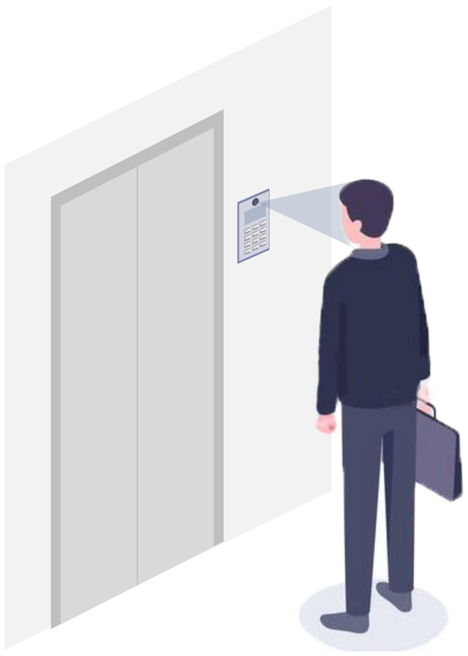
Mask Does Not Matter: Anti-Spoofing Face Authentication using mmWave without On-site Registration

Weiye Xu*^, Wenfan Song *^,Jianwei Liu *^, Yajie Liu *^, Xin Cui †, Yuanqing Zheng#, Jinsong Han *^, Xinhuai Wang†, Kui Ren *^

*Zhejiang University, Hangzhou, China
^ZJU-Hangzhou Global Scientific and Technological Innovation Center, Hangzhou, China
#The Hong Kong Polytechnic University, HongKong, China
† Xidian University, Xi'an, China

MobiCom 2022

Background: Face authentication is important

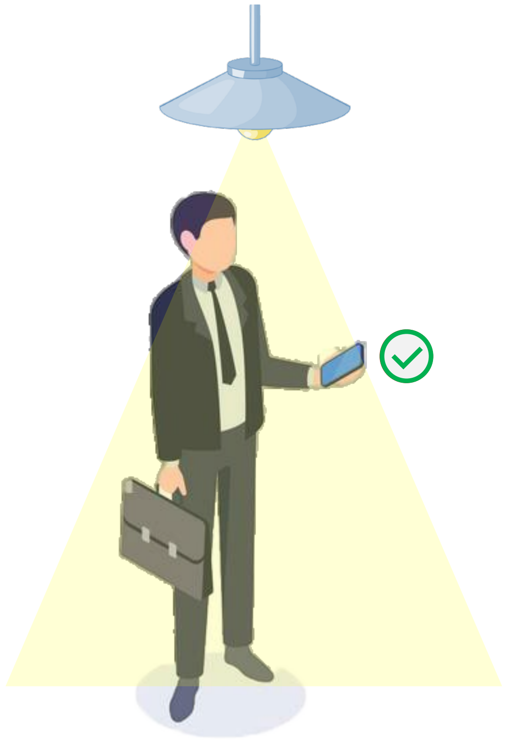


Access Control

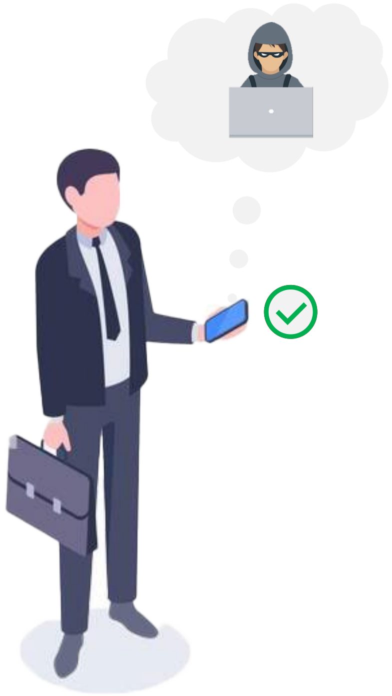
Online Payment

Individual Identification

Background: limitations of camera based Face authentication



Light Conditions



Spoofing Attacks

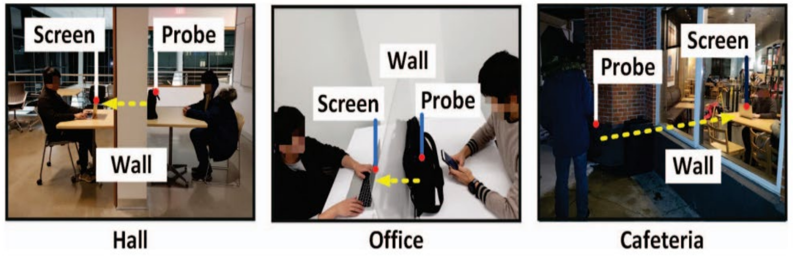
Occlusion

We want to explore
a *new facial authentication technique,* which is resilient to complex lighting conditions, *friendly to mask-wearing users*, and meanwhile *resistant to spoofing attacks*.

Turn to mmWave

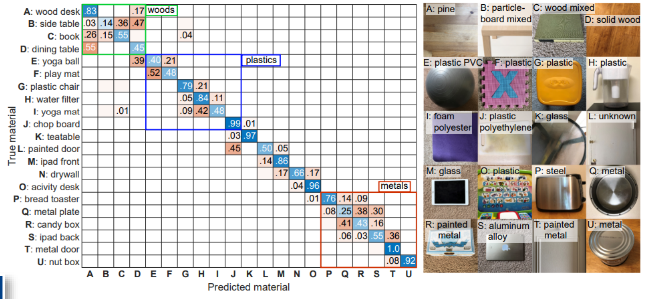
Penetrability

[Sheen et al. 2001]



[Li et al. 2020]

Material-sensitivity



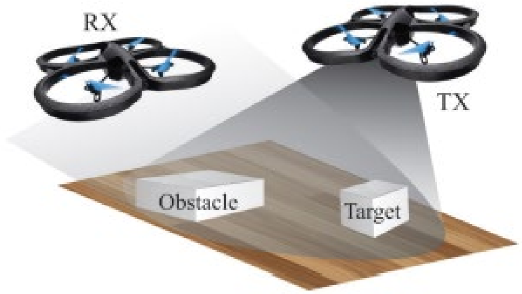
[Wu et al. 2020]

Advantages of mmWave

Fine-grained sensing capability

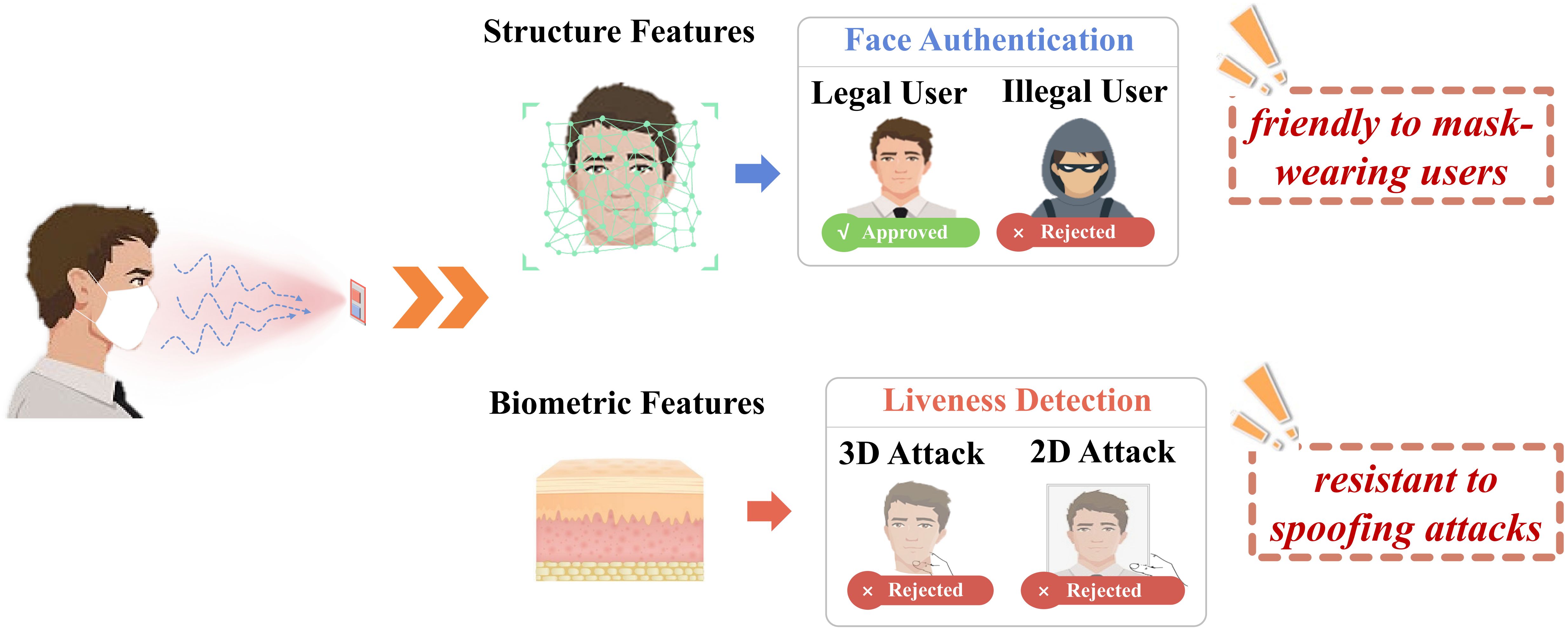
[Jiang et al. 2020]

Highly directional



[Zhu et al. 2015]

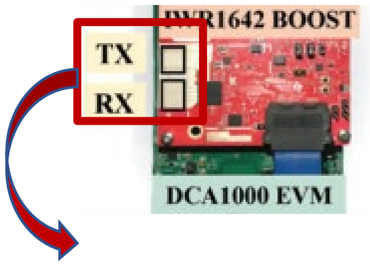
Basic idea


Structure Features
Face Authentication
Legal User
Illegal User
√ Approved
× Rejected
friendly to mask-wearing users
Biometric Features
Liveness Detection
3D Attack
2D Attack
× Rejected
× Rejected
resistant to spoofing attacks

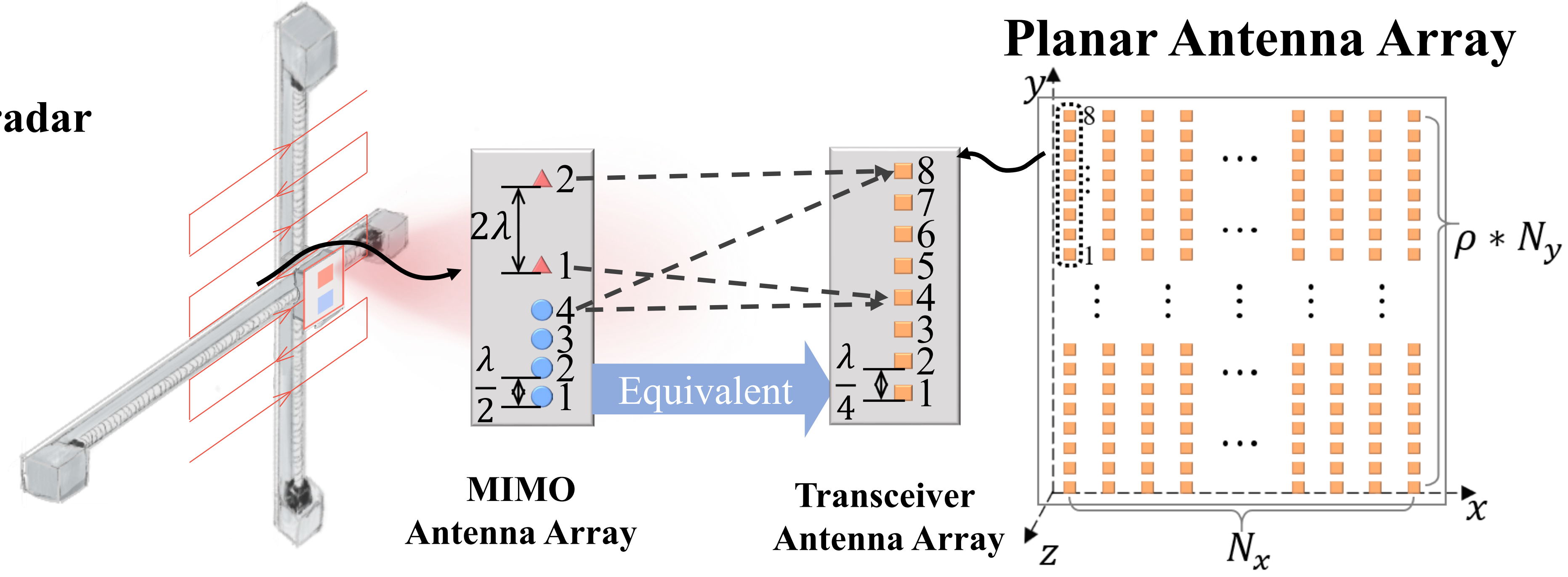
Enhancing the sensing resolution

Moving along a trajectory

Commercial mmWave radar



- ➢ ***few antennas***
- ➢ ***Small aperture***
- ➢ ***Limited sensing resolution***



- ➢ ***more antennas***
- ➢ ***large aperture size***
- ➢ ***millimeter-level fine-grained resolution***

Challenge 1: Mitigate the Registration Overhead

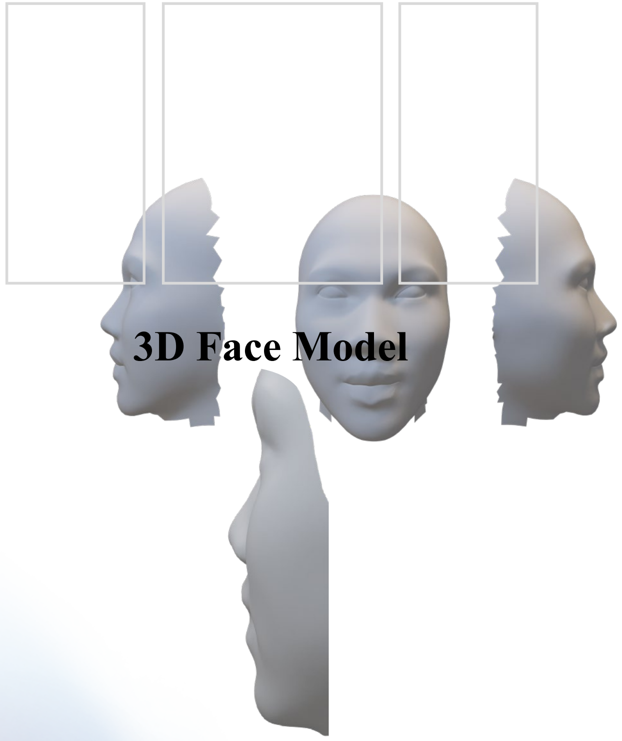
RF-based approaches usually require

- **on-site registration**
- **designated RF devices**
- **specific locations**
- **takes a long time**

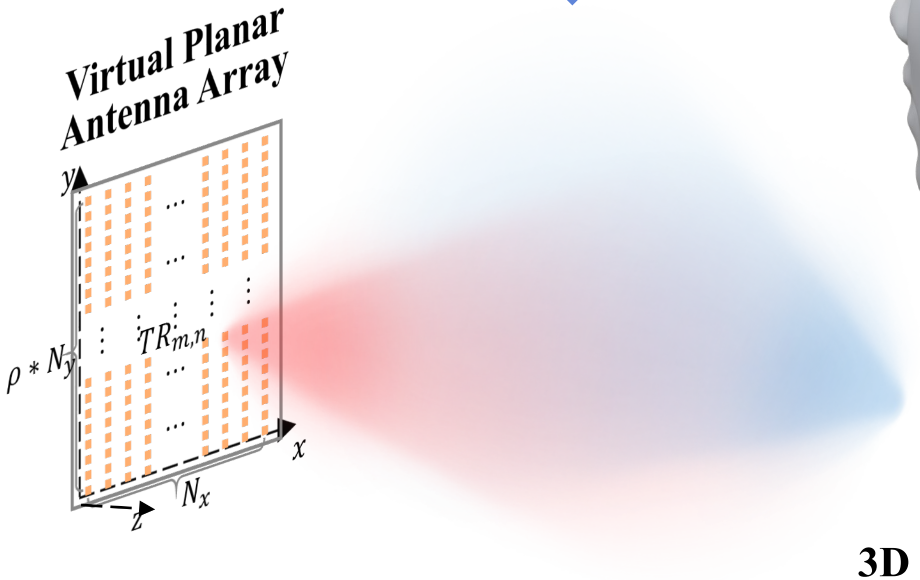
Complicated on-site registration prohibits the wide deployment!!

Virtual Registration Signal Generation

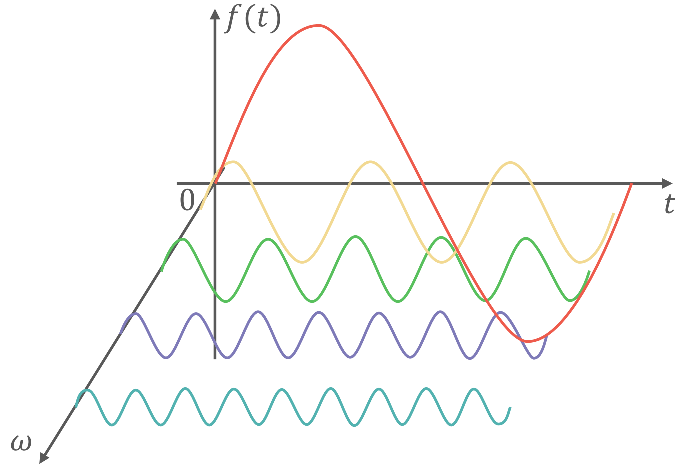
Three 2D Photos of the Face
in Different Perspectives



The key idea: **a *virtual registration* approach based on the *cross-modal transformation* from *photos to mmWave signals.***



3D Face Model



Virtual Registration Signal

Stage 1: transmitting from the radar to the face

$$\tau = {r_{m,n}}/{c}$$

$\in$: the reflection coefficient

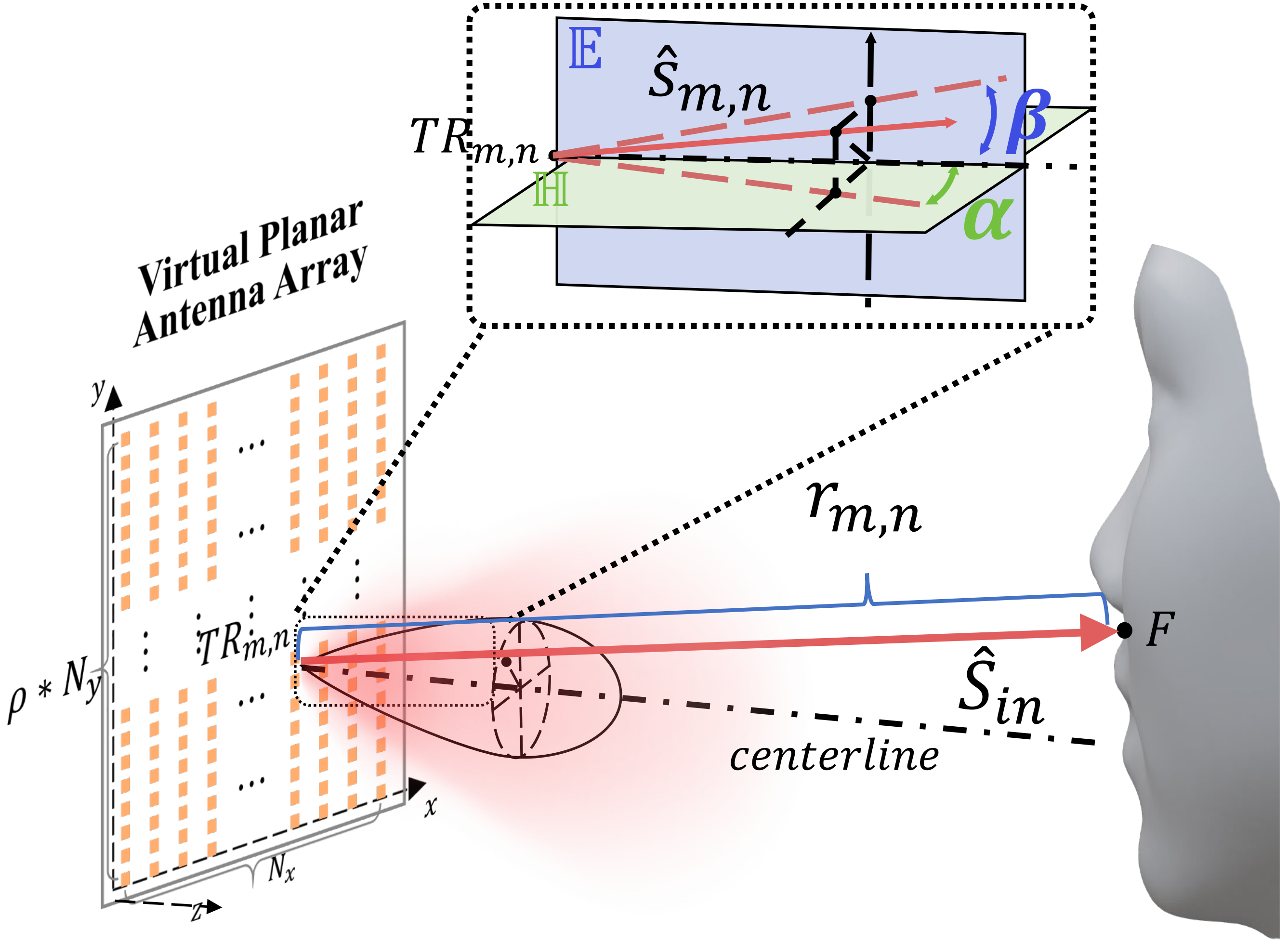
$\hat{S}_{m,n}$: the signal transmitted by $TR_{m,n}$

$$\hat{S}_{in} = \frac{\in \hat{S}_{m,n}(t-\tau)}{r_{m,n}} \boxed{p_{m,n}(F)}$$

$$p_{m,n}(F) = Ae^{[-\gamma(\frac{\alpha^2}{\alpha_h^2}+\frac{\beta^2}{\beta_h^2})]}$$

impact of the directionality of antennas

γ, α_h , β_h are constants determined by the physical characteristics of the antenna



3D Face Model

Stage 2: reflecting from the face to the radar

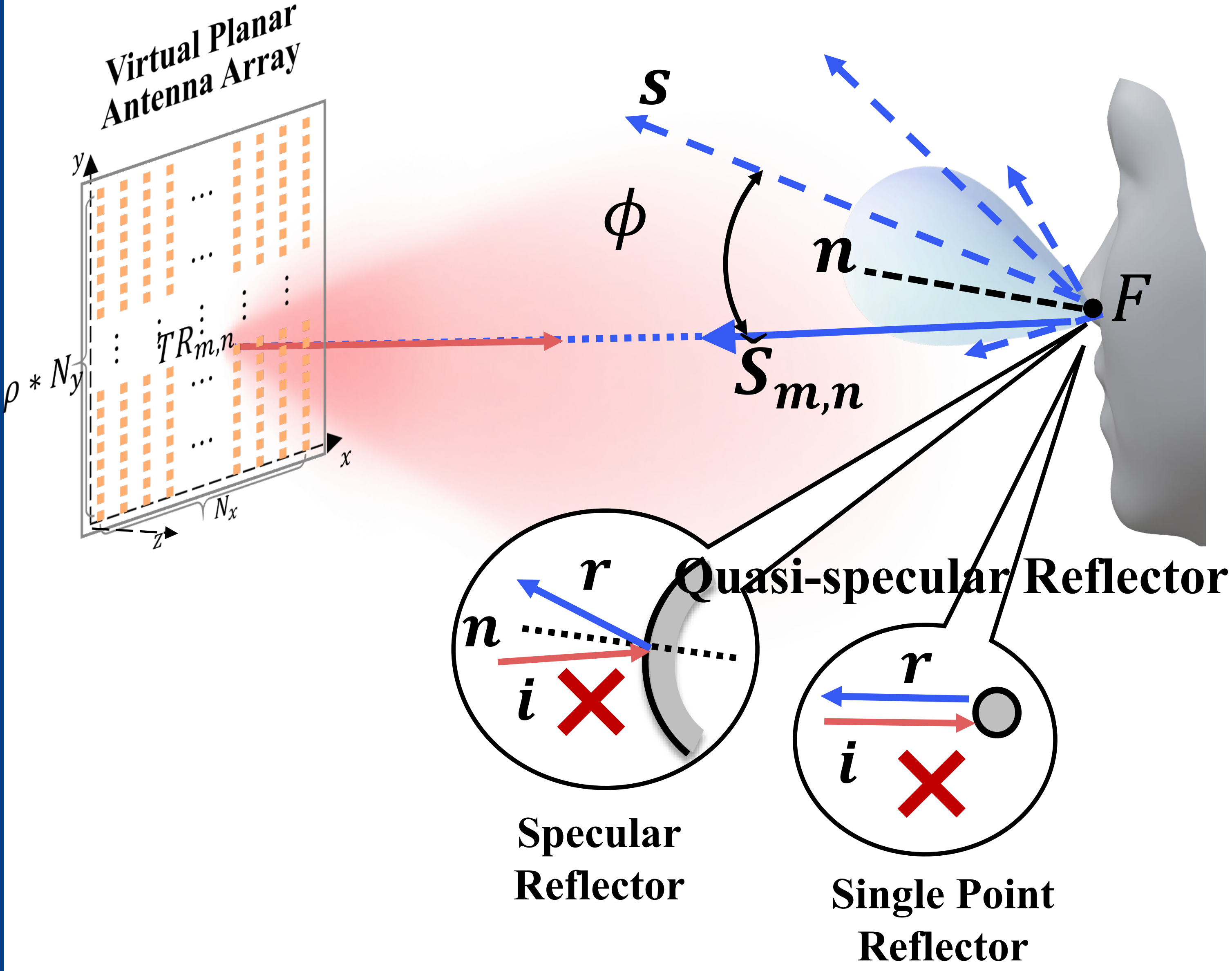
$$\check{S}_{m,n} = \boxed{\frac{\epsilon p_{m,n}(F)\hat{S}_{m,n}(t-\tau-\tau)}{r_{m,n}+r_{m,n}}}\ \boxed{g_{m,n}(F)}$$

impact of the propagation distance

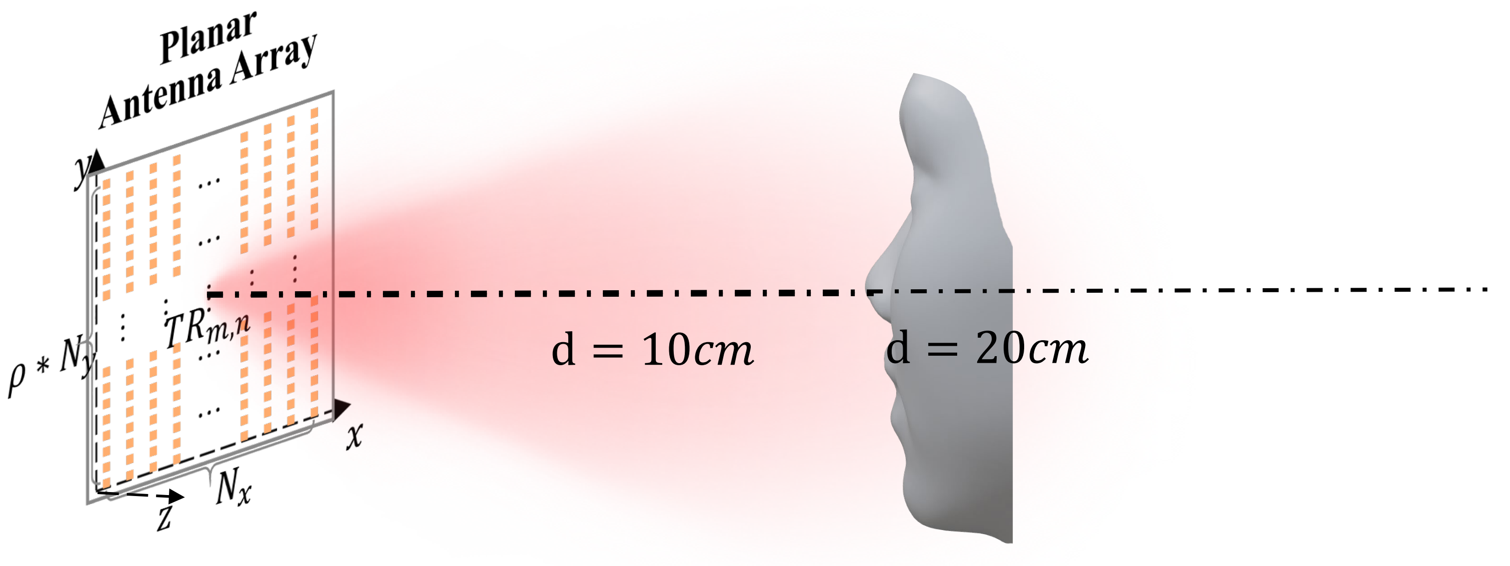
impact of the reflection characteristic of the face

$$g_{m,n}(F) = \exp(\phi^2/2\sigma^2)$$

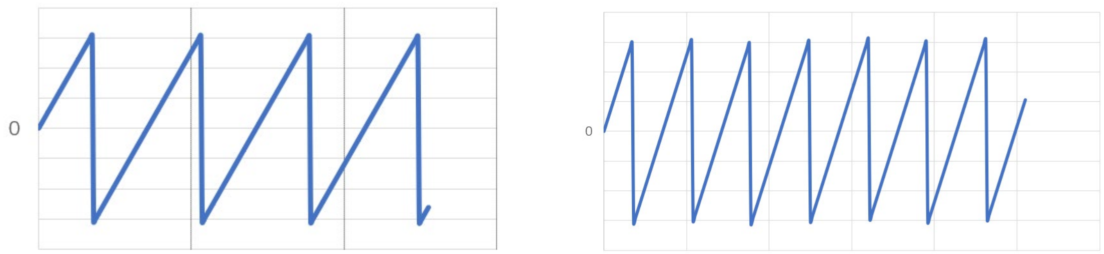
σ is a constant related to the reflection property of human face and relatively stable for different users.



Challenge 2: Robust FA under Variable Face-to-Device Distances

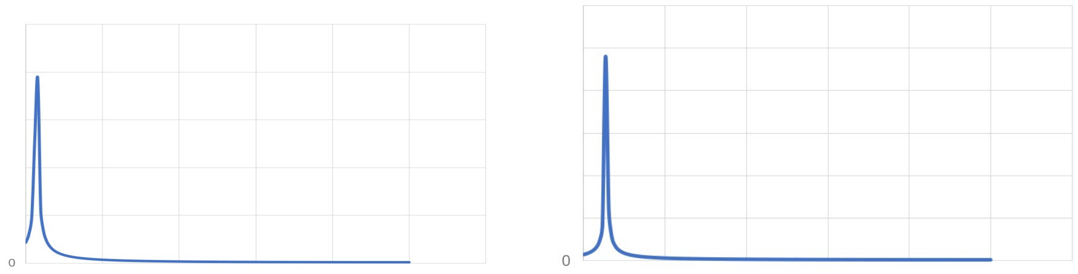


Phase



10cm **20cm**

FFT



10cm **20cm**

Extract **distance-resistant** facial structure features.

Imaging by SAR

3D Facial Image

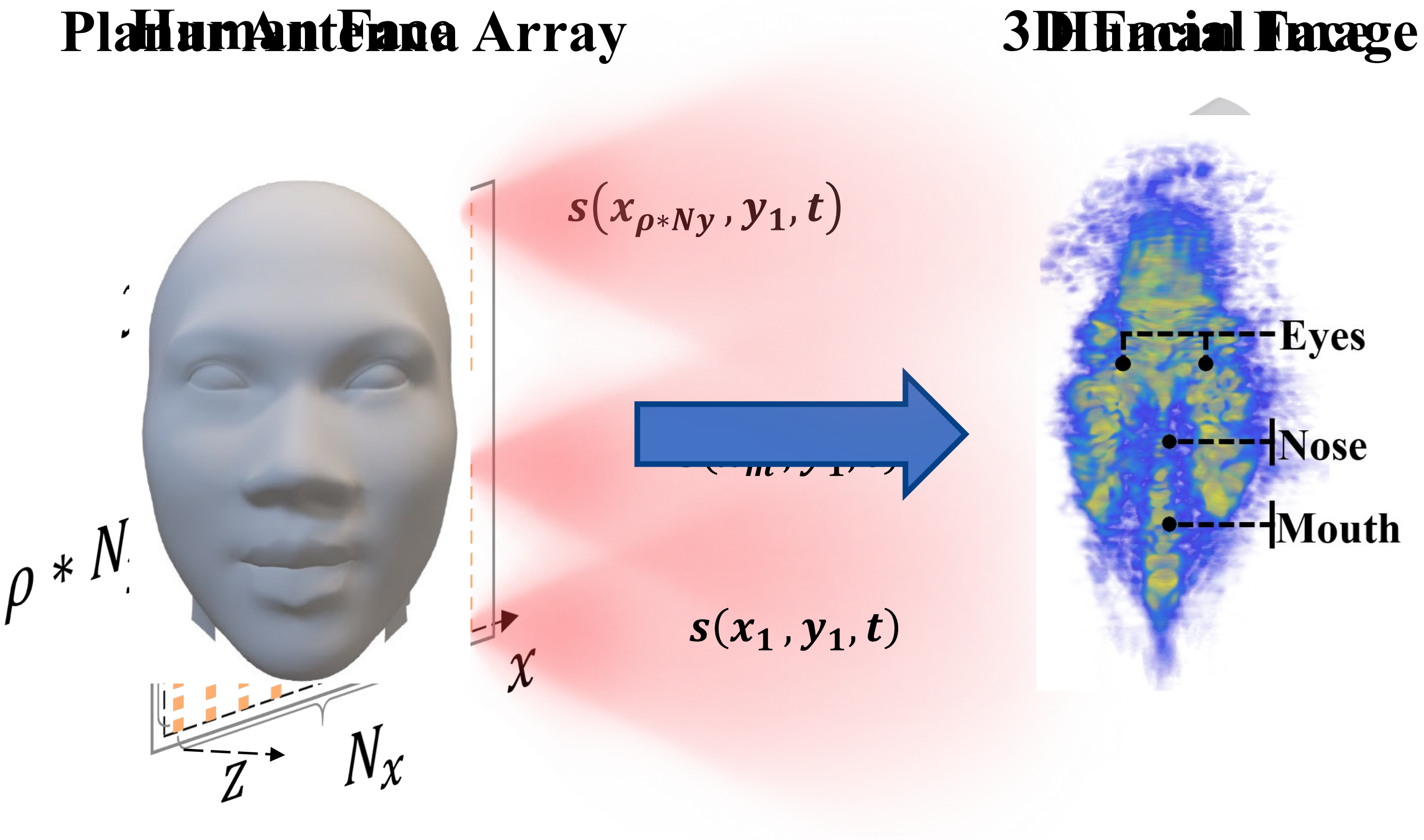
$$w(x',y',z')$$

$$=IFT_{3D}^{(k_x,k_y,k_z)}\{Stolt^{k_z}(s(k_x,k_y,k)k_z)\}$$

$$=\underbrace{\varepsilon o_{\{1,1\}}(x_F,y_F,z_F)}_{\text{distribution of the facial surface curvature}} * \underbrace{A(x,y)}_{\text{Position of the planar antenna array}}$$

Position of the planar antenna array
Related to the face-to-radar distance

distribution of the facial surface curvature

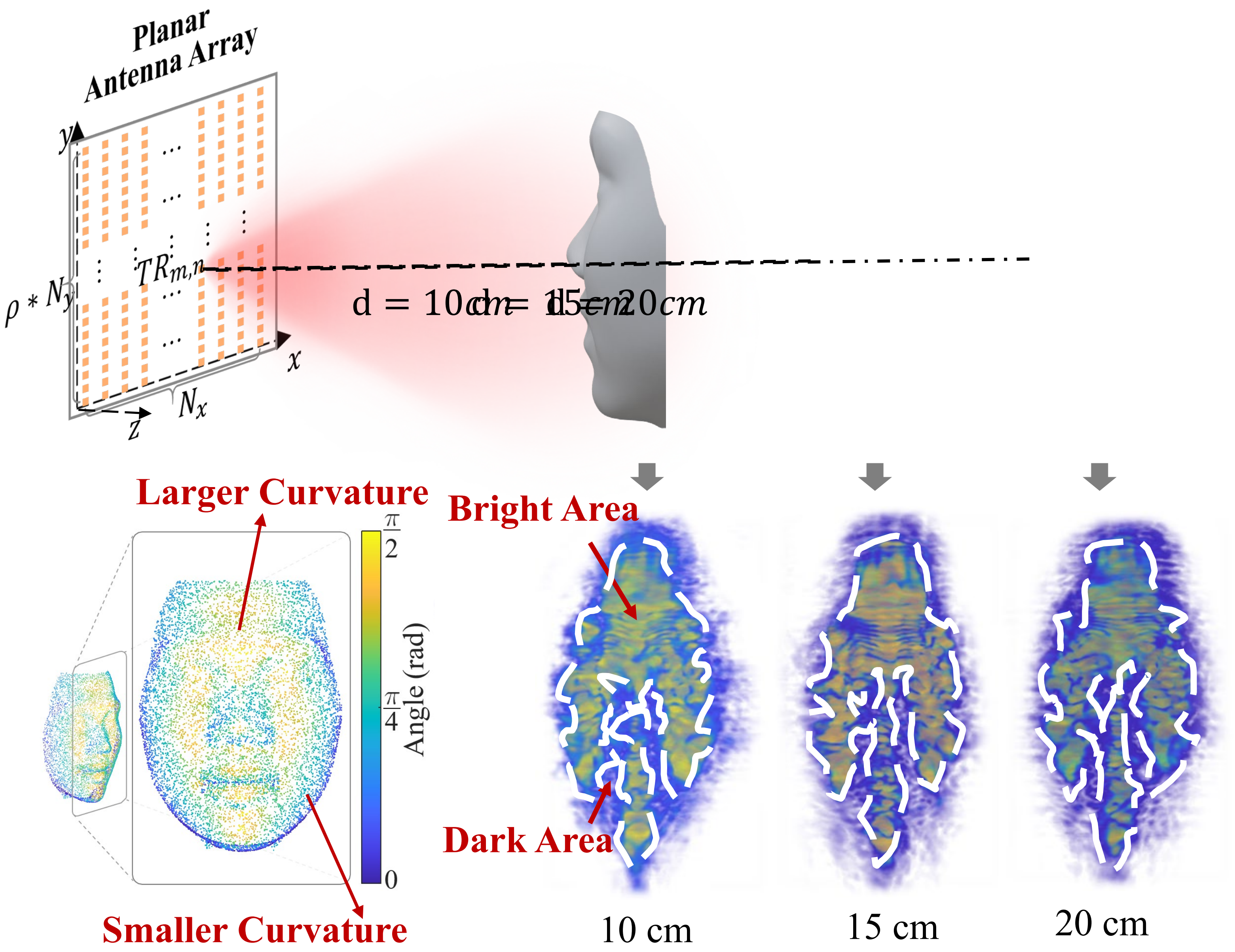


Observation

- “Bright Area" & “Dark Area“
- “Bright Area“ → Larger Curvature
  “Dark Area“ → Smaller Curvature
- Contour is stable

⬇

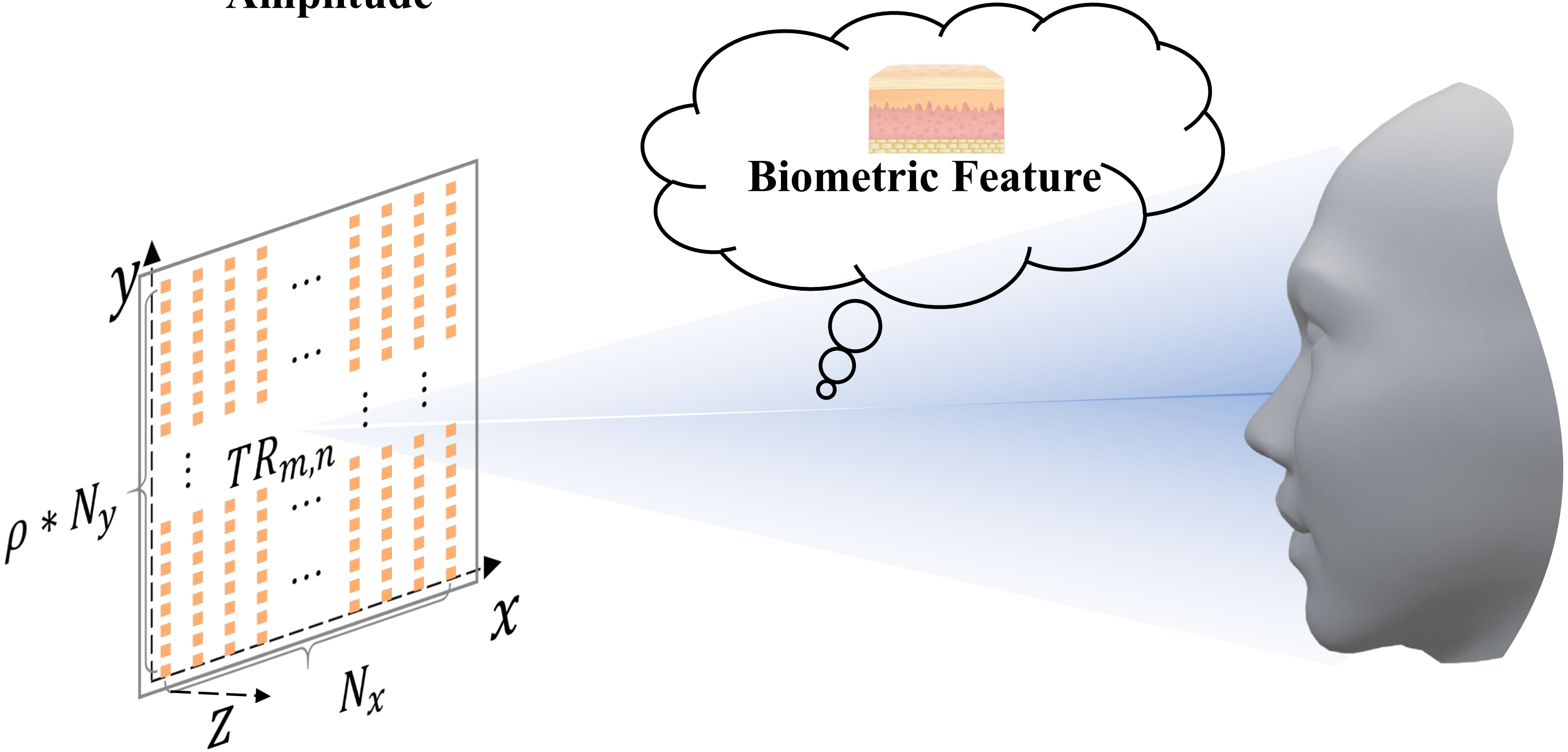
The contour of bright area can serve as the distance-resistant facial structure feature.



Challenge 3: Reliable Liveness Detection for Faces with Complex Structure

$$\underbrace{A_{m,n}}_{\text{Amplitude}} = \underbrace{\varepsilon}_{\text{Reflection Coefficient}} \iiint \frac{\boxed{o_{m,n}(F)}}{2r_{m,n}} dx_F dy_F dz_F$$

Facial Surface Curvature



Extract Biomatric Features

Step 1：

Selecting relatively flat regions

$$A_{m,n} = \varepsilon \boxed{\iiint} \frac{o_{m,n}(F)}{2r_{m,n}} dx_F dy_F dz_F \qquad \boxed{\Gamma \rightarrow \Gamma'}$$

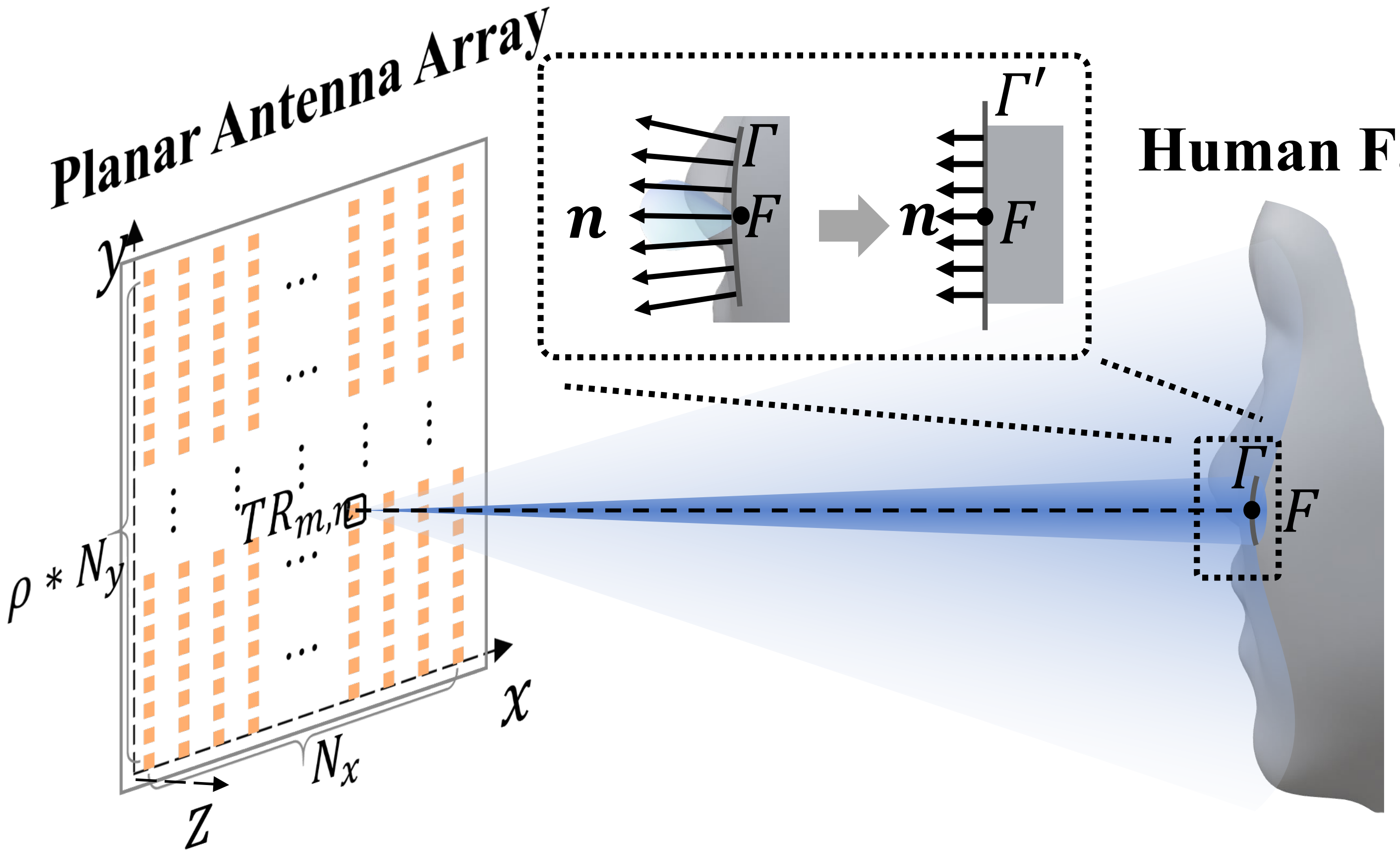
$$\approx \varepsilon \mathrm{N}^* \frac{\boxed{o_{m,n}(F)}}{2r_{m,n}} \rightarrow 1$$

$$\approx \frac{\varepsilon \mathrm{N}}{2r_{m,n}}$$

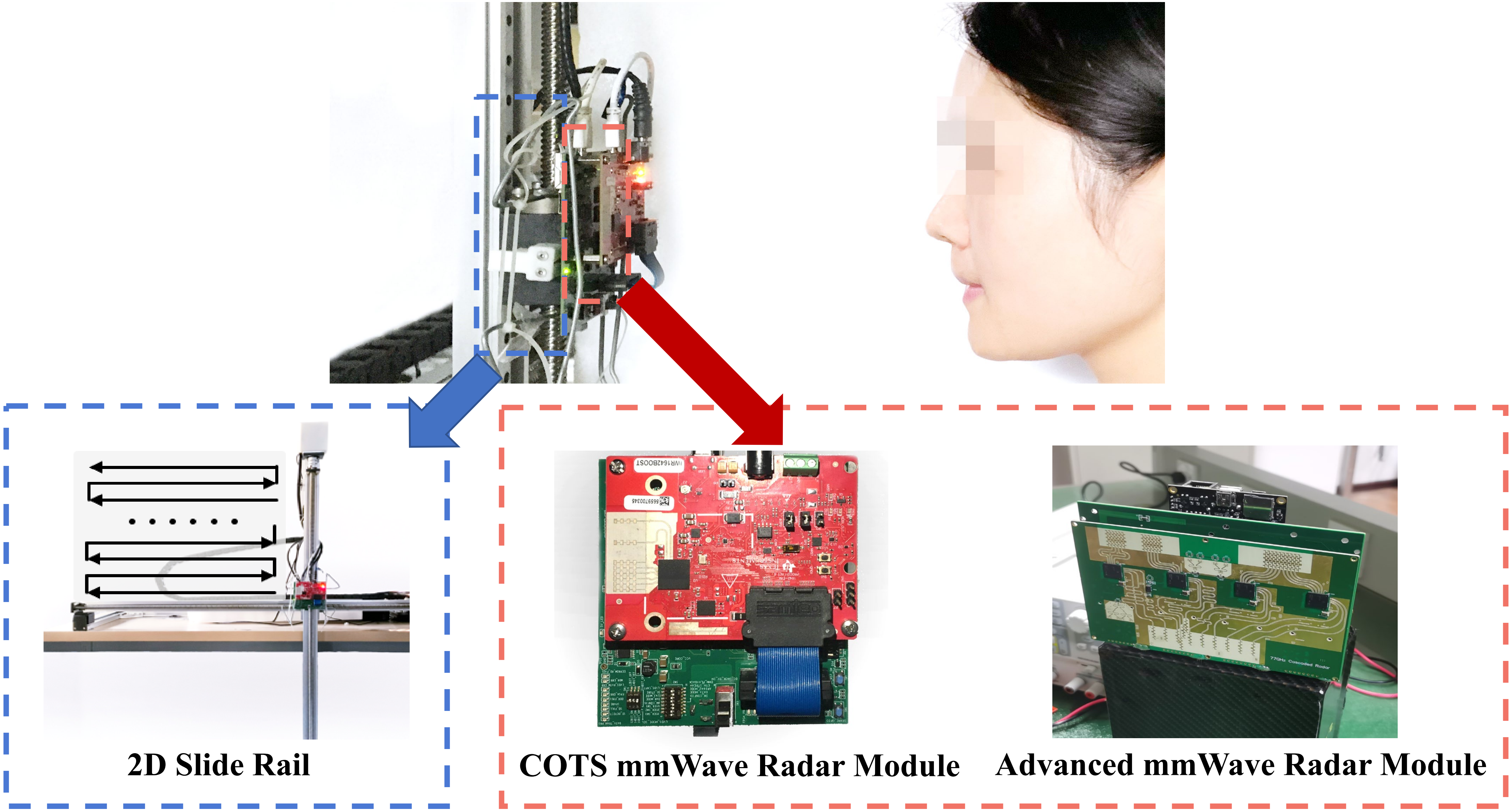
Step 2：

Biometric identification

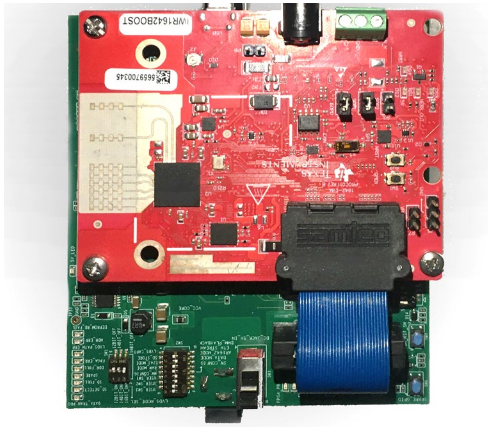
$$\varepsilon = \frac{A_{m,n}}{\mathrm{N}} * 2r_{m,n}$$



Experiment Setup



Experiment Setup



COTS mmWave Radar Module

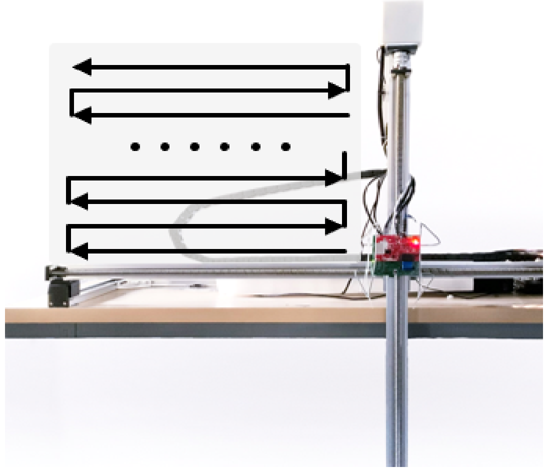
COTS mmWave Radar Module

- mmWave radar board: TI IWR1642-Boost

  Data acquisition board :TI DCA1000EVM
- 2 transmitting antennas

  4 receiving antennas

  8 transceivers

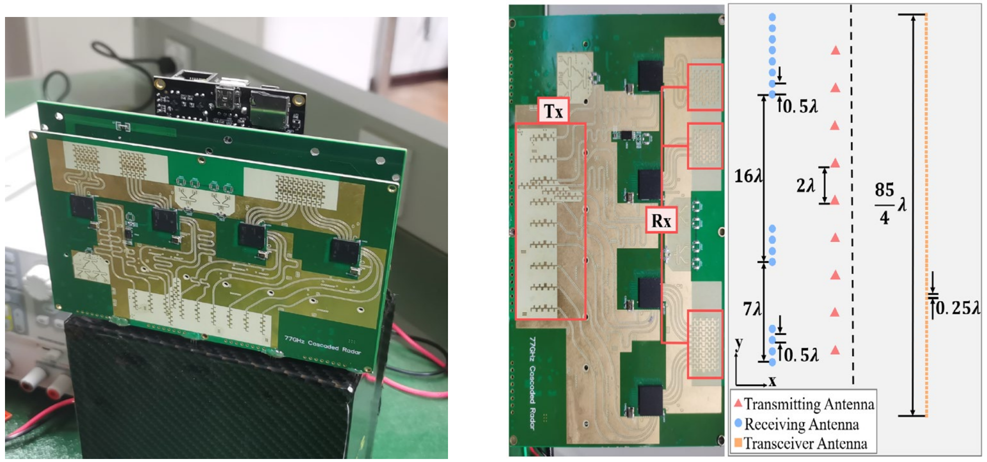


2D Slide Rail

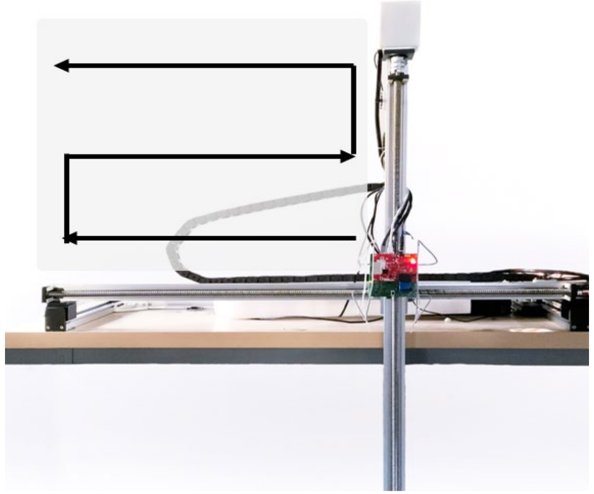
2D Slide Rail

- Size of the 2D scanning plane: 200mm*240mm
- Scanning speed: 0.5m/s
- Number of rows:30
- Sweeping delay: 13s

Experiment Setup



Advanced mmWave Radar Module



2D Slide Rail

Advanced mmWave Radar Module

- 4 TI AWR1243P radar chips
- 9 transmitting antennas

  12 receiving antennas

  86 transceivers

2D Slide Rail

- Size of the 2D scanning plane: 200mm*240mm
- Scanning speed: 0.5m/s
- Number of rows: 3
- Sweeping delay: < 2s

Data Collection & Metrics

Data Collection

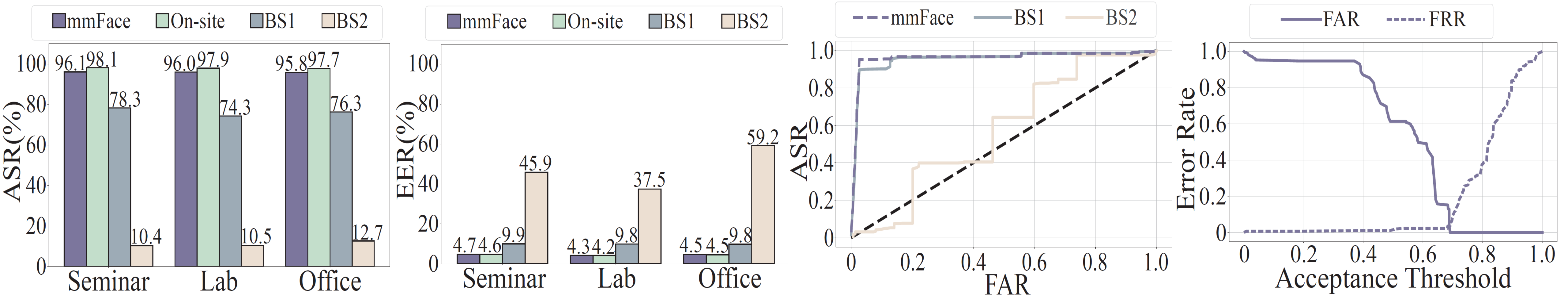
- 3 environments: seminar room & lab & and office
- 30 volunteers: 20 males & 10 females;

  5 spoofers & 25 legitimate users
- Face-to-Device Distance: 15cm
- 120 authentication attempts for each volunteer

Metrics

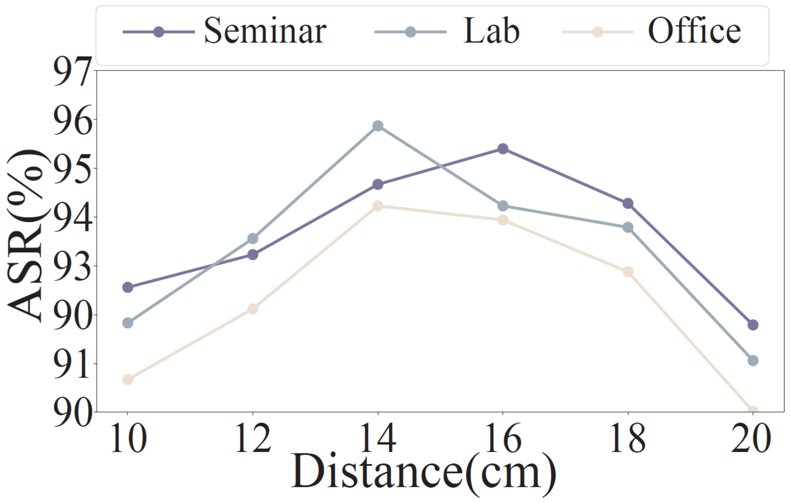
- False Accept Rate (FAR)
- False Reject Rate (FRR)
- Equal Error Rate (EER)
- Authentication success rate (ASR)
- Receiver Operating Characteristic (ROC)
- Defense Success Rate (DSR)

Overall Performance

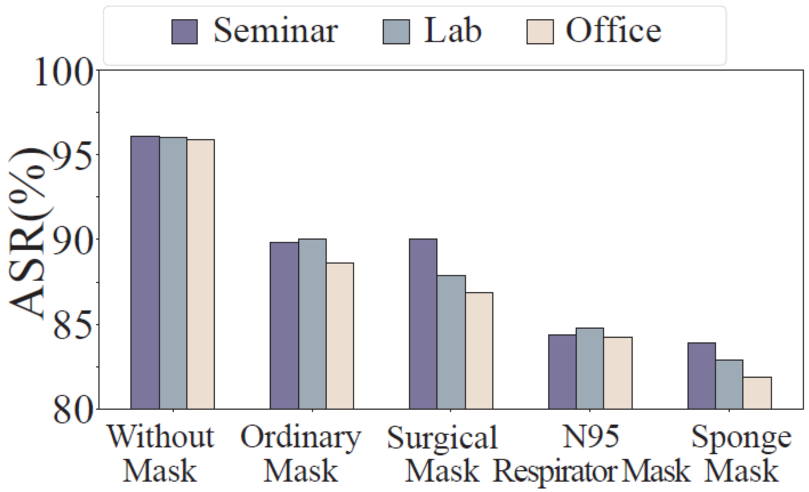


- The performance of facial structure feature extraction method is outstanding.
- mmFace can generate virtual registration signals accurately while mitigating the overhead of user registration.
- The ROC and FAR-FRR curves also show the outstanding performance of mmFace.

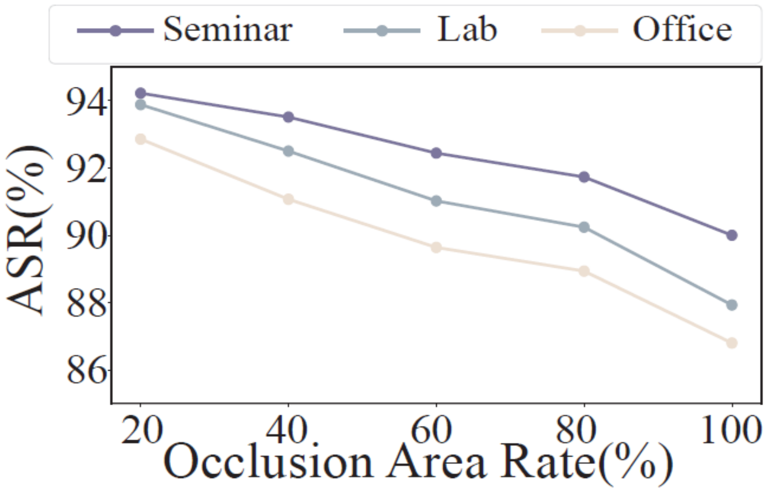
Robustness

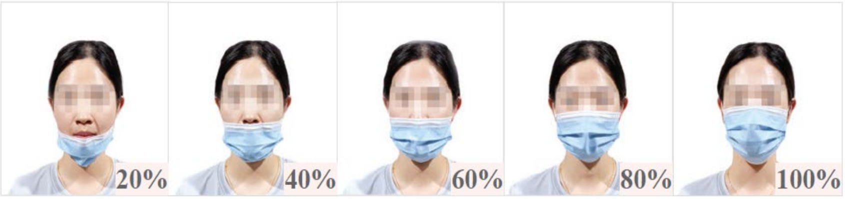


- 12 volunteers
- 10cm to 20cm with a step of 2cm



- 12 volunteers
- ordinary masks, surgical masks, N95 respirator masks, and sponge masks





Robust to various face-to-device distancs

Robust to different types of masks

Robust to the occlusion area of masks

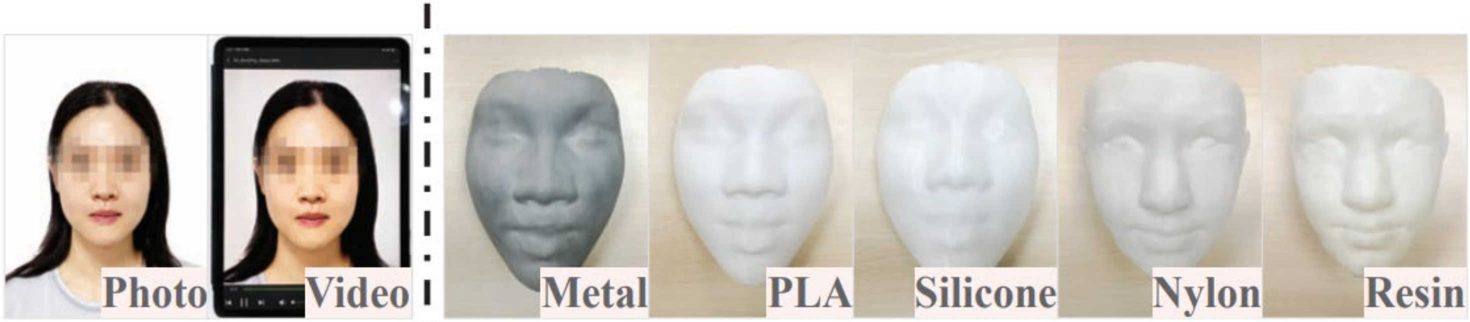
Attack and Defense

Spoofing attack realization

- Two types of 2D spoofing attacks
- Five types of 3D spoofing attacks

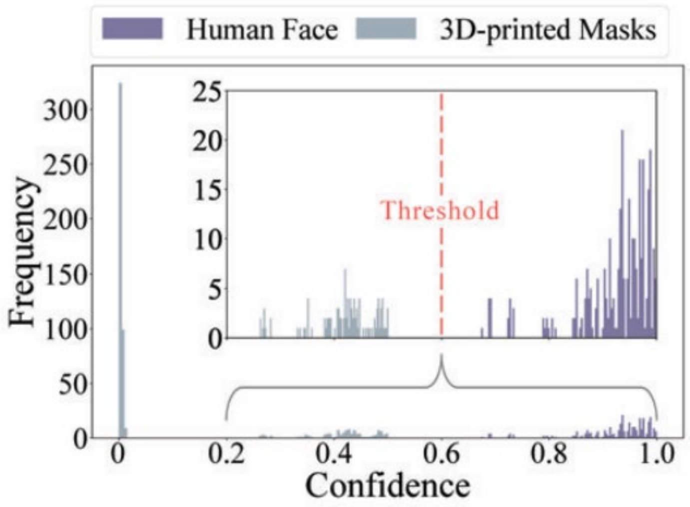
Defensive capability analysis

- All 2D spoofing attacks cannot deceive mmFace
- mmFace can distinguish real human faces from 3D-printed masks
- mmFace can effectively defend against 3D spoofing attacks under the distance variation

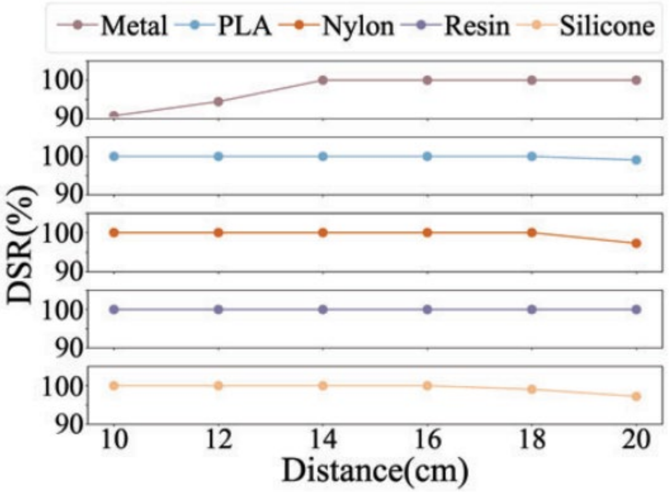


2D Spoofing

3D Spoofing



Confidence outputs of one-class SVM



Impact of distance on DSR

Conclusion

- **We develop a practical mmWave-based FA system that can still work well under the occlusion of face masks.**
- **We propose a virtual registration approach to avoid inconvenient on-site registration.**
- **We explore a distance-resistant facial structure features to achieve robust FA and an effective biometric feature to realize reliable liveness detection.**
- **We prototype two typical modes of mmFace and demonstrate that mmFace can realize precise and robust authentication as well as defend against spoofing attacks.**

Thank you!

Q&A