Face Spoofing

Thirimachos Bourlai

School of Electrical & Computer Engineering

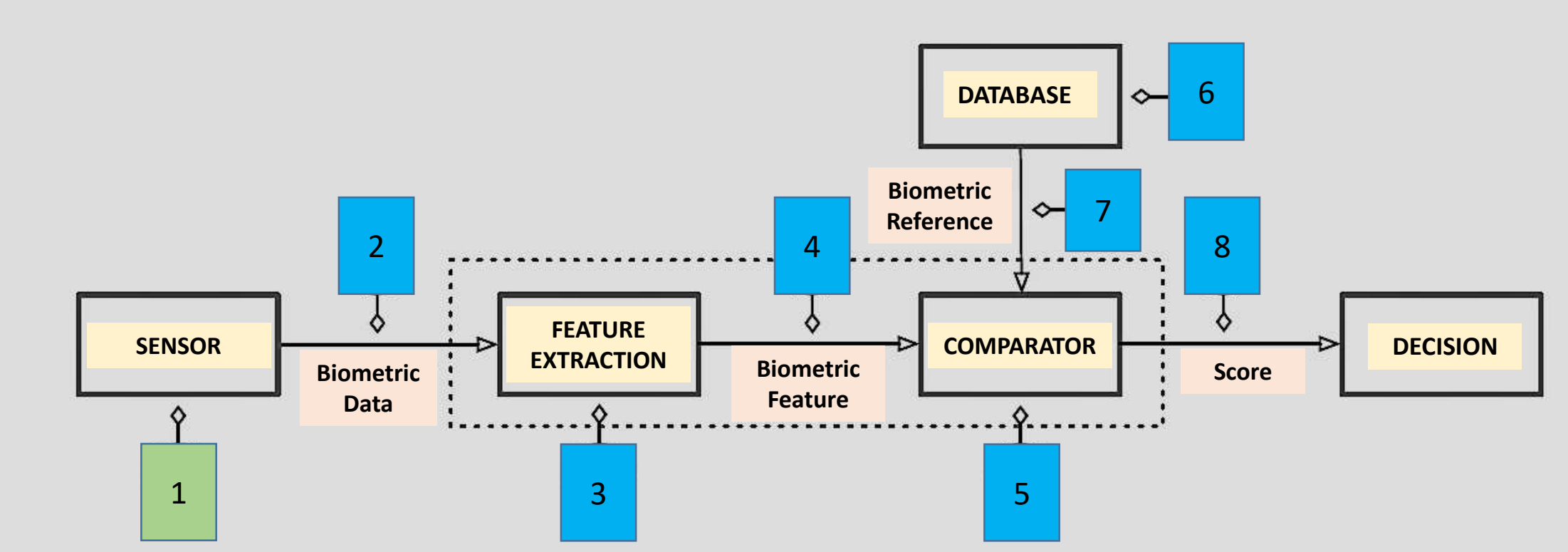
College of Engineering
UNIVERSITY OF GEORGIA

Phone: *832 713 9773*
Email: *Thirimachos.Bourlai@uga.edu*

Why is it important?

- Presentation Attack (PA) is a major threat
- PAs can be designed and applied by anyone
- No specific skills in computer science are required

BIOMETRICS SECURITY

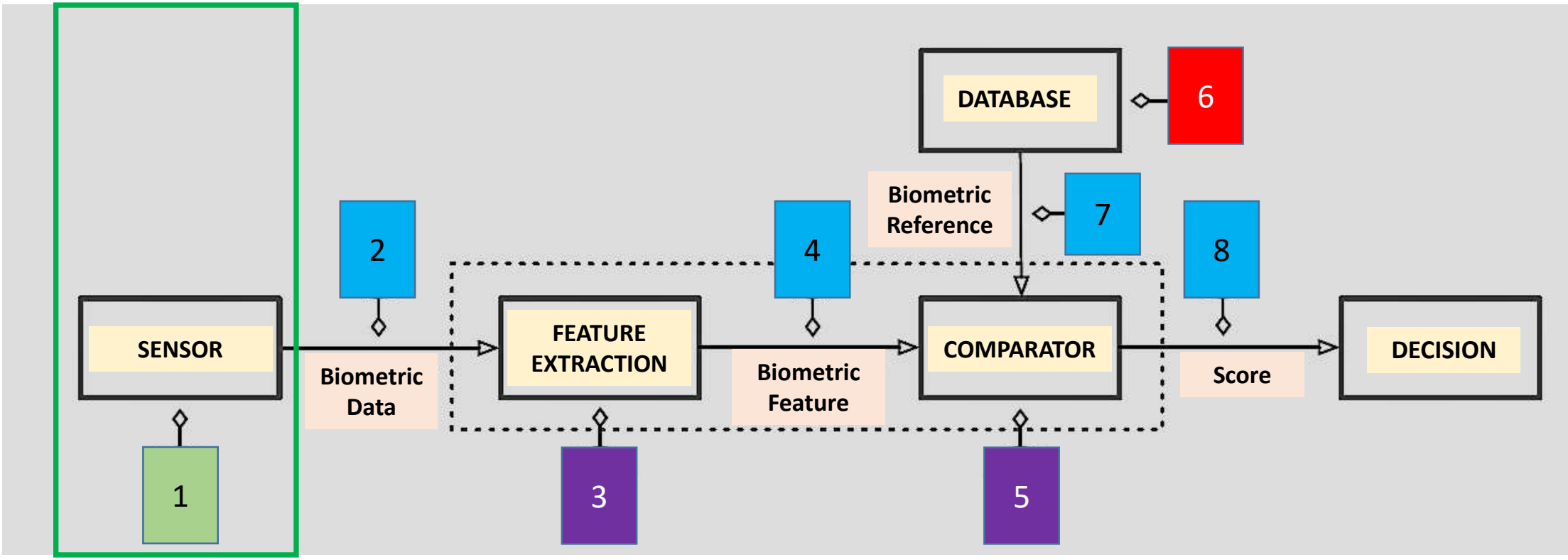


Direct Attacks

Indirect Attacks - Grouped

Source: NK Ratha et al., Enhancing security and privacy in biometrics-based authentication systems, IBM Systems Journal, 40(3):614634, 2001

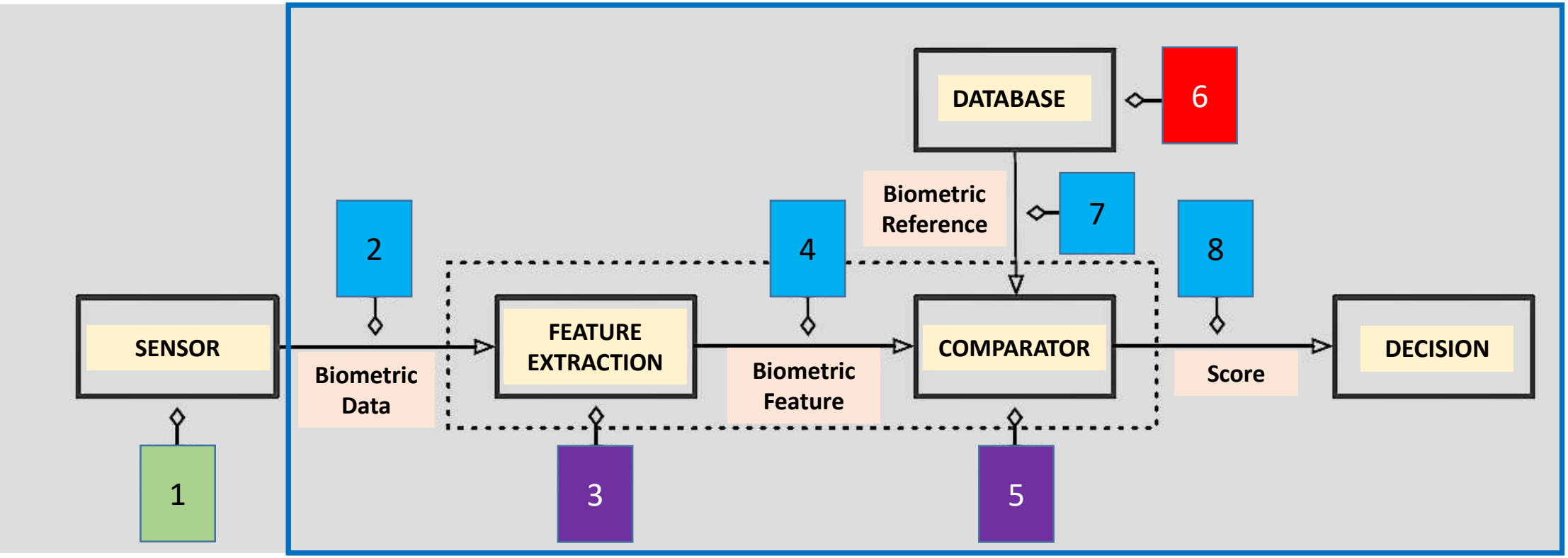
BIOMETRICS SECURITY



DIRECT Attacks

Source: NK Ratha et al., Enhancing security and privacy in biometrics-based authentication systems, IBM Systems Journal, 40(3):614634, 2001

BIOMETRICS SECURITY



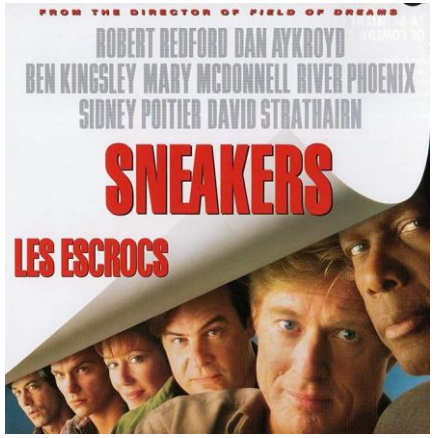
Indirect Attacks are performed inside the system in 3 different ways

Source: NK Ratha et al., Enhancing security and privacy in biometrics-based authentication systems, IBM Systems Journal, 40(3):614634, 2001

Presentation Attacks

Movies

MacGyver
(S02E01 1986)



Sneakers
1992

Demolition Man
1993

Minority Report
2002

Real Life

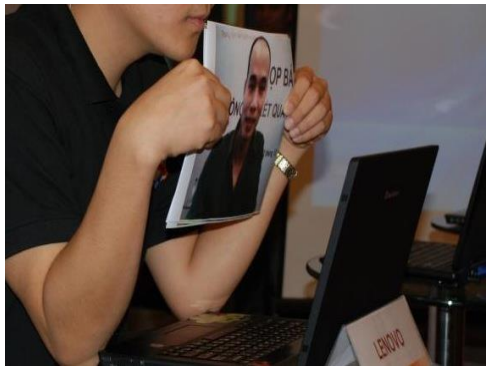
Bank Robbery
2010

HK - Vancouver
01/2011

Android Face Spoofing
2011 and 2012

Bank Robbery
2012

Presentation Attacks



Black Hat 2009*

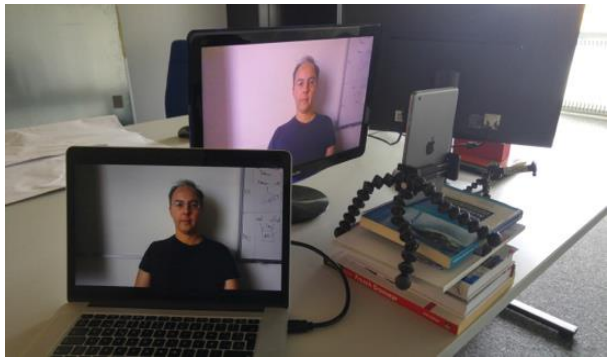
* D. Nguyen et al., Your Face Is NOT Your Password, 2009

2D face PA: printed paper

"Counter-Measures to Photo Attacks in Face Recognition: a public database and a baseline", A. Anjos and S. Marcel, IJCB, 2011.

2D face printed paper attacks:

- Image texture is lower
- Halftoning artifacts (printer)
- Other artifacts (horizontal lines)
- There is not localized motion (blinking)
- PA image perimeter can be recognizable

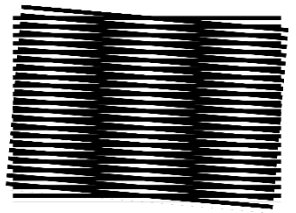


2D face PA: photo/video screen PA

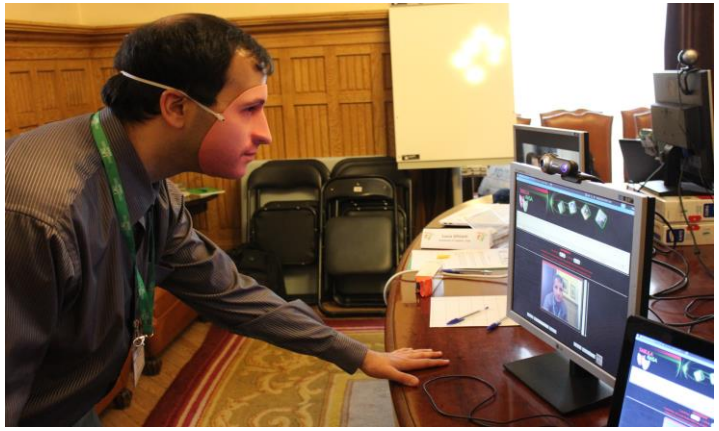
The REPLAY-MOBILE Face Presentation-Attack Database", A. Costa-Pazo and al., BioSig, 2016.

2D face photo/video replay:

- Image texture is blurred
- Color diversity reduced
- Moire' effect



Presentation Attacks



2D face PA: 3D mask (24bit color)

"Spoofing Face Recognition with 3D Masks", N. Erdogmus and S. Marcel, IEEE Transactions on Information Forensics and Security, 9(7):1084{1097, 2014.

2D face PA: 3D mask (PAPER) → ~ $20: Does not work

2D face PA: 3D masks (not paper)

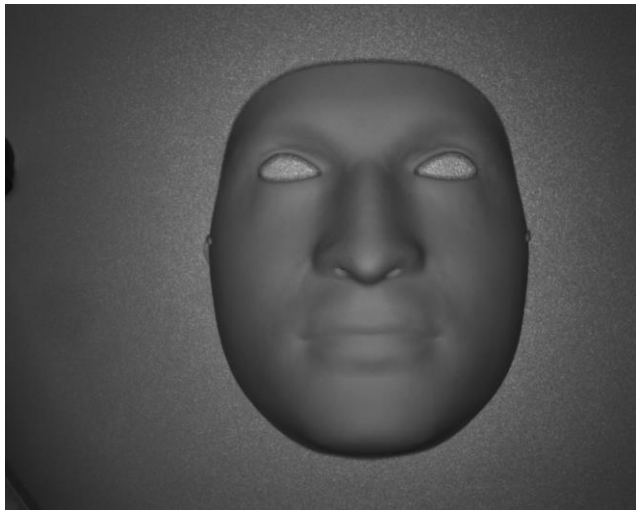
- Vivid colors
- No face-based skin motion (no lips or periocular/eye movement)

If the 3D masks have holes:

- There is localized motion (blinking) and can fool the system

Presentation Attacks

2D face PA: 3D mask with holes ~$400



2D face PA: 3D mask with holes - NIR

2D face PA -- 3D (mask with holes)

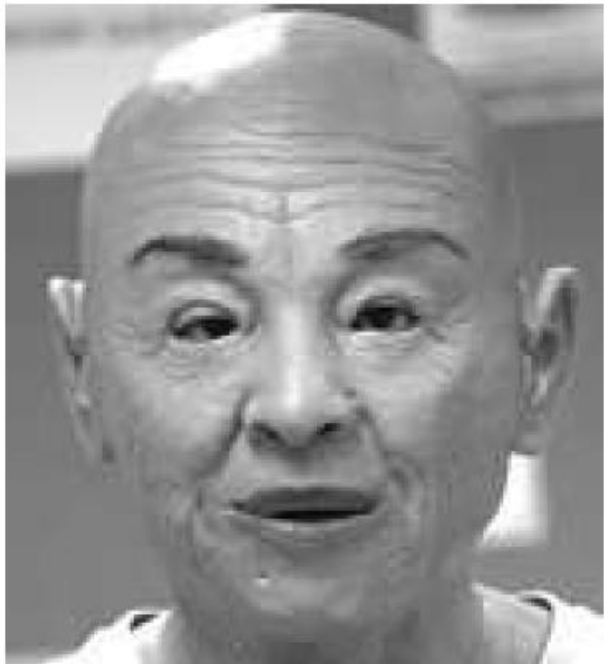
- They are generated to exhibit **bright colors**
- There is **no facial motion** present (global facial information is static)
- **Texture** information is absent in the **Near Infrared Band** (see bottom left figure)
- Clear in **thermal imaging**

"Spoofing Face Recognition with 3D Masks", N. Erdogmus and S. Marcel, IEEE Transactions on Information Forensics and Security, 9(7):1084{1097, 2014.

Presentation Attacks

2D/3D face PA: 3D silicon masks with holes ~$800

2D/3D face PA: 3D silicon CUSTOM MADE masks with holes ~$3,000



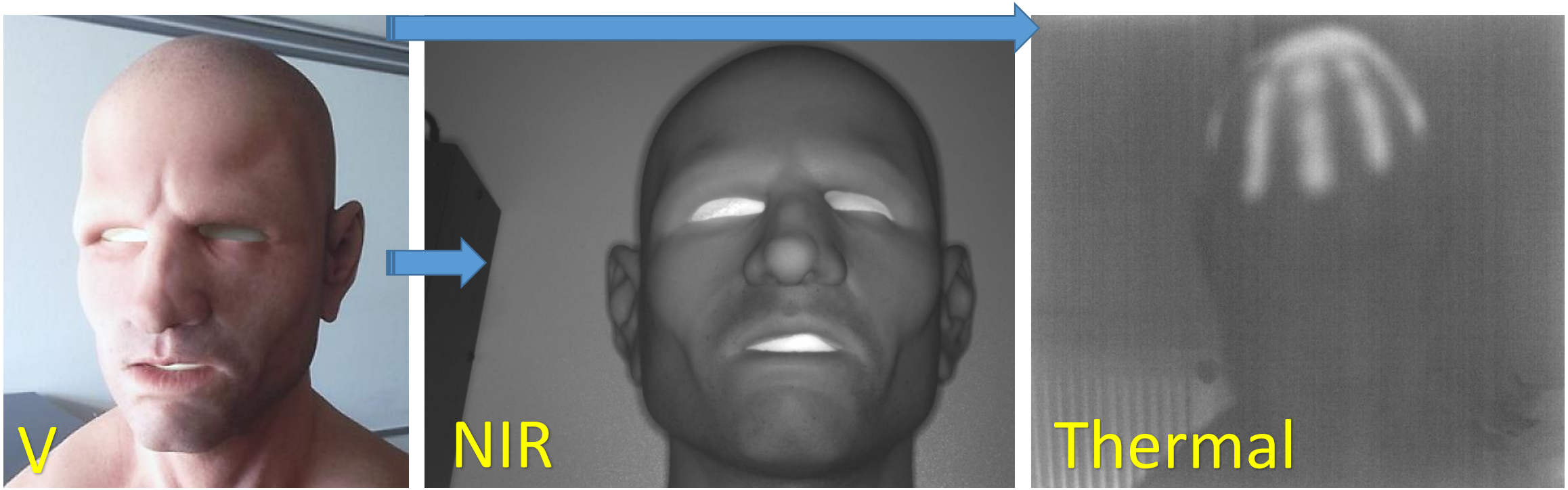
2D/3D face PA

Source: Liu, Kumar, “Detecting Presentation Attacks from 3D Face Masks under Multispectral Imaging”, CVPR 2018

Source: “What you can’t see can help you extended-range imaging for 3D-mask presentation attack detection", S. Battacharjee and al., BioSig, 2017.

Presentation Attacks

Silicon Masks / Various Spectra



2D/3D face PA: 3D silicon masks with holes ~$800

Texture of the silicon mask is clear in the Near Infrared

- Mask material absorbs the heat
- Compare to the human arm in the Thermal Band

Source: "What you can't see can help you extended-range imaging for 3D-mask presentation attack detection", S. Battacharjee and al., BioSig, 2017.

PAs – Three bands comparison

Source:

Sushil Bhattacharjee, Amir Mohammadi, Sébastien Marcel, Spoofing Deep Face Recognition with Custom Silicone Masks, BTAS, *October 2018*

Makeup Presentation Attacks

Source:

C. Rathgeb, P. Drozdowski, C. Busch, *Detection of Makeup Presentation Attacks based on Deep Face Representations*, Biometrics and Internet Security Research Group, *June 2020*

(a) before (b) after (c) target

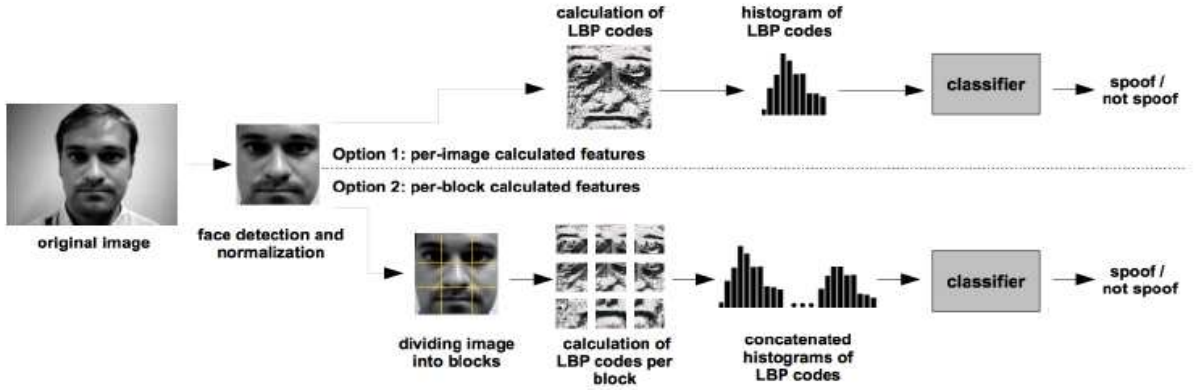
MAD (Morphing Attack Detection)

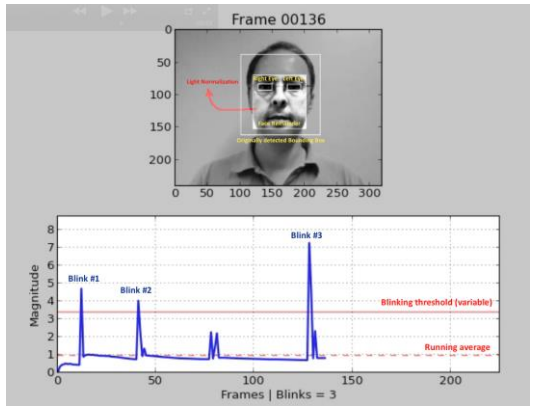
Illustration of a face morphing attack (left and right: source images, center: morphing attack) – Source - HERE.

U. Scherhag, J. Kunze, C. Rathgeb, C. Busch: "Face Morph Detection for Unknown Morphing Algorithms and Image Sources: A Multi-Scale Block Local Binary Pattern Fusion Approach", in IET Biometrics, (2020)

Presentation Attacks - Research

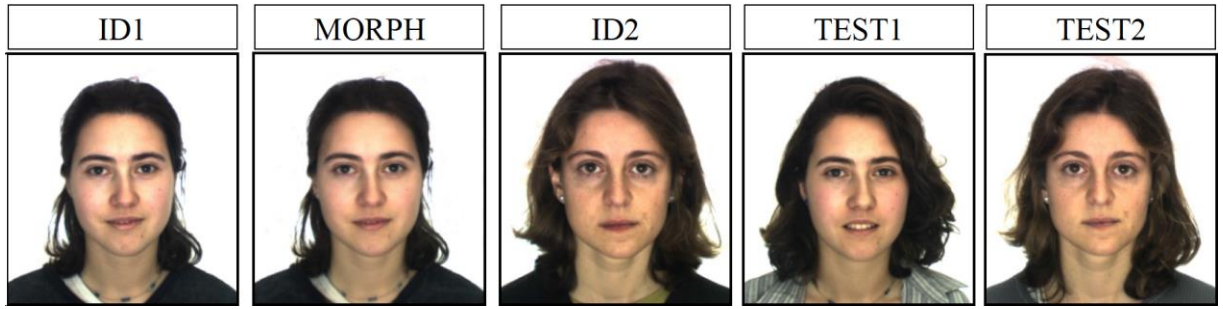
"On the effectiveness of local binary patterns (LBP) in face anti-spoofing", Chingovska et al., BioSig, **2012**.





"Motion-Based Counter-Measures to Photo Attacks in FR", A. Anjos and S. Marcel, IET Biometrics, **2013** – **Using Eye Blinking**

"The magic passport", M. Ferrara, A. Franco, D. Maltoni, IJCB **2014** - **morphing**

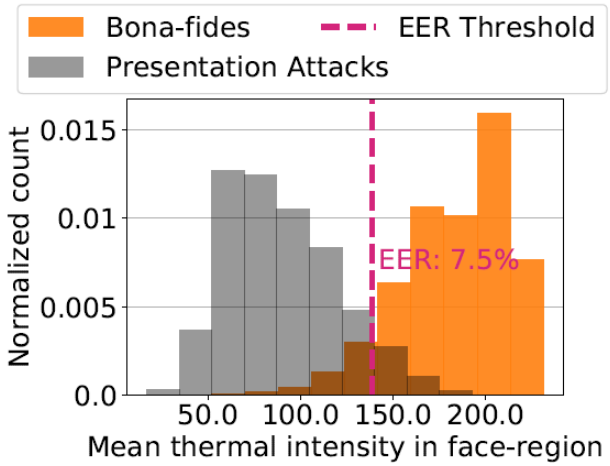


"**Live** face video vs. **spoof** face **video**: use of moire' patterns to detect replay video attacks", Patel et al., ICB, **2015**.

"**Image quality assessment** for fake biometric detection: Application to iris, fingerprint and FR", J. Galbally, S. Marcel, and J. Fierrez, IEEE Transactions on Image Processing, **2014**.

Presentation Attacks – Other Recent Work

"Spoofing Deep Face Recognition with Custom Silicone Masks", S. Battacharjee and al., BTAS, 2018.



- In 2016 a Morphing Attack Detection (MAD) mechanism was proposed by R. Raghavendra, K. Raja and C. Busch in the BTAS paper "Detecting Morphed Facial Images".
- **State of the art MAD** is investigated in the SOTAMD project and in the NIST FRVT MORPH study.

Avoiding Morphing Attacks

- "Passport applications should be done with live enrolment, meaning the facial photo is captured under supervision in the application process".
- "Only a few European countries (e.g. Sweden and Norway) have live enrolment in place"
- "Others (e.g. Germany) started within **2020** in recognition of the morphing attack problem."

https://christoph-busch.de/projects-mad.html

Face Presentation Attacks

Open source framework

Tools to run comparable/reproducible PAD experiments: http://pythonhosted.org/bob.pad.base

For Example: face PAD with native support for Replay Attack/Mobile and MSU MFSD

- **Source code**: https://gitlab.idiap.ch/bob/bob.pad.face
- **Documentation**:

  https://www.idiap.ch/software/bob/docs/bob/bob.pad.face/master/index.html

❖ Bob signal-processing and ML toolbox: https://www.idiap.ch/software/bob/

Source: BSS Presentation 2018: Biometric Spoofing and Anti-Spoofing, Presentation Attack Detection, Sebastien Marcel, Head of the Biometrics Security and Privacy group, http://www.idiap.ch/~marcel

Selected Literature and Sources

Book - Handbook of Biometric Anti-Spoofing, S. Marcel, Mark S. Nixon and Stan Z. Li (Eds.), Fingerprint, Iris, **Face**, Voice, Gait and Multi-Modal **Anti-Spoofing** -- http://link.springer.com/book/10.1007/978-1-4471-6524-8

Book - Face Recognition Across the Imaging Spectrum, ed. **T. Bourlai**, "**Face Recognition** Systems Under **Spoofing** Attacks", I. Chingovska, N. Erdogmus, A. Anjos, S. Marcel, Pages 165-194

IEEE Transactions on Information Forensics and Security (TIFS)

Special Issue on Biometric Spoofing and Countermeasures: many contributions relating to ocular, face, and voice modalities in addition to studies involving multiple biometric traits -- http://ieeexplore.ieee.org/document/7060794/

IEEE Signal Processing Magazine

Special Issue on Biometric Security and Privacy -- http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7192815

Other Links:

- https://www.informatik.hu-berlin.de/de/forschung/gebiete/viscom/res/morph
- https://christoph-busch.de/projects-mad.html

Acknowledgements

https://www.ntnu.edu/aimt/swan

IARPA ODIN BATL

- Swiss Center for Biometrics Research and Testing
- Sebastien Marcel www.idiap.ch/~marcel
- M. Tistarelli – Professor; Biometrics Summer School

milab.uga.edu

UNIVERSITY OF GEORGIA

MULTISPECTRAL IMAGERY LAB

THANK YOU

Office: 706.542-0940
Thirimachos.Bourlai@uga.edu

Member, Academic, Research and Innovation Group, Biometrics Institute

MILAB

Visit us at:

milab.uga.edu