RFace: Anti-Spoofing Facial Authentication Using COTS RFID

Weiye Xu*, Jianwei Liu*, Shimin Zhang*, Yuanqing Zheng^,
Feng Lin*, Jinsong Han*, Fu Xiao, and Kui Ren*

*Zhejiang University, Hangzhou, China
^The Hong Kong Polytechnic University, Hong Kong, China
Nanjing University of Posts and Telecommunications, China

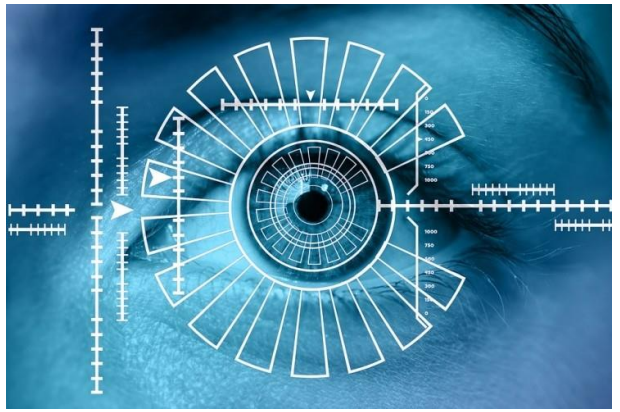
INFOCOM 2021, Online
May 2021

Background

- **User authentication has become an absolute necessity.**

Password-based

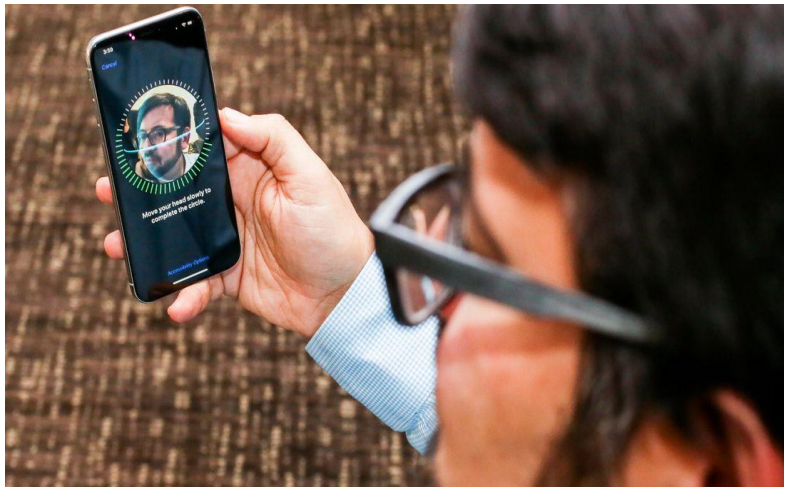
Fingerprint Scanning



Iris Scanning

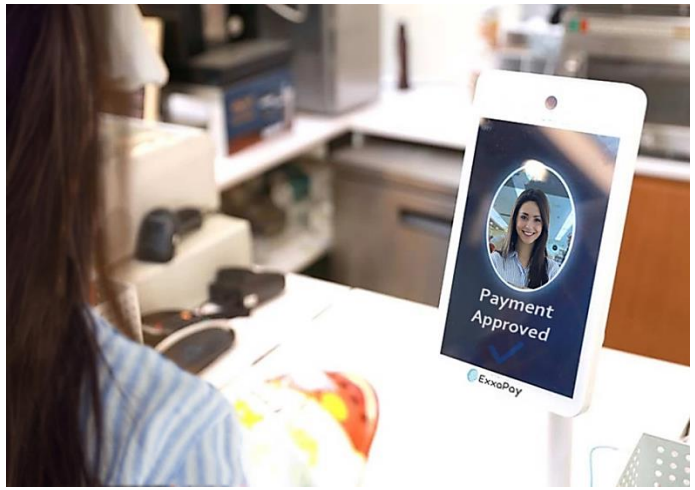
Background

➢ **Face authentication is promising due to its convenience and precision.**



Individual Identification

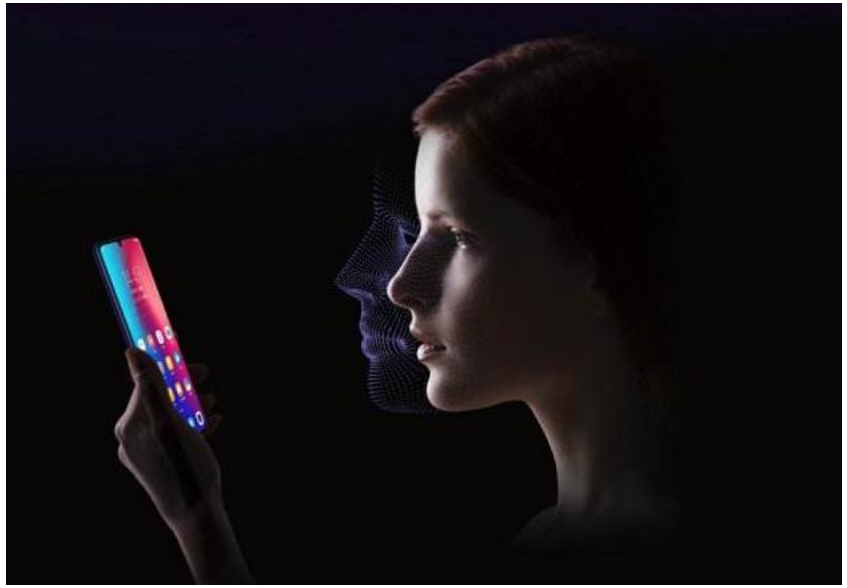
Access Control



Online Payment

Ambient light & Privacy Leakage

- **Camera-based face authentication is susceptible to ambient light.**
- **Vision-based face authentication raises privacy concerns.**

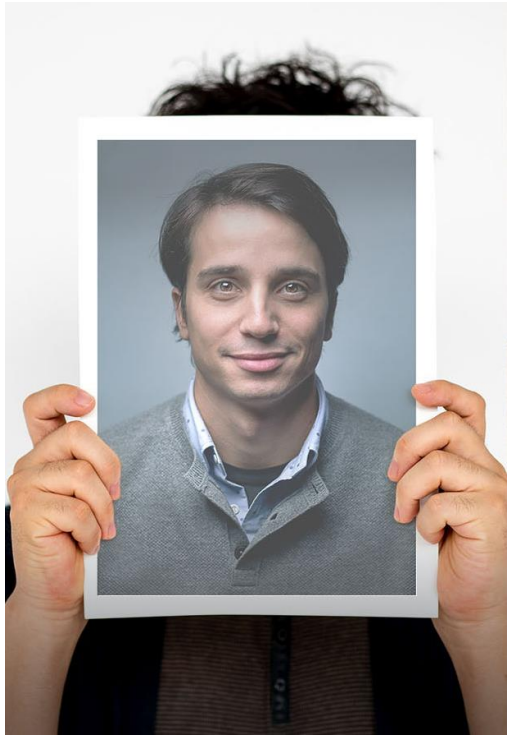


Ambient Light

Privacy Leakage

Spoofing Attacks

- **2D Spoofing Attacks: 2D static (photo) attack and dynamic (video) attack**
- **2D+ Spoofing Attacks: precise 2D image plus rough depth measurements**
- **3D Spoofing Attacks: precise 3D printed mask**



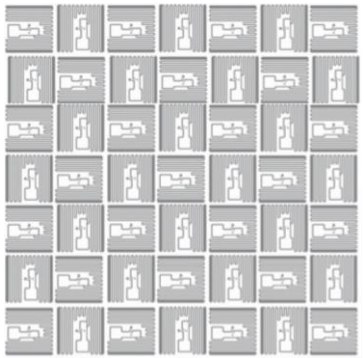
2D

2D+

3D

We want to ***explore a new facial feature based authentication technique,*** which can ***protect the visual privacy*** of users, and meanwhile ***resist spoofing attacks.***

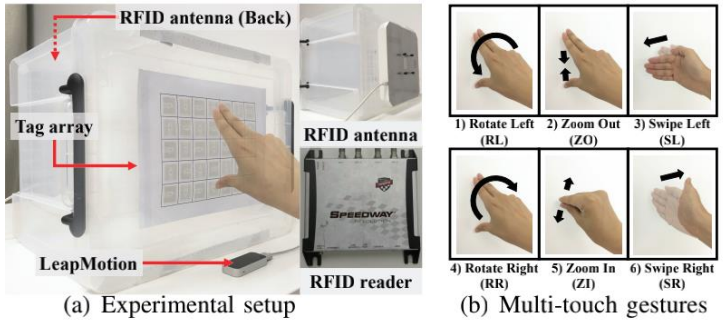
Turn to RFID



Tag Array

Fine-grained Wireless Sensing

Yang et al. [MOBICOM 2015]
Wang et al. [INFOCOM 2018]

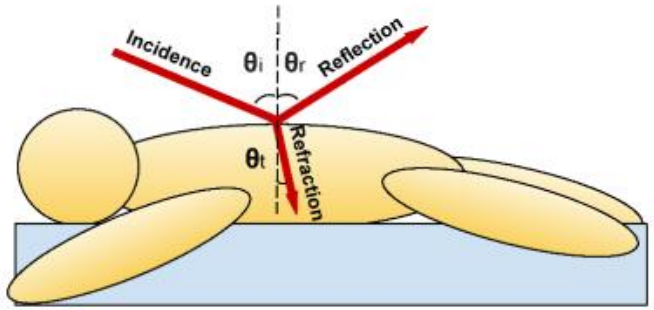


(a) Experimental setup (b) Multi-touch gestures

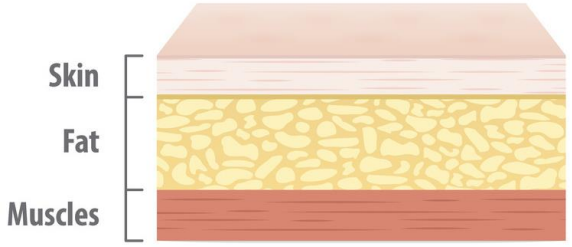
External 3D Geometry Features

Sensitive To The Material

Vasisht et al. [SIGCOMM 2018]



Inner Biomaterial Features

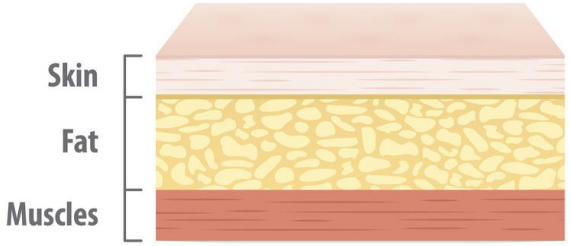


Fusion Feature

External
3D Geometry Features

Use RFID tag array to extract fusion feature

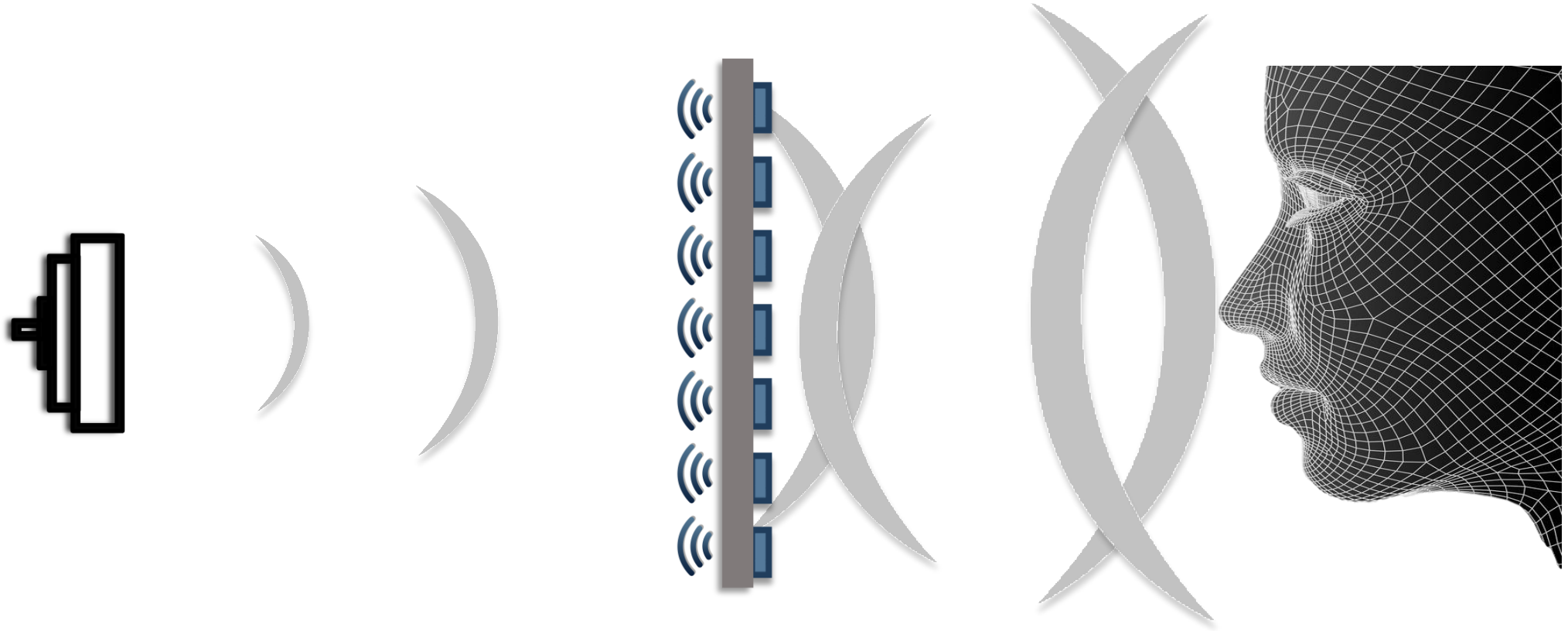
Inner
Biomaterial Features



Fusion Feature

protect the *visual privacy*
difficult to be *captured*
difficult to *reproduce*

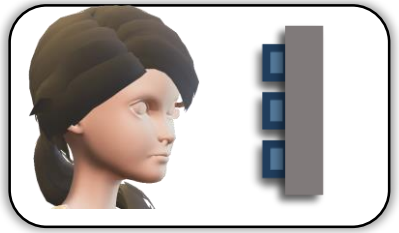
RFace



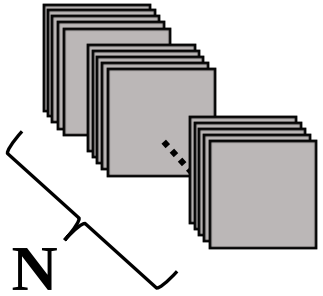
Denoising & Rearrangement

Fusion Feature

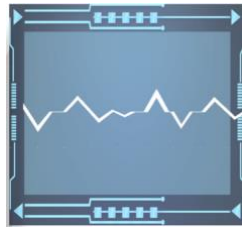
Recorded RF signals reflected from the face



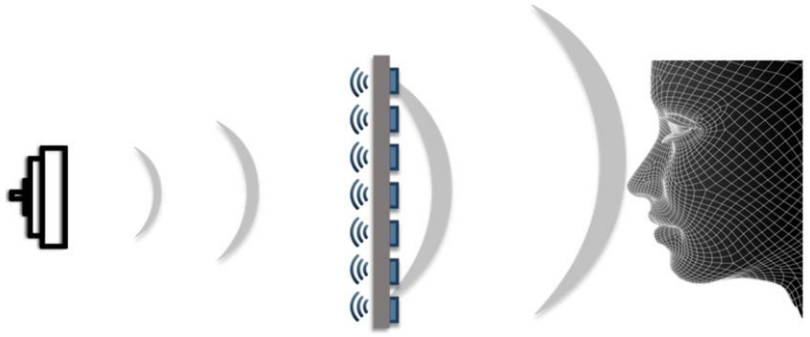
Preprocess



Feature Extraction



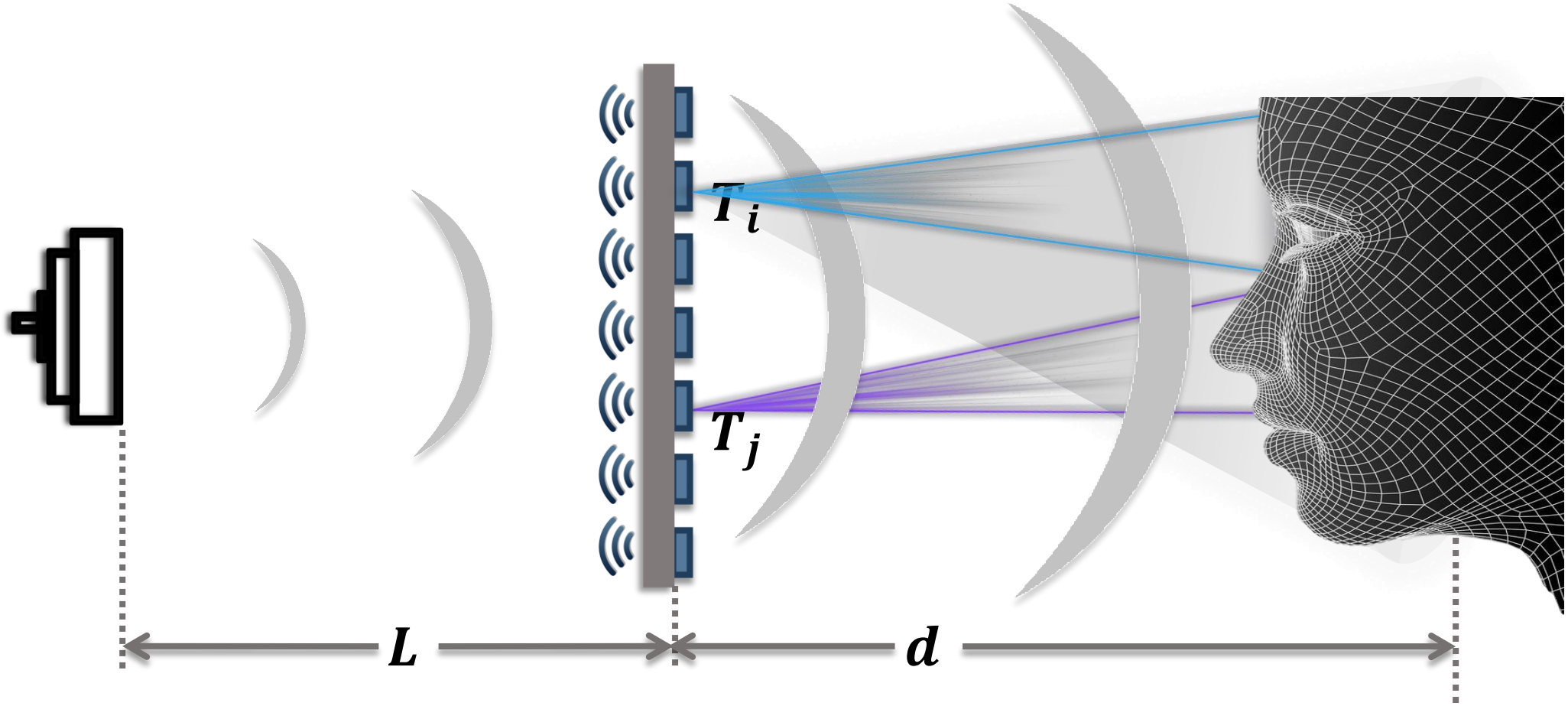
Authentication & Spoofer detection



User or Spoofer?

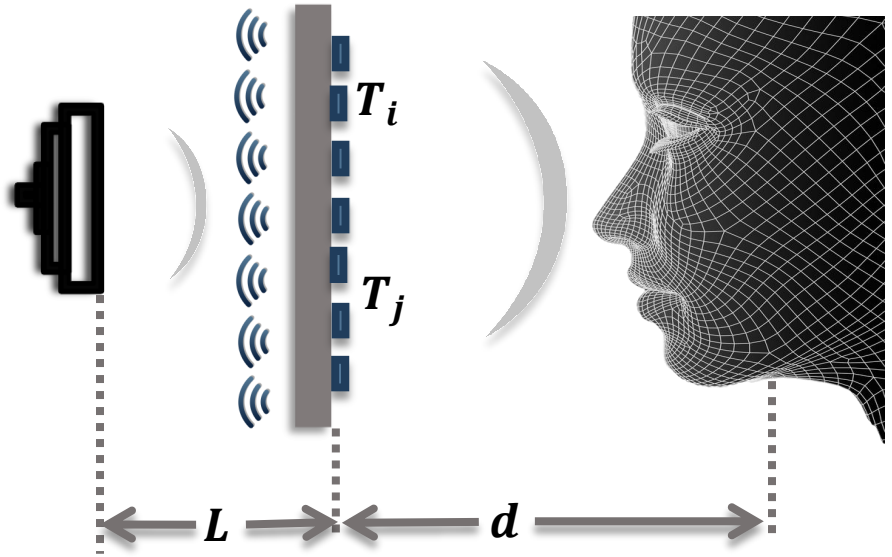
Challenge1

How to extract the fusion feature from the non-structured RF signals?



Facial Features Extracted by RSS

$$\mathrm{RSS} = 10\log\frac{P}{10^{-3}} = 20\log DA$$



The First Propagation Stage

$$A_{in} = A\mathrm{e}^{-\alpha(\mathrm{L}+\mathrm{d}-d_i)}$$

The Second Propagation Stage

$$A_{\_after} = \sqrt{R_{per\_i}}A_{in}$$

according to Fresnel Formula:

$$R_{per\_i} = R_s R_p$$
$$= \left|\frac{\sqrt{\varepsilon_{per}}\cos\beta_{refr\_i} - \sqrt{\varepsilon_{air}}\cos\beta_{in\_i}}{\sqrt{\varepsilon_{per}}\cos\beta_{refr\_i} + \sqrt{\varepsilon_{air}}\cos\beta_{in\_i}}\right|^2$$
$$\times \left|\frac{\sqrt{\varepsilon_{per}}\cos\beta_{in\_i} - \sqrt{\varepsilon_{air}}\cos\beta_{refr\_i}}{\sqrt{\varepsilon_{per}}\cos\beta_{in\_i} + \sqrt{\varepsilon_{air}}\cos\beta_{refr\_i}}\right|^2$$

only determined by ε_{per} and β_{in_i}

The Third Propagation Stage

$$A_r = \sqrt{R_{per\_i}}A\mathrm{e}^{-2\alpha(\mathrm{L}+\mathrm{d}-d_i)}$$

$$RSS_i = 20\log DA_r = 20\log D\sqrt{R_{per\_i}}A\mathrm{e}^{-2\alpha(\mathrm{L}+\mathrm{d}-d_i)}$$

$$RSS_j = 20\log DA_{r\_j} = 20\log D\sqrt{R_{per\_j}}A\mathrm{e}^{-2\alpha(\mathrm{L}+\mathrm{d}-d_j)}$$

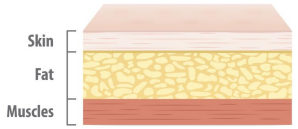
Facial Features Extracted by RSS

Unstable Factor

$$RSS_i = 20\log DA_r = 20\log D\sqrt{R_{per\_i}}Ae^{-2\alpha(L+d-d_i)}$$

To remove d

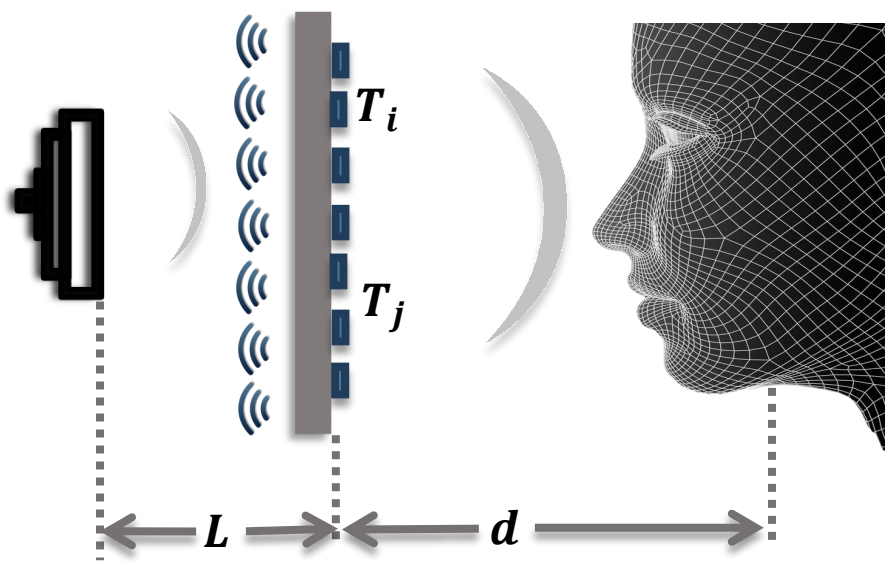
$$RSS_i - RSS_j = 20\log\left|\frac{\sqrt{R_{per\_i}}}{\sqrt{R_{per\_j}}}\right|e^{-2\alpha(d_i-d_j)}$$



ε_{per} represents the ***inner biomaterial feature,***
β_{in_i} represents the ***3D geometry feature.***

represents the horizontal distance between the center points of two different blocks on the human face.
Indicating the 3D geometry feature

Facial Features Extracted by Phase



The First Propagation Stage $\theta_{\_before} = \theta_t + \frac{2\pi}{\lambda}(\mathrm{L} + \mathrm{d} - d_i)$

The Second Propagation Stage $\theta_{\_after} = \theta_{\_before} + \theta_{per\_i}$

The Third Propagation Stage $\theta_r = \theta_{after} + \frac{2\pi}{\lambda}(L + d - d_i)$

$$\theta_i = \left[\theta_t + \theta_{per_i} + \theta_{tag_i} + \frac{4\pi}{\lambda}(L + d - d_i)\right]$$

To remove ***d*** → $\theta_i - \theta_j = (\theta_{per_i} - \theta_{per_j}) + (\theta_{tag_i} - \theta_{tag_j}) + \frac{4\pi}{\lambda}(d_j - d_i) + 2k\pi, k \in Z$

inner biomaterial feature and 3D geometry feature

Indicating the 3D geometry feature

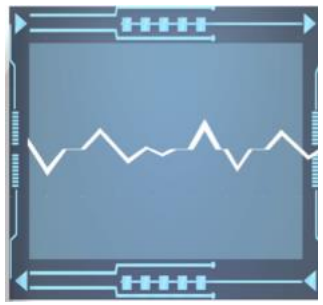
related to Brewster Angle:

$$\begin{cases}\theta_{per\_i} = 0, \beta_{in\_i} \leq \beta_B \\ \theta_{per\_i} = \pi, \beta_{in\_i} > \beta_B\end{cases}$$

$$\beta_B = arctan\sqrt{\frac{\varepsilon_{per}}{\varepsilon_{air}}}$$

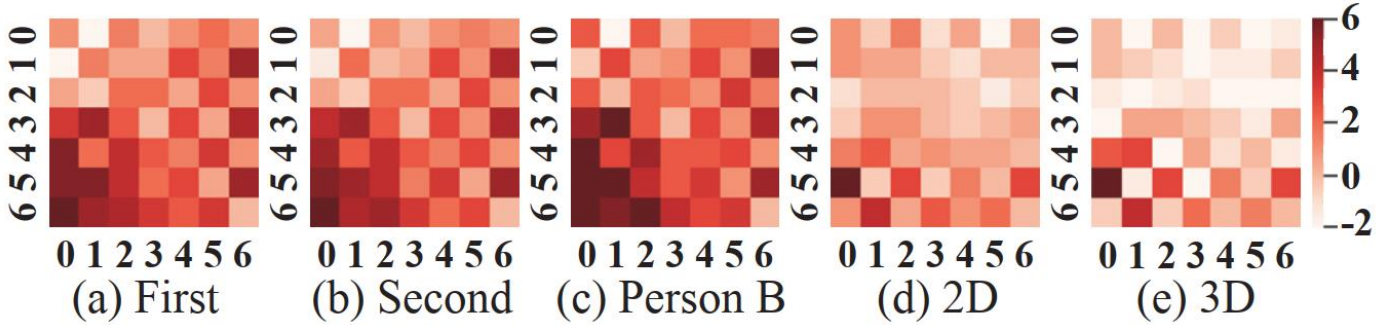
only determined by ε_{per} and β_{in_i}

Extracted Fusion Facial Feature

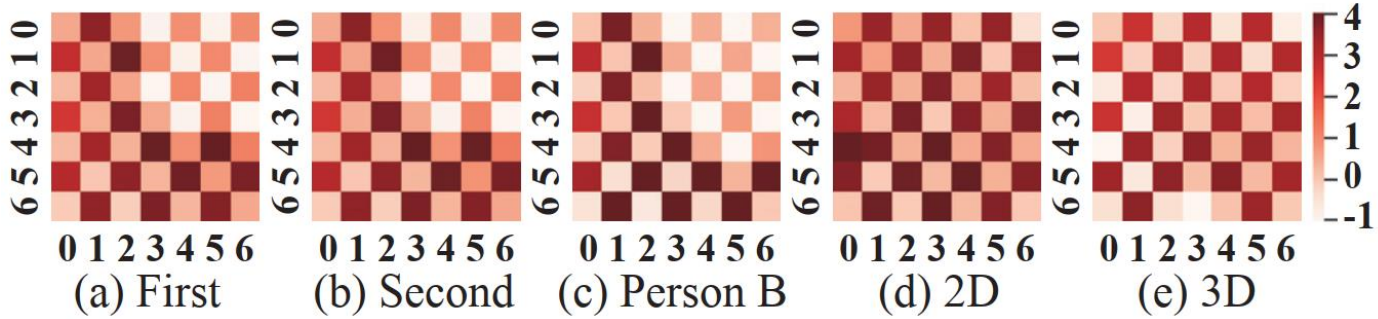


Fusion Feature

RSS Difference

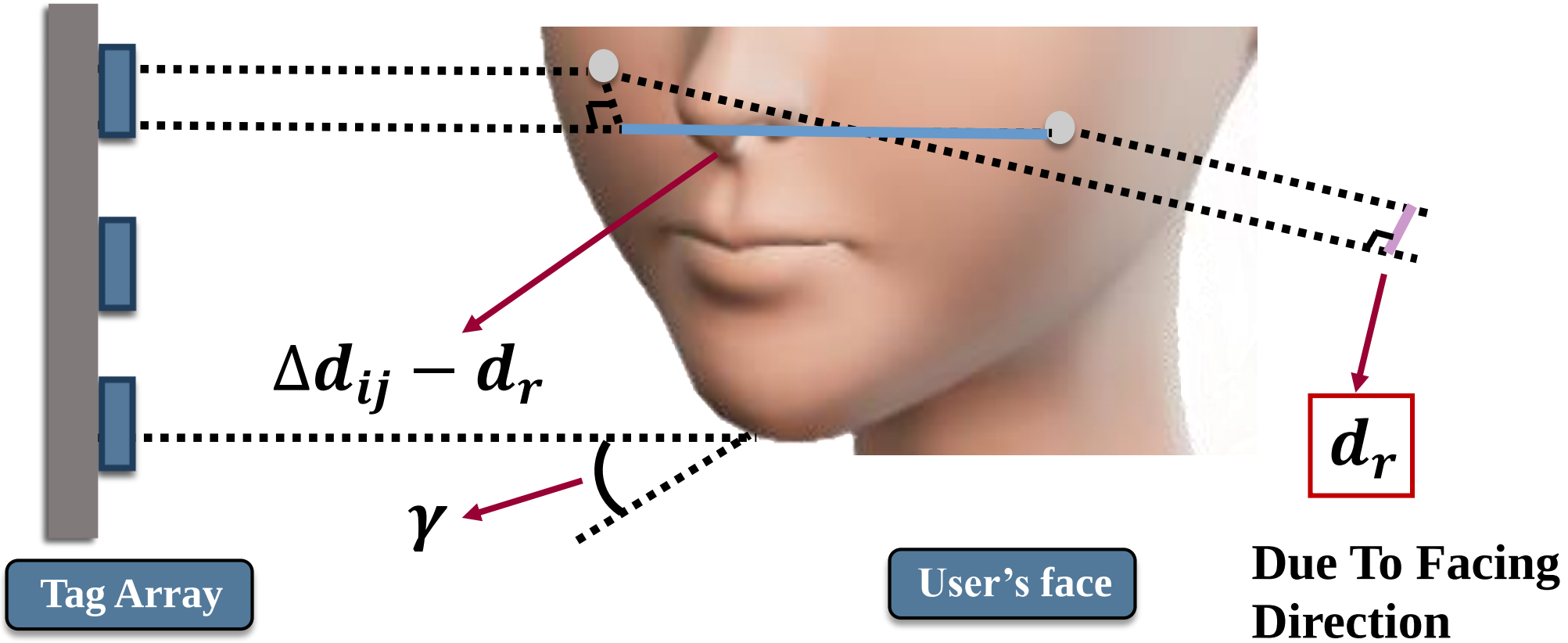


Phase Difference



Challenge2

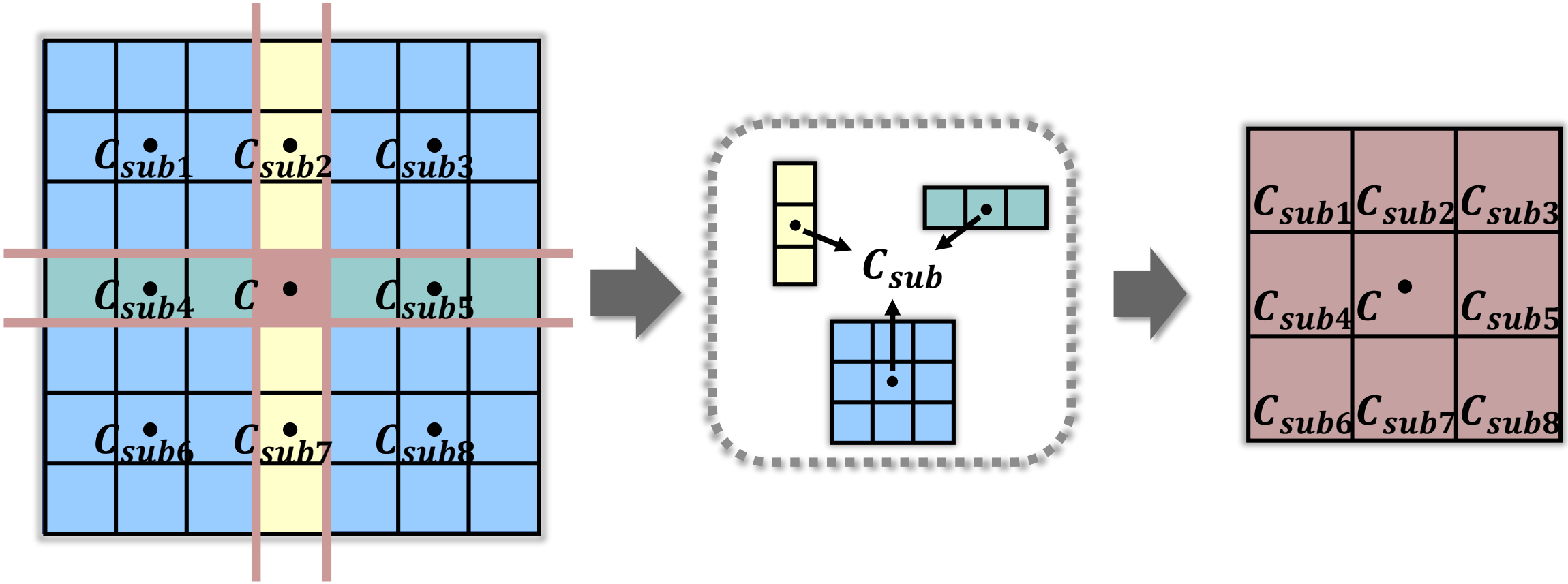
How to make RFace robust to the disturbance of distance and deflection?



It is vital to mitigate the unexpected distance difference d_r!!!

Distance-Deflection Disturbance Suppression

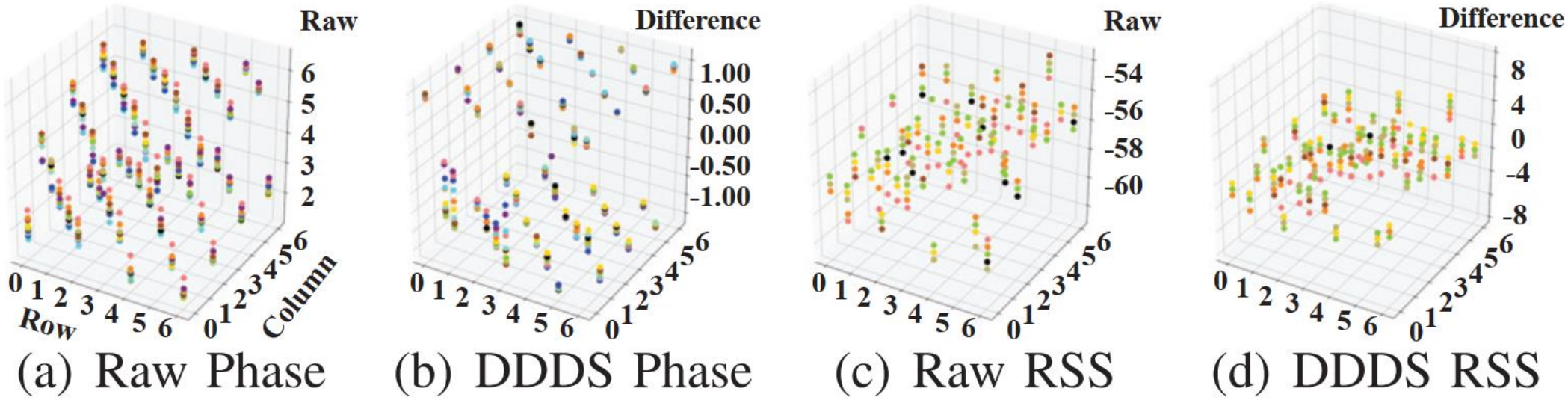
The closer the two tags are selected for subtraction, the smaller the d_r is.
The key idea:* *narrow the difference calculation range in the tag array.



7*7 Tag Array **Smallest Blocks** **SubCenter Block**

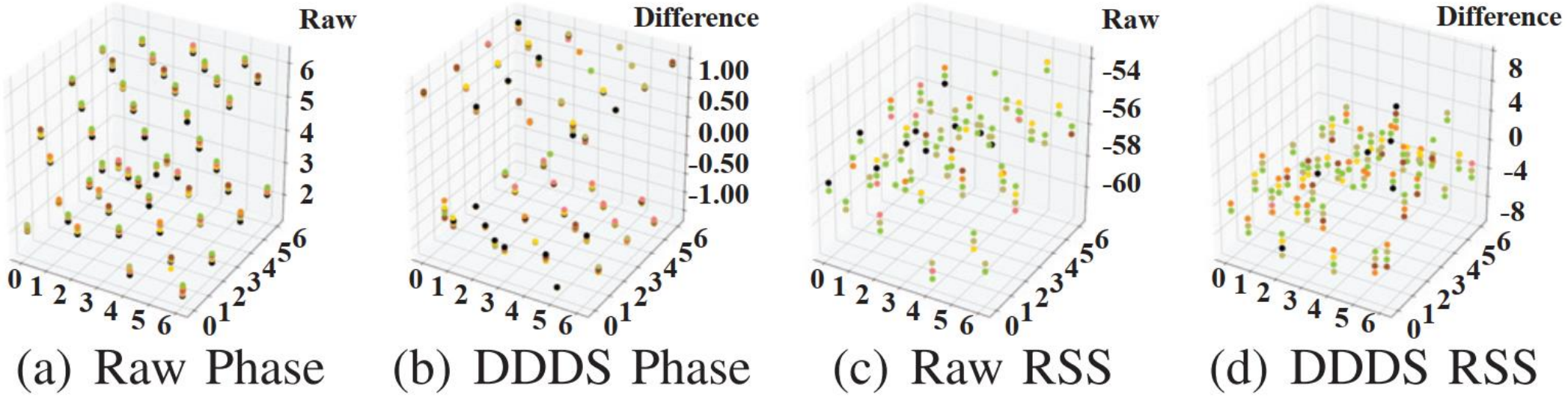
Performance of DDDS

Different Distance Conditions



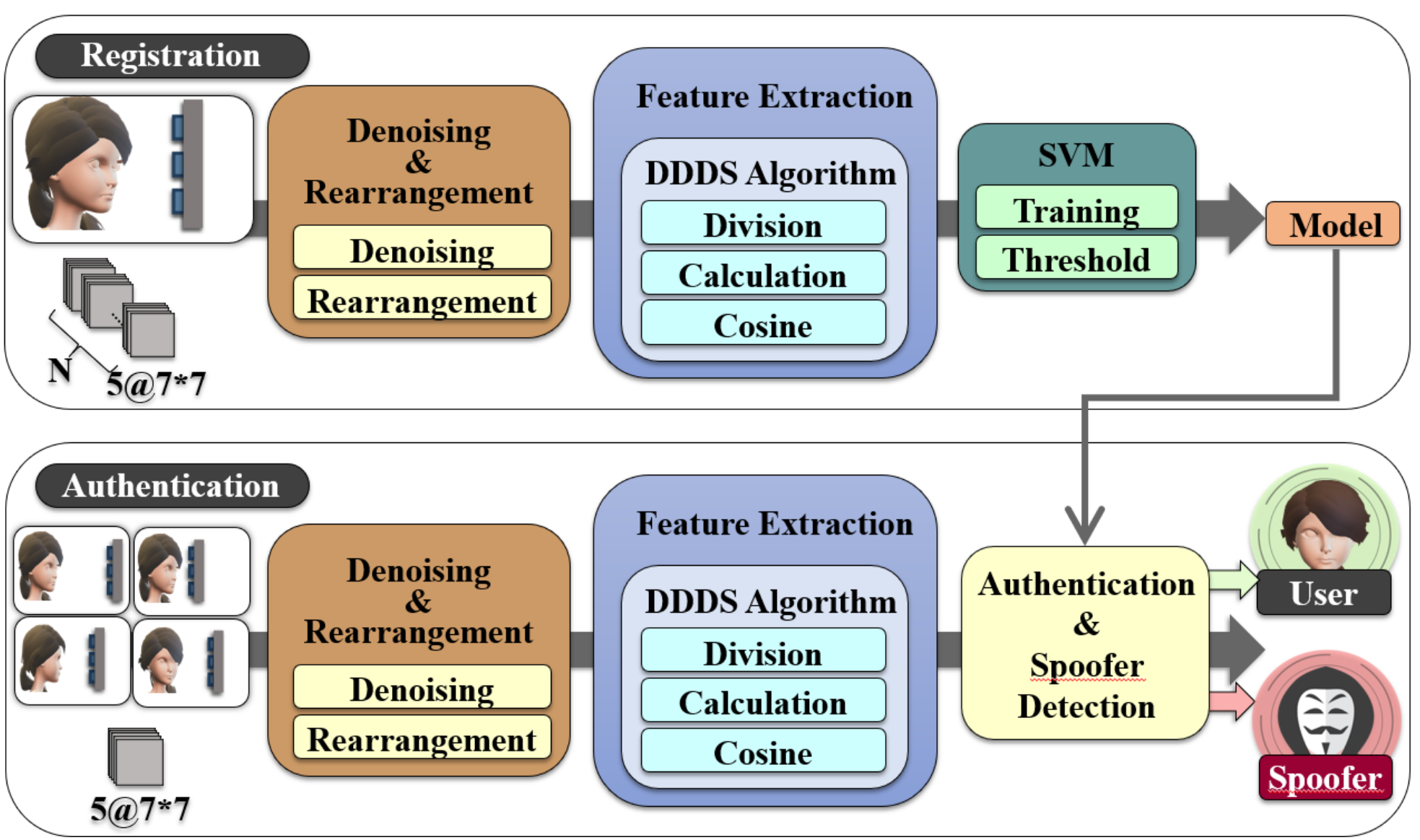
(a) Raw Phase (b) DDDS Phase (c) Raw RSS (d) DDDS RSS

Different Deflection Conditions



(a) Raw Phase (b) DDDS Phase (c) Raw RSS (d) DDDS RSS

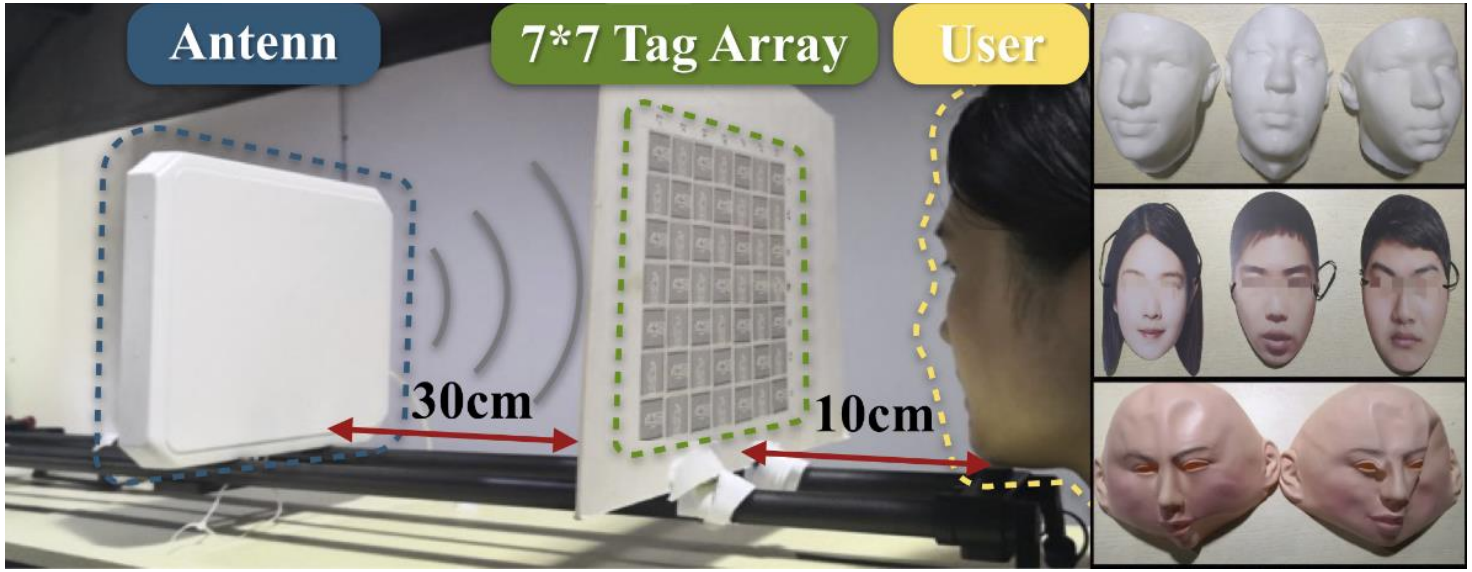
Anti-Spoofing Authentication



Evaluation

- **Experiment setting**
- **Overall performance**
- **Under different system settings**
- **Security assessment**

Experiment Setting



Volunteers
- 10 females and 20 males
- 5 spoofers and 25 legitimate users

Hardware
- Impinj R420 Reader
- Larid A9028 antenna
- Alien 9629 tag

Data collection

225 seconds for registration

120 times for authentication (1.25s each time)

The antenna is placed 30 centimeters away from the reader. The user poses her face 10 centimeters away from the tag array for registration or authentication.

Metric and Training Process

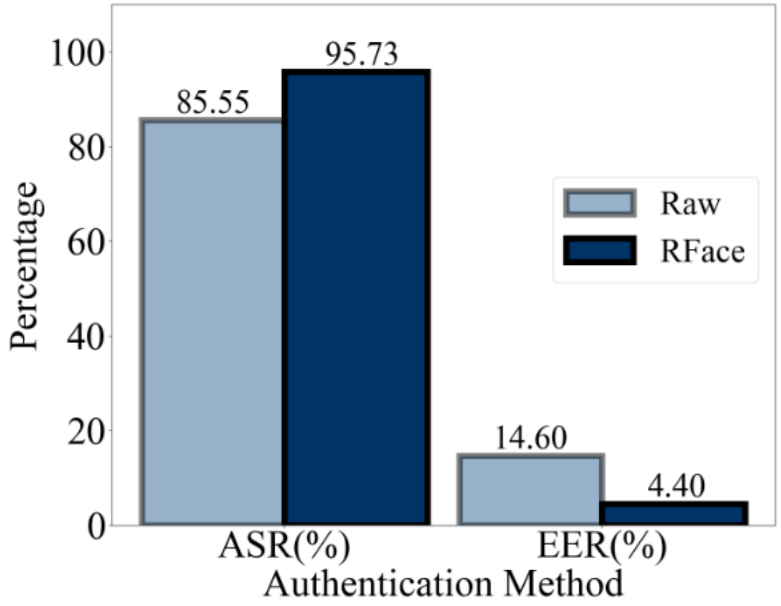
Metric

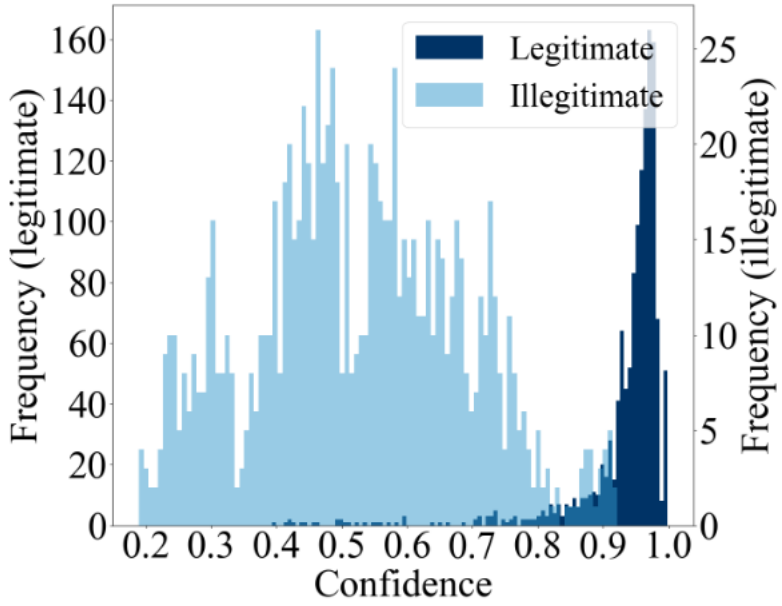
- **Authentication success rate (ASR)**
- **False Accept Rate (FAR)**
- **False Reject Rate (FRR)**
- **Equal Error Rate (EER)**
- **Defense Success Rate (DSR)**

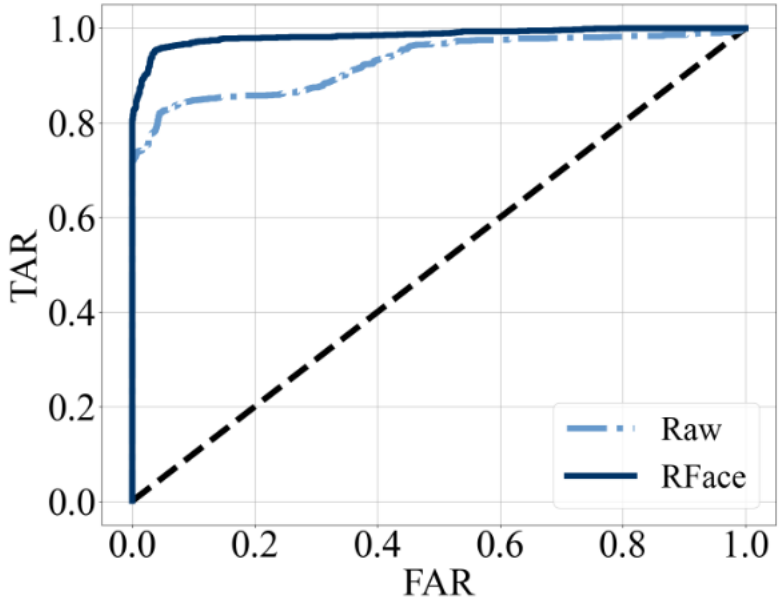
Training with 80% feature blocks and test with the rest 20% ones

The acceptance threshold is set as 0.8

Overall performance





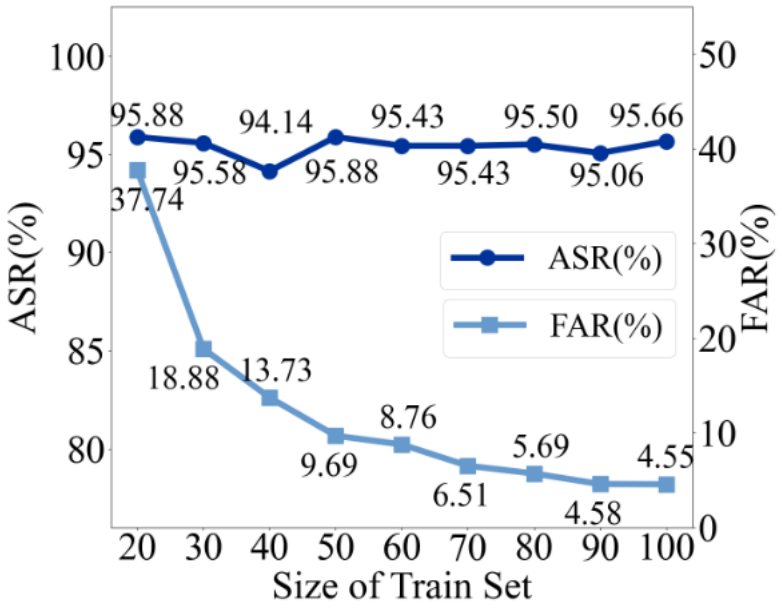


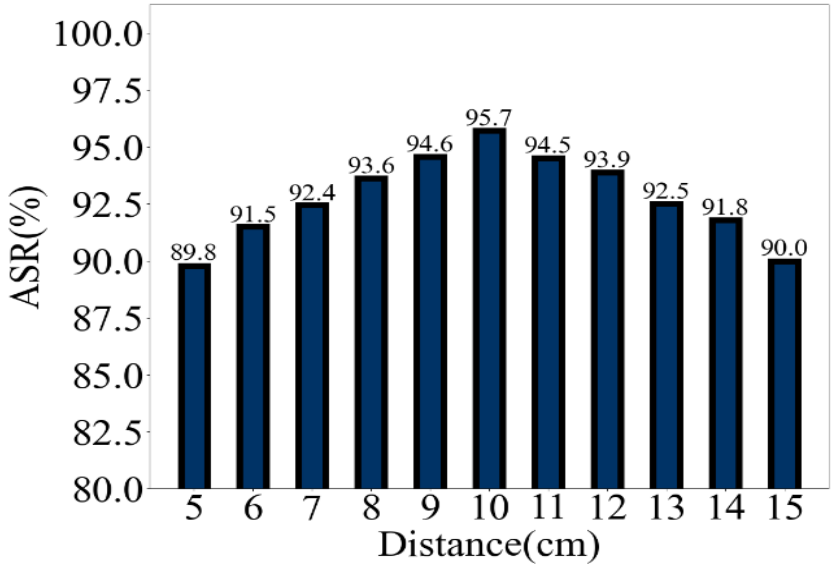
(1) The authentication success rate is 95.73% and the equal error rate is 4.40%

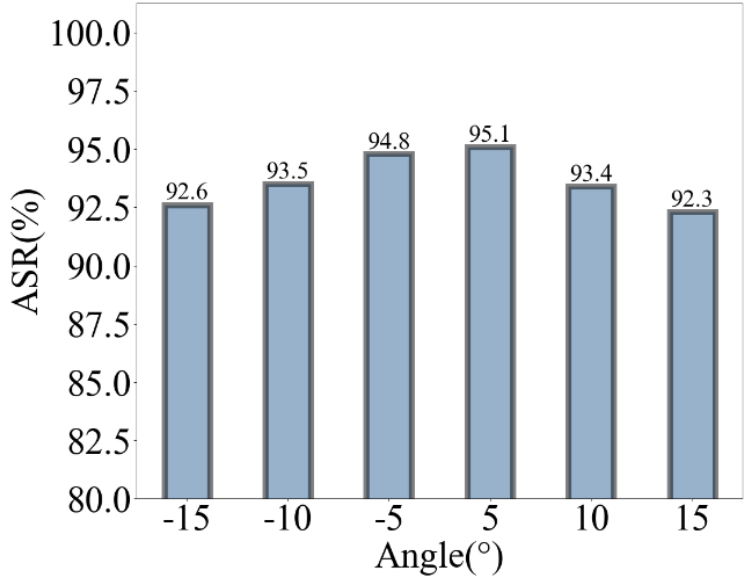
(2) The false accept rate is 4.48% when the acceptance threshold is 0.8

(3) The receiver operating characteristic curve shows the outstanding performance of RFace

Different Settings





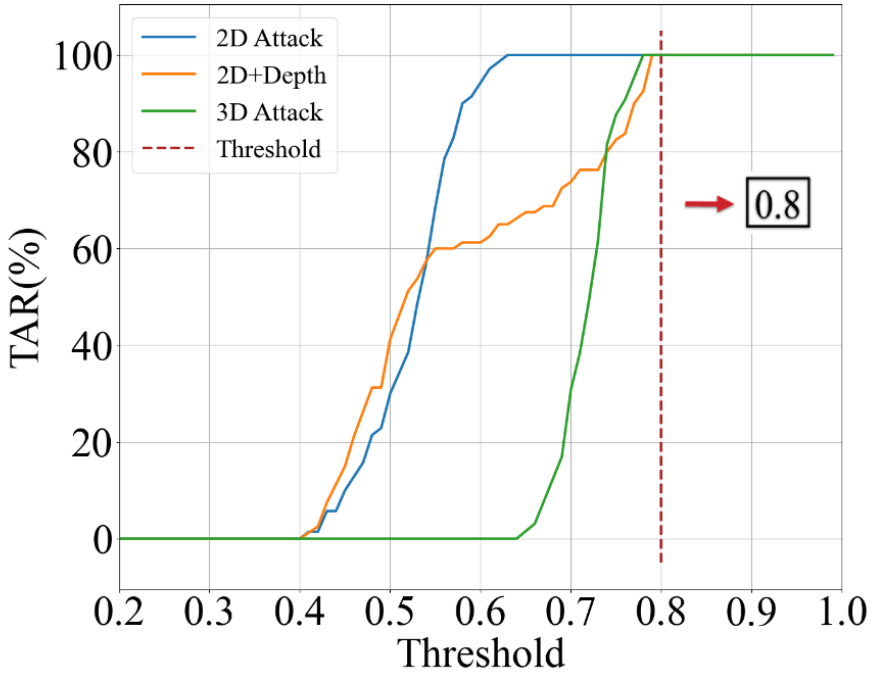


(1) With 90 feature blocks for each user, Rface achieves 95.5 authentication success rate

(2) The authentication reduces less than 6% even when the distance difference is 5 centimeters

Rface can still achieve high authentication success rate when deflection angle Is 15 degrees

Security Assessment



System	2D Attack Resistance	2D+ Attack Resistance	3D Attack Resistance	Privacy Preserved
Samsung FR [1]	×	×	×	×
EchoFace [2]	✓	✓	×	×
FaceHeart [3]	✓	✓	×	×
Face Flashing [4]	✓	✓	×	×
RFace	✓	✓	✓	✓

[1] https://www.samsung.com/global/galaxy/what-is/face-recognition/

[2] EchoFace: Acoustic Sensor-Based Media Attack Detection for Face Authentication, Internet of Things Journal, 2019

[3] Your face your heart: Secure mobile face authentication with photoplethysmograms, INFOCOM, 2017

[4] Face Flashing: a Secure Liveness Detection Protocol based on Light Reflections, NDSS, 2018

Conclusion

We propose a novel anti-spoofing facial authentication system via commodity RFID.

We prove that RF signals can be used to capture human biological features through a rigorous theoretical model.

We design a DDDS algorithm to improve the usability and practicality of our system, namely Rface.

RFace can achieve high authentication siccess rate, more importantly, it is able to defend against various spoofing attacks, which cannot be achieved by existing camera-based facial authentication systems