* *Pintura de Rajib Roy, Case Investigation - 2012*

Digital Forensics

MO447 / MC919

Prof. Dr. Anderson Rocha

Microsoft Research Faculty Fellow
Affiliate Member, Brazilian Academy of Sciences
Reasoning for Complex Data (Recod) Lab.

anderson.rocha@ic.unicamp.br
http://www.ic.unicamp.br/~rocha

Reasoning for Complex Data (RECOD) Lab.
Institute of Computing,
University of Campinas (Unicamp)

Av. Albert Einstein, 1251 – Cidade Universitária
CEP 13083-970 • Campinas/SP – Brasil

RECOD

Spoofing in Biometrics

Techniques for creation and detection

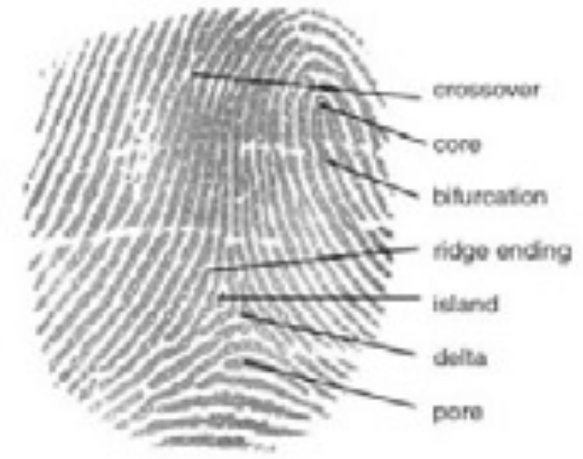
Outline

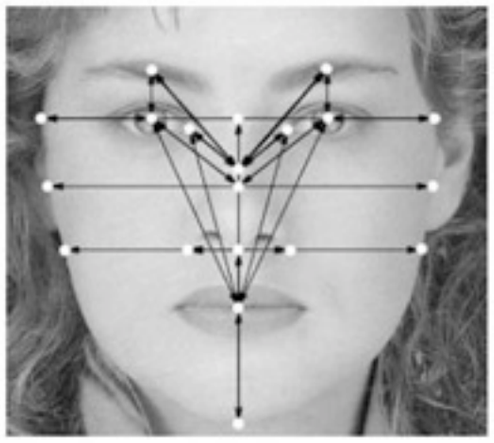
- Introduction
- Motivation
- General Vision
  - Fingerprints
  - Iris
  - Face
- Anti-spoof for fingerprints
- Anti-spoof for faces

Introduction

Introduction

- Biometrics: set of methods for identifying, automatically, an individual based on physical or behavioral traits
  - Fingerprint
  - Iris
  - Face





Biometric Systems

Nixon et al., 2007

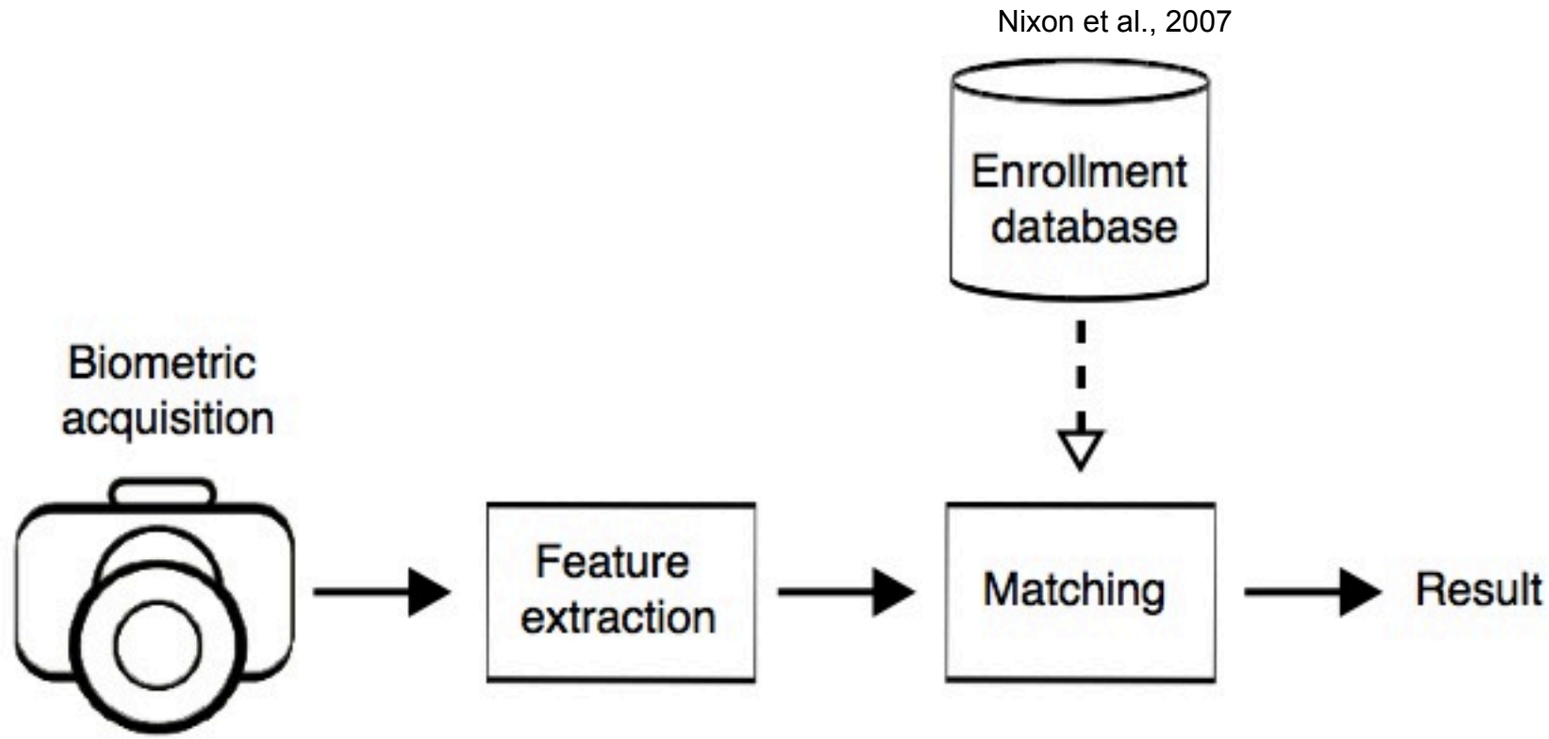


Fig. 1. An example of how biometric data travels to obtain a result.

Motivation

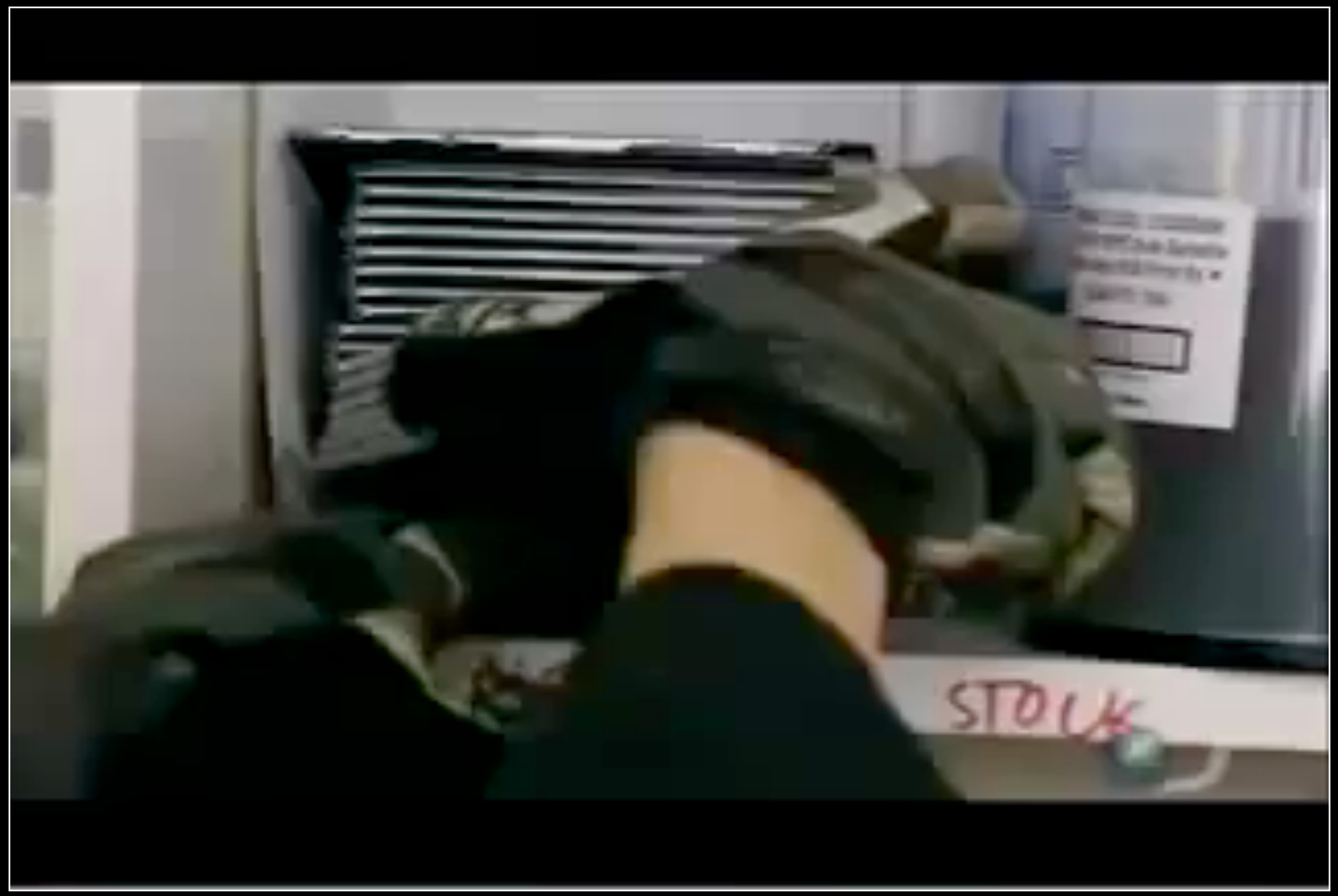
Motivation

- Biometrics burst
  [Thalheim et al. 2002] fingerprints are more common, facial recognition and voice recognition more acceptable and reliable; signature and way of typing still catching up

- Several research for optimizing how to differentiate humans

- Unfortunately, until recently, few research on method's reliability and how to avoid attacks

Video Demo


STOP

General Vision

[Nixon et al. 2007]

Complemented with [Thalheim et al. 2002]

Attacks

- Objective: to hide one identity or to obtain privileges of someone else
- Types:
  - Replay (sniffer in USB), Trojan (change the matcher or the DB)
  - Spoof
    - Consists of presenting to the sensor a fake biometric data
    - More susceptible (everyone has access to this part of the system)
    - Can be a fake gelatin/silicon finger with some else's fingerprint, a fake photo, or a contact lens
    - The 1st attacks on a biometric system dates of 1920s, by Albert Wehde, then an inmate at a Kansas penitentiary. He used his experience in photography and engraving to forge latent prints.

Attacks

- Recently, it has been shown that soft material artificial fingers could be falsely accepted as real fingers on widely available biometric fingerprint sensors.
- This pioneering work prompted the development of a research area focused on probing sensor vulnerabilities and finding countermeasures to attacks.

Attacks

- When the goal of the spoof is to gain access that another person has, the first step is to retrieve the fingerprint of that person – i.e., a person that is already enrolled.
- There are two approaches to acquiring an enrolled subject's fingerprint: cooperative retrieval and non-cooperative retrieval.

Attacks

- In cooperative retrieval, the subject allows the collection of one or more fingerprints. The fingerprint is usually collected by pressing the finger in a small amount of suitable material such as wax or dental mold material;
- the impression creates a mold from which artificial fingers can be cast.
- A variety of materials have been used for casting such as silicone, moldable plastic, plaster, clay, and dental molding material.

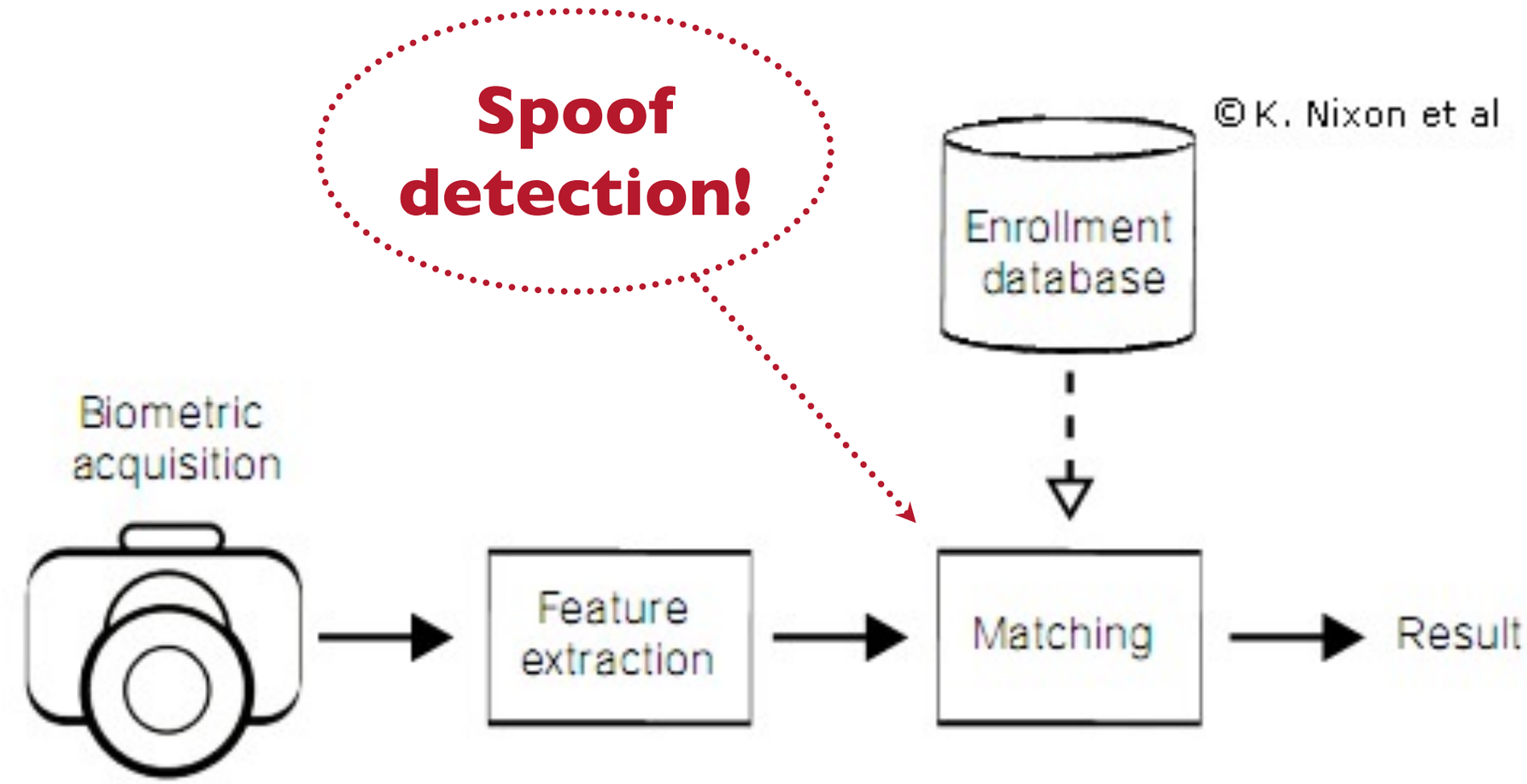
Attacks

- In a real-world scenario, it is highly unlikely that a person would agree to produce a mold from a finger.
- For non-cooperative retrieval, the method devised by Albert Wehde is still in use: today, printed circuit board etching is a successful molding technique for producing "gummy" and other soft material artificial fingers

Spoofing Detection

- Check if a biometric sample really comes from a real person (live). It can consider:
  - Use the same data used for identification
  - Collect more data in time
  - Employ additional hardware

Biometric System



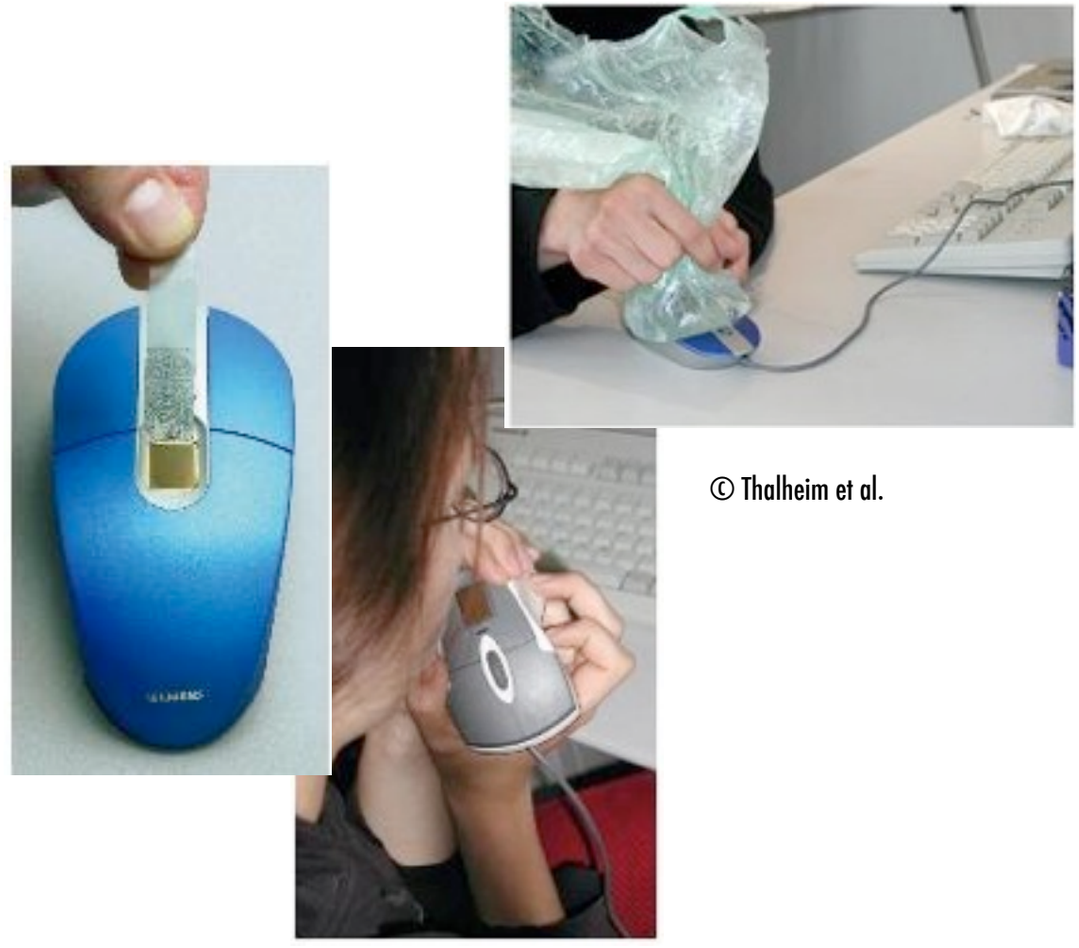
An example of how biometric data travels to obtain a result.

Fingerprints

“How To Fool a Fingerprint Security System As Easy As ABC”

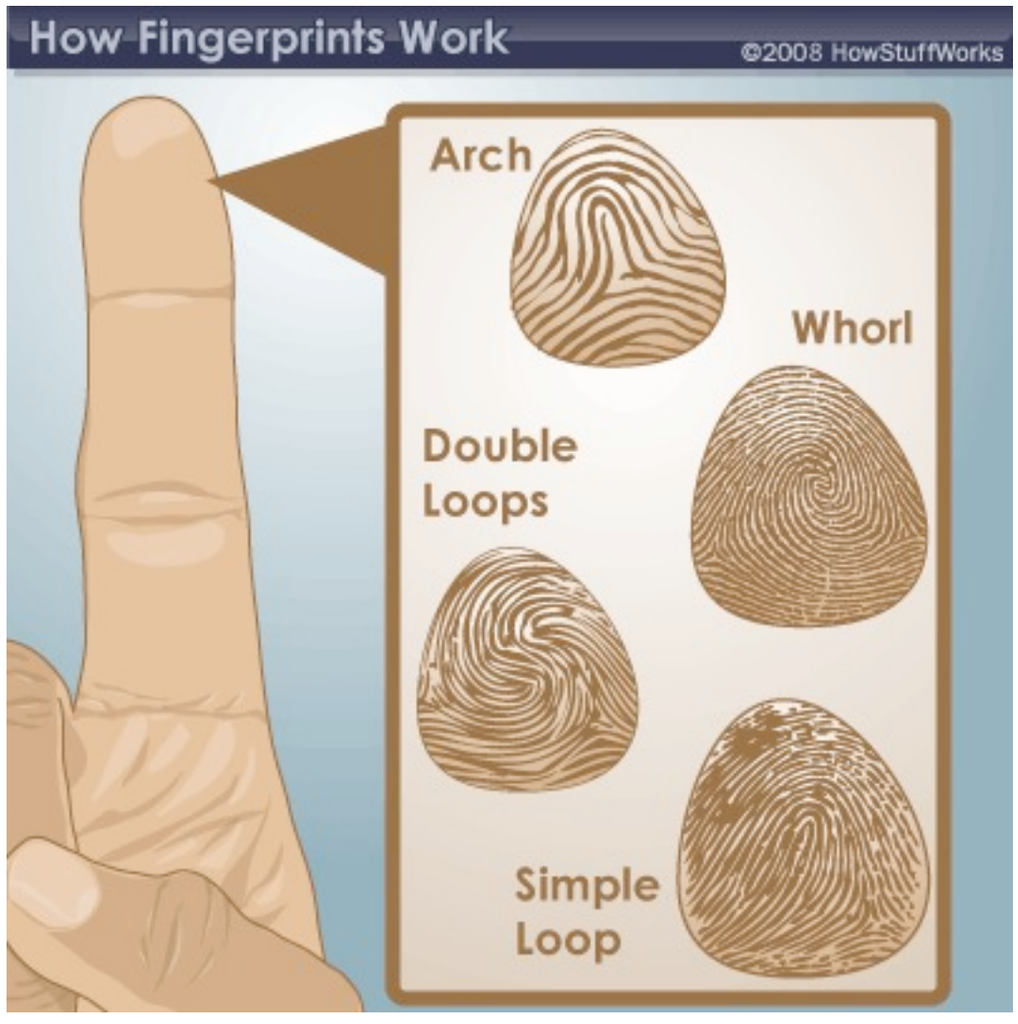
Spoof Creation

- How does it work?
  - Based on the position of details (*minutiae*), as terminations and bifurcations of the finger
    10 to 12 are enough to uniquely identify a person
- Spoofs
  - Latent fingerprints
    - Graphite powder and adhesive tape – almost 100% efficacy
    - Breath
      doesn't work always
    - Water bag
      Highly accurate



© Thalheim et al.

Spoof Creation



Spoof Creation

- More spoofs

© Nixon et al

- Artificial finger
  - Obtaining a fingerprint of someone else's
    in cooperation or using a photography of an enhanced/contrasted latent fingerprint
  - Mold it in a soft material
    silicon, plastic, gelatin, wax, dental powder
- Dismembered finger

Fingerprint acquisition sensors

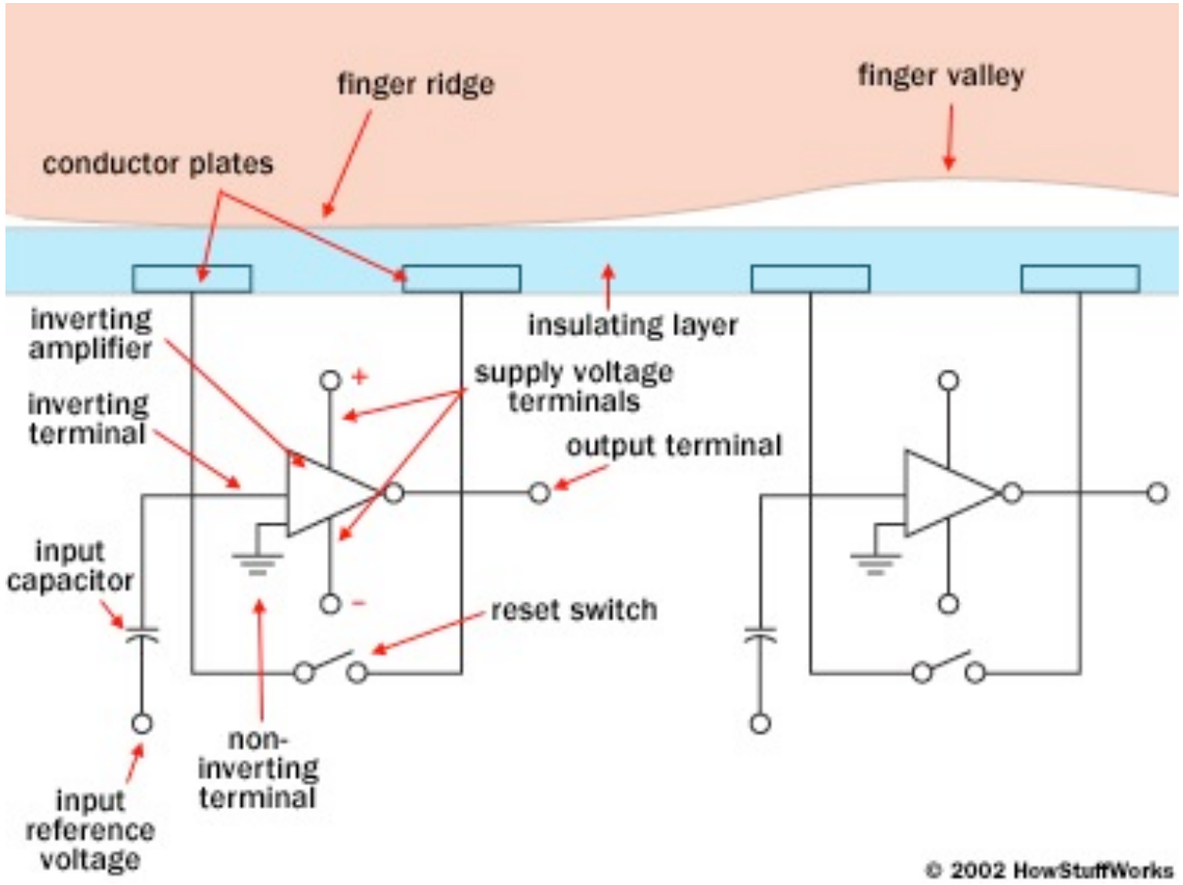
- **Optical**
  - **Total internal reflection (TIR):** different reflection patterns in the ridges (contact with the glass) and ridges espaces (air).
  - Attacks
    - artificial fingers with similar skin reflectance material
    - Latent fingerprints
      [Thalheim et al. 2002] adesive tapes, graphite powder
- **Multispectral imaging (MSI):** More details in a bit

Fingerprint acquisition sensors

- **Ultrasound:** difference of acoustic speed waves for ridges and the air
  - Attacks:
    - gelatin artificial fingers (same skin properties with respect to echo)

Fingerprint acquisition sensors

- **Capacitive:** difference in capacitance for the ridges
  - Attacks:
    - Latent fingerprints
      [Thalheim et al. 2002] Easy!
    - Gelatin artificial fingers



- **Thermic:** temperature difference for ridges (contact with glass) and non-ridge areas (air).
  - Attacks:
    - Artificial gelatin or silicon fingers
      [Thalheim et al. 2002] Harder to spoof than optical and capacitive sensors

Detecting Fingerprint Spoof

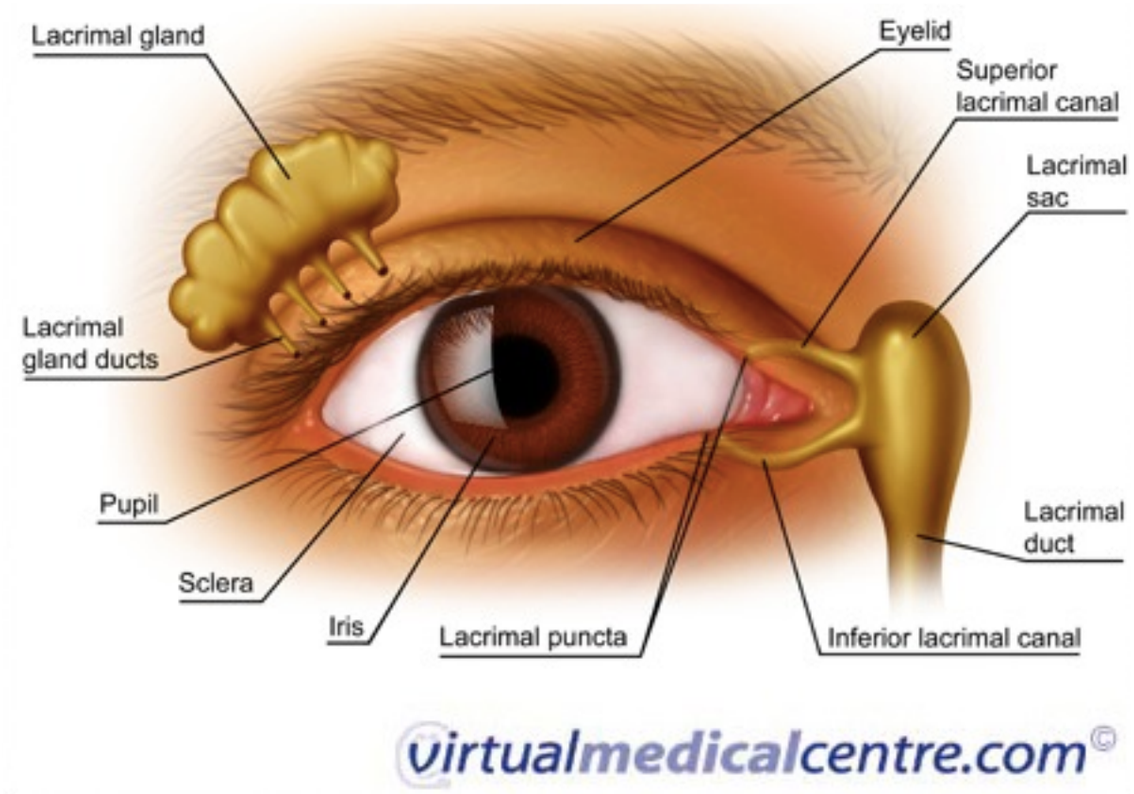
- Exudation/Sweating
  - Temporal changes in the amount of sweat in the finger's surface
  - Several images across time
  - Optical and capacitive sensors
- Skin absortion
  blood cells, hemoglobin, oxigen
- Skin temperature
  A spoof can be put in a real finger but part of the temperature will be dissipated
- Pulsation
  Varies from one person to another and according to the situation
- Other possibilities
  Skin electrical resistence, ultrasound detection of dermic structures

Iris

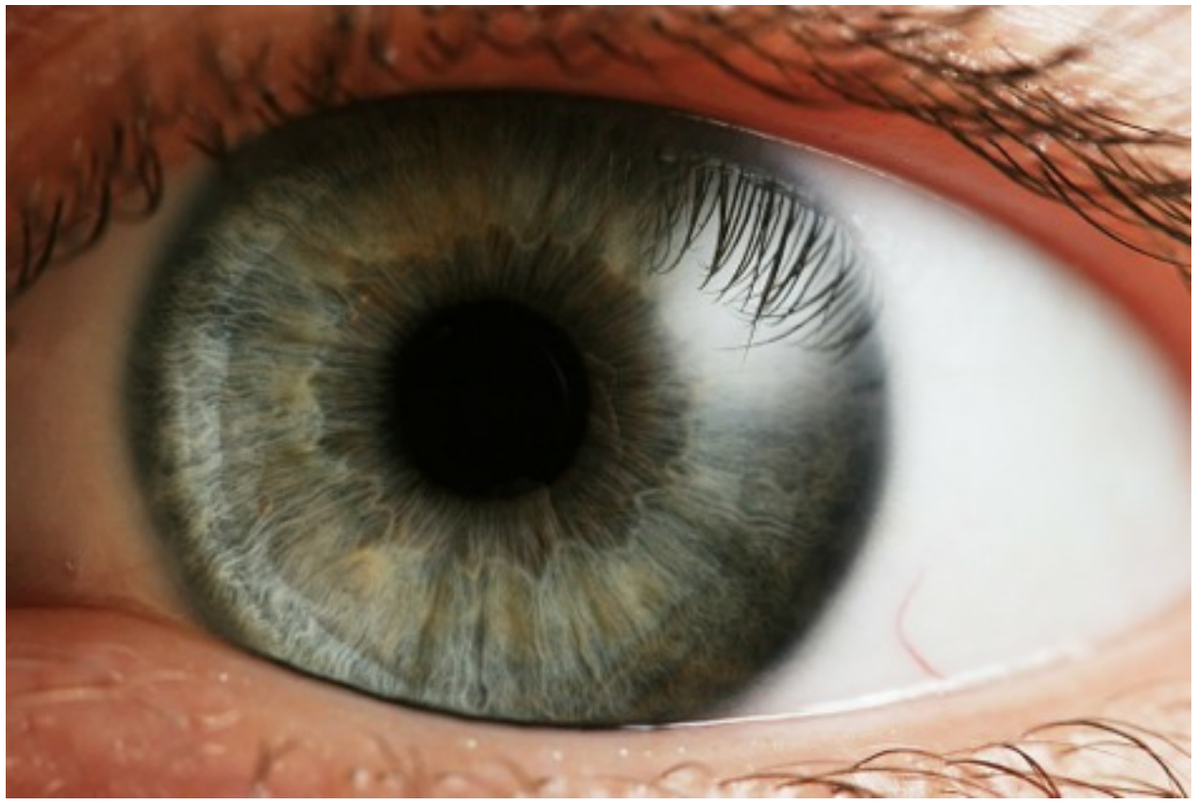
Spoof Creation

- How does it work
  - Based on the textured region of the eye around the pupil
  - Uses infrared light
  - Creates templates through filter banks

© Thalheim et al.



http://s3.amazonaws.com/



Attacks

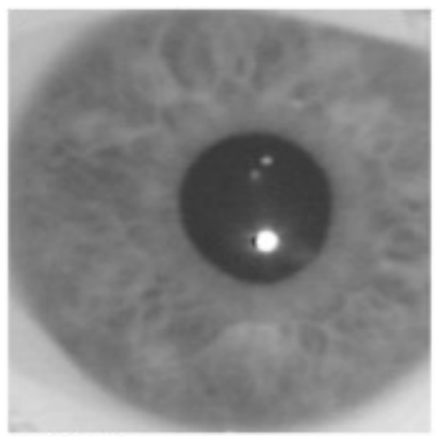
- Spoofs
  - High res photo or video of an eye [Thalheim et al. 2002] photo with an inkjet printer, 2400 x 1200 dpi, hole in the pupil
  - Iris pattern printed in contact lenses
  - Artificial 3D irises

© Thalheim et al.

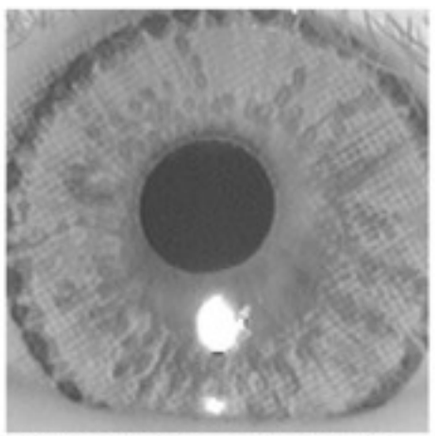
Attacks

- Spoofs

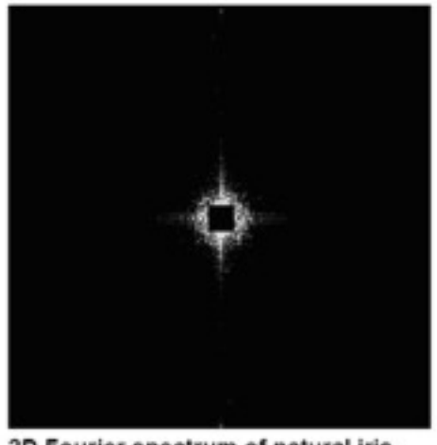
Nixon et al. 2007



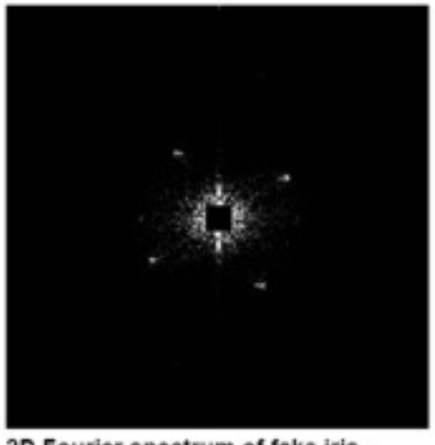
Natural iris



Fake iris printed on a contact lens



2D Fourier spectrum of natural iris



2D Fourier spectrum of fake iris

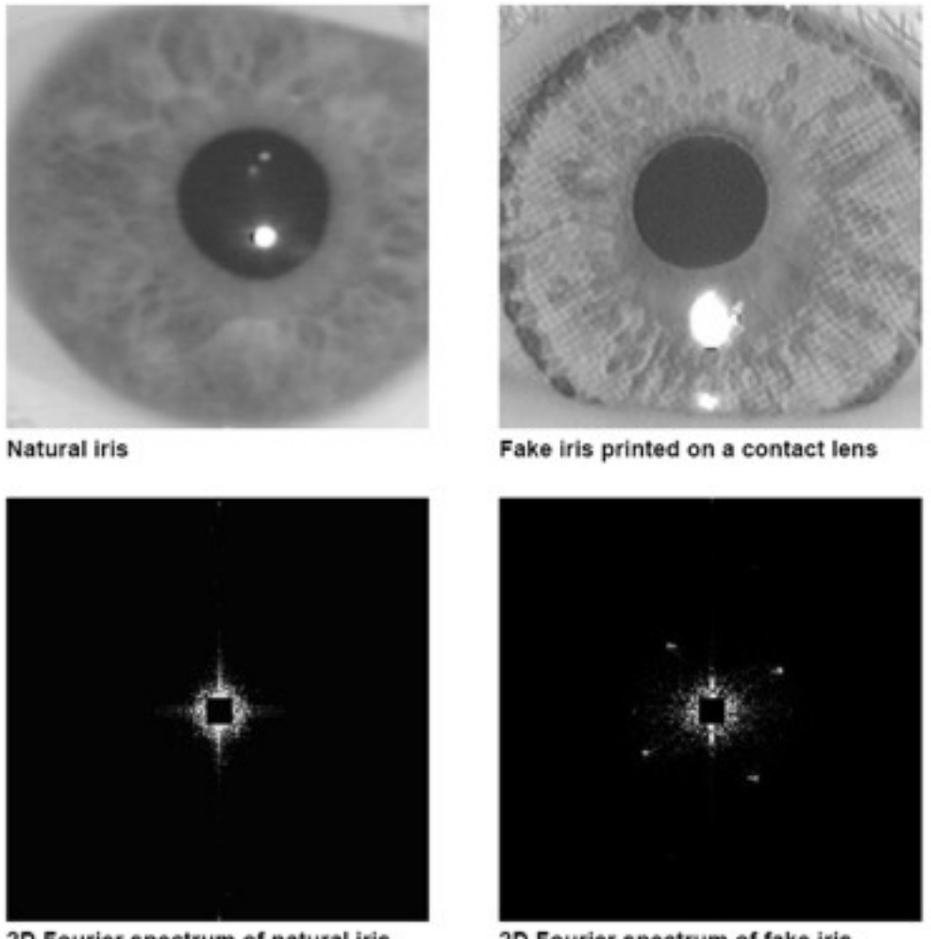
Images of a real and fake iris and their associated Fourier spectrums

Detecting Iris Spoofing

- Detect involuntary eye movements (*hippus*), or reaction to light, blinking
- Challenges (blink, move sideways)

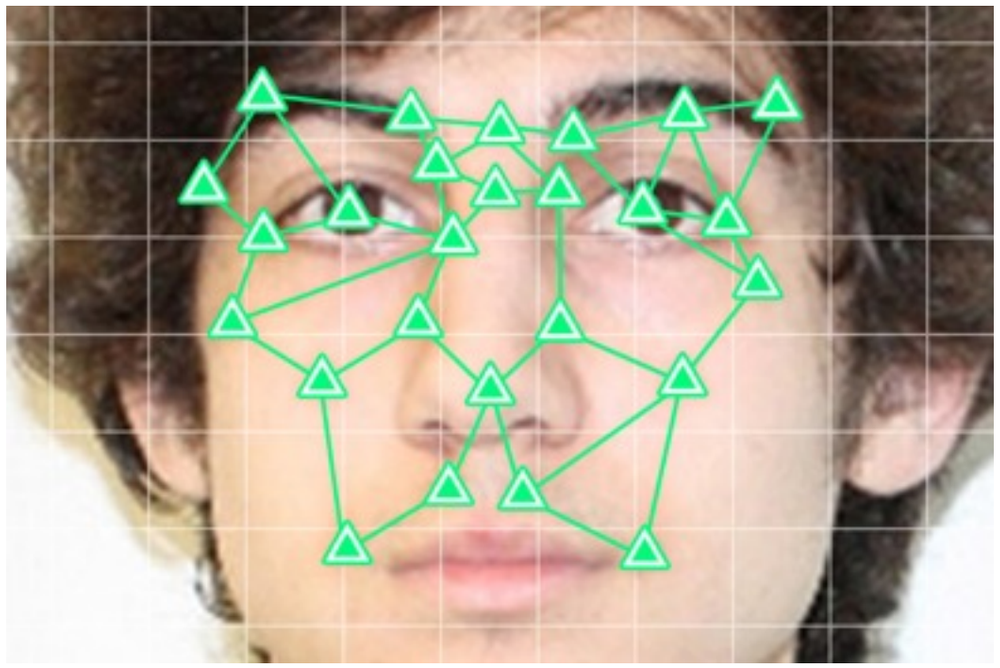
Detecting Iris Spoofing

- Fourier Analysis



Images of a real and fake iris and their associated Fourier spectrums [44].

Face



http://media.salon.com/

Spoof Creation

- How does it work
  - Take pictures under visible or infrared light
  - Matching uses different features
  - Can be 2D or 3D.

- Spoofs
  - Printed photos
  - Videos (notebook/cellphones)
  - 3D models

How to detect

- Involuntary movements of the eyes, head
- Blinking
- Skin texture, light reflection/refraction (active)

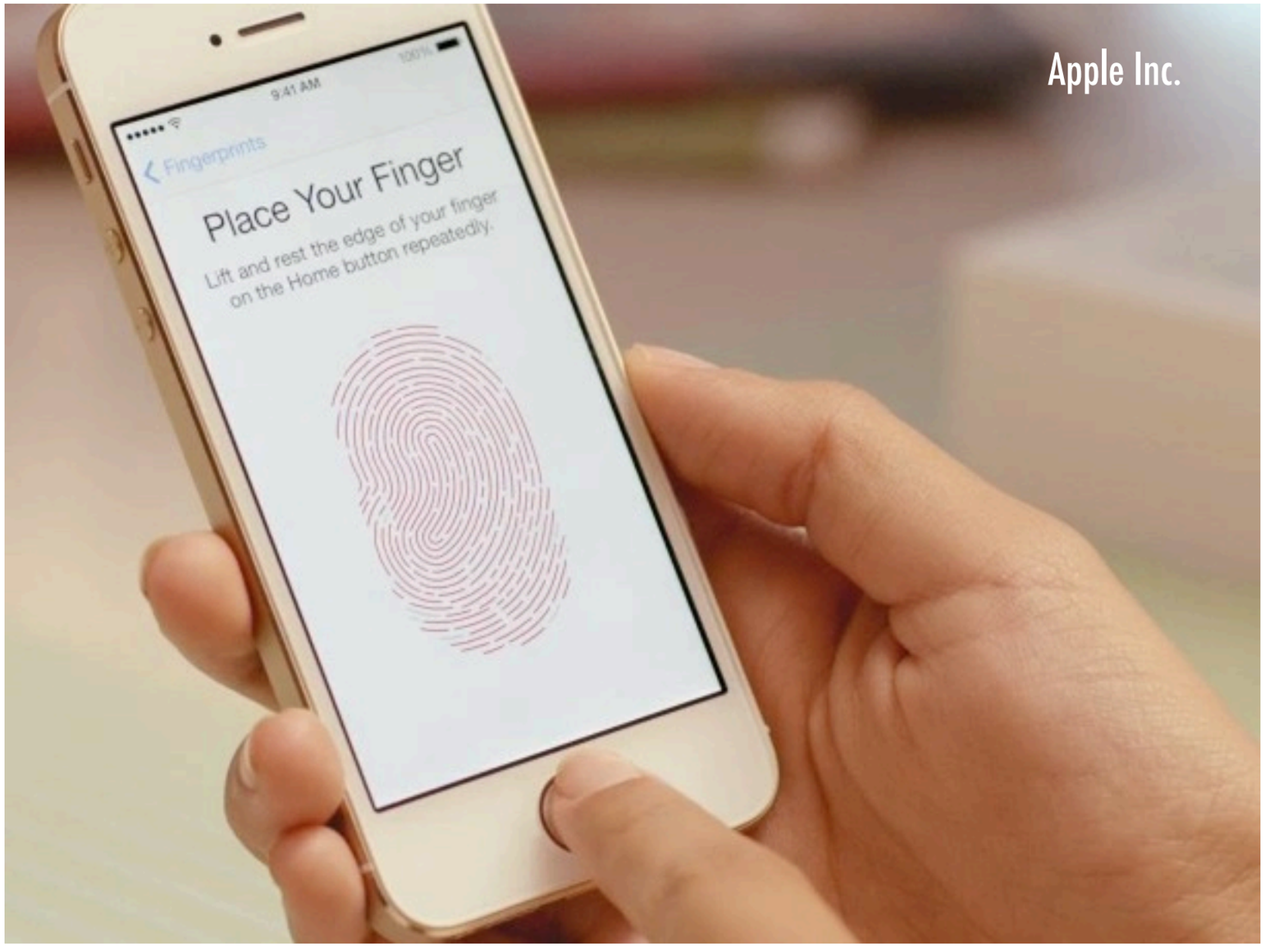
How to detect

- Light reflection 2D *x* 3D [Tan et al. 2010]
- Image Fourier Analysis
- 3D sensor
- Challenges (blinking, smiling, spelling)

Reflections

Reflections [Thalheim et al. 2002]

- Tested devices are not for high-security premises but
  - Cost x Benefit (how much does it cost to move to biometric authentication? Is it secure?)
  - Biometric devices are already able to fully replace passwords?


Apple Inc.
9:41 AM
Fingerprints
Place Your Finger
Lift and rest the edge of your finger on the Home button repeatedly.

Multispectral Imaging in Fingerprints

[Nixon et al. 2007]

Sensor

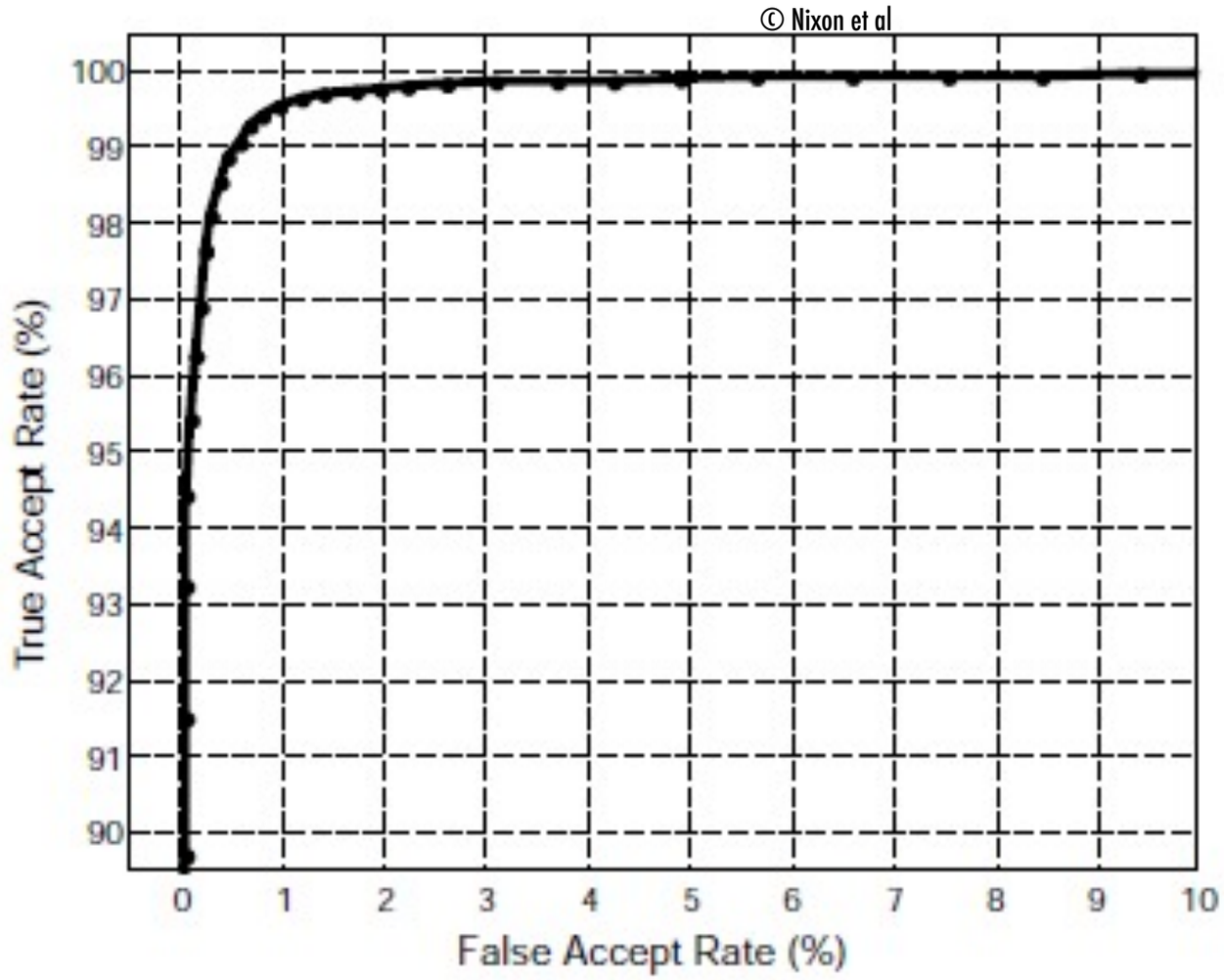
- Lumidigm MSI – J110
- Setup to acquire surface and sub-surface of the finger with different optical conditions
- Subsurface optical features discriminate real and fake fingers
- The combinations allow for different conditions of acquiring fingerprints (physiological and environmental)
  Strong lighting, humidity, poor finger contact with the sensor, dry skin

Spoof tests

- 3 sensors, 118 volunteers (18/80 yrs)
- 3-week visits (no special instruction to wash hands or prepare fingers)
- Total of 49 spoof types: latex, silicon, play-doh, glue, resin, gelatin, etc.
- Total of 17,454 collected images from real fingers and 27,486 fake ones.

Spoof tests

- TPR: 99.5%
- False positives: 0.9%.
- MSI sensors reasonably robust



Face Spoofing Detection in Detail

[Pinto et al., 2012]

Some conclusions

Conclusions

- Cat and mouse / Arm's race
- More research (independent of manufactures) are important
- There are promising anti-spoofing devices such as the Lumidigm MSI for fingerprints and [Tan et al. 2010] and [Pinto et al. 2012] for faces. But a lot of more research is necessary.

References

Referências

- **[Nixon et al. 2007]** Kristin Adair Nixon, Valerio Aimale, and Robert K. Rowe. Spoof detection schemes. White paper, Lumidigm Inc., 2007.

- **[Thalheim et al. 2002]** L. Thalheim, J. Krissler, P.-M. Ziegler; Body Check: Biometric Access Protection Devices and their Programs Put to the Test. Heise Online. November 2002

- **[Tan et al. 2010]** Tan, X.; Li, Y.; Liu, J.; Jiang, L.: Face Liveness Detection from A Single Image with Sparse Low Rank Bilinear Discriminative Model. In European Conference on Computer Vision (2010)

- **[Li et al. 2004]** Jiangwei Li , Yunhong Wang , Tieniu Tan , A. K. Jain: Live face detection based on the analysis of Fourier spectra. In Biometric Technology for Human Identification (2004)

- **[Pinto et al. 2012]** PINTO, Allan da Silva; PEDRINI, Hélio; SCHWARTZ, William Robson; ROCHA, Anderson. Video-Based Face Spoofing Detection through Visual Rhythm Analysis In: Conference on Graphics, Patterns and Images (Sibgrapi), 2012, Ouro Preto, Brazil.

Obrigado!

Thank you!