED
  - Monocular
- Infrared illuminates Iris to pick up patterns not visible to human eye
- Acquire image and enhance by preprocessing, detecting the pupil and limbus circles, and normalizing the iris

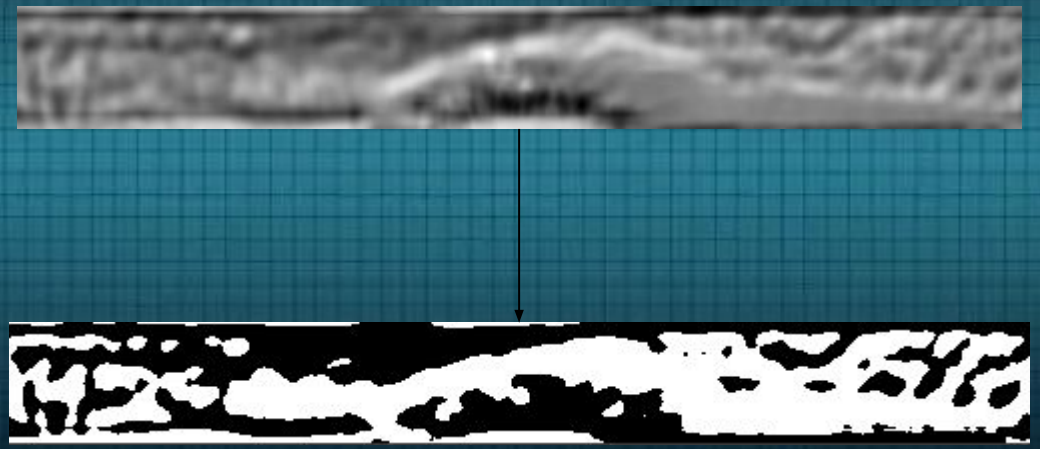
About our System (II)



- Next: Describe Iris' BSIF features (Binarized Statistical Image Features)
  - Patterns of image patches learned from eye-tracking data
- Finally: Compute hamming distance between two irises
- Decision Threshold: **.3274 (FMR = FNMR**

About our System (III)

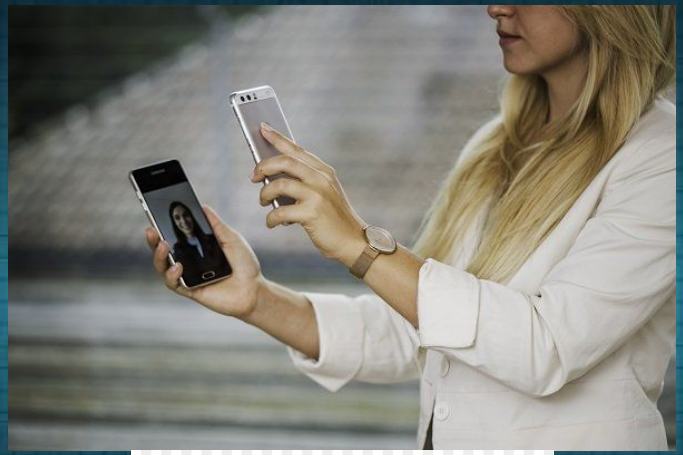
BSIF Filter Example



Attack Methods – Successful Scans

- Print Attack
  - Paper printouts of scans
- Textured Contact Lens Attack
  - Normal scan tested against scan of same subject wearing contact lens
- Zero-Effort Attack
  - Iris scan tested against that of another individual

Attack Methods – Unsuccessful Scans



Display Attack

- Video Attacks
- Latent RGB Images

Why not?

- Our system's image collection device leverages infrared LED, which presented problems for our phone screens

Report – Printout Attacks

- Method: Printed image of a genuine scan and attempted to fool our system
  - Resized scan to 120x90 pixels in order to register w/ device
  - Manually input dimensions using digital image software → pupil/limbus detection did not work with printout

```
def hack_02_detect_pupil_and_limbus(iris, view=False):
    return ((350,220,60), (315,220,140))
```

Results: Our system proved robust to printout attacks, measuring a hamming distance well above the genuine threshold.

Report – Zero Effort Attacks

Method: Comparisons of one user's iris scans against another, comparisons of one user's left eye vs his right eye

- One user v. another → Robust (~)
- Left eye v. right eye (no contact) → Robust

Findings: Despite still passing the impostor threshold, our system did surprisingly poor distinguishing between one user and another. Specifically, Ryan and Prof. Moreira's irises scored a hamming distance of .384. It did perform well distinguishing between right and left eye

Report – Contact Lens Attacks

Method: Two differently textured contact lens, three bases for comparison

- Lens v. no lens → Robust
- Lens 1 v. lens 2 → Not Robust
- Left eye v. right eye (same contact) → Partially robust

Finding: When wearing the same contact lens, the left eye and right eye produced more similar hamming distance than the lens vs. no lens comparison

Report – Contact Lens Attacks

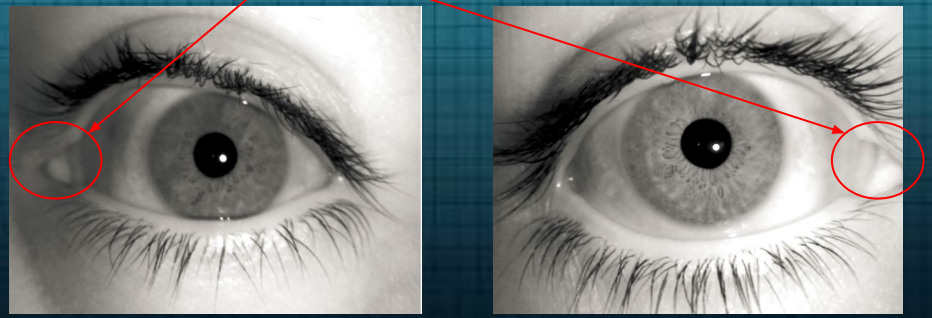
W/ Contact Lens

Note the distinct ridge outline from the contact lens

W/O Contact Lens

Proposed Fixes

1) Rework system to detect borderline between contact lens texture and real iris
   → Compare only on the basis of the true irises, able to better differentiate
2) Implement a feature to determine whether right or left eye is being scanned →
   Prevents the system from being confused between left and right →
   Based on location of caruncle



Left eye

Right eye

Proposed Fixes (Cont.)

3) Iris Template Fusion
- → Fuse together multiple captures of a user's iris
- → Features in fused image are weighted based on amount of noise in original
- → Pro: More robust comparisons
- → Con: Computationally Costly

4) Vary lighting and take multiple captures
- → Take one capture then shine additional light on the iris and capture again
- → Check for change in pupil size between two captures
- → Pro: Quickly and robustly defends against video, image, and paper attacks
- → Con: People may not like the extra light on their eyes

https://www.sciencedirect.com/science/article/pii/S2090447911000177

Quiz Time!

Thank you!
Questions?