NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

# Red Bleed: A Pragmatic Near-Infrared Presentation Attack on Facial Biometric Authentication Systems

*Bowen Hu, Kuo Wang and Chip Hong Chang*

*Presenter: Bowen Hu*

*15 Aug 2025*

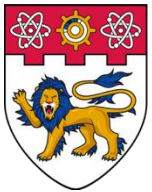

# Red Bleed: A Pragmatic Near-Infrared Presentation Attack on Facial Biometric Authentication Systems

Bowen Hu, Kuo Wang and Chip Hong Chang

Accepted by USENIX Security 2025

Seattle, WA, USA
Aug 15, 2025

CICS

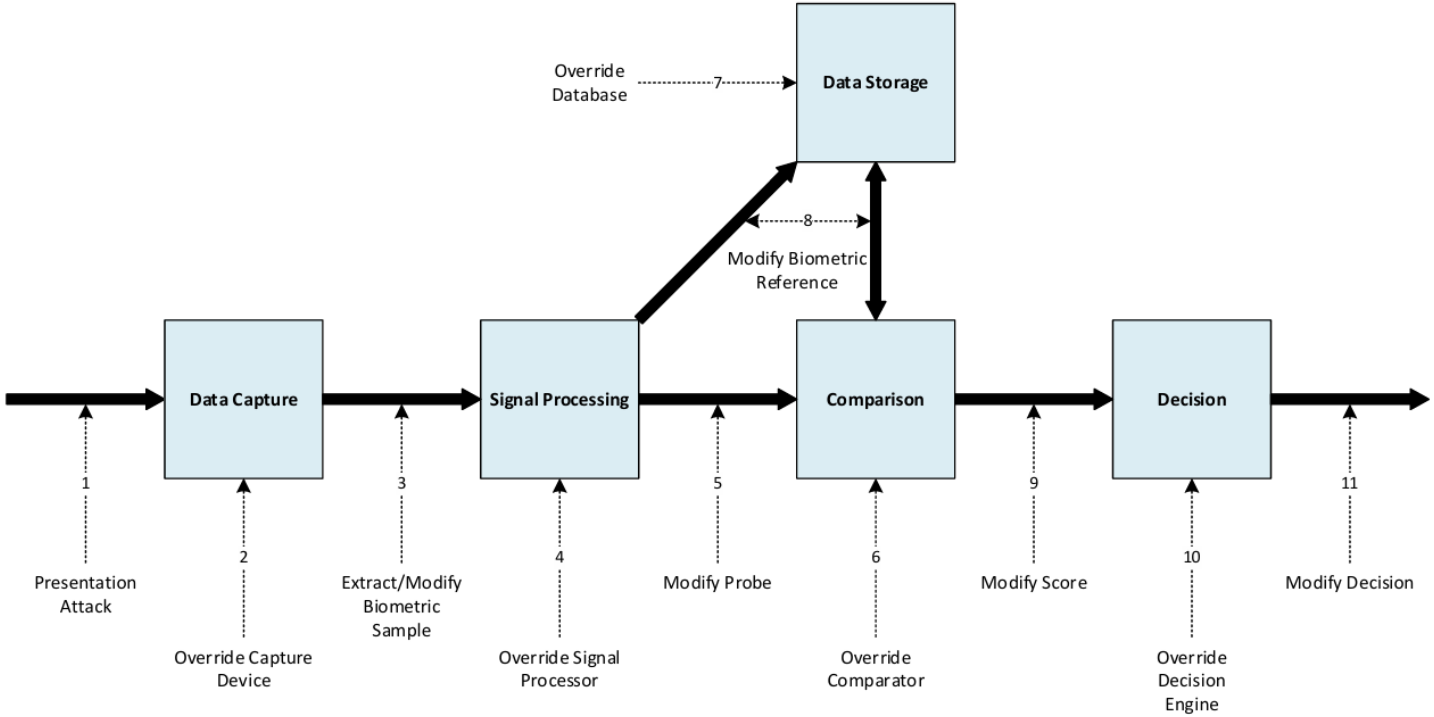


NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

# Face Recognition - The Most Popular Biometric Today

- Unique and Universal
- Contactless, passive and non-intrusive
- Easy to use and fast
- Low cost
- High acceptance
- Widely used for
  - Verification (Personal ID)
  - Identification (Surveillance, Forensic)
  - Monitoring (Robots, personalized care)
- Facial recognition drivers:
  - Sensor technology
  - Artificial intelligent
  - Hardware acceleration
  - ...

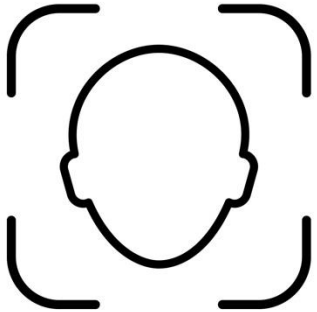
# Scheme of a Generic Face Recognition System




https://www.nist.gov/system/files/nstic-strength-authentication-discussion-draft.pdf

# Vulnerability of Face Recognition Systems

- Specialty of the Vulnerability of Face Recognition Systems:



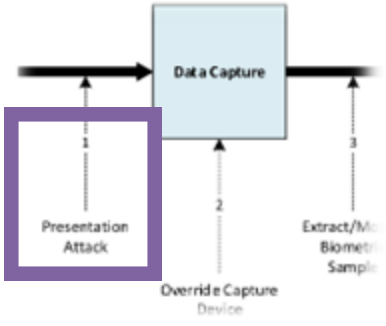
⚠ Face data is easy to obtain

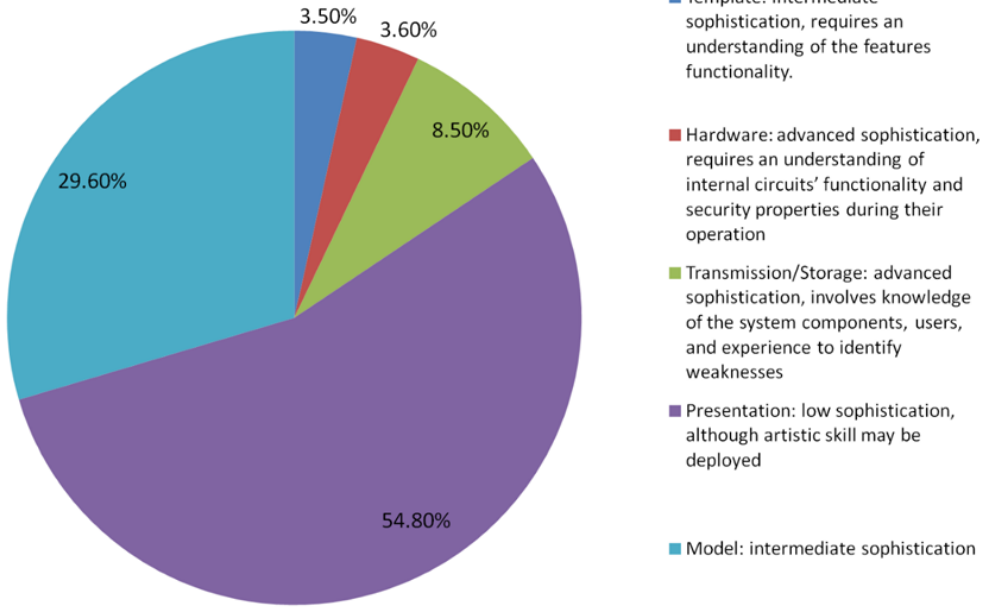
⚠ Face artifacts are easy to generate

⚠ Face is the “PASSWORD” that cannot be changed

# Vulnerability of Face Recognition Systems: Presentation Attack

- Attacks by proportion groups.
- From 2018–2021, studies focus on the presentation attack more frequently than any other sort of attack.



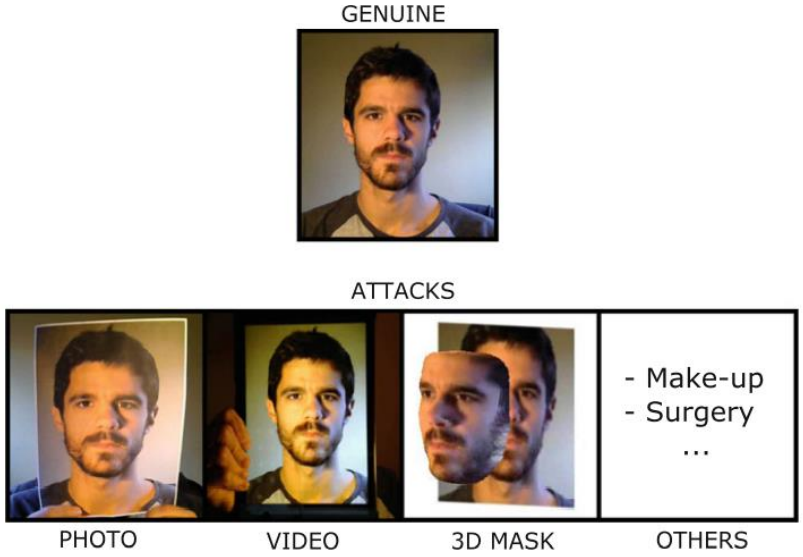






https://www.turing.ac.uk/sites/default/files/2023-05/attacks_against_facial_recognition_systems_technical_briefing_final_copyedit.pdf

# Presentation Attacks

- Printed photo presentation
- Display photo presentation
- Video presentation
- 3D mask presentation
- …

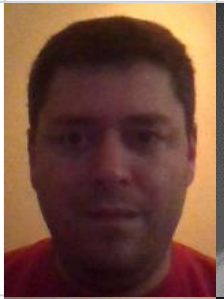





https://link.springer.com/chapter/10.1007/978-3-319-92627-8_9

# Face Recognition with Near-Infrared

- Traditional color recognition systems rely on turning up the brightness, exposure, or other settings to create a useable image – all of which expose artifacts that impact the robustness of the system.
- In contrast, near infrared images are consistent across ambient lighting scenarios

| Scenario | Color Image from integrated Camera | IR Image from Microsoft Reference Sensor |
|---|---|---|
| Low light representative of watching TV or giving a PowerPoint presentation |  |  |
| Side lighting when sitting near a window or desk lamp |  |  |



https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello-face-authentication

# Face Recognition with Near-Infrared

- NIR for anti-spoofing
- NIR doesn't display in photos and displays

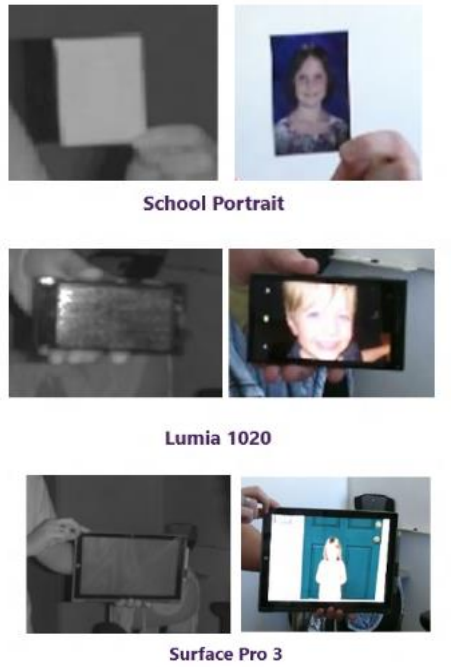





https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello-face-authentication

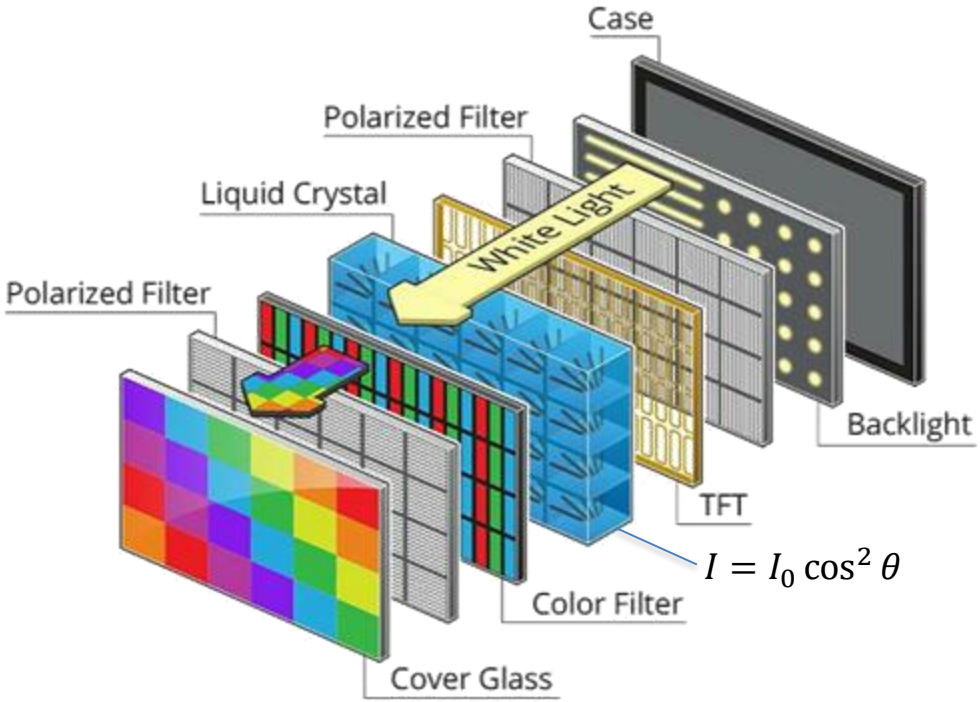
# Face Recognition with Near-Infrared

- NIR for anti-spoofing
- NIR doesn't display in photos and displays

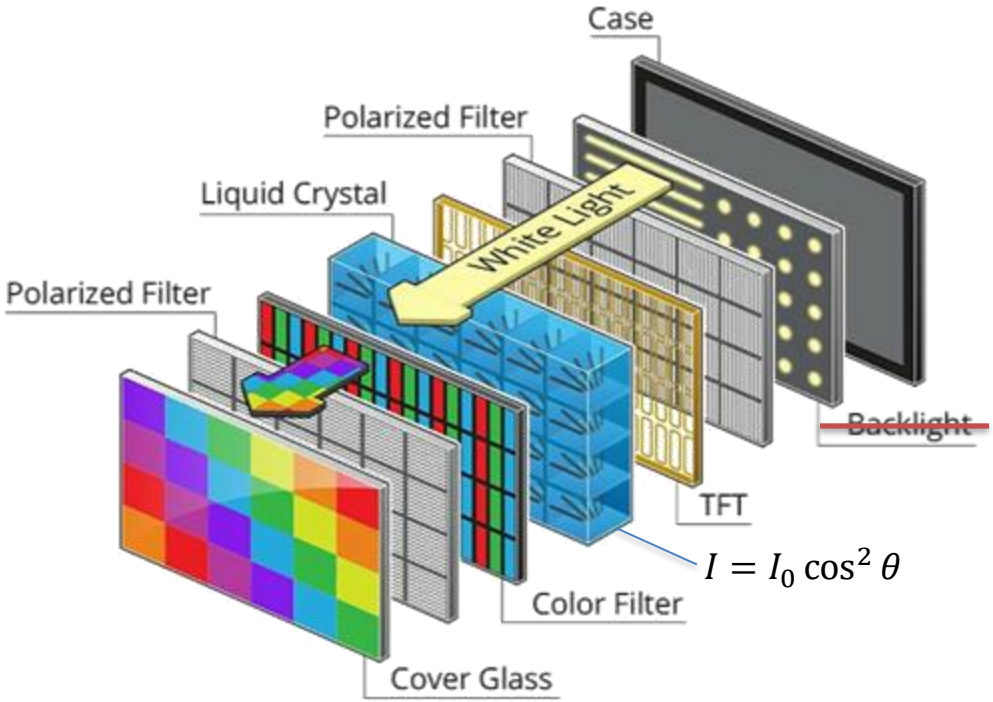



https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello-face-authentication

# Liquid Crystal Display (LCD)

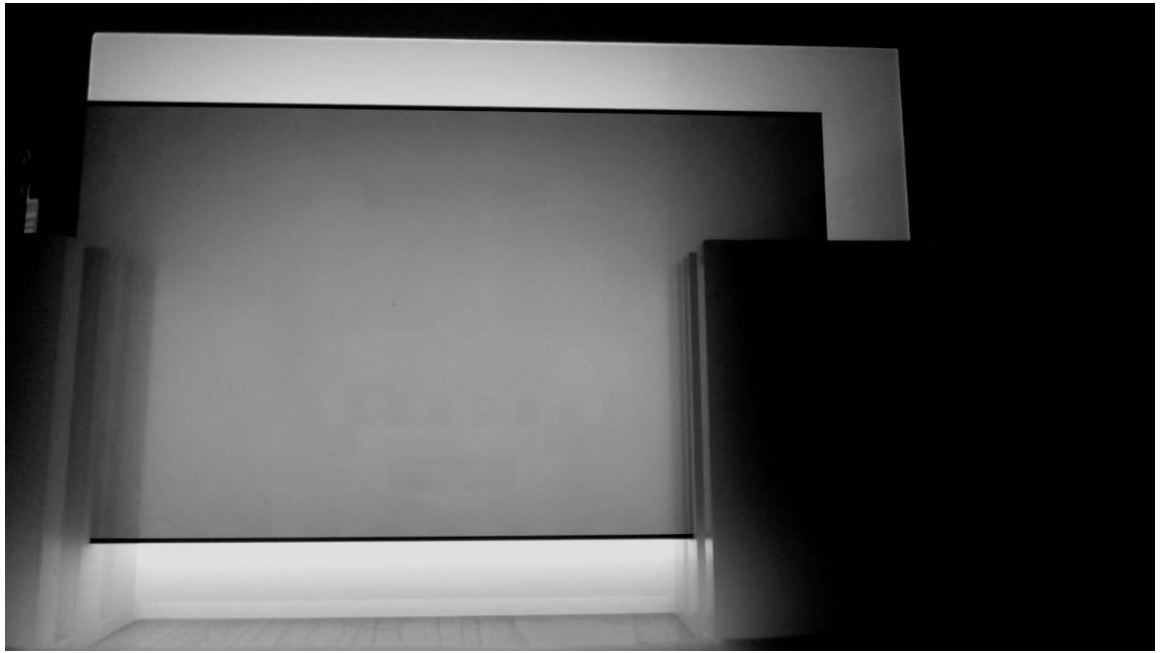



# Liquid Crystal Display (LCD)



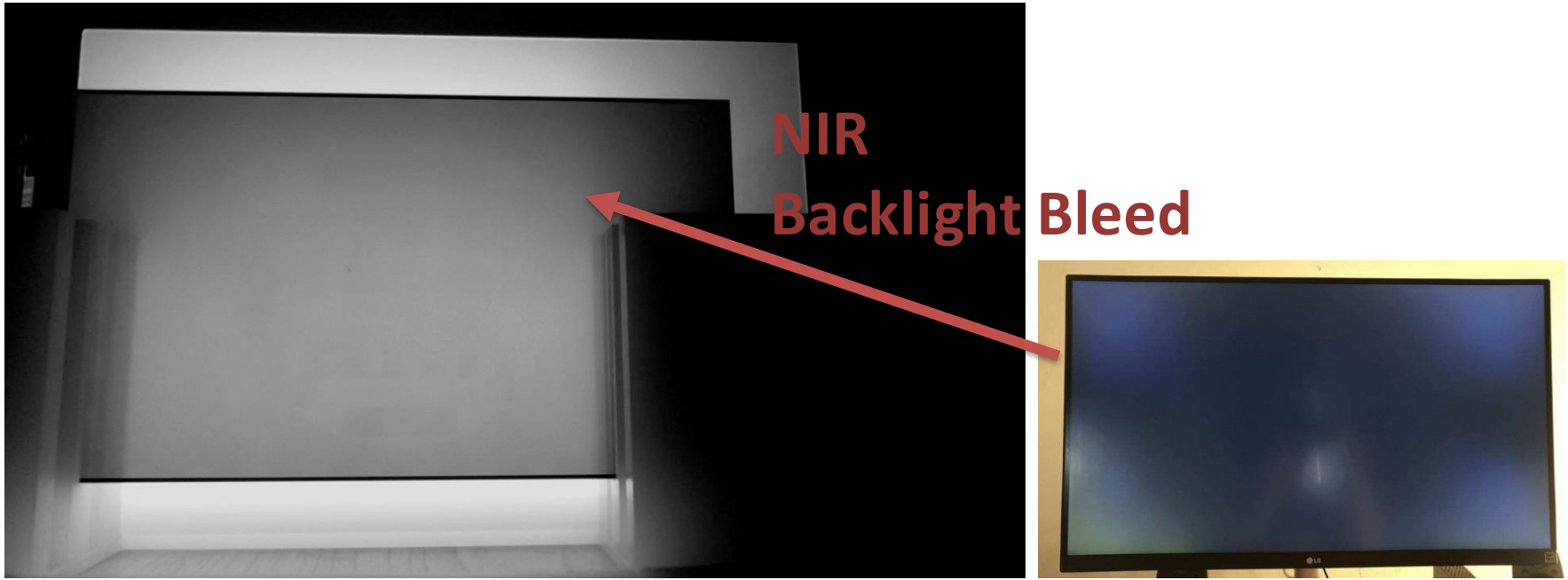

What if we swap it for the NIR backlight?

# Liquid Crystal Display with NIR Backlight



With only the backlight changed to NIR, some very shallow patterns can be seen on the screen.

# Liquid Crystal Display with NIR Backlight

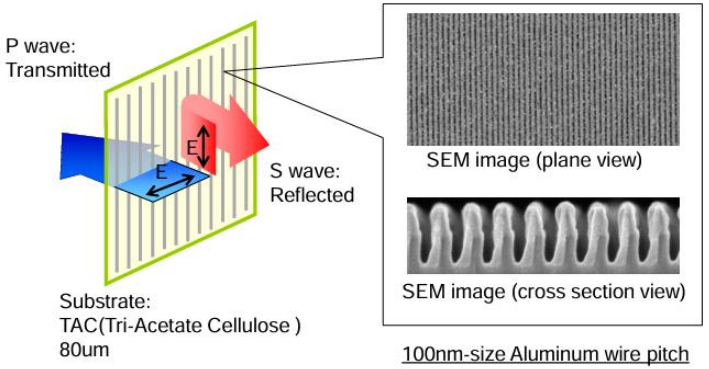


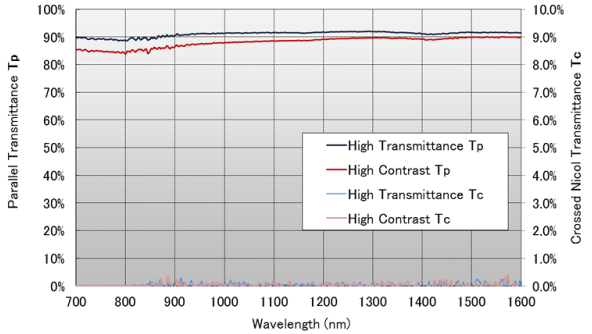



Recall the title of this paper: Red Bleed

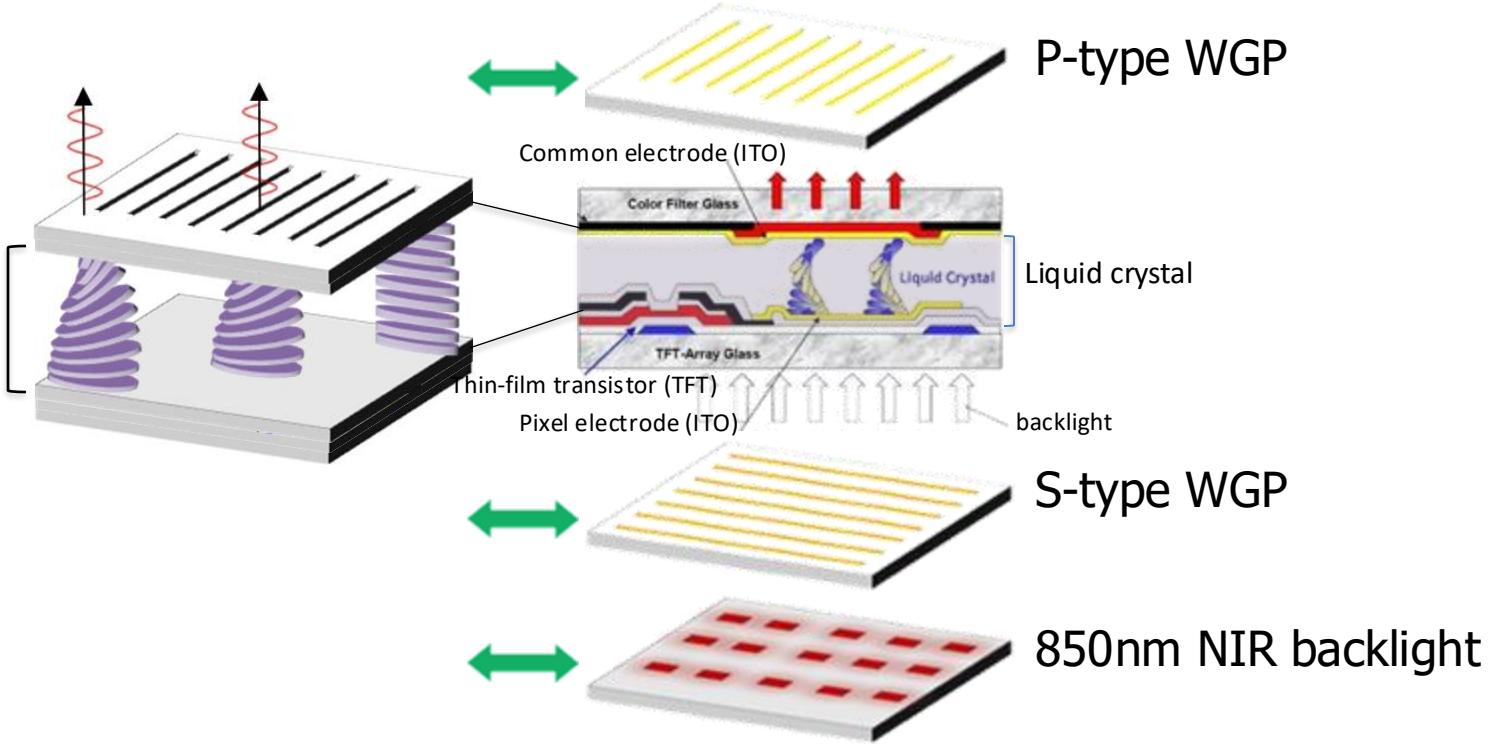
# Polarizer of LCDs

- Polarizers on LCDs are designed for 400-700 nm visible light wavelength.
- Wire grid polarizer can polarize effectively in a wide range from Visible to NIR

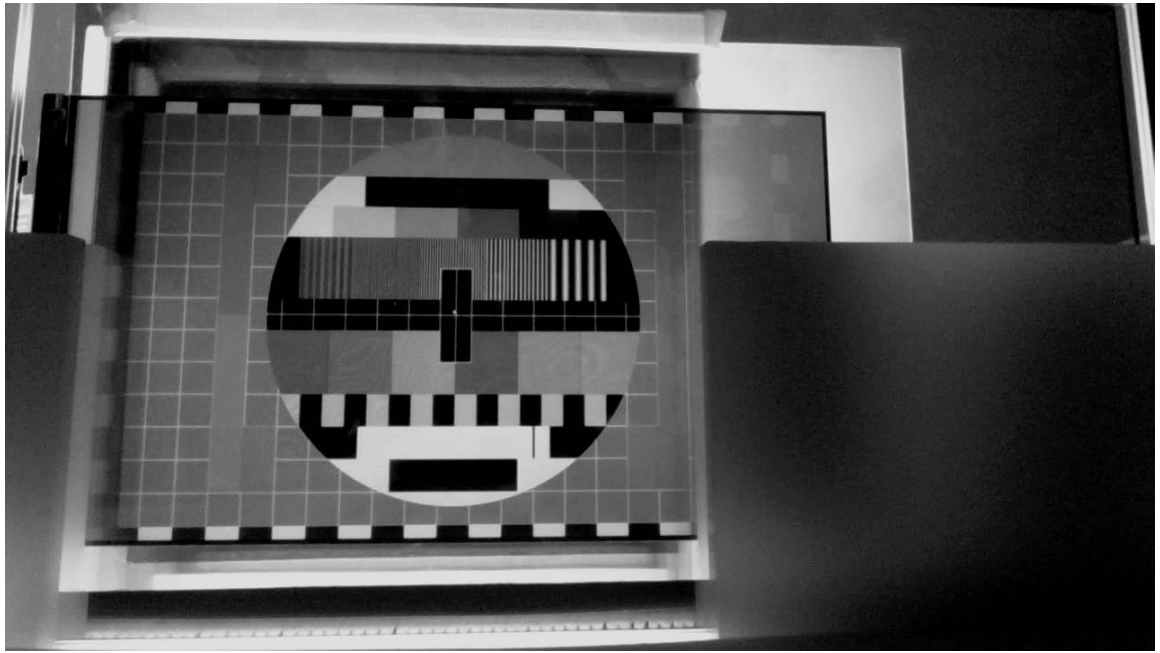


# Polarizer of LCDs



# LCD with NIR Backlight and WG polarizers



Good polarizers makes wonders

With WG polarizers added, very clear pattern is displayed on the screen under NIR spectrum.

# Material Costs

**850nm LED Board**

150mm×100mm

**$15.50**

**PP Diffuser**

150mm×100mm

**$0.07**


**Asaki KASEI HC12N Wired Grid Polarizer**

240mm×80mm

**$309.90**

**Sharp 5.5-inch 2K LCD**

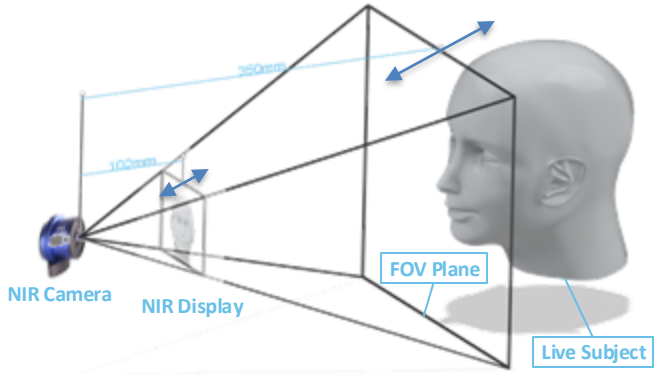
1140(RGB)×2560

LS055R1SX04A

**$30.90**

**356.37**

# Ready for attack




**Geometric Alignment Between Camera, LCD and Real Face**

# Victims: Windows hello modules

**HP:** 340×340 pixels, 30 fps

**Dell:** 340×340 pixels, 30 fps

**Lenovo:** 640×360 pixels, 15 fps

- 6.6s (200 frames), 1280 ×720 NIR video each of 22 subjects.
- OmniVision OV9281 monochrome camera with Gamma adjustment.
- Looped to create a 13.2 s continuous video for replay attack.
- The video uses FFV1 lossless encoding.

**100%** attack successful rate on all three modules

# Live Captured Frame Vs Captured Replay Frame

LIVE NIR

REPLAY NIR

# Limitations of the NIR presentation attack

- Require Acquisition of a 2~3 seconds of NIR **video** of the target
  - The subject should be illuminated with NIR light
  - The image should be captured with a NIR camera
  - Not stealthy enough

- Whereas, VIS facial images are omnipresent and easily accessible.
  - Secret videography from distance
  - Wedding and other group activities
  - Social medias
  - Video conferencing
  - …

# Addressing the Challenge of Dataset Limitation

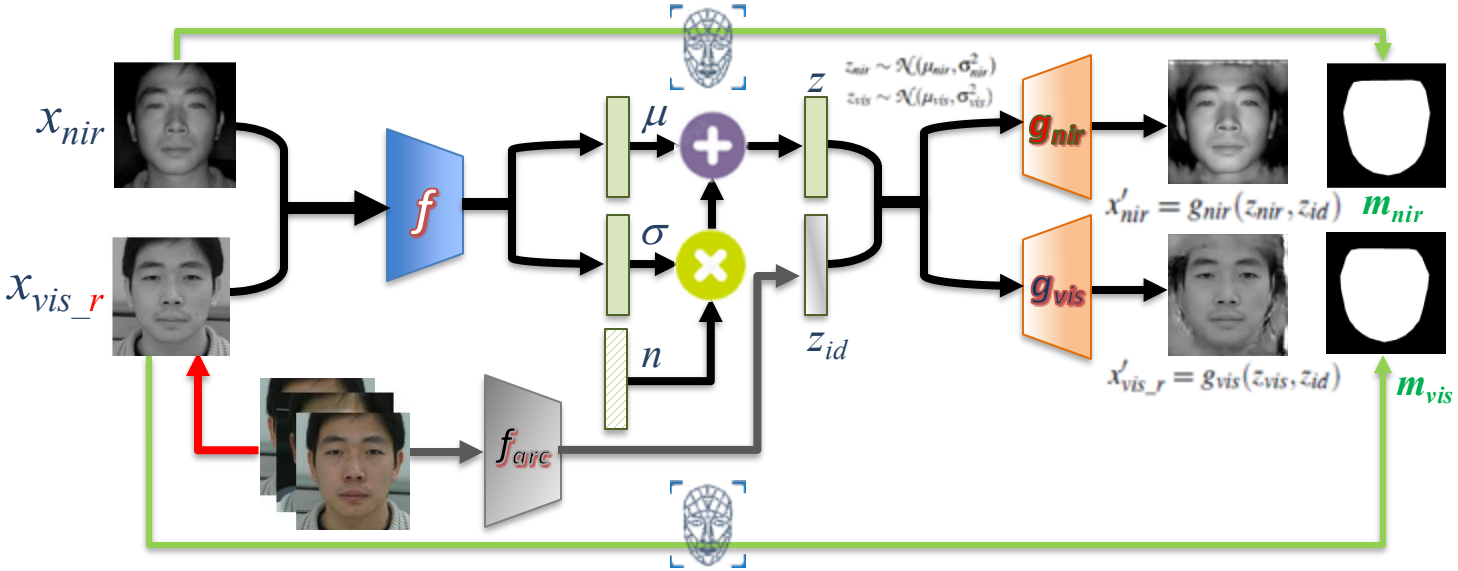
- Dataset: CASIA NIR-VIS Face 2.0 database
  - Released in 2013 CVPR Workshop
  - 725 subjects (from children to old people) with 1~22 VIS sample and 5~50 NIR samples
  - No pixel-level correspondence

- Our Data: Target subject samples
  - Few-shot learning: **nine** pairs of VIS-NIR samples are used for training
  - One-shot learning: **one** pair of VIS-NIR samples are used for training
  - No pixel-level correspondence required

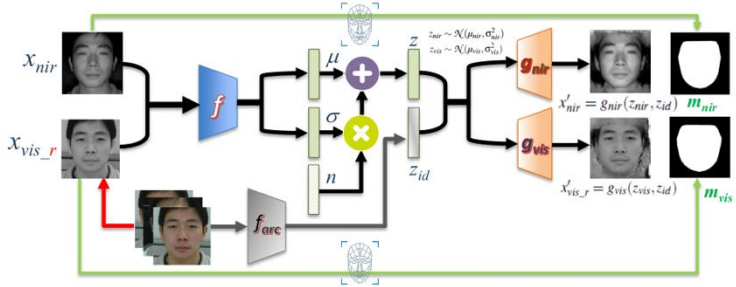
Uneven class distribution

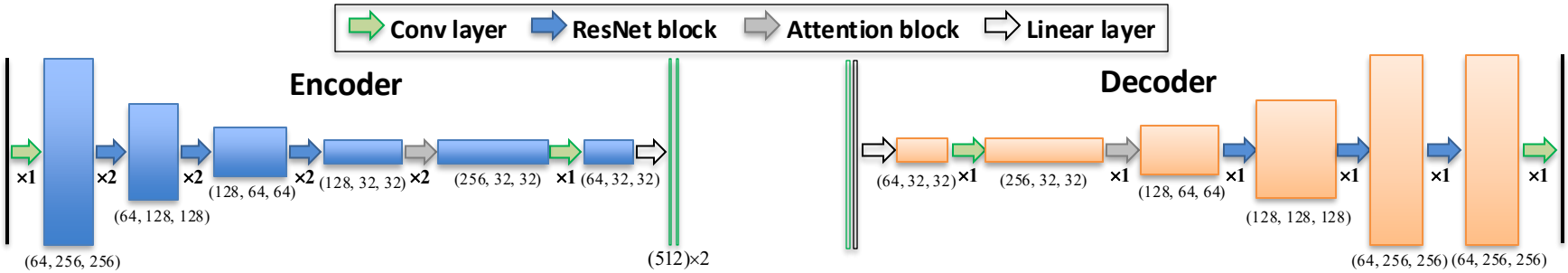
NIR-VIS Face 2.0 database: VIS and NIR face images, with variations in resolution, lighting conditions, pose and age, of one subject.

# Variational Autoencoder (VAE) based NIR Identity Preserving Face Generation



# Variational Autoencoder (VAE) based NIR Identity Preserving Face Generation



# Synthesis Results and Attack Performance

Generated NIR face

RGB video, Red channel

DeepFaceLab Face Swap

We generate a 5 seconds video
by swapping 100 frames.
22 subjects tested.

Nine-shot learning
Success rate 97.73%

One-shot learning
Success rate 61.25%

# Limitations of the Red Bleed Attack

- Cannot break "Enhanced Face Anti-spoofing" of Windows Hello Upon Windows April Updates (KB5055547, ver 24H2).

- Cannot break Apple Face ID and other 3D FRS.

# Limitations of the VIS to NIR Generative Model

- At least one shot from the target sample is required.
- A larger dataset with cross-spectral pixel correspondence is required for an unseen subject synthesis.
- Some artifacts appear in the generative result.

# Responsible Research

- Upon confirming the effectiveness of the attack on September 25, 2024, we immediately notified the security departments of Microsoft (MSRC), HP (HP PSRT), Dell (DELL PSIRT), and Lenovo (LENOVO PSIRT).

- We provided complete technical details in a report to each vendor and actively addressed their questions. We have agreed to withhold public release of this research until Microsoft has fully mitigated the issue.

- Microsoft managed to address this vulnerability with the **CVE-2025-26644** published and the patch released in the KB5055523 security update for all in-service Windows versions on April 8, 2025.

# Acknowledgments


- This research is supported by the Ministry of Education, Singapore, under its Academic Research Fund (AcRF) Tier 2 under Award MOE-T2EP50220-0003, and the National Research Foundation, Singapore under the Imperial/NTU CYber Protection for HEalthcaRe (IN-CYPHER) @ Campus for Research Excellence and Technological Enterprise (CREATE) programme.


- The presenter: Dr. Dirmanto Jap

# Thanks

For inquiries and research collaboration, please contact
Bowen Hu, Kuo Wang and Chip-Hong Chang
bowen006@e.ntu.edu.sg kuo.wang@ntu.edu.sg echchang@ntu.edu.sg