# Face Presentation Attack Detection (a.k.a. Face Anti-spoofing)

P C Yuen

Department of Computer Science
Hong Kong Baptist University

# Outline

1. Background and Motivations
2. Face Presentation Attack Detection: Review
3. Face Presentation Attack Detection: Our work
4. Conclusions

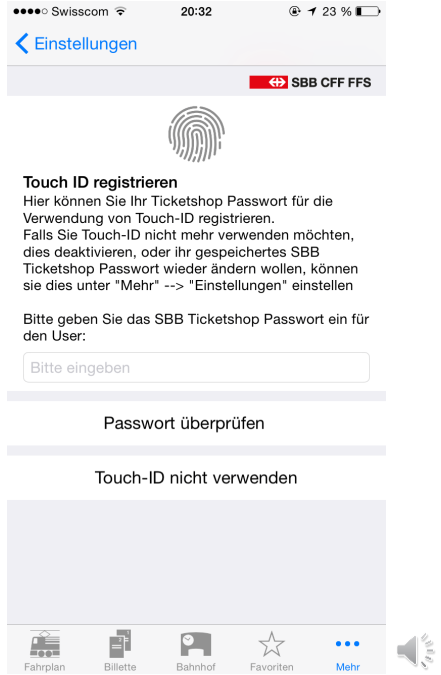
# Background and Motivations

- Deployed biometrics practical applications

Border Control

Door Access Control

Touch ID (iPhone)




SBB for buying ticket

# Background and Motivations

- Face Recognition Technology

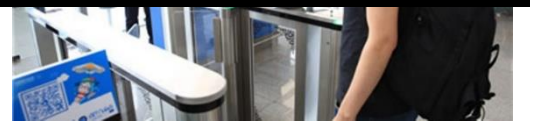
Jack Ma's first unmanned supermarket

Today, on a street in Hangzhou (Zhejiang province), Jack Ma's first unmanned supermarket officially opened for business. Because there are no costs for manpower, the expenses for running the unmanned supermarket only add up to about a quarter of those of traditional supermarkets. The shop owner just needs to replenish the inventories every morning - nothing else needs to be done.

*Entrance to the unmanned supermarket*

**MIT Technology Review:**
**10 breakthrough technologies 2017**


face-recognition payment Alipay



'World's first' facial recognition ATM unveiled in China

PUBLISHED : Sunday, 31 May, 2015, 6:38am
UPDATED : Monday, 01 June, 2015, 11:31am

COMMENTS: 2

Source: china.com and iomniscient.com

# E-payment using Facial Recognition Technology in China

https://www.youtube.com/watch?v=9HHWomj2EDc

# Background and Motivations


Passenger flow analysis


Pay-per-laugh: the comedy club that charges punters having fun

Image from http://www.yunbiao.tv/web/news/casenavdetail195.html
Image from https://www.huaweicloud.com/zhishi/frs3.html

# Background and Motivations

## Is Face Recognition Secure?

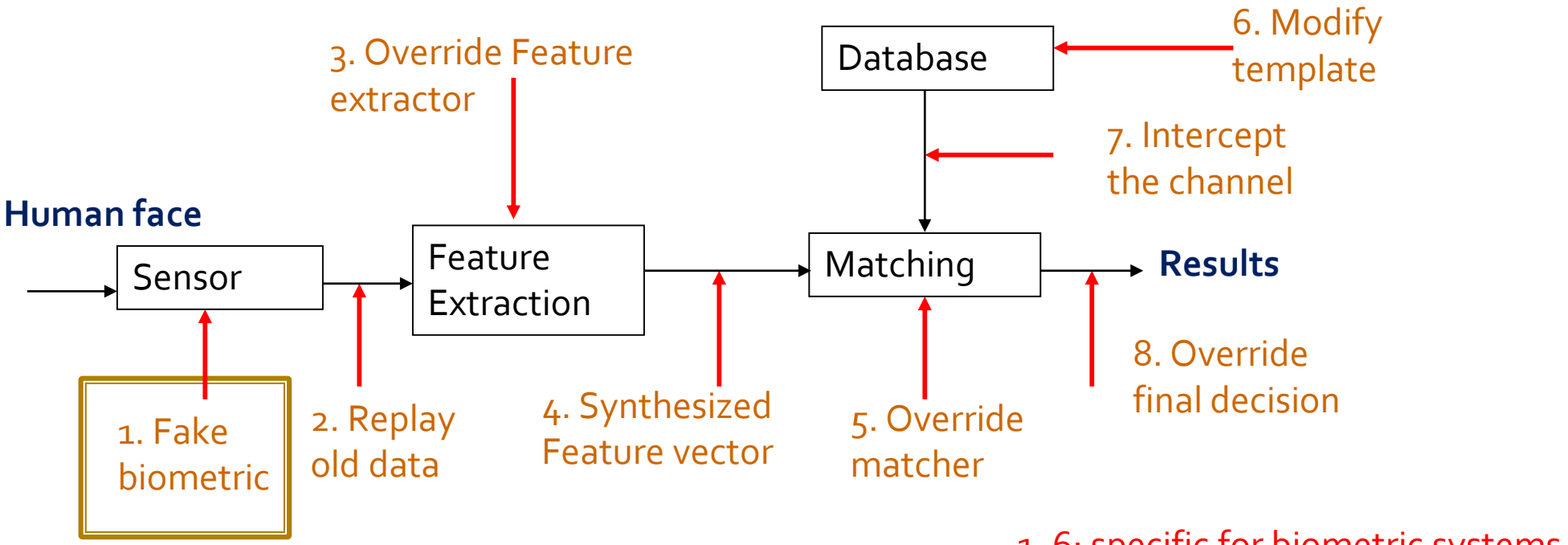

Student spoof the face recognition system of auto courier cabinet with a photo print

News from https://www.sohu.com/a/347612078_115479

# What happens if
# a face recognition system is NOT secure?

# Background and Motivations

- Vulnerabilities: Ratha *et al*. [IBM Sys J 2001] pointed out eight possible attacks on biometric systems



# Background and Motivations

- Face Presentation Attack Detection (PAD)
  - Face information can be easily acquired (facebook, twitter) and abused
  - 3 popular attacks: Print (image), Replay (video), and 3D mask


Low Cost

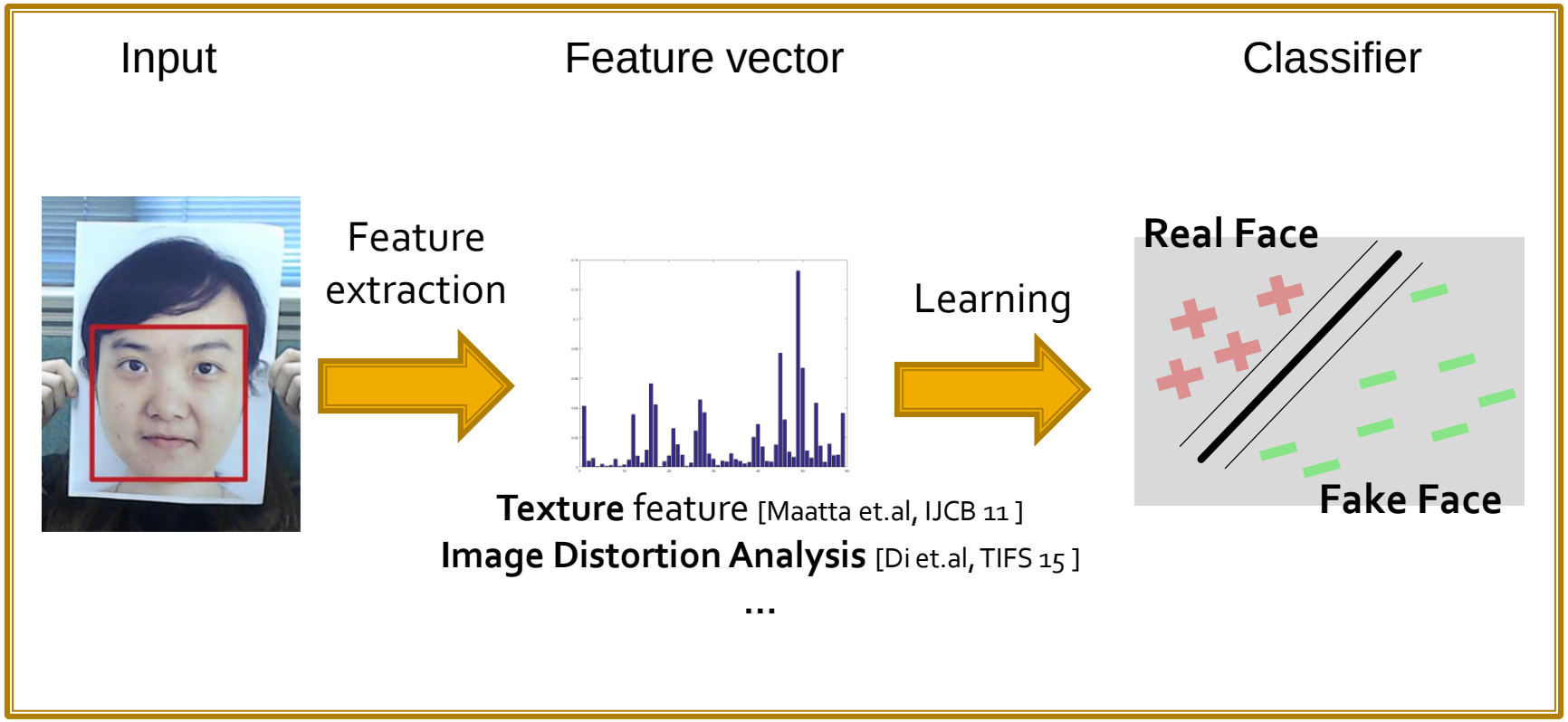
High cost, but hard to detect

# Image and Video Face PAD

- Review on existing approaches
  - Appearance-based
  - Motion-based
  - Deep Representation Learning
  - Domain Adaptation and Generalization

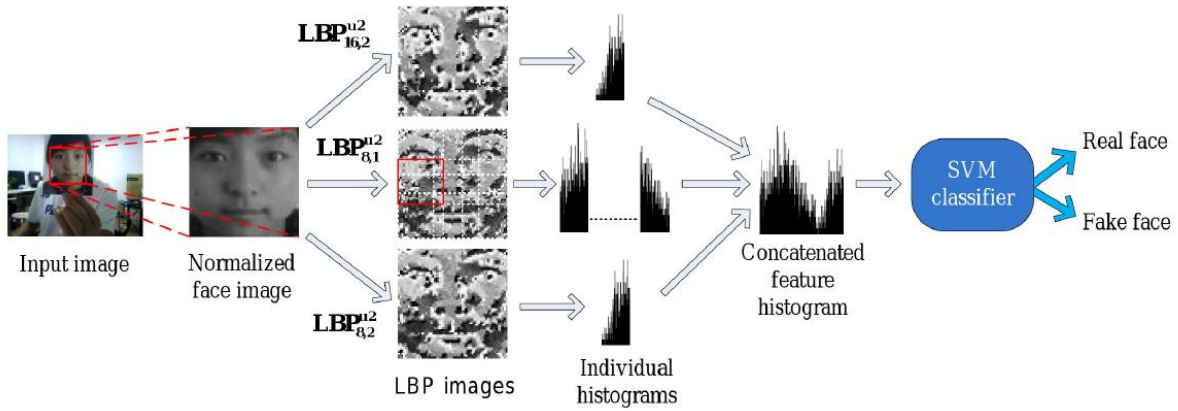
# Image and Video Face PAD

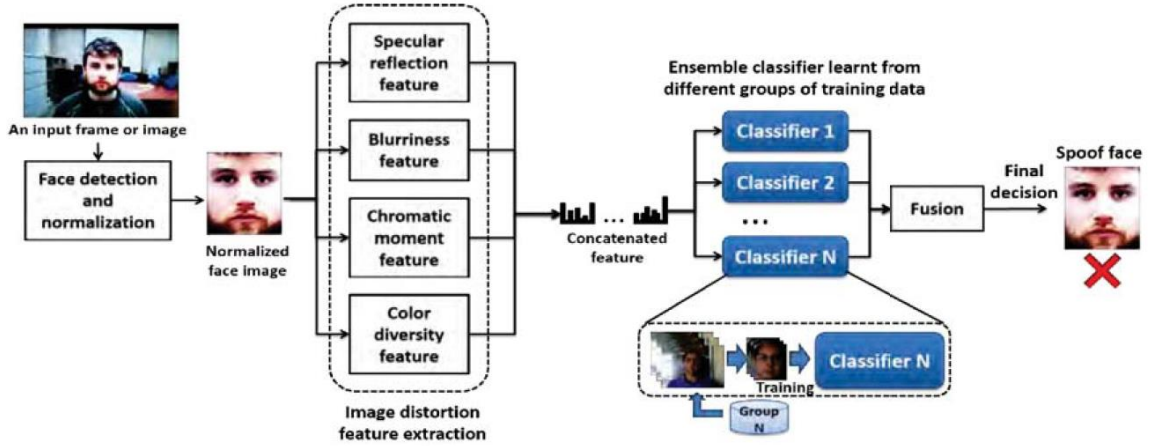
- Anti-spoofing approach: Appearance-based
  - Spoof media (print and screen) and genuine face has different appearance



# Image and Video Face PAD

- Anti-spoofing approach: Appearance-based
  - Spoof media (Prints and screen) has different texture, comparing with genuine face



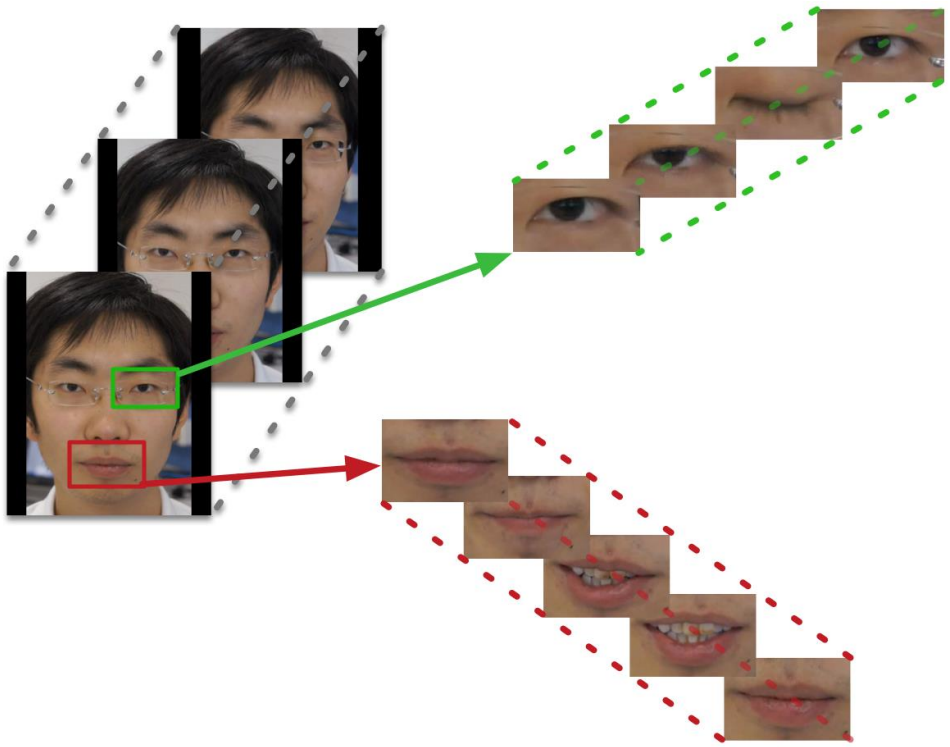




Jukka Maatta, Abdenour Hadid, Matti Pietikainen, "Face Spoofing Detection From Single Images Using Micro-Texture Analysis", *IJCB* 2011

Di Wen, Hu Han, Anil K. Jain, "Face Spoof Detection with Image Distortion Analysis", *TIFS* 2015

# Image and Video Face PAD

- Anti-spoofing approach: Motion-based
  - 2D spoofing medium cannot move, or has different motion pattern compare with real face



# Image and Video Face PAD

- Anti-spoofing approach: Motion-based
  - **Eyeblink-based** anti-spoofing in face recognition from a generic web-camera (G.Pan et al., ICCV'07)
  - Real-time face detection and **motion analysis** with application in liveness assessment. (K. Kollreider et al., TIFS'07)
  - A liveness detection method for face recognition based on **optical flow field** (W. Bao et al., IASP'09)
  - Face liveness detection using **dynamic texture** (Pereira et al., JIVP'14)
  - Detection of face spoofing using **visual dynamics** (S. Tirunagari et al., TIFS'15)
  - Rank-pooling-based visual dynamics (Z. Yu et al., PAMI'20)
  - Spatial gradient and temporal depth (Z. Wang et al., CVPR'20)

# Image and Video Face PAD

- Performance on traditional face spoofing attack

| | Replay Attack | | Print attack | |
|---|---|---|---|---|
| ***Pipelines*** | ***Dev*** | ***Test*** | ***Dev*** | ***Test*** |
| DMD+SVM (face region) | 8.50 | 7.50 | 0.00 | 0.00 |
| DMD+LBP+SVM (face region) | 5.33 | 3.75 | 0.00 | 0.00 |
| PCA+SVM (face region) | 20.00 | 21.50 | 16.25 | 15.11 |
| PCA+LBP (face region) | 11.67 | 17.50 | 9.50 | 5.11 |
| DMD+LBP+SVM (entire video) | 0.50 | 0.00 | 0.00 | 0.00 |
| PCA+LBP+SVM (entire video) | 21.75 | 20.50 | 11.50 | 9.50 |

[S. Tirunagari et al., TIFS'15]

# Public Datasets of Face PAD

| Datasets | Year | Modality | #Subjects | #Data | #Sensor | Spoof type |
|---|---|---|---|---|---|---|
| *Replay-Attack [1]* | *2012* | *RGB* | *50* | *1,200 (V)* | *2* | *Print + Replay* |
| *CASIA-MFSD [2]* | *2012* | *RGB* | *50* | *600 (V)* | *3* | *Print +Replay* |
| *3DMAD [3]* | *2014* | *RGB/Depth* | *14* | *255 (V)* | *2* | *3D mask* |
| *MSU-MFSD [4]* | *2015* | *RGB* | *35* | *440 (V)* | *2* | *Print + Replay* |
| *Msspoof [5]* | *2015* | *RGB/IR* | *21* | *4,704 (I)* | *2* | *Print* |
| HKBU-MARs V2 [6] | 2016 | RGB | 12 | 1,008 (V) | 7 | 3D masks |
| MSU-USSA [7] | 2016 | RGB | 1,140 | 10,260 (I) | 2 | Print + Replay |
| Oulu-NPU [8] | 2017 | RGB | 55 | 5,940 (V) | 6 | Print + Replay |
| SiW [9] | 2018 | RGB | 165 | 4,620 (V) | 2 | Print + Replay |
| CASIA-SURF [10] | 2018 | RGB/IR/Depth | 1,000 | 21,000 (V) | 1 | Paper Cut |
| CSMAD [11] | 2018 | RGB/IR/Depth/LWIR | 14 | 246 (V),17 (I) | 1 | silicone mask |

# Public Datasets of Face PAD (con't)

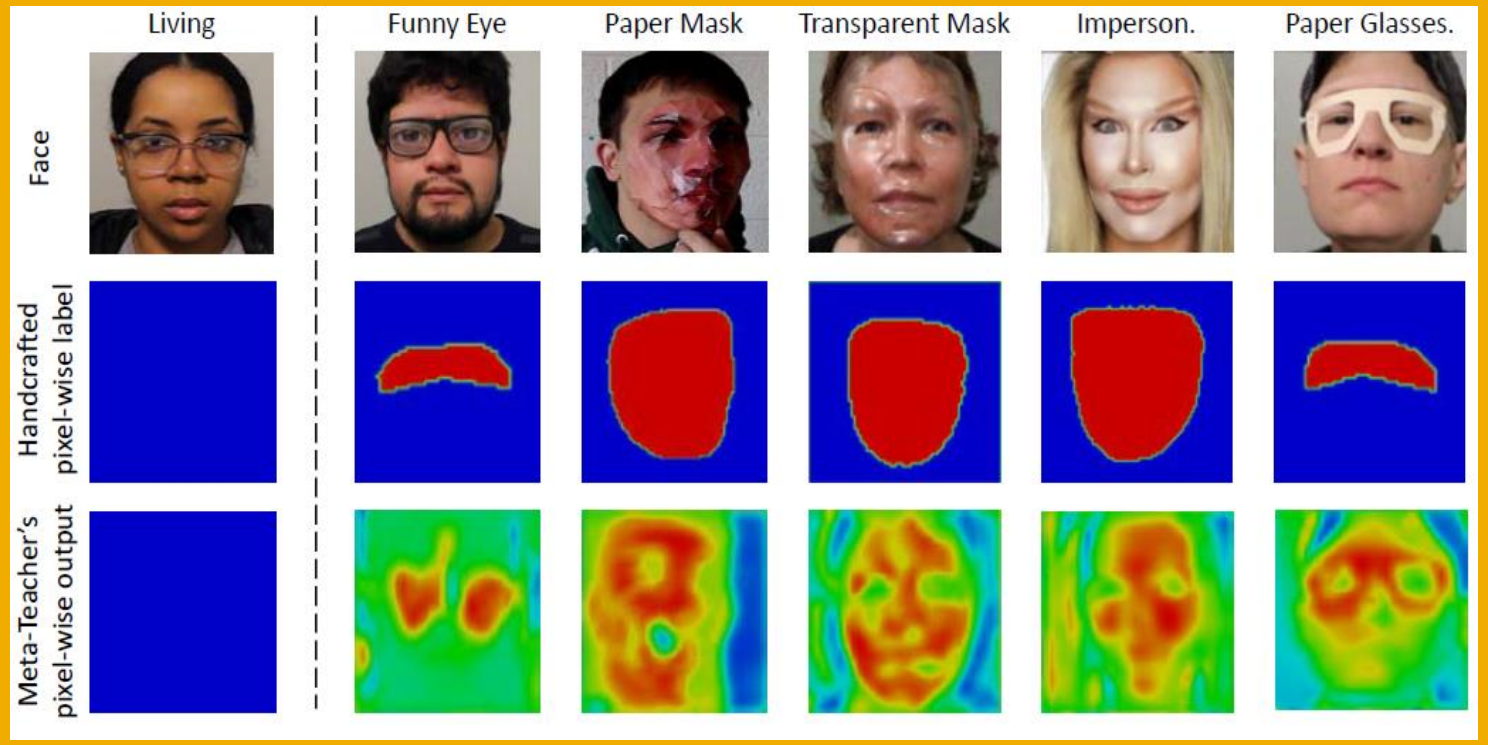
| Datasets | Year | Modality | #Subjects | #Data | #Sensor | Lighting Cond. | Spoof type |
|---|---|---|---|---|---|---|---|
| SiW-M [13] | 2019 | RGB | 493 | 1,628 (V) | 4 | Room Light | Print + Replay +3D Mask + Make Up |
| WMCA [14] | 2019 | RGB/NIR/Depth/LWIR | 72 | 1679 (V) | 4 | Room Light/LED-lamps/Day Light | 3D Mask made of (Plastic, Silicone, Paper) |
| CelebA-Spoof [15] | 2020 | RGB | 10,177 | 625,537 (I) | >10 | Room Light/Strong Front Light/Back Light/Dark | 3 Print, 3 Replay 1 3D Mask, 3 Paper Cut |
| HQ-WMCA [16] | 2020 | RGB/NIR/Depth/SWIR/LWIR | 51 | 2904 | 5 | Room Light/Halogen-lamps/LED-lamps/Day Light/ | Print. Replay, 3D masks: (Rigid, Paper, Flexible), Mannequine, Glasses, Makeup, Tattoo, Wig |
| CASIA-SURF 3DMask [17] | 2020 | RGB | 48 | 1152 (v) | 3 | Room Light/Back Light/ Front-light/Sidelight/Sun-light/Shadow | 3D masks |
| HiFiMask [18] | 2021 | RGB | 75 | 54600 | 7 | Room Light/Dim Light/Bright Light/Back Light//Side Light/Top Light | Transparent Mask Plaster, Hi-Fidelity 3D Masks |

# Image and Video Face PAD

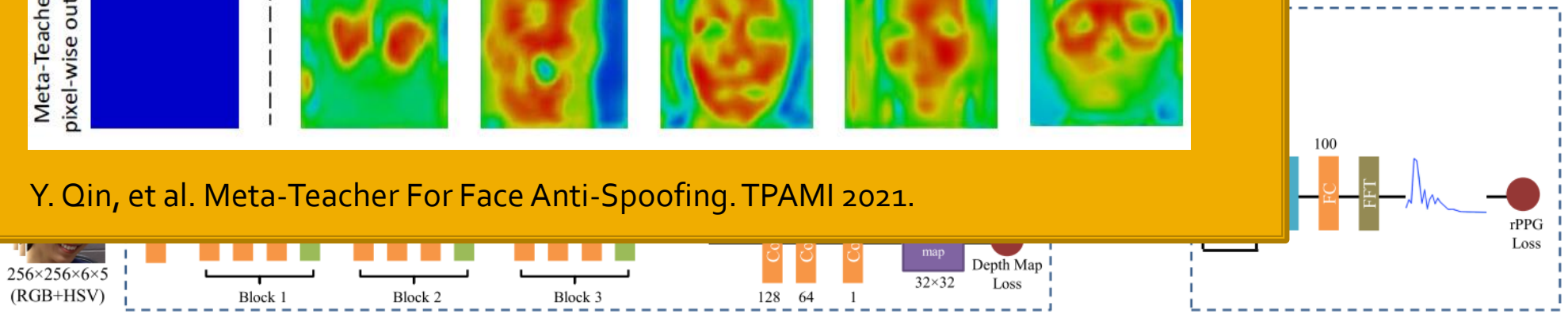
## Deep Representation Learning

# Image and Video Face PAD

**Generate better pixel-wise label**



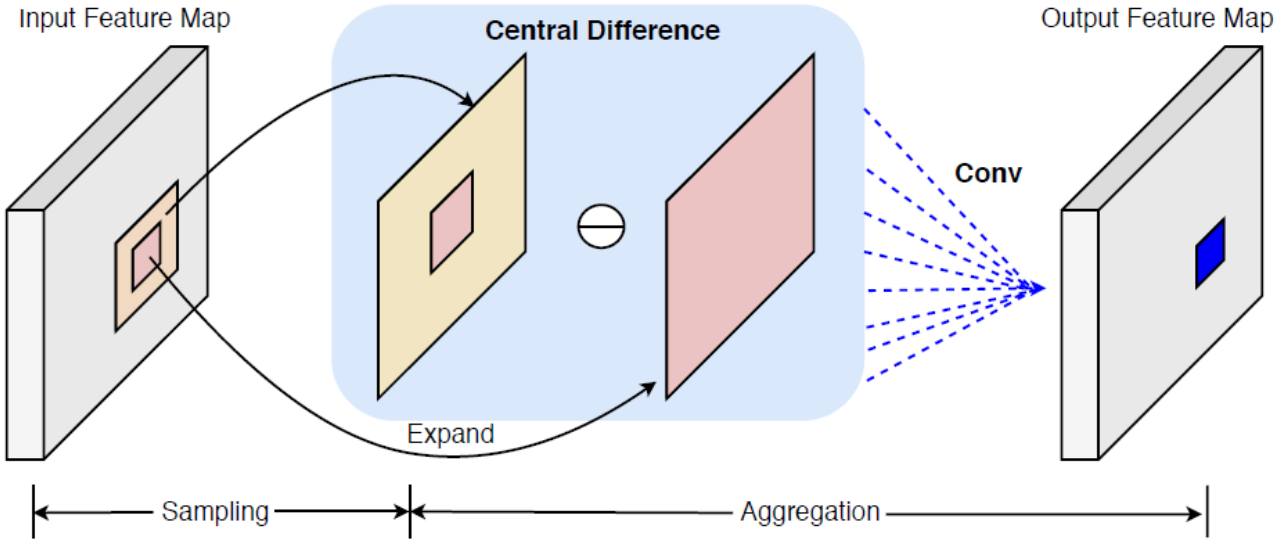

Y. Qin, et al. Meta-Teacher For Face Anti-Spoofing. TPAMI 2021.

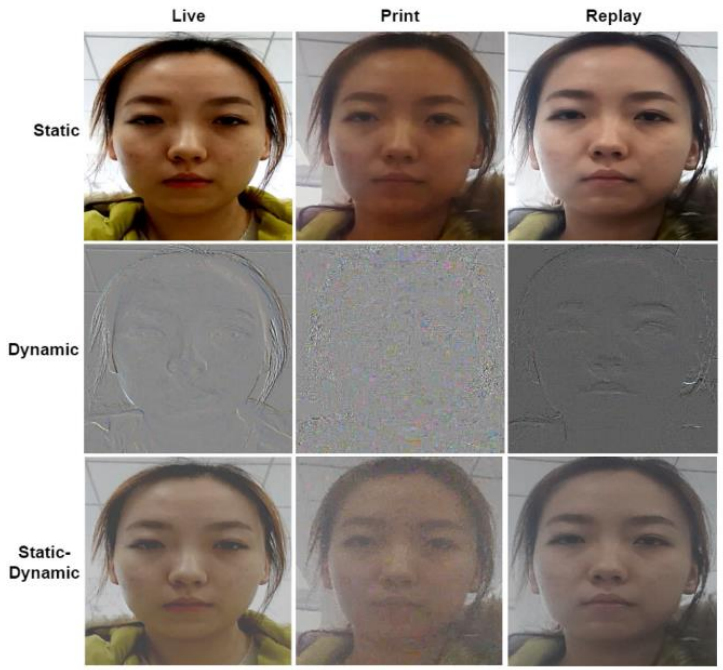



Y. Liu, A. Jourabloo, and X. Liu. Learning deep models for face anti-spoofing: Binary or auxiliary supervision, CVPR 2018

# Image and Video Face PAD

- Central Difference Convolutional Network (CDCN) and Variations
  - A new convolution kernel inspired by the rationale of LBP
  - Aim to learn detailed patterns via aggregating both **intensity** and **gradient** information



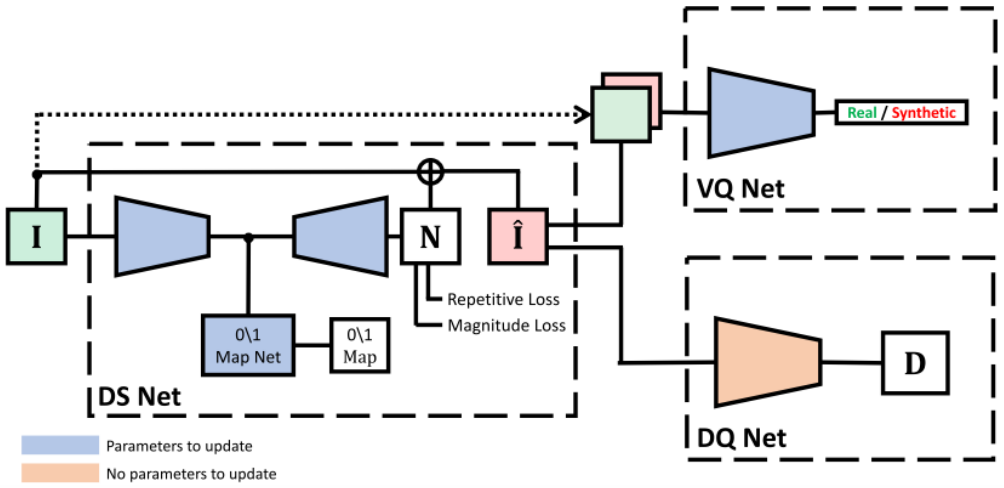

**Static-dynamic Image**

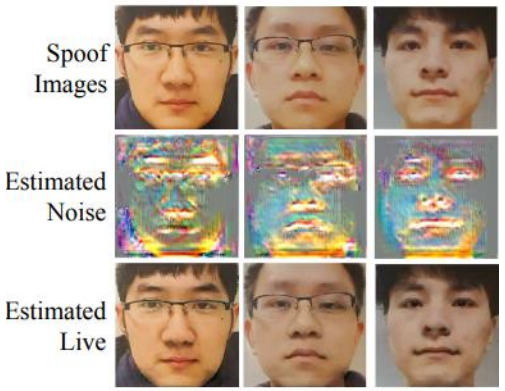

Z. Yu, et al. Searching central difference convolutional networks for face anti-spoofing. CVPR 2020.
Z. Yu, et al. Nas-fas: Static-dynamic central difference network search for face antispoofing. TPAMI 2020
Yu, Zitong, et al. Dual-cross central difference network for face anti-spoofing. IJICAI 2021.

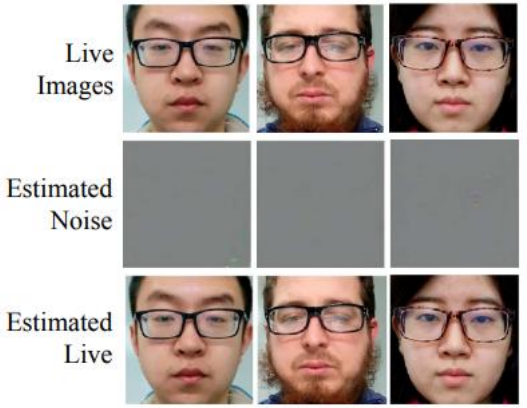
# Image and Video Face PAD

## Noise Modeling

- Inversely decompose a spoofed face into a spoof noise and a live face, and then utilizing the spoof noise for classification.
- Real face: no spoof noise vs. Fake face: clear spoof noise



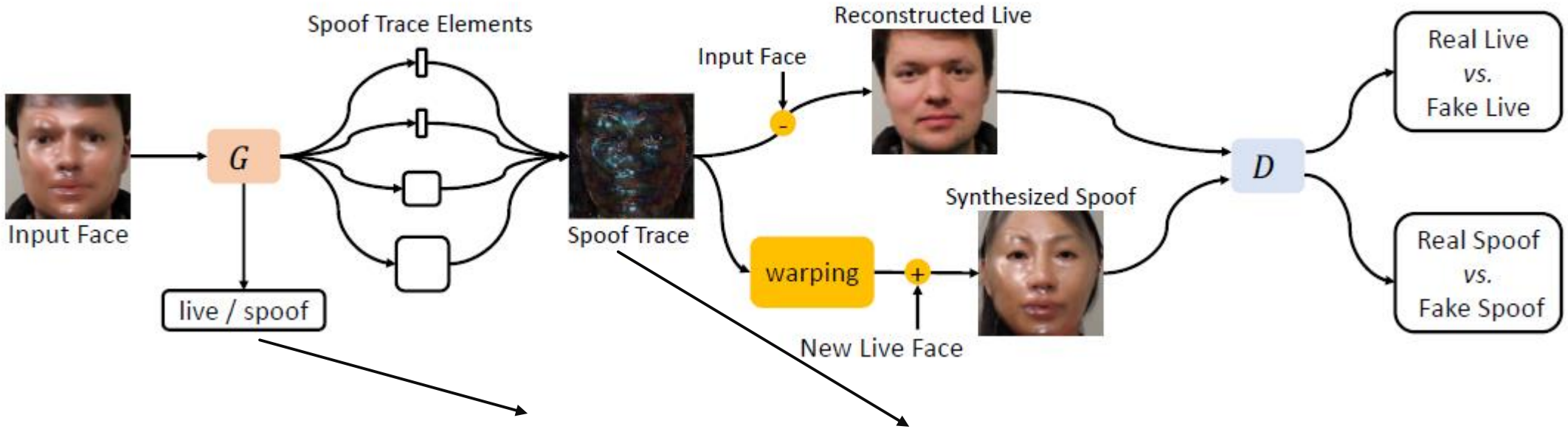




Y. Liu, A. Jourabloo, and X. Liu. Face De-Spoofing: Anti-Spoofing via Noise Modeling, ECCV 2018
Y. Liu, et al. On disentangling spoof trace for generic face anti-spoofing. ECCV 2020.

# Image and Video Face PAD

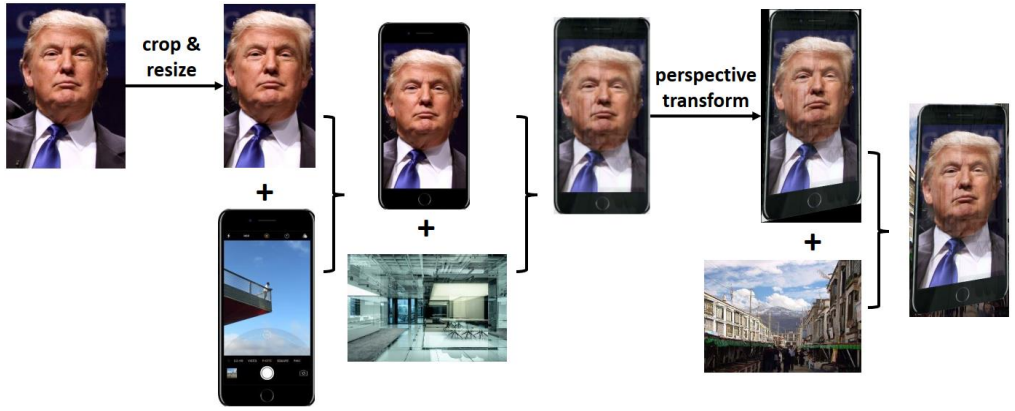
- Spoof Trace Disentanglement Network (STDN)
  - Disentangled spoof trace via adversarial learning and hierarchical combination of patterns at multiple scales.




Y. Liu, et al. On disentangling spoof trace for generic face anti-spoofing. ECCV 2020.

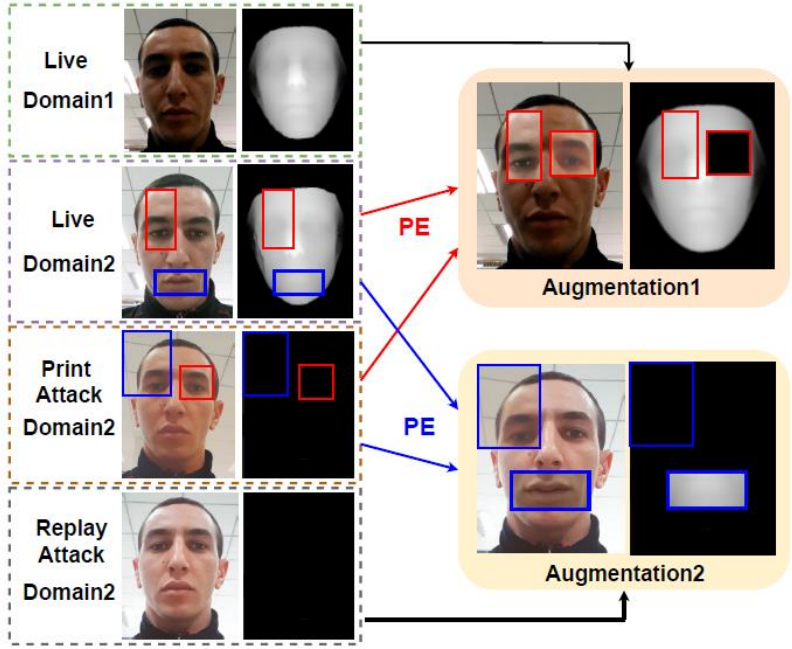
# Image and Video Face PAD

- Data Augmentation
  - Simulate digital medium-based face spoofing attacks to obtain a large amount of training data well reflecting the real-world scenarios
  - Synthetic reflection artifacts




Yang X, Luo W, Bao L, et al. Face Anti-Spoofing: Model Matters, So Does Data, CVPR 2019

- Patch Exchange Augmentation
  - Exchange face patches from different domains
  - Random mixup of live and PA patches
  - Corresponding pixel-wise supervision for augmented data



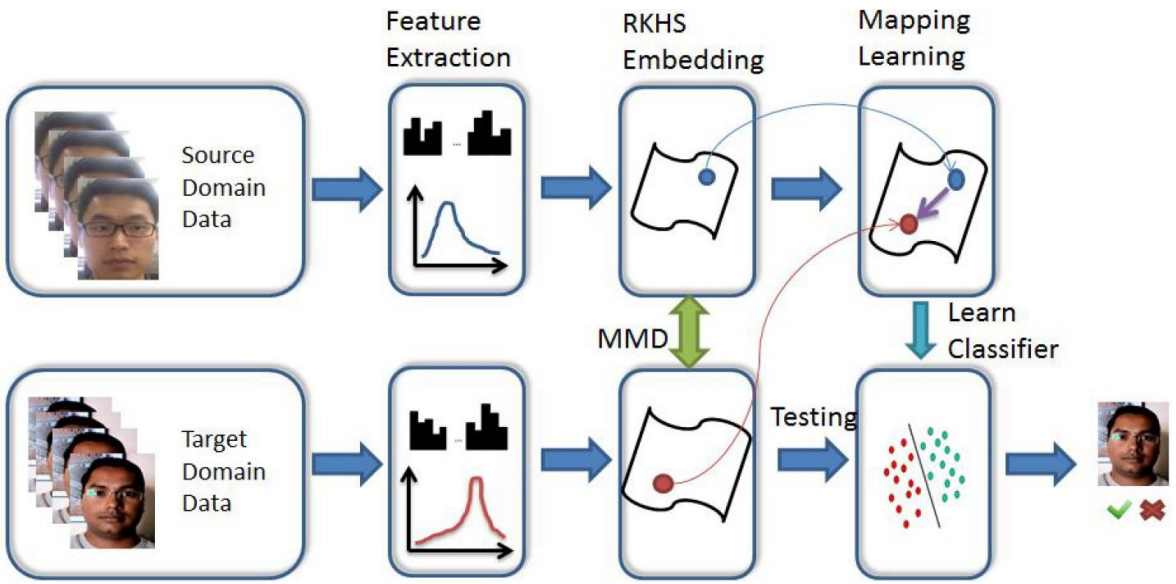

Yu, Zitong, et al. Dual-cross central difference network for face anti-spoofing. IJICAI 2021.

# Image and Video Face PAD

## Domain Adaptation and Generalization

# Image and Video Face PAD

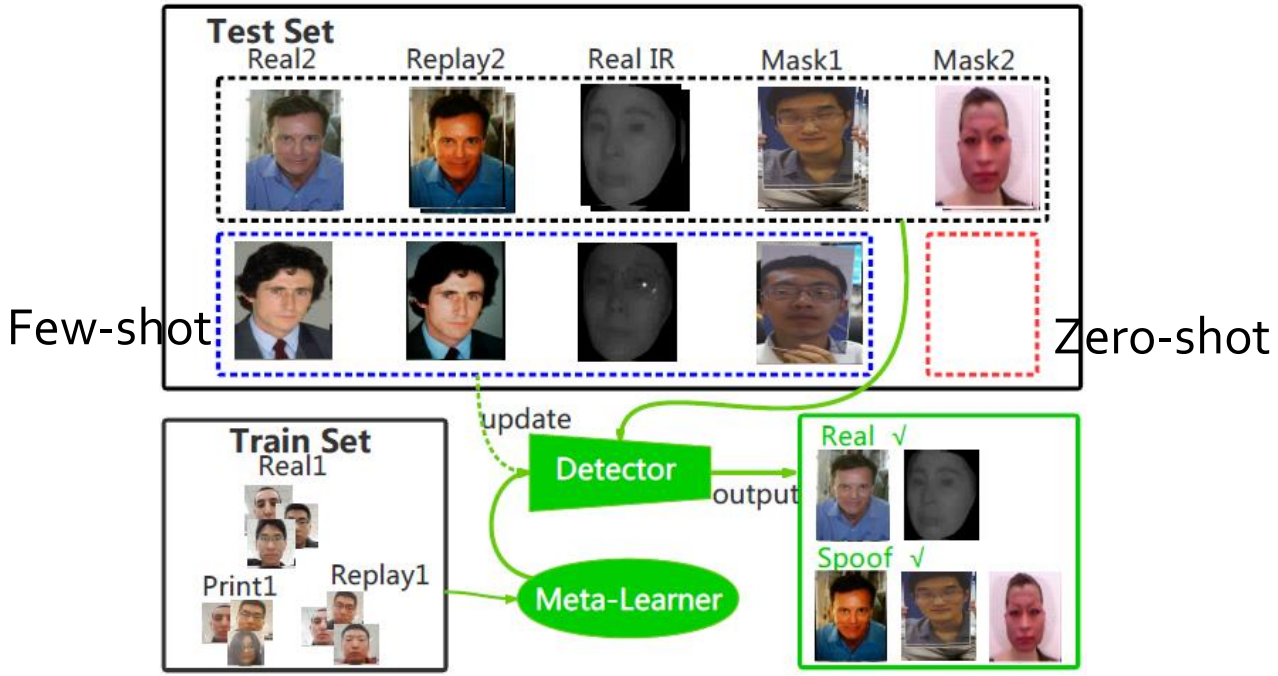
- Domain adaptation approach
  - Learn a mapping function to align the eigenspaces between source domain data and target domain data.
  - Maximum Mean Discrepancy between the source and target latent features is minimized




H Li, W Li, H Cao and et al. Unsupervised domain adaptation for face anti-spoofing, TIFS 2018

# Image and Video Face PAD

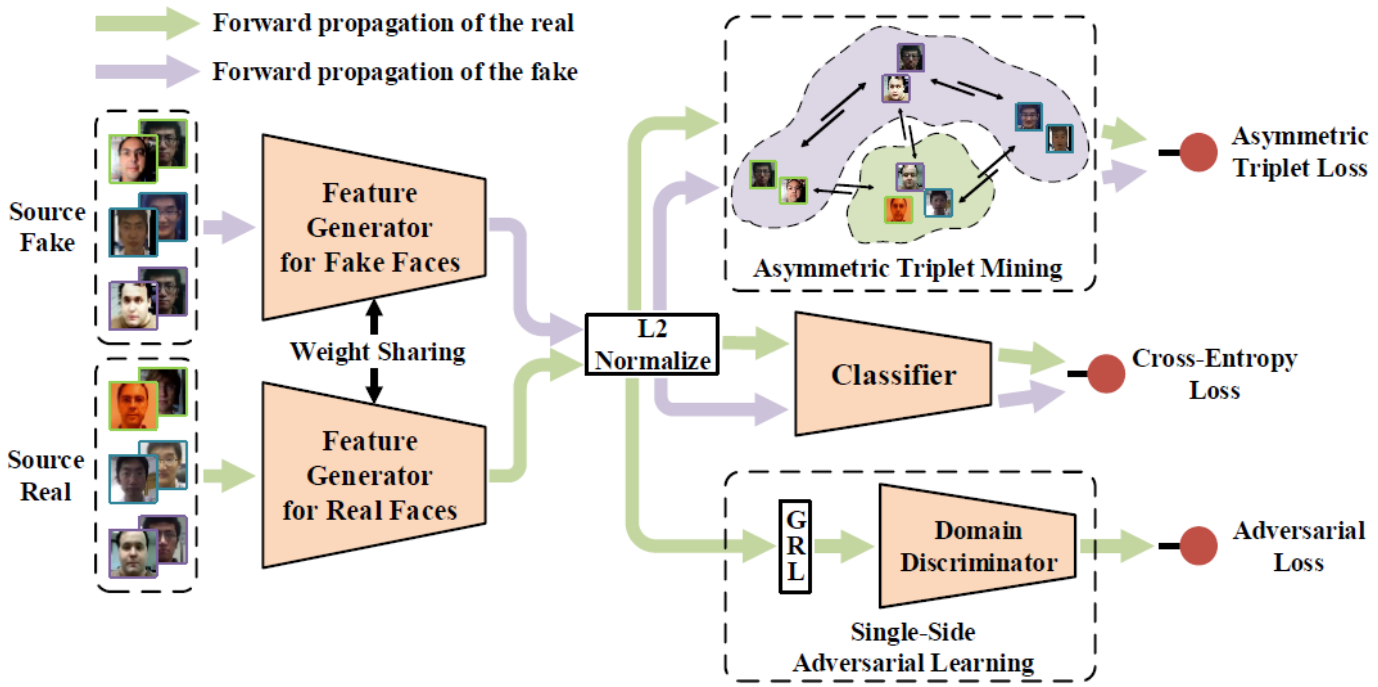
- Adaptive Inner-update Meta learning
  - Aim to quickly adapt to new spoofing types by learning from both the predefined attacks and a few examples of the new spoofing types.

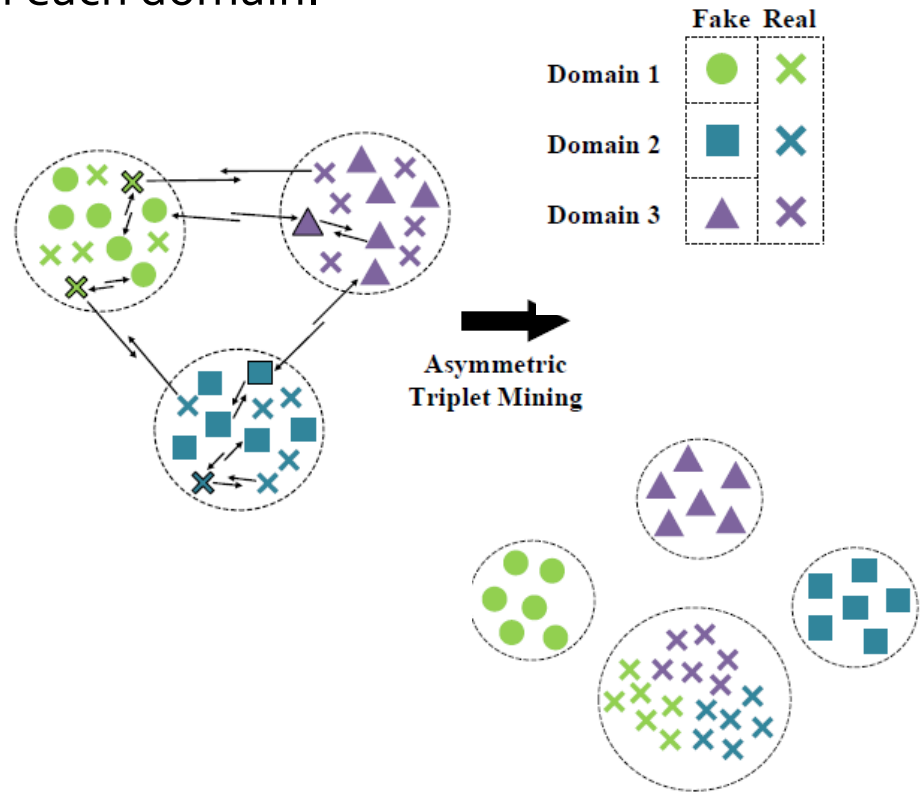



Y. Qin, et al. Learning Meta Model for Zero- and Few-shot Face Anti-spoofing. AAAI 2020.

# Image and Video Face PAD

- Single-side domain generalization
  - Learn a generalized space where the feature distribution of real faces is compact
  - Fake faces are separated among domains but compact within each domain.

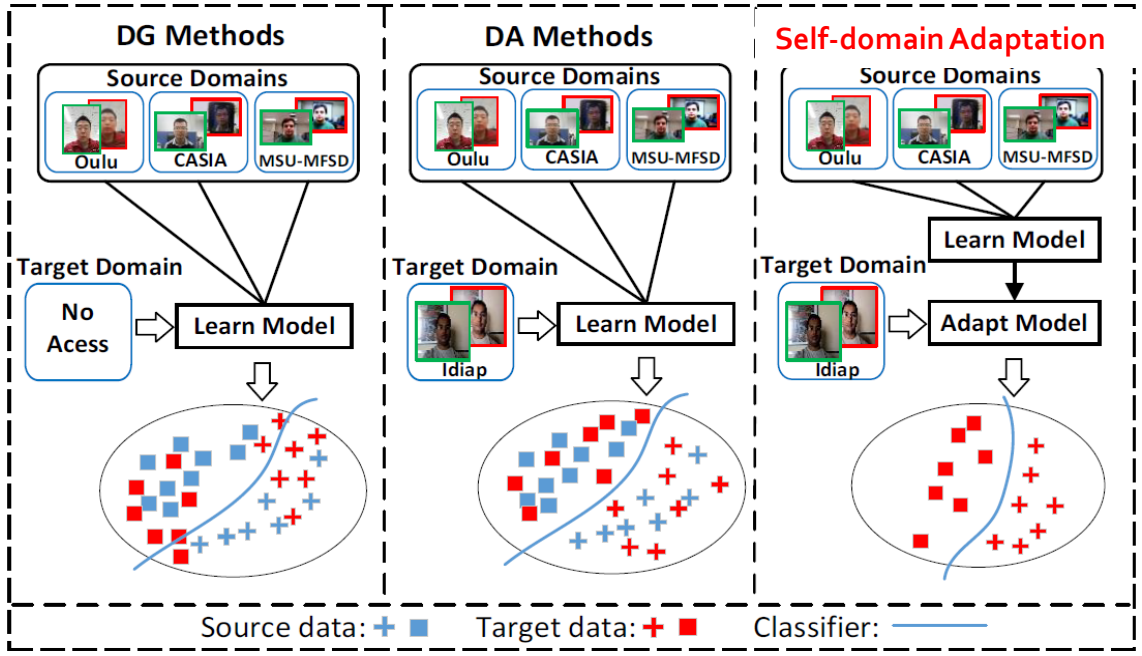


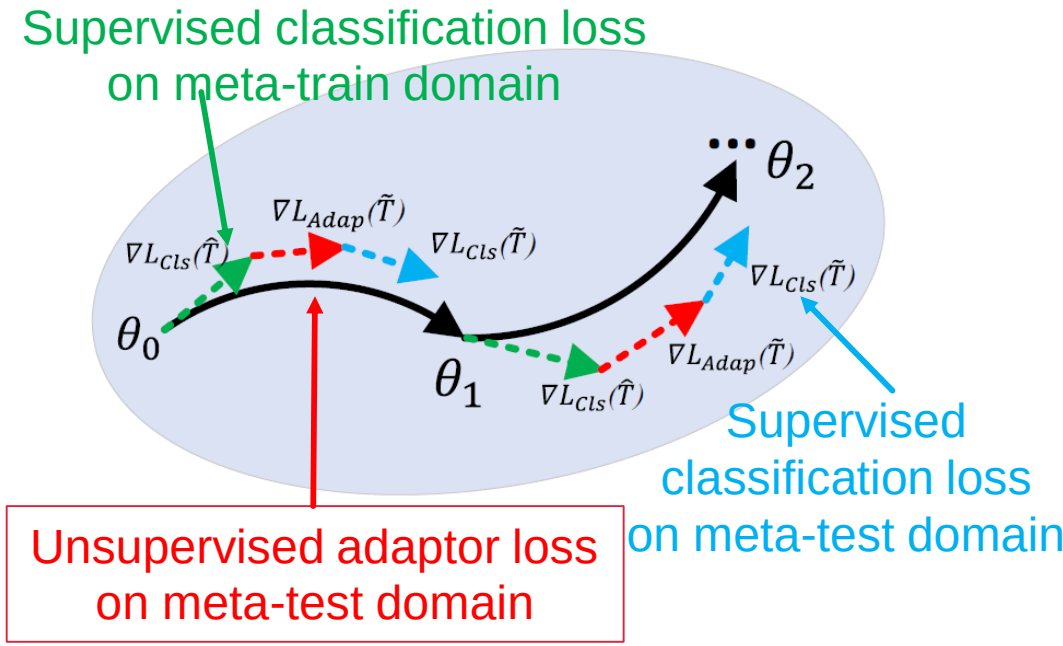




Y. Jia, et al. Single-side domain generalization for face anti-spoofing. CVPR 2020.

# Image and Video Face PAD

- Self-domain adaptation with unlabeled testing data
  - Using the information of the test domain to improve the performance at inference stage
    - Meta learning framework with domain adaptor
    - Domain adaptor is also updated at inference stage

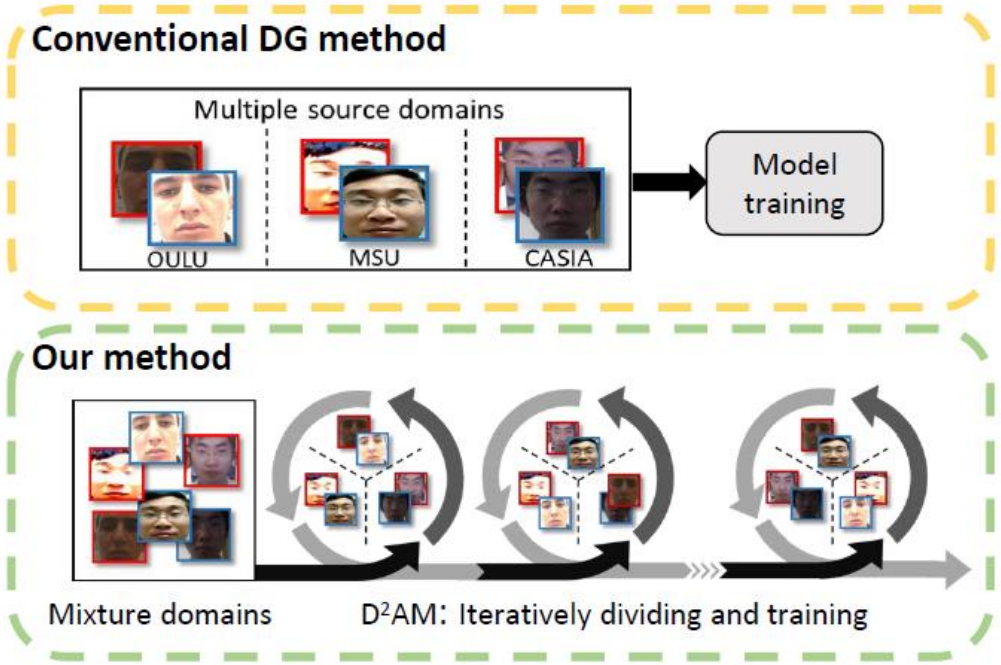



J. Wang, et al. Self domain adaptation for face anti-spoofing. AAAI 2021.

# Image and Video Face PAD

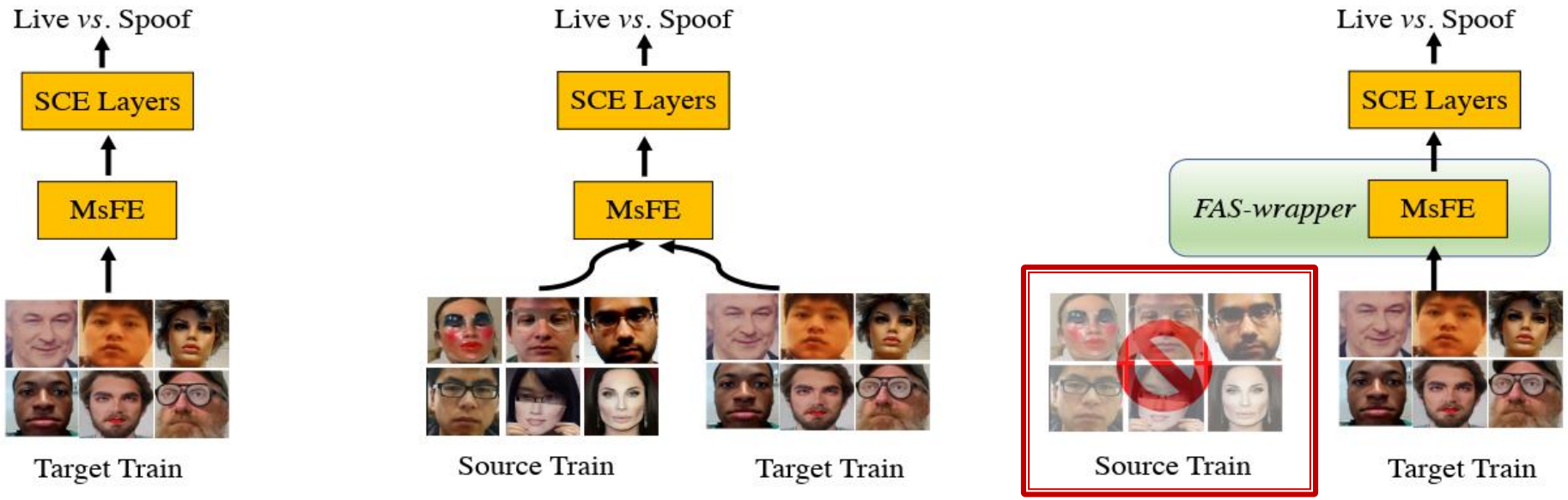
- Unknown domain label: Domain dynamic adjustment meta-learning
  - Training data always contains mixture domains, where the domain label is unknown
  - Iteratively assign pseudo domain labels and be trained using meta-learning




Z. Chen, et al. Generalizable representation learning for mixture domain face anti-spoofing. AAAI 2021.

# Image and Video Face PAD

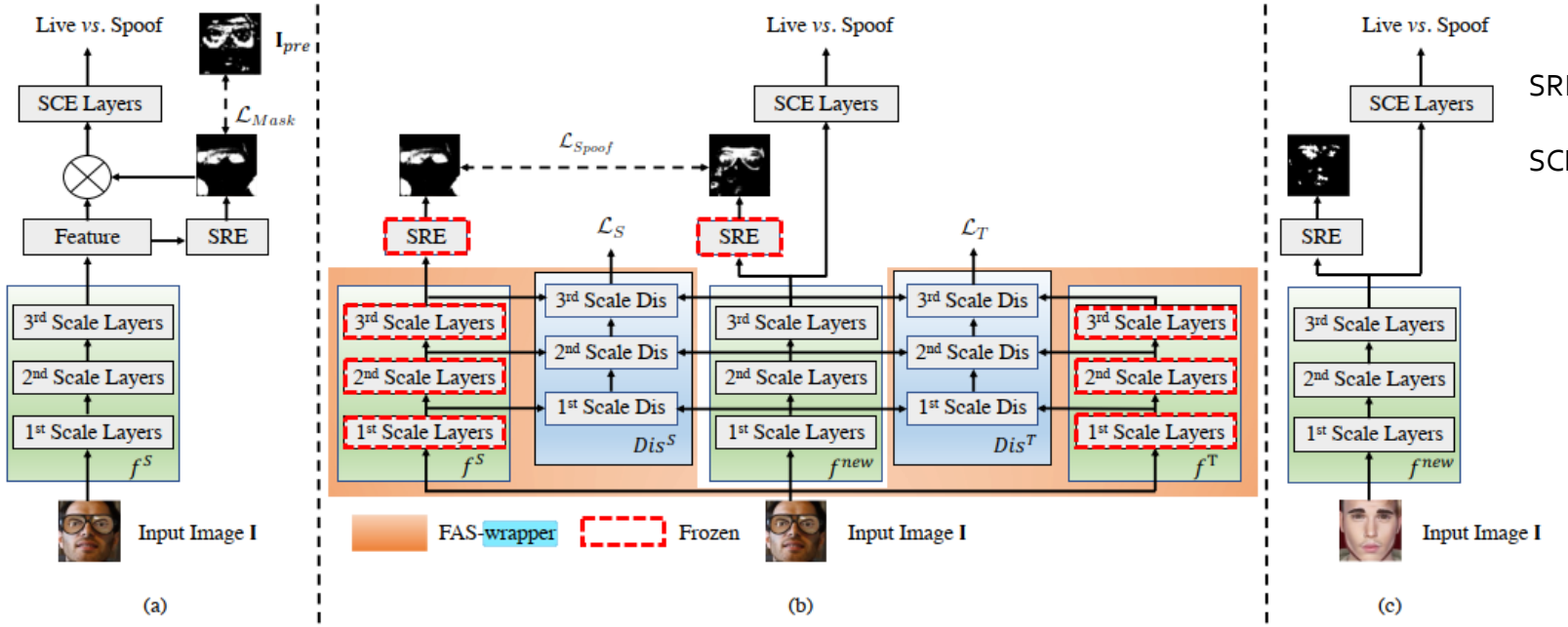
- Source-free Domain Adaptation
  - Update a FAS model using only target domain data, so that the upgraded model can perform well in both the source and target domains




X. Guo, et al. Multi-domain Learning for Updating Face Anti-spoofing Models. ECCV 2022.

# Image and Video Face PAD

- Source-free Domain Adaptation
  a) Given feature extractor: $f_S$ (pretrained on source data) ,finetune it with SRE on target data-> $f_T$
  b) Two teacher models $f_S$, $f_T$ train $f_{new}$ with adversarial learning
     - $L_S, L_T$ : Transfer knowledge from two teacher model via adversarial losses
     - $L_{spoof}$: Prevents divergence between estimated spoof traces to combat catastrophic forgetting
  c) Inference stage

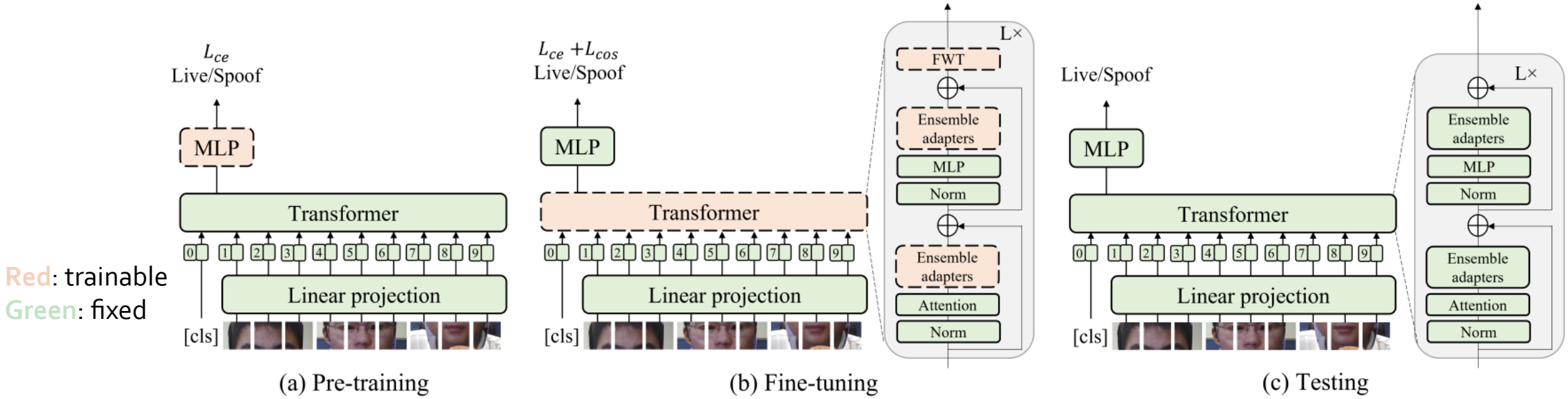



SRE: Spoof Region Estimator (pixel level supervision)
SCE: Spoof Cue Estimator (classifier)

X. Guo, et al. Multi-domain Learning for Updating Face Anti-spoofing Models. ECCV 2022.

# Image and Video Face PAD

- Adaptive ViT for FAS
  - ViT captures the long-range dependency among different patches via the global self-attention mechanism
  - Steps:
    a) ViT backbone is pretrianed on ImageNet, only MLP head is trained for FAS with cross entropy loss
    b) Insert Ensemble Adaptors and FWT (feature wise transform)
    c) FWT layers are removed during testing

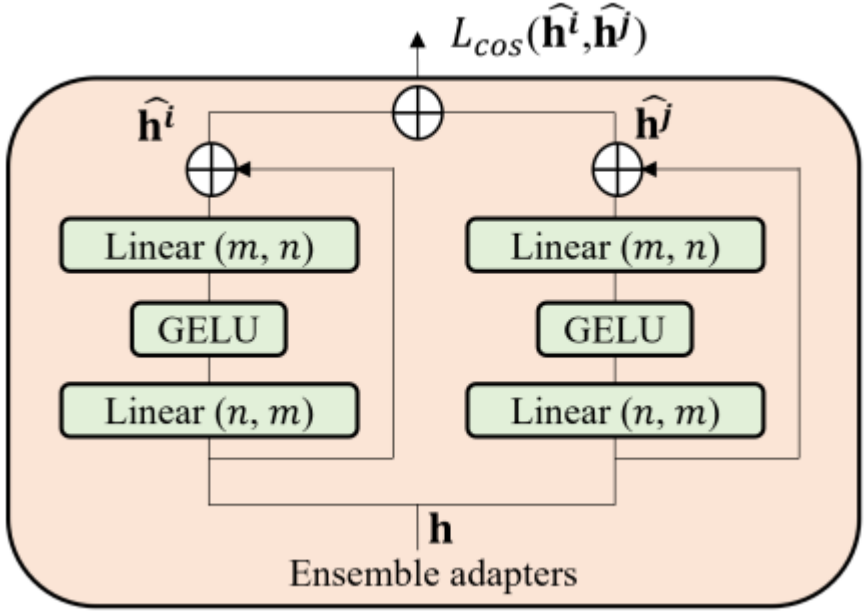



Red: trainable
Green: fixed

H.P. Huang, et al. Adaptive Transformers for Robust Few-shot Cross-domain Face Anti-spoofing. ECCV 2022.

# Image and Video Face PAD

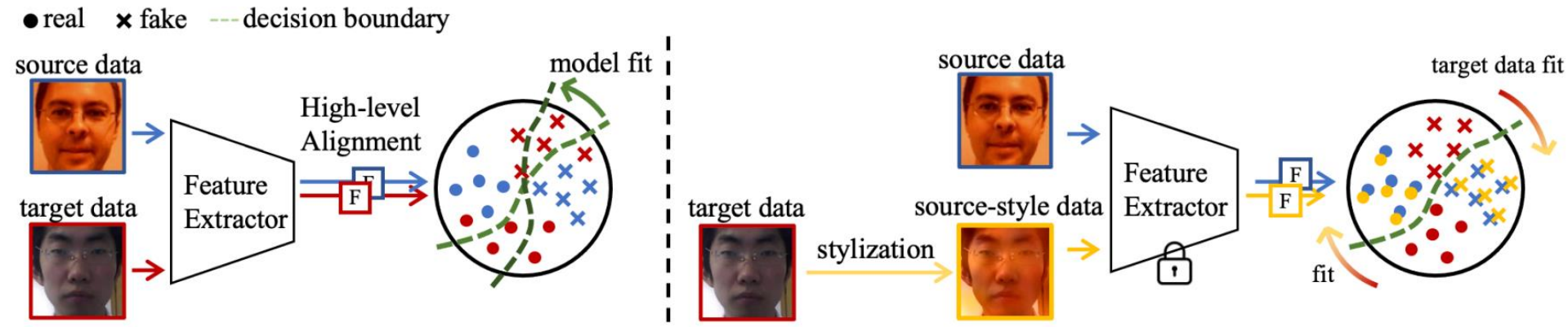
- Adaptive ViT for FAS
  - Ensemble Adaptors
    - Inspired by adapterBERT
    - Cosine similarity loss constrains multiple outputs of adapters to be complementary
  - Feature Wise Transform (FWT)
    - Feature-level data augmentation
    - Apply affine transformations to intermediate features




H.P. Huang, et al. Adaptive Transformers for Robust Few-shot Cross-domain Face Anti-spoofing. ECCV 2022.

# Image and Video Face PAD

- Generative Domain Adaptation: Stylize target data to source data
  a) Typical solution: Fit the trained models to the target domain via aligning the distribution of semantic high-level features
  b) New perspective: Stylizes the target data to the source-domain style via image translation

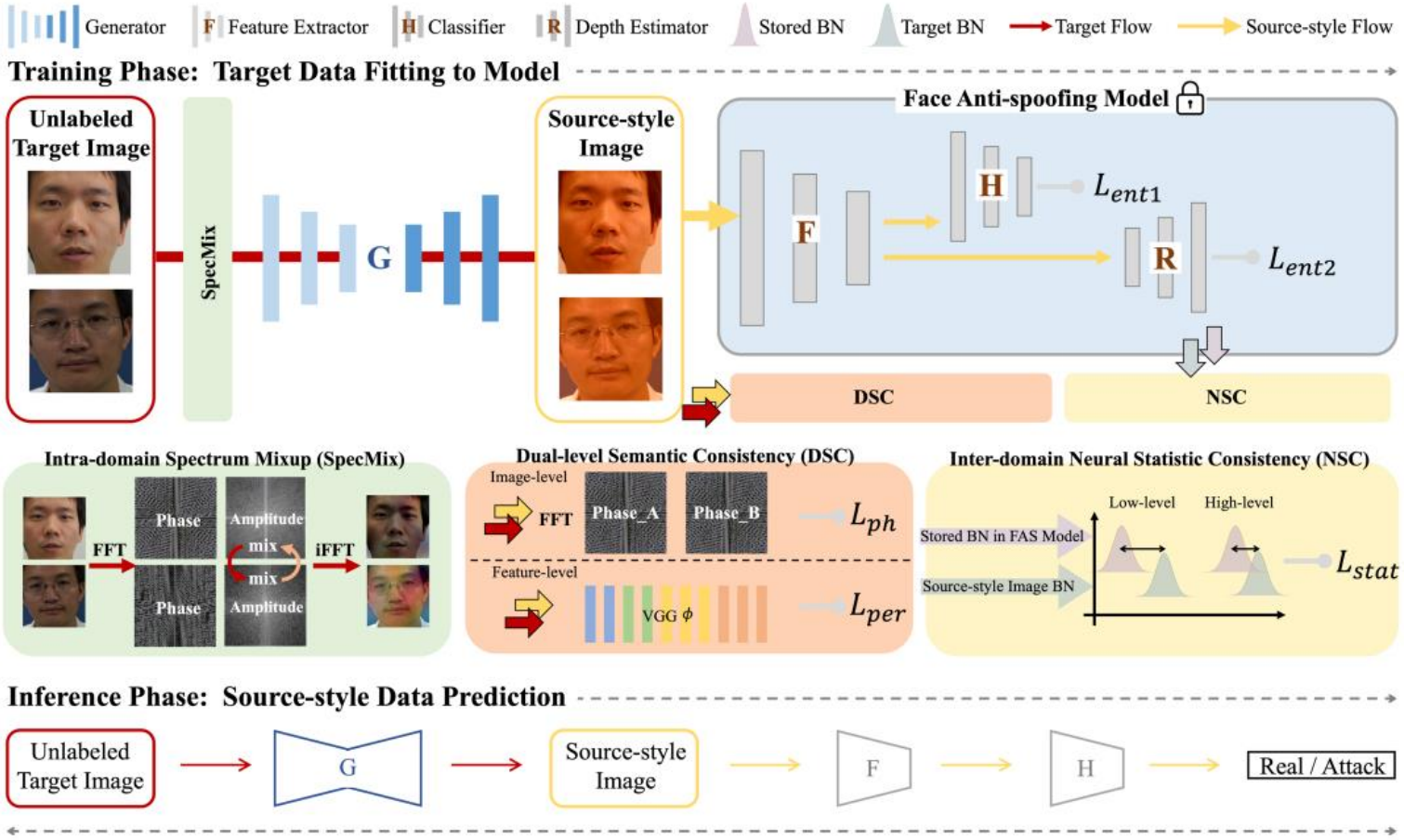



(a) Previous UDA in FAS: Model fit to Target data (b) UDA in FAS: Target data fit to Model

Q. Zhou et al. Generative Domain Adaptation for Face Anti-Spoofing. ECCV 2022.

# Image and Video Face PAD

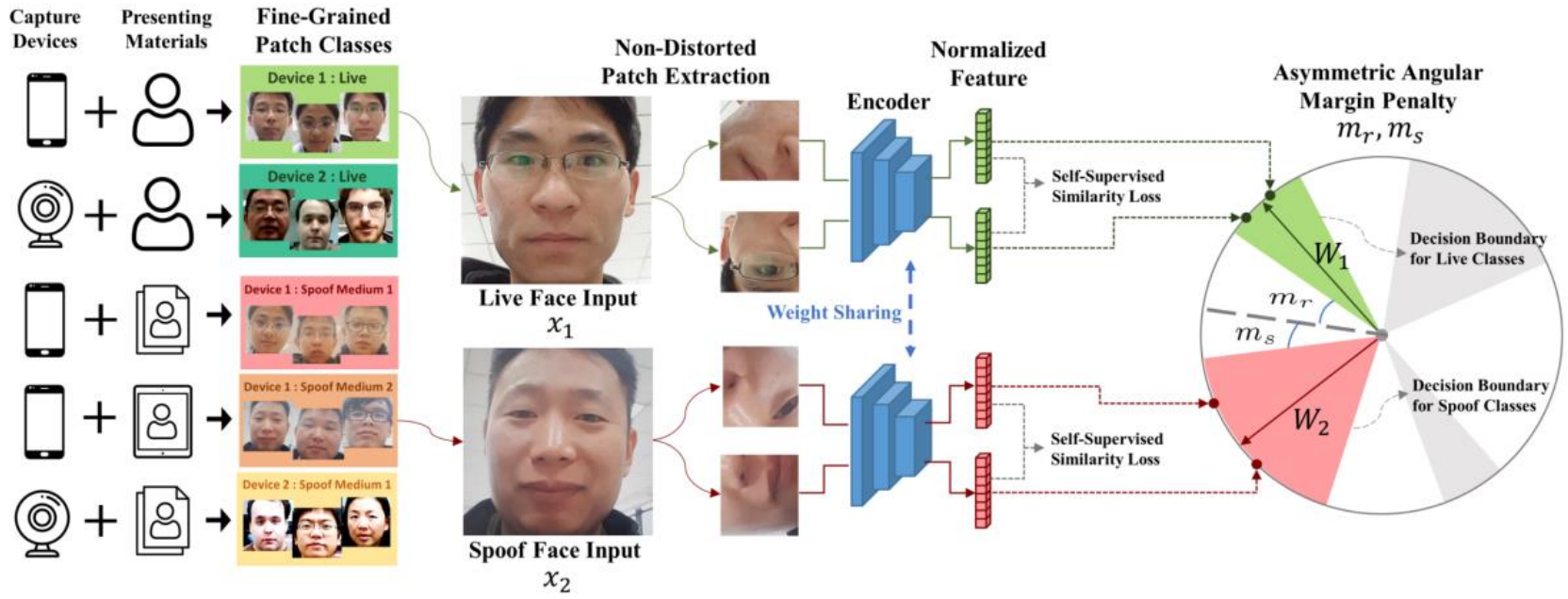
- Stylize target data to source data
  - Two Consistency constraints
    - Neural statistic consistency (NSC)
    - dual-level semantic consistency (DSC)
  - Expand target data distribution
    - Spectrum Mixup




Q. Zhou et al. Generative Domain Adaptation for Face Anti-Spoofing. ECCV 2022.

# Image and Video Face PAD

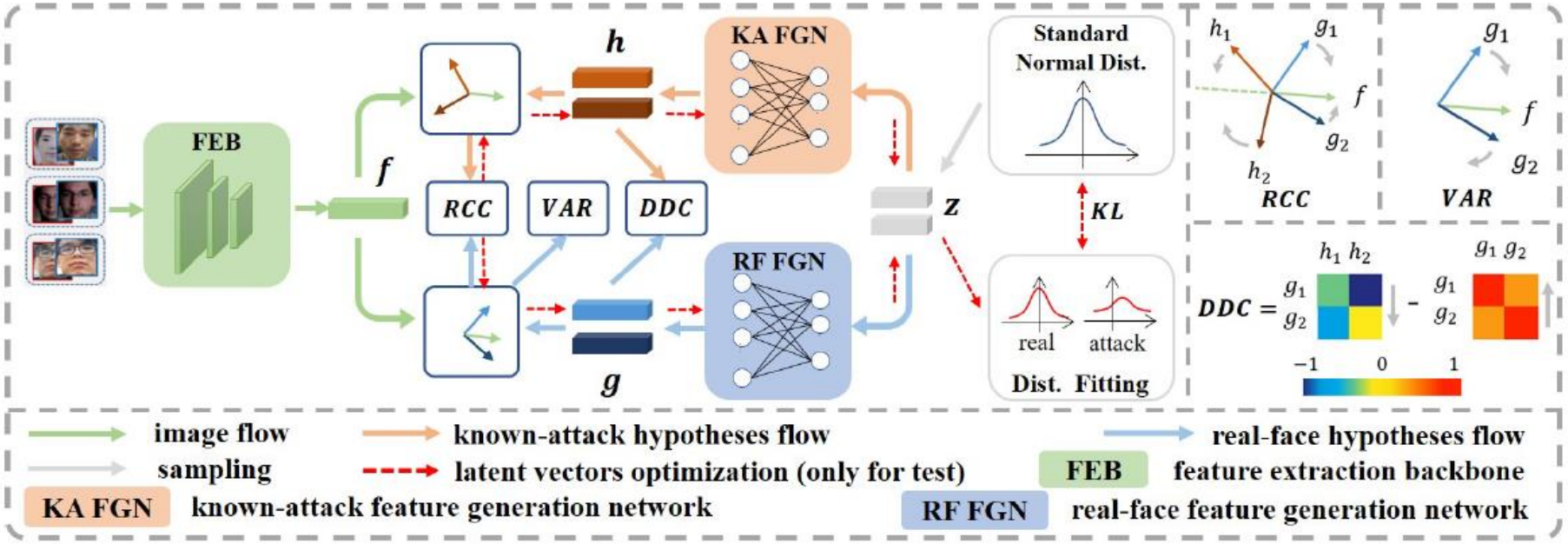
- Fine-Grained Patch Recognition FAS
  - Patch-type classes: Capture device, Presenting material
  - Asymmetric Angular Margin Softmax Loss: larger angular margin on live classes
  - Self-Supervised Similarity Loss:  enforce the patch feature invariance within a single




C.Y. Wang et al, PatchNet: A Simple Face Anti-Spoofing Framework via Fine-Grained Patch Recognition. CVPR 2022.

# Image and Video Face PAD

- Feature Generation and Verification for Reliable FAS
  - Generate real-face feature ***g*** and spoofing-attack feature ***h*** with constraints:
    - Variance constraint (VAR): Input face feature and real-face hypothesis tend to be similar
    - Relative Correlation Constraint (RCC): Triplet-loss-like constraint for real face feature, real-face hypothesis, and attack hypothesis
    - Distribution Discrimination Constraint (DDC): Enlarge distance between real-face hypothesis and attack hy

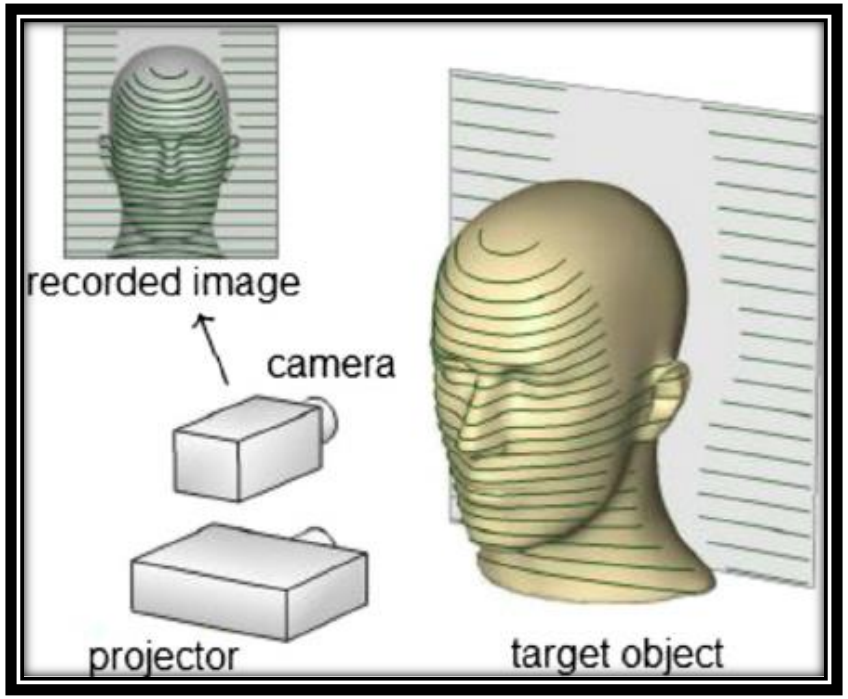



S. Liu et al, Feature Generation and Hypothesis Verification for Reliable Face Anti-spoofing. AAAI 2022.

# 3D Face Recognition


**FaceID in iPhone X**

**Announced on 12 September 2017**

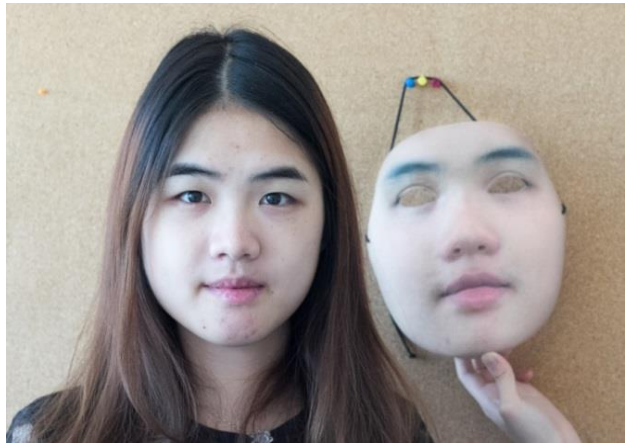

**3D Face Recognition:**

Employed Structured-light 3D technology

https://matterandform.net/blog/how-do-3d-scanners-work

# 3D Mask Face PAD

- 3D Mask Attack
  - With the advanced development on 3D reconstruction and 3D printing technology, 3D face model can easily be constructed and used to spoof recognition systems



Source: idiap.ch

Mask is made from ThatsMyFace.com

# 3D Mask Face PAD

- Super-realistic 3D Mask


(a) Life face

(b) Real-F hyper real mask

Source: real-f.jp

BBC NEWS

# Brazil drug dealer dresses up as daughter in bungled jail escape

05 August 2019 | Latin America & Caribbean

# Airport and Payment Facial Recognition Systems Fooled by Masks and Photos, Raising Security Concerns

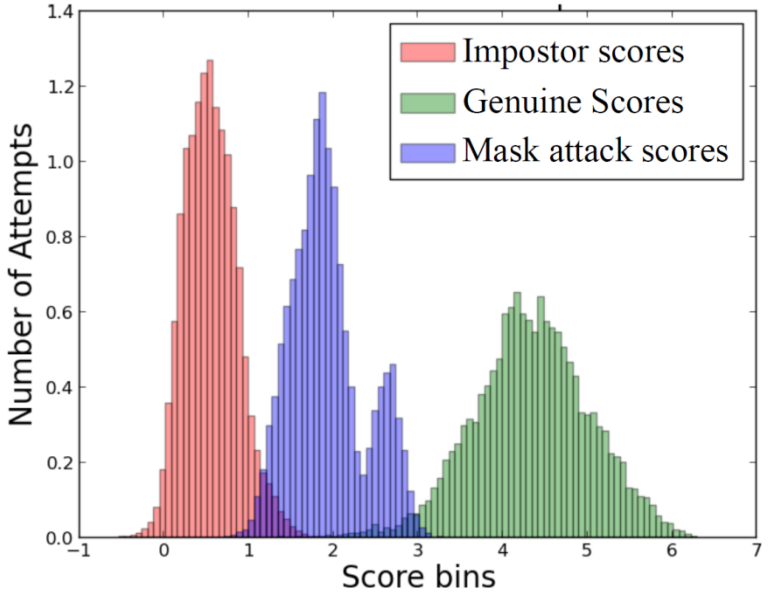
By Jeff John Roberts December 12, 2019

The test, by artificial intelligence company Kneron, involved visiting public locations and tricking facial recognition terminals into allowing payment or access. For example, in stores in Asia—where facial recognition technology is deployed widely—the Kneron team used high quality 3-D masks to deceive AliPay and WeChat payment systems in order to make purchases.

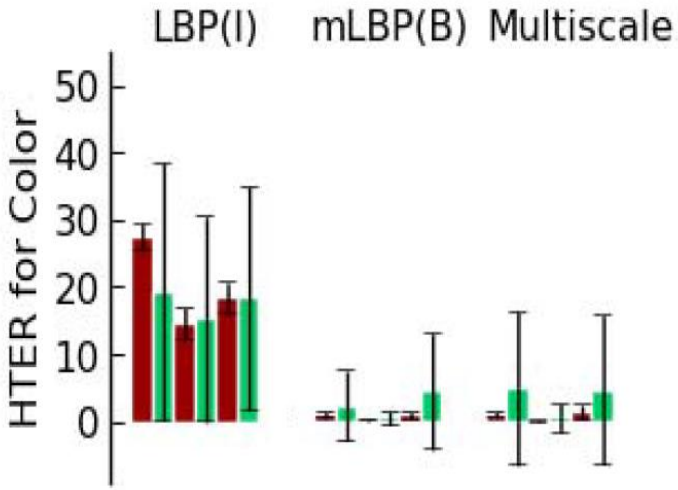
More alarming were the tests deployed at transportation hubs. At the self-boarding terminal in Schiphol Airport, the Netherlands' largest airport, the Kneron team tricked the sensor with just a photo on a phone screen. The team also says it was able to gain access in this way to rail stations in China where commuters use facial recognition to pay their fare and board trains.

# 3D Mask Face PAD

- The 3DMAD dataset
  - Score distributions of genuine, impostor, and mask attack scores of 3DMAD using ISV for 2D face verification

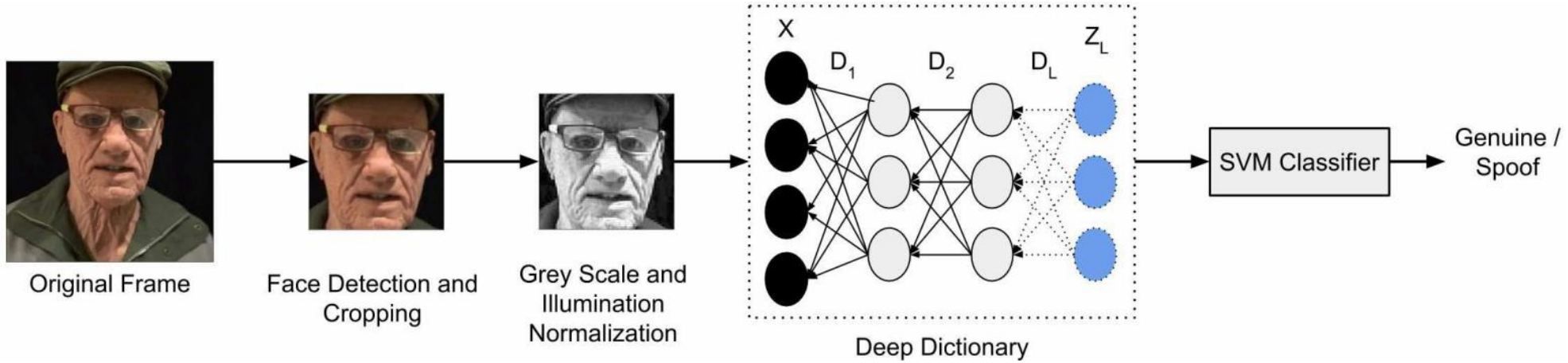



[Erdogmus et al., BTAS'13 ]



# 3D Mask Face PAD

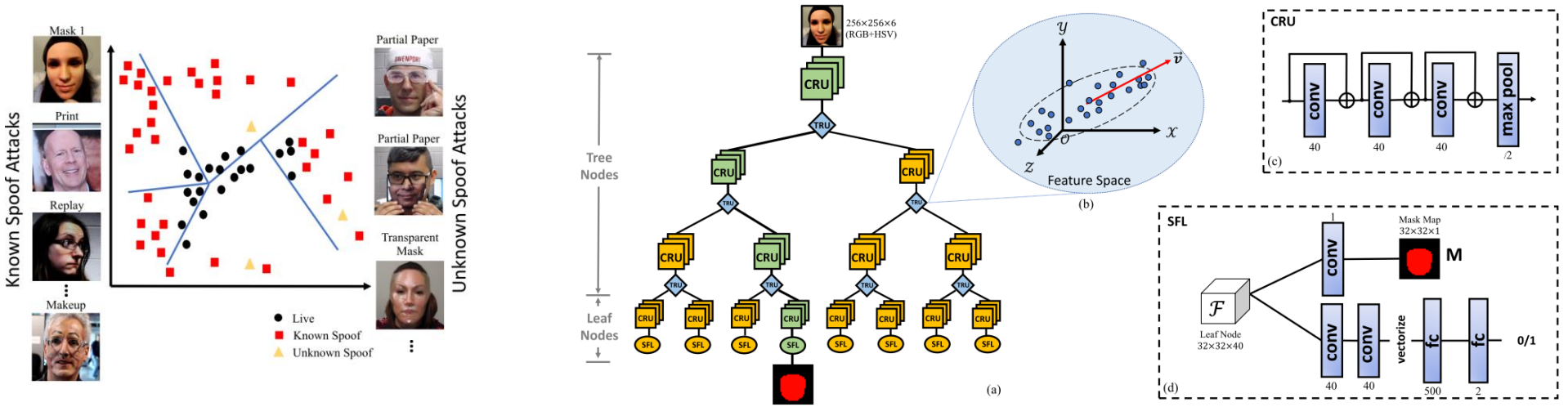
- Deep Dictionary Learning approach
  - Detecting Silicone Mask-based Presentation Attack.
  - Multilevel deep dictionary learning-based presentation attack detection algorithm




Manjani I, Tariyal S, Vatsa M, et al. Detecting silicone mask-based presentation attack via deep dictionary learning, TIFS 2017

# 3D Mask Face PAD

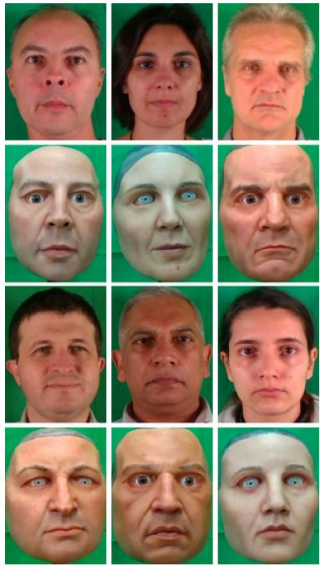
- Zero-shot learning approach
  - Investigate the Zero-Shot Face Anti-spoofing problem in a wide range of 13 types of spoof attacks including 3D masks.
  - A novel Deep Tree Network is proposed to partition the spoof samples into semantic sub-groups

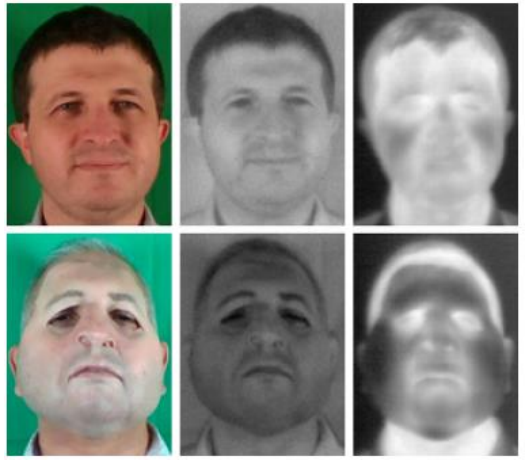



Liu Y, Stehouwer J, Jourabloo A, et al. Deep Tree Learning for Zero-shot Face Anti-Spoofing, CVPR 2019

# 3D Mask Face PAD

- Custom Silicone Masks Datasets
  - Consider PAs performed using custom-made flexible silicone masks..
  - A new dataset based on six custom silicone masks

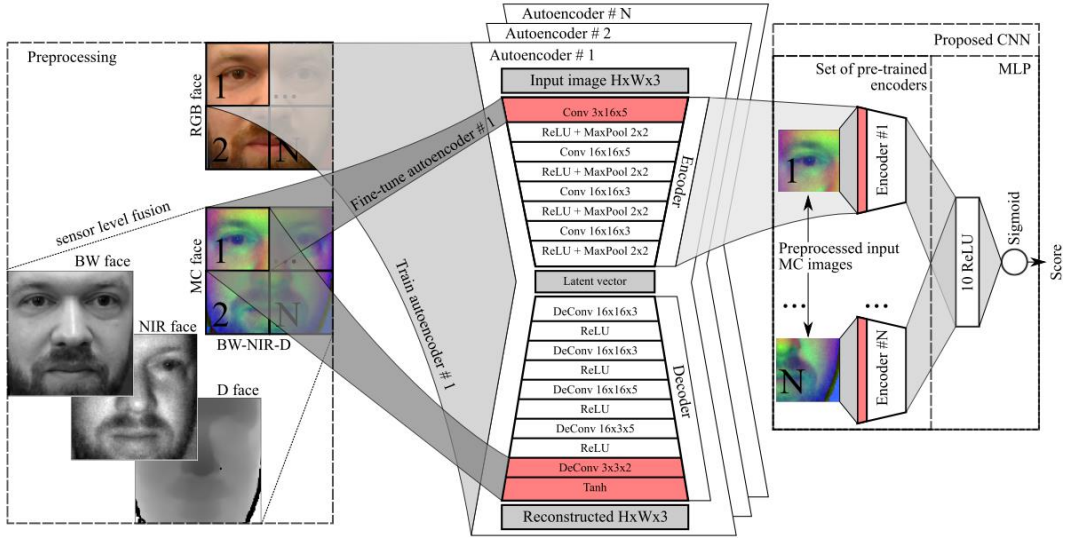


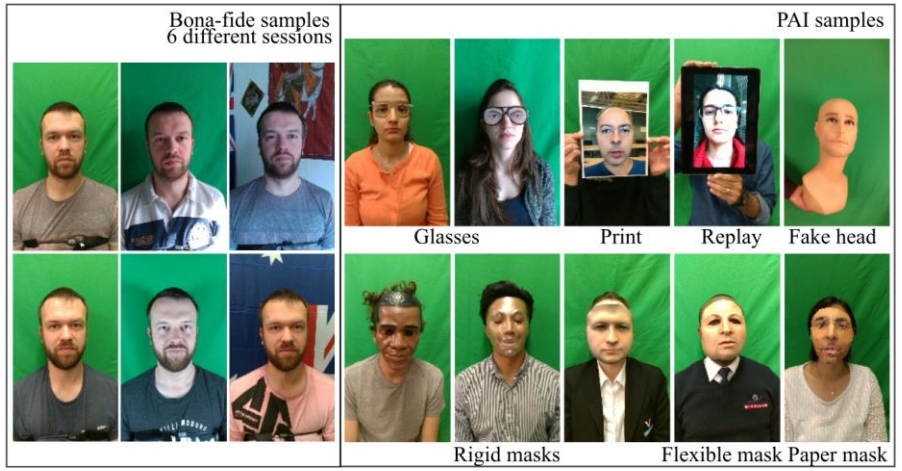


Bhattacharjee S, Mohammadi A, Marcel S. Spoofing deep face recognition with custom silicone masks, BTAS 2018

# 3D Mask Face Anti-spoofing

- Domain adaptation approach
  - Transfer the knowledge of facial appearance from RGB to multi-channel domain.
  - Learn the features of individual facial regions




Nikisins O, George A, Marcel S. Domain Adaptation in Multi-Channel Autoencoder based Features for Robust Face Anti-Spoofing, ICB 2019

# Our Recent Works

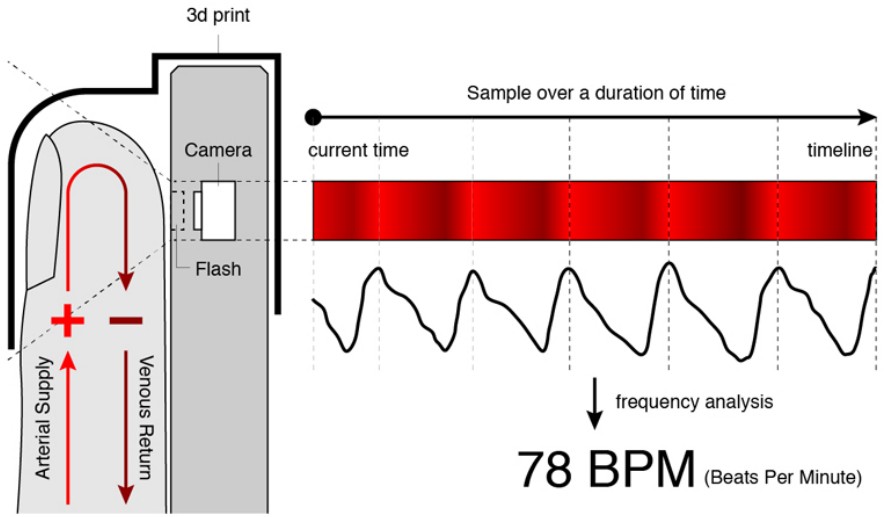
- PhotoPlethysmoGraphy based Approach
- Deep Dynamic Feature Approach
- Domain Generalization Approach
- Federated Learning Approach

# PhotoPlethysmoGraphy based Face Anti-spoofing Approach for 3D Mask Attack

## Reference:

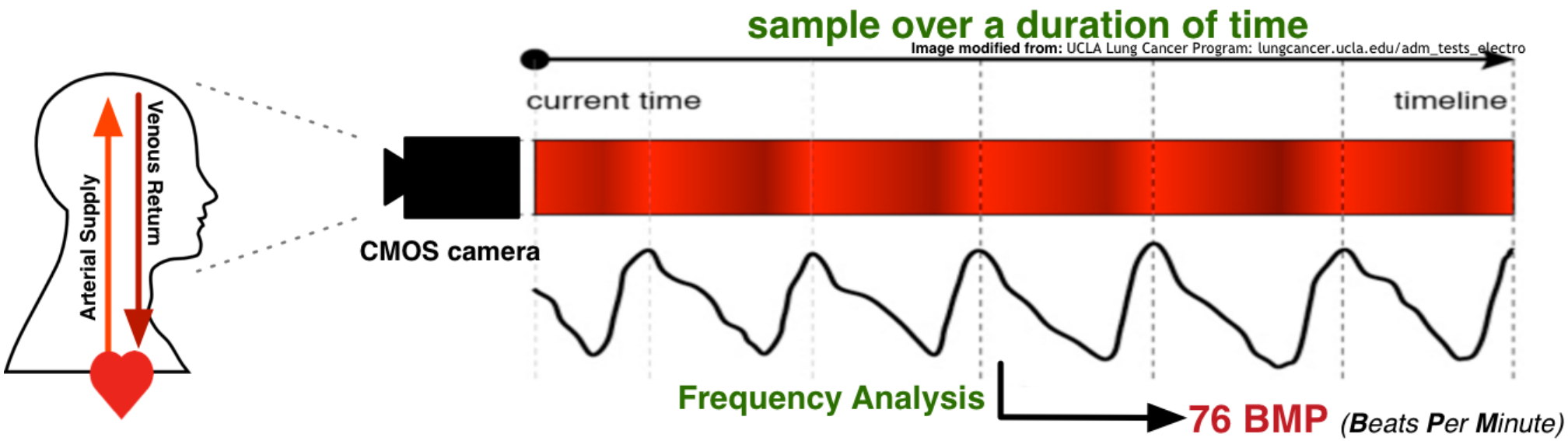

1. S Q Liu, X Y Lan and P C Yuen, "Multi-Channel Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection", *IEEE Transactions on Information Forensics and Security (TIFS)*, In press 2021
2. S Q Liu, X Lan, P C Yuen, "Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection", *Proceedings of the European Conference on Computer Vision (ECCV)*, pp. 558-573, Sept. 2018.
3. S Q Liu, P C Yuen, S Zhang and G Zhao, "3D Mask Face Anti-spoofing with Remote Photoplethysmography" *European Conference on Computer Vision (ECCV)*, Oct 2016.
4. X Li, J Määttä, G Zhao and P C Yuen and M Pietikäinen, "Generalized face anti-spoofing by detecting pulse from face videos", *International Conference on Pattern Recognition (ICPR)*, Dec 2016.

# PhotoPlethysmoGraphy (PPG)

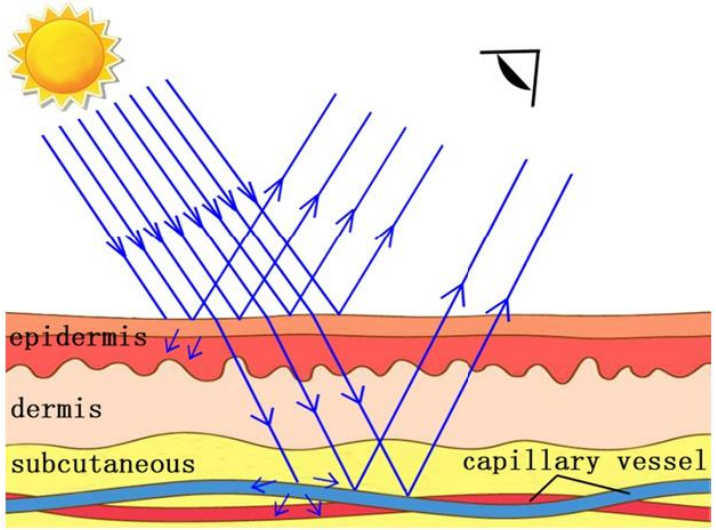



Pic. from UCLA Lung Cancer Program http://lungcancer.ucla.edu/adm_tests_electro.html

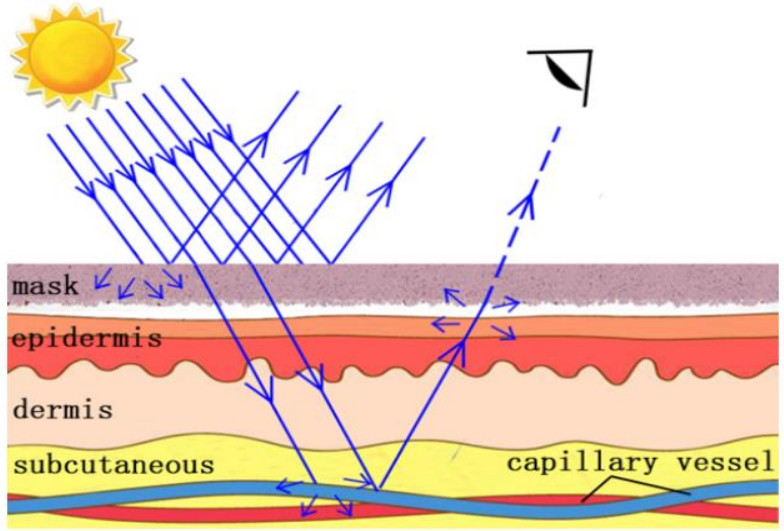
# remote PhotoPlethysmoGraphy (rPPG)



# Principle of rPPG Based Face Anti-Spoofing




(a)




(b)

(a) rPPG signal can be extracted from genuine face skin.

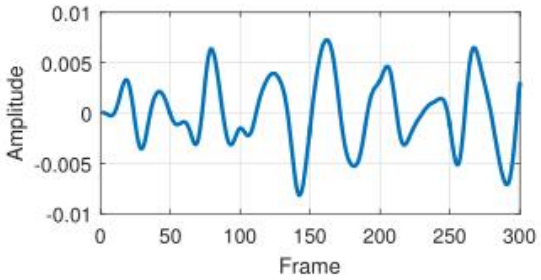
(b) rPPG signals will be **too weak** to be detected from a masked face.

- light source needs to penetrate the mask before interacting with the blood vessel.
- rPPG signal need to penetrate the mask before capturing by camera

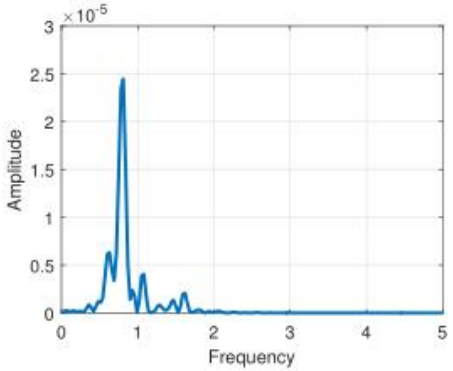
# Principle of rPPG Based Face Anti-Spoofing

genuine face

(a)



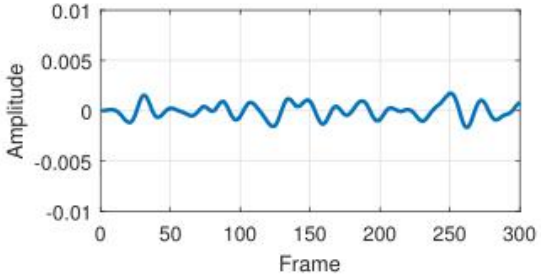

(b)



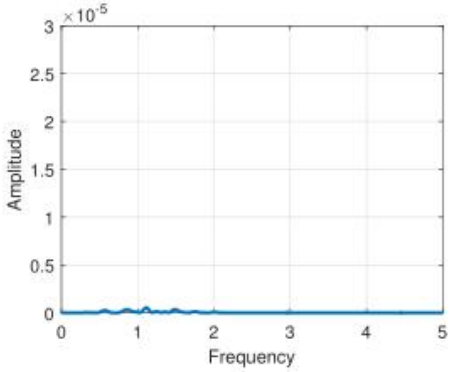

(c)

masked face

(d)

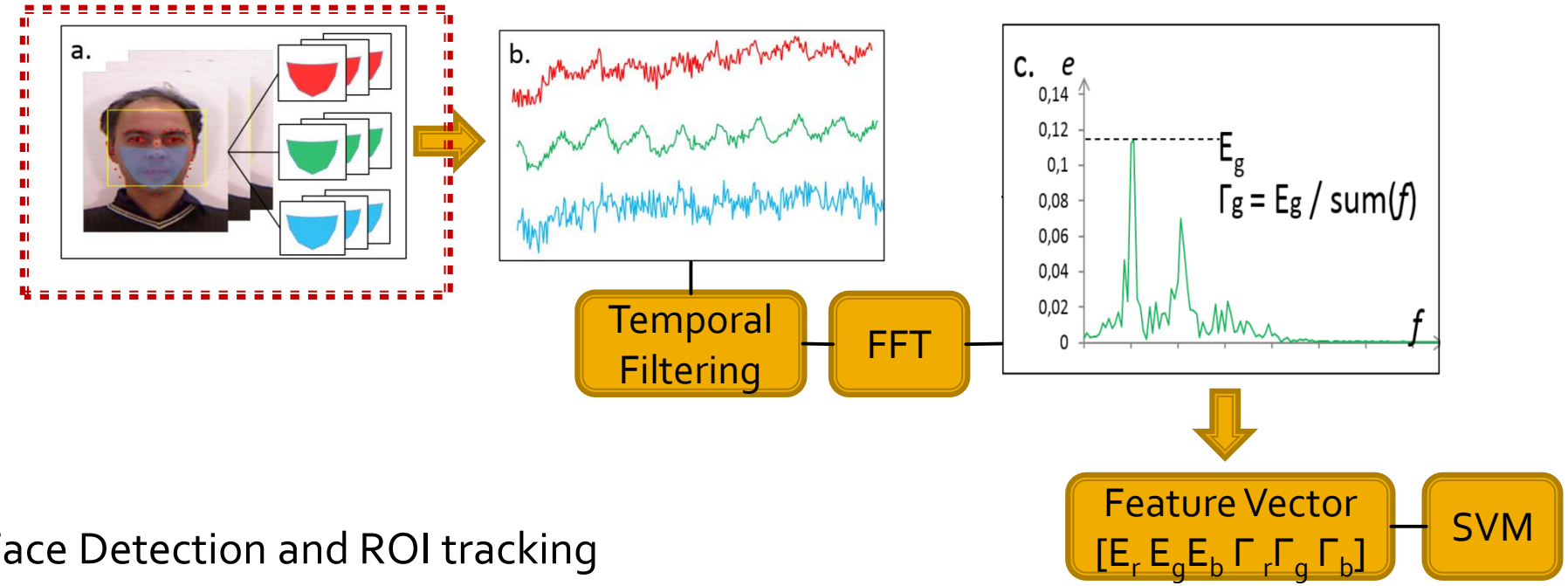



(e)




(f)

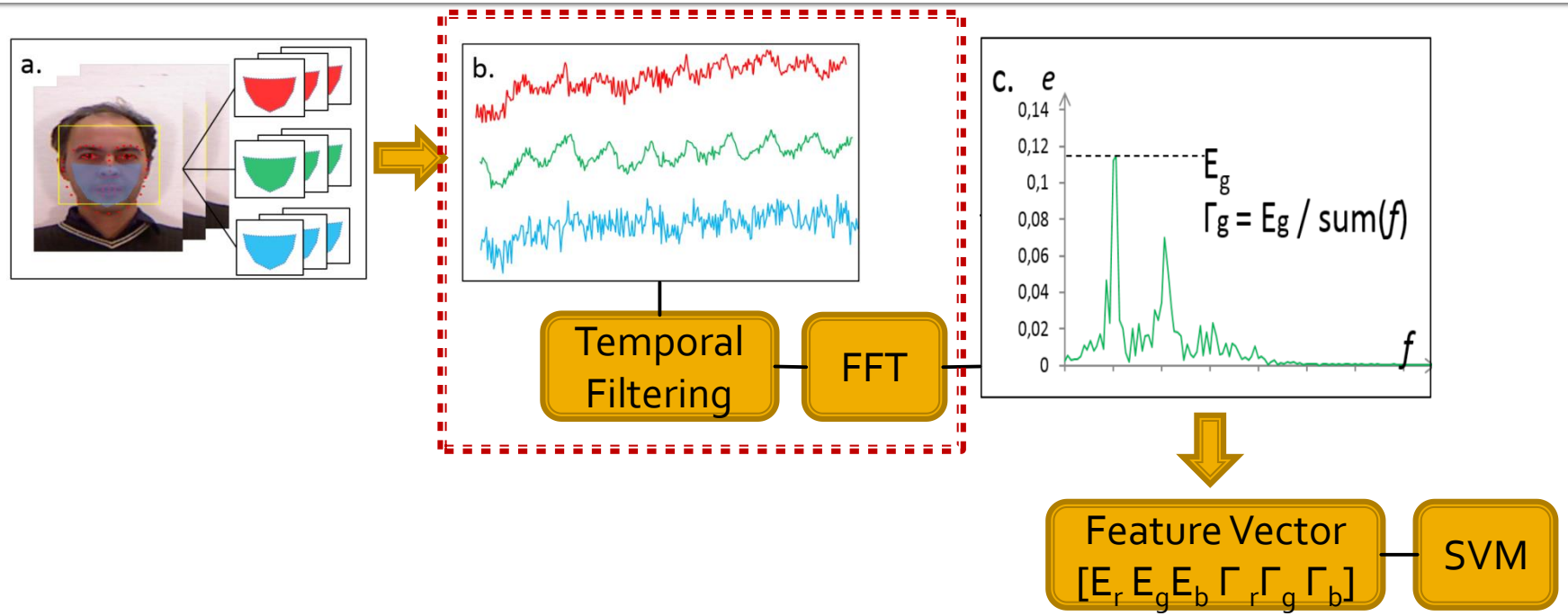
# Global rPPG-based Face Anti-Spoofing [ICPR 2016]




a. Face Detection and ROI tracking
   - Use Viola-Jones face detector on the first frame
   - Find 66 facial landmarks [CVPR'13 Asthana et.al] within the face bounding box. Use 9 of them to define the ROI
   - ROI is tracked through all frames using KLT

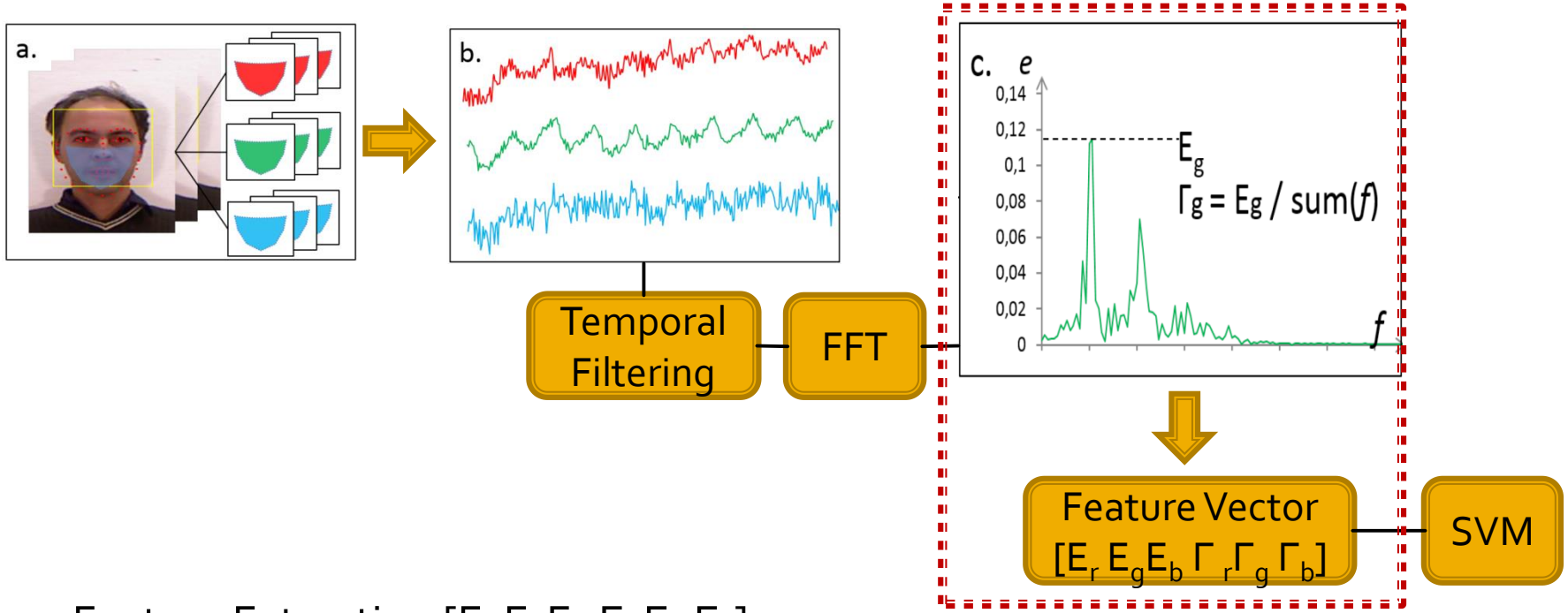
X Li, J Komulainen, G Zhao, P C Yuen and M Pietikainen, "Generalized face anti-spoofing by detecting pulse from face videos" *ICPR* 2016

# Global rPPG-based Face Anti-Spoofing




b. Three raw pulse signals $r_{raw}$ $g_{raw}$ and $b_{raw}$ are computed; one from each RGB channel, respectively.
   - FIR bandpass filter with a cutoff frequency range of [0.7; 4] Hz ([42; 240] beat-per-minute)
   - Use fast Fourier transform (FFT) to convert the pulse signals into frequency domain-> PSD curve: $f$

# Global rPPG-based Face Anti-Spoofing




c. Feature Extraction $[E_r\ E_g E_b\ \Gamma_r \Gamma_g\ \Gamma_b]$

- $E = \max(e(f))$
- $\Gamma = \frac{E}{\sum_{\forall f \in [0.7,4]} e(f)}$

# Experimental Results

- Data:
  - 3DMAD [Erdogmus et.al TIFS'14]
    - 255 videos recorded from 17 subjects
    - Masks made from *ThatsMyFace.com*
  - 2 REAL-F Masks
    - 24 videos recorded from 2 subjects
    - Hyper real masks from *REAL-F*

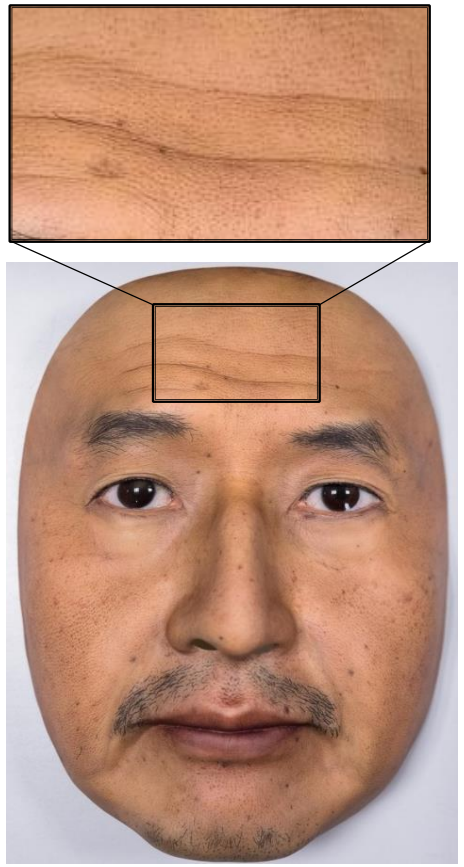
# Experimental Results

- Results on REAL-F (cross dataset)
  - Randomly select 8 subjects from 3DMAD for training and the other 8 subjects as the development set

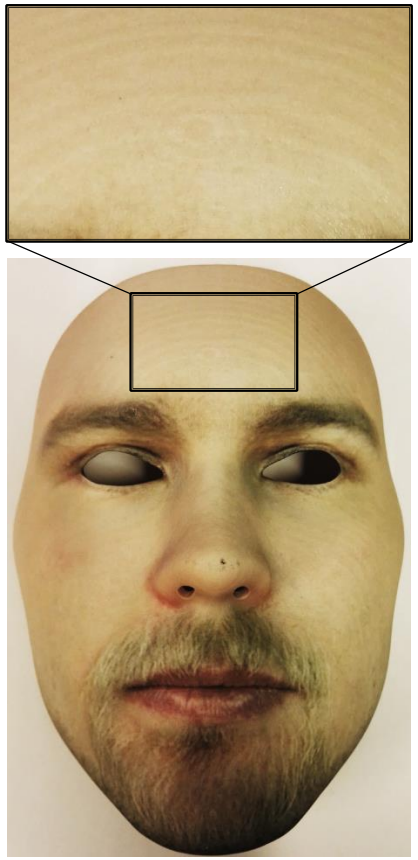
| | REAL-F | | | |
|---|---|---|---|---|
| Method | HTER(%) | EER(%) | FPR (@FNR=0.1%) | FPR (@FNR=0.01%) |
| **Pulse (ours)** | **4.29** | **1.58** | **0.25** | **3.83** |
| LBP-blk | 26.3 | 25.08 | 37.92 | 48.25 |
| LBP-blk-color | 25.92 | 20.42 | 31.5 | 48.67 |
| LBP-ms | 39.87 | 46.5 | 59.83 | 73.17 |
| LBP-ms-color | 47.38 | 46.08 | 86.5 | 95.08 |

# Analysis of Results

- Observations:
  - LBP-based texture method gives *zero error for 3DMAD* dataset but very *large error in REAL-F*
  - Global rPPG method (pulse) provides *very small errors in both 3DMAD and REAL-F datasets*



REAL-F



3DMAD

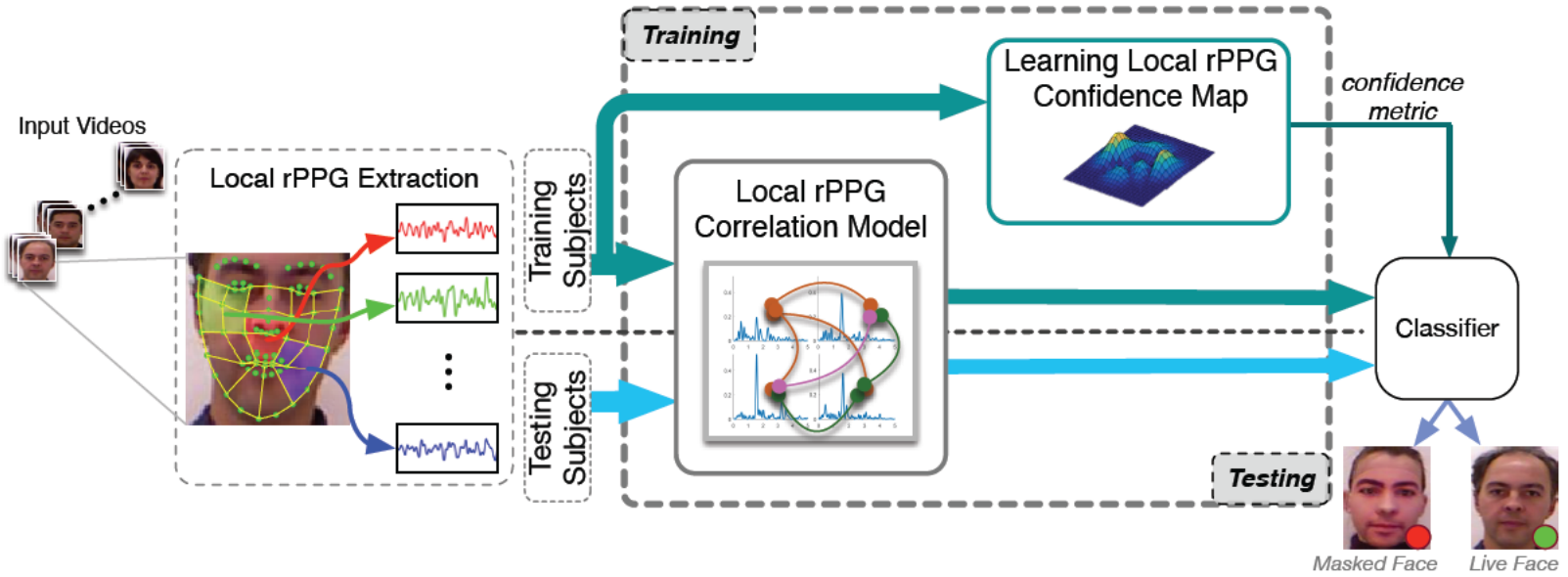
# Limitations on Global rPPG method

- Global rPPG signal is sensitive to certain variations such as illuminations, head motion and video quality
- rPPG signal strength may vary with different subjects

# How to increase the robustness of rPPG-based Face Anti-spoofing?

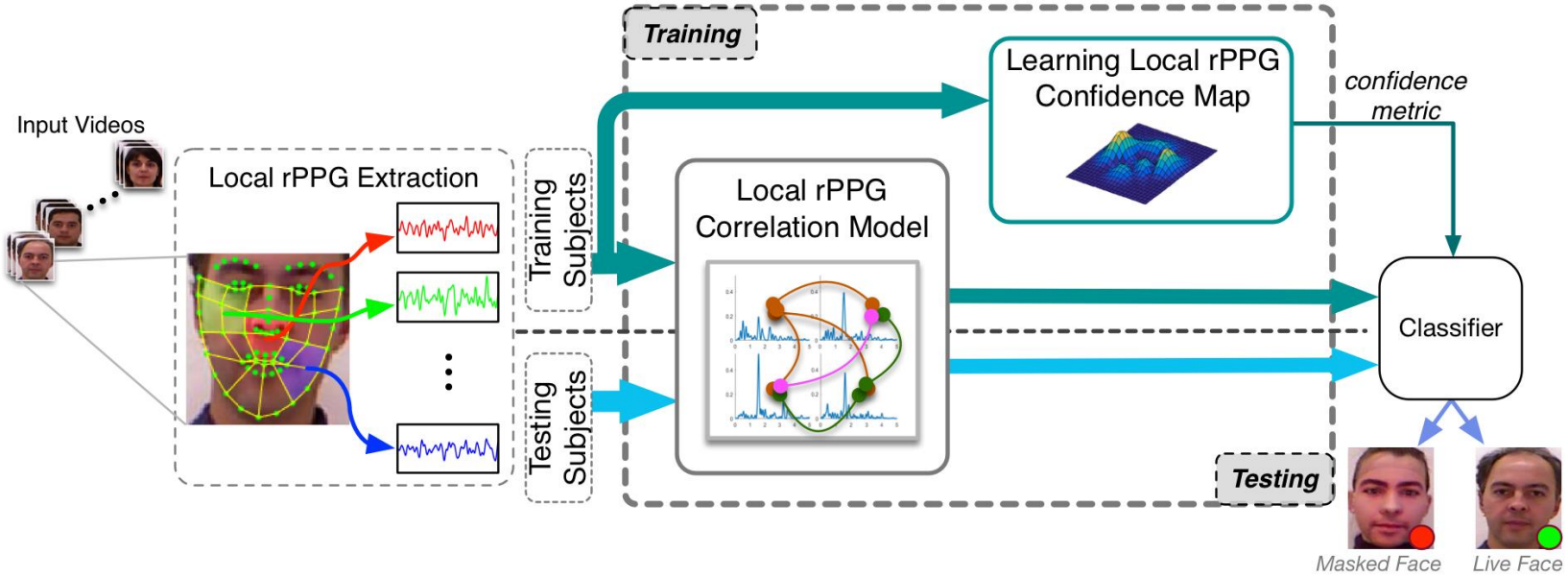
# Local rPPG based Face Anti-Spoofing Method

## [ECCV 2016]




S Q Liu, P C Yuen, S P Zhang and G Y Zhao, "3D Mask Face Anti-spoofing with Remote Photoplethysmography" *ECCV 2016*

# Local rPPG based Face Anti-Spoofing Method




(a) Local ROIs are pre-defined based on the facial landmarks. Local rPPG signals are extracted from these local face regions.

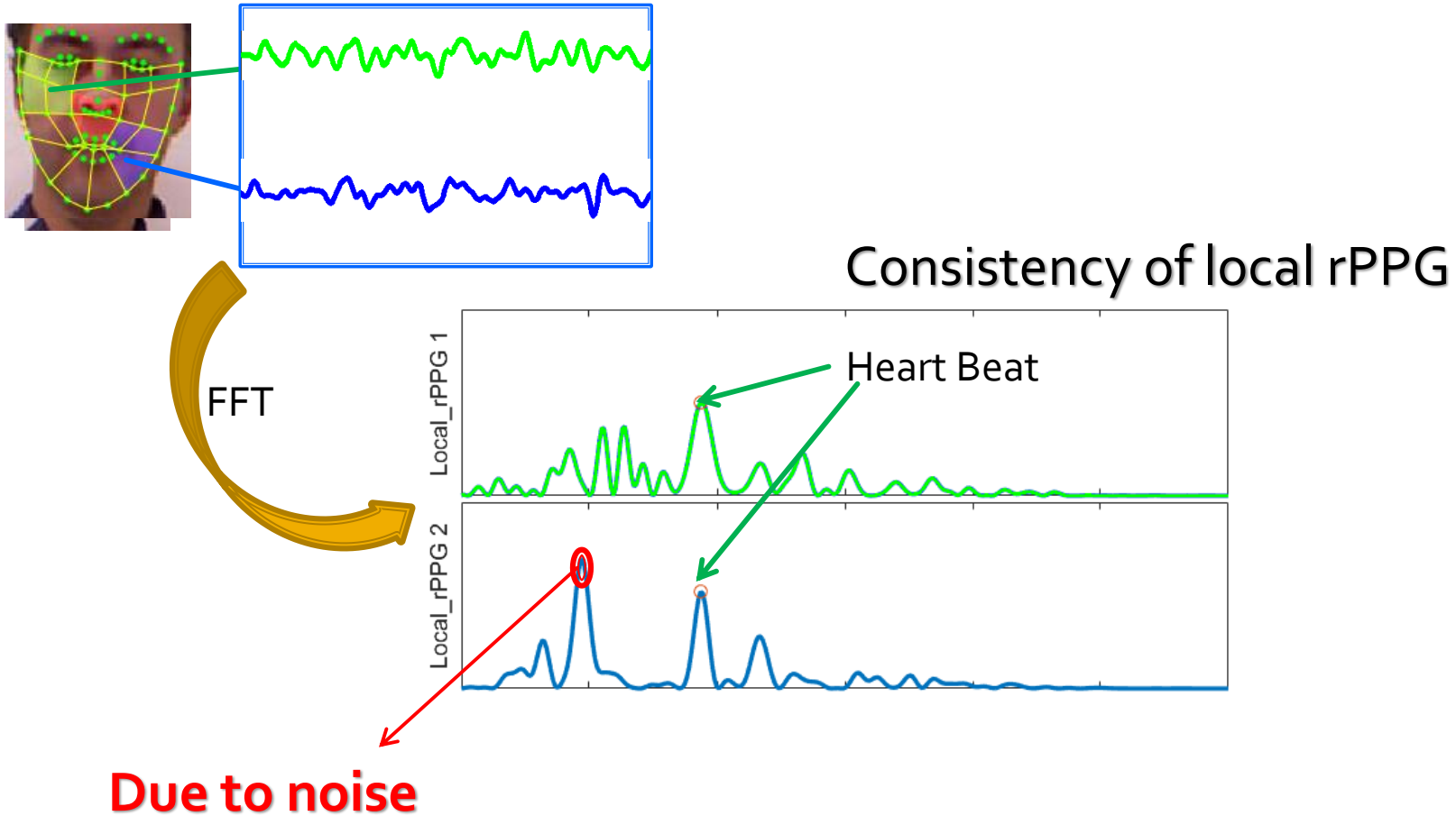
(b) Extract Local rPPG patterns through the proposed **local rPPG correlation model**.

(c) Training stage: local rPPG confidence map is learned, and then transformed into distance metric for classification.

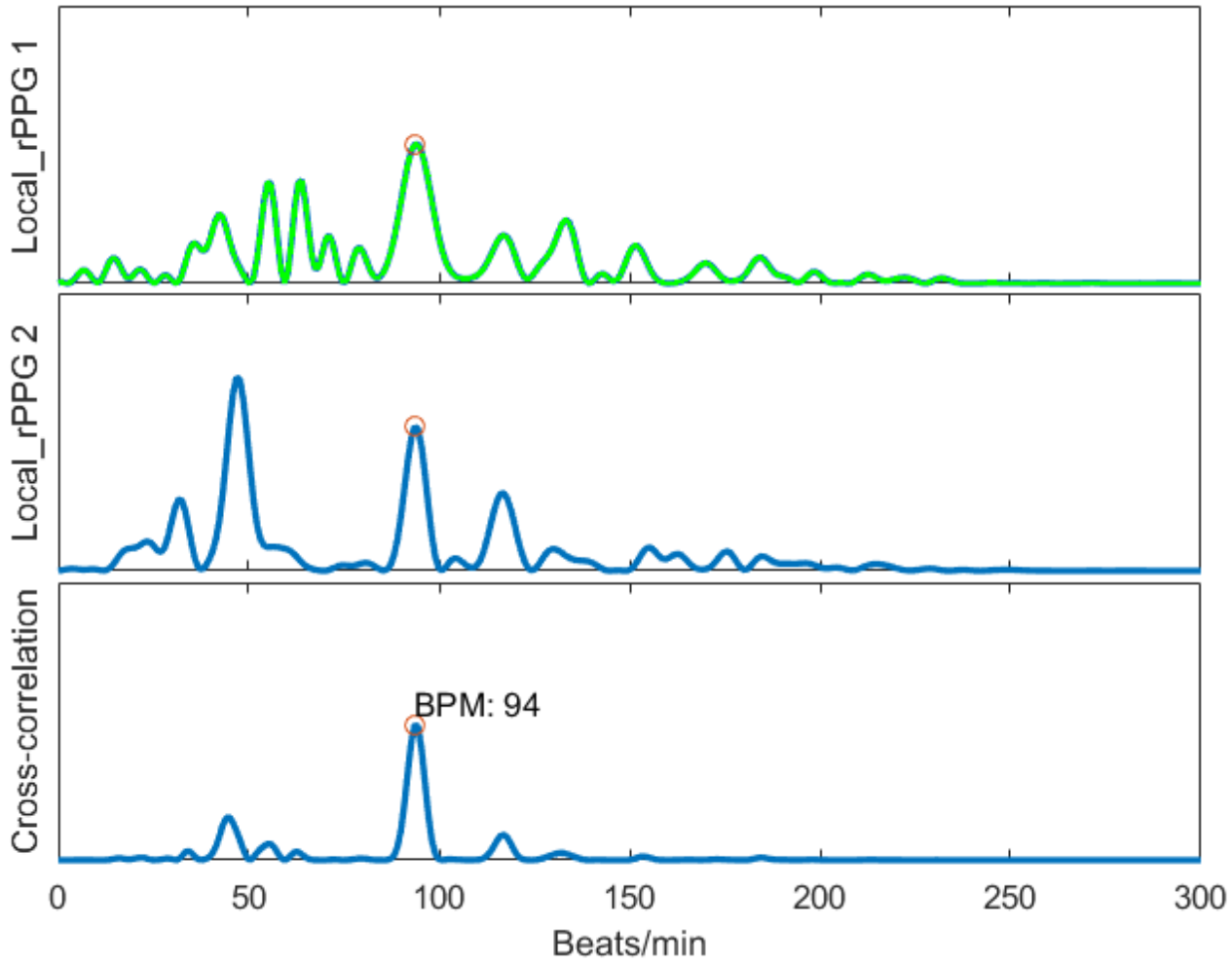
(d) Classifier: SVM

# Contribution 1: Local rPPG Correlation Model

- Local rPPG on genuine face

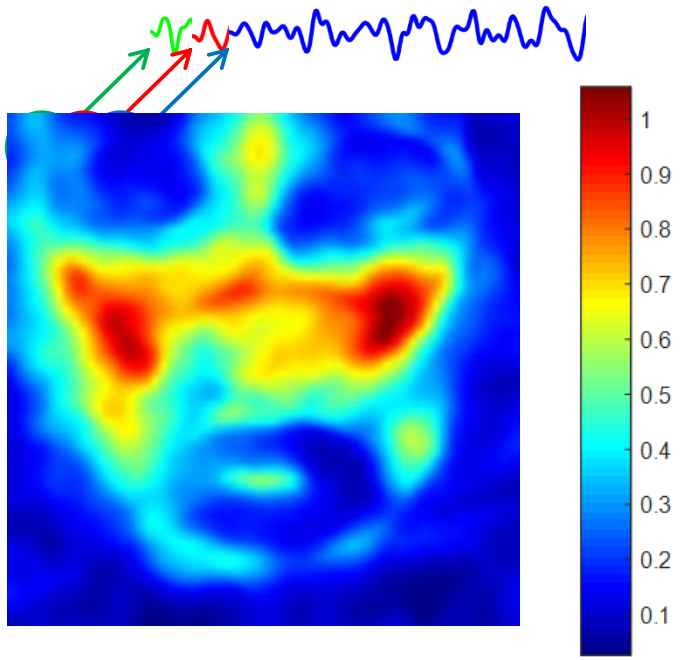


# 2. Local rPPG Correlation Model



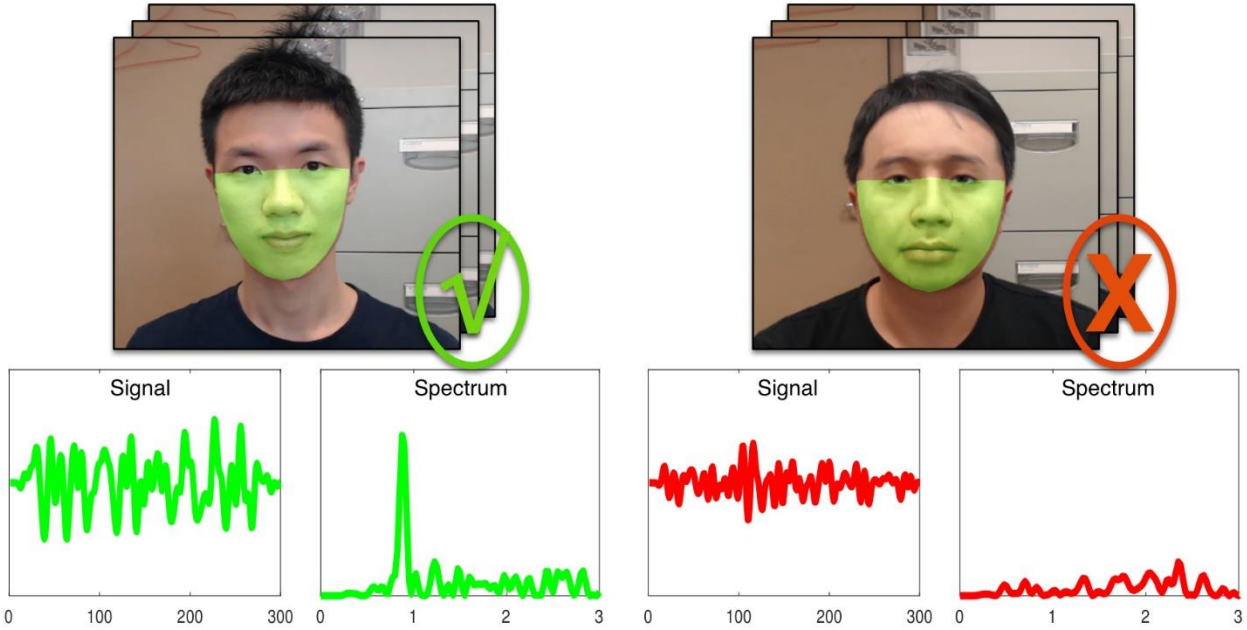
# Contribution 2: Learning Local rPPG Confidence Map


Generic map of blood vessels on the face




**The distribution of local rPPG signals should be considered**

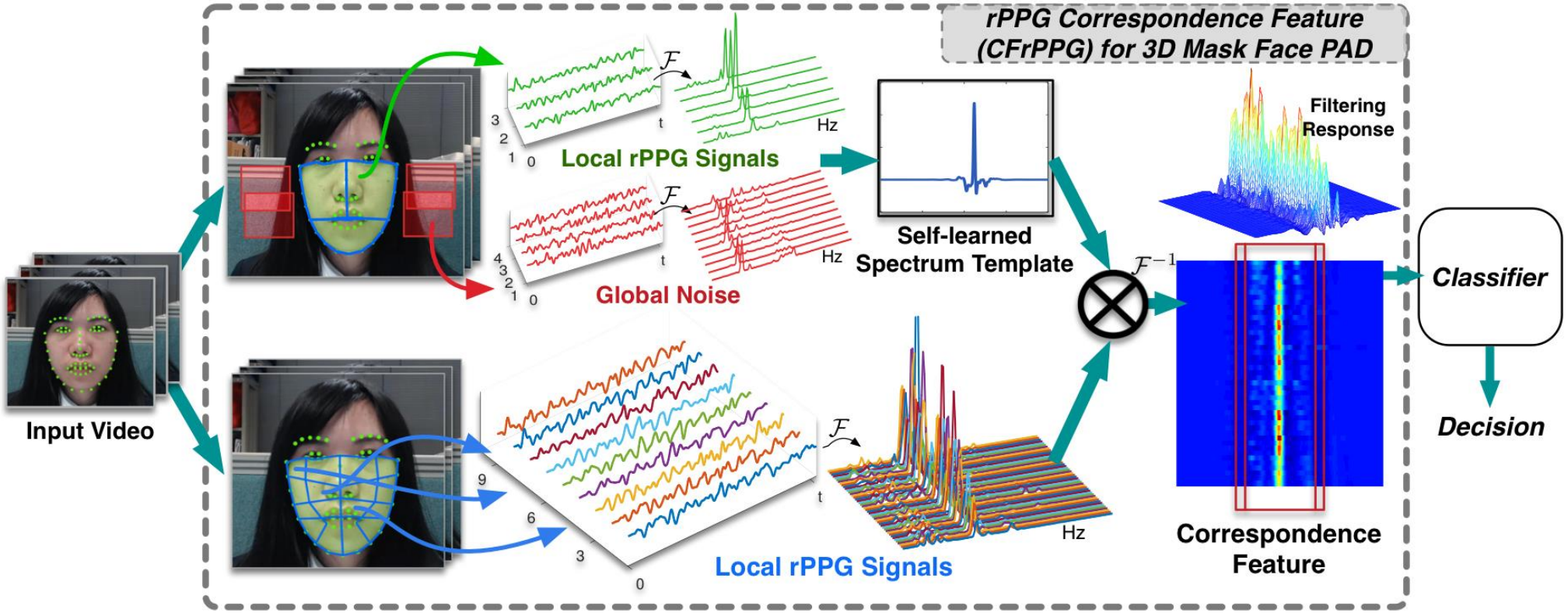
# Limitation on Local rPPG Approach




How to **accurately obtain the liveness evidence** from the observed noisy rPPG signals**?**

# Improved Method: rPPG Correspondence Feature

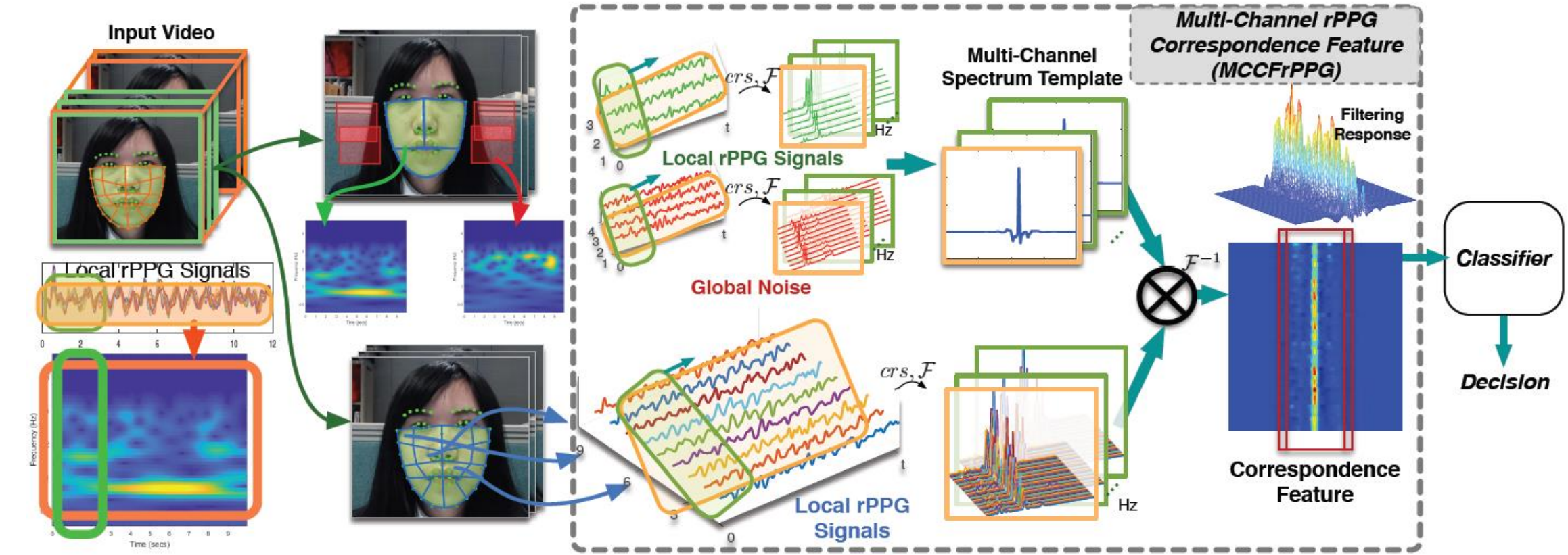
## [ECCV 2018]




1. S Q Liu, X Y Lan and P C Yuen, "Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection", *ECCV* 2018

# Improved Method: rPPG Correspondence Feature

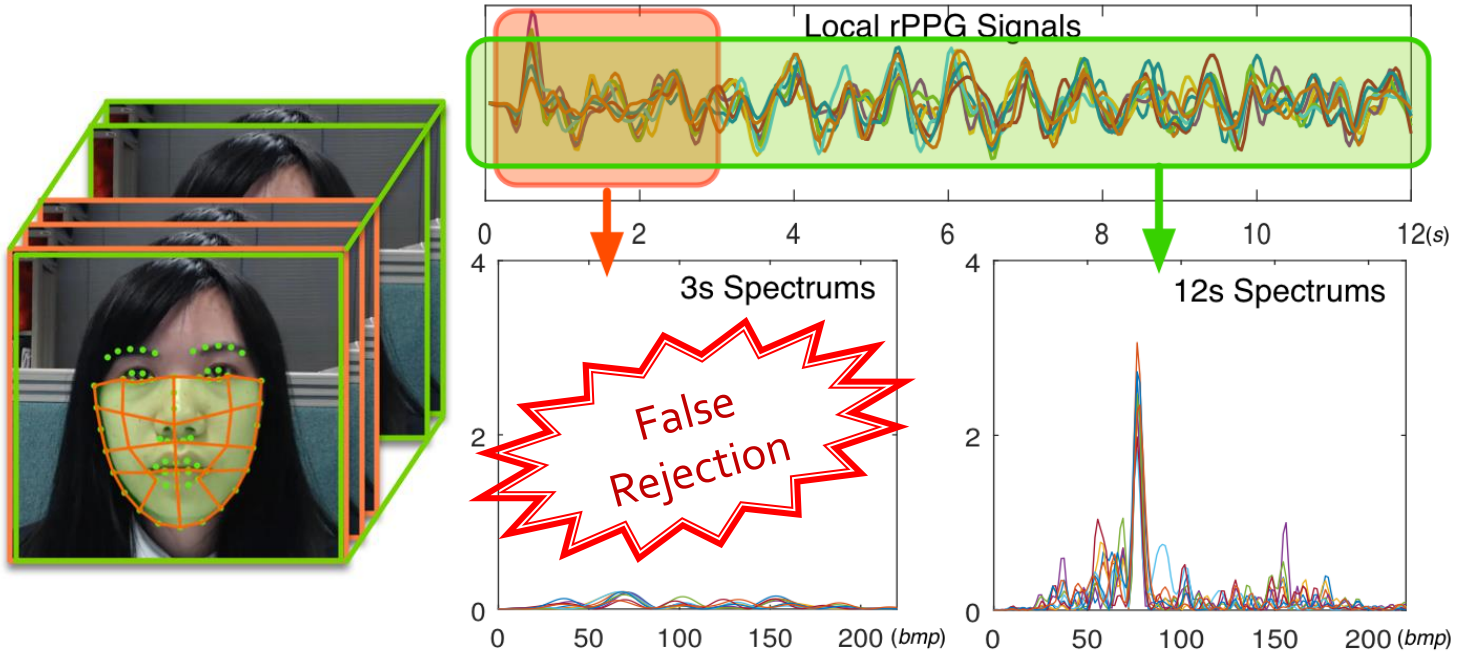
## [TIFS 2021]

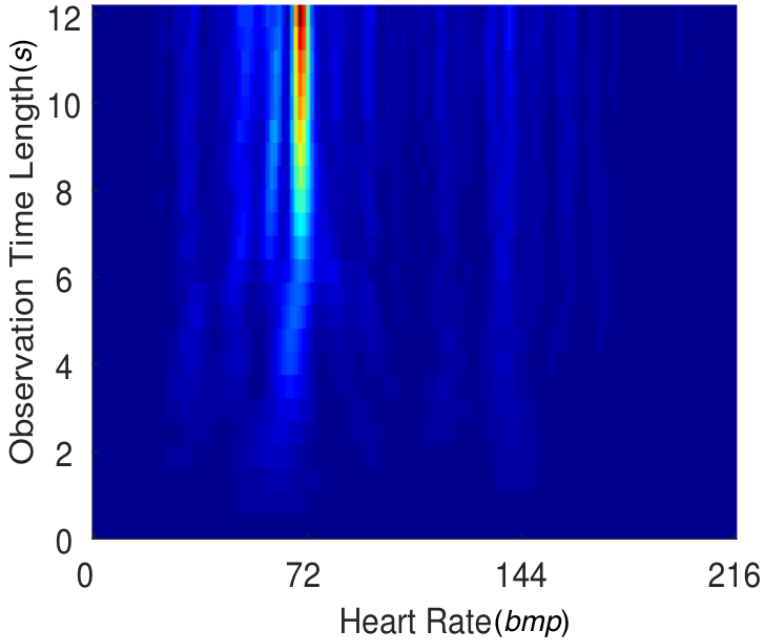




1. S Q Liu, X Y Lan and P C Yuen, "Multi-Channel Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection", *IEEE Transactions on Information Forensics and Security (TIFS)*, 2021.

# Limitations on existing rPPG Methods

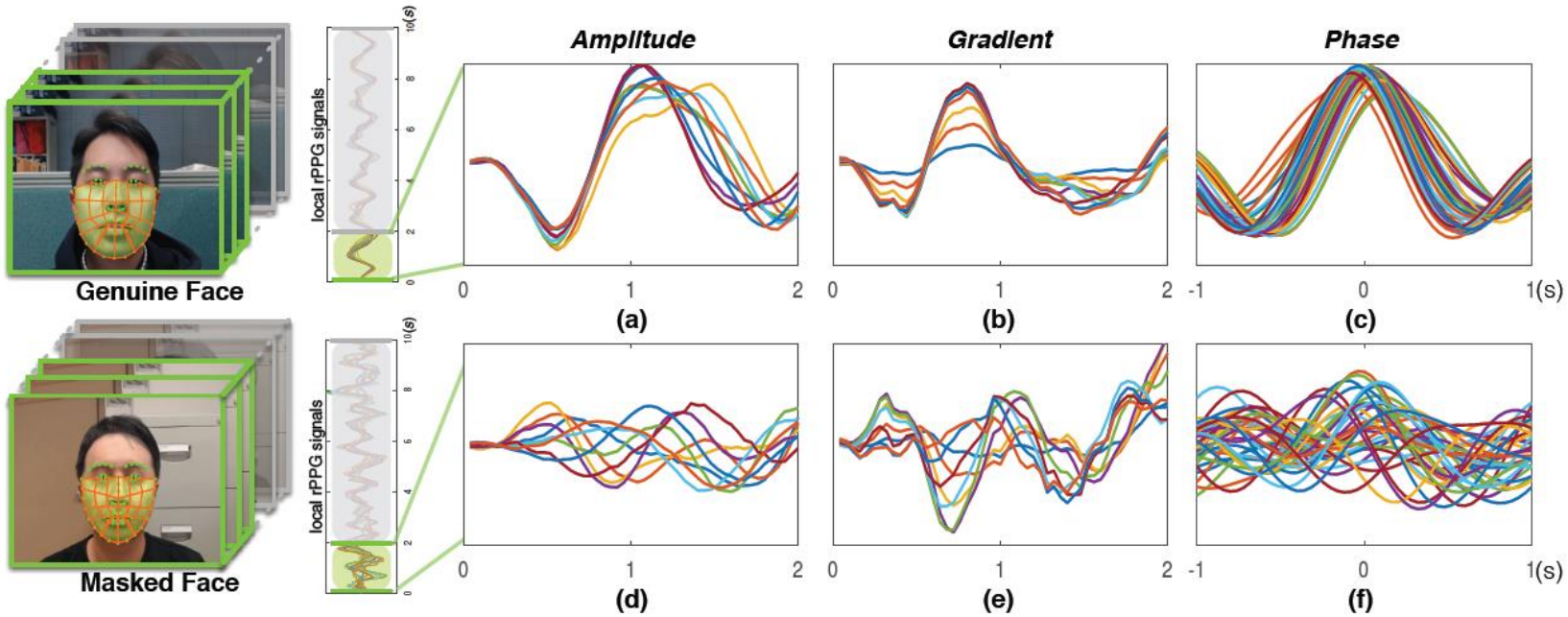



Existing rPPG-based 3D mask PAD methods are based on spectrum analysis

→ Require long observation time (8-10 seconds) to identify heartbeat information

# Temporal Similarity Analysis of rPPG (TSrPPG) for Fast 3D Mask Face PAD



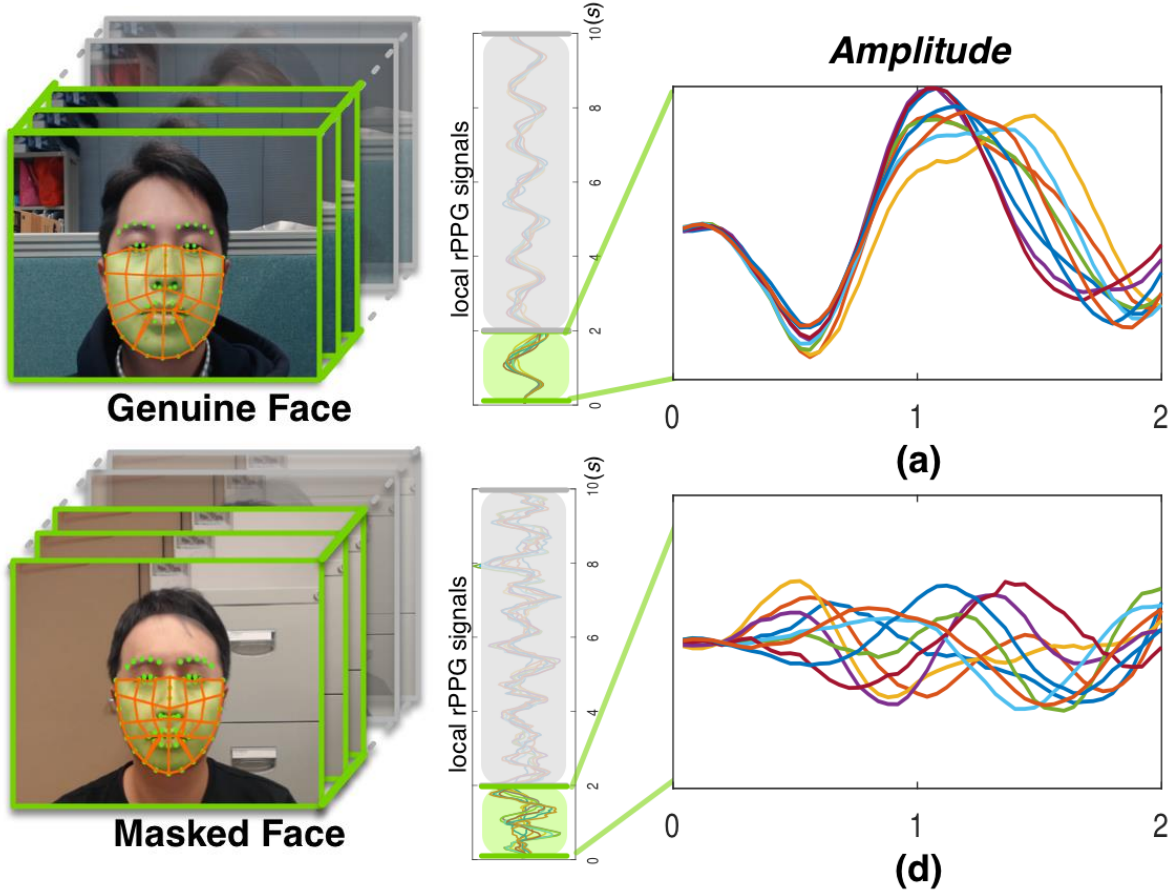


Reference:

1. S Q Liu, X Y Lan, and P C Yuen, "Temporal Similarity Analysis of Remote Photoplethysmography (TSrPPG) for Fast 3D Mask Face Presentation Attack Detection", *WACV*, 2020.

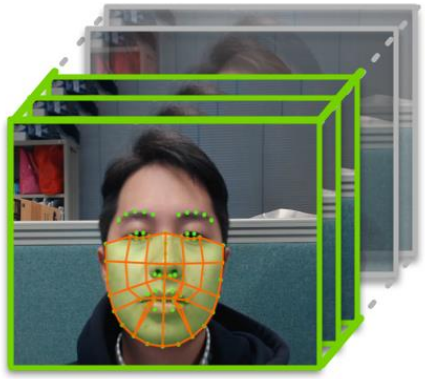
2. S Q Liu, X Y Lan and P C Yuen, "Learning Temporal Similarity of Remote Photoplethysmography for Fast 3D Mask Face Presentation Attack Detection", *IEEE Transactions on Information Forensics and Security (TIFS),* In press, 2022.

# The proposed TSrPPG

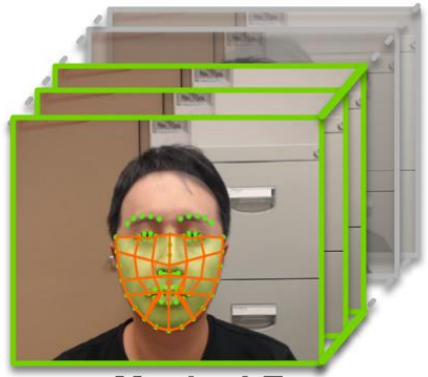



- Rationale
  - Correlation of local rPPG signals on genuine faces is higher compared with those on masked faces.
  - The periodicity information is not available within short observation time.
    - Hard to adopt spectrum analysis
  - Design liveness feature in temporal space

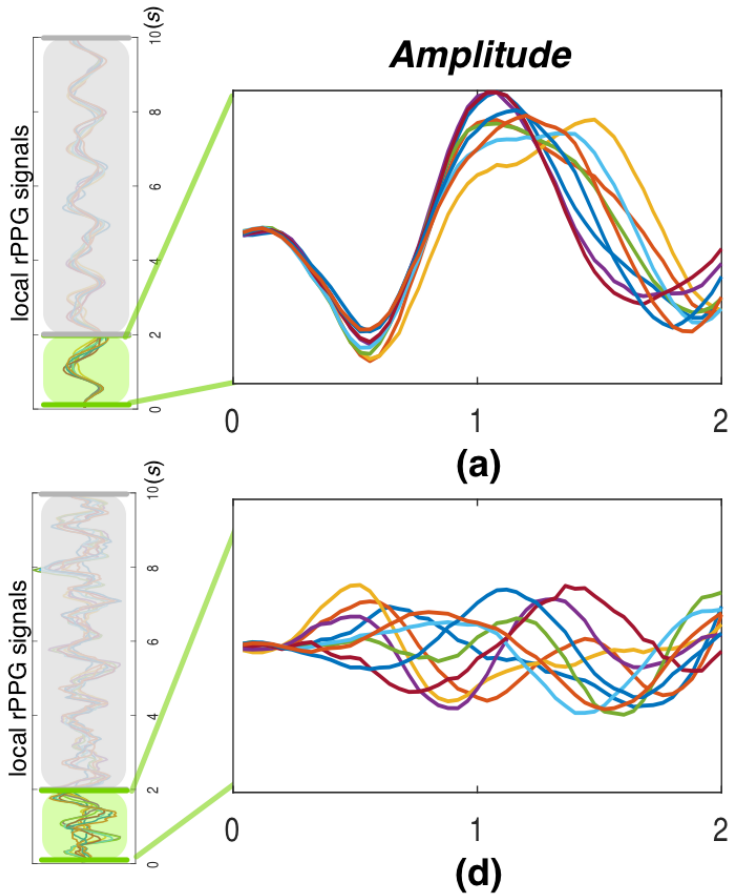
# The proposed TSrPPG



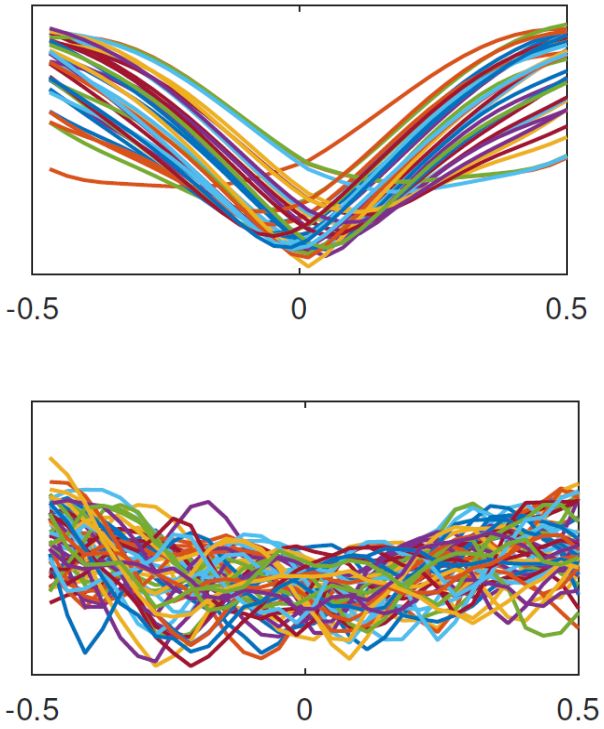
Genuine Face



Masked Face




$$\boldsymbol{TSrPPG}_{i,j}[m] = \int_{-\infty}^{+\infty} \mathcal{D}(\boldsymbol{s}_i[t], \boldsymbol{s}_j[t+m])dt$$

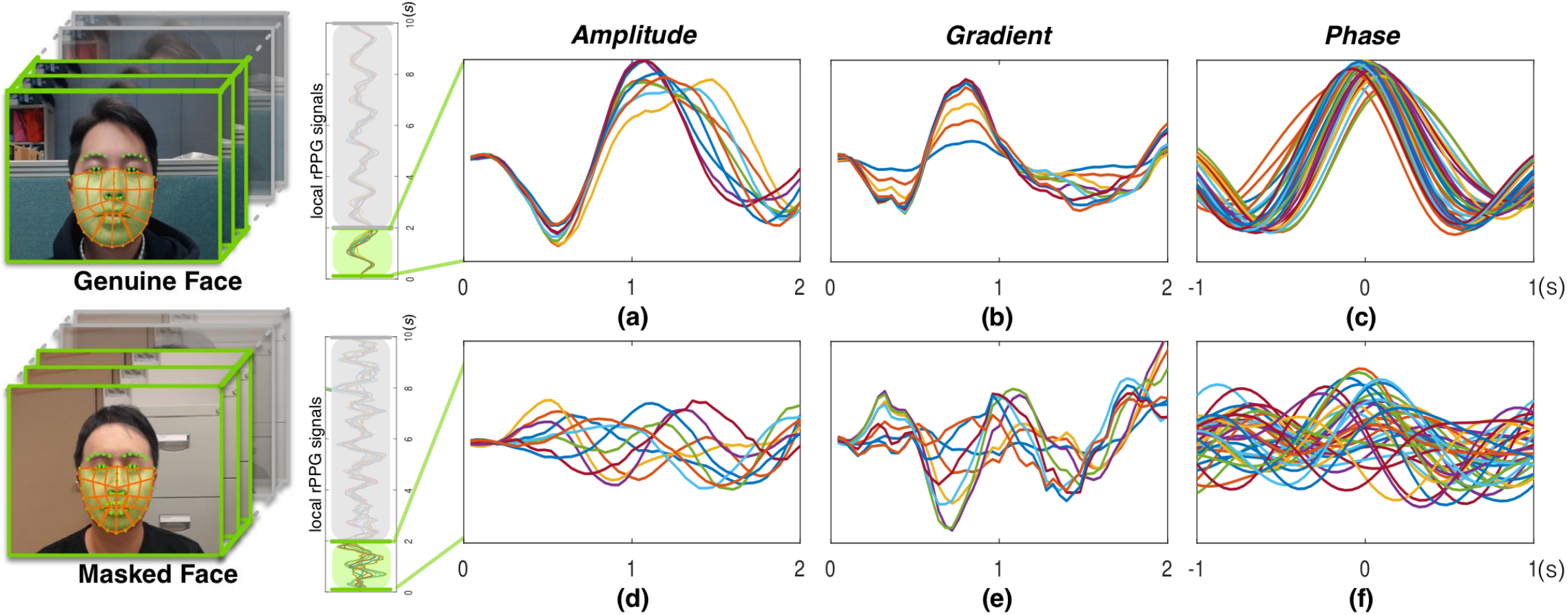



Extract features on the result pattern

→ Min, Mean, Std (… etc.)

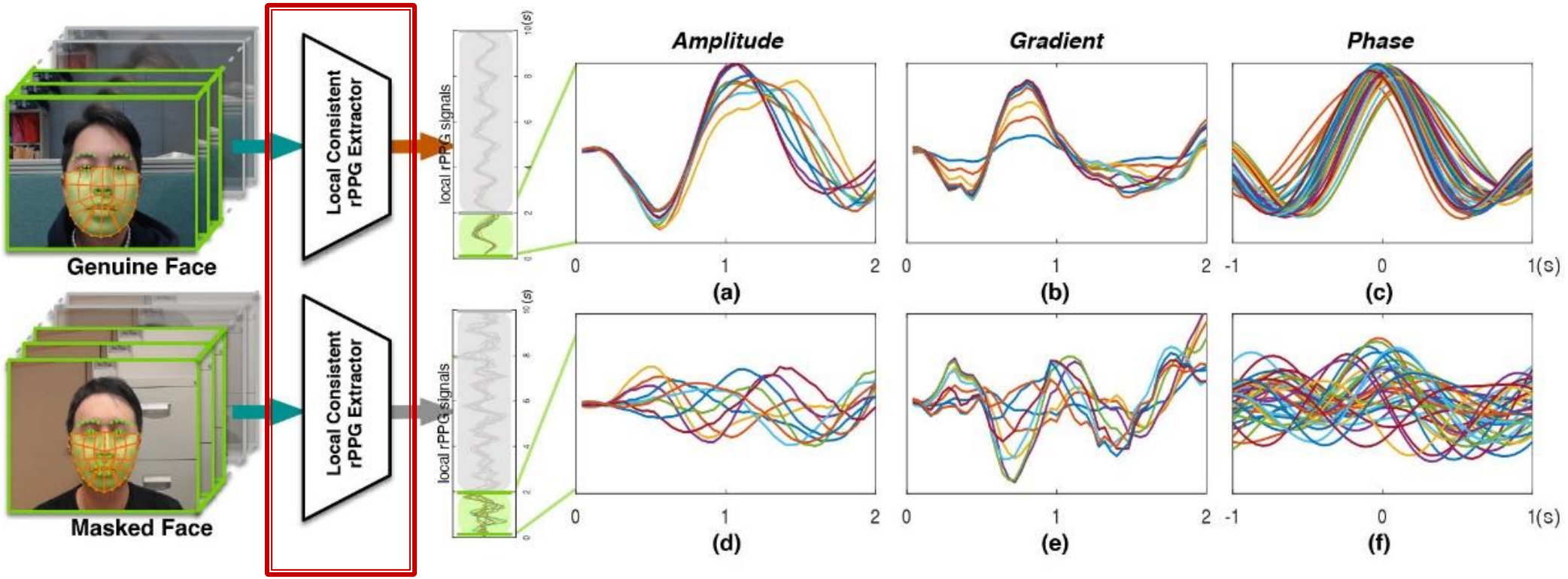
# The proposed TSrPPG

$$TSrPPG_{i,j}[m] = \int_{-\infty}^{+\infty} \mathcal{D}(s_i[t], s_j[t+m])dt$$



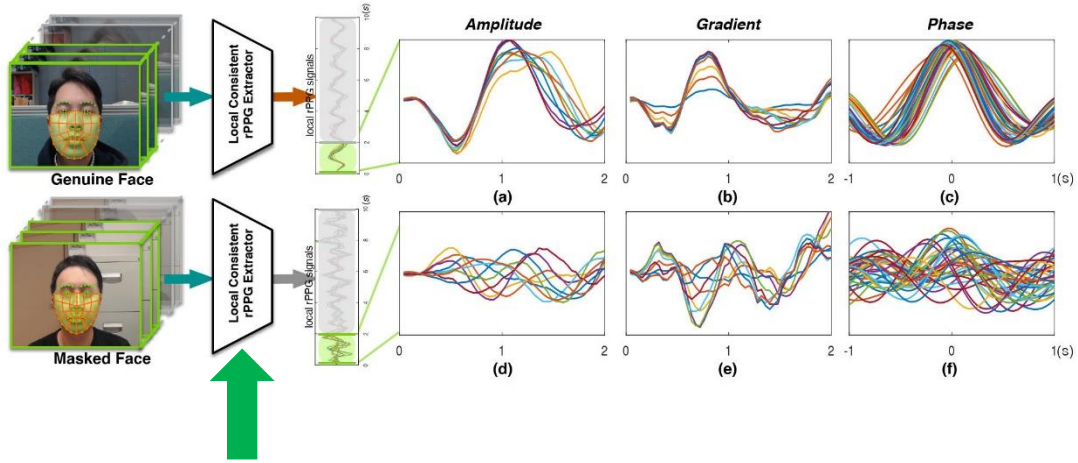

Final result is obtained through score-level-fusion

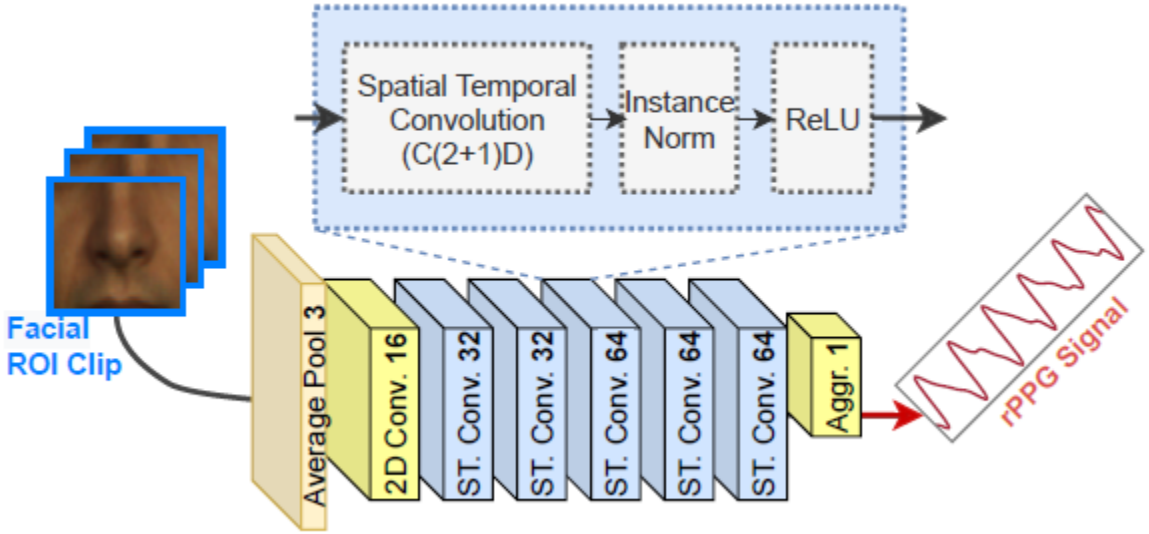
# LeTSrPPG: Learnable rPPG to enhance temporal similarity of TSrPPG



# LeTSrPPG: Learnable rPPG to enhance temporal similarity of TSrPPG

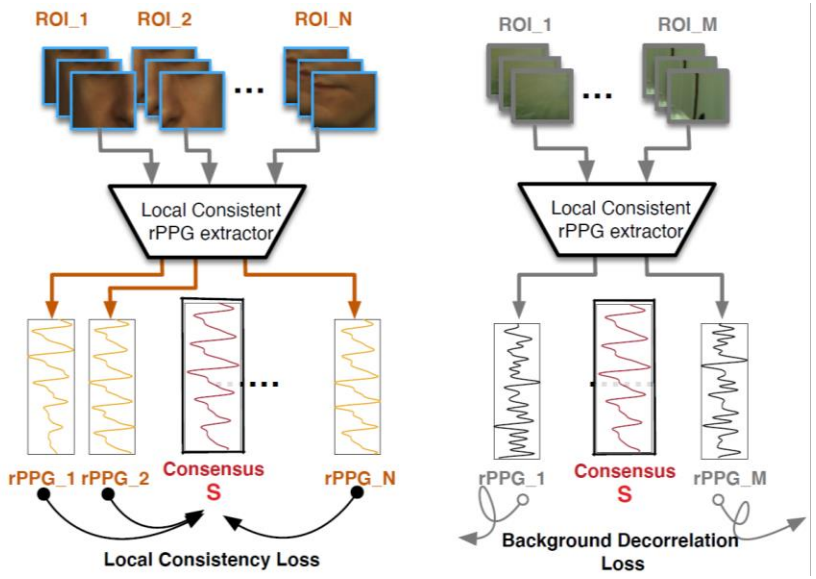
- Learnable rPPG estimator:
  - Learn robust rPPG feature through 3D convolution

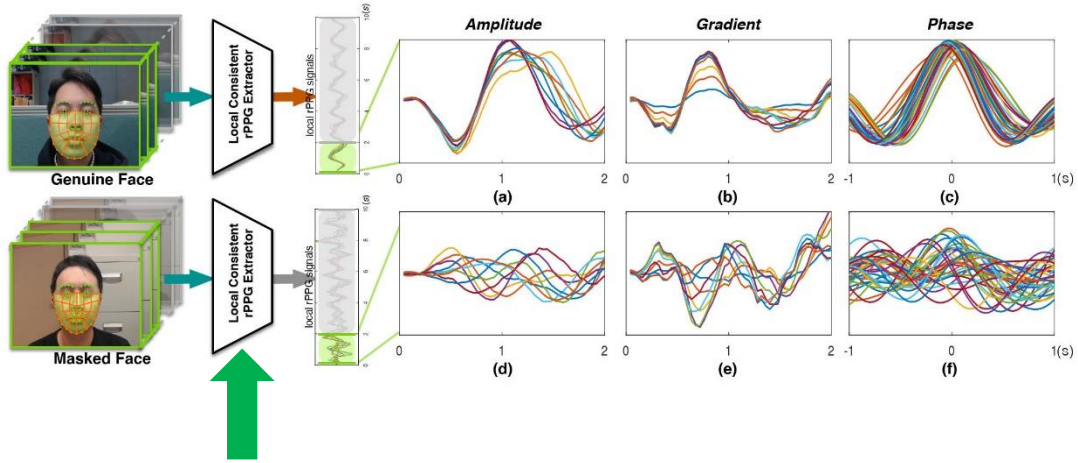


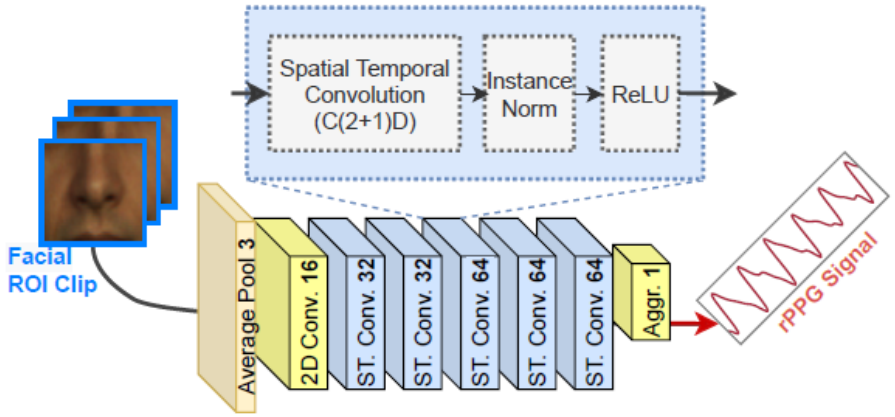



# LeTSrPPG: Learnable rPPG to enhance temporal similarity of TSrPPG

- Learnable rPPG estimator:
  - Learn robust rPPG feature through 3D convolution
  - Further boost the discriminability of TSrPPG
    - Genuine face: Enhance the temporal similarity
    - Fake face: Reduce the temporal similarity

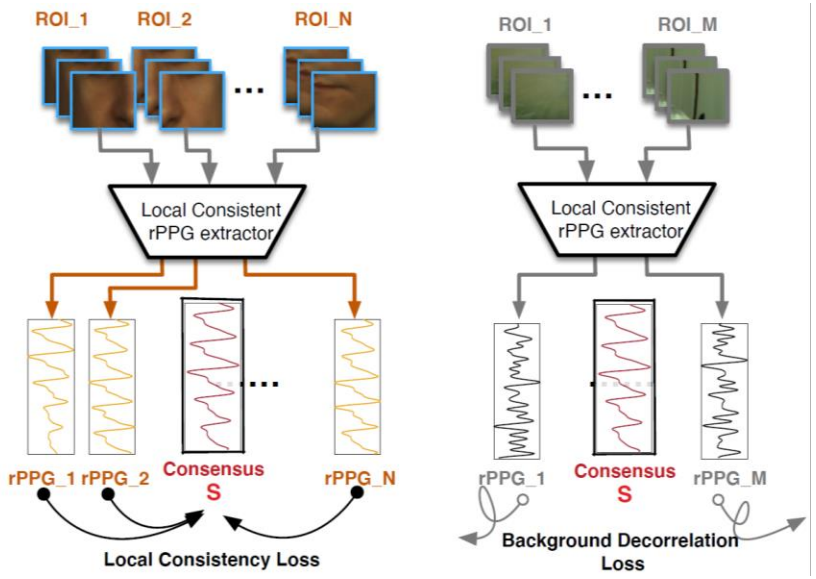


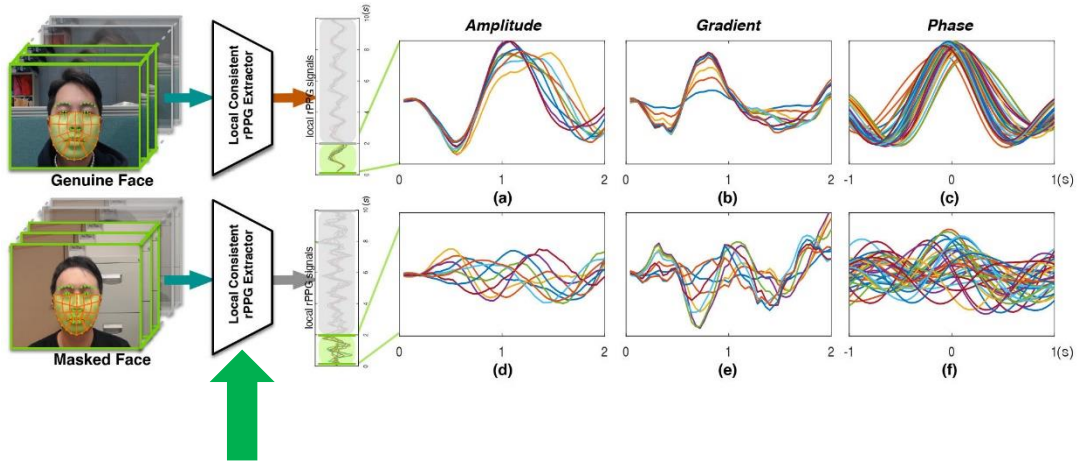



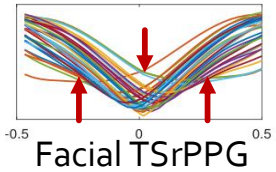



# LeTSrPPG: Learnable rPPG to enhance temporal similarity of TSrPPG

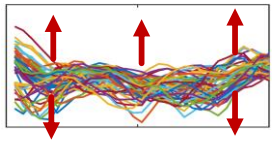
- Learnable rPPG estimator:
  - Learn robust rPPG feature through 3D convolution
  - Further boost the discriminability of TSrPPG
    - Genuine face: Enhance the temporal similarity
    - Fake face: Reduce the temporal similarity




Facial TSrPPG



Background TSrPPG

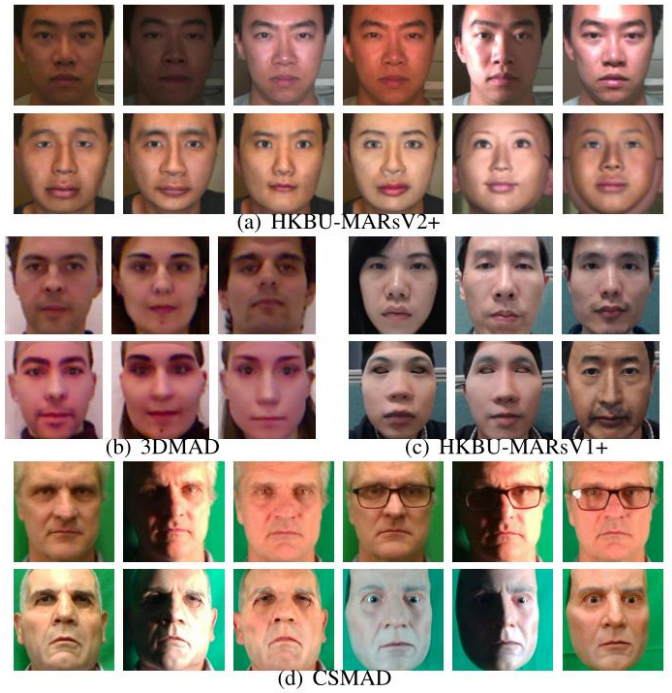
- Improve TSrPPG in rPPG extraction stage
  - Enhance the consistency of local rPPG signals
  - Reduce the correlation of background rPPG and facial rPPG
    - Can be trained without fake face samples

# LeTSrPPG: Learnable rPPG to enhance temporal similarity of TSrPPG

- Experimental Setting:

| | #Subjects/Masks | #Video Slots | Mask Type | Lighting Condition | Camera | Face (pixel) Resolution | Compression |
|---|---|---|---|---|---|---|---|
| 3DMAD [13] | 17 17 | 2550 | TMF | 1(Studio) | Kinect | 80×80 | Motion JPEG |
| HKBU-MARsV1+ [15] | 12 12 | 2160 | TMF+RF | 1(Room) | Logitech C920 | 200×200 | H.264 |
| CSMAD [30] | 14 6 | 1582 | Silicon | 4 | RealSense SR300 | 350×350 | H.264 |
| HKBU-MARsV2+ | 16 16 | 12480 | TMF+RF | 6 | 3 | 3 | 2 |
| Summary | 59 39 | 18772 | 3 | 12 | 6 | 5* | 2 |

(a) ThatsMyface (b) REAL-f (c) Silicone



(a) HKBU-MARsV2+ (b) 3DMAD (c) HKBU-MARsV1+ (d) CSMAD

- Evaluation Protocols:
  - Intra-dataset evaluation
    - Leave one subject out cross validation (**LOOCV**)
  - Cross-dataset evaluation
    - Train and test on different datasets

# LeTSrPPG: Learnable rPPG to enhance temporal similarity of TSrPPG

- Intra dataset evaluation with short observation time (1 second) :

| | HTER_dvlp | HTER_test | EER | AUC |
|---|---|---|---|---|
| GrPPG | 34.1 ± 5.7 | 33.7 ± 11.6 | 38.3 | 65.9 |
| PPGSec | 33.3 ± 3.1 | 33.0 ± 8.1 | 34.8 | 69.4 |
| LrPPG | 45.2 ± 3.2 | 44.8 ± 8.8 | 45.3 | 55.7 |
| CFrPPG | 32.8 ± 1.7 | 32.7 ± 7.4 | 32.5 | 70.8 |
| TransrPPG | 20.7 ± 2.2 | 20.6 ± 8.3 | 20.8 | 84.5 |
| TSrPPG | 13.1 ± 3.0 | 13.4 ± 11.2 | 13.3 | 93.8 |
| LeTSrPPG | **11.5 ± 2.7** | **11.8 ± 8.6** | **11.9** | **94.4** |

3DMAD

| | HTER_dvlp | HTER_test | EER | AUC |
|---|---|---|---|---|
| GrPPG | 29.2 ± 4.7 | 29.1 ± 9.7 | 33.8 | 72.0 |
| PPGSec | 42.4 ± 2.1 | 42.9 ± 5.8 | 43.0 | 59.3 |
| LrPPG | 45.3 ± 3.7 | 45.1 ± 12.0 | 45.3 | 56.2 |
| CFrPPG | 41.6 ± 3.3 | 42.1 ± 5.6 | 42.0 | 60.8 |
| TransrPPG | 32.9 ± 2.8 | 32.7 ± 6.4 | 33.1 | 72.0 |
| TSrPPG | 21.5 ± 2.6 | 22.3 ± 8.8 | 22.0 | 85.2 |
| LeTSrPPG | **15.3 ± 2.2** | **15.8 ± 6.5** | **15.7** | **91.5** |

HKBU-MARsV1+

| | 3DMAD | | | | HKBUMARsV1+ | | | |
|---|---|---|---|---|---|---|---|---|
| | 1s | 2s | 3s | 4s | 1s | 2s | 3s | 4s |
| GrPPG [14] | 65.9 | 79.1 | 84.6 | 87.7 | 72.0 | 79.2 | 80.3 | 82.3 |
| LrPPG [13] | 69.4 | 84.1 | 89.3 | 92.0 | 59.3 | 71.5 | 78.8 | 84.5 |
| PPGSec [40] | 55.7 | 68.3 | 74.5 | 80.0 | 56.2 | 74.4 | 76.7 | 79.8 |
| CFrPPG [15] | 70.8 | 88.1 | 93.1 | 94.4 | 60.8 | 78.6 | 85.8 | 89.0 |
| TransrPPG [41] | 84.5 | 87.3 | 89.4 | 88.1 | 72.0 | 76.8 | 77.6 | 79.6 |
| TSrPPG | 93.8 | 97.0 | 97.7 | 98.4 | 85.2 | 89.0 | 89.9 | 90.3 |
| LeTSrPPG | **94.4** | **97.1** | **98.0** | **98.6** | **91.5** | **96.0** | **97.3** | **98.0** |

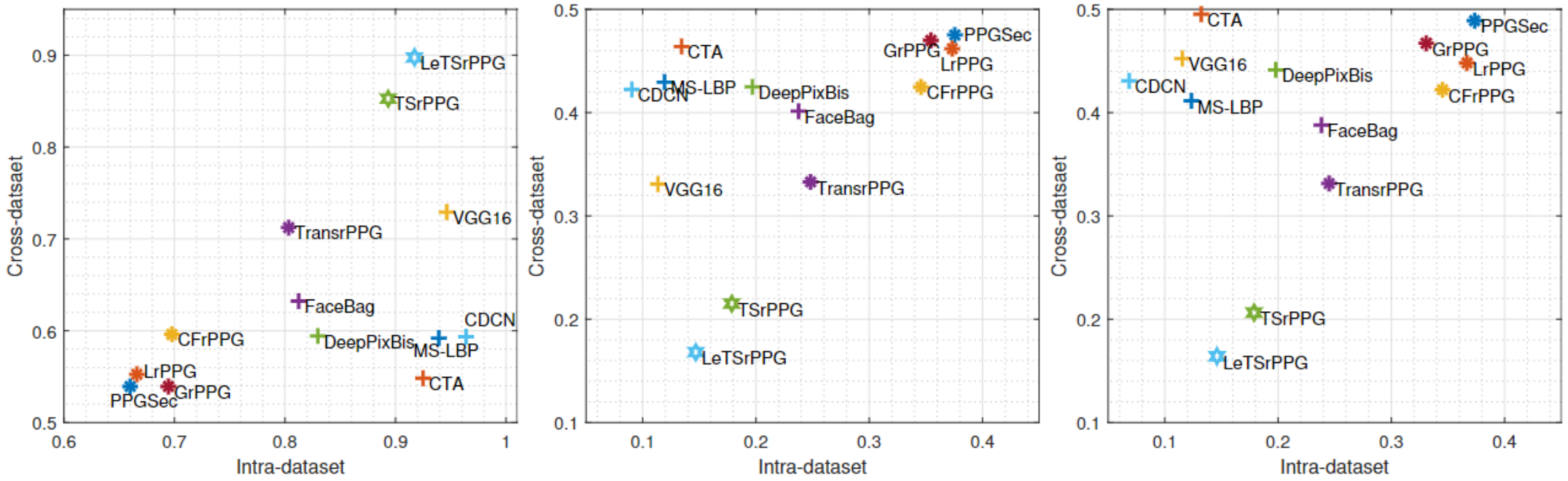
Performance (AUC) with different length of observation

| | | HTER_dvlp | HTER_test | EER | AUC |
|---|---|---|---|---|---|
| 3DMAD | TSrPPG | 13.1 ± 3.0 | 13.4 ± 11.2 | 13.3 | 93.8 |
| | LeTSrPPG-w/o$\mathcal{L}_{cnst}$&$\mathcal{L}_{decr}$ | 13.1 ± 2.5 | 13.3 ± 8.1 | 13.4 | 92.9 |
| | LeTSrPPG | **11.4 ± 2.7** | **11.8 ± 8.9** | **11.7** | **94.5** |
| MARs V1+ | TSrPPG | 21.5 ± 2.6 | 22.3 ± 8.8 | 22.0 | 85.2 |
| | LeTSrPPG-w/o$\mathcal{L}_{cnst}$&$\mathcal{L}_{decr}$ | 16.6 ± 2.0 | 17.1 ± 5.7 | 17.2 | 90.7 |
| | LeTSrPPG | **15.5 ± 2.1** | **15.8 ± 6.7** | **15.8** | **91.4** |

Ablation study of learnable rPPG extractor

# LeTSrPPG: Learnable rPPG to enhance temporal similarity of TSrPPG

- Overall comparison with state of the arts for both intra and cross dataset evaluation (1 second)
  - TSrPPG and LeTSrPPG achieve the best robustness and top-level discriminability




(a) AUCs ↑ (b) EERs ↓ (c) HTERs ↓

# Real-time Implementation of our rPPG-based Face Anti-spoofing Method

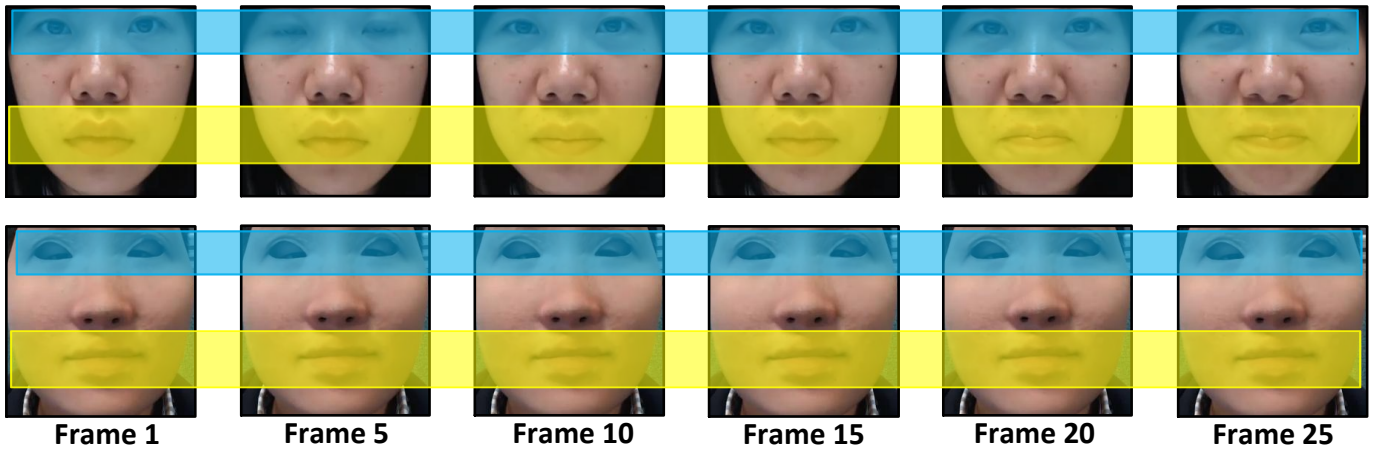
# Deep Dynamic Feature Learning Approach

**Reference:**


1. R Shao, X Y Lan and P C Yuen, “Deep Convolutional Dynamic Texture Learning with Adaptive Channel-discriminability for 3D Mask Face Anti-spoofing”, *IAPR/IEEE International Joint Conference on Biometrics (IJCB)*, Oct 2017
2. R Shao, X Y Lan and P C Yuen, “Joint Discriminative Learning of Deep Dynamic Textures for 3D Mask Face Anti-spoofing”, *IEEE Transactions on Information Security and Forensics (TIFS)*, Vol. 14, No. 4, pp. 923-938, 2019.

# Joint Discriminative Learning of Deep Dynamic Textures
## [IJCB 2017, TIFS 2019]

- **Basic Idea**



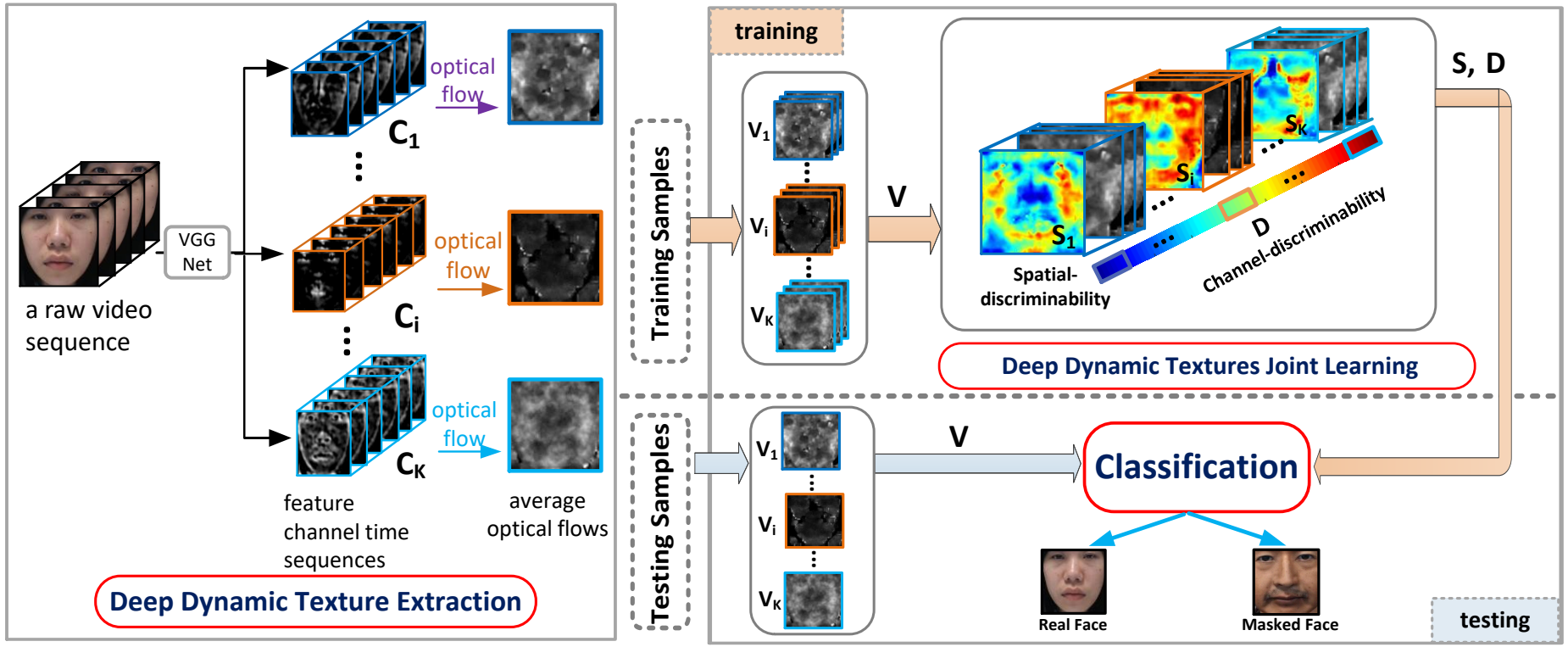

- Eye blinking
- Lip movements
- Some other facial components movements

} **Captured by dynamic textures**


1. R Shao, X Y Lan and P C Yuen, "Deep Convolutional Dynamic Texture Learning with Adaptive Channel-discriminability for 3D Mask Face Anti-spoofing", *IAPR/IEEE International Joint Conference on Biometrics (IJCB)*, Oct 2017
2. R Shao, X Y Lan and P C Yuen, "Joint Discriminative Learning of Deep Dynamic Textures for 3D Mask Face Anti-spoofing", *IEEE Transactions on Information Security and Forensics (TIFS)*, Vol. 14, No. 4, pp. 923-938, 2019.

# Joint Discriminative Learning of Deep Dynamic Textures

## [IJCB 2017, TIFS 2019]





1. R Shao, X Y Lan and P C Yuen, "Deep Convolutional Dynamic Texture Learning with Adaptive Channel-discriminability for 3D Mask Face Anti-spoofing", *IAPR/IEEE International Joint Conference on Biometrics (IJCB)*, Oct 2017
2. R Shao, X Y Lan and P C Yuen, "Joint Discriminative Learning of Deep Dynamic Textures for 3D Mask Face Anti-spoofing", *IEEE Transactions on Information Security and Forensics (TIFS)*, Vol. 14, No. 4, pp. 923-938, 2019.

# Can we develop a generalized detection method in which the attack type is not known?

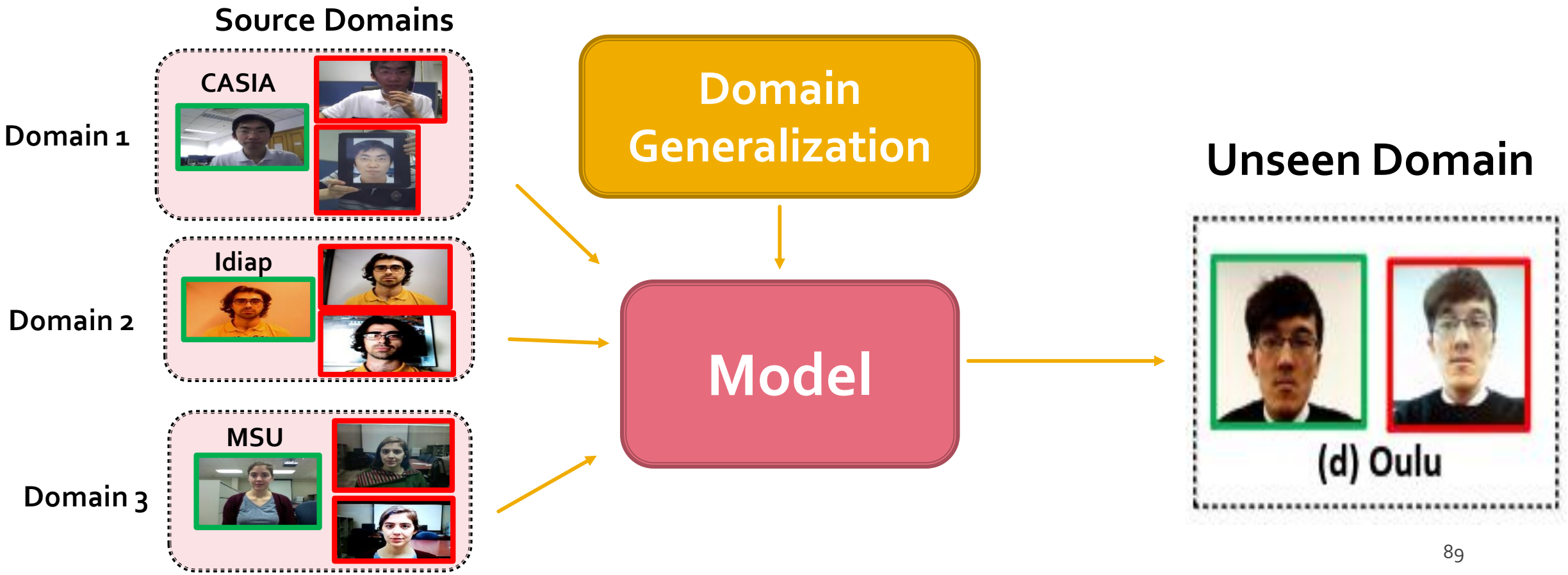
# Domain Generalization Approach

**Reference:**

1. R Shao, X Y Lan, J W Li and P C Yuen, "Multi-adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection" *Proceedings of IEEE International Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019.
2. R Shao, X Lan, P C Yuen, "Regularized Fine-grained Meta Face Anti-spoofing", *The Thirty-Fourth AAAI Conference on Artificial Intelligence (AAAI)*, 2020.

# Multi-adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection [CVPR2019]

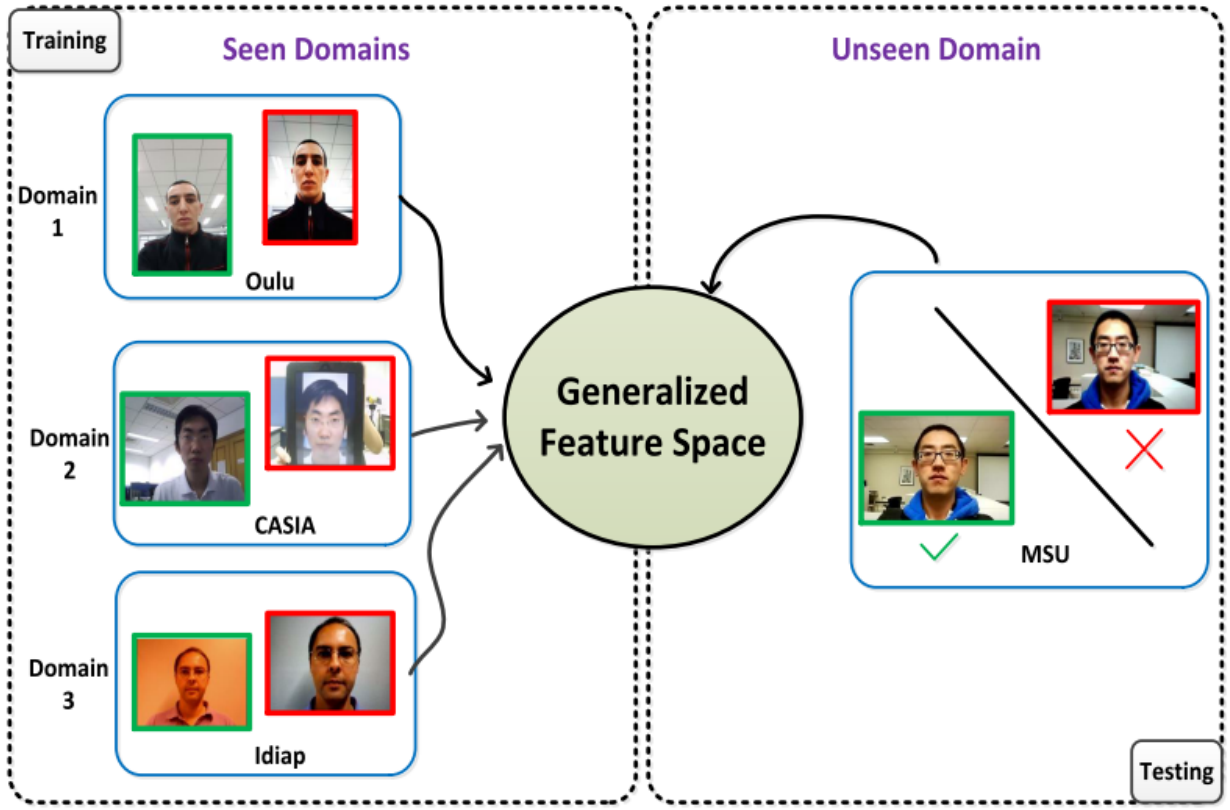
- **Domain Generalization:**






R Shao, X Y Lan, J W Li and P C Yuen, "Multi-adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection" *Proceedings of IEEE International Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019.

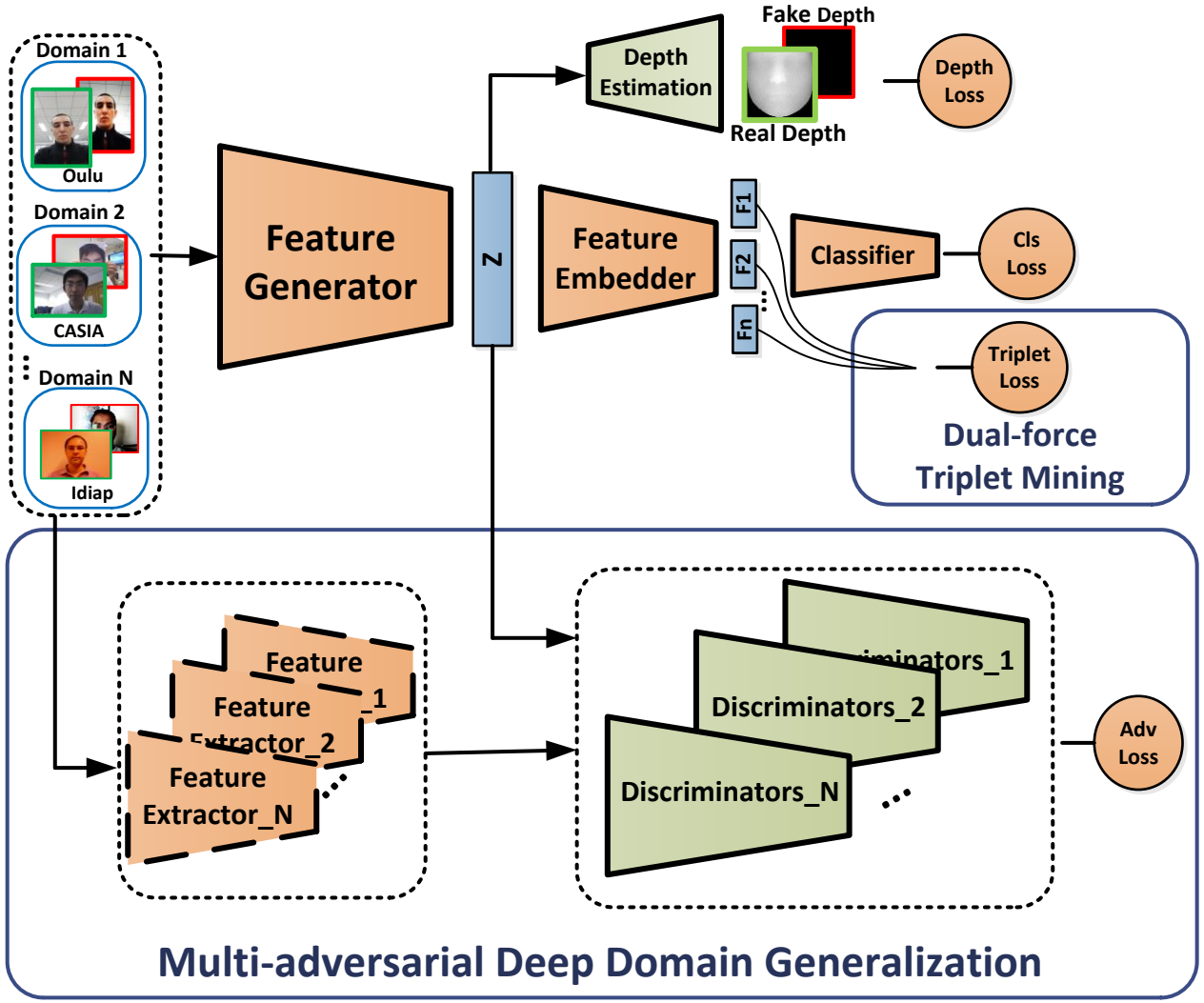
# Multi-adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection [CVPR 2019]




- The **generalized feature space** learned by the domain generalization approach should be:
  - **Shared** by multiple source domains
  - **Discriminative**

R Shao, X Y Lan, J W Li and P C Yuen, "Multi-adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection" *Proceedings of IEEE International Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019.

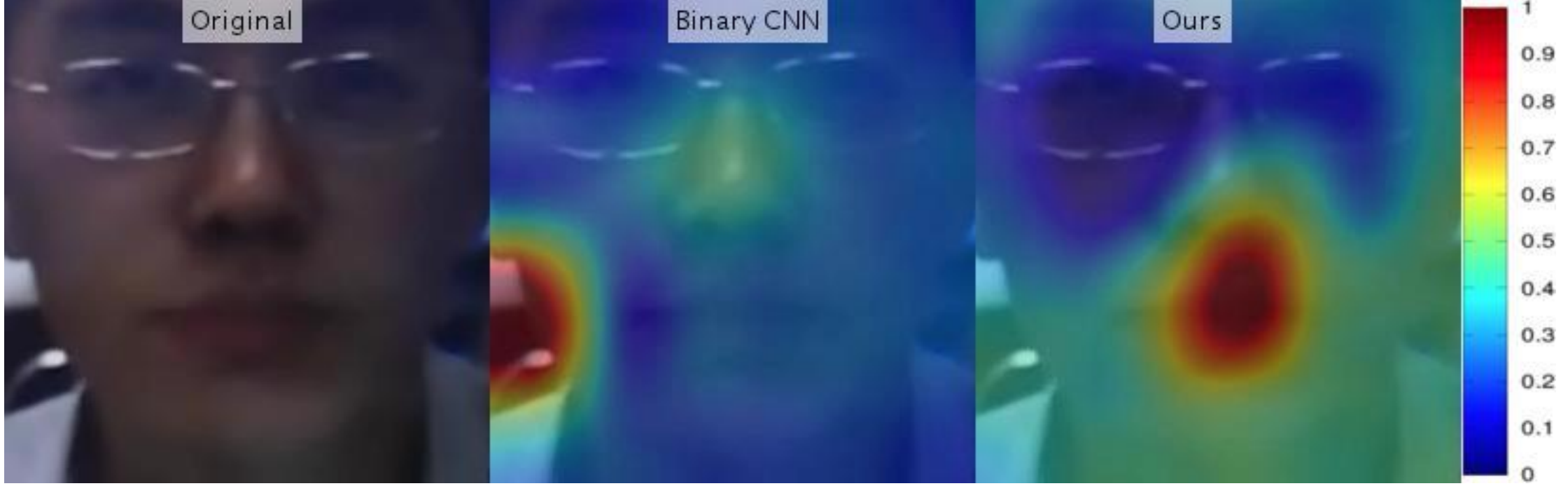
# Multi-adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection [CVPR 2019]

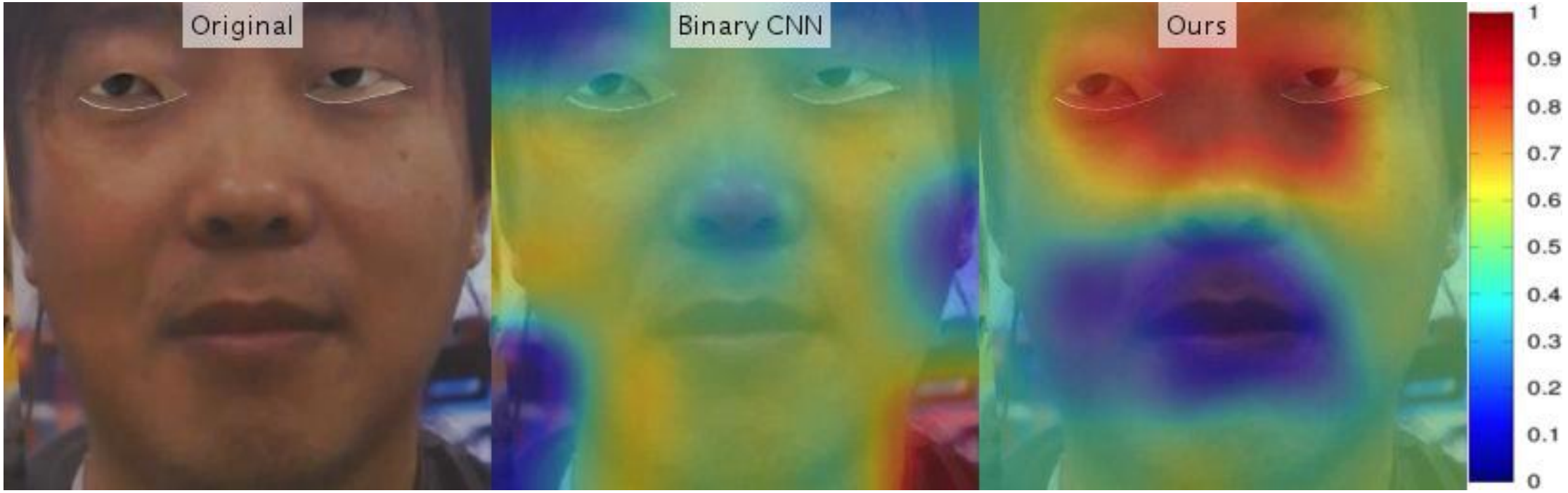



- A unified multi-adversarial discriminative deep domain generalization framework **(MADDG)**:

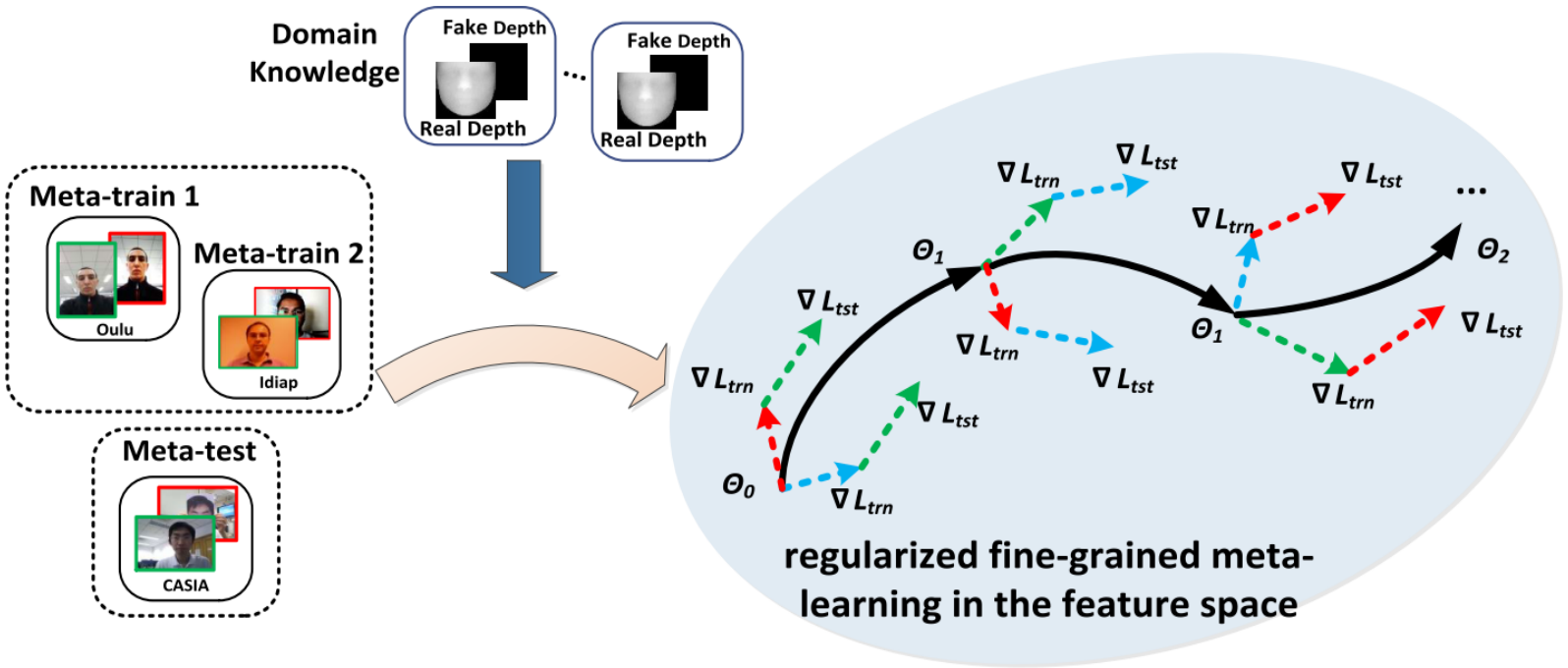
$$\min_{G,E,C,Dep} \max_{D_1,D_2,\ldots,D_N} \mathcal{L}_{MADDG} =$$

$$\mathcal{L}_{DG} + \mathcal{L}_{Trip} + \mathcal{L}_{Dep} + \mathcal{L}_{Cls}$$


Original
Binary CNN
Ours
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0


Original
Binary CNN
Ours
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0

# Regularized Fine-grained Meta Face Anti-spoofing [AAAI2020]




The first paper to address problem of domain generalization for face anti-spoofing **in a meta-learning framework**.

R Shao, XY Lan and P C Yuen, "Regularized fine-grained meta face anti-spoofing". *AAAI*, 2020.

# Regularized Fine-grained Meta Face Anti-spoofing [AAAI2020]

- Two issues if directly applying existing vanilla meta-learning for DG algorithms on face anti-spoofing：
  - First issue:

    Face anti-spoofing models only with binary class supervision discover **arbitrary** differentiation cues with **poor generalization** [1].

    Learning directions in the meta-train and meta-test steps will be **arbitrary** and **biased**, which makes it difficult for the meta-optimization step to find a generalized learning direction.

R Shao, X Y Lan and P C Yuen, "Regularized fine-grained meta face anti-spoofing". *AAAI*, 2020.

# Regularized Fine-grained Meta Face Anti-spoofing [AAAI2020]

- Two issues if directly applying existing vanilla meta-learning for DG algorithms on face anti-spoofing：
  - Second issue:

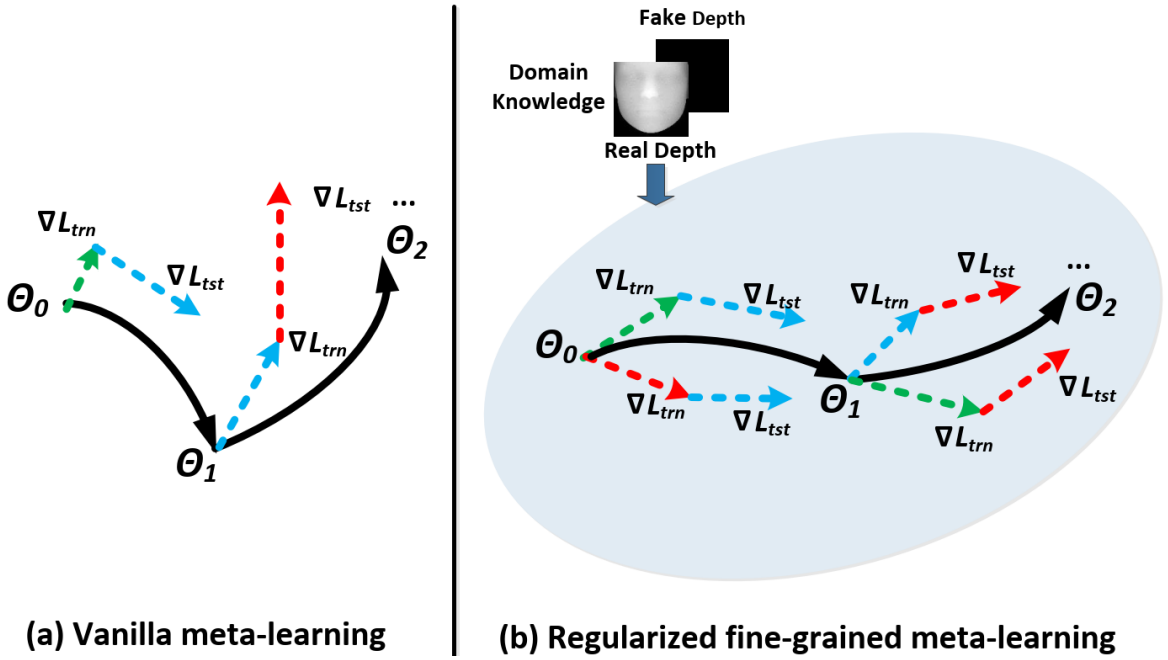
Coarsely divide multiple source domains into **two groups** to form one aggregated meta-train and one aggregated meta- test domains in each iteration of meta-learning

Only **a single** domain shift scenario is simulated in each iteration

R Shao, X Y Lan and P C Yuen, "Regularized fine-grained meta face anti-spoofing". *AAAI*, 2020.

# Regularized Fine-grained Meta Face Anti-spoofing [AAAI2020]

- Idea :




(a) Vanilla meta-learning

(b) Regularized fine-grained meta-learning

- For first issue:

Incorporate the domain knowledge of face anti-spoofing as regularization into feature learning process

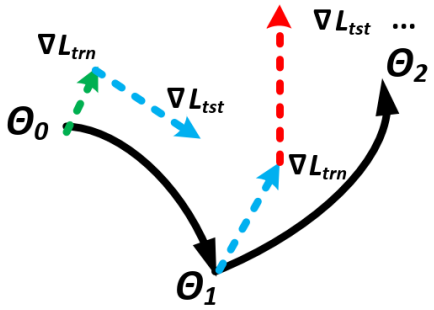
Meta-learning is conducted in the feature space regularized by the auxiliary supervision of domain knowledge.

**Regularized meta-learning** can focus on more **coordinated** and **better-generalized** learning directions in the meta-train and meta-test

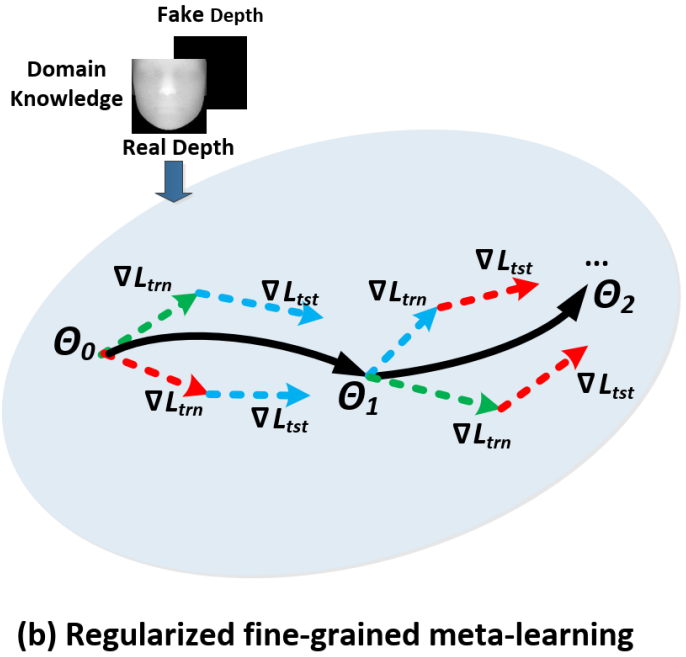
R Shao, XY Lan and P C Yuen, "Regularized fine-grained meta face anti-spoofing". *AAAI*, 2020.

# Regularized Fine-grained Meta Face Anti-spoofing [AAAI2020]

- Idea :




(a) Vanilla meta-learning




(b) Regularized fine-grained meta-learning

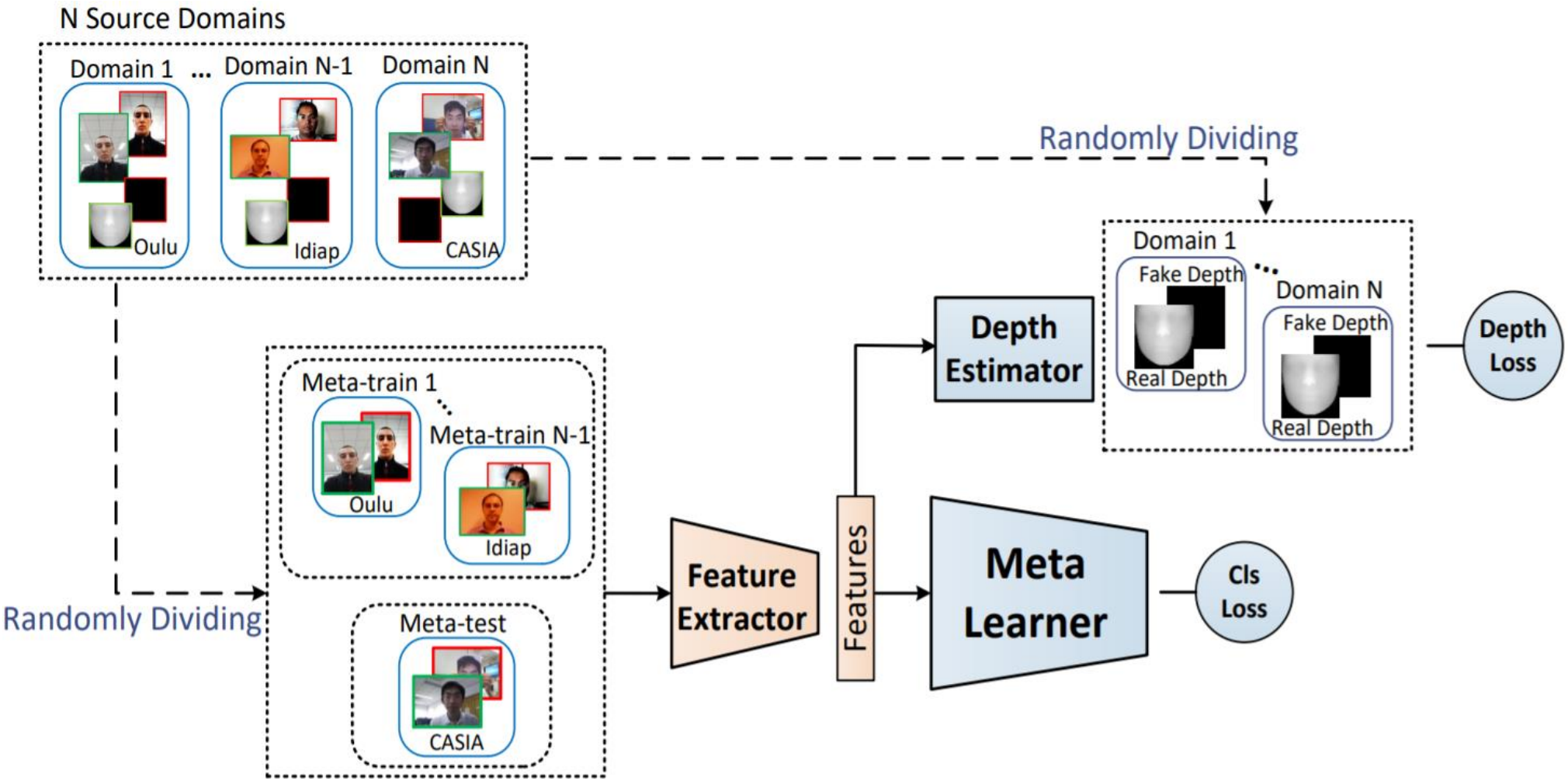
- For second issue:

**Fine-grained learning strategy** divides source domains into **multiple** meta-train and meta-test domains, and **jointly** conducts meta-learning between each pair of them in each iteration.

**A variety of domain shift scenarios** are **simultaneously** simulated and thus more abundant domain shift information can be exploited

R Shao, XY Lan and P C Yuen, "Regularized fine-grained meta face anti-spoofing". *AAAI*, 2020.

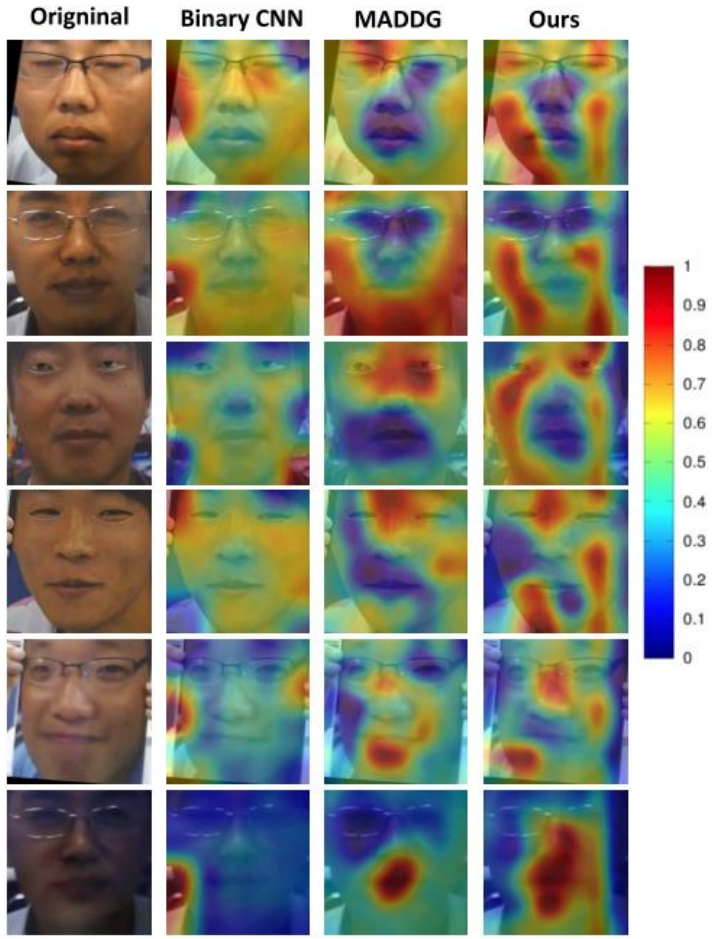
# Regularized Fine-grained Meta Face Anti-spoofing [AAAI2020]




R Shao, X Y Lan and P C Yuen, "Regularized fine-grained meta face anti-spoofing". *AAAI*, 2020.

# Experimental Results

- **Visualization** (comparison with Binary CNN and MADDG (Our CVPR19))



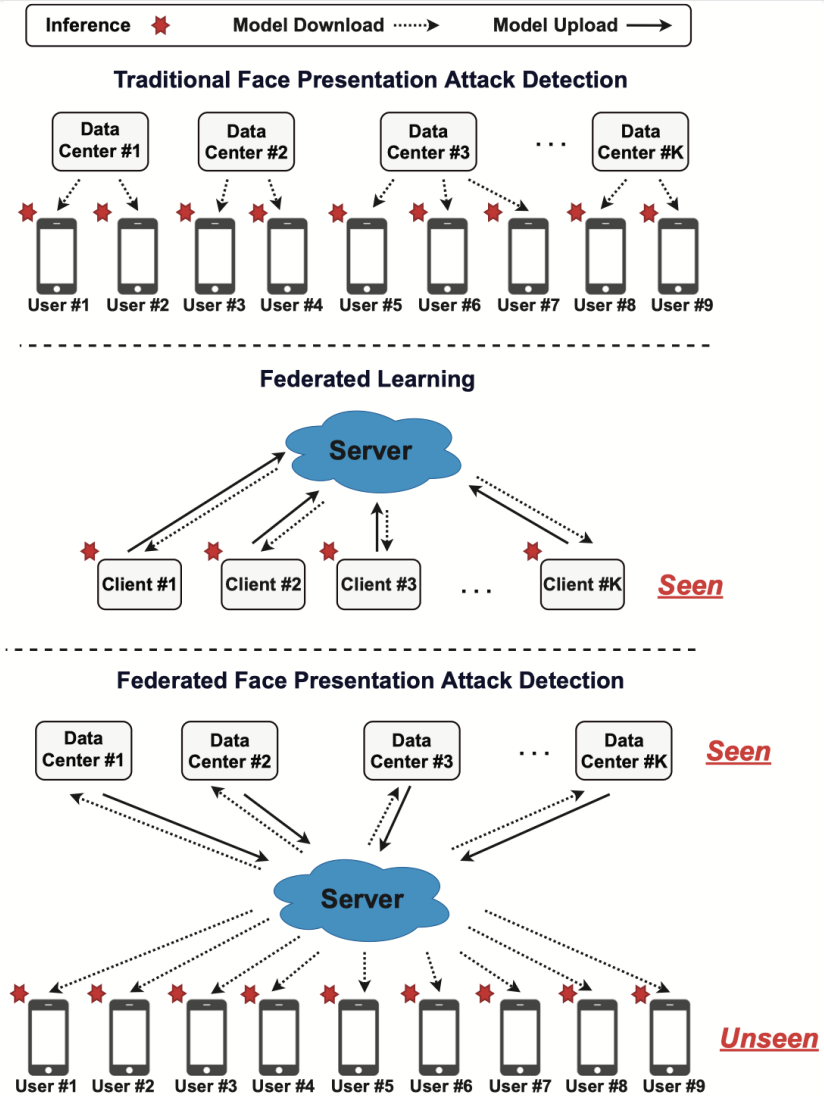

- Binary_CNN pays most attention to extracting the differentiation cues in the background (row 1-2) or on paper edges/holding fingers (row 3-5).
- Our method is more able to focus on the region of internal face for searching generalized differentiation cues.

# Federated Learning Based Approach:
## Addressing Generalization Issue for Unseen Attacks and Data Privacy


**References:**

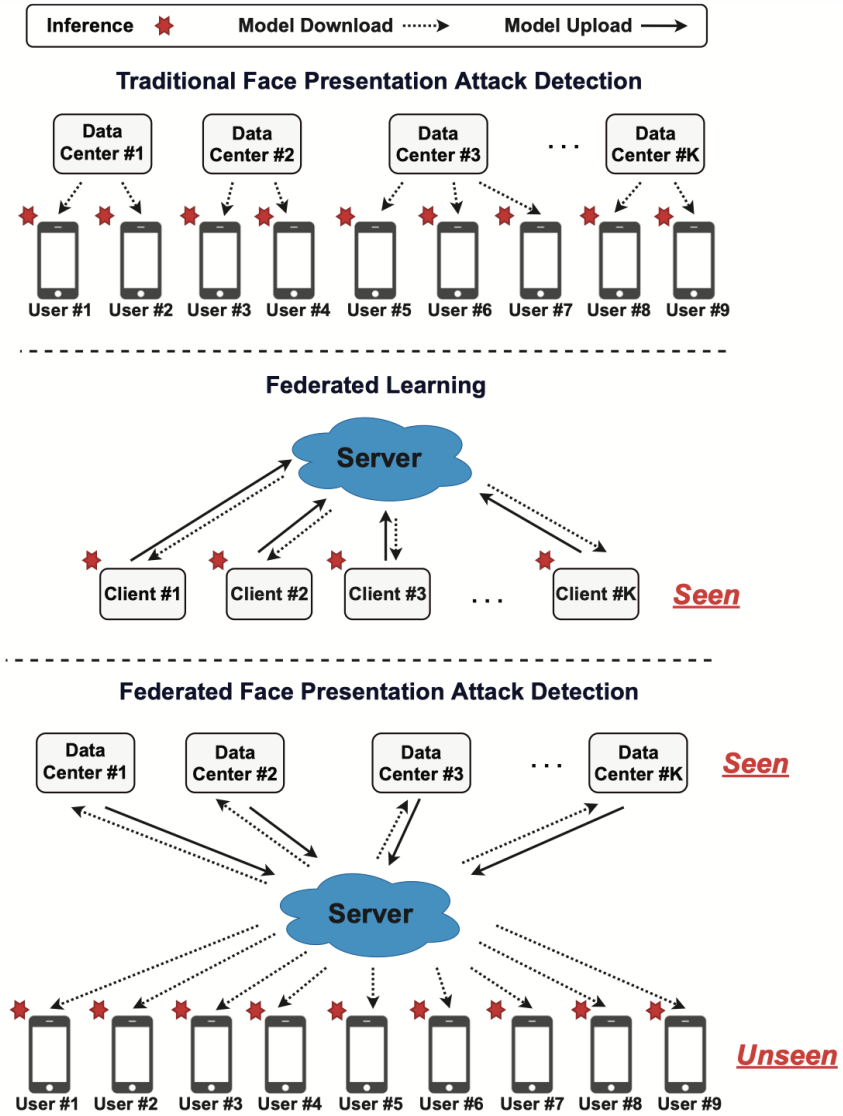
1. R Shao, B Zhang, P C Yuen, V M Patel, "Federated Test-Time Adaptive Face Presentation Attack Detection with Dual-Phase Privacy Preservation", *IEEE International Conference on Automatic Face & Gesture Recognition (FG)*, Dec 2021.
2. R Shao, P Perera, P C Yuen and V M Patel, "Federated Generalized Face Presentation Attack Detection", *IEEE Transactions on Neural Network and Learning Systems (TNNLS)*, In press, 2022.

# Background and Motivation




- **Traditional fPAD (top):**
  - Two types of stakeholders: Data center and User
  - Problem: Lacks generalization ability in each data center
  - Solution: Combine data from all centers
  - Issue: Due to data sharing agreements and privacy policies, data centers are not allowed to share data.

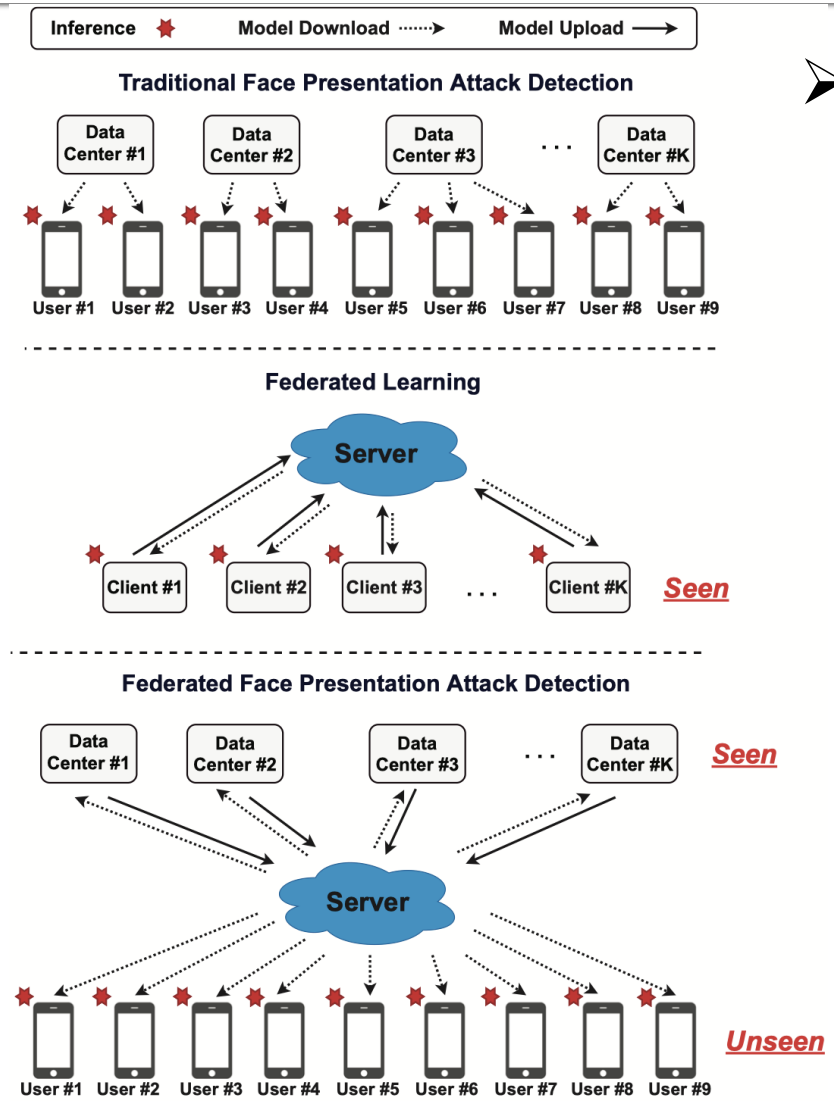
# Background and Motivation




## ➢ Federated Learning (middle):

- Nice framework for **distributed** and **privacy preserving** machine learning technique
- Data stays local client. Each client trains their own local model.
- Server aggregates local models and generates a global model without getting access to private data in data centers.
- The updated global model deploys to local client. This process is repeated until the global model is trained.
- All clients carry out inference **locally** and clients in the testing are usually **seen** during the training.

# Background and Motivation

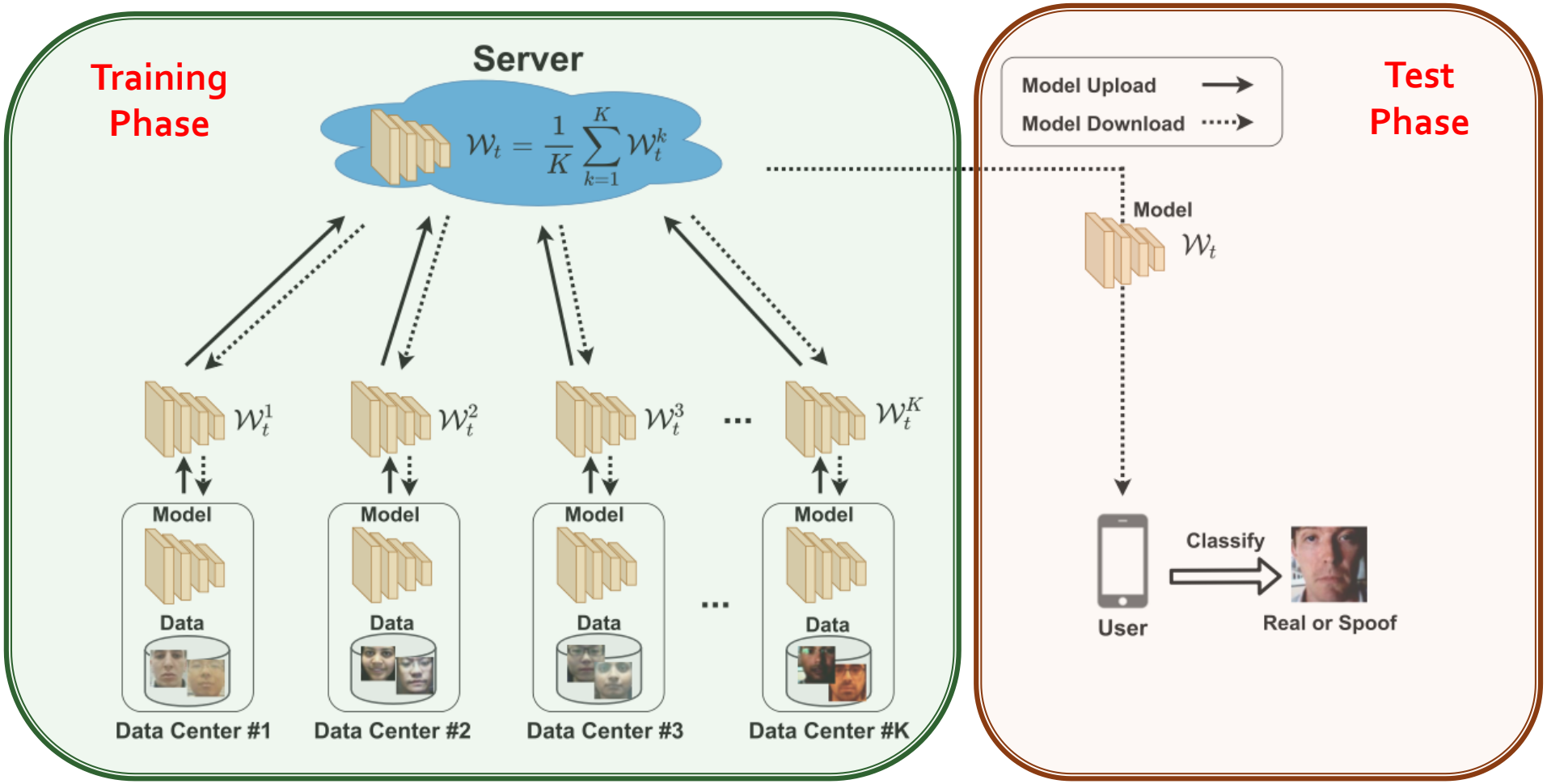



- **FedPAD - Fed**erated **P**resentation **A**ttack **D**etection (bottom)**:**

  - **Only data centers** carry out local model training and share their models with the server to aggregate the global model.
  - **Users** download the global model and **carry out inference**.
  - The downloaded model will encounter various **unseen face presentation attacks** from the users.
  - Proposed FedPAD focuses on exploring the **generalization** of FL model which aims to **generalize well to unseen attacks** from users in the testing.

# Our Work: Federated Learning + Test Time Training

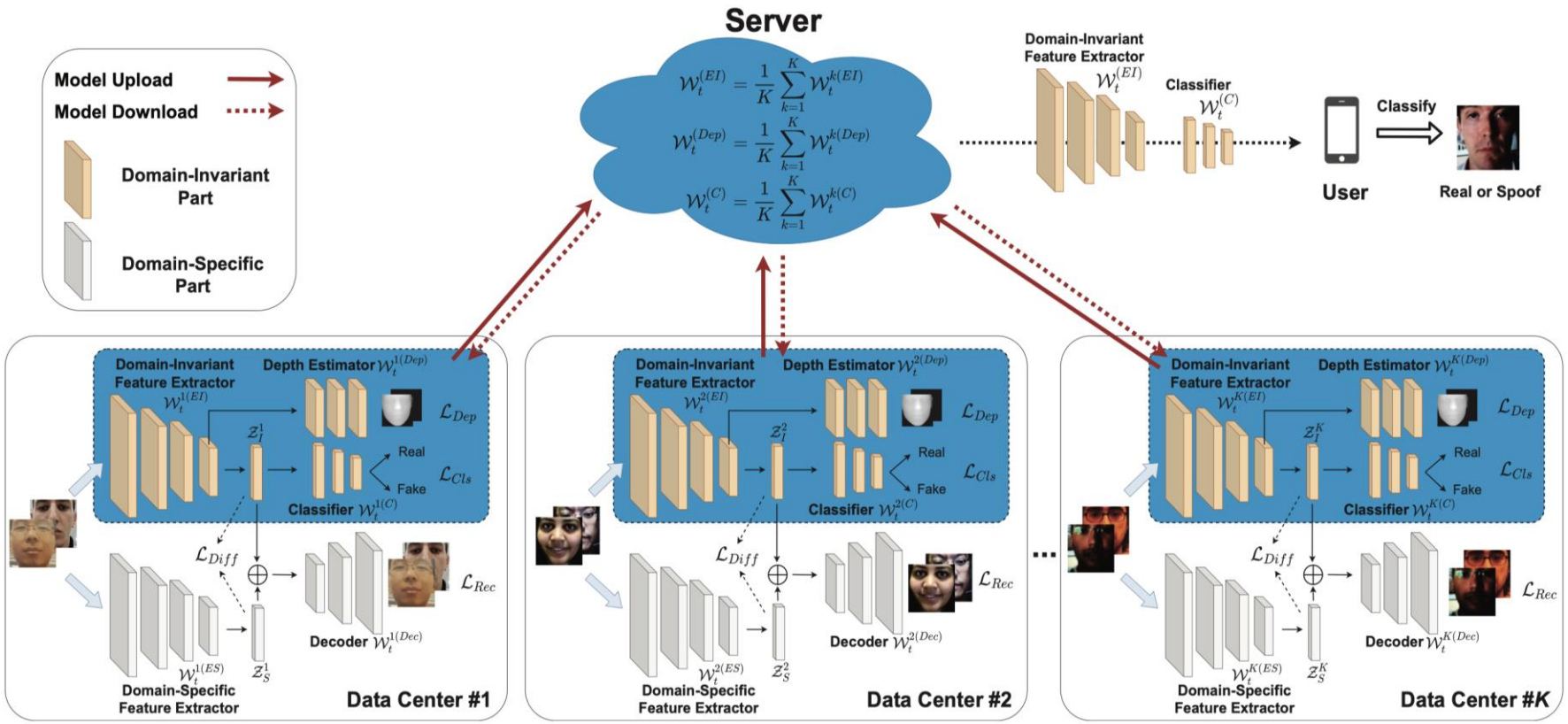
FedPAD




Federated Generalization Face PAD

Test Time Adaptation

# Federated Generalized Face Presentation Attack Detection (FedGPAD) [TNNLS2022]




Federated domain disentanglement strategy:

- Local domain disentanglement learning
- Domain-invariant model parameters communications

R Shao, P Perera, PC Yuen and V M Patel, "Federated Generalized Face Presentation Attack Detection", *IEEE Transactions on Neural Network and Learning Systems (TNNLS)*, In press, 2022.

# Local Domain Disentanglement Learning

- Feeding data into domain-invariant and domain-specific feature extractors

$$\mathcal{Z}_I^k = EI^k(x),\ \mathcal{Z}_S^k = ES^k(x)$$

- Train a domain-invariant fPAD model using the domain-invariant features by minimizing the ***cross-entropy classification loss***

$$\mathcal{L}_{Cls}(\mathcal{W}^{k(EI)}, \mathcal{W}^{k(C)}) = \sum_{(x,y)\sim\mathcal{D}^k} y \log C^k(\mathcal{Z}_I^k) + (1-y)\log(1 - C^k(\mathcal{Z}_I^k))$$

- Face depth map as the auxiliary supervision to regularize the domain-invariant feature learning => ***depth estimation loss***

$$\mathcal{L}_{Dep}(\mathcal{W}^{k(EI)}, \mathcal{W}^{k(Dep)}) = \sum_{(x,M)\sim\mathcal{D}^k} \left\| Dep^k(\mathcal{Z}_I^k) - M \right\|_2^2$$

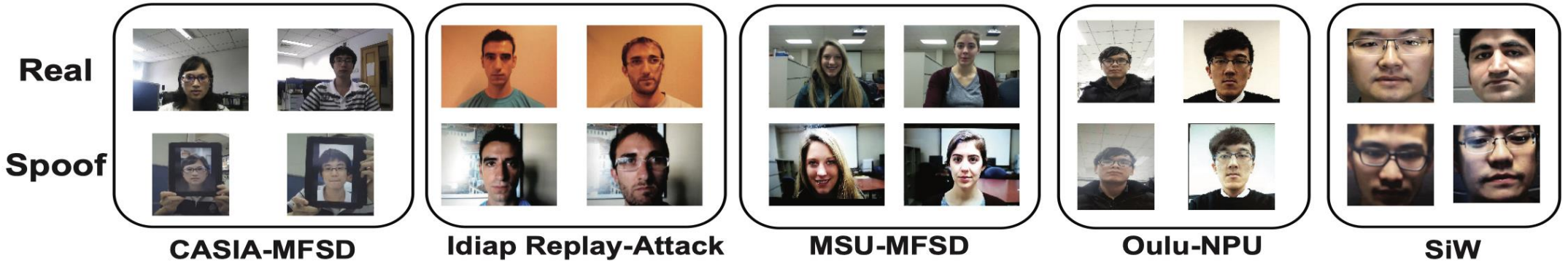
- Domain-invariant features + domain-specific features should encode the complete features from the input data, => ***reconstruction loss***

$$\mathcal{L}_{Rec}(\mathcal{W}^{k(EI)}, \mathcal{W}^{k(ES)}, \mathcal{W}^{k(Dec)}) = \sum_{x\sim\mathcal{D}^k} \left\| Dec^k(\mathcal{Z}_I^k + \mathcal{Z}_S^k) - x \right\|_2^2$$

- Domain-invariant and domain-specific encoders should encode different aspects of the input data, => ***a soft subspace orthogonal constraint via a difference loss***

$$\mathcal{L}_{Diff}(\mathcal{W}^{k(EI)}, \mathcal{W}^{k(ES)}) = \sum_{x\sim\mathcal{D}^k} \left\| (\mathcal{Z}_I^k)^T (\mathcal{Z}_S^k) \right\|_F^2$$

# Experiments: Datasets




- **Oulu-NPU (O for short)** [Zinelabinde et.al FG2017]
- **CASIA-MFSD (C for short)** [Zhang et.al ICB2012]
- **Idiap Replay-Attack (I for short) [**Chingovska et.al BIOSIG 2012]
- **MSU-MFSD (M for short)** [Wen et.al TIFS 2015]
- **SiW (S for short)** [Liu et.al CVPR 2018]

TABLE I: Comparison of five experimental datasets.

| Dataset | Extra light | Complex background | Attack type | Display devices |
|---|---|---|---|---|
| C | No | Yes | Printed photo<br>Cut photo<br>Replayed video | iPad |
| I | Yes | Yes | Printed photo<br>Display photo<br>Replayed video | iPhone 3GS<br>iPad |
| M | No | Yes | Printed photo<br>Replayed video | iPad Air<br>iPhone 5S |
| O | Yes | No | Printed photo<br>Display photo<br>Replayed video | Dell 1905FP<br>Macbook Retina |
| S | Yes | Yes | Printed photo<br>Display photo<br>Replayed video | Dell 1905FP<br>iPad Pro<br>iPhone 7<br>Galaxy S8<br>Asus MB168B |

# Experiments: Setting

- Evaluate the generalization ability of fPAD models under the FL framework.
- Leave-one-dataset-out: Choose one dataset at a time to emulate the role of users and consider all other datasets as data centers.
- Real images and spoof images of data centers are used to train a fPAD model. The trained model is tested considering the dataset that emulates the role of users.
- Evaluation metrics:
  - Half Total Error Rates (HTER)
  - Equal Error Rates (EER)
  - Area Under Curve (AUC)

# Experimental Results

TABLE III: Comparison with models trained by data from single data center and various data centers.

| Methods | Data Centers | User | HTER (%) | EER (%) | AUC (%) | Avg. HTER | Avg. EER | Avg. AUC |
|---|---|---|---|---|---|---|---|---|
| **Single** | O | M | 41.29 | 37.42 | 67.93 | 36.43 | 34.31 | 70.36 |
| | C | M | 27.09 | 24.69 | 82.91 | | | |
| | I | M | 49.05 | 20.04 | 85.89 | | | |
| | O | C | 31.33 | 34.73 | 73.19 | | | |
| | M | C | 39.80 | 40.67 | 66.58 | | | |
| | I | C | 49.25 | 47.11 | 55.41 | | | |
| | O | I | 42.21 | 43.05 | 54.16 | | | |
| | C | I | 45.99 | 48.55 | 51.24 | | | |
| | M | I | 48.50 | 33.70 | 66.29 | | | |
| | M | O | 29.80 | 24.12 | 84.86 | | | |
| | C | O | 33.97 | 21.24 | 84.33 | | | |
| | I | O | 46.95 | 35.16 | 71.58 | | | |
| **Fused** | O&C&I | M | 34.42 | 23.26 | 81.67 | 35.75 | 31.29 | 73.89 |
| | O&M&I | C | 38.32 | 38.31 | 67.93 | | | |
| | O&C&M | I | 42.21 | 41.36 | 59.72 | | | |
| | I&C&M | O | 28.04 | 22.24 | 86.24 | | | |
| **FedPAD** | O&C&I | M | 19.45 | 17.43 | 90.24 | 32.17 | 28.84 | 76.51 |
| | O&M&I | C | 42.27 | 36.95 | 70.49 | | | |
| | O&C&M | I | 32.53 | 26.54 | 73.58 | | | |
| | I&C&M | O | 34.44 | 34.45 | 71.74 | | | |
| **FedGPAD** | O&C&I | M | **12.73** | **13.36** | **91.25** | **18.59** | **17.48** | **89.25** |
| | O&M&I | C | **28.69** | **27.55** | **80.58** | | | |
| | O&C&M | I | **10.97** | **11.11** | **95.34** | | | |
| | I&C&M | O | **21.95** | **17.91** | **89.85** | | | |
| **All** | O&C&I | M | 21.80 | 17.18 | 90.96 | 27.26 | 25.09 | 80.42 |
| | O&M&I | C | 29.46 | 31.54 | 76.29 | | | |
| | O&C&M | I | 30.57 | 25.71 | 72.21 | | | |
| | I&C&M | O | 27.22 | 25.91 | 82.21 | | | |

- **Single**: fPAD model trained from a single data center and users from one of the data centers.
- **Fused**: fuse the prediction scores of the trained model from various data centers by calculating the average.
- **FedPAD**: The simple federated framework
- **FedGPAD**: Proposed method
- **All**: fPAD model is trained with data from all available data centers

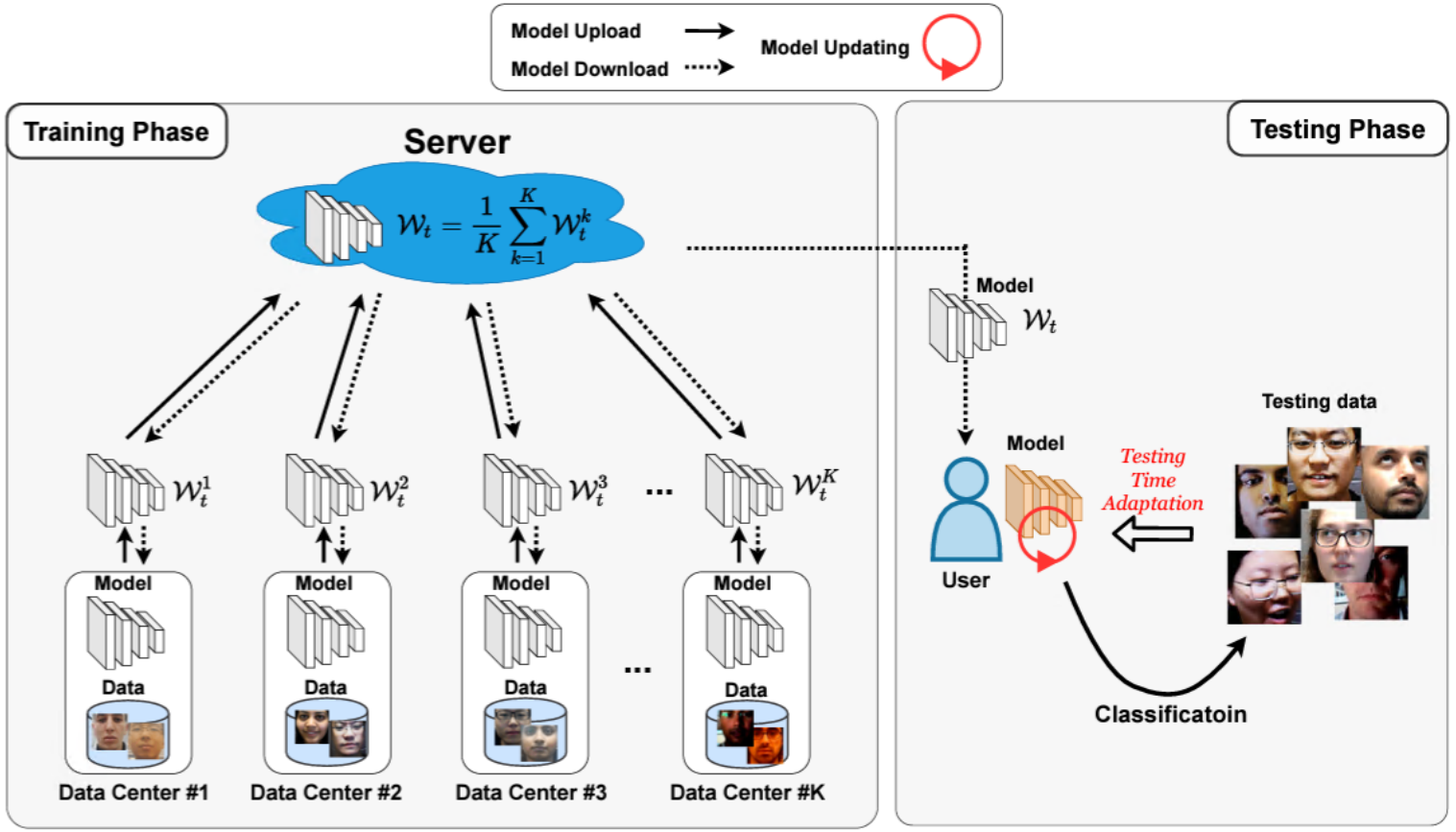
# Experimental Results

| Method | O&C&I to M | | O&M&I to C | | O&C&M to I | | I&C&M to O | | Avg. | |
|---|---|---|---|---|---|---|---|---|---|---|
| | HTER | AUC | HTER | AUC | HTER | AUC | HTER | AUC | HTER | AUC |
| | **Without Considering Privacy Issue** | | | | | | | | | |
| MS_LBP [21] | 29.76 | 78.50 | 54.28 | 44.98 | 50.30 | 51.64 | 50.29 | 49.31 | 46.15 | 56.10 |
| Binary CNN [45] | 29.25 | 82.87 | 34.88 | 71.94 | 34.47 | 65.88 | 29.61 | 77.54 | 32.05 | 74.55 |
| IDA [43] | 66.67 | 27.86 | 55.17 | 39.05 | 28.35 | 78.25 | 54.20 | 44.59 | 51.09 | 47.43 |
| Color Texture [3] | 28.09 | 78.47 | 30.58 | 76.89 | 40.40 | 62.78 | 63.59 | 32.71 | 40.66 | 62.71 |
| LBPTOP [8] | 36.90 | 70.80 | 42.60 | 61.05 | 49.45 | 49.54 | 53.15 | 44.09 | 45.52 | 56.37 |
| Auxiliary(Depth Only) [16] | 22.72 | 85.88 | 33.52 | 73.15 | 29.14 | 71.69 | 30.17 | 77.61 | 28.88 | 77.08 |
| MMD-AAE [12] | 27.08 | 83.19 | 44.59 | 58.29 | 31.58 | 75.18 | 40.98 | 63.08 | 36.05 | 69.93 |
| MADDG [29] | 17.69 | 88.06 | 24.50 | 84.51 | 22.19 | 84.99 | 27.98 | 80.02 | 23.09 | 84.39 |
| DR-MD-Net [40] | 17.02 | 90.10 | 19.68 | 87.43 | 20.87 | 86.72 | 25.02 | 81.47 | 20.64 | 86.43 |
| RFMeta [33] | 13.89 | 93.98 | 20.27 | 88.16 | 17.30 | 90.48 | 16.45 | 91.16 | 16.97 | 90.94 |
| NAS-Baseline [48] | 14.63 | 94.26 | 17.24 | 87.48 | 19.73 | 88.52 | 19.81 | 86.80 | 17.85 | 89.26 |
| NAS-Baseline w/ D-Meta [48] | 11.62 | 95.85 | 16.96 | 89.73 | 16.82 | 91.68 | 18.64 | 88.45 | 16.01 | 91.42 |
| NAS-FAS [48] | 19.53 | 88.63 | 16.54 | 90.18 | 14.51 | 93.84 | 13.80 | 93.43 | 16.09 | 91.52 |
| NAS-FAS w/ D-Meta [48] | 16.85 | 90.42 | 15.21 | 92.64 | 11.63 | 96.98 | 13.16 | 94.18 | 14.21 | 93.55 |
| DC-CDN [47] | 25.51 | 81.80 | 15.00 | 92.80 | 15.88 | 91.61 | 18.82 | 89.86 | 18.80 | 89.01 |
| | **Considering Privacy Issue** | | | | | | | | | |
| **FedPAD** | 19.45 | 90.24 | 42.27 | 70.49 | 32.53 | 73.58 | 34.44 | 71.74 | 32.17 | 76.51 |
| **FedGPAD** | 12.73 | 91.25 | 28.69 | 80.58 | 10.97 | 95.34 | 21.95 | 89.85 | 18.59 | 89.25 |

**Comparison with the state-of-the-art face presentation attack detection methods**

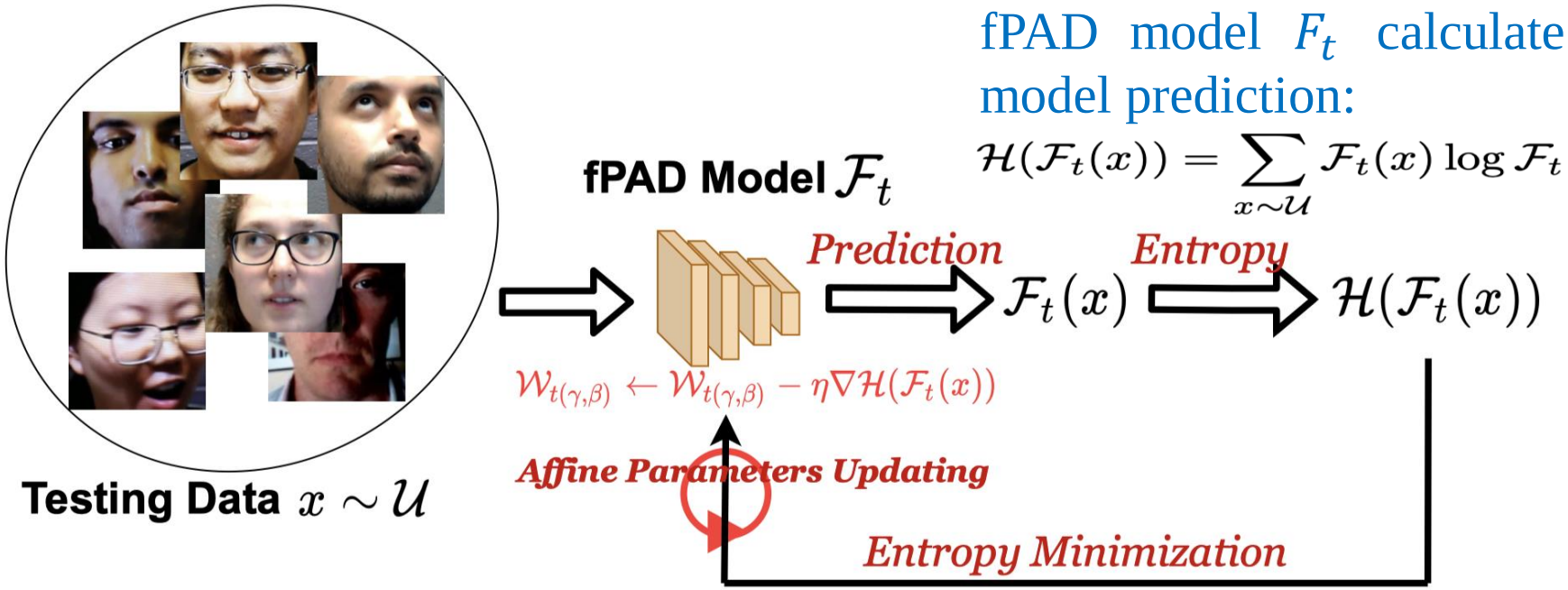
# Federated Face PAD with Test-Time Adaptation [FG2021]

- FedGPAD performs very well. Generalization is very hard to unseen test data
- Conduct test-time adaptation




R Shao, B Zhang, P C Yuen, V M Patel, "Federated Test-Time Adaptive Face Presentation Attack Detection with Dual-Phase Privacy Preservation", *IEEE International Conference on Automatic Face & Gesture Recognition (FG)*, Dec 2021.

# Test-Time Adaptation




Given the testing data presented to user $U$, and the fPAD model $F_t$ calculate the **entropy** of fPAD model prediction:

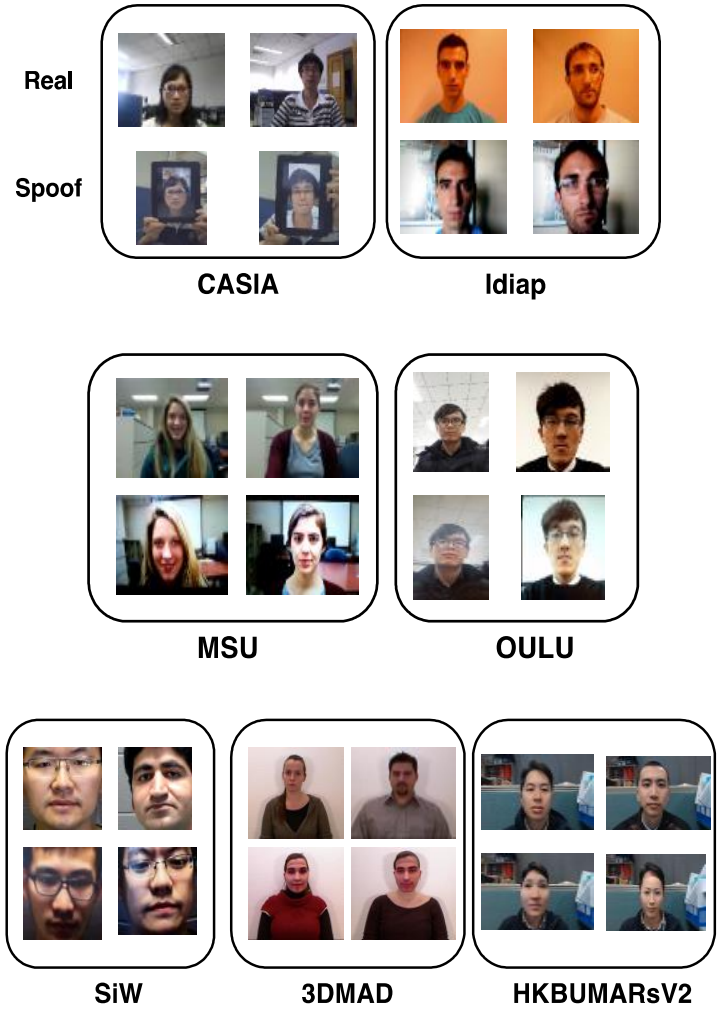
$$\mathcal{H}(\mathcal{F}_t(x)) = \sum_{x\sim\mathcal{U}} \mathcal{F}_t(x)\log\mathcal{F}_t(x) + (1-\mathcal{F}_t(x))\log(1-\mathcal{F}_t(x))$$

After test time adaptation, updated fPAD model for the final real/fake classification.

To reduce the probability of overfitting during test-time adaptation, minimize the above entropy with respect to **affine transformation parameters of all batch normalization layers** in the fPAD model

# Experimental Results

| Methods | Data Centers | User | HTER (%) | EER (%) | AUC (%) | Avg. HTER | Avg. EER | Avg. AUC |
|---|---|---|---|---|---|---|---|---|
| Single | O | M | 41.29 | 37.42 | 67.93 | 41.61 | 36.66 | 67.07 |
| | C | M | 27.09 | 24.69 | 82.91 | | | |
| | I | M | 49.05 | 20.04 | 85.89 | | | |
| | O | C | 31.33 | 34.73 | 73.19 | | | |
| | M | C | 39.80 | 40.67 | 66.58 | | | |
| | I | C | 49.25 | 47.11 | 55.41 | | | |
| | O | I | 42.21 | 43.05 | 54.16 | | | |
| | C | I | 45.99 | 48.55 | 51.24 | | | |
| | M | I | 48.50 | 33.70 | 66.29 | | | |
| | M | O | 29.80 | 24.12 | 84.86 | | | |
| | C | O | 33.97 | 21.24 | 84.33 | | | |
| | I | O | 46.95 | 35.16 | 71.58 | | | |
| Fused | O&C&I | M | 34.42 | 23.26 | 81.67 | 35.75 | 31.29 | 73.89 |
| | O&M&I | C | 38.32 | 38.31 | 67.93 | | | |
| | O&C&M | I | 42.21 | 41.36 | 59.72 | | | |
| | I&C&M | O | 28.04 | 22.24 | 86.24 | | | |
| FedPAD | O&C&I | M | 19.45 | 17.43 | 90.24 | 32.17 | 28.84 | 76.51 |
| | O&M&I | C | 42.27 | 36.95 | 70.49 | | | |
| | O&C&M | I | 32.53 | 26.54 | 73.58 | | | |
| | I&C&M | O | 34.44 | 34.45 | 71.74 | | | |
| All | O&C&I | M | 21.80 | 17.18 | 90.96 | 27.26 | 25.09 | 80.42 |
| | O&M&I | C | 29.46 | 31.54 | 76.29 | | | |
| | O&C&M | I | 30.57 | 25.71 | 72.21 | | | |
| | I&C&M | O | 27.22 | 25.91 | 82.21 | | | |
| Ours | O&C&I | M | 14.70 | 16.64 | 90.57 | 23.18 | 23.88 | 83.40 |
| | O&M&I | C | 26.33 | 29.75 | 77.77 | | | |
| | O&C&M | I | 28.61 | 26.04 | 82.07 | | | |
| | I&C&M | O | 23.09 | 23.09 | 83.21 | | | |



# Experimental Results

- **Generalization ability to 3D mask attacks**

IMPACT OF ADDING DATA CENTERS WITH DIVERSE ATTACKS

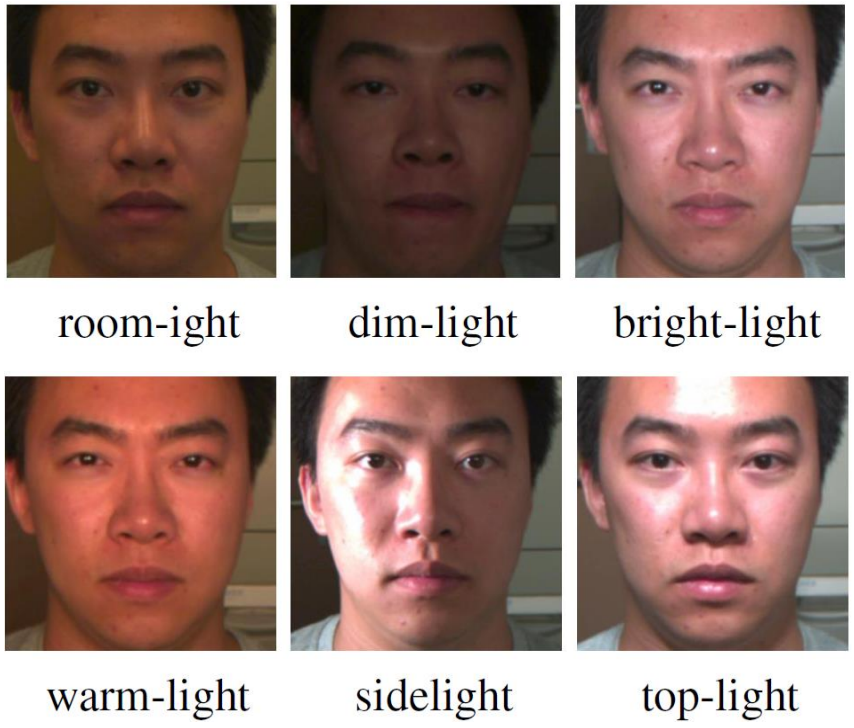
| Methods | Data Centers | User | HTER | AUC |
|---|---|---|---|---|
| **FedPAD** | O&C&M (2D) | 3 (3D) | 27.21 | 76.05 |
| | O&C&M (2D) &H (3D) | | 34.70 | **92.35** |
| **Ours** | O&C&M (2D) &H (3D) | | **16.97** | 90.25 |

- **FedPAD**: Increasing one data center with 3D mask attacks (**H**: HKBUMARsV2) within the FL framework can improve the generalization ability of fPAD model to the novel 3D mask attacks (**3**: 3DMAD).

- **Ours**: after adapted with novel 3D mask attack data **by test-time adaptation** during testing, fPAD model trained with FL in the training phase is more able to generalize well to the novel types of 3D mask attacks

# Our dataset: HKBU-MARs

- http://rds.comp.hkbu.edu.hk/mars




# Conclusions

- PAD is an important and un-solved issue in biometric systems
- Rapid progress in the past 5 years, still a lot issues needed to be solved
- Face PAD has high academic and commercial values
- Very good topic for PhDs or early stage researchers

# Special Thanks …

Collaborators:
- ✓ Prof. GY Zhao, The University of Oulu
- ✓ Prof. Vishal Patel, Johns Hopkins University

Current/Former PhD Students:
- ✓ Dr. Siqi Liu
- ✓ Dr. Rui Shao
- ✓ Ms. Bochao Zhang

Funding:
- ✓ Hong Kong Research Grant Council

# Hong Kong PhD Fellowship Scheme (HKPFS)

- Outstanding applicants (top students from top universities) will be recommended for nomination to the **HKPFS** scheme

| HKPFS Applicants | Scholarship |
|---|---|
| Nominated by HKBU and awarded by HK Government | HKD 1,920,000 during 4-year PhD study (Plus up to HKD 220,000 tuition fee waive & overseas conference/attachment support)* |
| Nominated by HKBU but not awarded by HK Government | HKD 960,000 during 4-year PhD study (Plus up to HKD 55,000 overseas conference/attachment support)* |

** Visit [http://www.comp.hkbu.edu.hk/hkpfs](http://www.comp.hkbu.edu.hk/hkpfs) for a detailed breakdown*

# Thank you!

# References


1. N. Erdogmus and S. Marcel, "Spoofing face recognition with 3d masks", *TIFS*, 2014
2. J. Maatta, A. Hadid, and M. Pietikainen. "Face spoofing detection from single images using micro-texture analysis", *IJCB*, 2011.
3. D. Wen, H. Han, and A. K. Jain, "Face spoof detection with image distortion analysis", *TIFS*, 2015.
4. G. Pan, L. Sun, Z. Wu, and S. Lao. "Eyeblink-based antispoofing in face recognition from a generic webcamera", *ICCV*, 2007.
5. T. de Freitas Pereira, J. Komulainen, A. Anjos, J. M. De Martino, A. Hadid, M. Pietikainen, and S. Marcel, "Face liveness detection using dynamic texture.", *EURASIP JIVP*, 2014.
6. X. Li, J. Komulainen, G. Zhao, P. C. Yuen, and M. Pietikainen, "Generalized face anti-spoofing by detecting pulse from face videos", *ICPR*, 2016.
7. S. Liu, P C. Yuen, S. Zhang, and G. Zhao, "3D Mask Face Anti-spoofing with Remote Photoplethysmography" , *ECCV*, 2016.
8. S. Liu, B. Yang, P C. Yuen, G. Zhao, "A 3D Mask Face Anti-spoofing Database with RealWorld Variations" , *CVPRW*, 2016.
9. S Liu, X Y Lan and P C Yuen, "Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection", *ECCV*, 2018
10. R Shao, X Y Lan and P C Yuen, "Deep Convolutional Dynamic Texture Learning with Adaptive Channel-discriminability for 3D Mask Face Anti-spoofing", *IJCB*, Oct 2017
11. R Shao, X Y Lan and P C Yuen, "Joint Discriminative Learning of Deep Dynamic Textures for 3D Mask Face Anti-spoofing", *TIFS*, 2019.

# References


12. R Shao, X Y Lan, J W Li and P C Yuen, "Multi-adversarial discriminative deep domain generalisation for face presentation attack detection", *CVPR*, 2019.
13. R Shao, X Y Lan and P C Yuen, "Regularized fine-grained meta face anti-spoofing". *AAAI*, 2020.
14. S. Liu, X Y Lan and P C Yuen, "Temporal similarity analysis of remote photoplethysmography for fast 3d mask face presentation attack detection", *WACV*, 2020.
15. Y Liu, A Jourabloo and X Liu, "Learning deep models for face anti-spoofing: binary or auxiliary supervision", *CVPR*, 2018.
16. Y. Liu, A. Jourabloo, and X. Liu. "Face De-Spoofing: Anti-Spoofing via Noise Modeling", *ECCV* 2018
17. Y Liu, J Stehouwer, A Jourabloo and et al., "Deep tree learning for zero-shot face anti-spoofing." *CVPR*, 2019.
18. C Lin, Z Liao and et al. "Live Face Verification with Multiple Instantialized Local Homographic Parameterization", *IJCAI* 2018
19. H Li, W Li, H Cao and et al. "Unsupervised domain adaptation for face anti-spoofing", *TIFS* 2018
20. X Yang, W Luo, L Bao and et al. "Face Anti-Spoofing: Model Matters, So Does Data", *CVPR* 2019
21. X Qu, J Dong and S Niu. "shallowCNN-LE: A shallow CNN with Laplacian Embedding for face anti-spoofing", *FG* 2019
22. S Zhang, X Wang, A Liu and et al. "A Dataset and Benchmark for Large-scale Multi-modal Face Anti-spoofing", *CVPR* 2019
23. I Manjani, S Tariyal, M Vatsa and et al. "Detecting silicone mask-based presentation attack via deep dictionary learning", *TIFS* 2017

# References


24. S Bhattacharjee, A Mohammadi and S Marcel. "Spoofing deep face recognition with custom silicone masks", *BTAS* 2018
25. O Nikisins, A George and S Marcel. "Domain Adaptation in Multi-Channel Autoencoder based Features for Robust Face Anti-Spoofing", *ICB* 2019
26. H Li, P He, S Wang et al, "Learning generalized deep feature representation for face anti-spoofing." *TIFS*, 2018.
27. F Xiong and W AbdAlmageed, "Unknown presentation attack detection with face RGB images." *BTAS*, 2018.
28. D Pérez-Cabo, D Jiménez-Cabello, A Costa-Pazo and et al. "Deep anomaly detection for generalized face anti-spoofing." *CVPR Workshops*, 2019.
29. A Liu, J Wan, S Escalera et al., "Multi-modal face anti-spoofing attack detection challenge at CVPR2019", *CVPR Workshops*, 2019.
30. Yu, Z., Wan, J., Qin, Y., Li, X., Li, S.Z. and Zhao, G. NAS-FAS: Static-Dynamic Central Difference Network Search for Face Anti-Spoofing. *TPAMI,* 2020.
31. Cai, R., Li, H., Wang, S., Chen, C. and Kot, A.C. DRL-FAS: A Novel Framework Based on Deep Reinforcement Learning for Face Anti-Spoofing. *TIFS*, 2020.
32. Li, H., Wang, S., He, P. and Rocha, A. Face anti-spoofing with deep neural network distillation. *JSTSP*, 2020.

# References


33. Zhang, K.Y., Yao, T., Zhang, J., Tai, Y., Ding, S., Li, J., Huang, F., Song, H. and Ma, L. Face Anti-Spoofing via Disentangled Representation Learning. ECCV, 2020.
34. Liu, Y., Stehouwer, J. and Liu, X. On Disentangling Spoof Trace for Generic Face Anti-Spoofing. ECCV, 2020.
35. Zhang, Y., Yin, Z., Li, Y., Yin, G., Yan, J., Shao, J. and Liu, Z. CelebA-Spoof: Large-Scale Face Anti-Spoofing Dataset with Rich Annotations. ECCV, 2020.
36. Yu, Z., Zhao, C., Wang, Z., Qin, Y., Su, Z., Li, X., Zhou, F. and Zhao, G. Searching central difference convolutional networks for face anti-spoofing. CVPR, 2020.
37. Jia, Y., Zhang, J., Shan, S. and Chen, X. Single-Side Domain Generalization for Face Anti-Spoofing. CVPR, 2020.
38. Wang, G., Han, H., Shan, S. and Chen, X. Cross-domain Face Presentation Attack Detection via Multi-domain Disentangled Representation Learning. CVPR, 2020.
39. Wang, Z., Yu, Z., Zhao, C., Zhu, X., Qin, Y., Zhou, Q., Zhou, F. and Lei, Z. Deep spatial gradient and temporal depth learning for face anti-spoofing. CVPR, 2020.
40. Sun, W., Song, Y., Chen, C., Huang, J. and Kot, A.C. Face spoofing detection based on local ternary label supervision in fully convolutional networks. TIFS, 2020.
41. Yu, Z., Li, X., Niu, X., Shi, J. and Zhao, G. Face anti-spoofing with human material perception. ECCV, 2020.
42. Liu S, Lan X and Yuen PC, "Multi-Channel Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection", TIFS, In press, 2021.

# References


43. X. Guo, et al. "Multi-domain Learning for Updating Face Anti-spoofing Models", *ECCV* 2022
44. H.P. Huang, et al. "Adaptive Transformers for Robust Few-shot Cross-domain Face Anti-spoofing", *ECCV* 2022
45. Q. Zhou et al. "Generative Domain Adaptation for Face Anti-Spoofing", *ECCV* 2022.
46. C.Y. Wang et al, "PatchNet: A Simple Face Anti-Spoofing Framework via Fine-Grained Patch Recognition", *CVPR* 2022.
47. S. Liu et al, "Feature Generation and Hypothesis Verification for Reliable Face Anti-spoofing", *AAAI* 2022.
48. S Q Liu, X Y Lan and P C Yuen, "Learning Temporal Similarity of Remote Photoplethysmography for Fast 3D Mask Face Presentation Attack Detection", *IEEE Transactions on Information Forensics and Security (TIFS),* In press, 2022.
49. R Shao, P Perera, P C Yuen and V M Patel, "Federated Generalized Face Presentation Attack Detection", *IEEE Transactions on Neural Network and Learning Systems (TNNLS)*, In press, 2022.