Face Presentation Attack Detection

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

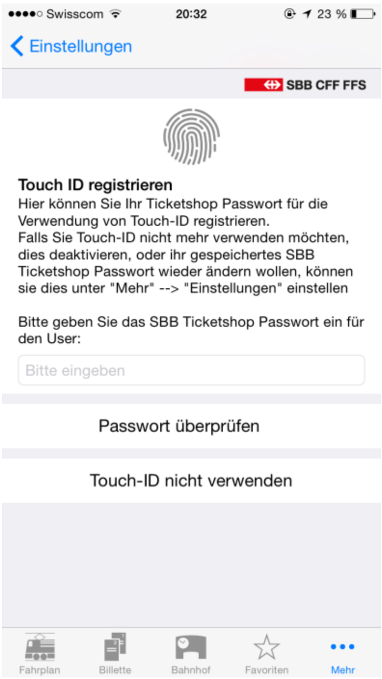
Background and Motivations

- Deployed biometrics practical applications

Border Control

Door Access Control

Touch ID (iPhone)



SBB for buying ticket

Background and Motivations

- Face Recognition Technology

MIT Technology Review:
10 breakthrough technologies 2017

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

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?

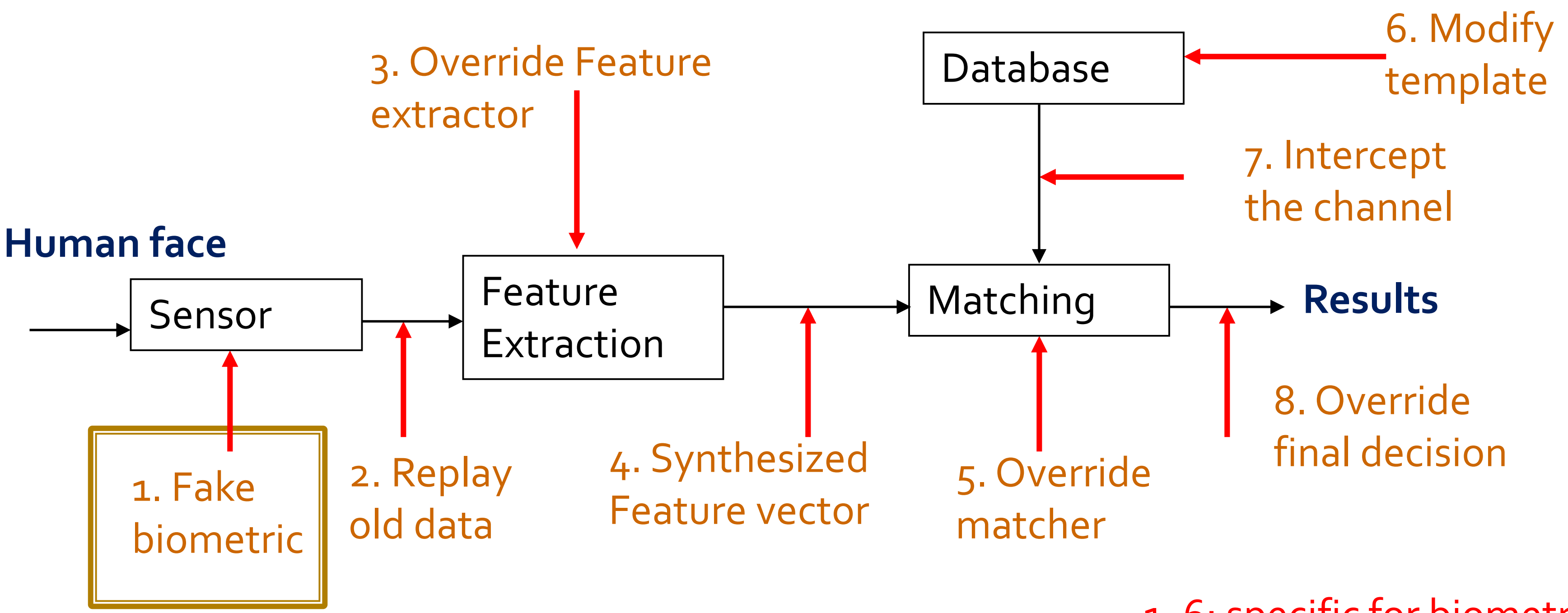
Student spoof the face recognition system of auto courier cabinet with a photo print

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



1, 6: specific for biometric systems

Background and Motivations

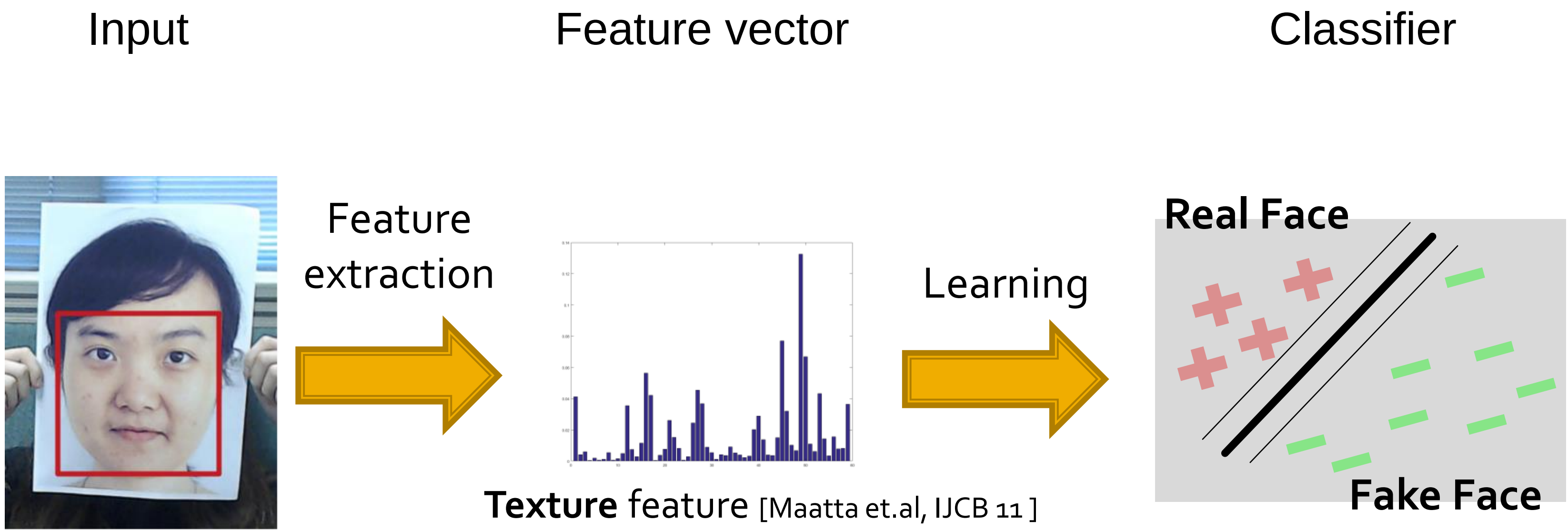
- Face Presentation Attack Detection (PAD)
  - Face information can be easily acquired (facebook, twitter) and abused
  - 3 popular attacks: Print (image), Replay (video), and 3D mask

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

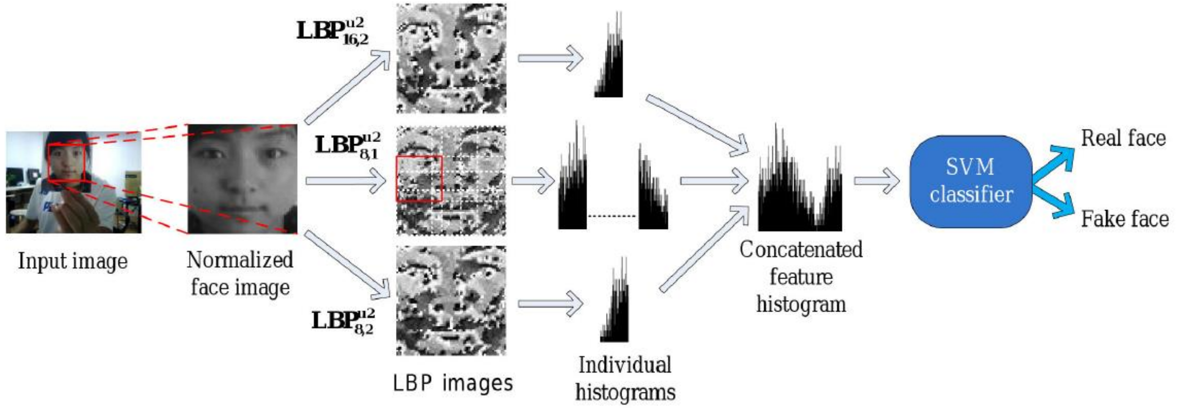
- Anti-spoofing approach: Appearance-based
  - Spoof media (print and screen) and genuine face has different appearance

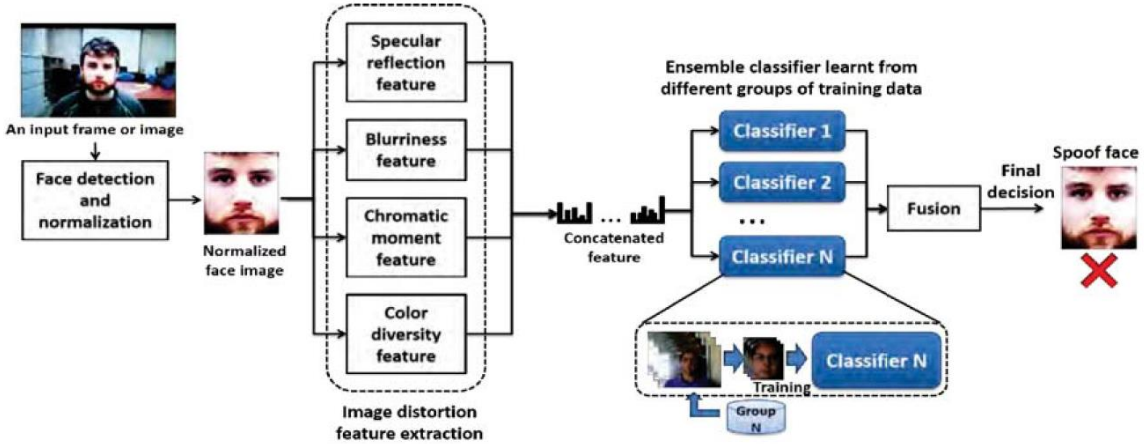


Texture feature [Maatta et.al, IJCB 11]
Image Distortion Analysis [Di et.al, TIFS 15]
...

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

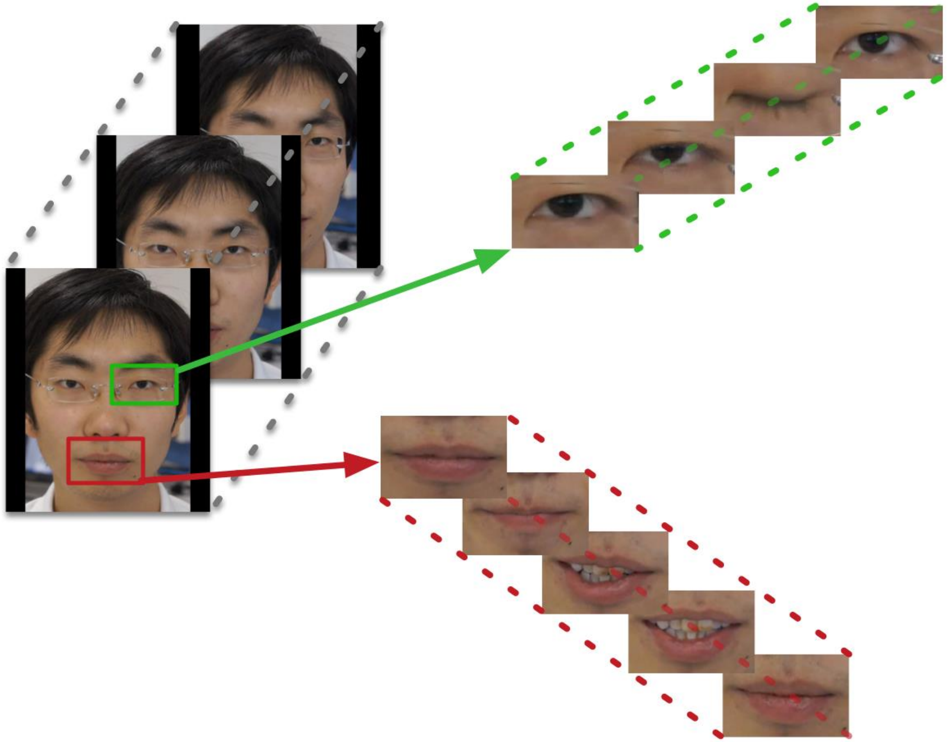


Image and Video Face PAD

- 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)

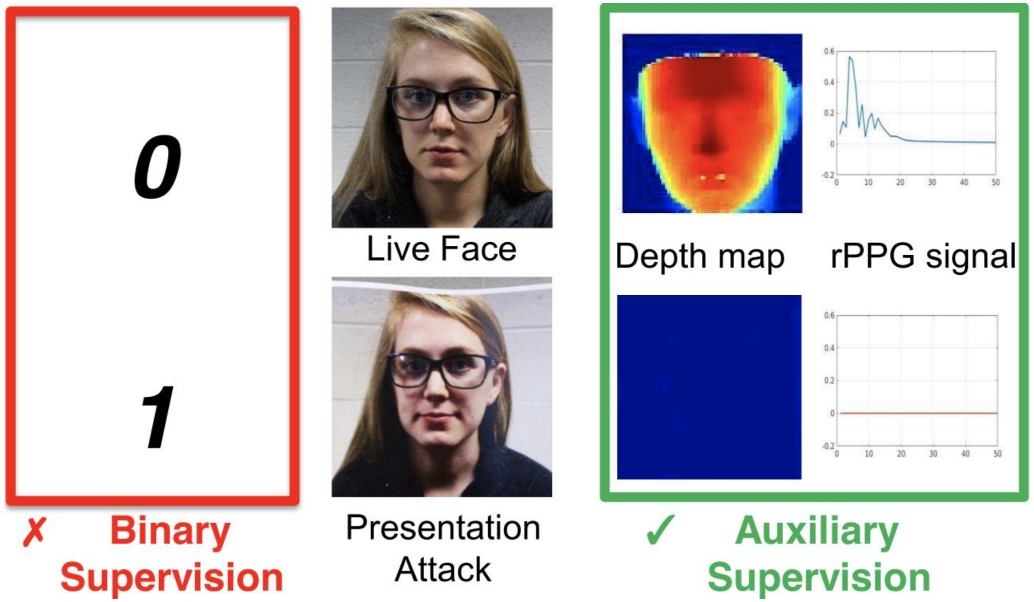
Datasets	Year	Modality	#Subjects	#Data	#Sensor	Lighting Cond.	Spoof type
SiW-M [13]	2019	RGB	493	1,628 (V)	4	Room Light	Print + Replay +3D Mask + Make Up
WMCA [14]	2019	RGB/NIR/Depth/LWIR	72	1679 (V)	4	Room Light/LED-lamps/Day Light	3D Mask made of (Plastic, Silicone, Paper)
CelebA-Spoof [15]	2020	RGB	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

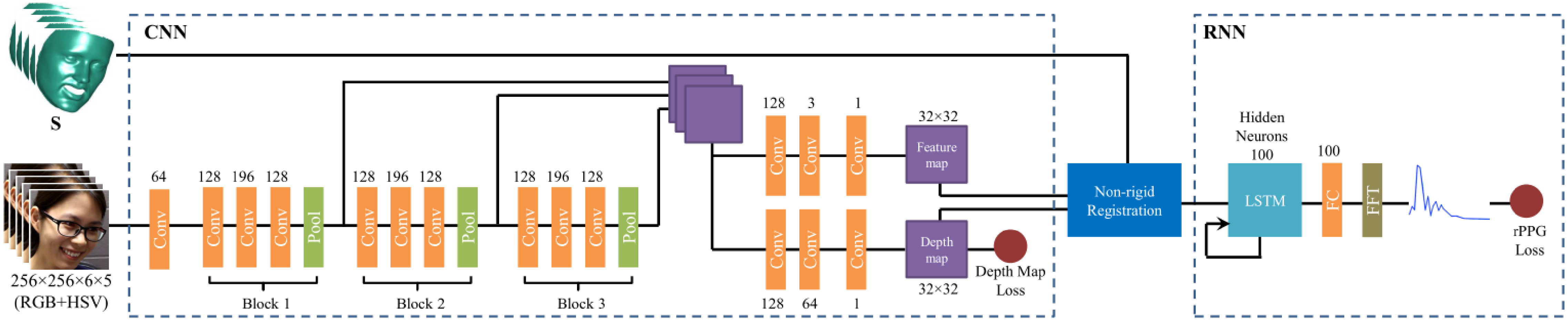
- Pixel-wise supervision with auxiliary tasks
  - Auxiliary tasks encourage the network to learn “fine-grained” details.



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

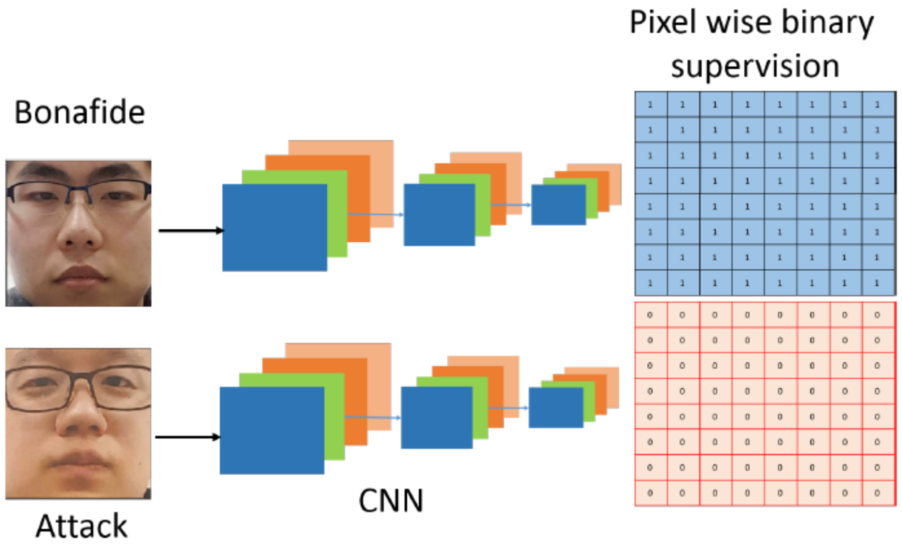
- Pixel-wise supervision with auxiliary tasks
  - CNN: Learn different face depth maps at **pixel-wise** level
  - RNN: Learn different rPPG signals at **sequence-wise** level



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

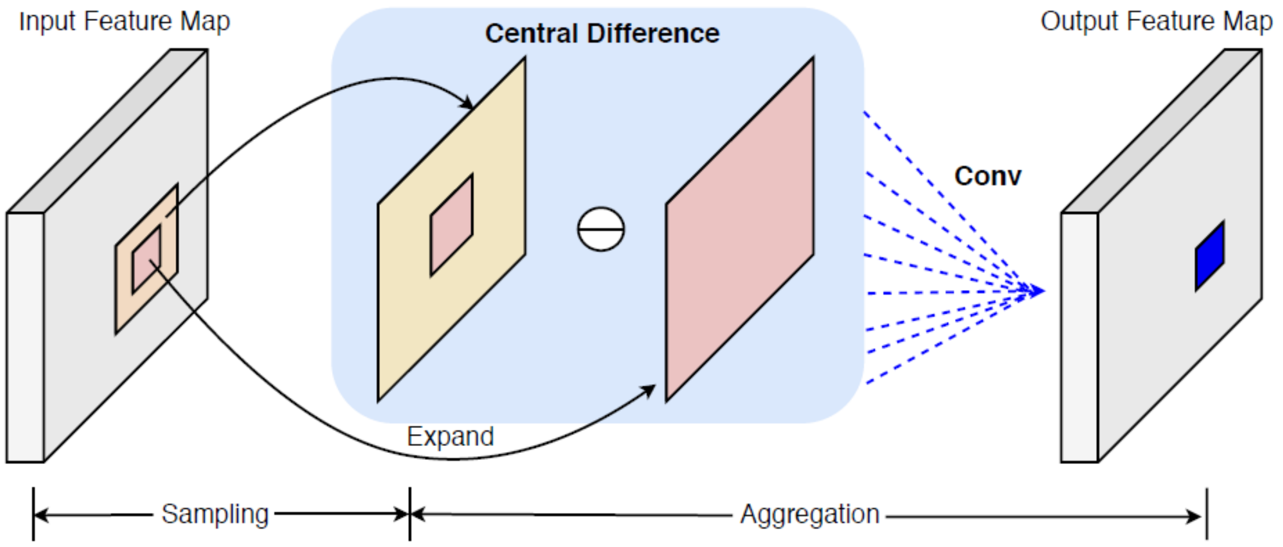
- Pixel-wise supervision with auxiliary tasks
  - Use binary map with classification loss instead of depth map with regression loss



A. George and S. Marcel. Deep Pixel-wise Binary Supervision for Face Presentation Attack Detection, ICB 2019

Image and Video Face PAD

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



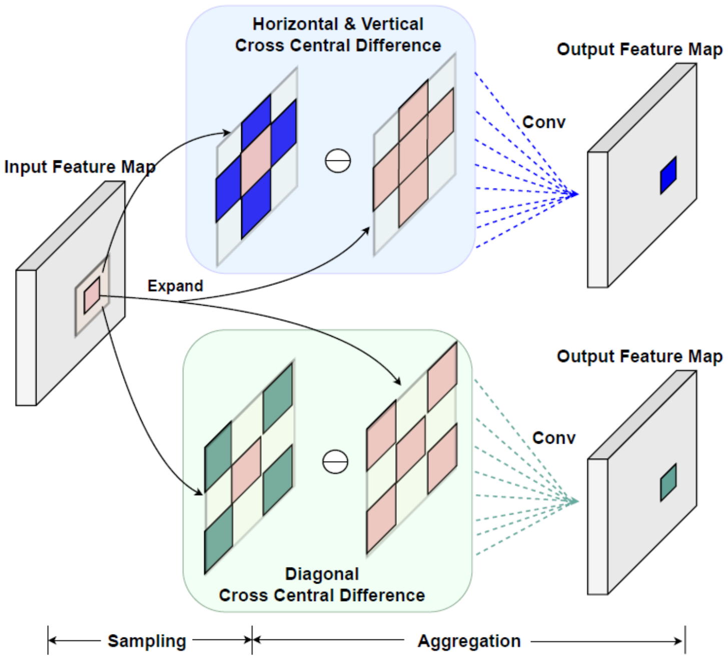
$$y(p_0) = \underbrace{\theta \cdot \sum_{p_n \in \mathcal{R}} w(p_n) \cdot (x(p_0 + p_n) - x(p_0))}_{\text{central difference convolution}} + \underbrace{(1-\theta) \cdot \sum_{p_n \in \mathcal{R}} w(p_n) \cdot x(p_0 + p_n)}_{\text{vanilla convolution}},$$

Z. Yu, et al. Searching central difference convolutional networks for face anti-spoofing. CVPR 2020.

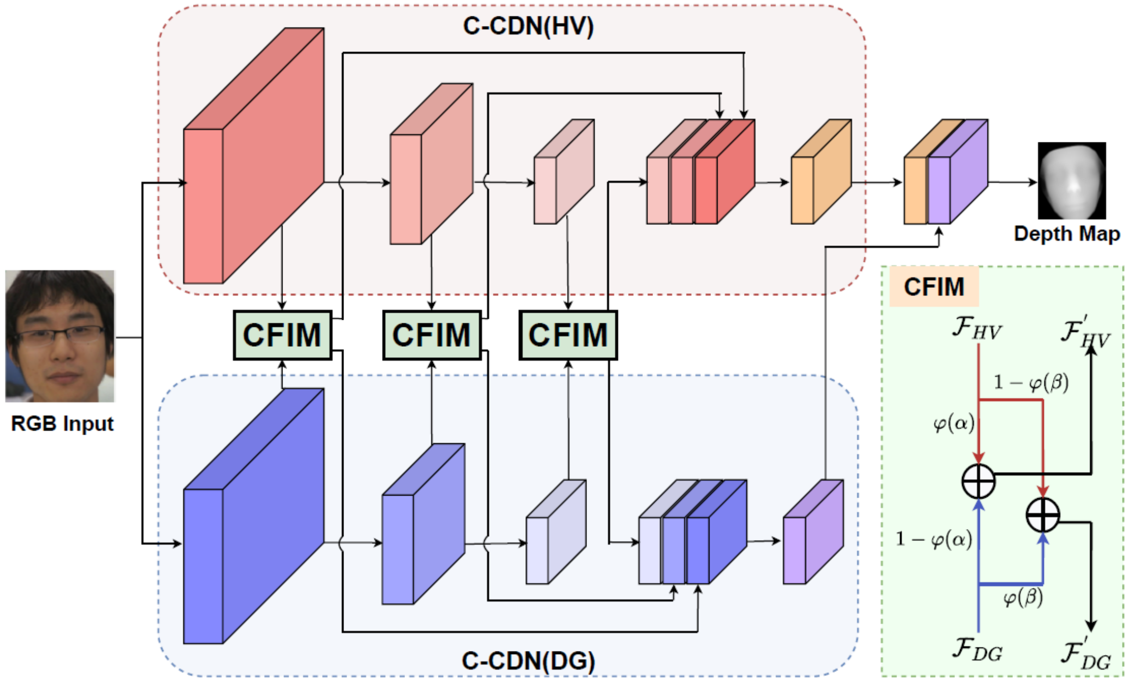
Z. Yu, et al. Nas-fas: Static-dynamic central difference network search for face antispoofing. TPAMI 2020

Image and Video Face PAD

- Dual-Cross Central Difference
  - Less computational cost but better performance
    - Dual-stream features from different views



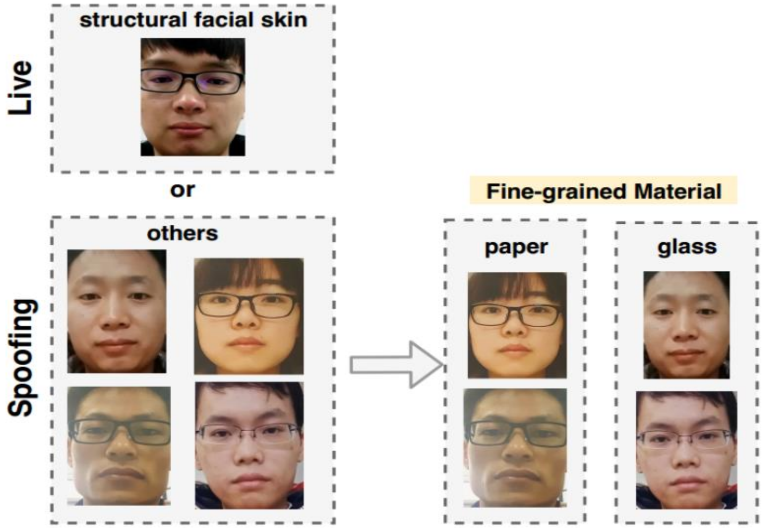
  - Cross Feature Interaction Module (CFIM):
    - Mutual relation mining and local detailed representation enhancement

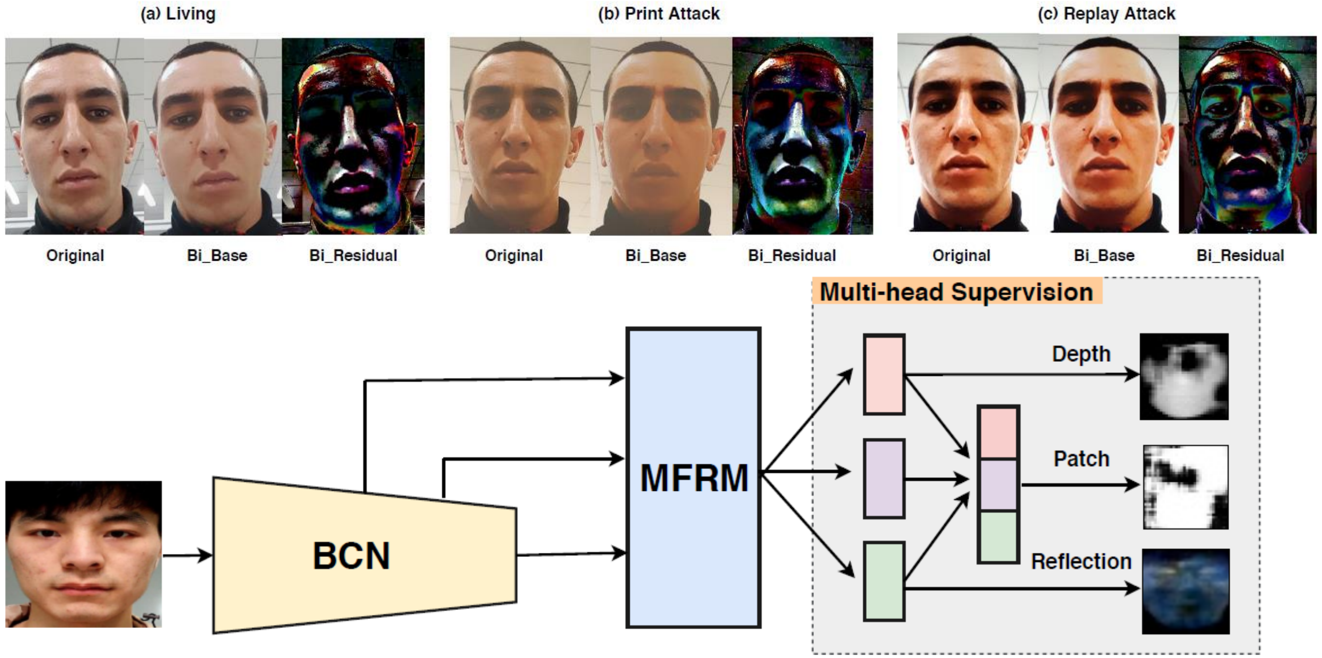


Yu, Zitong, et al. Dual-cross central difference network for face anti-spoofing. IJICAI 2021.

Image and Video Face PAD

- Bilateral Convolutional Network (BCN)
  - Face PAD task can be treated as a material perception task
    - Three supervision of material perception and face PAD
  - Combine bilateral filtering with convolutional network

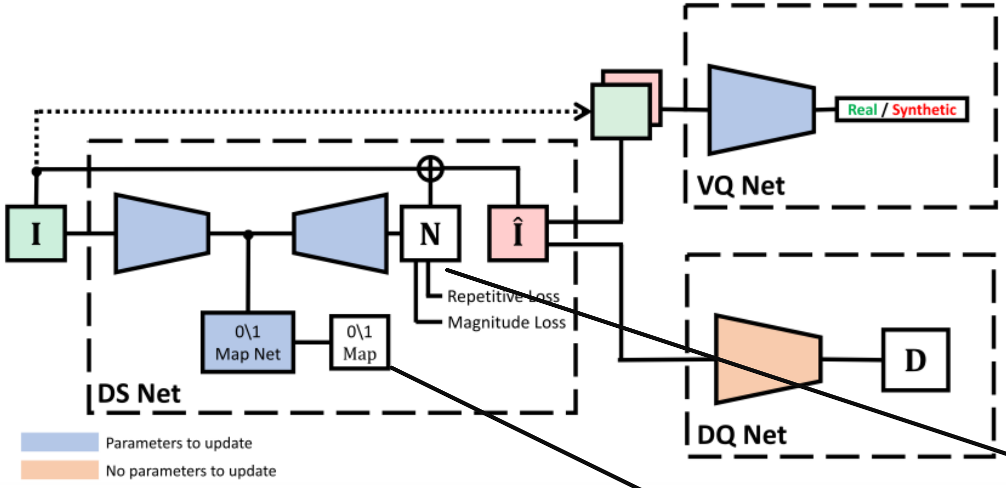


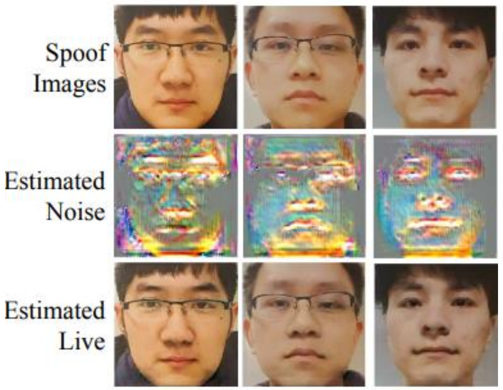


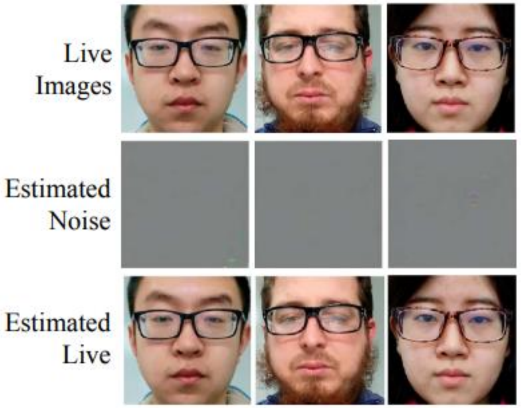
Yu, Zitong, et al. Face anti-spoofing with human material perception. ECCV 2020.

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





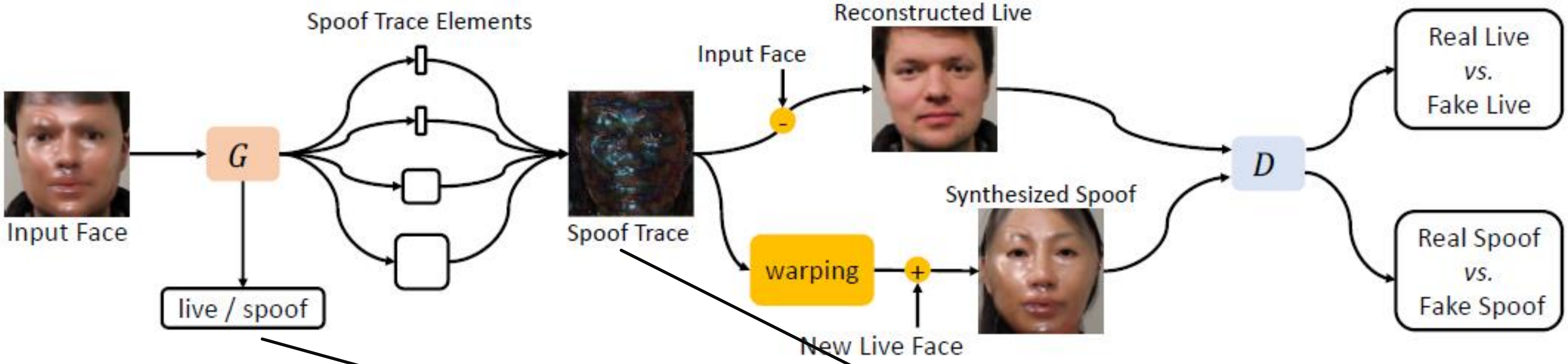


Final result: Average fusion of the spoof prediction map and spoof noise

Y. Liu, A. Jourabloo, and X. Liu. Face De-Spoofing: Anti-Spoofing via Noise Modeling, ECCV 2018

Image and Video Face PAD

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

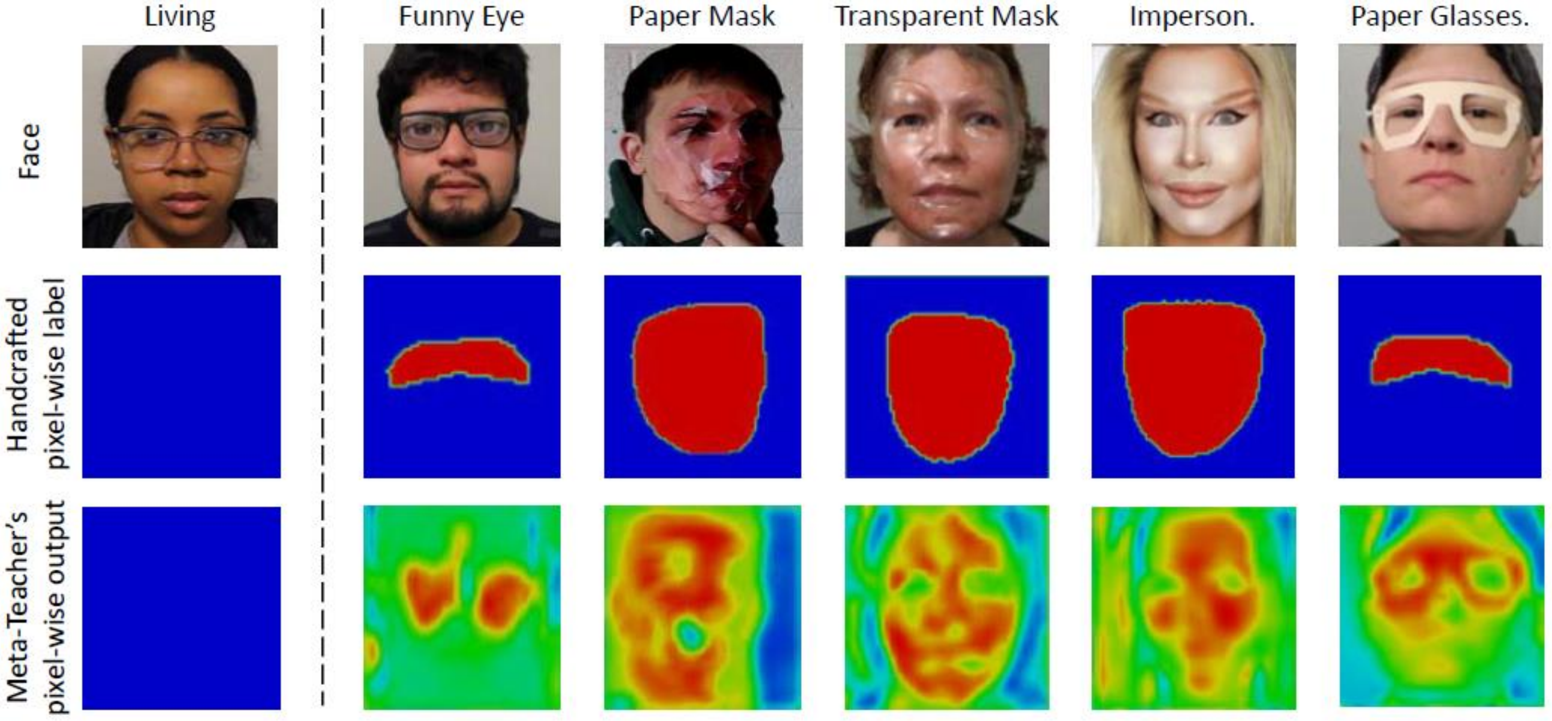


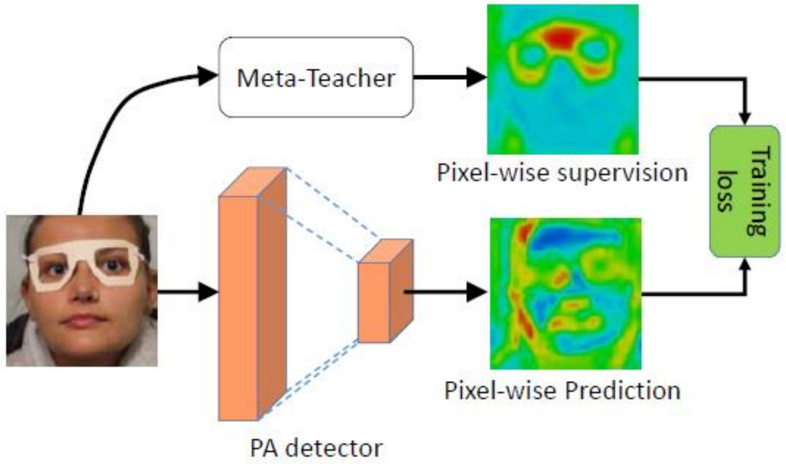
Final result: Average of the spoof prediction map and intensity of spoof trace

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

Image and Video Face PAD

- Generate better pixel-wise label
  - Teacher-Student framework: Meta-teacher generates better pixel-wise label to train the attack detector

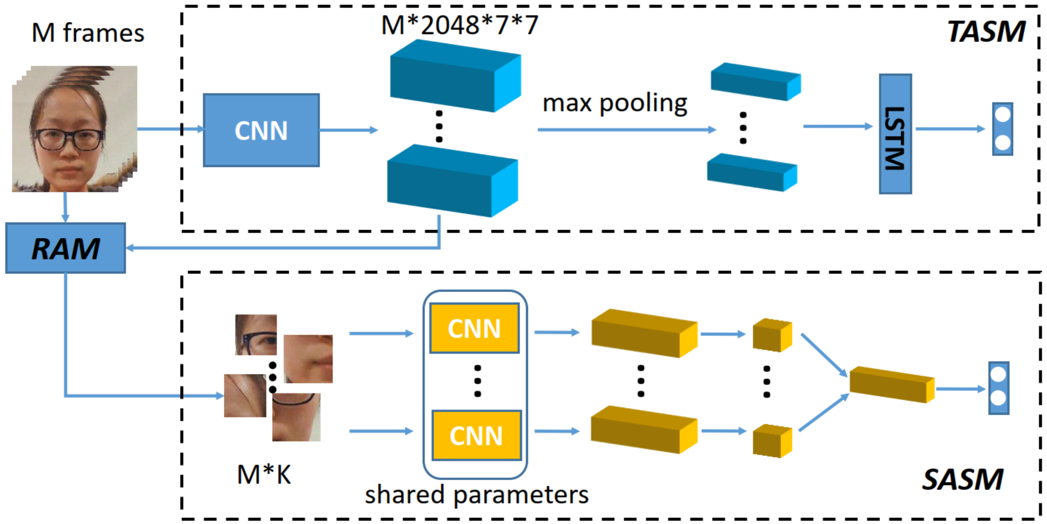




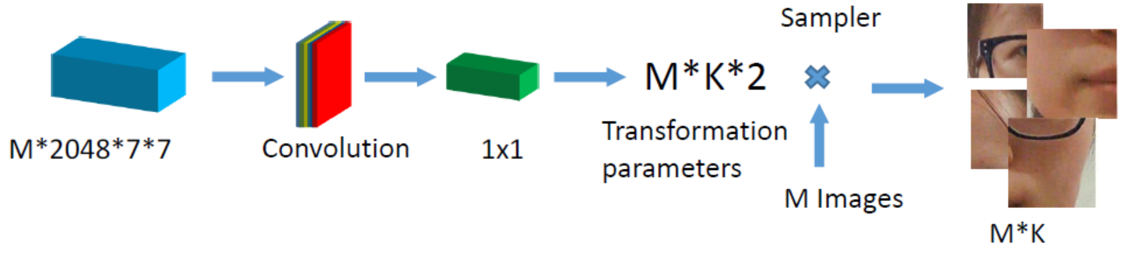
Y. Qin, et al. Meta-Teacher For Face Anti-Spoofing. TPAMI 2021.

Image and Video Face PAD

- Appearance + Motion Cues
  - Spatio-Temporal Anti-Spoof Network: consider both global temporal and local spatial cues
    - Temporal Anti-Spoofing Modul
    - Spatial Anti-Spoofing Module
  - Region Attention Module (RAM) learns the offset based on CNN features from TASM and outputs attended regions



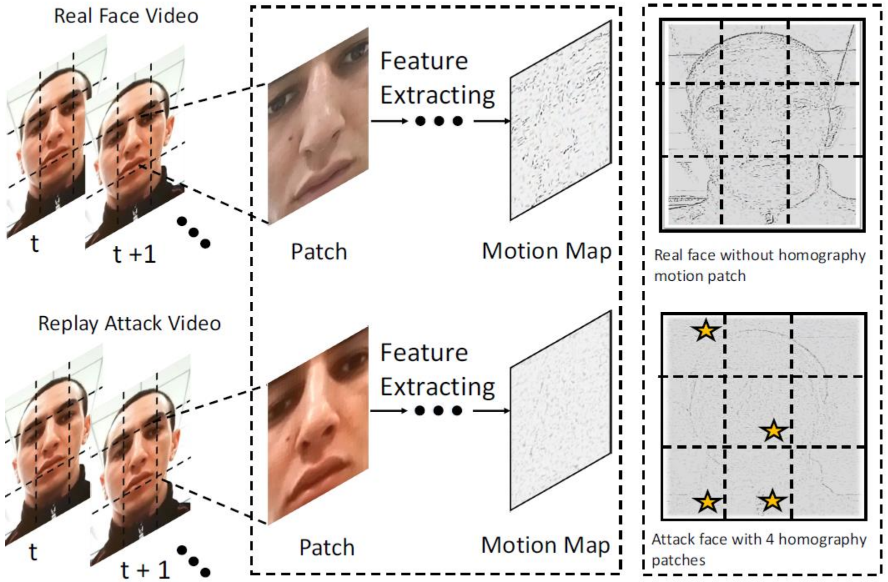
RAM:



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

Image and Video Face PAD

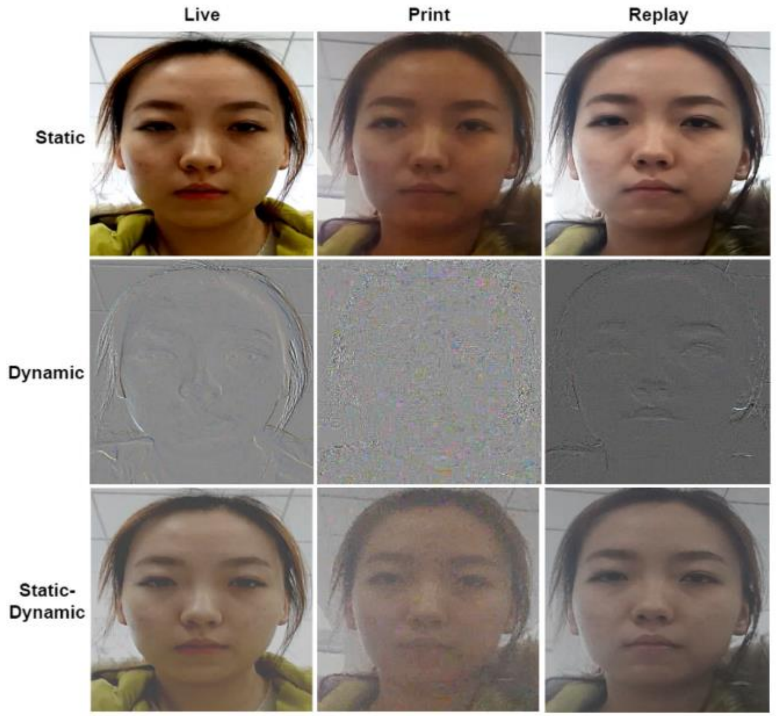
- Local homographic parameterization approach
  - Capture subtle motion difference between the facial movements from a planer screen and those from a real face
  - Multi-patch examination module enhances the recall rate of the attack videos



C Lin, Z Liao and et al. Live Face Verification with Multiple Instantialized Local Homographic Parameterization, IJCAI 2018

Image and Video Face PAD

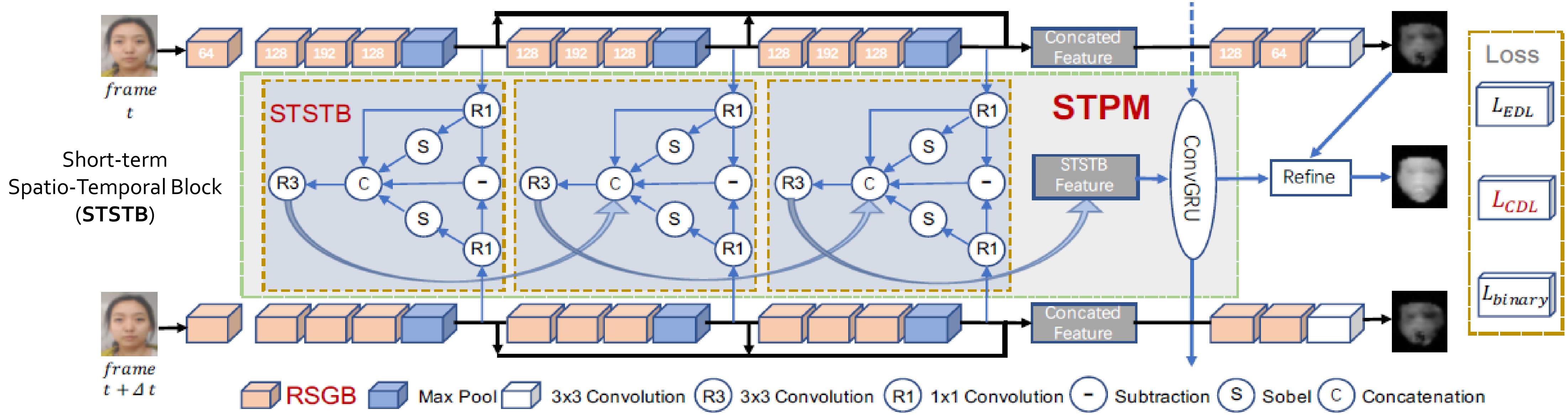
- Static-Dynamic CDCN
  - Combine dynamic information using Ranking pooling [*] in action recognition



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. PAMI 2020
* P. Wang, et al. Cooperative training of deep aggregation networks for RGB-D action recognition. AAAI 2018

Image and Video Face PAD

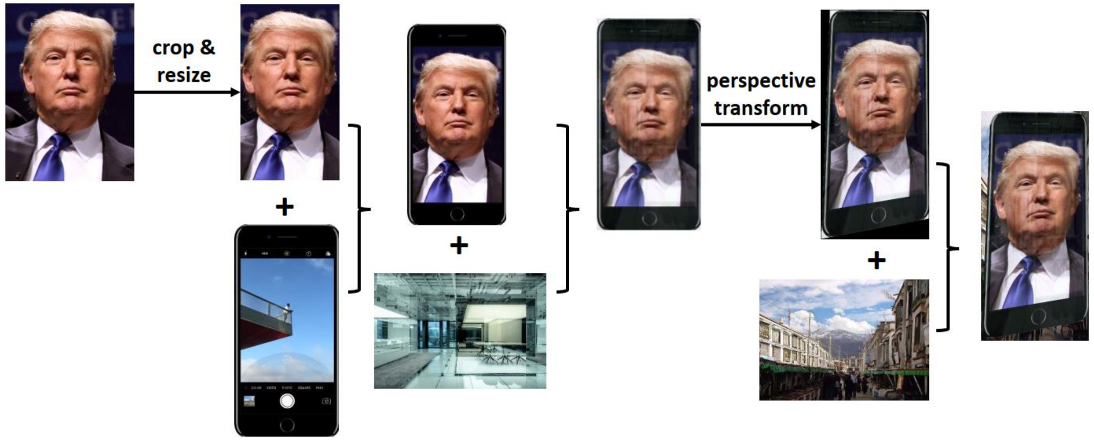
- Spatial Gradient and Temporal Depth (SGTD)
  - Learn detailed discriminative dynamics cues from stacked Residual Spatial Gradient Block (RSGB) and Spatio-Temporal Propagation Module (STPM).
    - Gradient: Sobel operator



Z. Wang, et al. Deep spatial gradient and temporal depth learning for face anti-spoofing. CVPR 2020.

Image and Video Face PAD

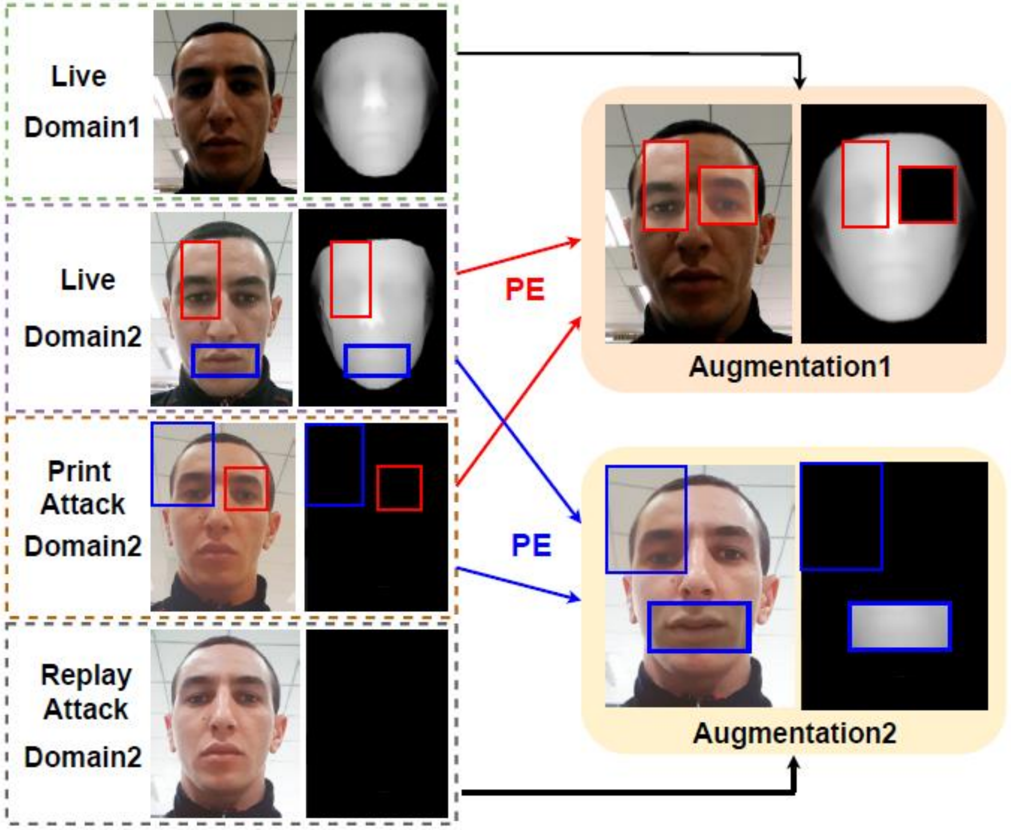
- Data Augmentation
  - Simulate digital medium-based face spoofing attacks to obtain a large amount of training data well reflecting the real-world scenarios
  - Synthetic reflection artifacts



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

Image and Video Face PAD

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



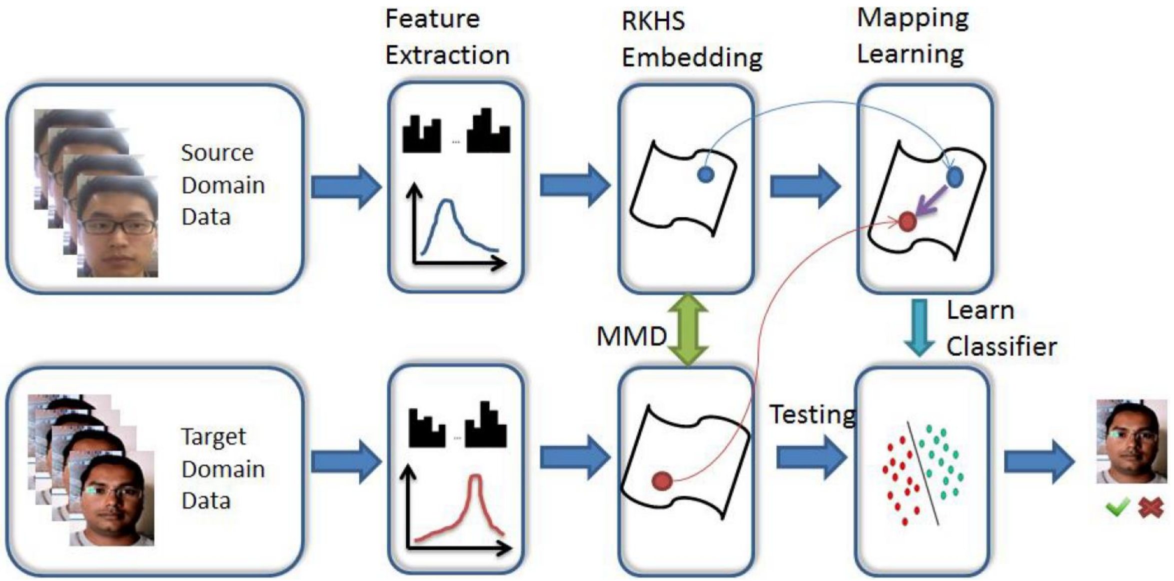
Yu, Zitong, et al. Dual-cross central difference network for face anti-spoofing. IJCAI 2021.

Image and Video Face PAD

Domain Adaptation and Generalization

Image and Video Face PAD

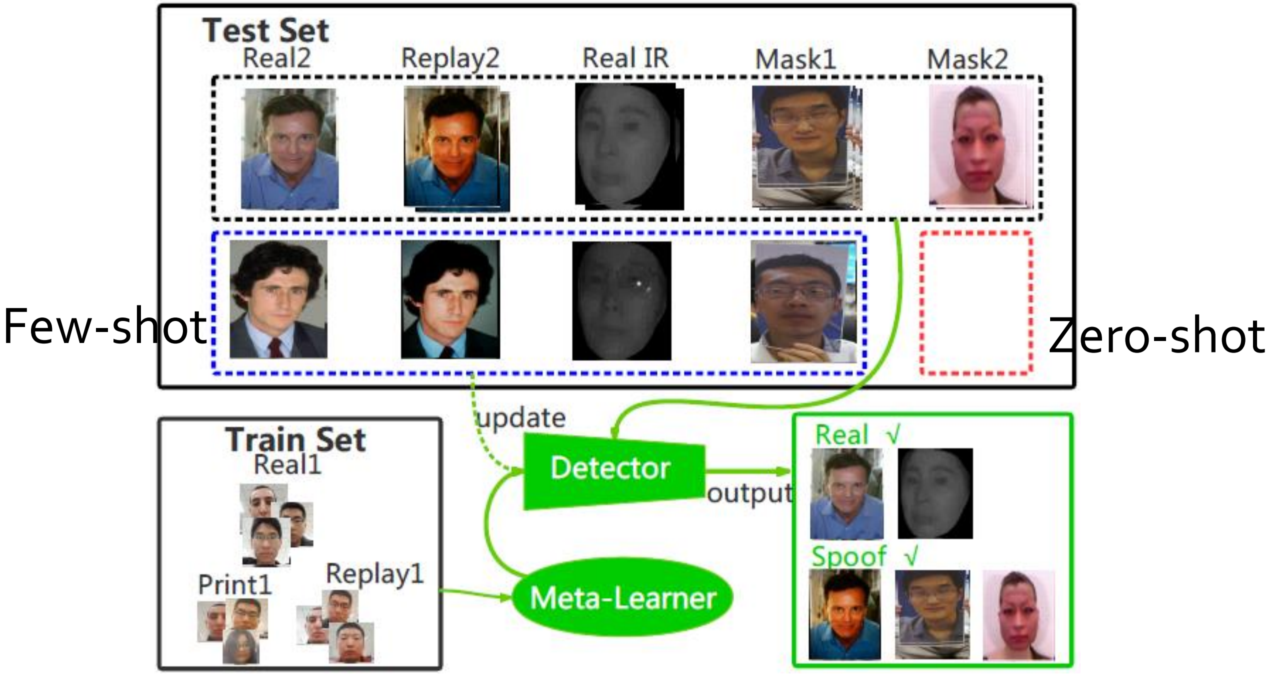
- Domain adaptation approach
  - Learn a mapping function to align the eigenspaces between source domain data and target domain data.
  - Maximum Mean Discrepancy between the source and target latent features is minimized



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

Image and Video Face PAD

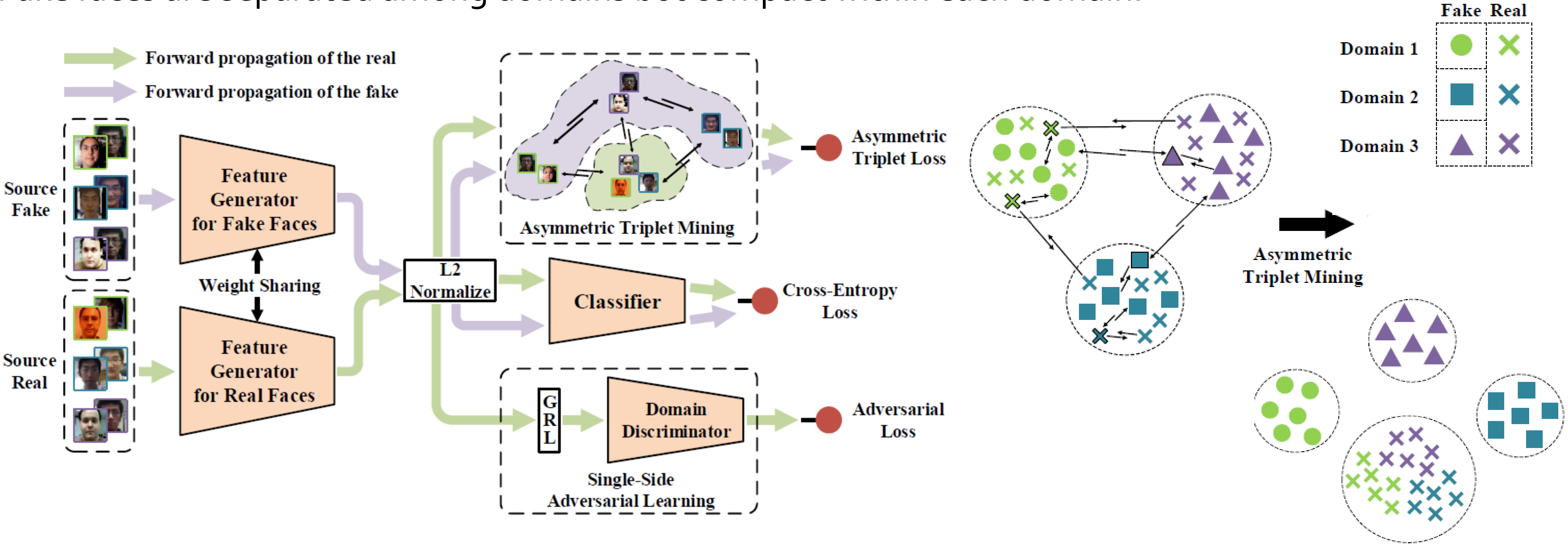
- Adaptive Inner-update Meta learning
  - Aim to quickly adapt to new spoofing types by learning from both the predefined attacks and a few examples of the new spoofing types.



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

Image and Video Face PAD

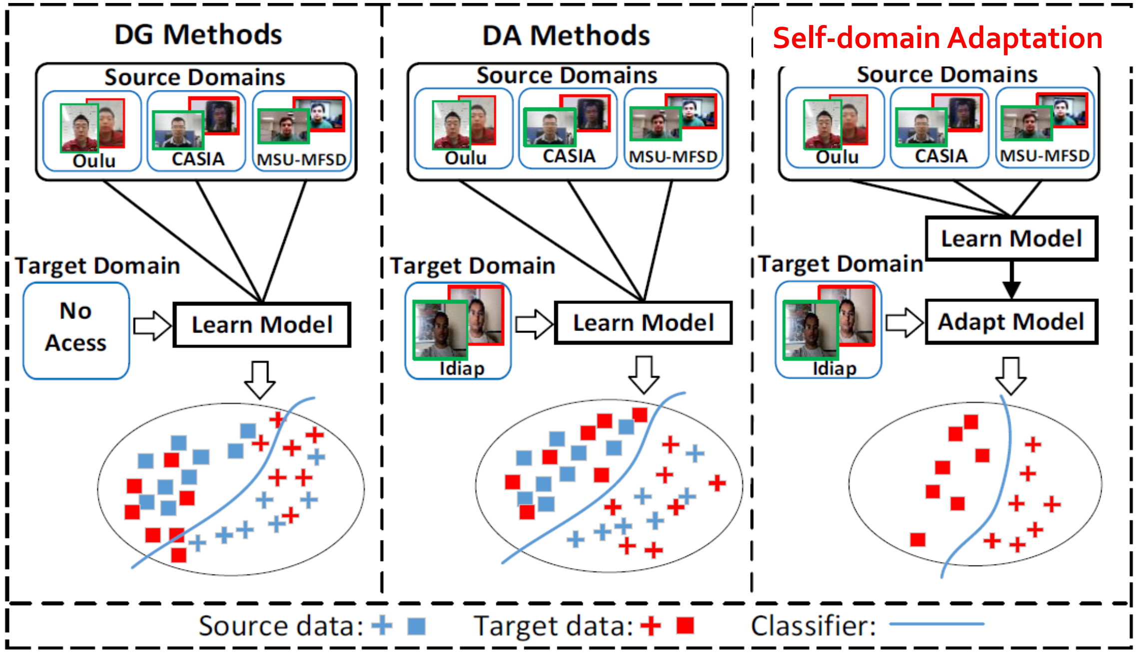
- Single-side domain generalization
  - Learn a generalized space where the feature distribution of real faces is compact
  - Fake faces are separated among domains but compact within each domain.

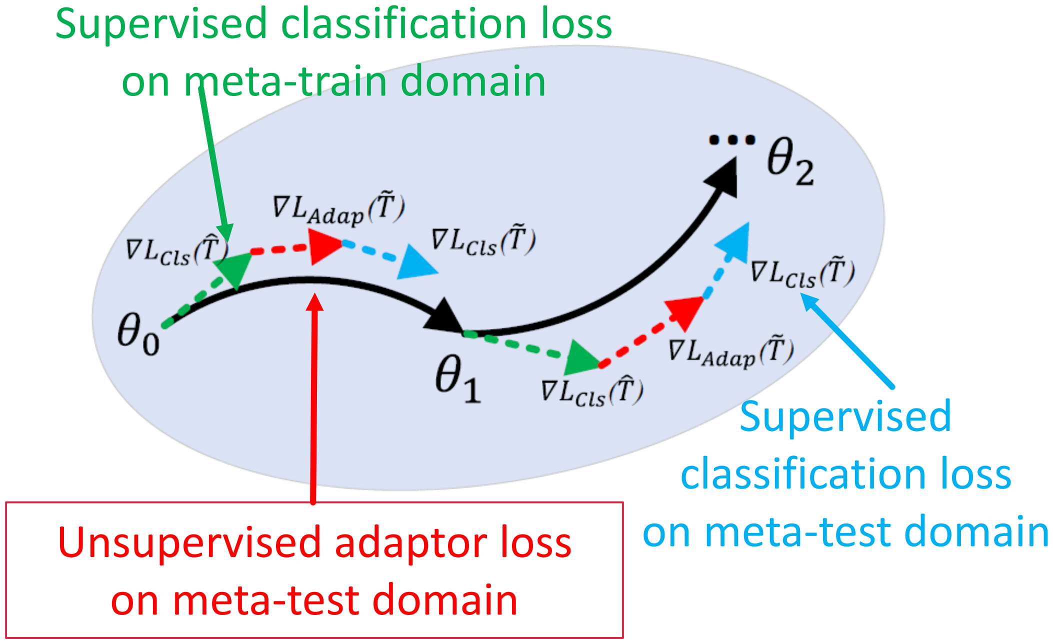


Y. Jia, et al. Single-side domain generalization for face anti-spoofing. CVPR 2020.

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

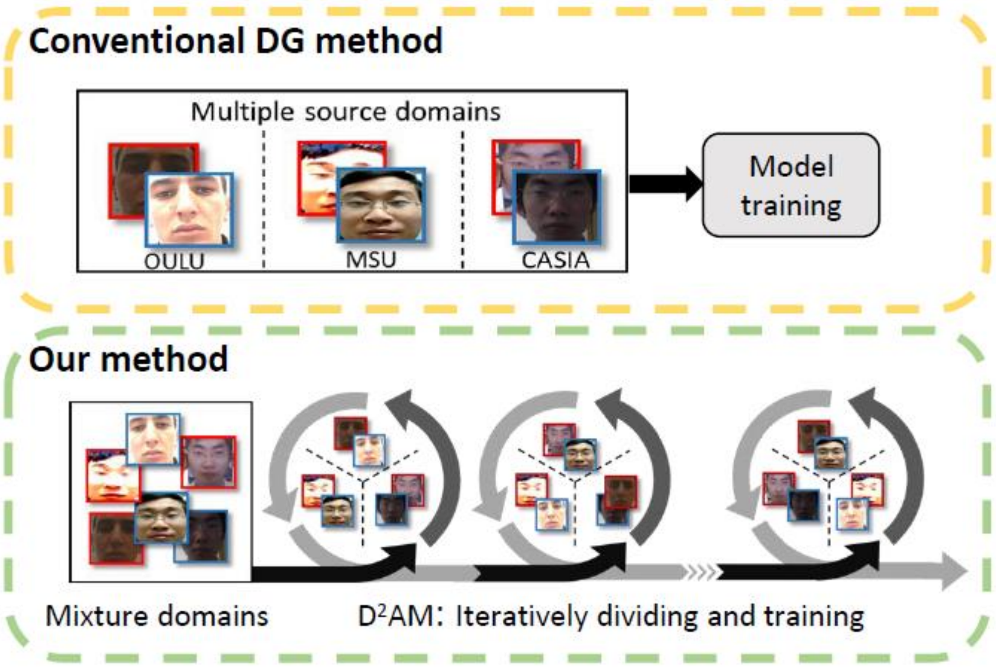




J. Wang, et al. Self domain adaptation for face anti-spoofing. AAAI 2021.

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

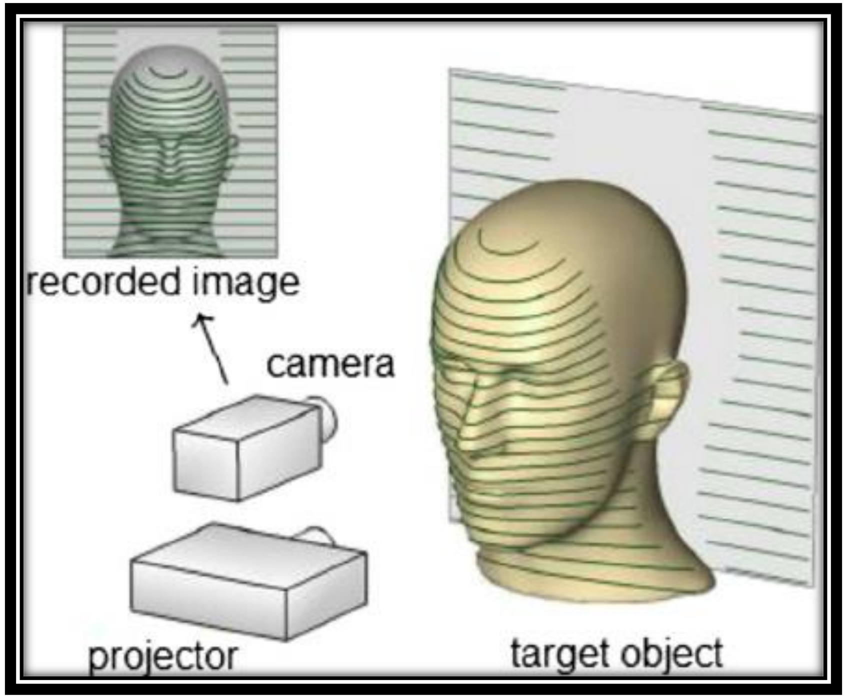


Z. Chen, et al. Generalizable representation learning for mixture domain face anti-spoofing. AAAI 2021.

3D Face Recognition

FaceID in iPhone X

Announced on 12 September 2017

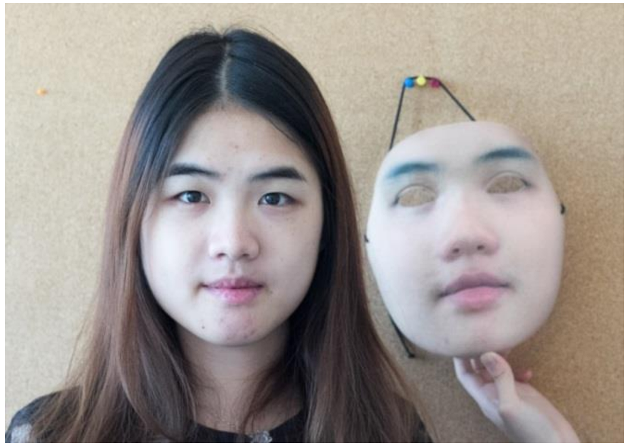


3D Face Recognition:
Employed Structured-light 3D technology

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

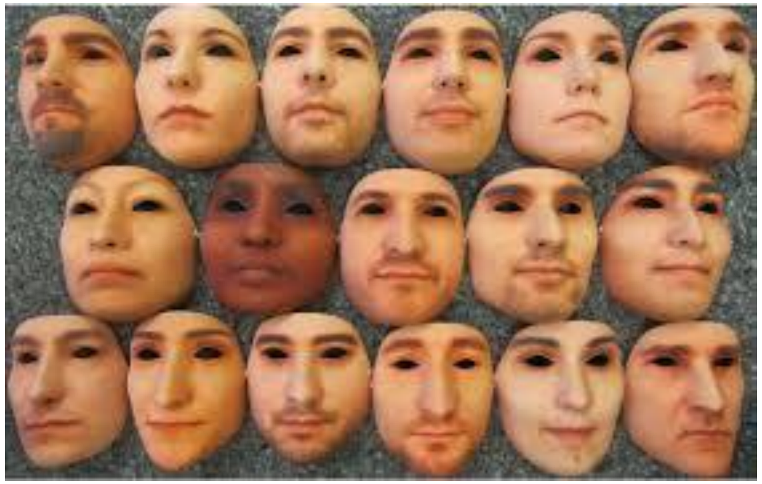
By Jeff John Roberts December 12, 2019

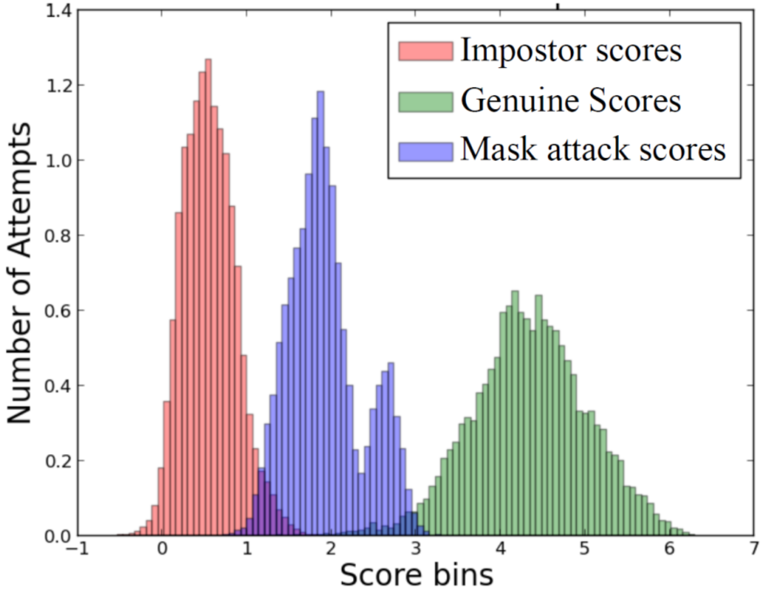
The test, by artificial intelligence company Kneron, involved visiting public locations and tricking facial recognition terminals into allowing payment or access. For example, in stores in Asia—where facial recognition technology is deployed widely—the Kneron team used high quality 3-D masks to deceive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

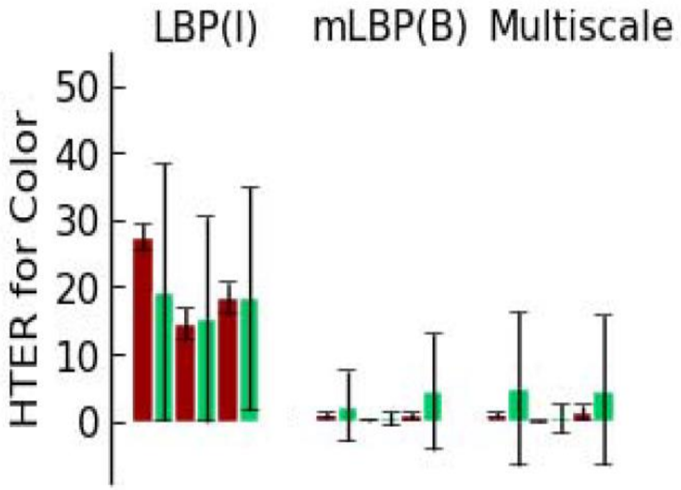
More alarming were the tests deployed at transportation hubs. At the self-boarding terminal in Schiphol Airport, the Netherlands' largest airport, the Kneron team tricked the sensor with just a photo on a phone screen. The team also says it was able to gain access in this way to rail stations in China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



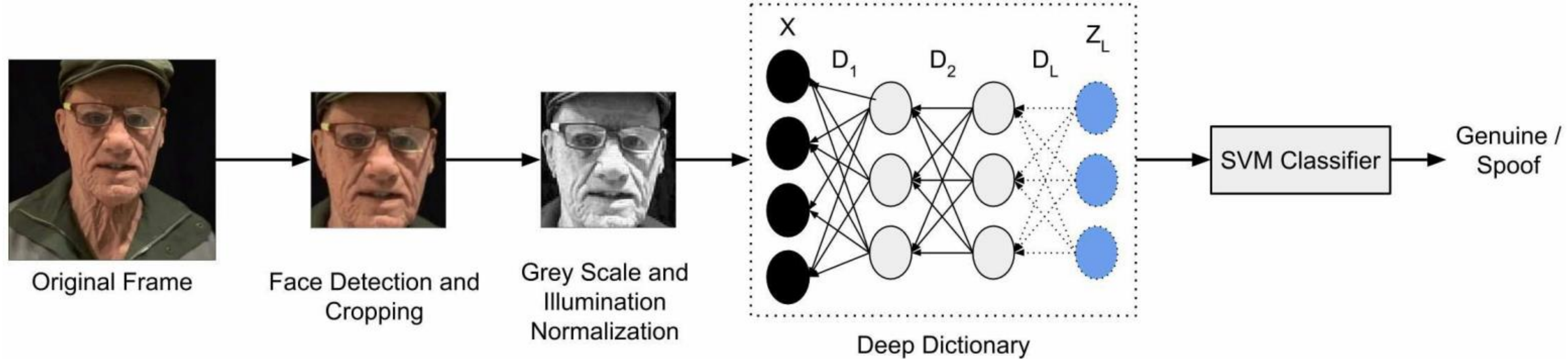




[Erdogmus et al., BTAS'13]

3D Mask Face PAD

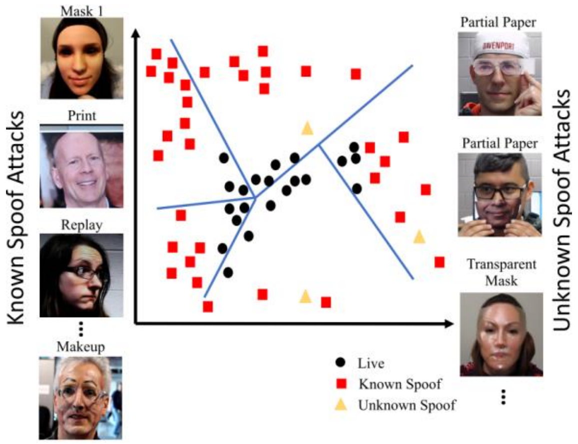
- Deep Dictionary Learning approach
  - Detecting Silicone Mask-based Presentation Attack.
  - Multilevel deep dictionary learning-based presentation attack detection algorithm

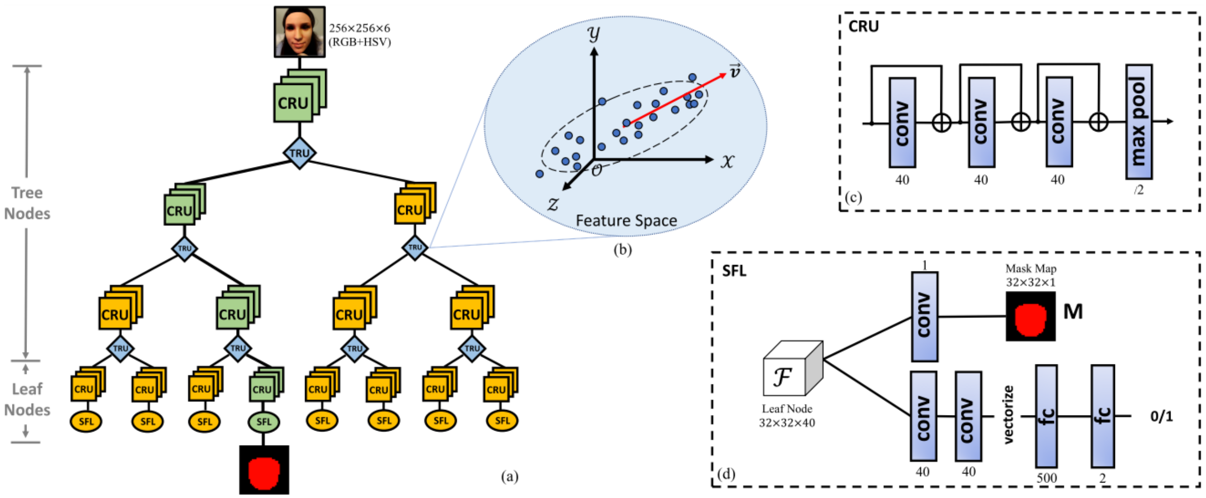


Manjani I, Tariyal S, Vatsa M, et al. Detecting silicone mask-based presentation attack via deep dictionary learning, TIFS 2017

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

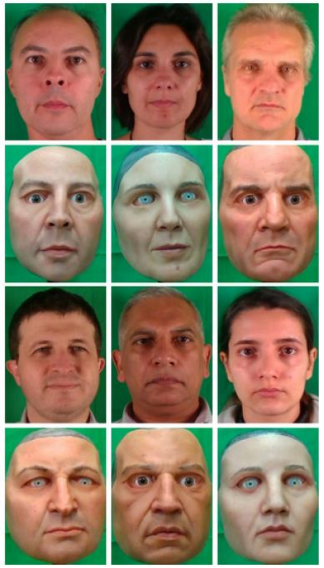


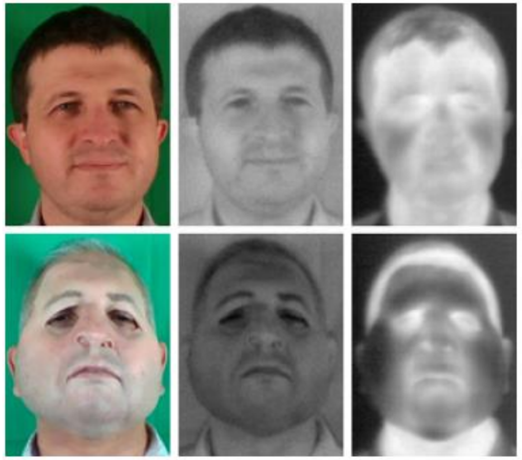


Liu Y, Stehouwer J, Jourabloo A, et al. Deep Tree Learning for Zero-shot Face Anti-Spoofing, CVPR 2019

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

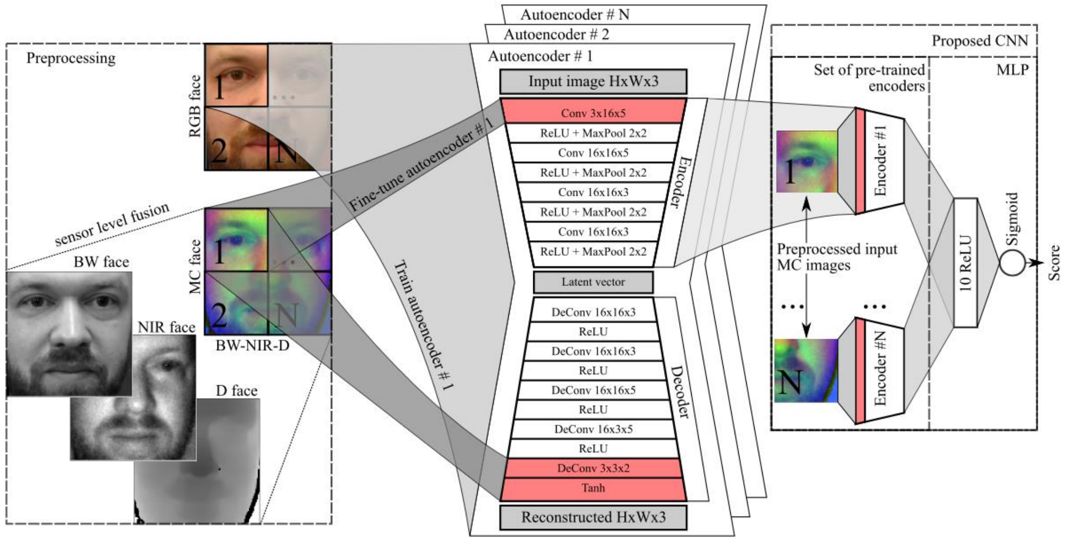


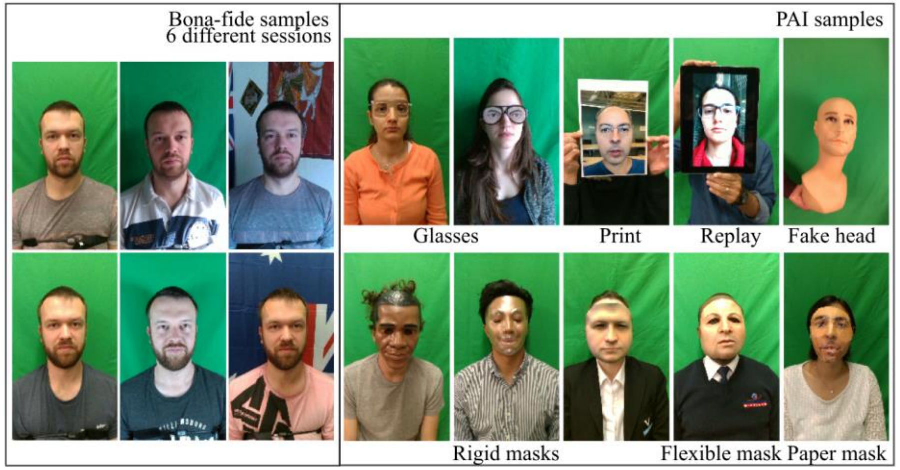


Bhattacharjee S, Mohammadi A, Marcel S. Spoofing deep face recognition with custom silicone masks, BTAS 2018

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

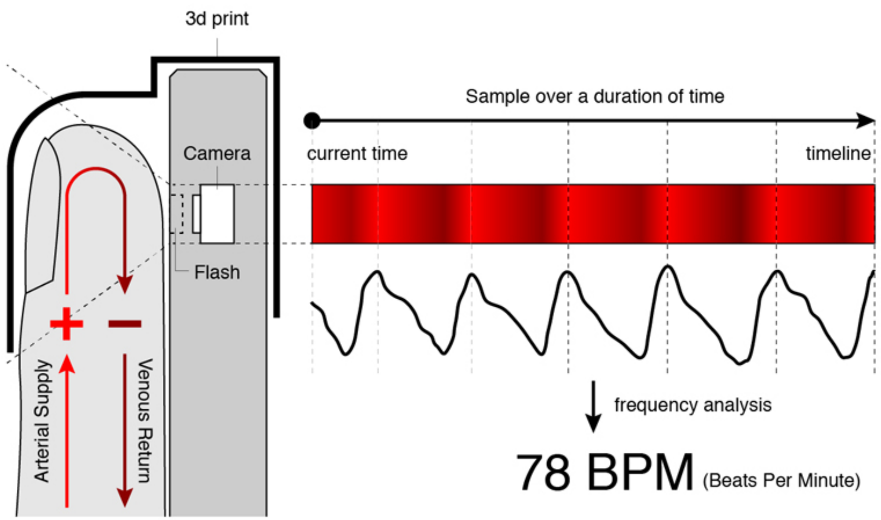
- PhotoPlethysmoGraphy based Approach
- Deep Dynamic Feature Approach
- Domain Generalization Approach
- Federated Learning Approach

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

Reference:

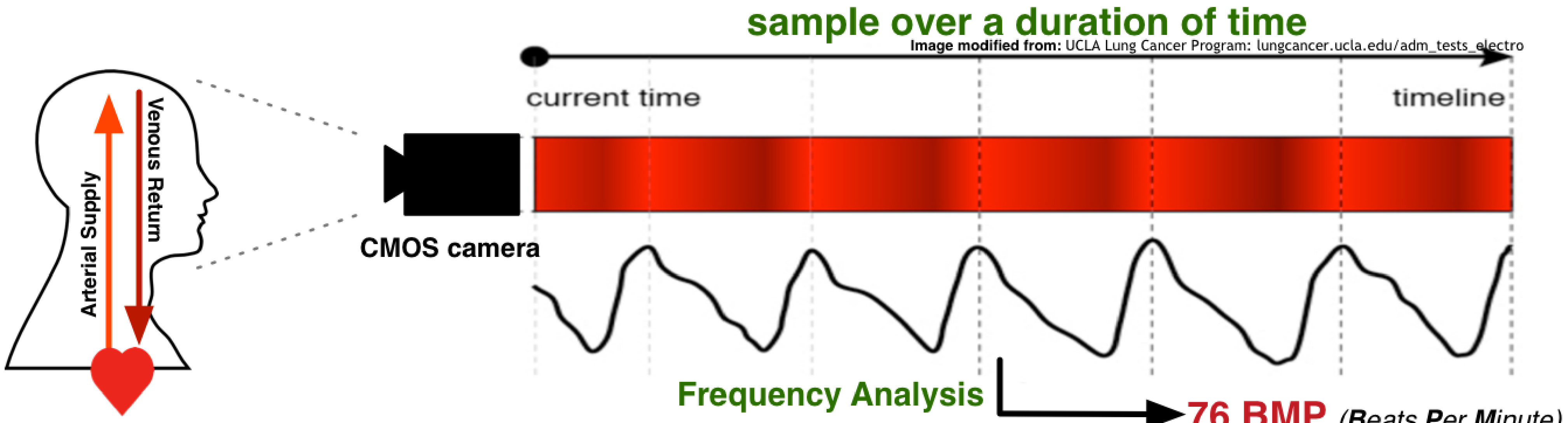
1. S Q Liu, X Y Lan and P C Yuen, "Multi-Channel Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection", *IEEE Transactions on Information Forensics and Security (TIFS)*, In press 2021
2. S Q Liu, X Lan, P C Yuen, "Remote Photoplethysmography Correspondence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

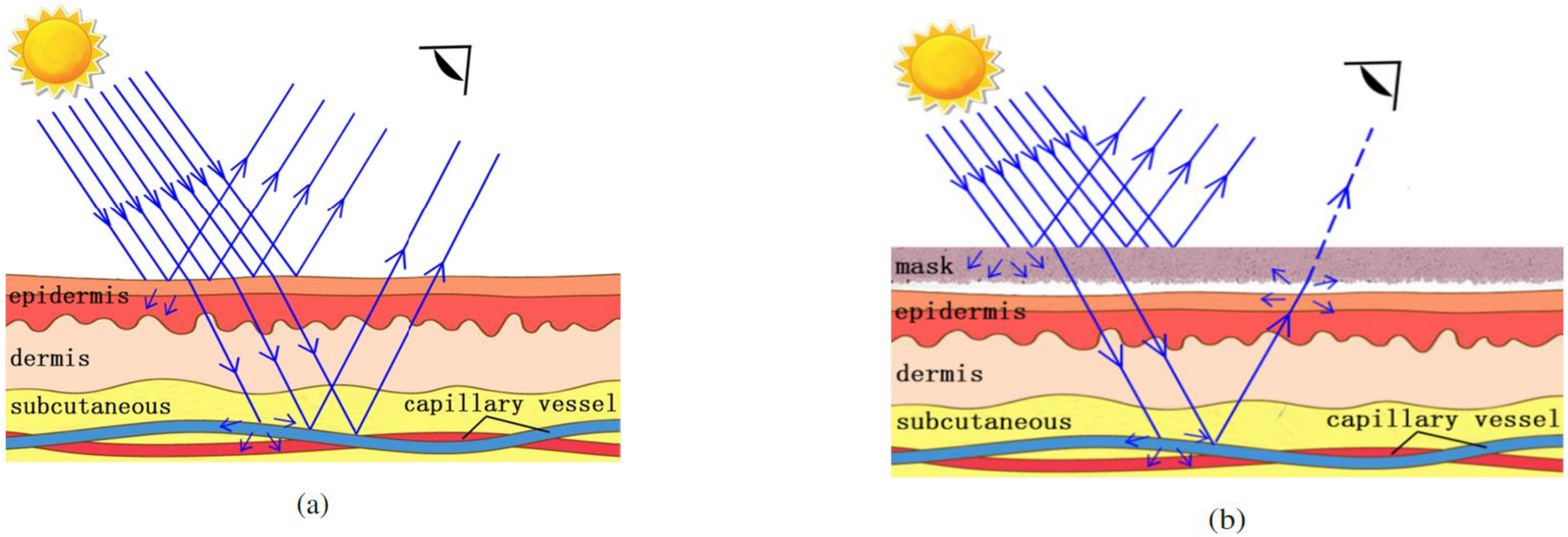


Pic. from UCLA Lung Cancer Program http://lungcancer.ucla.edu/adm_tests_electro.html

remote PhotoPlethysmoGraphy (rPPG)



Principle of rPPG Based Face Anti-Spoofing



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

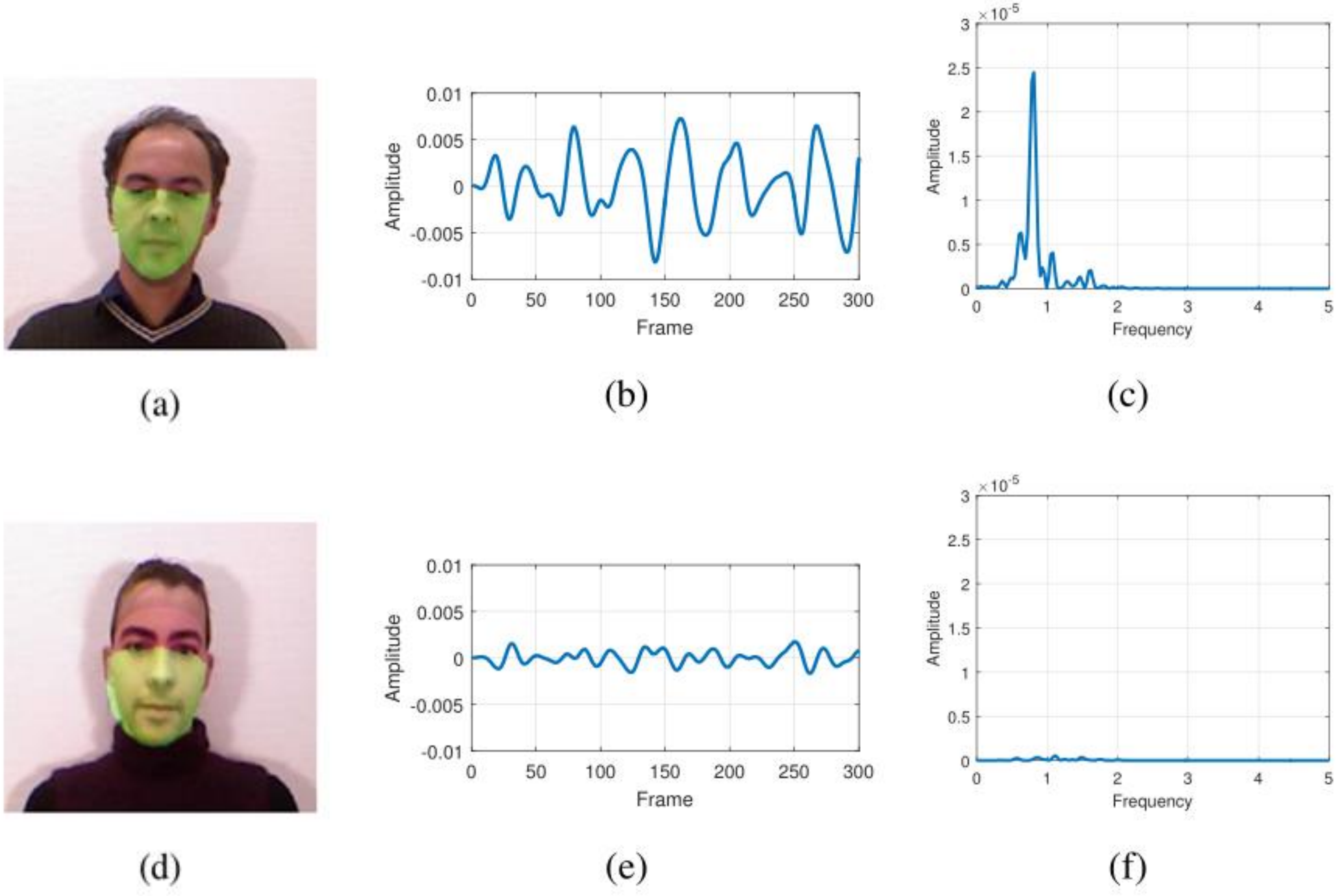
(b) rPPG signals will be **too weak** to be detected from a masked face.

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

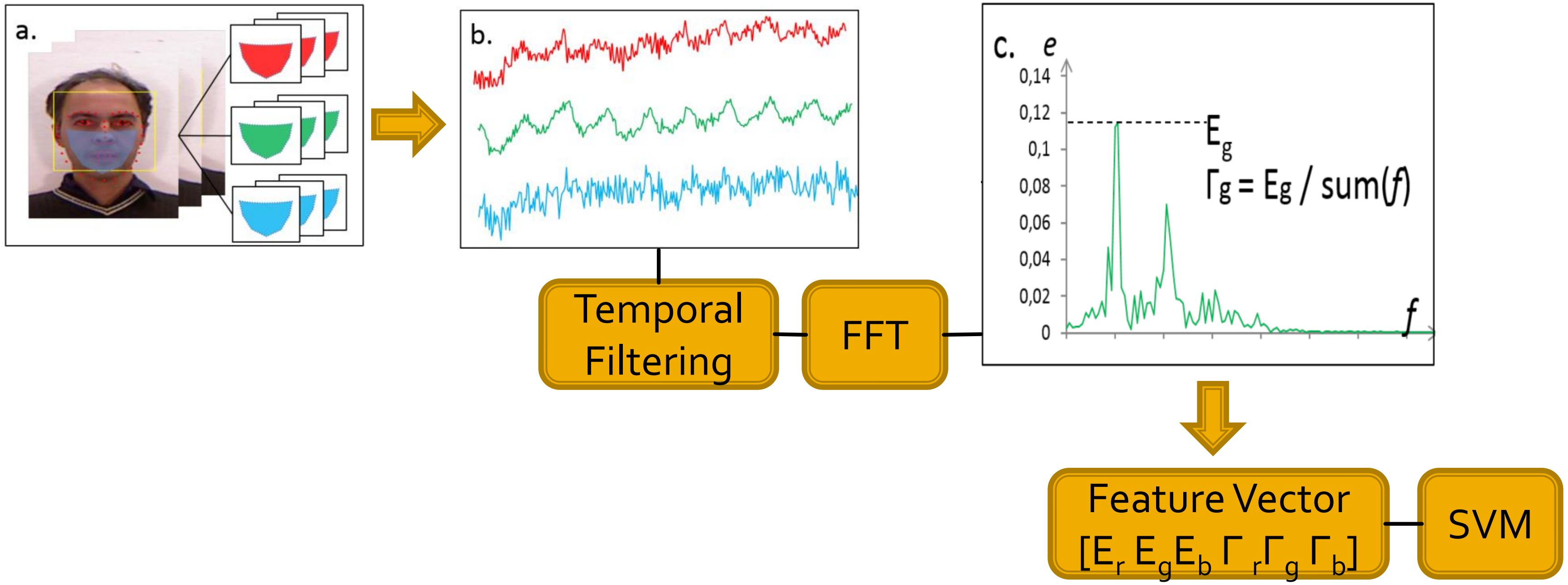
Principle of rPPG Based Face Anti-Spoofing

genuine face

masked face

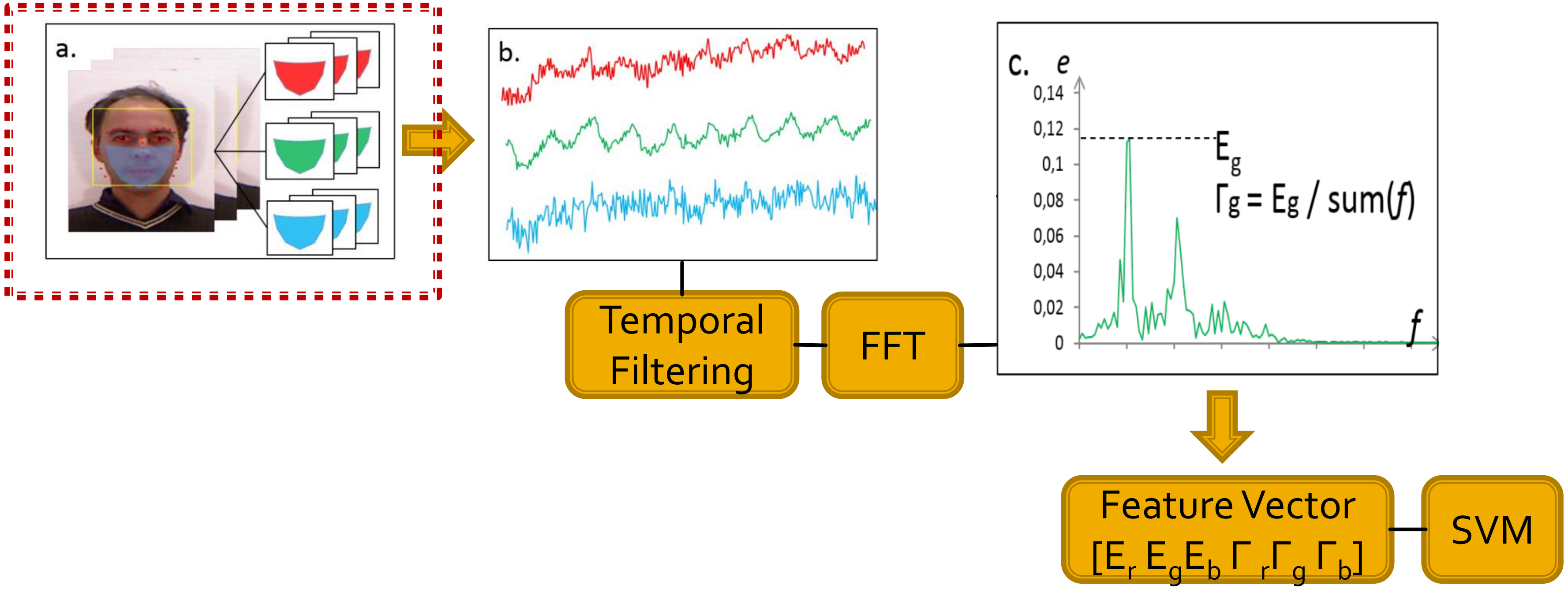


Global rPPG-based Face Anti-Spoofing [ICPR 2016]



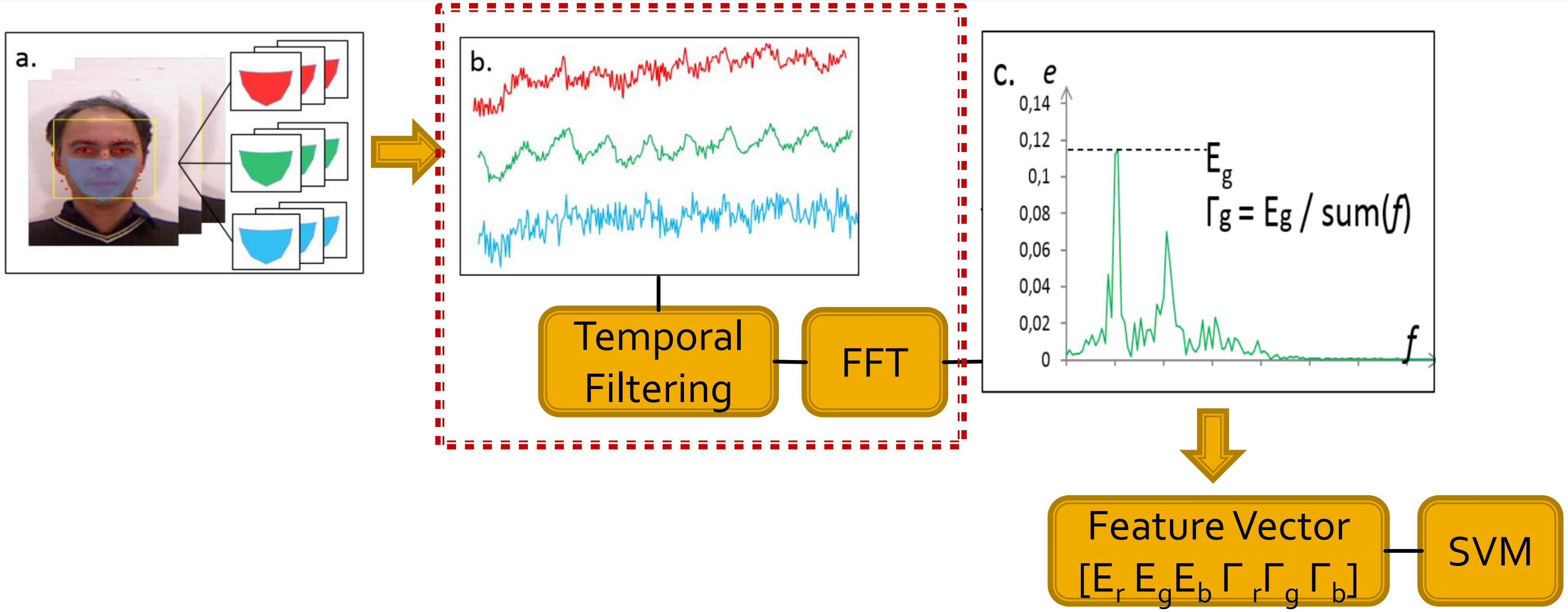
X Li, J Komulainen, G Zhao, P C Yuen and M Pietikainen,
"Generalized face anti-spoofing by detecting pulse from face videos"
ICPR 2016

Global rPPG-based Face Anti-Spoofing



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

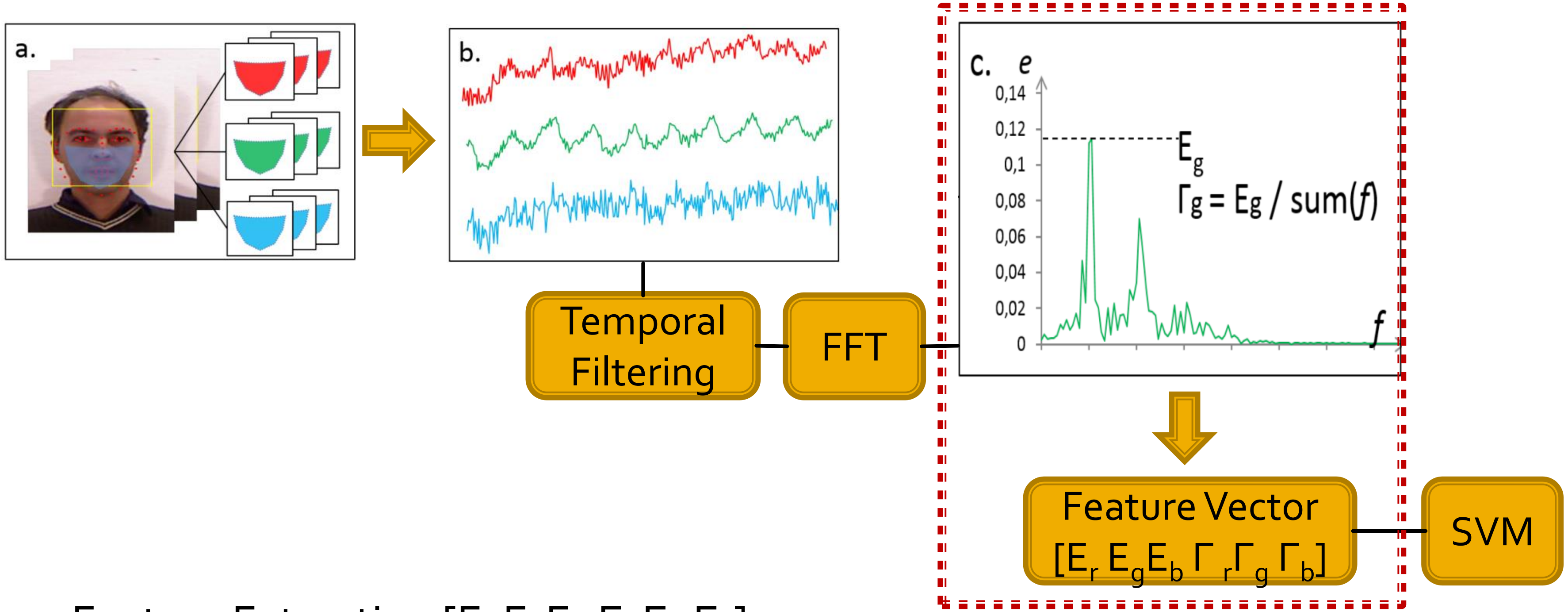
Global rPPG-based Face Anti-Spoofing



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*

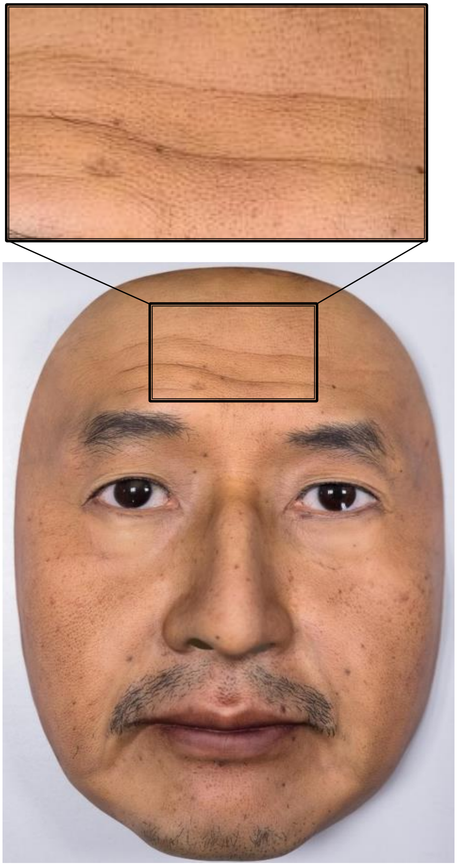
Experimental Results

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

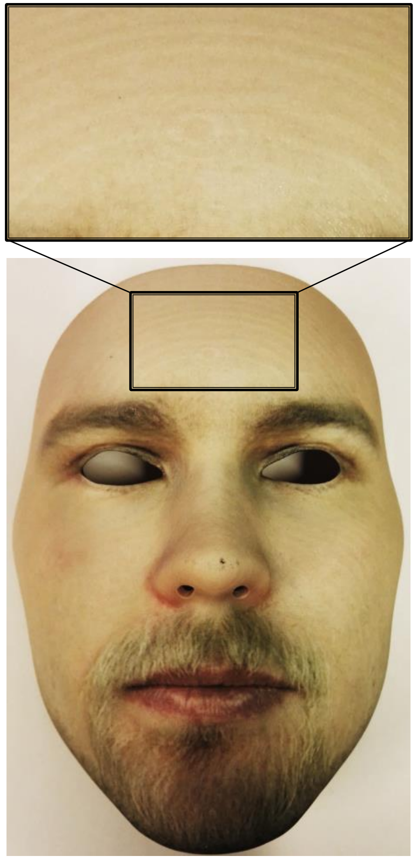
	REAL-F			
Method	HTER(%)	EER(%)	FPR (@FNR=0.1%)	FPR (@FNR=0.01%)
Pulse (ours)	**4.29**	**1.58**	**0.25**	**3.83**
LBP-blk	26.3	25.08	37.92	48.25
LBP-blk-color	25.92	20.42	31.5	48.67
LBP-ms	39.87	46.5	59.83	73.17
LBP-ms-color	47.38	46.08	86.5	95.08

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

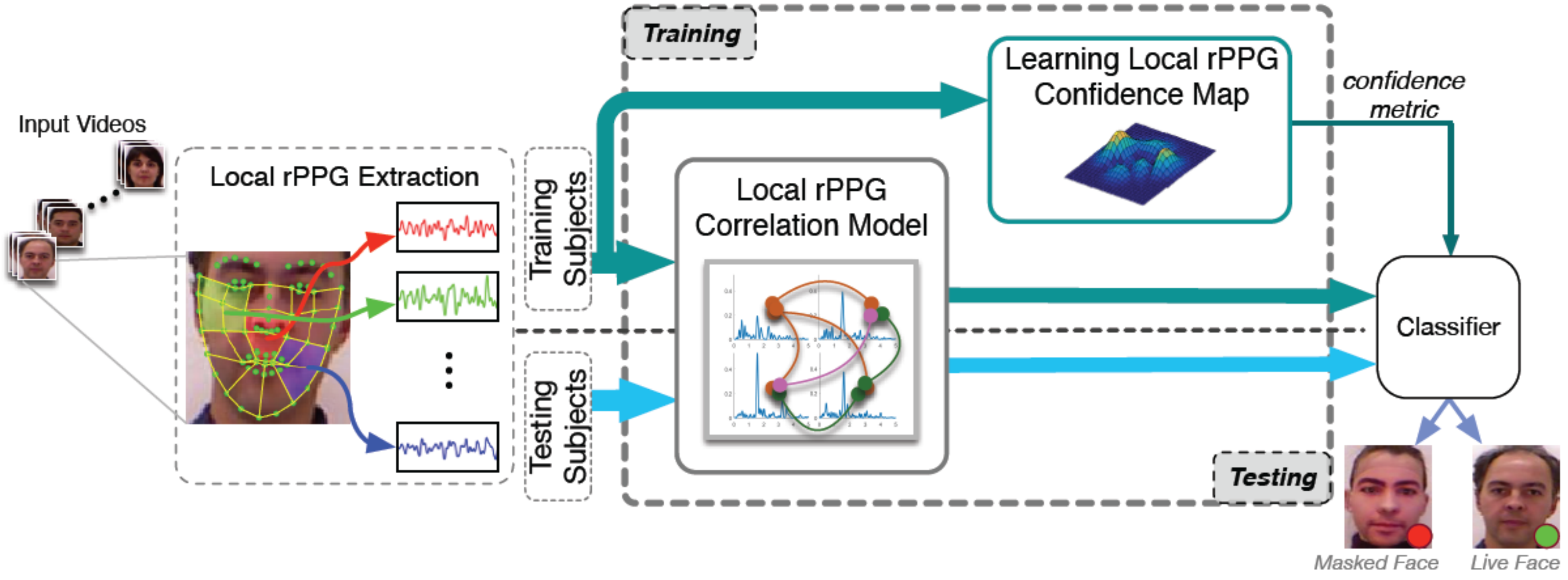
Limitations on Global rPPG method

- 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?

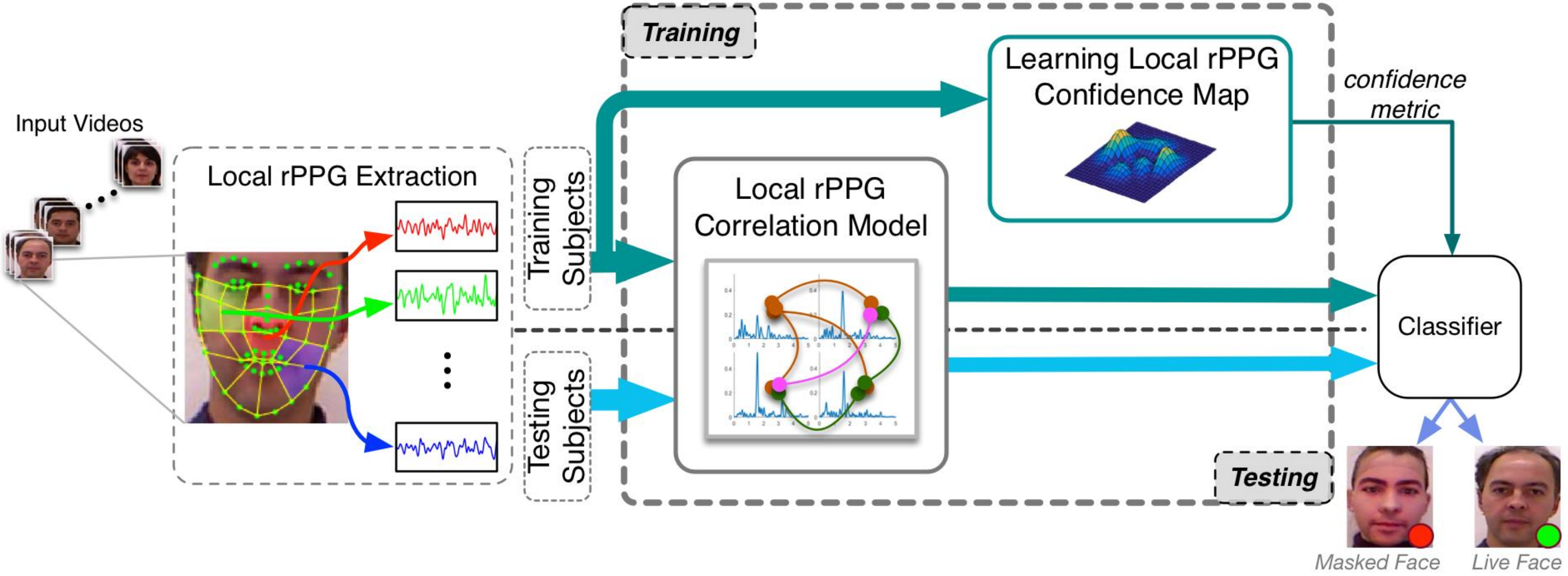
Local rPPG based Face Anti-Spoofing Method

[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.

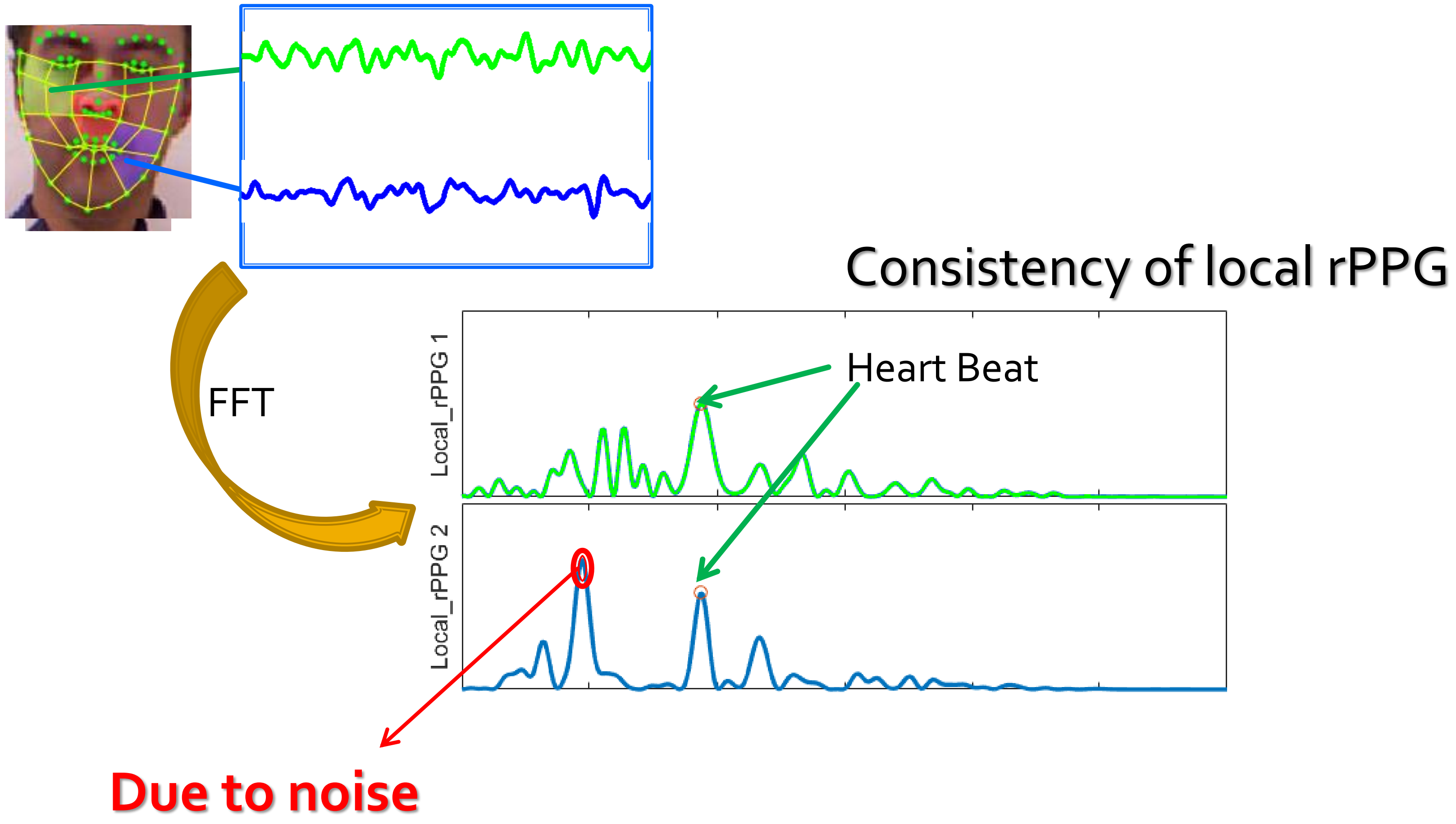
(b) Extract Local rPPG patterns through the proposed **local rPPG correlation model**.

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

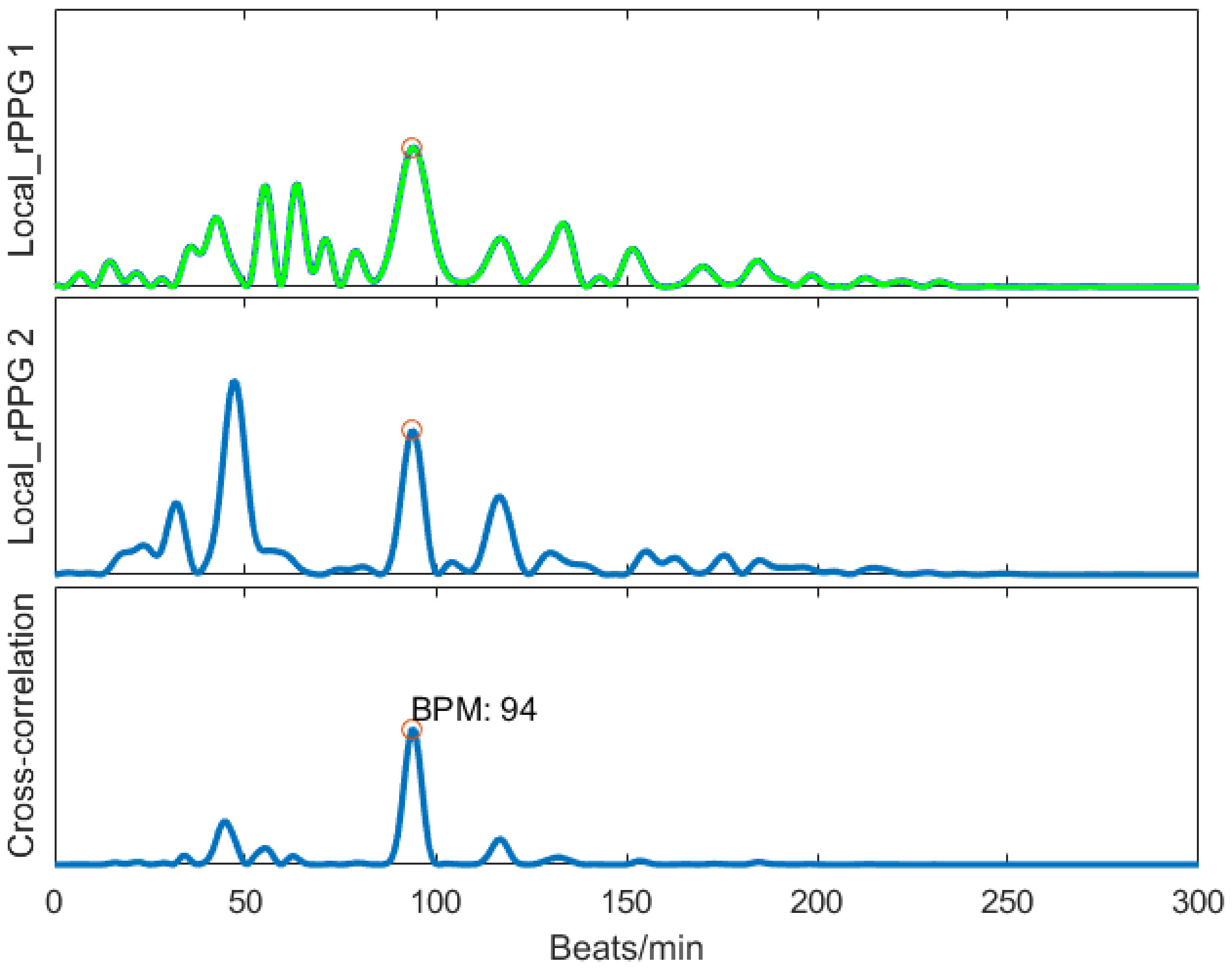
(d) Classifier: SVM

Contribution 1: Local rPPG Correlation Model

- Local rPPG on genuine face

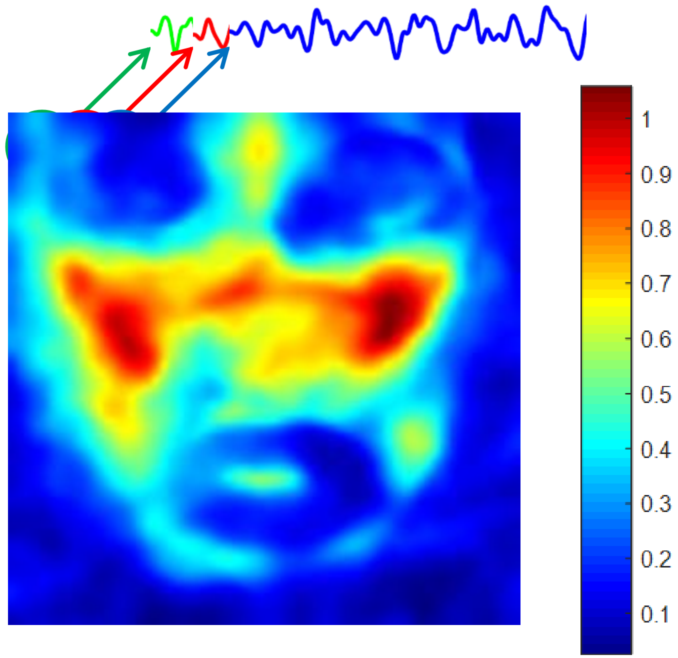


2. Local rPPG Correlation Model



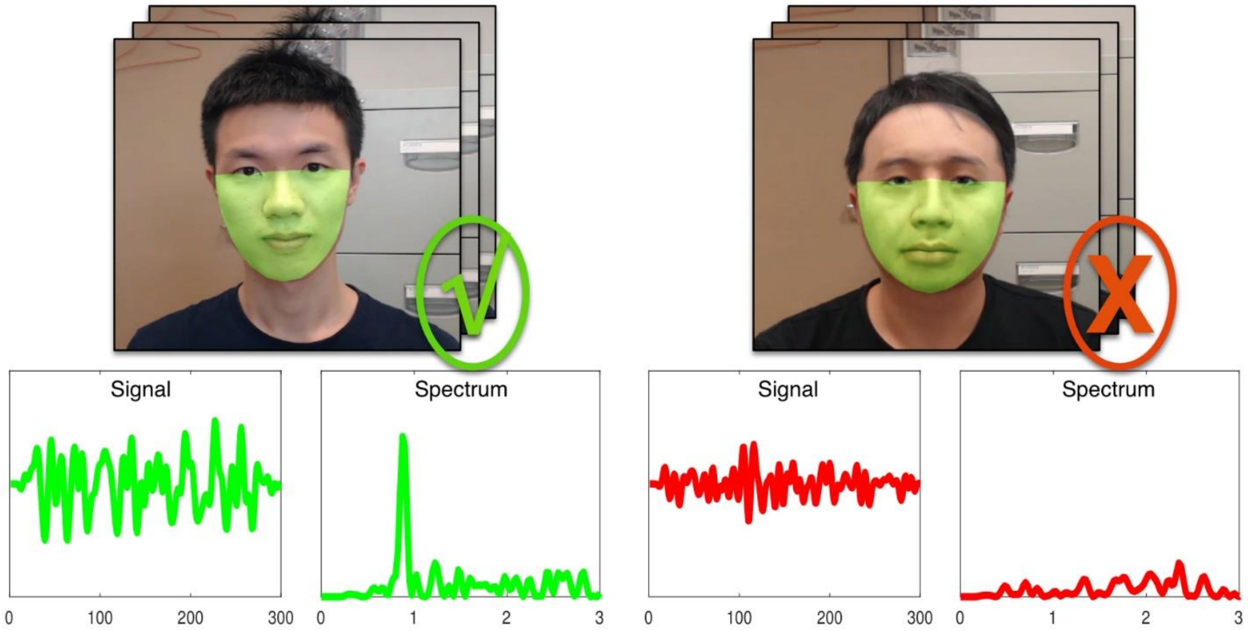
Contribution 2: Learning Local rPPG Confidence Map

Generic map of blood vessels on the face



The distribution of local rPPG signals should be considered

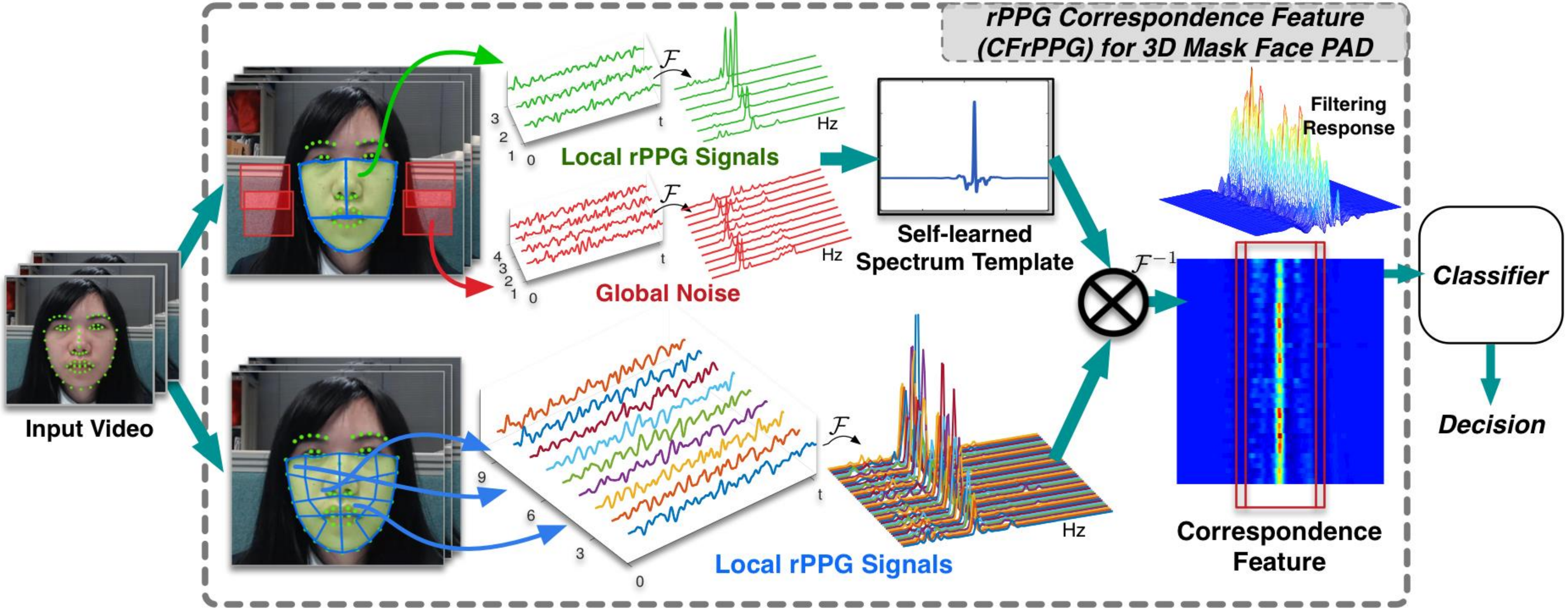
Limitation on Local rPPG Approach



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

Improved Method: rPPG Correspondence Feature

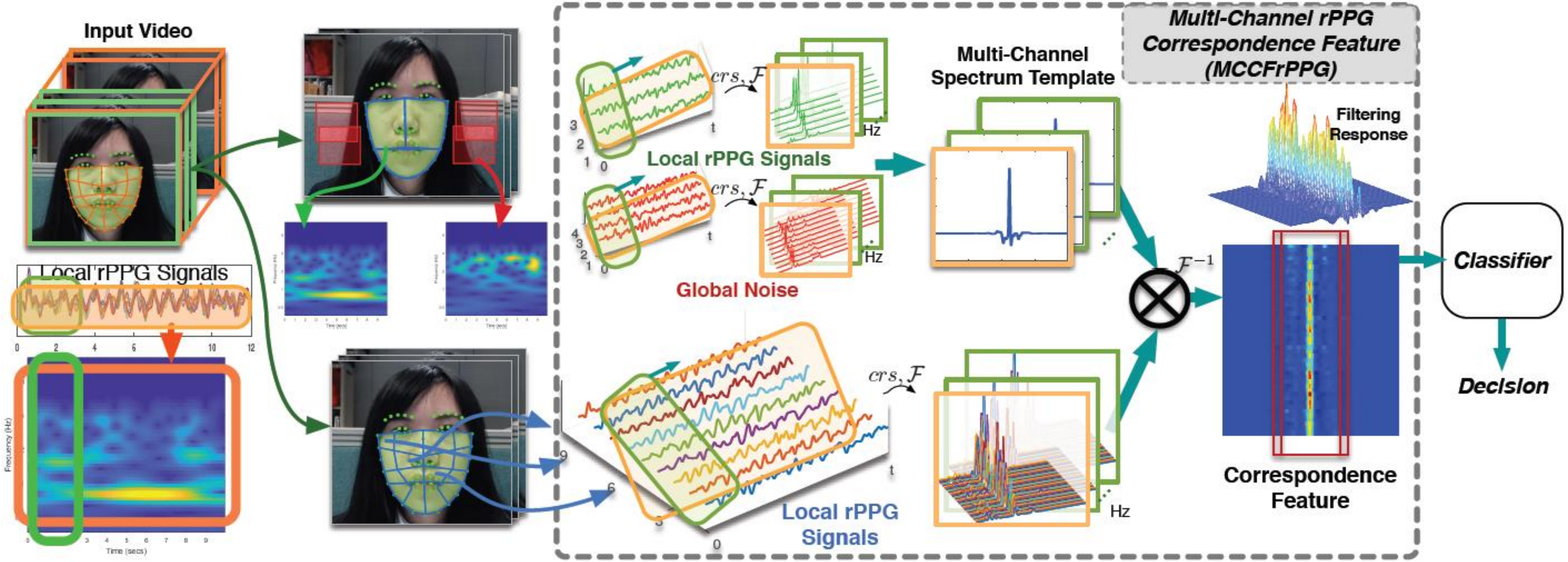
[ECCV 2018]



1. S Q Liu, X Y Lan and P C Yuen, "Multi-Channel Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection", *IEEE Transactions on Information Forensics and Security (TIFS)*, 2021.
2. S Q Liu, X Y Lan and P C Yuen, "Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection", *ECCV* 2018

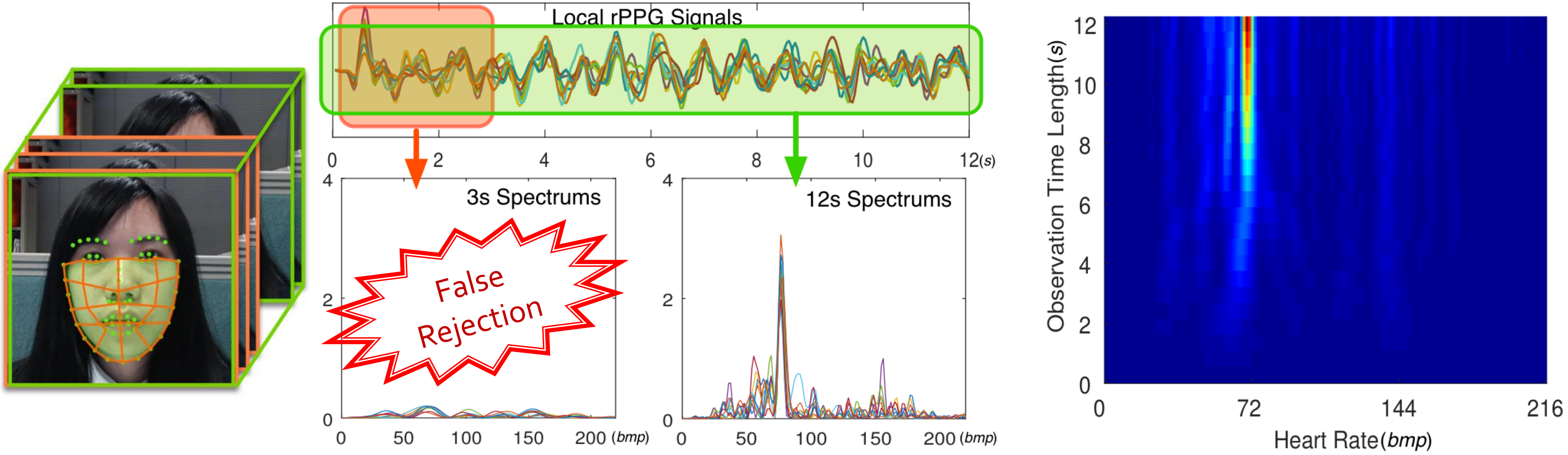
Improved Method: rPPG Correspondence Feature

[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.

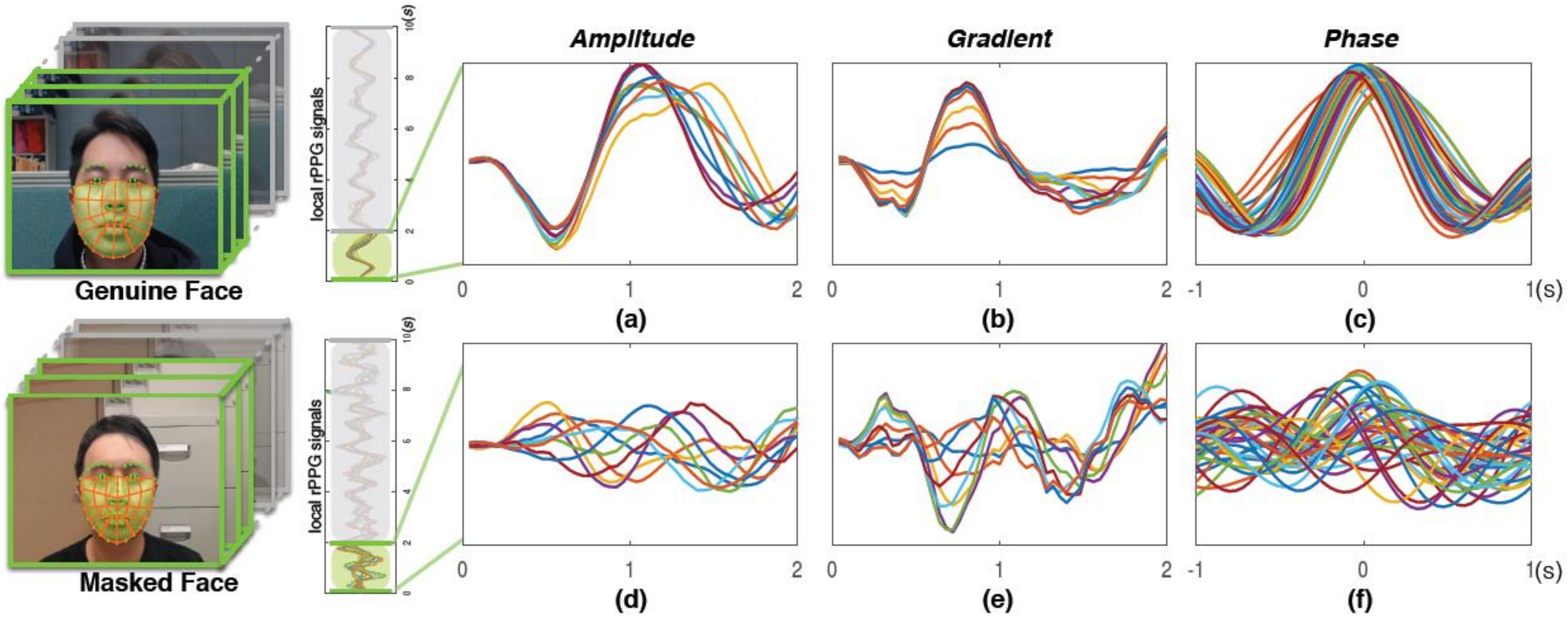
Limitations on existing rPPG Methods



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

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

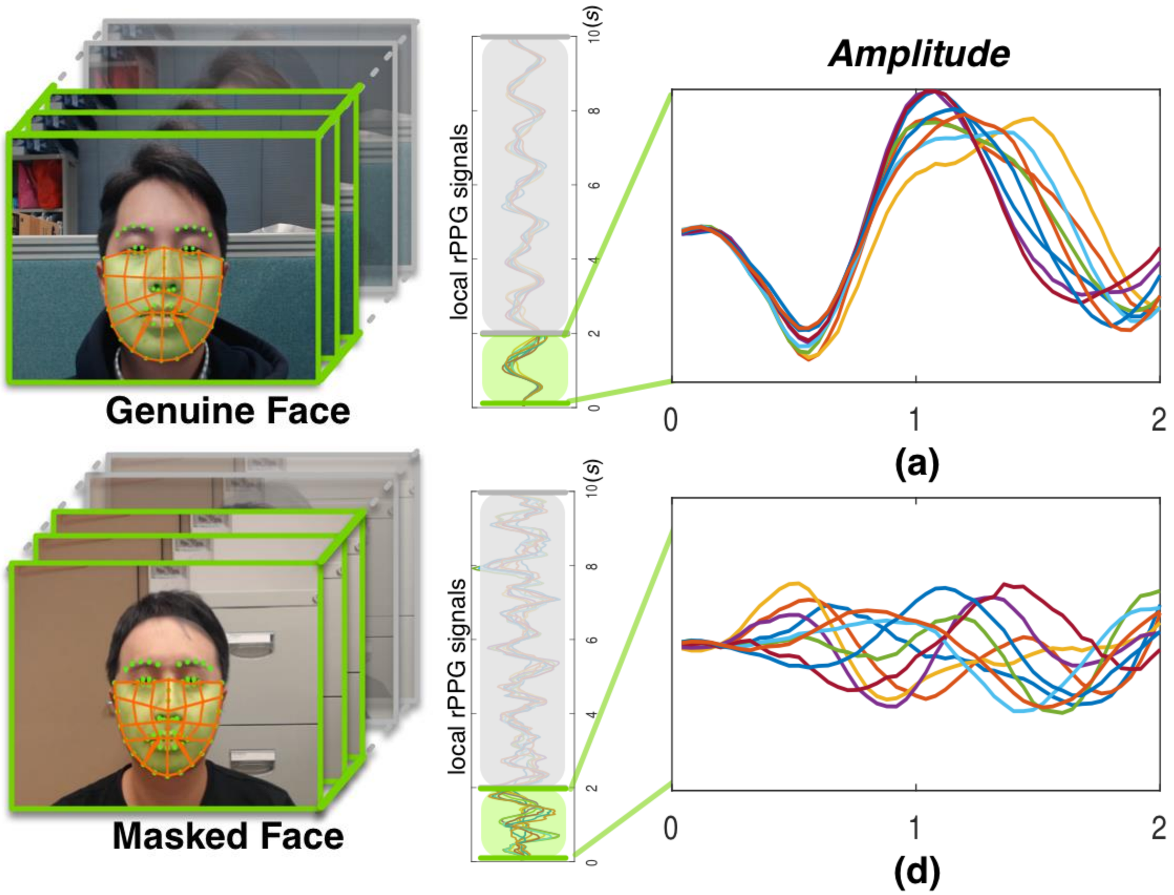
Temporal Similarity Analysis of rPPG (TSrPPG) for Fast 3D Mask Face PAD



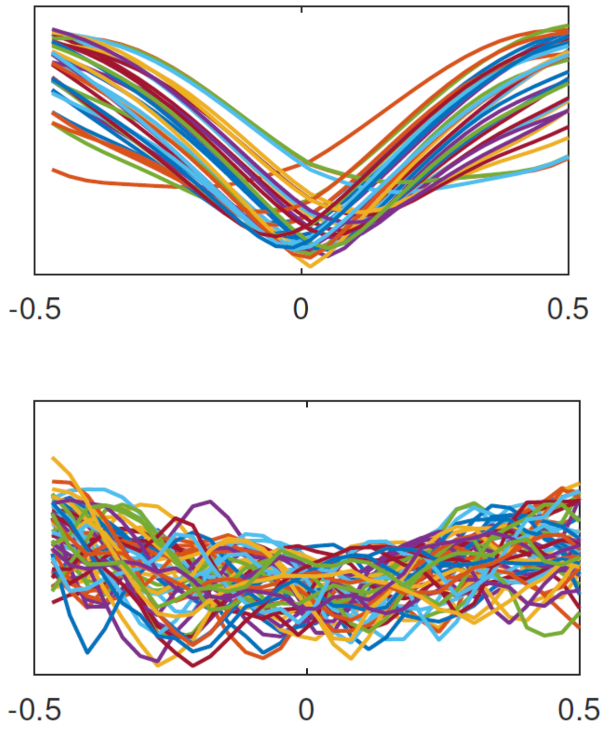
Reference:

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.

The proposed TSrPPG



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

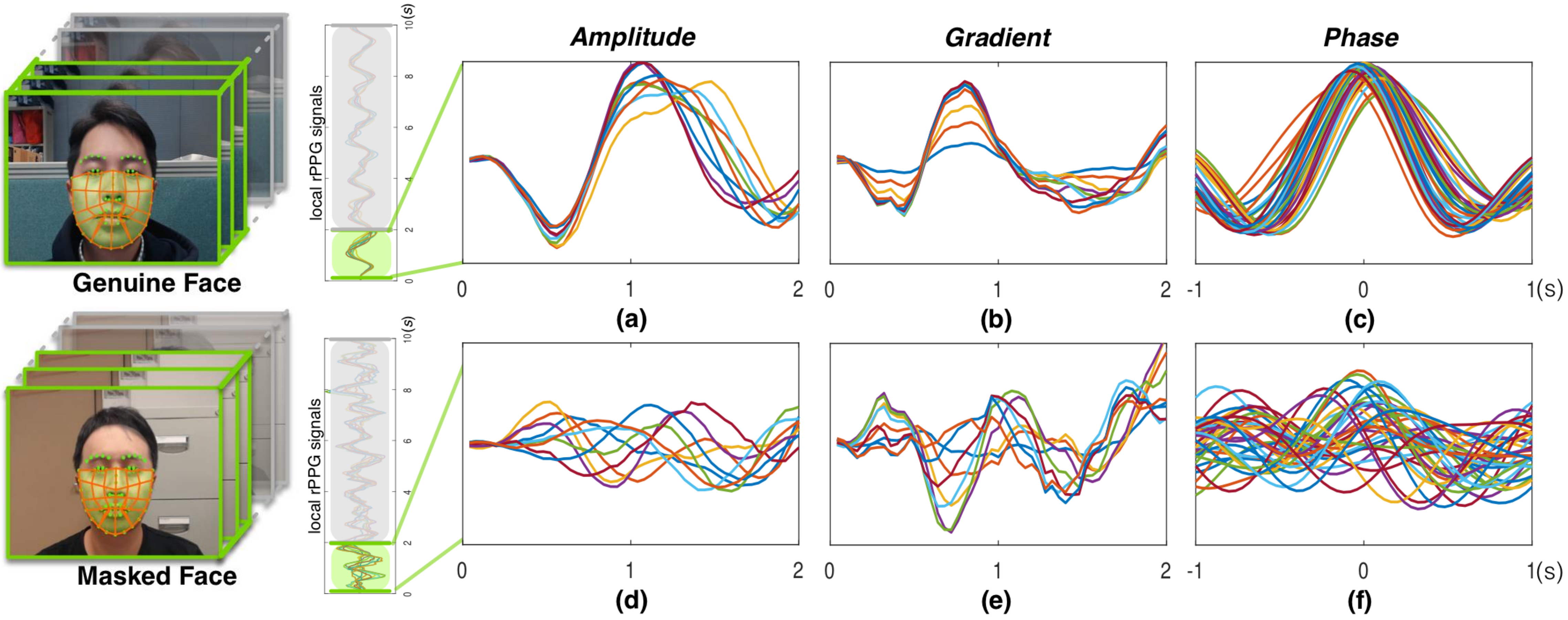


Extract features on the result pattern

→ Min, Mean, Std (… etc.)

The proposed TSrPPG

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



pt
nt

Final result is obtained through score-level-fusion

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

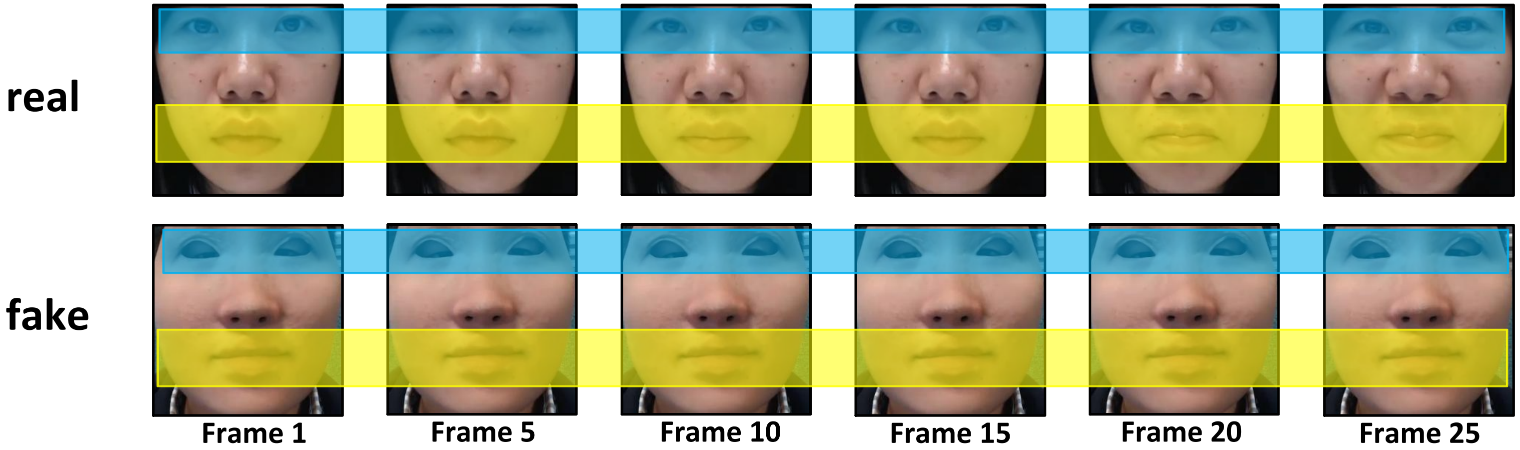
Deep Dynamic Feature Learning Approach

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**

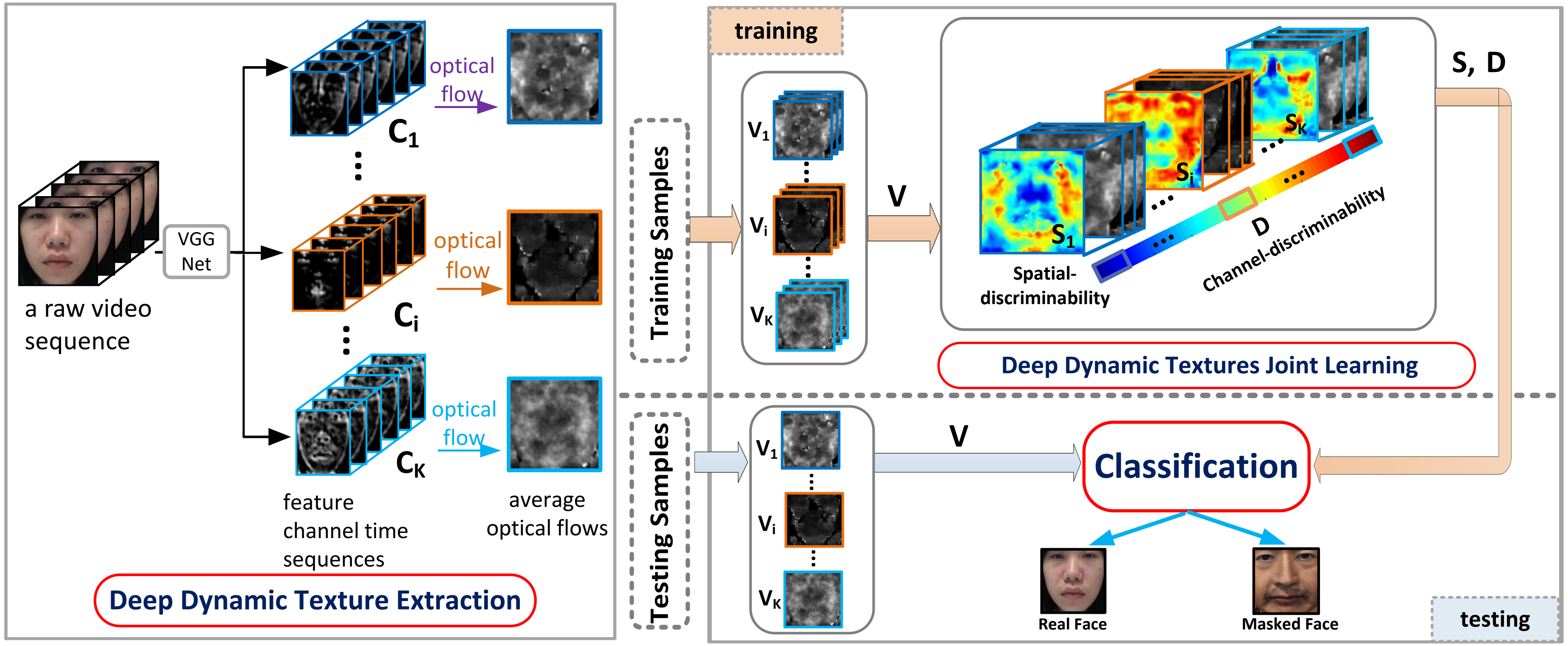


- Eye blinking
- Lip movements
- Some other facial components movements

Captured by dynamic textures

Joint Discriminative Learning of Deep Dynamic Textures

[IJCB 2017, TIFS 2019]



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

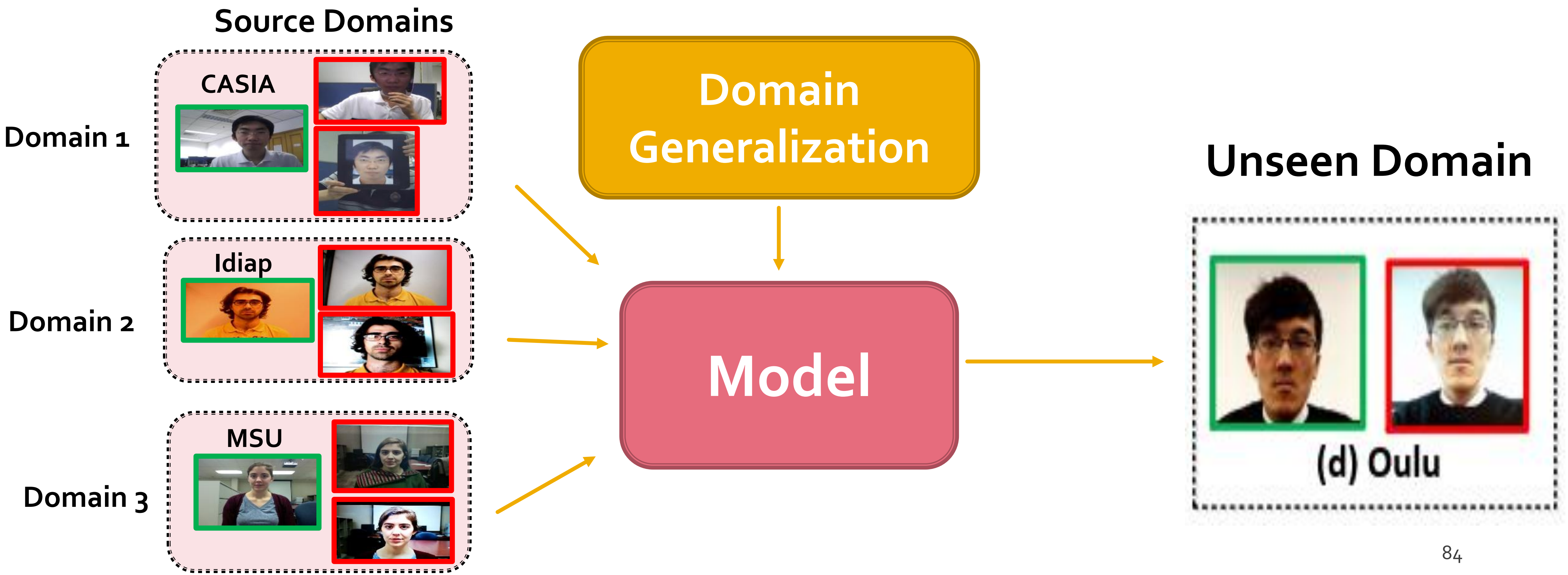
Domain Generalization Approach

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.

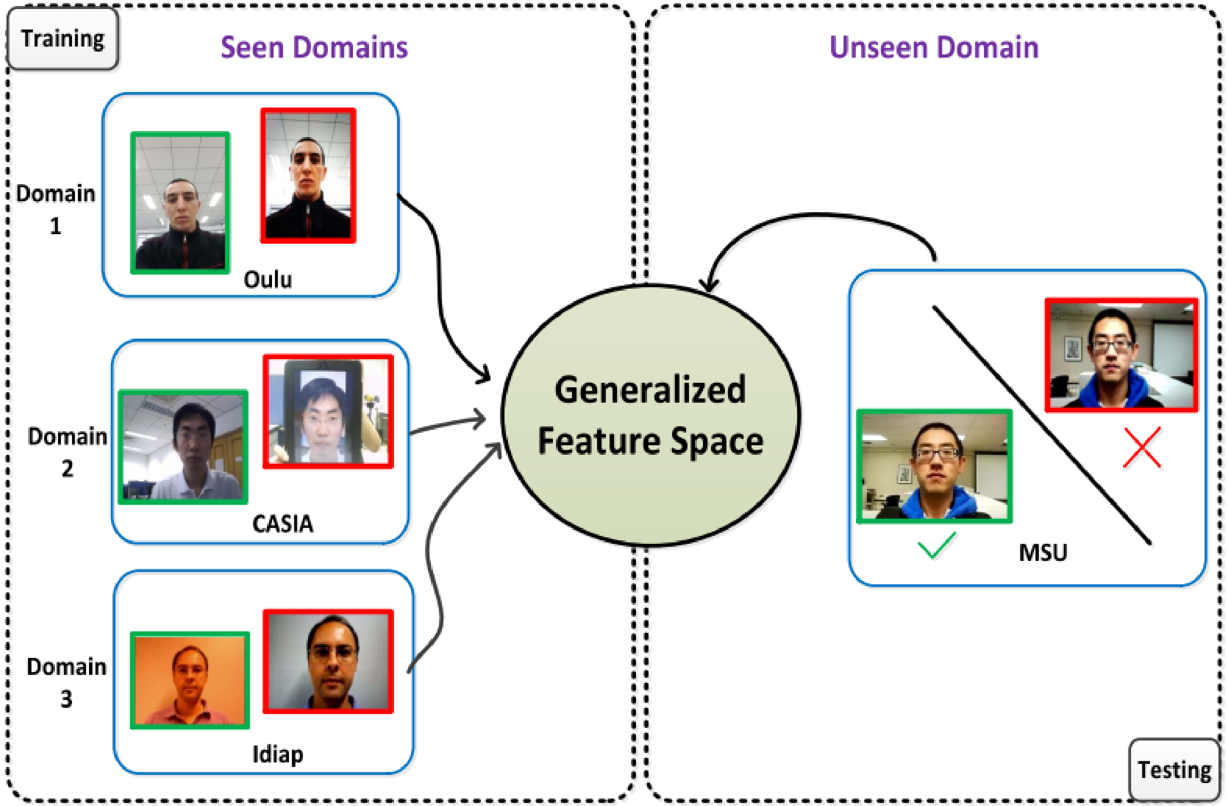
Multi-adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection [CVPR2019]

- **Domain Generalization:**



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.

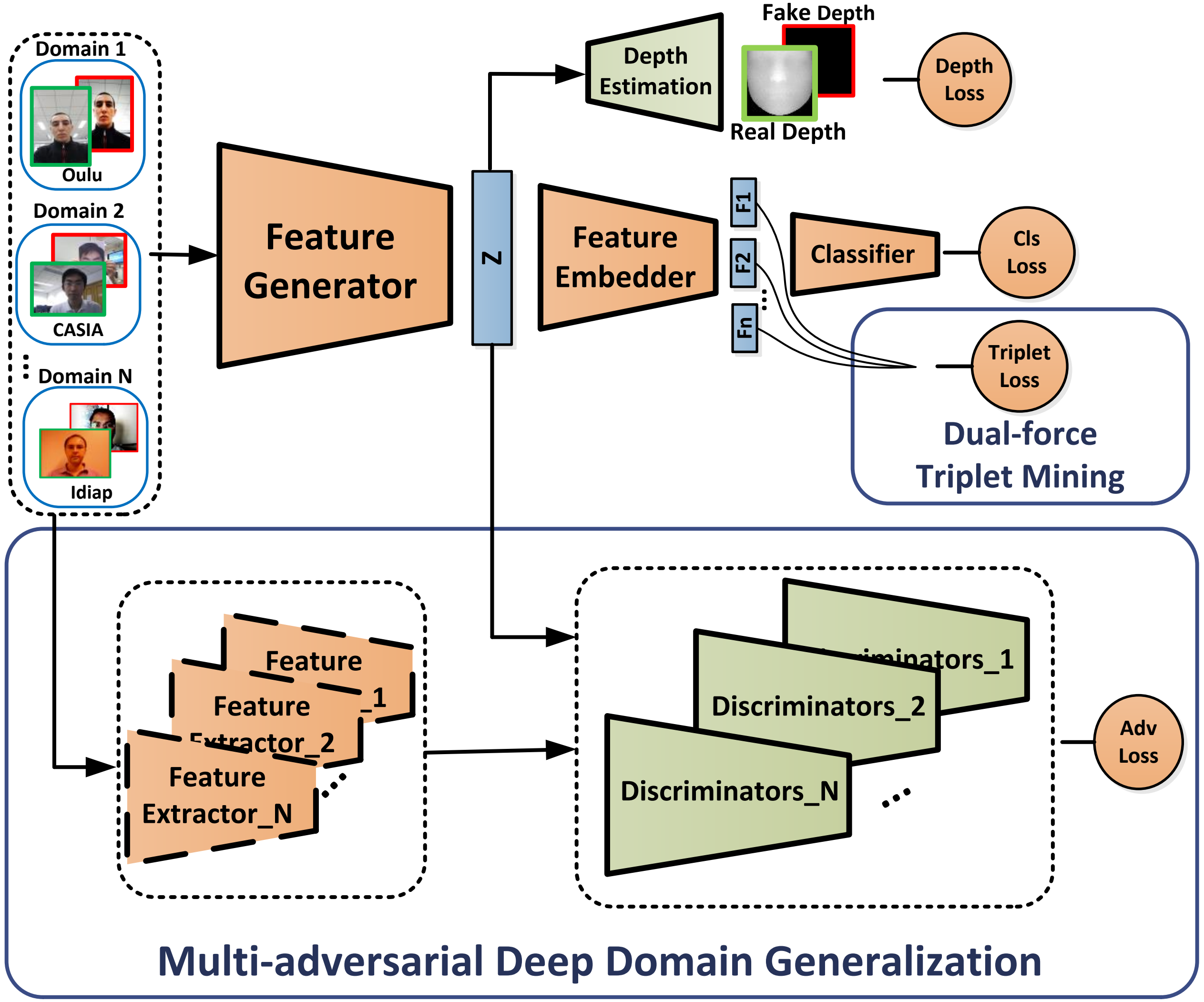
Multi-adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection [CVPR 2019]



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

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.

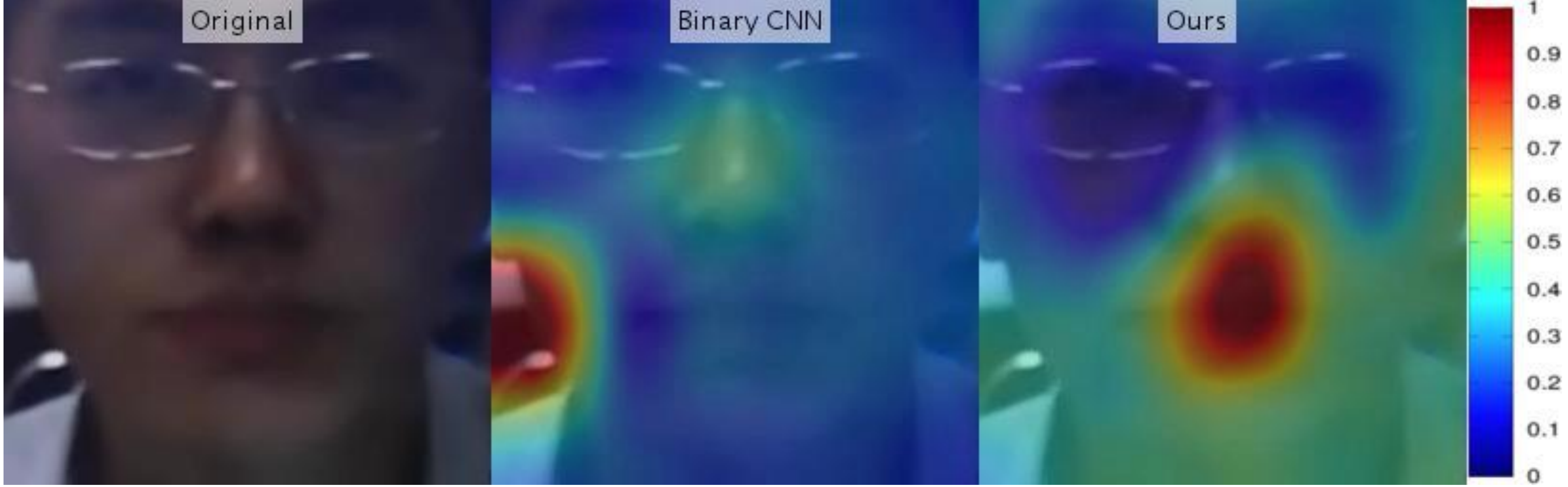
Multi-adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection [CVPR 2019]

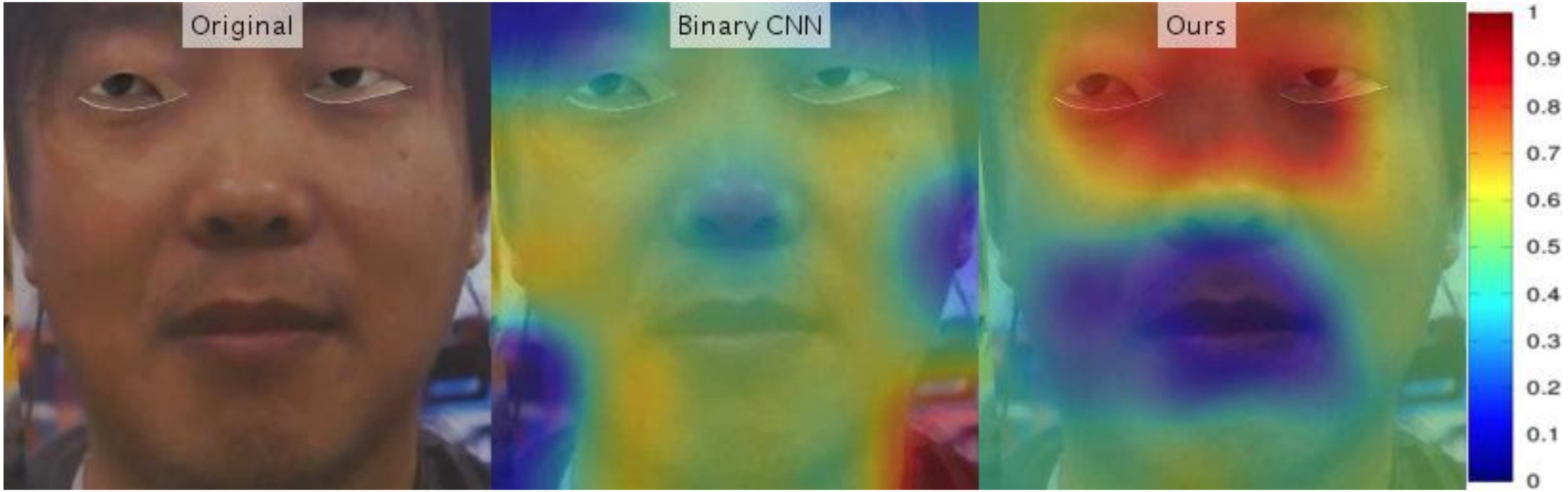


- A unified multi-adversarial discriminative deep domain generalization framework **(MADDG)**:

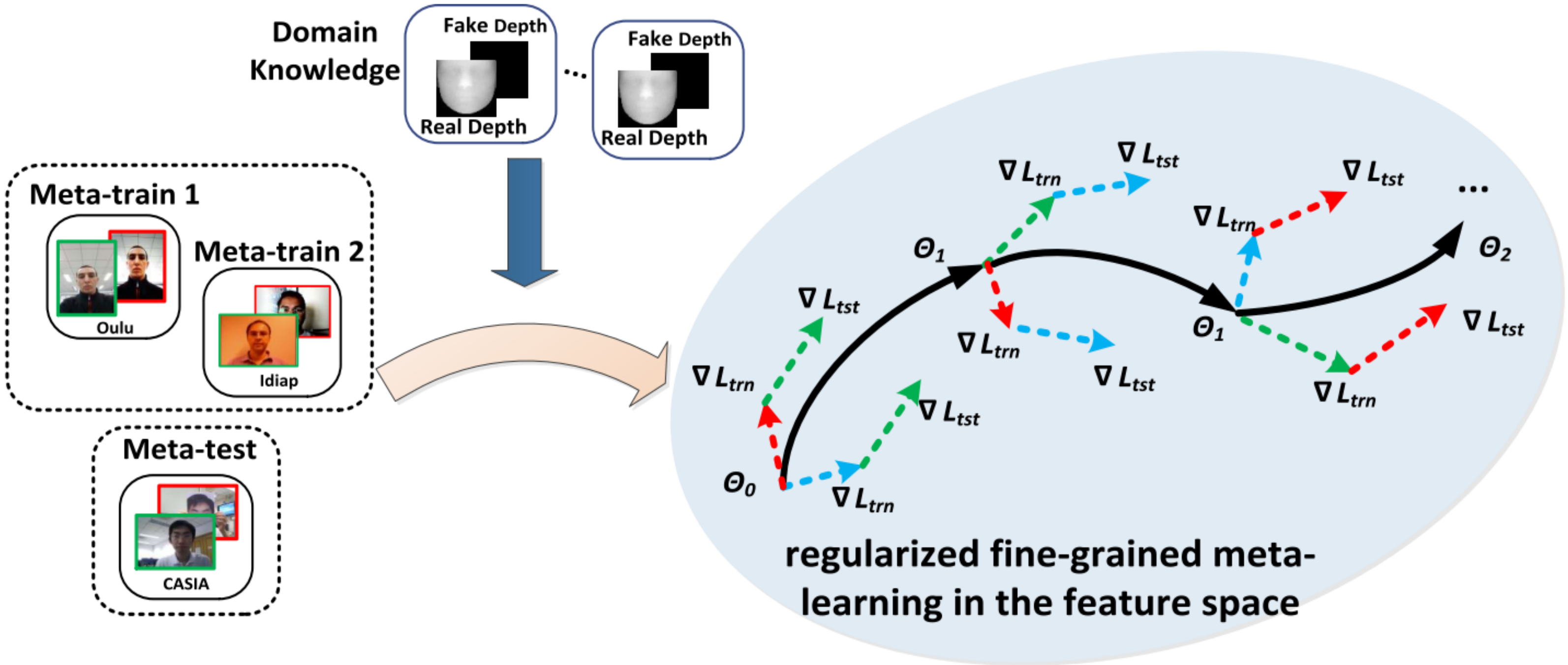
$$\min_{G,E,C,Dep}\ \max_{D_1,D_2,\ldots,D_N}\ \mathcal{L}_{MADDG} =$$

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


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, 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 ：
  - 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:

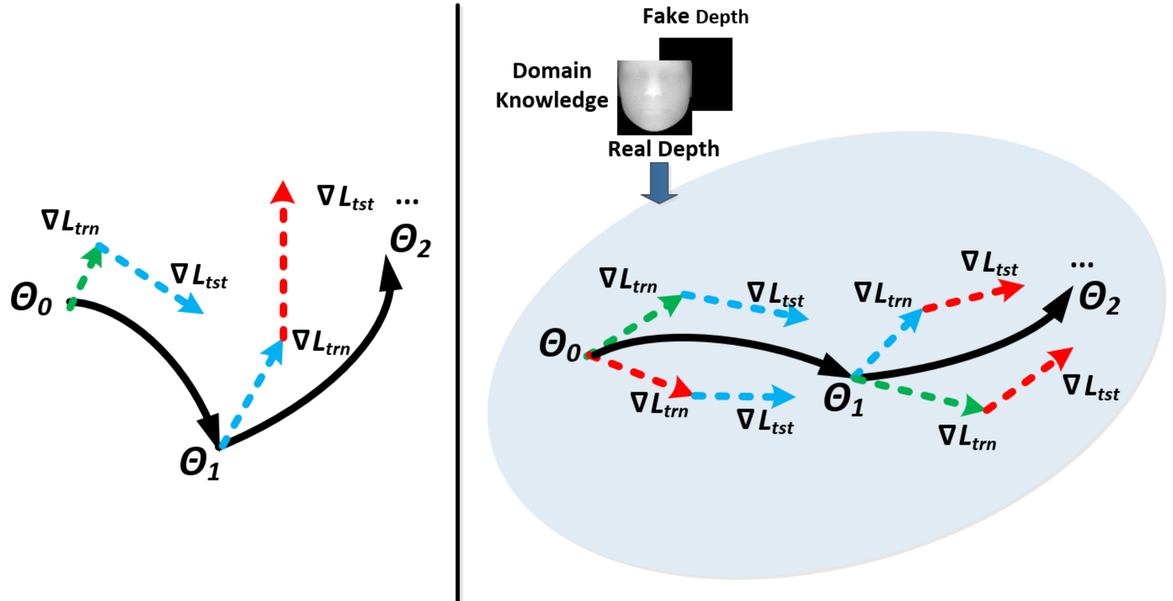
Coarsely divide multiple source domains into **two groups** to form one aggregated meta-train and one aggregated meta- test domains in each iteration of meta-learning

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

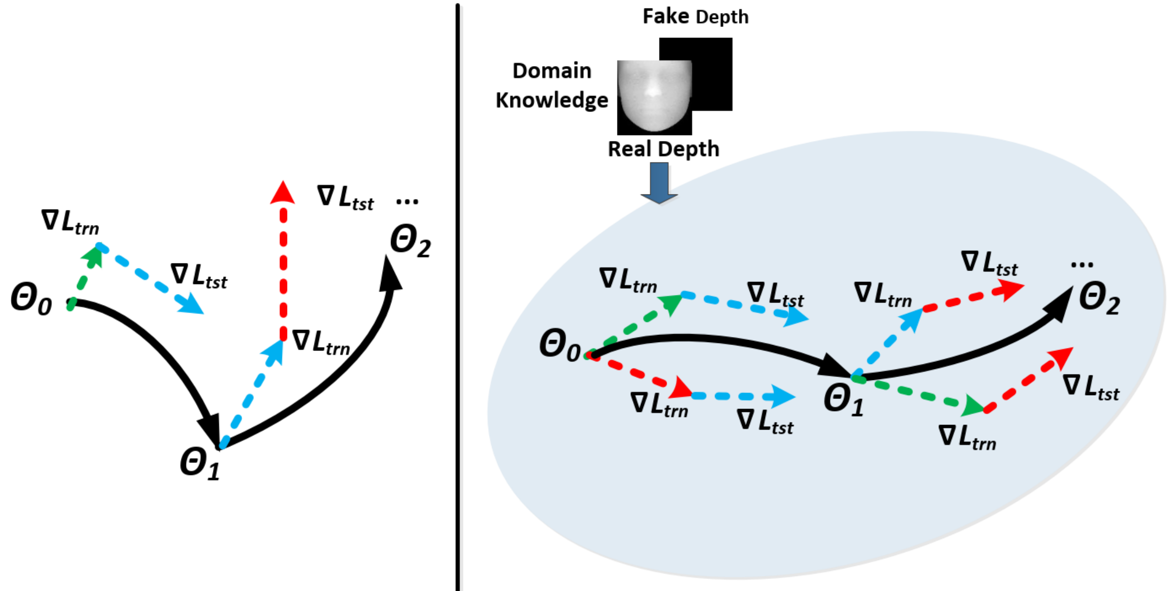
Meta-learning is conducted in the feature space regularized by the auxiliary supervision of domain knowledge.

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

R Shao, 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

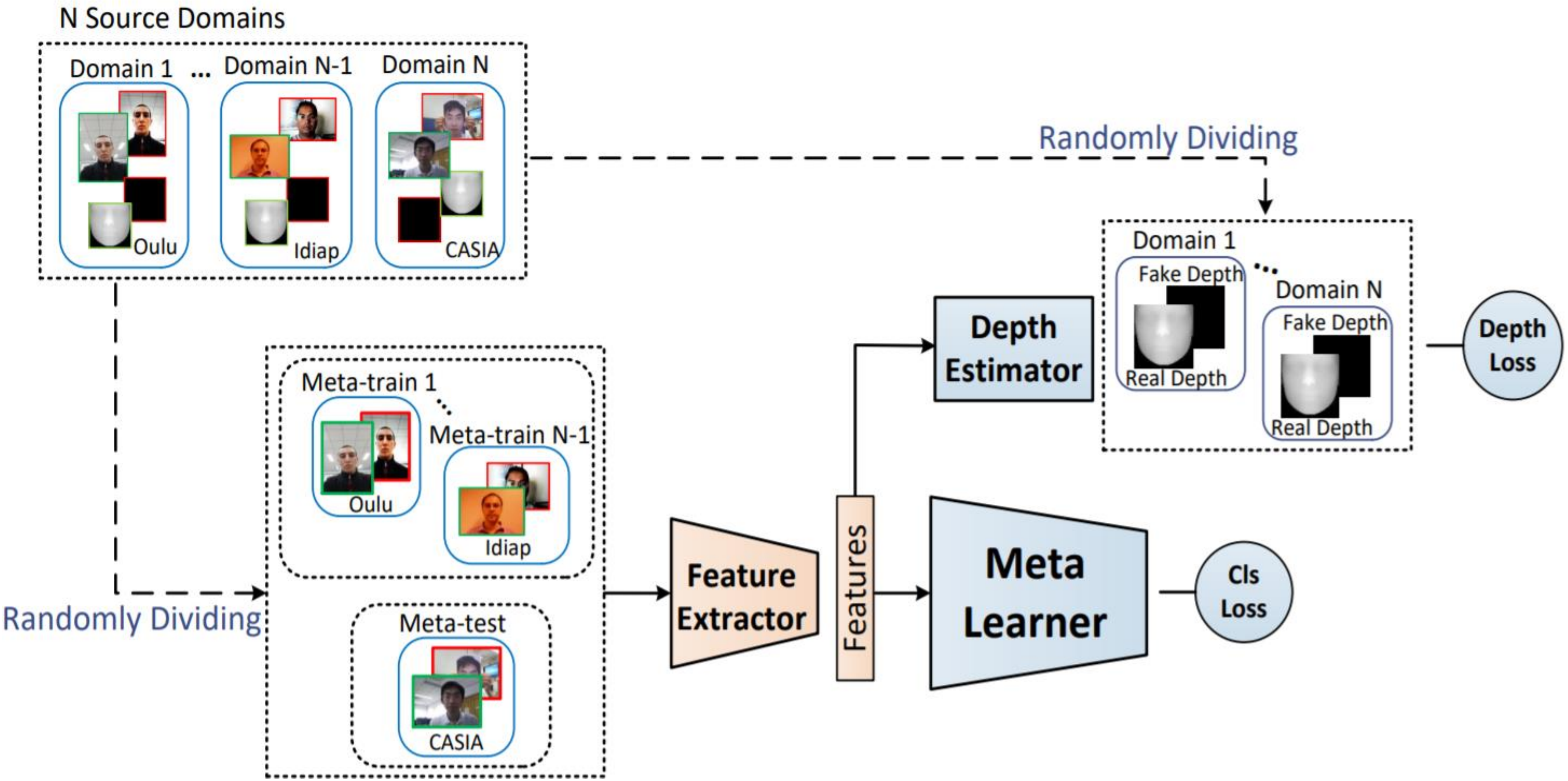
- For second issue:

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

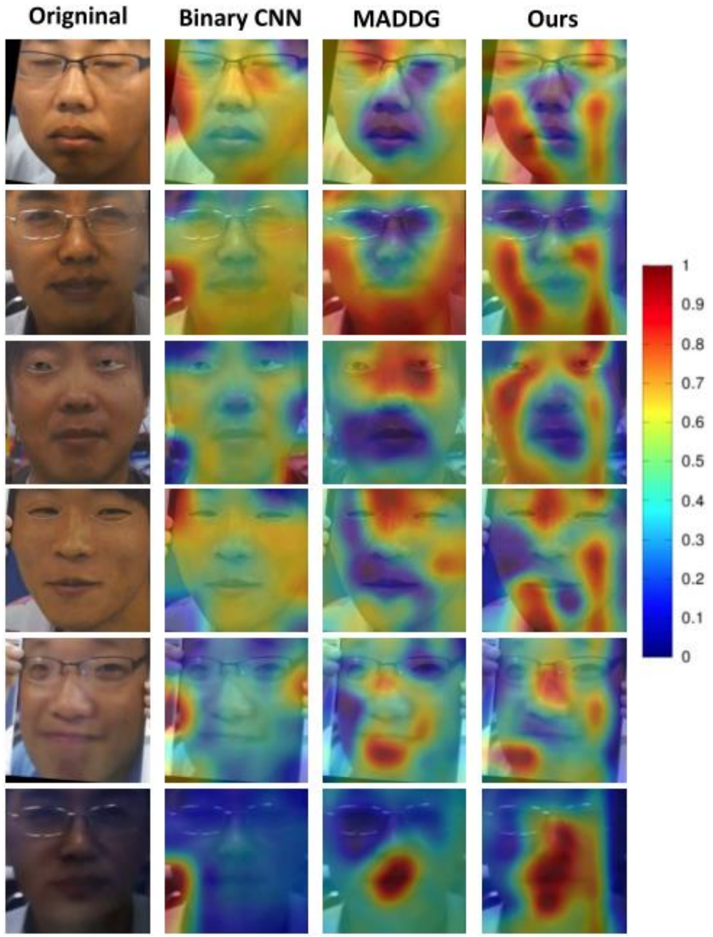
Regularized Fine-grained Meta Face Anti-spoofing [AAAI2020]



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))

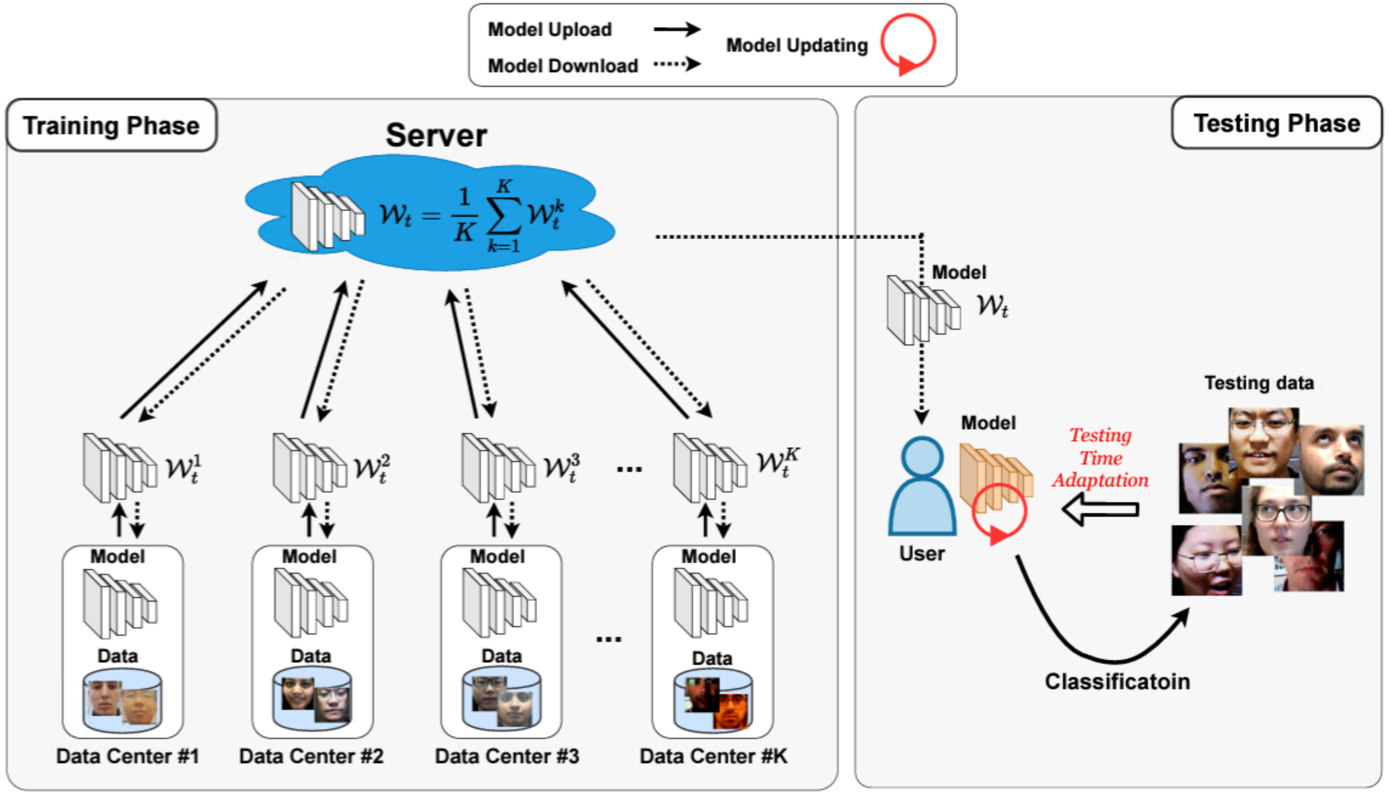


- Binary_CNN pays most attention to extracting the differentiation cues in the background (row 1-2) or on paper edges/holding fingers (row 3-5).

- Our method is more able to focus on the region of internal face for searching generalized differentiation cues.

Federated Face PAD with Test-Time Adaptation [FG2021]

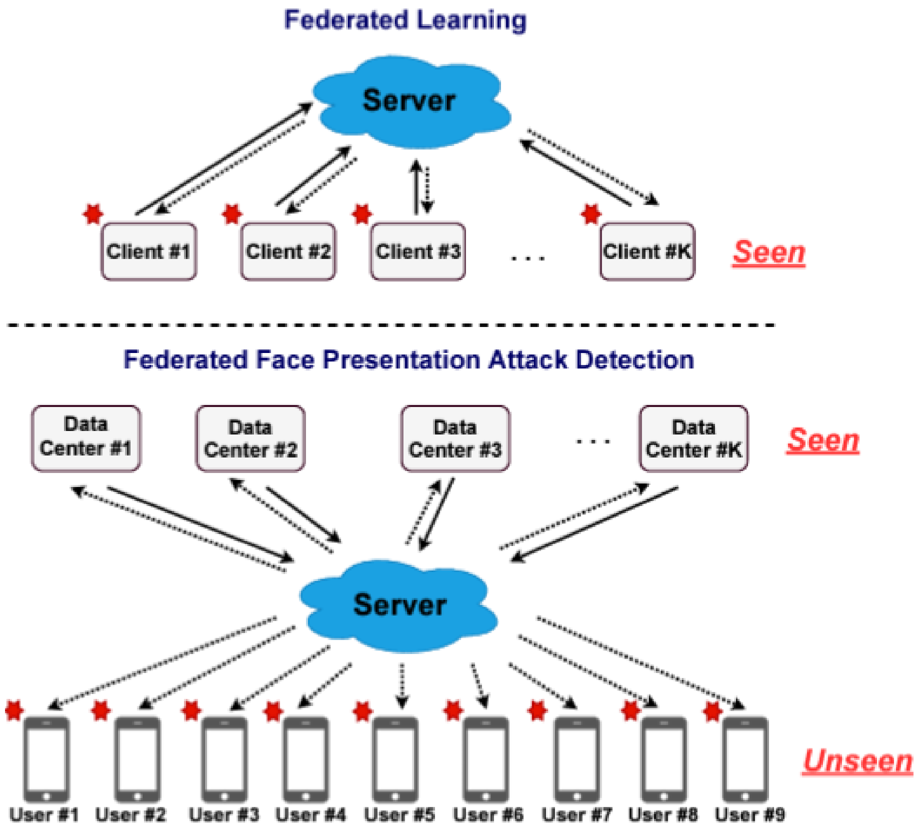
- Conduct test-time adaptation by minimizing the entropy of face PAD model prediction on the testing data.

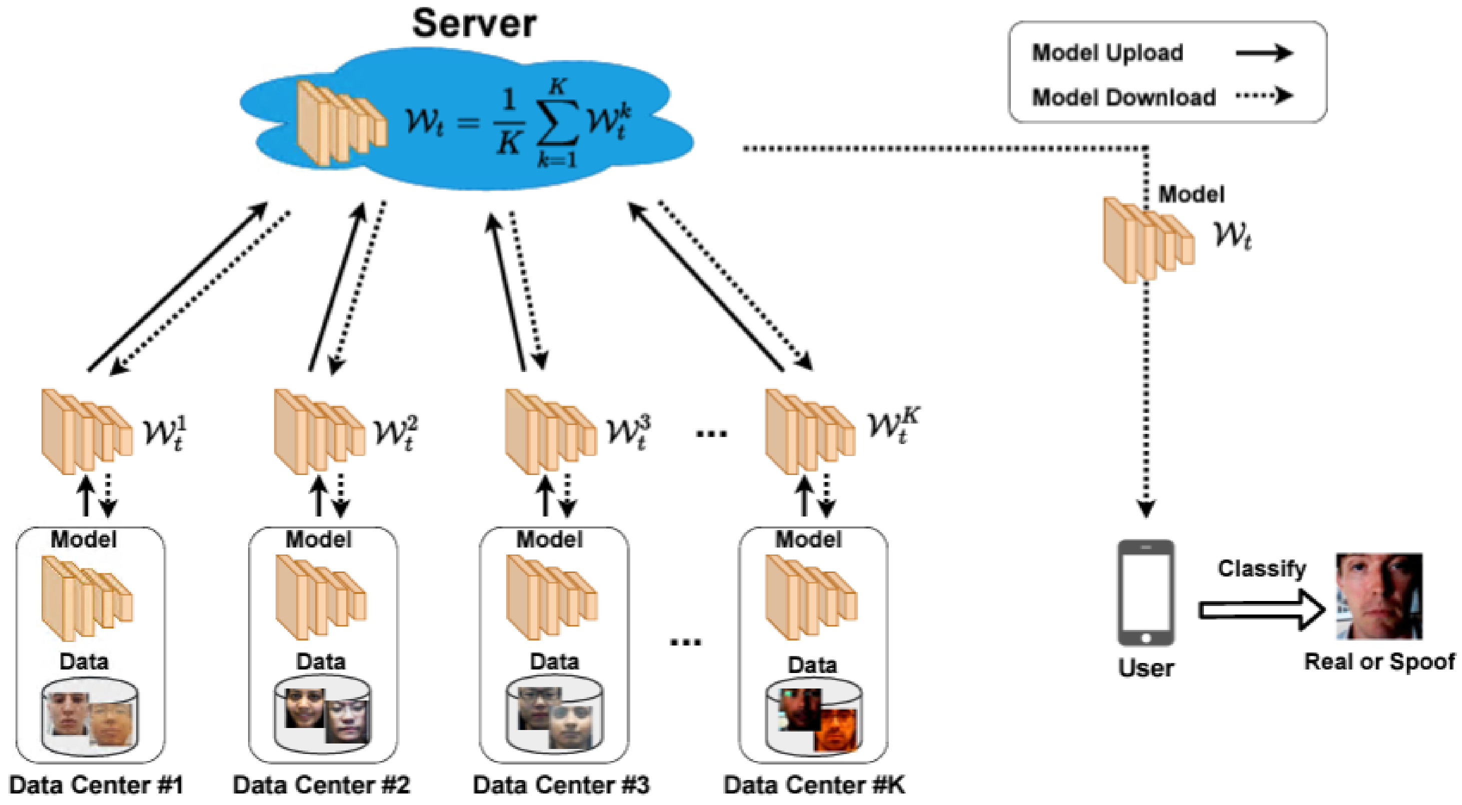


R Shao, B Zhang, P C Yuen, V M Patel, "Federated Test-Time Adaptive Face Presentation Attack Detection with Dual-Phase Privacy Preservation", *IEEE International Conference on Automatic Face & Gesture Recognition (FG)*, Dec 2021.

Federated Face PAD (Under Review)

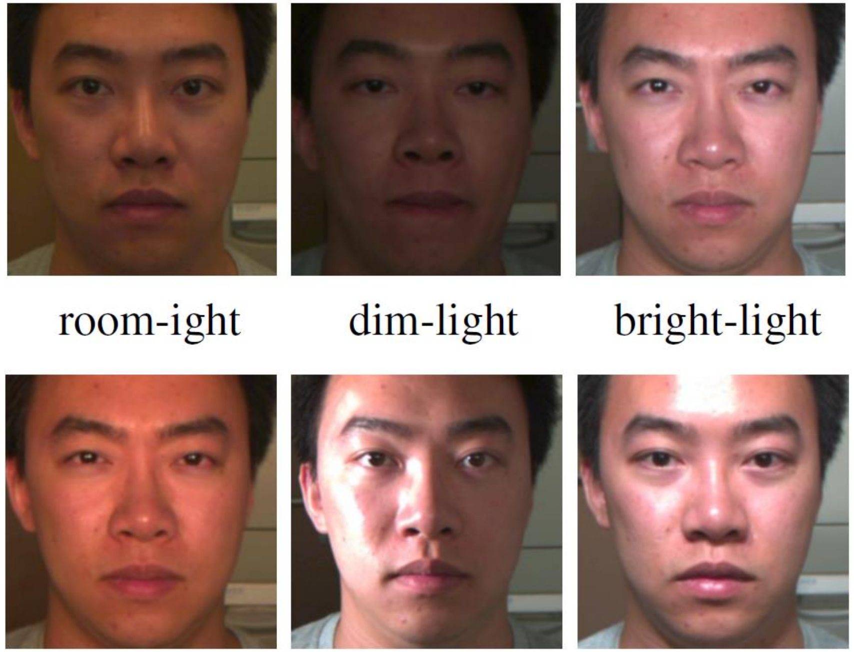
- Server learns a global model by iteratively aggregating model updates from all data centers without accessing private data in each of them





Our dataset: HKBU-MARs

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



room-ight dim-light bright-light

warm-light sidelight top-light

(a) ThatsMyFace

(b) REAL-f

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

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.