NDSS SYMPOSIUM/2025

山东大学 SHANDONG UNIVERSITY

EMIRIS: Eavesdropping on Iris Information via Electromagnetic Side Channel

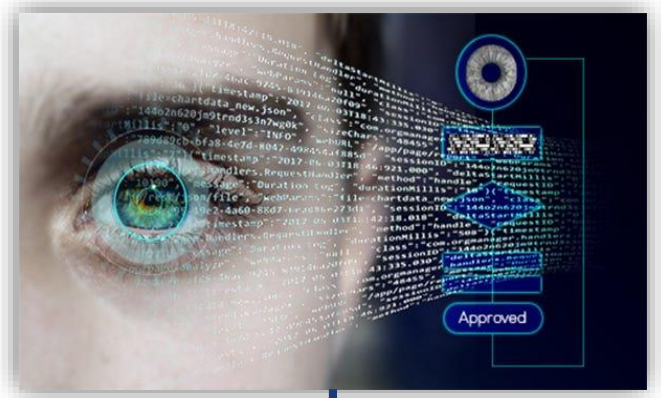
Wenhao Li, Jiahao Wang, Guoming Zhang, Yanni Yang, Riccardo Spolaor,
Xiuzhen Cheng, Pengfei Hu

Shandong University

February 2025

Iris Recognition & Its Hidden Risks

- ✅ High-entropy biometric authentication method
- ✅ Widely Used in various authentication scenarios
- ✅ Typically uses near-infrared (NIR) sensors



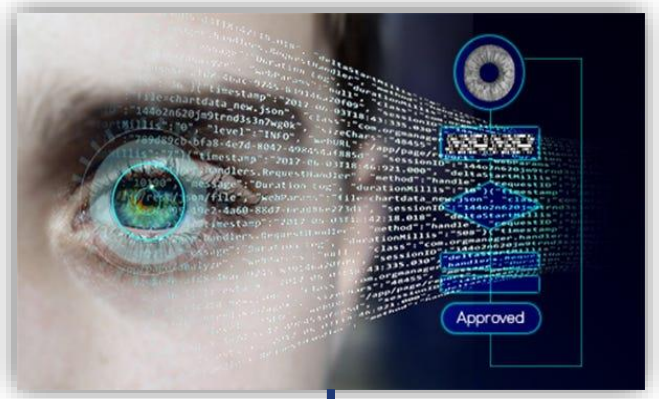
ID Recognition

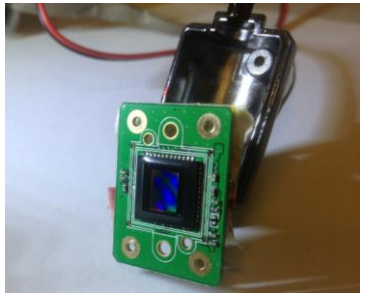
Airport Security

Bank ATMs

Iris Recognition & Its Hidden Risks

- ✅ High-entropy biometric authentication method
- ✅ Widely Used in various authentication scenarios
- ✅ Typically uses near-infrared (NIR) sensors





Electromagnetic Emissions

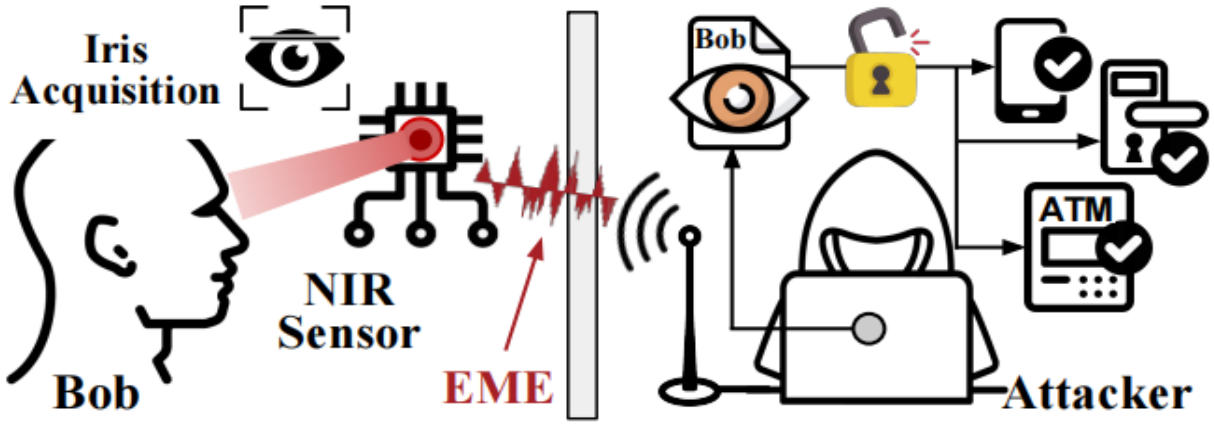
ID Recognition

Airport Security

Bank ATMs

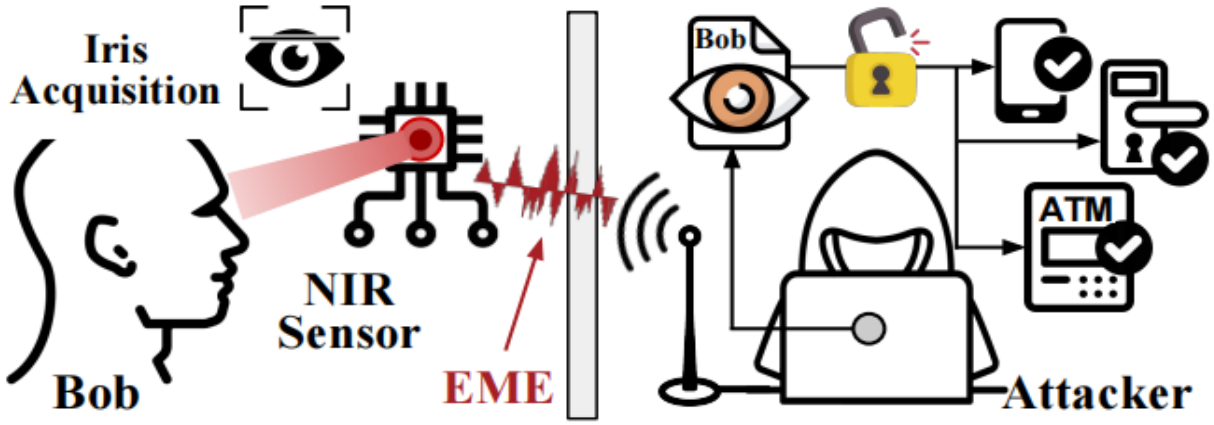
Threat Model

- No physical access to device
- No prior knowledge of victim
- Only capture EM signal at a distance

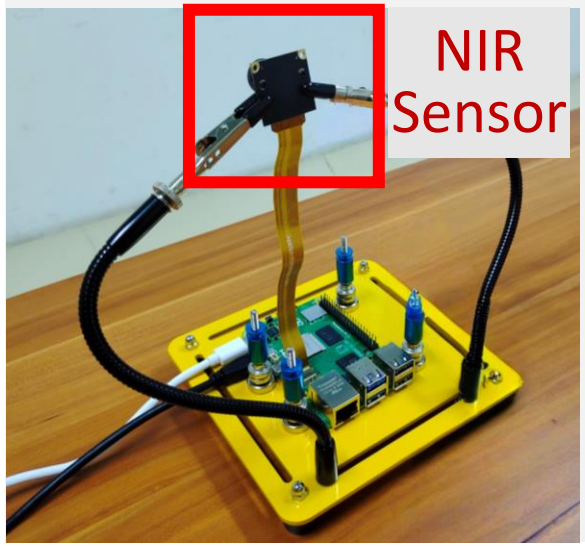


Threat Model

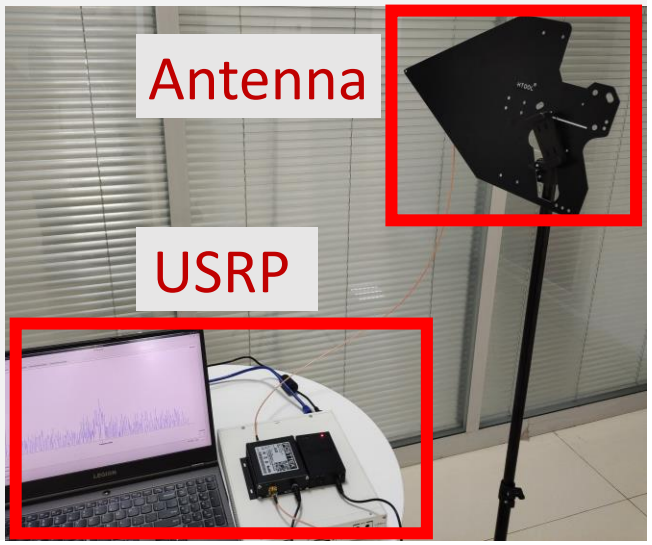
- No physical access to device
- No prior knowledge of victim
- Only capture EM signal at a distance



Target Device

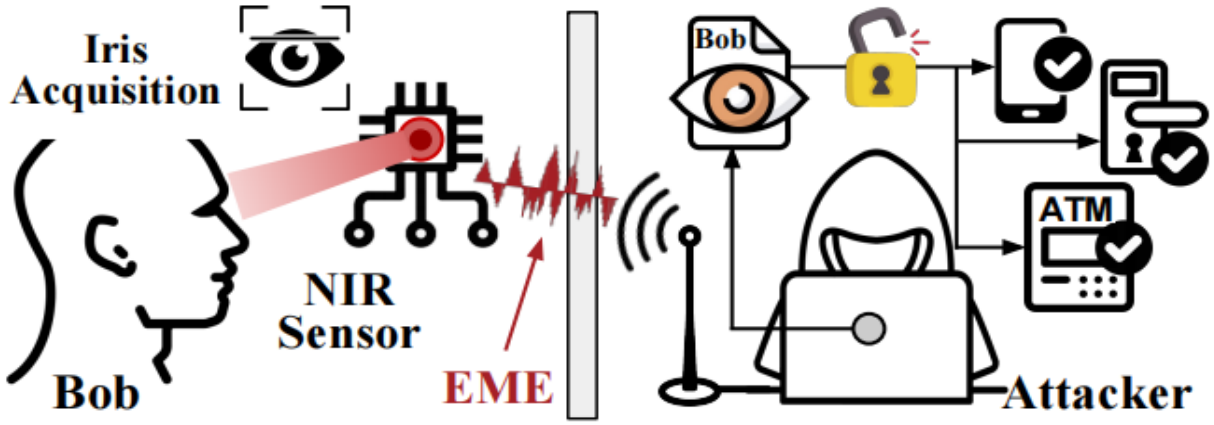


Attacker Equipment

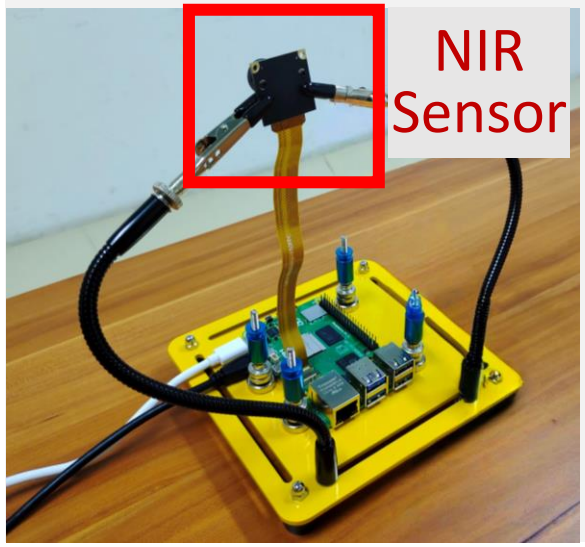


Threat Model

- No physical access to device
- No prior knowledge of victim
- Only capture EM signal at a distance



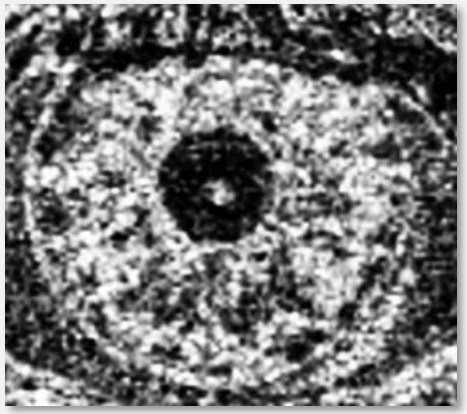
Target Device



Attacker Equipment

Original Iris

Reconstructed Iris



Iris Reconstruction from EM signal

$$\mathrm{IRIS}_{\mathrm{raw}}(f) = M_{E2I}\{f, E, M_{D2I}(D_{\mathrm{digi}}, G)\} + W(f)$$

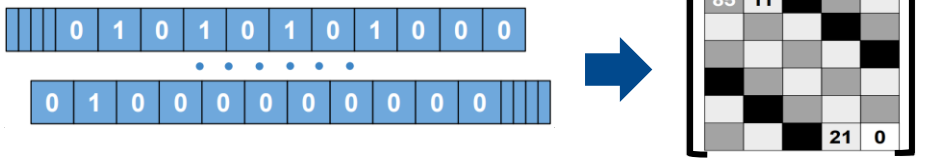
Iris grayscale matrix 

Iris Reconstruction from EM signal

$$\mathrm{IRIS}_{\mathrm{raw}}(f) = M_{E2I}\{f, E, M_{D2I}(D_{\mathrm{digi}}, G)\} + W(f)$$

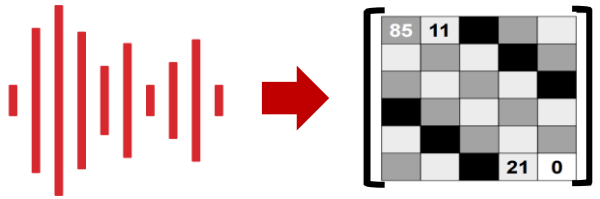
Iris grayscale matrix

Digital signal to iris data mapping function



Iris Reconstruction from EM signal

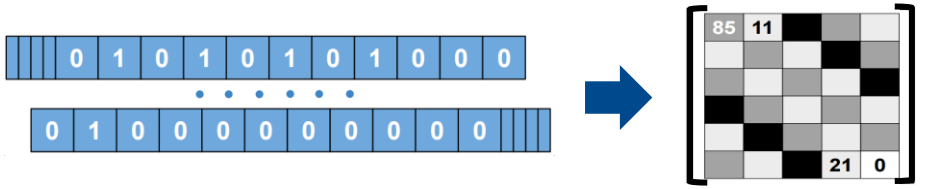
EM signal to iris data mapping



$$\mathrm{IRIS}_{\mathrm{raw}}(f) = M_{E2I}\{f, E, M_{D2I}(D_{\mathrm{digi}}, G)\} + W(f)$$

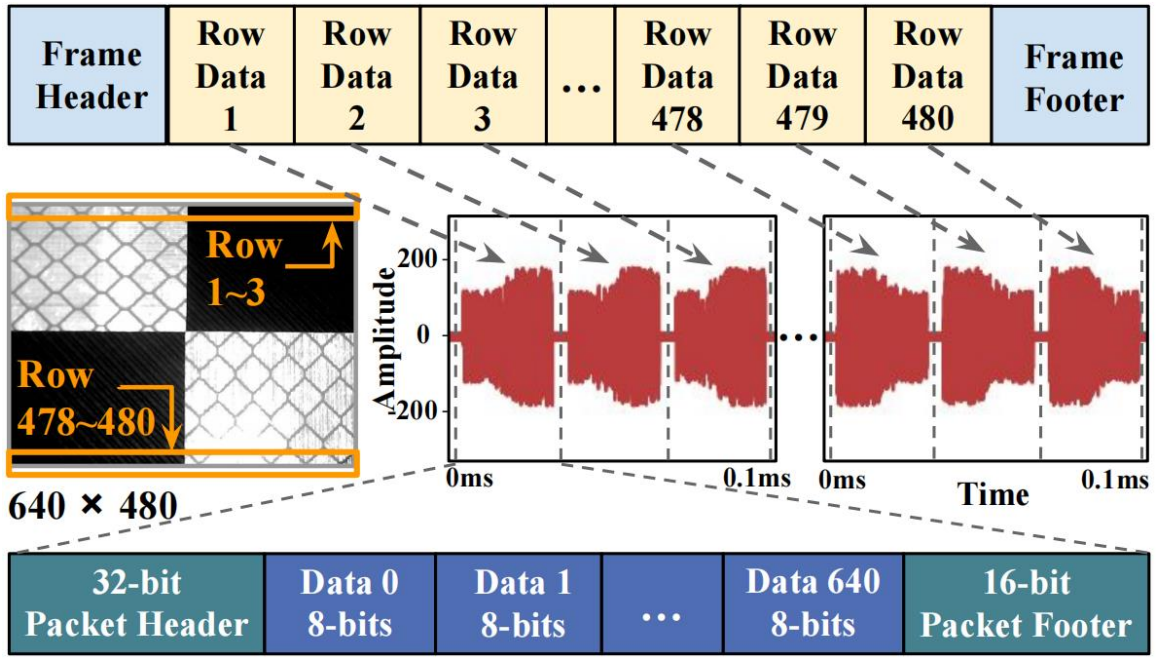
Iris grayscale matrix

Digital signal to iris data mapping function



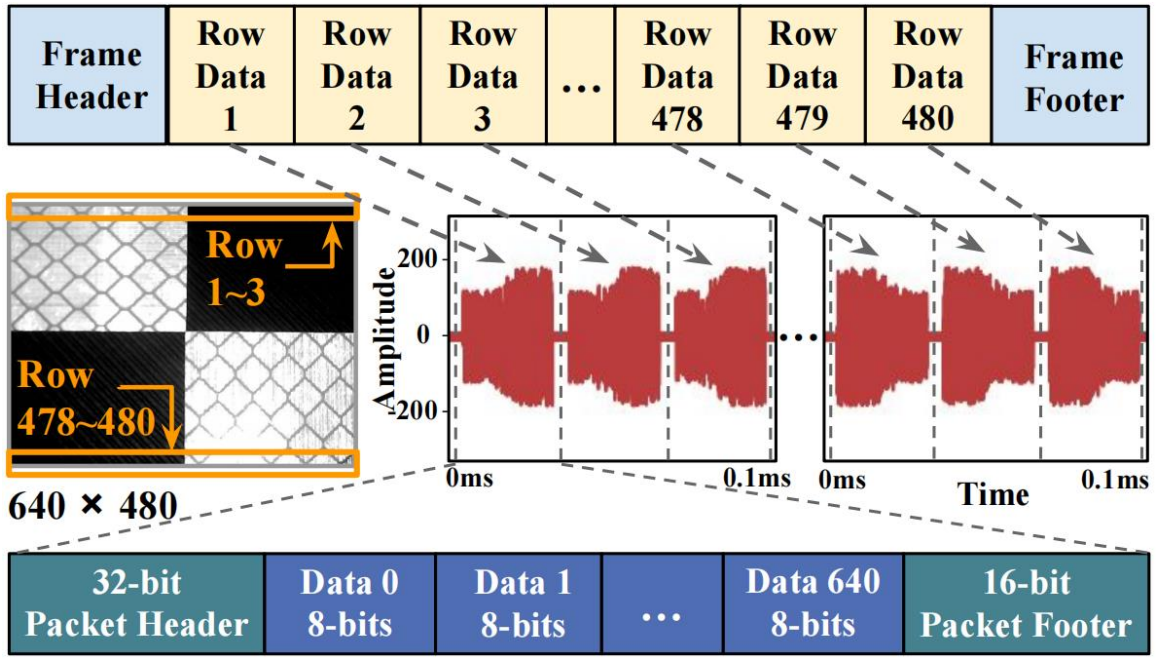
Iris Reconstruction from EM signal

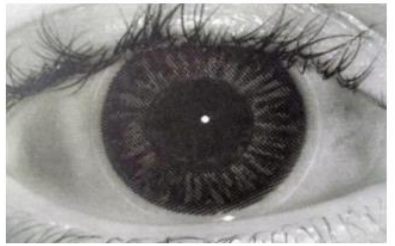
📌Example: Electromagnetic Leakage & Data Format



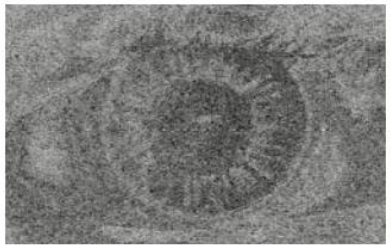
Iris Reconstruction from EM signal

📌Example: Electromagnetic Leakage & Data Format

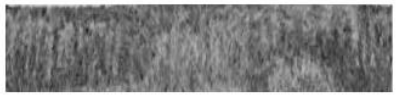




(a) Ground truth



(b) Reconstructed iris



Segmentation and normalization

Iris Reconstruction from EM signal

$$\mathrm{IRIS}_{\mathrm{raw}}(f) = M_{E2I}\{f, E, M_{D2I}(D_{\mathrm{digi}}, G)\} + W(f)$$

Noise introduced by the channel

Iris Reconstruction from EM signal

$$\mathrm{IRIS}_{\mathrm{raw}}(f) = M_{E2I}\{f, E, M_{D2I}(D_{\mathrm{digi}}, G)\} + W(f)$$

Noise introduced by the channel

Denoising:

Digital domain

$$\tilde{E}[n] = \sum_{m=0}^{L-1} b_m E[n-m]$$

$$\hat{E}[n] = \mathrm{IDFT}\{\mathrm{DFT}(\tilde{E}[n])H[k]\}$$

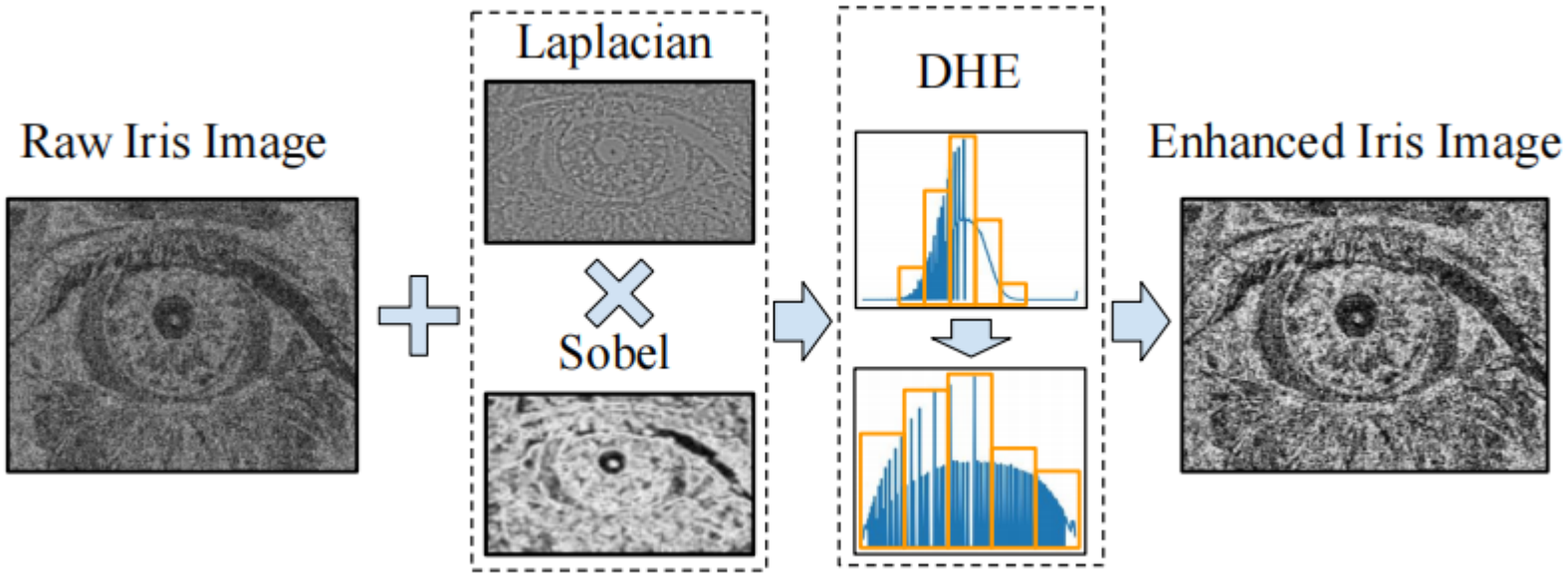
+

Physical domain

Low-Noise Amplifiers (LNA)

Enhancing Iris Structure

- Emphasize key structural components:

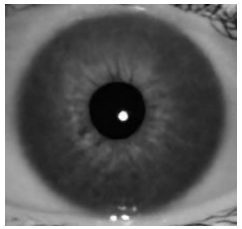


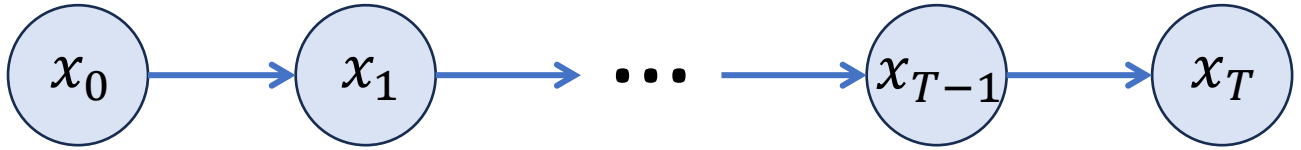
Iris Denoising and Detail Generation

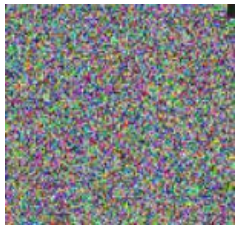
- Diffusion Model:

Forward process

Additive gaussian noise

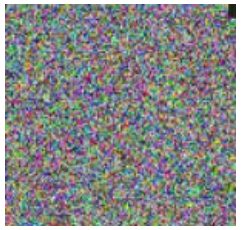


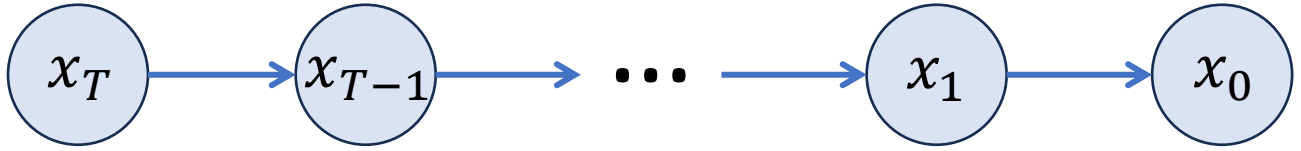


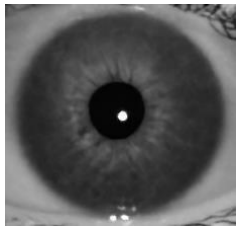


Reverse process

Denoising

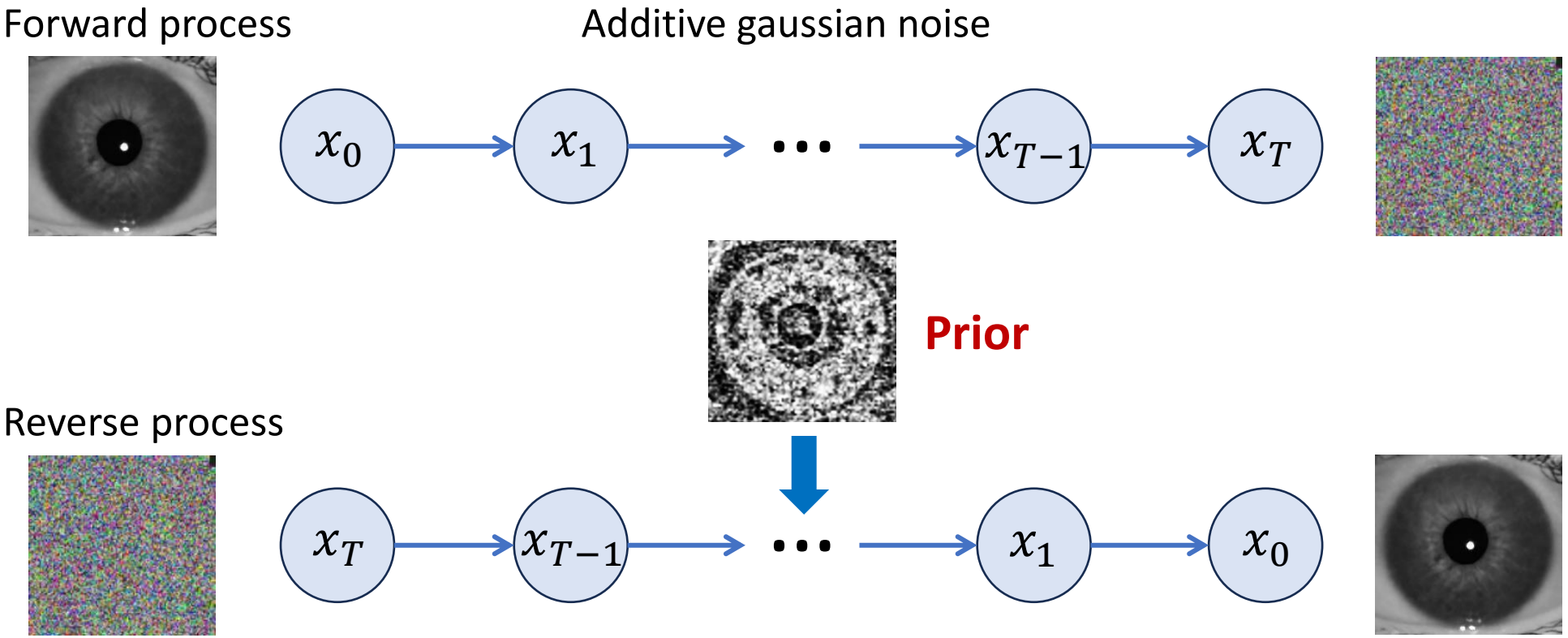






Iris Denoising and Detail Generation

- Diffusion Model:



Iterative Denoising with HQS

💡 Enforcing consistency between x and the captured EM-based iris reconstruction

Subiteration:

$$(1) \quad z_t = \arg\min_z \frac{1}{2\sigma_t^2} ||z - x_t||^2 + P(z)$$

Prior

Iterative Denoising with HQS

💡 Enforcing consistency between x and the captured EM-based iris reconstruction

Subiteration:

(1) $$z_t = \arg\min_z \frac{1}{2\sigma_t^2}||z - x_t||^2 + P(z)$$

Prior

(2) $$x_{t-1} = \arg\min_x ||y - H(x)||^2 + \lambda||x - z_t||^2$$

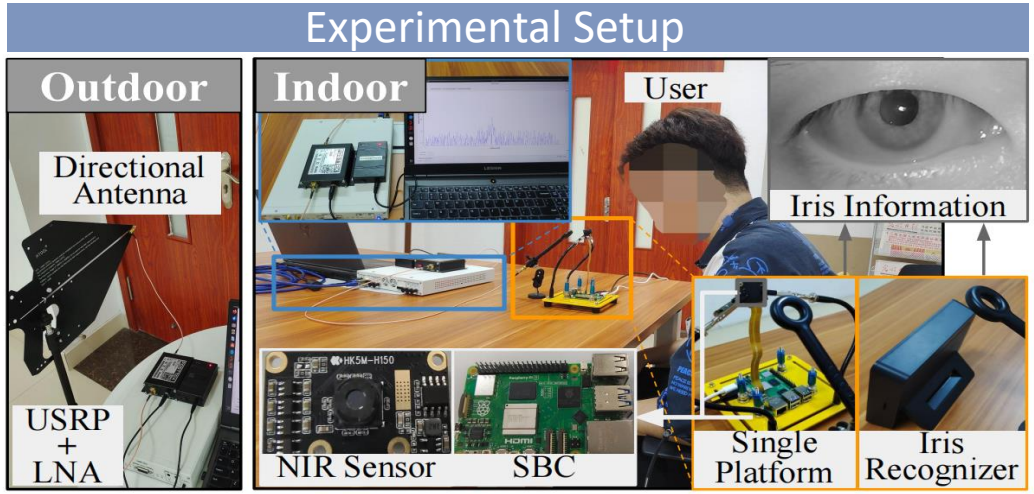
Enforce x to stay close to z_t

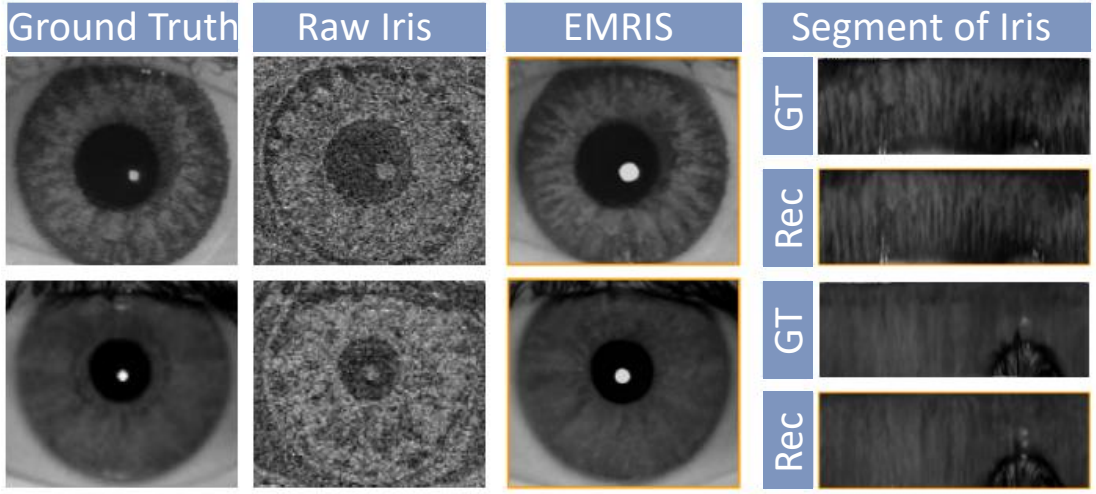
Diffusion Model

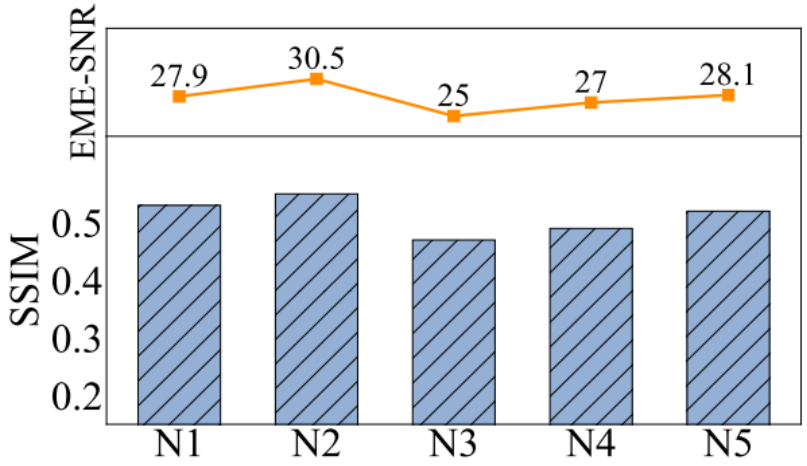
- Model Training:
  - 4 different datasets
  - 46,451 iris images in total
  - Diffusion model: DDPM
  - Optimizer: AdamW
  - Epochs: 50
  - Diffusion steps: 1000

Datasets	CASIA-IrisV4	ND-IRIS-0405	IITD v1	LivDet-Iris 2020
Subjects	1,800	356	224	118
Image format	JPEG	JPEG	BMP	PNG
Environment	Variety	Standard light	Standard light	Standard light
Devices	IrisKing IKEMB-100	LG 2200	JIRIS, JPC1000	Iris ID iCAM7000
Sensors	NIR	NIR	NIR	NIR
Liveness detection	No	No	No	Yes
Age	-	18-75	14-55	-
Resolution	640×480	640×480	320×480	640×480
Images for training	54,601(20,000)	64,980(20,000)	1,120(all)	5,331(all)

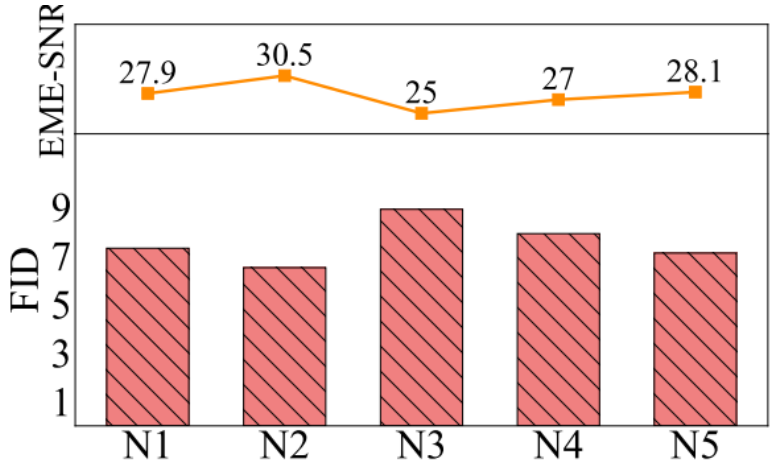
Iris Reconstruction Results







SSIM for different NIR sensors

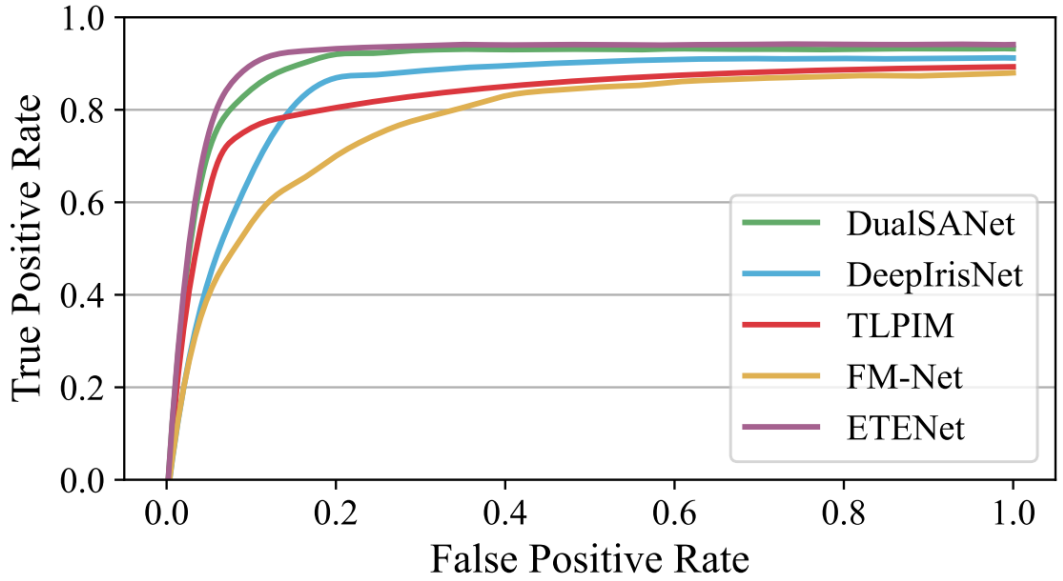


FID for different NIR sensors

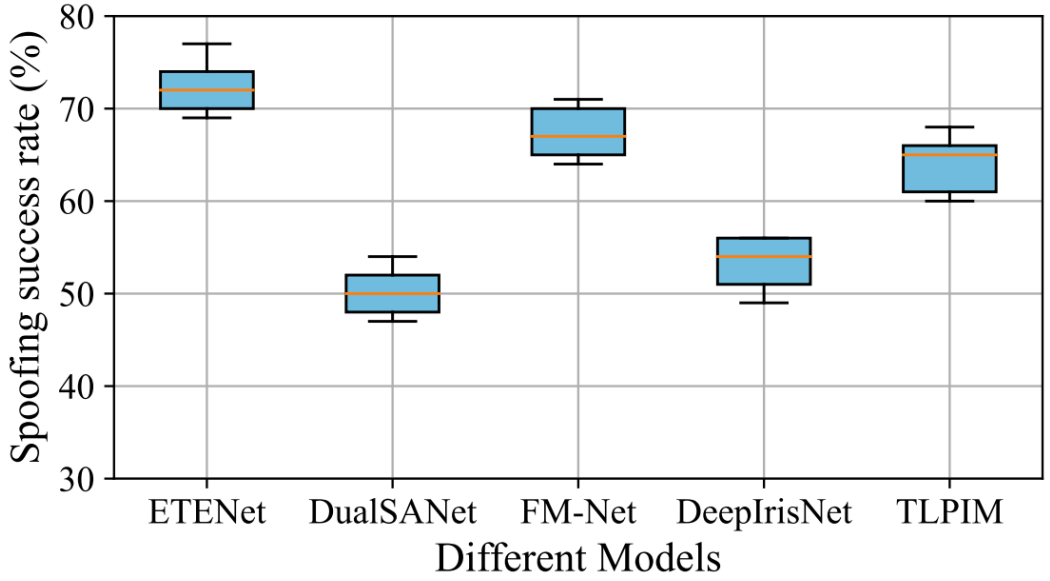
Spoofing Iris Recognition Models

➢ Target models

Models		Input Size	Activation Function	Optimizer	Learning Rate	Datasets	FRR (FAR=0.1%)	Accuracy* (%)
DeepIrisNet [30]	DCNN	128×128	ReLU	SGD	0.01	ND-iris-0405, ND-CrossSensor-Iris-2013	0.008	97.31
FM-Net [31]	FCN+MCNN	28×28	ReLU	SGD	0.01	CASIA-Iris-Thousand	4.27	95.63
ETENet [32]	DNN	160×120	ReLU	Adam	0.0001	CASIA-IrisV4, IITD	0.75	99.76
DualSANet [33]	CNN	64×512	ReLU	SGD	0.001	CASIA-IrisV4,IITD	0.58	99.69
TLPIM [34]	ResNet	256×256	ReLU	Adam	0.00001	CASIA-Iris-Thousand	0.8	96.00



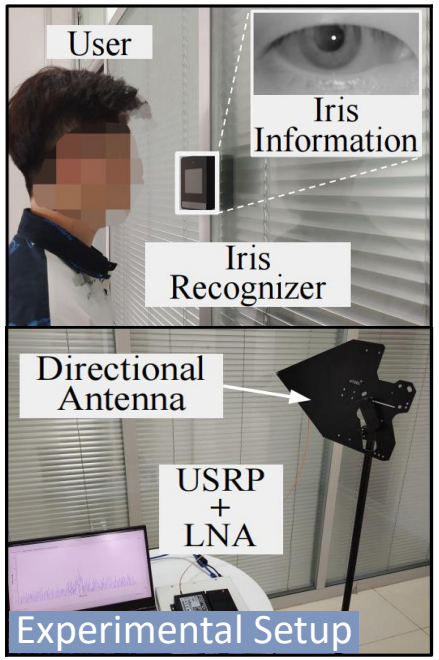
ROC curves of different models

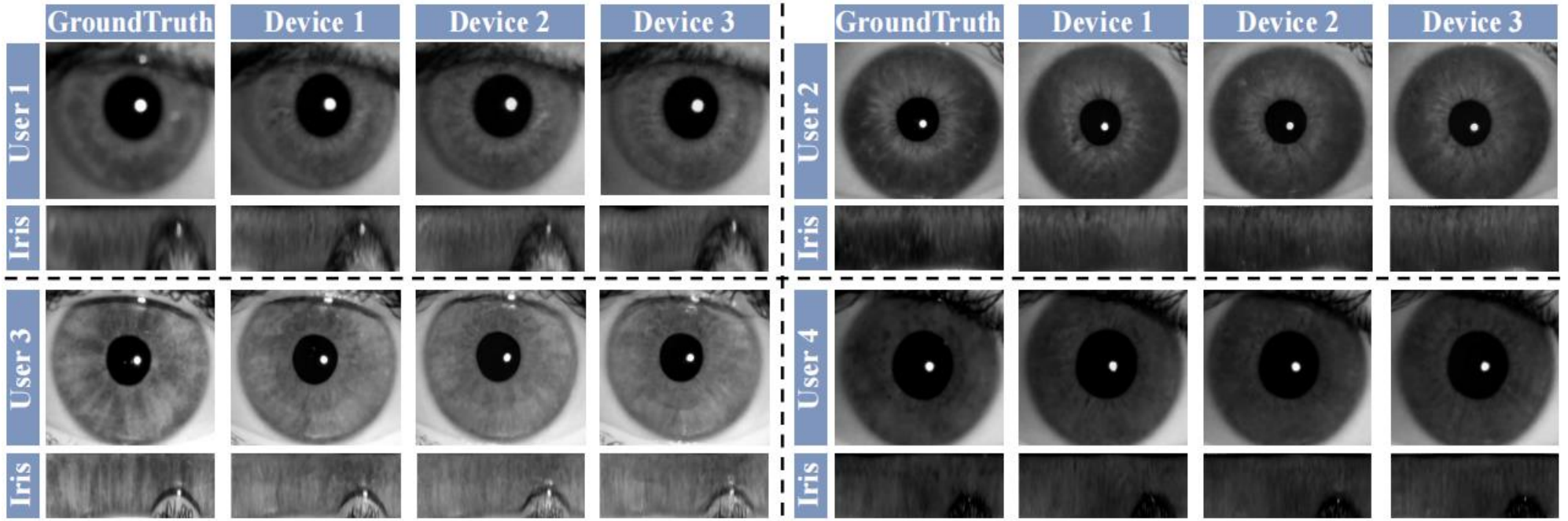


SSR for different models

Iris Reconstruction Results

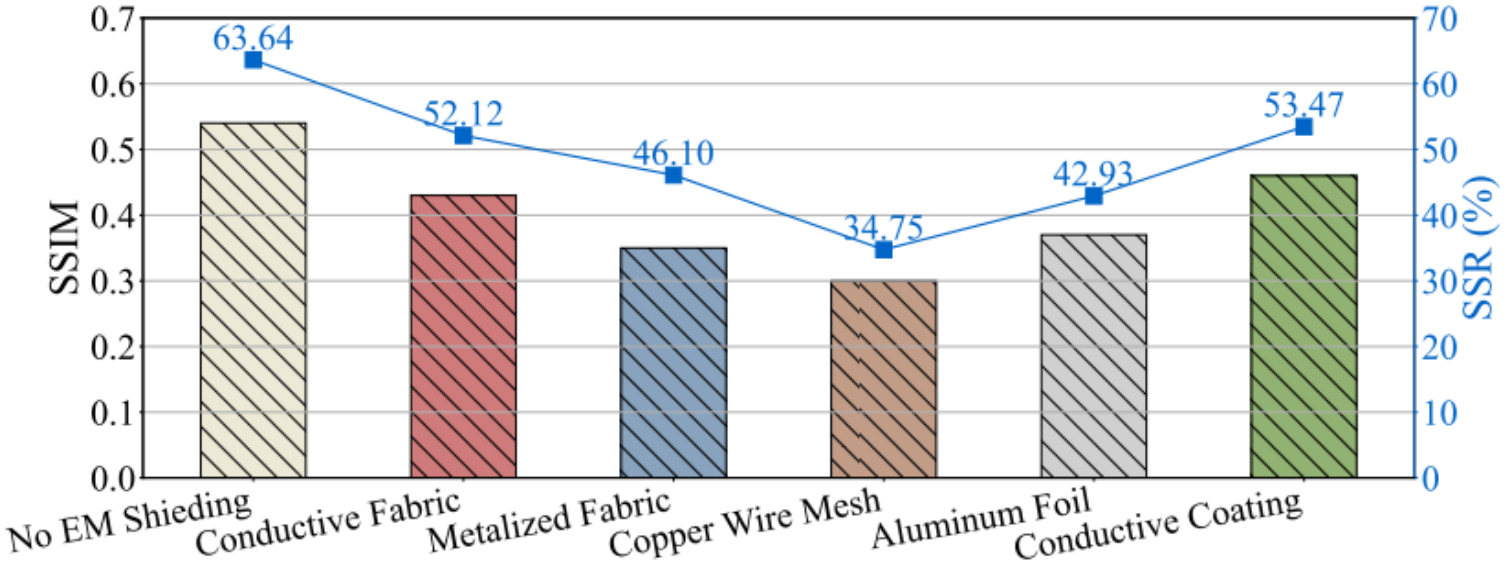
- Target different iris recognition devices





- How to against EMIRIS?

  Enhancing EM Shielding.

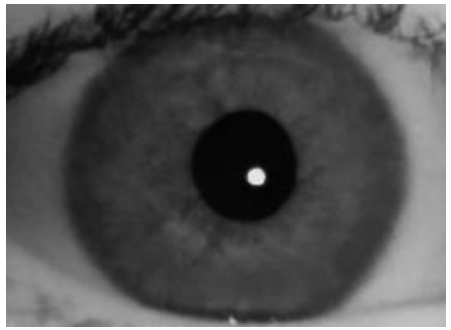


Discussion: Limitations

- Limitations

EMIRIS may not bypass liveness detection.

Two-dimension Iris



Liveness detection

- Pupil response detection
- Blink detection

Discussion: Future work

- Future work

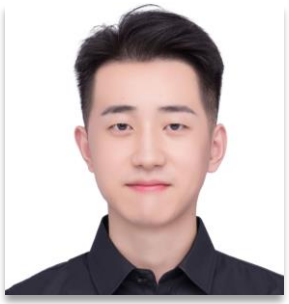
Apply reconstructed iris information to bionic eyes or contact lenses.

Bionic eye

Contact lenses

Thank You! Questions and Discussions Are Welcome!

Our Team



Wenhao Li

Jiahao Wang

Guoming Zhang

Yanni Yang

Riccardo Spolaor

Xiuzhen Cheng

Pengfei Hu

山东大学 SHANDONG UNIVERSITY

IIC 智能计算研究所 Institute of Intelligent Computing

IIC Website:

http://iic.sdu.edu.cn/

Contact Authors:

li_wenhao@mail.sdu.edu.cn

guomingzhang@sdu.edu.cn

phu@sdu.edu.cn