

# Face Recognition System Security: Anti-spoofing and Template Protection

P C Yuen

Department of Computer Science  
Hong Kong Baptist University

# Outline

1. Background and Motivations
2. Face Presentation Attack Detection
3. Face Template Protection (very brief)
4. Conclusions

# Biometrics

- Deployed practical applications



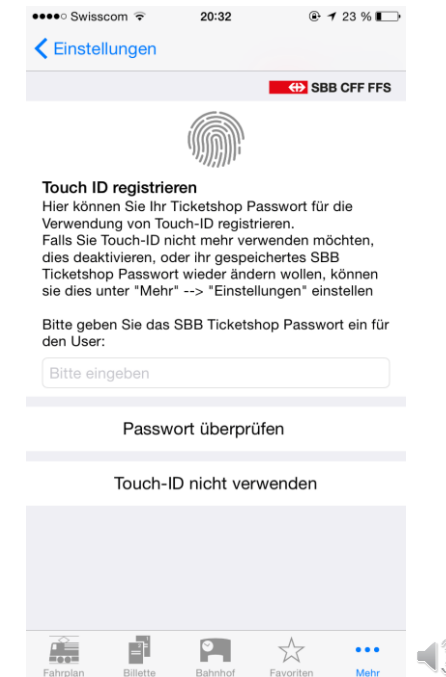
Border Control



Door Access Control



Touch ID (iPhone)



SBB for buying ticket

# Face Biometrics

## ■ 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, 11:51am

COMMENTS: 2



Source: china.com and iomniscient.com



# E-payment using Facial Recognition Technology in China

# Face Biometrics



Facial Mapping

Face ID is enabled by the TrueDepth camera and is simple to set up. It projects and analyzes more than 30,000 invisible dots to create a precise depth map of your face.

## FaceID in iPhone X

Announced on 12 September 2017

“With a simple glance, Face ID securely unlocks your iPhone X. You can use it to *authorize purchases from the iTunes Store, App Store, iBooks Store, and payments with Apple Pay*. Developers can also allow you to use Face ID to sign into their apps. ....”

## 3D Face Recognition:

Employed Structured-light 3D technology

Your face is your  
secure password.



With Face ID, iPhone X unlocks only when you're looking at it. It's designed to resist spoofing by photos or masks. Your facial map is encrypted and protected by the Secure Enclave. And authentication happens instantly on the device, not in the cloud.

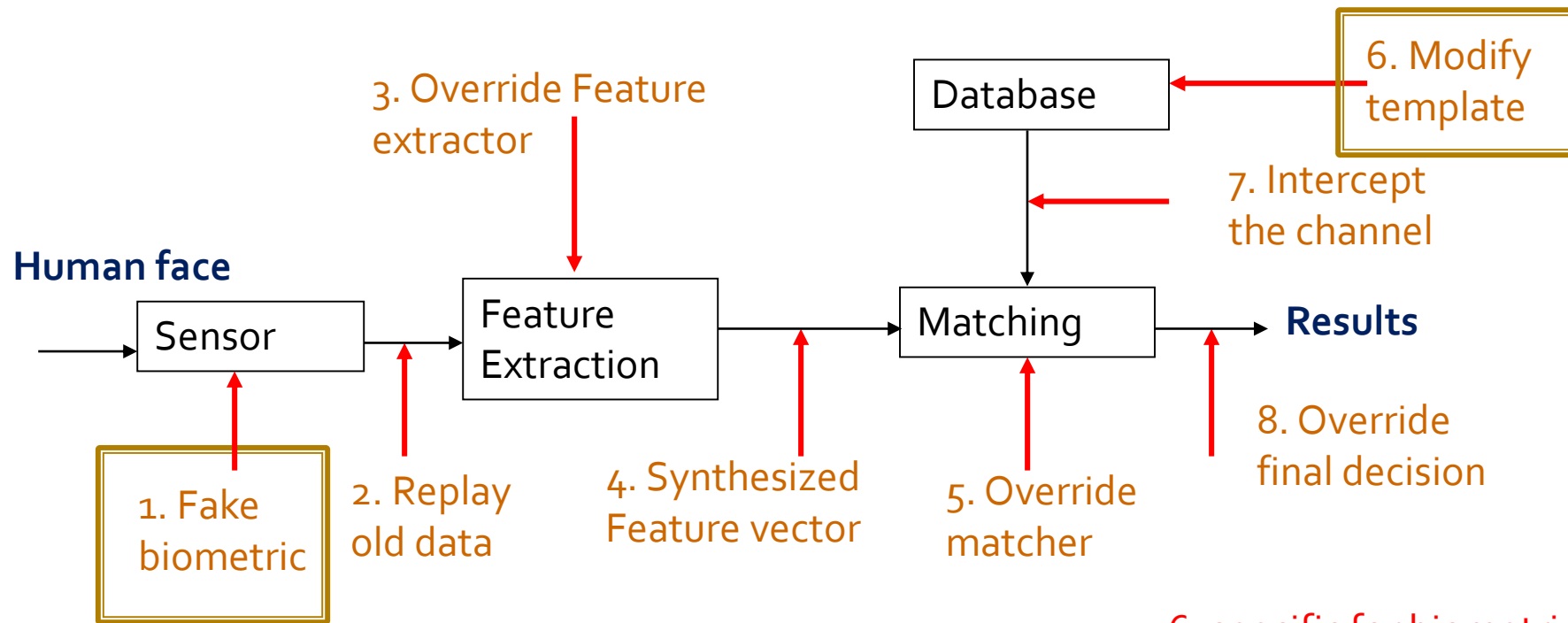


**What happens if  
a face recognition system is NOT secure?**



# 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

**Part I:**  
**Face Presentation Attack Detection**  
**(a.k.a. Face Anti-Spoofing)**

# Background and Motivations

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



✓ Real Face



✗ Prints Attack



✗ Replay Attack

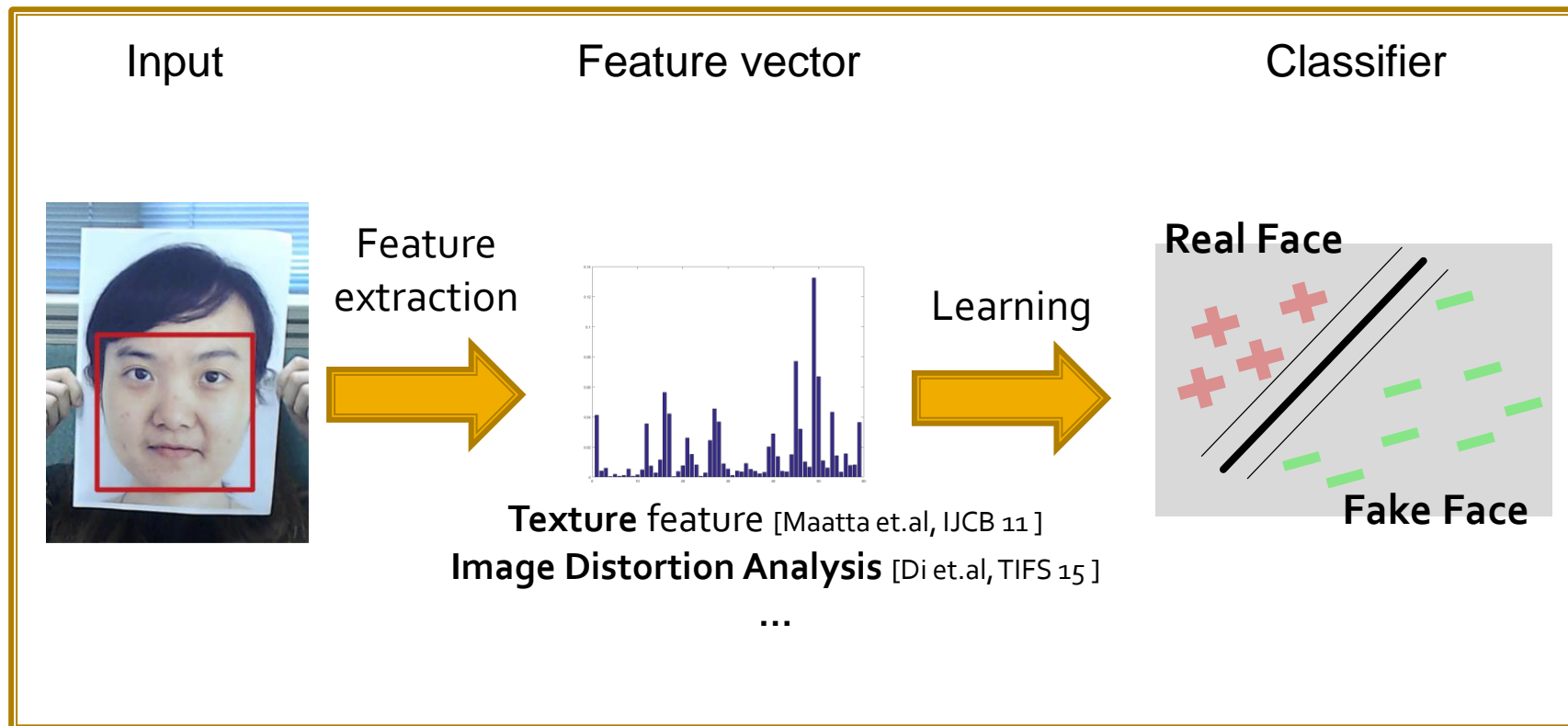


✗ 3D Mask Attack



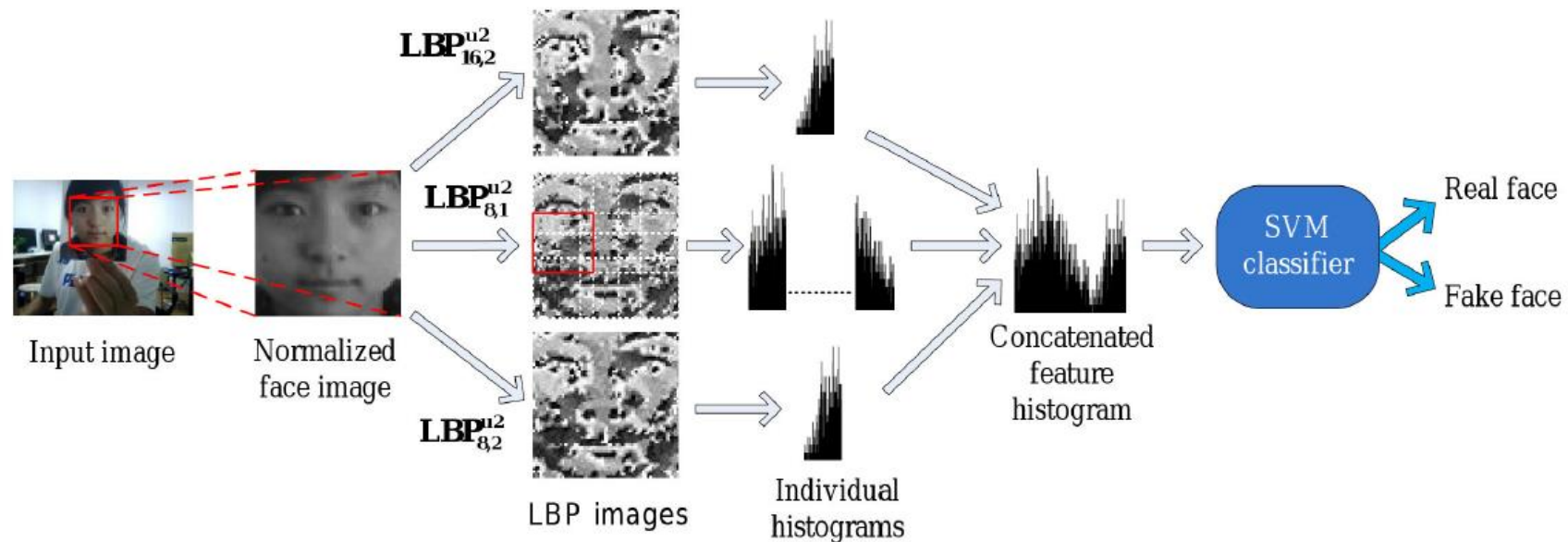
# Image and Video Face Anti-spoofing

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



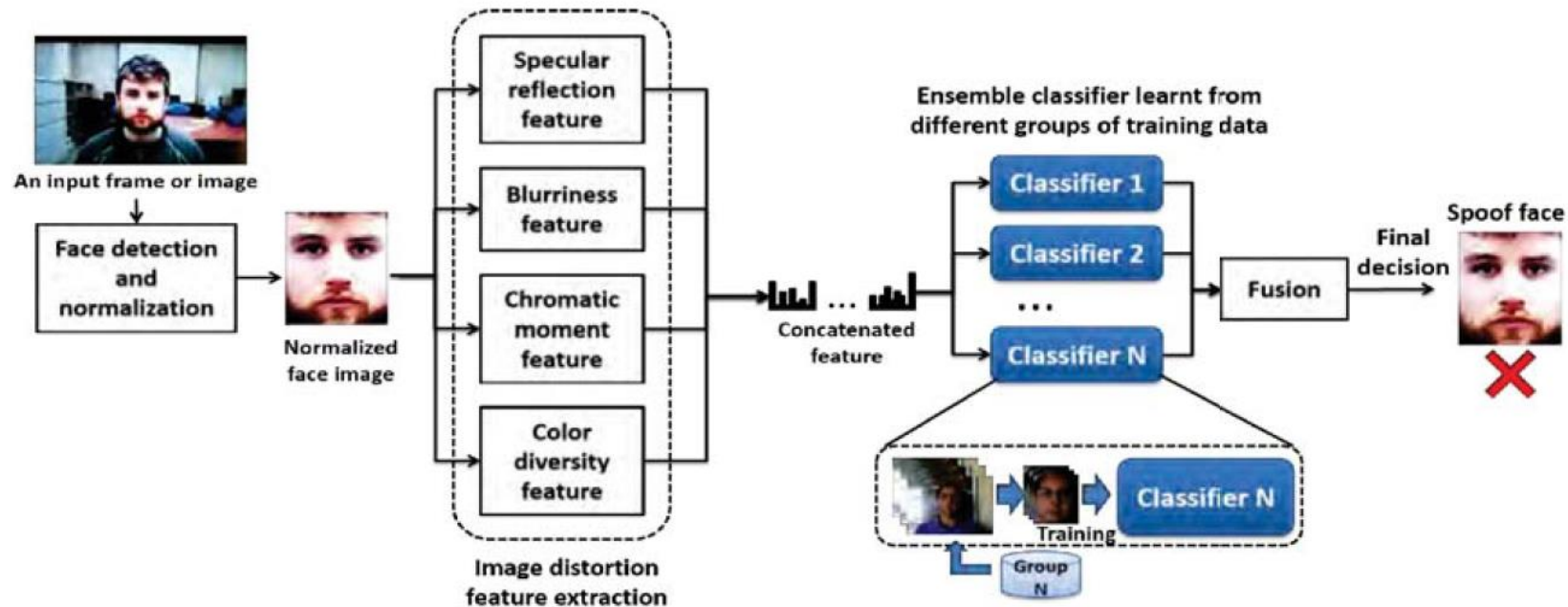
# Image and Video Face Anti-spoofing

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



# Image and Video Face Anti-spoofing

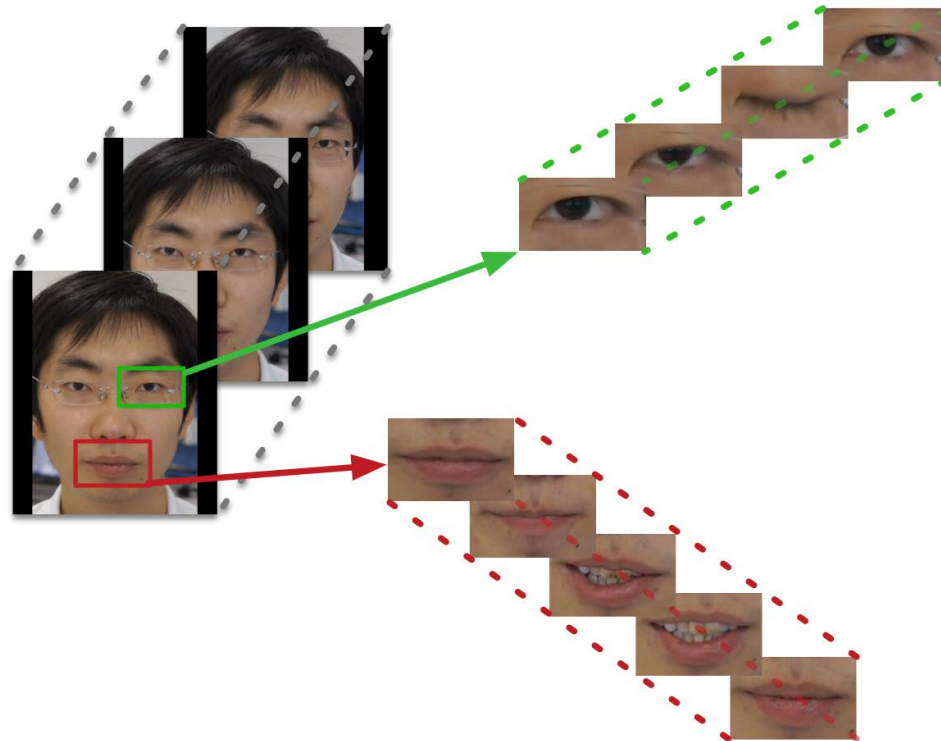
- Anti-spoofing approach: Appearance-based
  - Spoof media (prints and screen) has specific quality defects



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

# Image and Video Face Anti-spoofing

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



# Image and Video Face Anti-spoofing

- Anti-spoofing approach: Motion-based
  - **Eyeblick-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)

# Image and Video Face Anti-spoofing

- Performance on traditional face spoofing attack

<i>Pipelines</i>	<b>Replay Attack</b>		<b>Print attack</b>	
	<i>Dev</i>	<i>Test</i>	<i>Dev</i>	<i>Test</i>
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

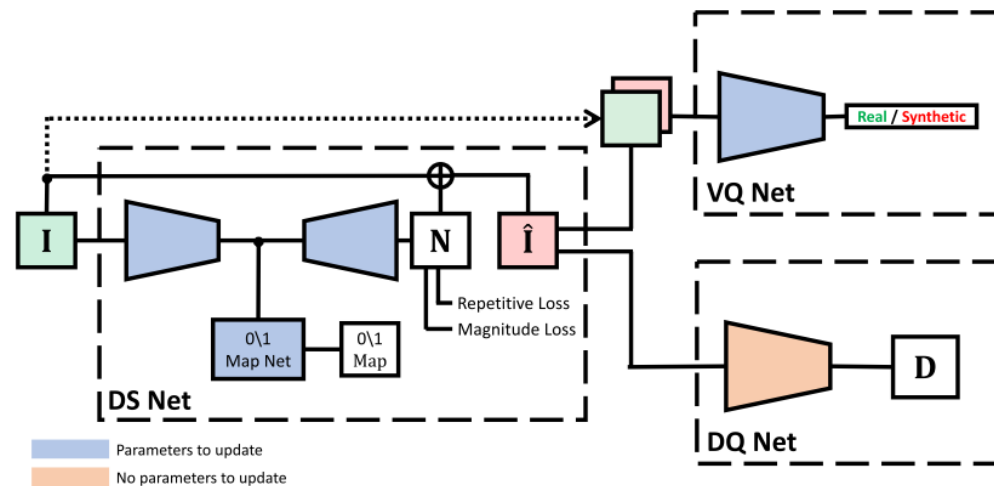
[S. Tirunagari et al., TIFS'15]



# Image and Video Face Anti-spoofing

## ■ Face de-spoofing approach

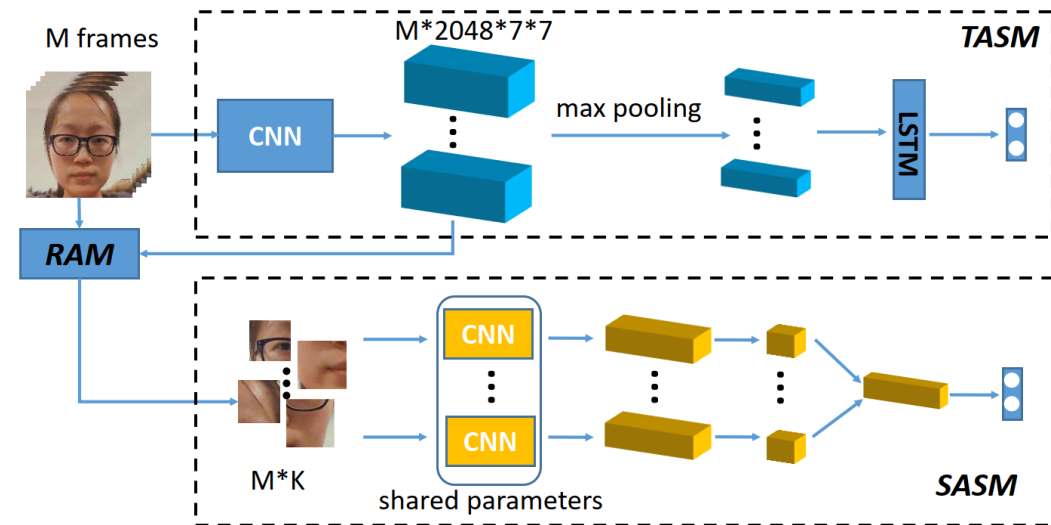
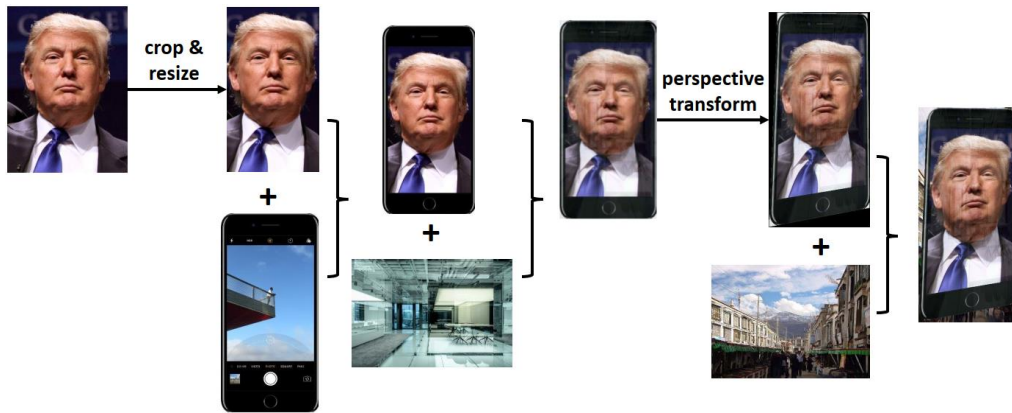
- Inversely decompose a spoofed face into a spoof noise and a live face, and then utilizing the spoof noise for classification.
- Real face: no spoof noise vs. Fake face: clear spoof noise



# Image and Video Face Anti-spoofing

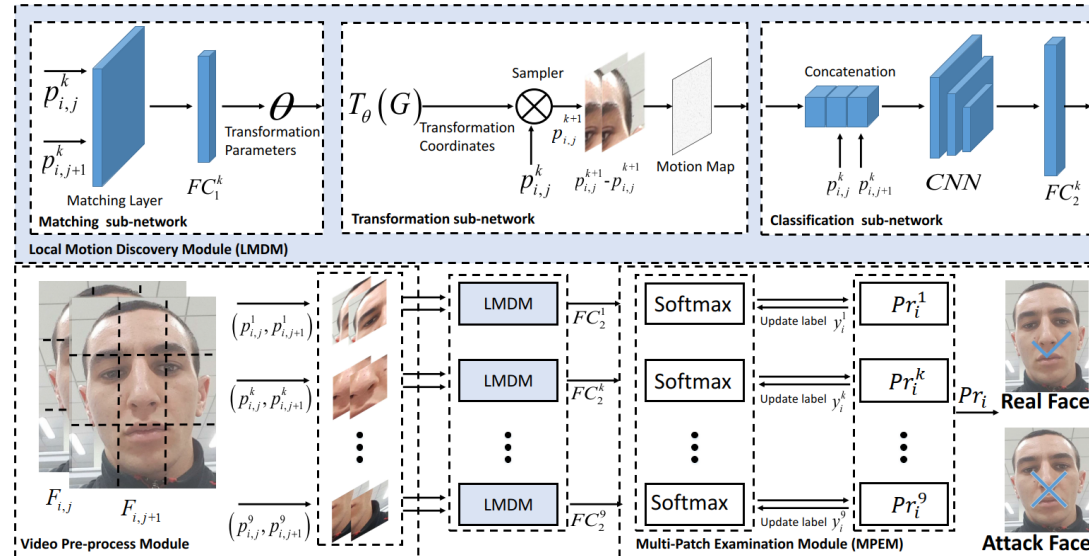
## ■ Spoof data synthesis approach

- Simulate digital medium-based face spoofing attacks to obtain a large amount of training data well reflecting the real-world scenarios
- Spatio-Temporal Anti-Spoof Network is proposed to consider both global temporal and local spatial cues



# Image and Video Face Anti-spoofing

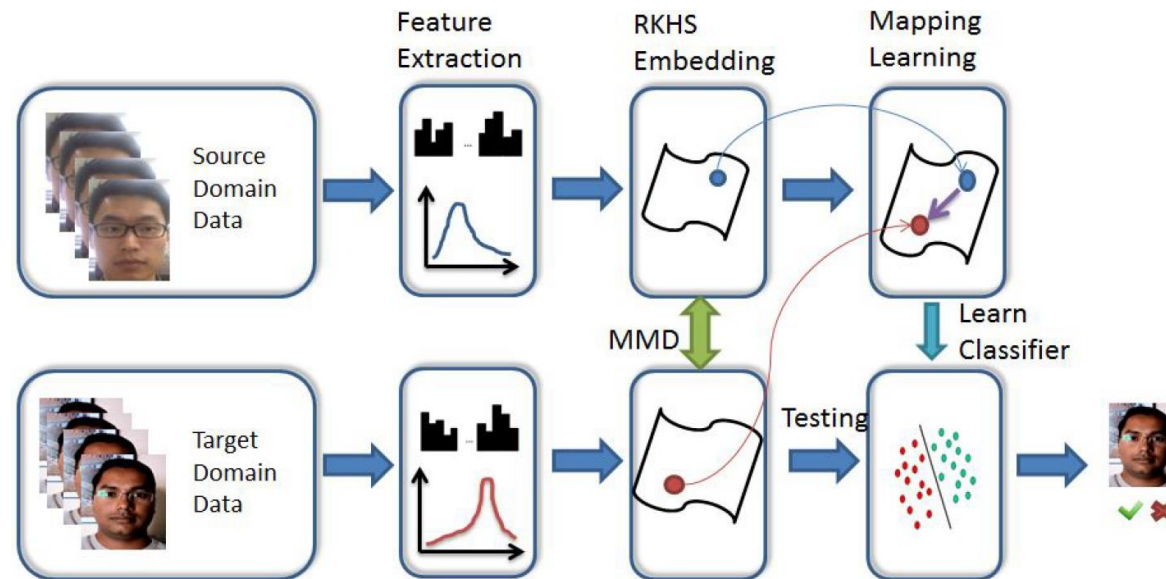
- Local homographic parameterization approach
  - Capture subtle motion difference between the facial movements from a planer screen and those from a real face
  - Multi-patch examination module enhances the recall rate of the attack videos



# Image and Video Face Anti-spoofing

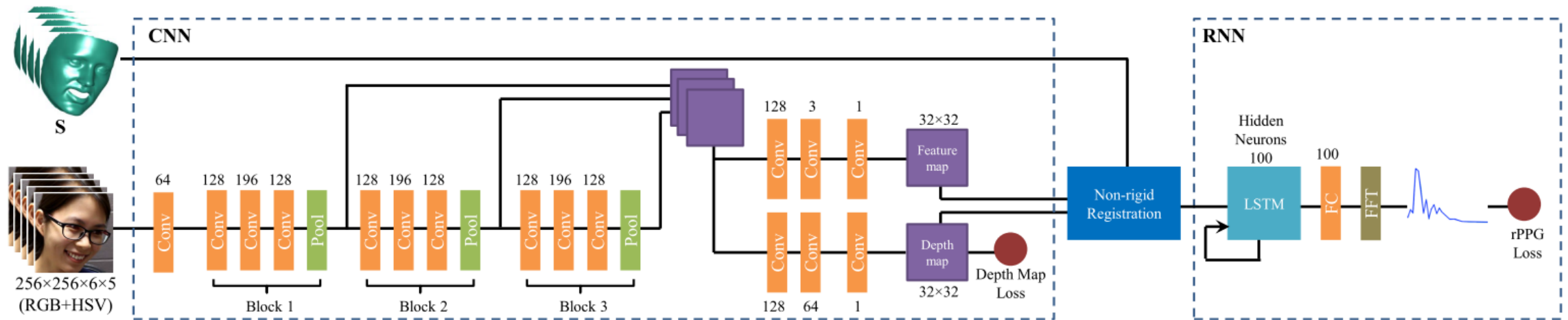
## ■ Domain adaptation approach

- An embedding function is imposed to map the data to a new space where source and target distribution similarity can be measured
- Maximum Mean Discrepancy between the source and target latent features is minimized



# Image and Video Face Anti-spoofing

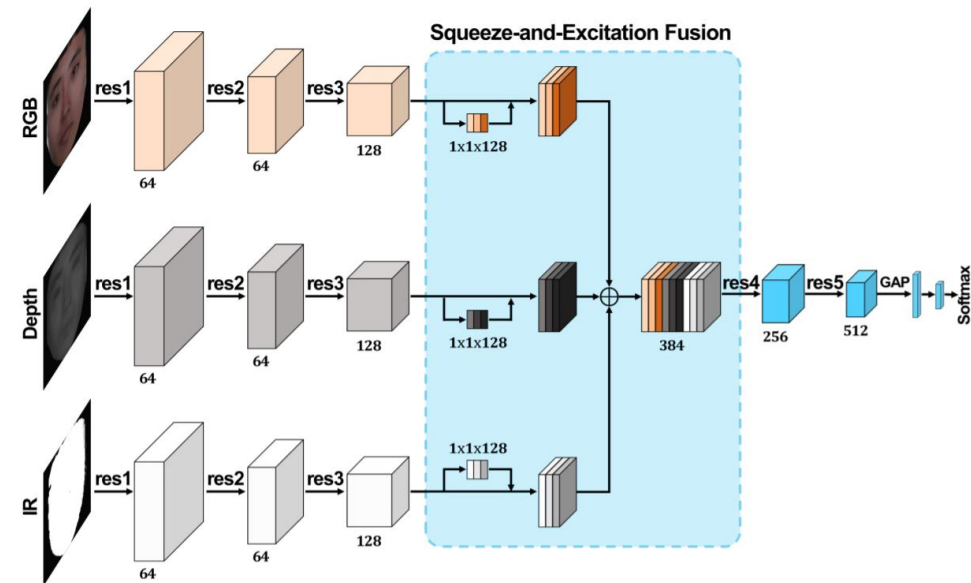
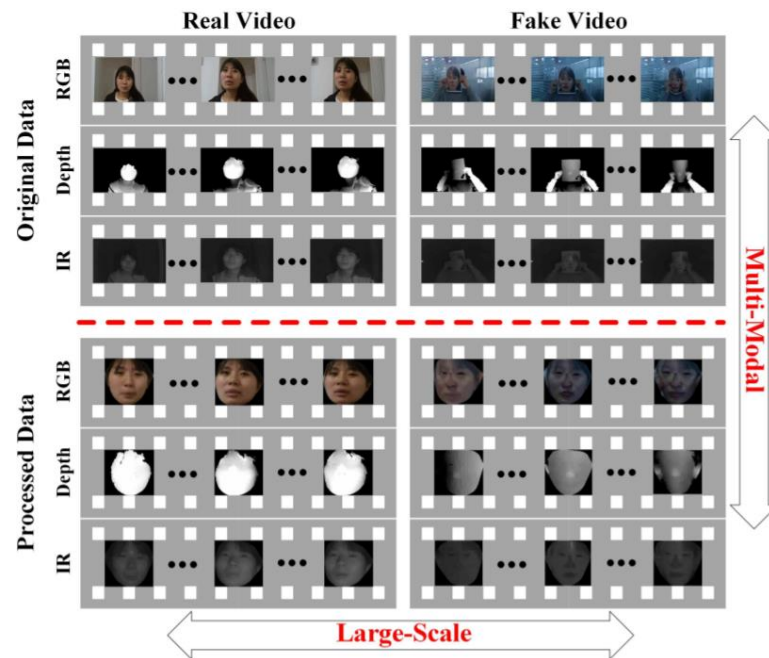
- Multiple modality approach
  - CNN: Learn different **face depth maps** at pixel-wise level +
  - RNN: Learn different **rPPG signals** with sequence-wise



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

# Image and Video Face Anti-spoofing

- Large-scale multi-modal dataset and benchmark
  - A large-scale multi-modal dataset, namely CASIA-SURF
  - A new multi-modal fusion method





# Face Presentation Attack Detection Challenge@CVPRW2020

## Results

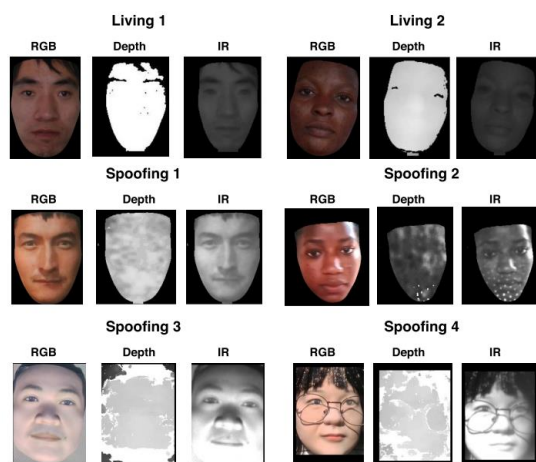


Figure 1. Examples of living and spoofing faces from CASIA-SURF CeFA dataset [21].

Chalearn Single-modal (RGB) Face Anti-spoofing Attack Detection Challenge Results (Rank by ACER) at CVPR 2020					
Leader Name, Affiliation	Team	APCER (Avg±Std)	BPCER (Avg±Std)	ACER (Avg±Std)	Rank
Alexander Parkin, visionlabs	VisionLabs	0.11±0.11	5.33±2.37	<b>2.72±1.21</b>	<b>1</b>
Zitong Yu, OULU unv.	BOBO	7.18±3.74	2.50±0.50	<b>4.84±1.79</b>	<b>2</b>
Jiachen Xue, Horizon	harvest	4.74±2.62	13.83±2.55	<b>9.28±2.28</b>	<b>3</b>
Zhang Tengpeng, CMB	ZhangTT	5.40±2.10	18.91±7.88	12.16±2.89	4
Xinying Wang, Newland Inc.	newland_tianyan	15.66±13.33	11.16±15.67	13.41±3.77	5
Wenwei Zhang, huya	Dopamine	24.59±9.37	2.50±3.12	13.54±3.95	6
Jin Yang, HUST	IecLab	33.16±5.76	6.08±0.72	19.62±2.59	7
Li-Ren Hou, Chunghwa Telecom	Chunghwa Telecom Lab.	24.66±5.16	19.00±8.69	21.83±1.82	8
Guoqing Wang, ICT	Wgqtmac	51.57±17.24	0.66±0.94	26.12±8.15	9
Yang, Qing, Intel	Hulking	45.00±11.07	19.50±13.27	32.25±3.18	10
Qiudi	dqiu	47.16±22.62	29.00±12.13	38.08±15.57	11
Chalearn Multi-modal Face Anti-spoofing Attack Detection Challenge Results (Rank by ACER) at CVPR 2020					
Leader Name, Affiliation	Team	APCER (Avg±Std)	BPCER (Avg±Std)	ACER (Avg±Std)	Rank
Zitong Yu, OULU unv.	BOBO	1.05±0.62	1.00±0.66	<b>1.02±0.59</b>	<b>1</b>
Zhihua Huang, USTC	Super	0.62±0.43	2.75±1.50	<b>1.68±0.54</b>	<b>2</b>
Qing Yang, Intel	Hulking	3.25±1.98	1.16±1.12	<b>2.21±1.26</b>	<b>3</b>
Zebin Huang, Newland Inc.	newland_tianyan	0.24±0.25	4.33±3.12	2.28±1.66	4
Tengteng Zhang, CMB	ZhangTT	3.11±2.87	4.41±4.25	3.76±2.02	5
Yuxi Feng, Horizon	harvest	5.77±4.69	3.33±3.21	4.55±3.82	6
Yunxiao Qin, NWPU	Qyxqyx	5.12±7.93	6.66±5.86	5.89±4.46	7
Sun Ke, XMU	skjack	56.24±24.85	11.74±11.37	33.99±7.08	8

# Face Presentation Attack Detection Challenge@CVPR2020

- Multi-Modal Face Anti-Spoofing Based on Central Difference Networks [1] (1st place)

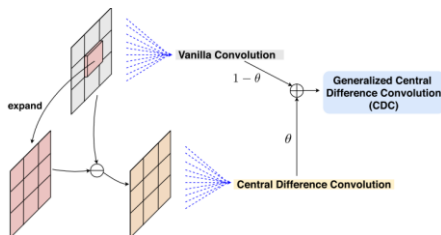
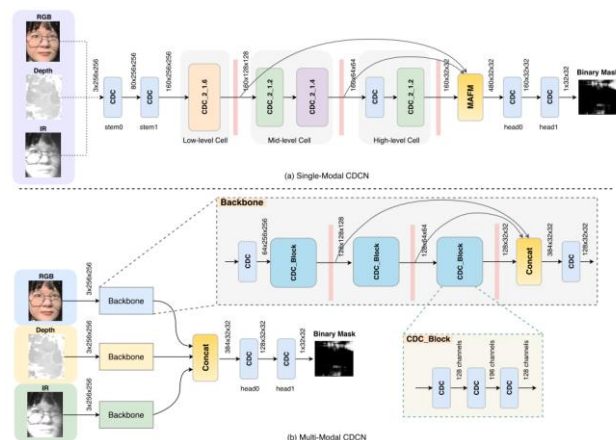
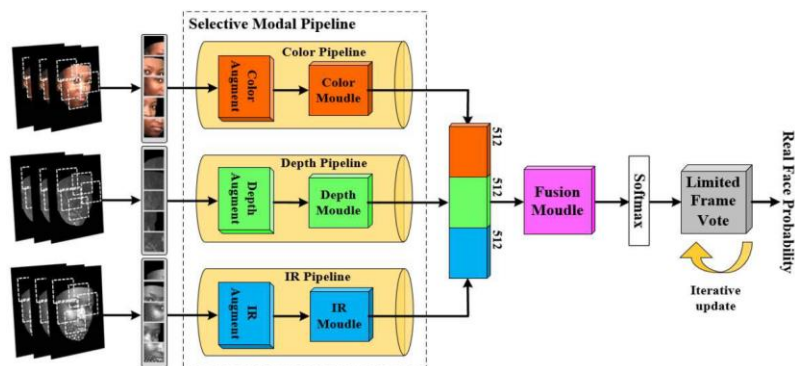


Figure 2. Generalized central difference convolution (CDC).

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



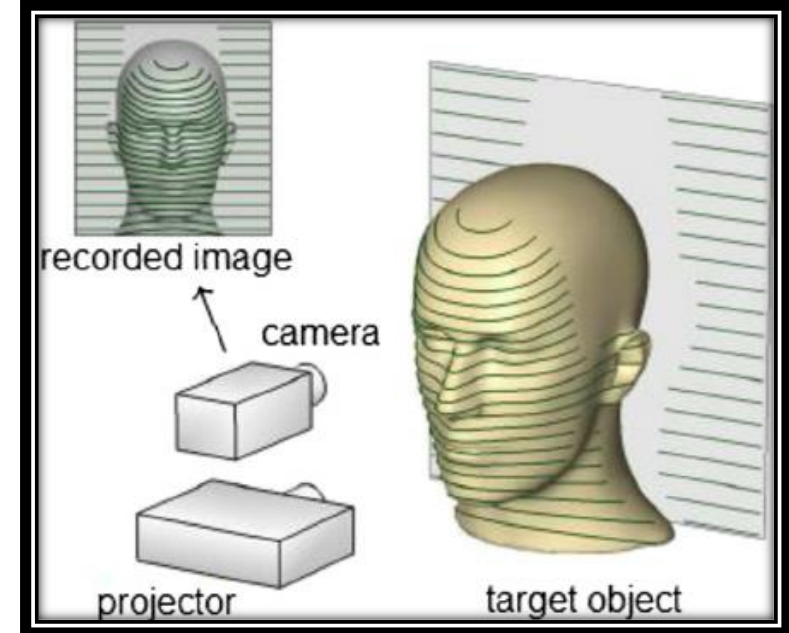
- PipeNet: Selective Modal Pipeline of Fusion Network for Multi-Modal Face Anti-Spoofing [2] (3rd place)



[1] Yu, Z., Qin, Y., Li, X., Wang, Z., Zhao, C., Lei, Z. and Zhao, G. Multi-Modal Face Anti-Spoofing Based on Central Difference Networks. *CVPR Workshop*, 2020.

[2] Yang, Q., Zhu, X., Fwu, J.K., Ye, Y., You, G. and Zhu, Y. PipeNet: Selective Modal Pipeline of Fusion Network for Multi-Modal Face Anti-Spoofing. *CVPR Workshop*, 2020.

# Structured-light 3D Technology

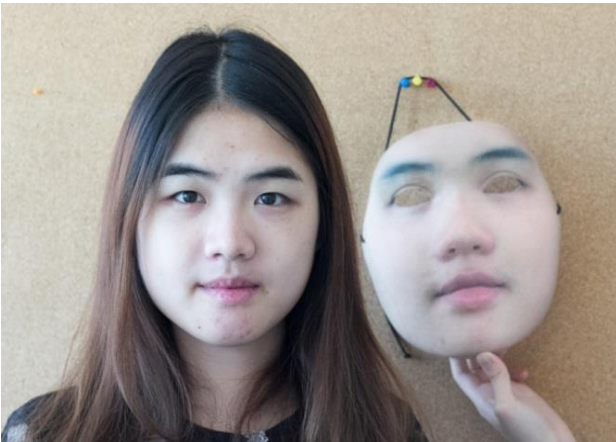




# 3D Mask Face Anti-spoofing

## ■ 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

# 3D Mask Face Anti-spoofing

- Super-realistic 3D Mask



(a)

Life face

(b)

Real-F hyper real mask

# 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

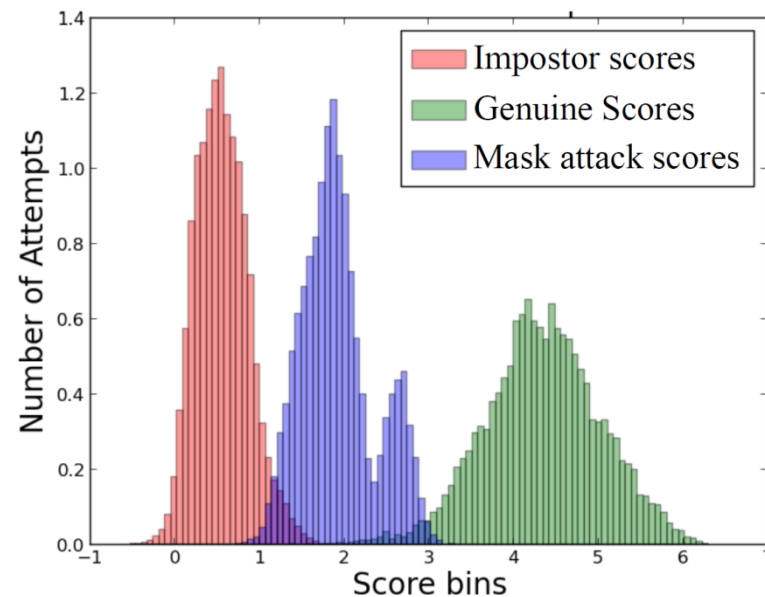
By [Jeff John Roberts](#) December 12, 2019

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.

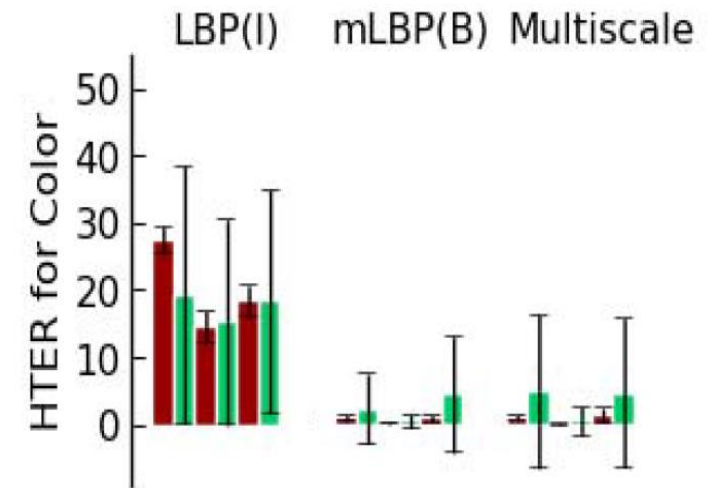
More alarming were the tests deployed at transportation hubs. At the [self-boarding terminal in Schiphol Airport](#), the Netherlands' largest airport, the Kneron team tricked the sensor with just a photo on a phone screen. The team also says it was able to gain access in this way to [rail stations in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

# 3D Mask Face Anti-spoofing

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



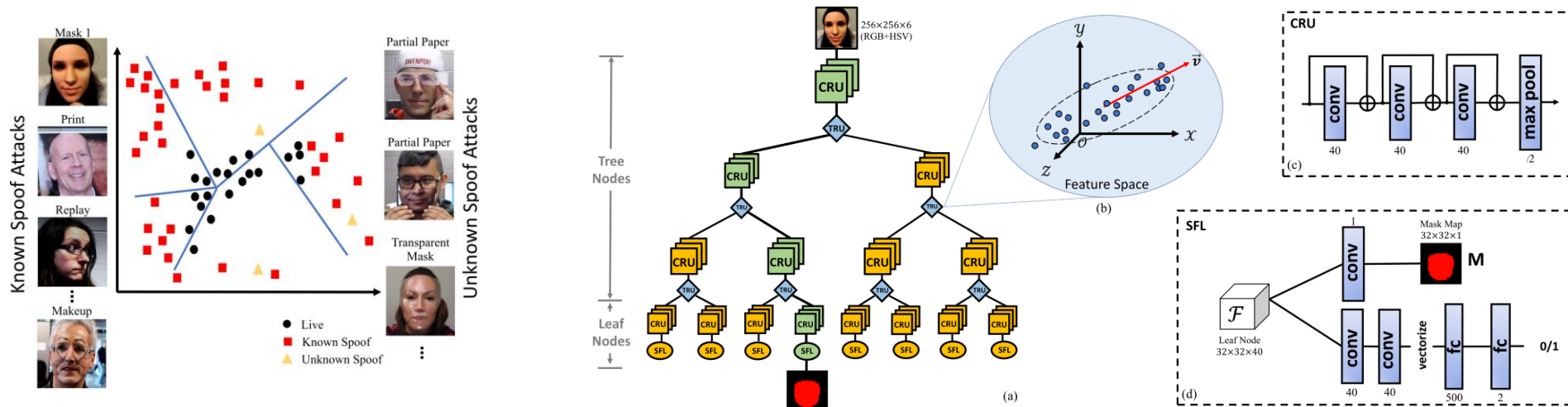
[Erdogmus et al., BTAS'13]



# 3D Mask Face Anti-spoofing

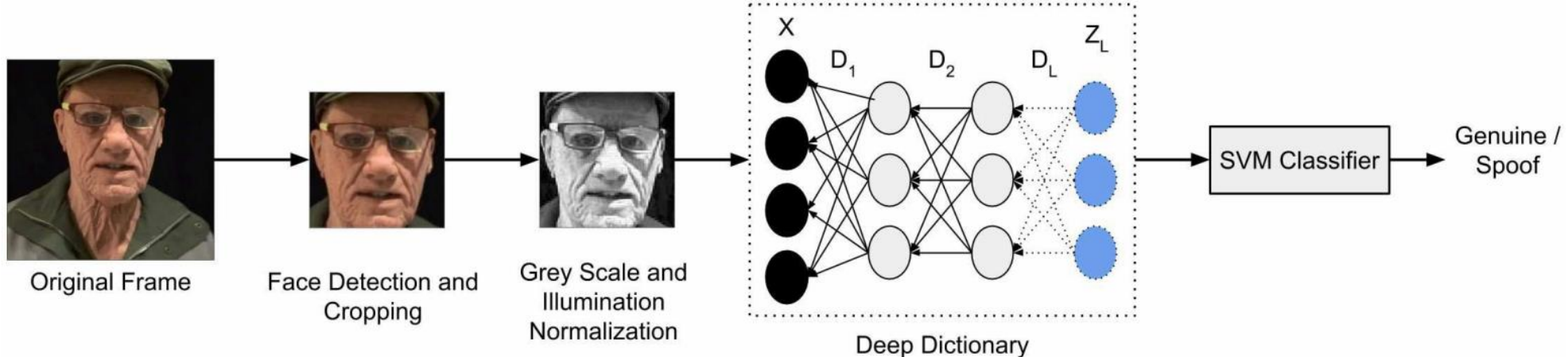
## ■ Zero-shot Learning approach

- 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



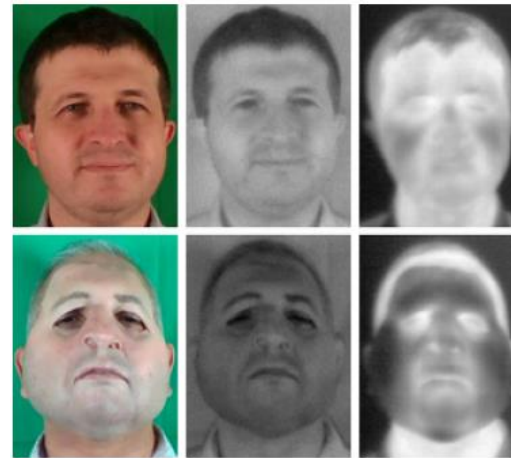
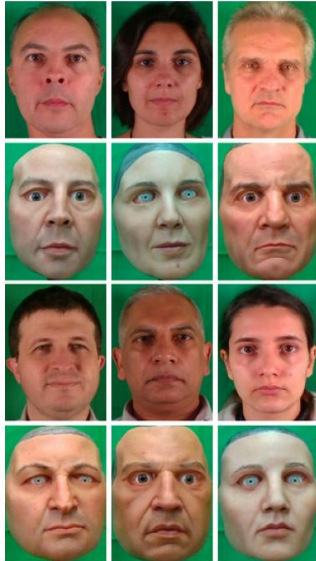
# 3D Mask Face Anti-spoofing

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



# 3D Mask Face Anti-spoofing

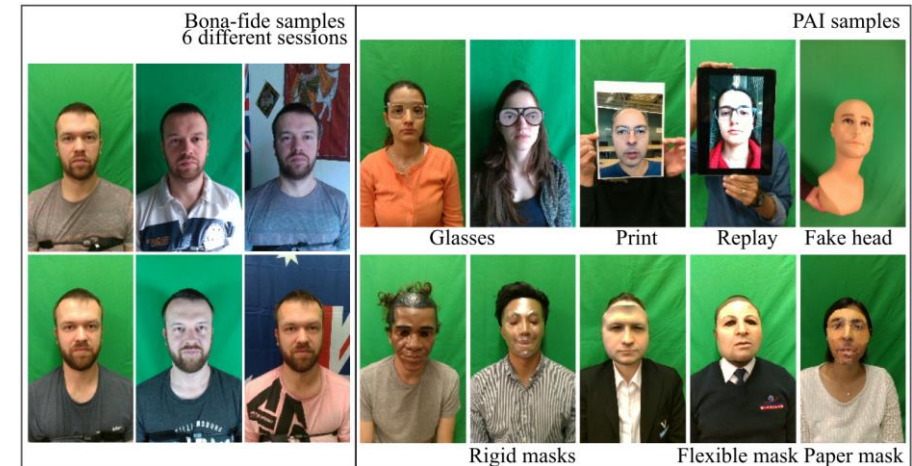
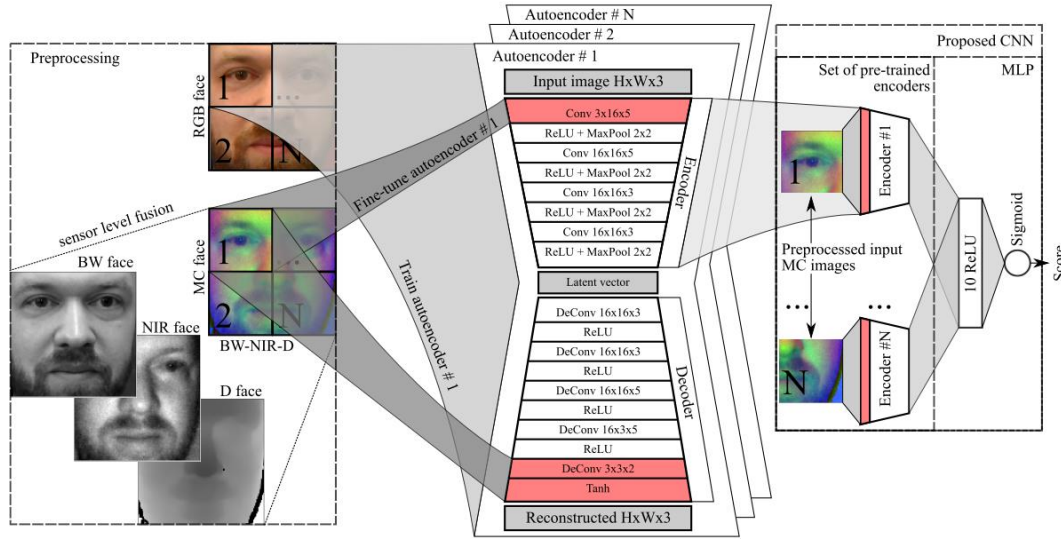
- Custom Silicone Masks Datasets
  - Consider PAs performed using custom-made flexible silicone masks..
  - A new dataset based on six custom silicone masks





# 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



# Our Recent Works

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

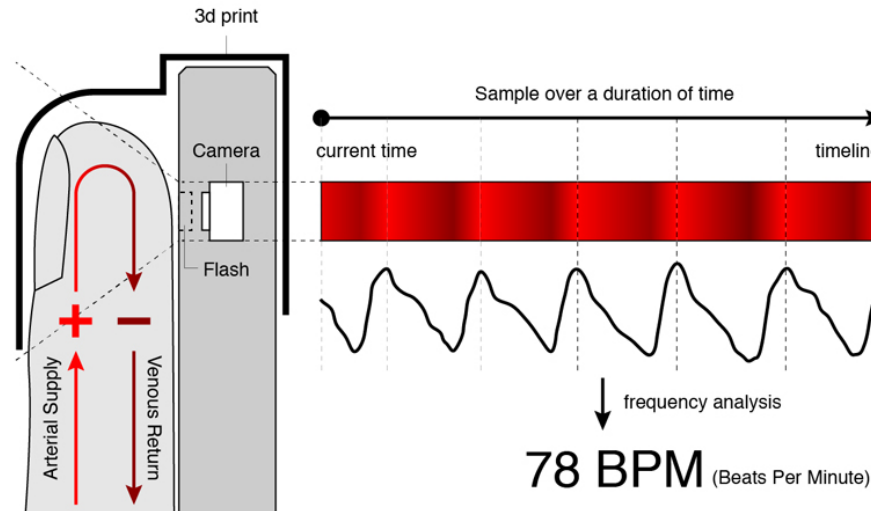


# PhotoPlethysmoGraphy based Face Anti-spoofing Approach for 3D Mask Attack

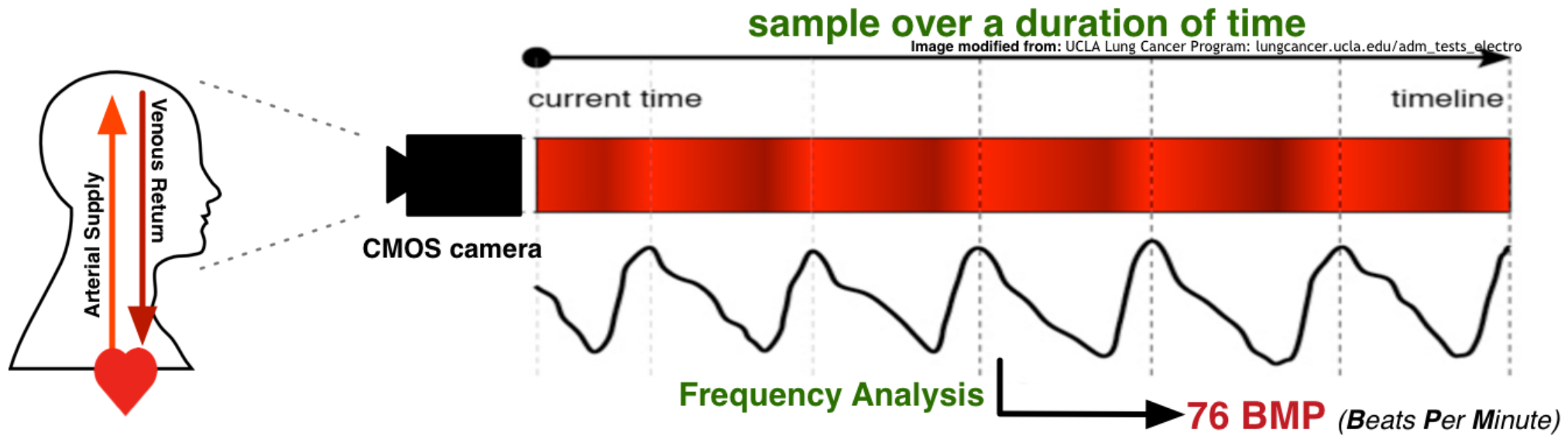
## ■ Reference:

1. S Q Liu, XY Lan and P CYuen, "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 CYuen, "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 CYuen, 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.

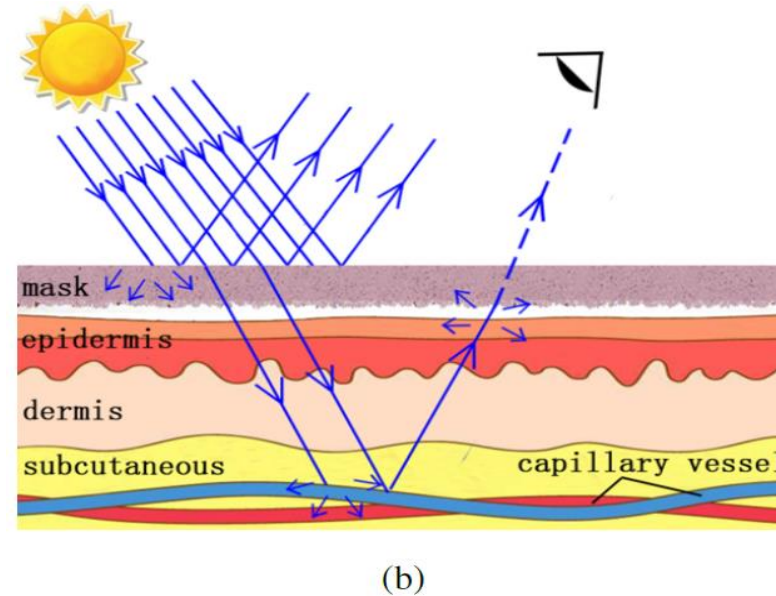
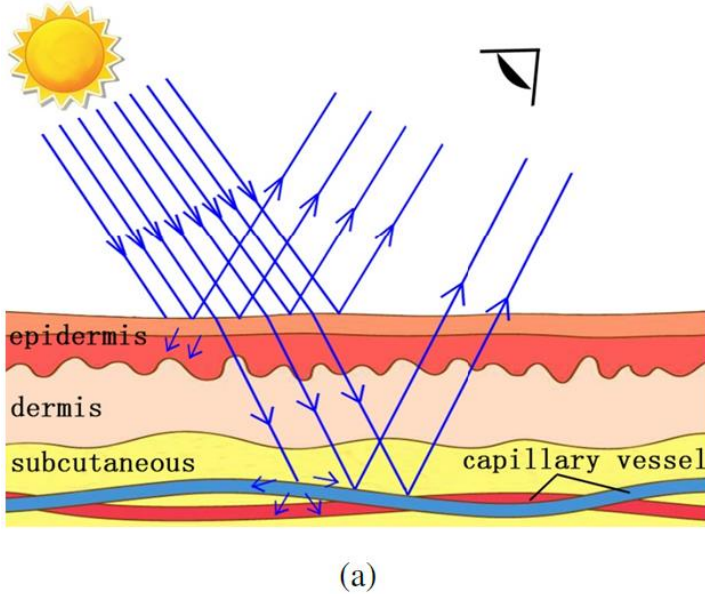
# PhotoPlethysmoGraphy (PPG)



# remote PhotoPlethysmography (rPPG)



# Principle of rPPG Based Face Anti-Spoofing



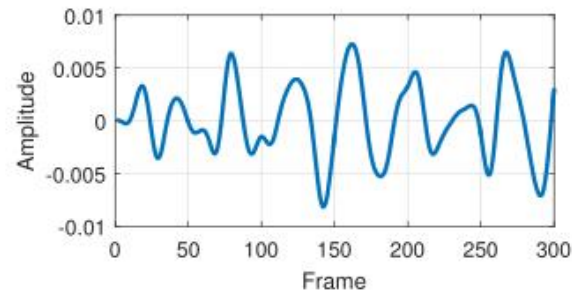
- (a) rPPG signal can be extracted from genuine face skin.
- (b) rPPG signals will be **too weak** to be detected from a masked face.
- light source needs to penetrate the mask before interacting with the blood vessel.
  - rPPG signal need to penetrate the mask before capturing by camera

# Principle of rPPG Based Face Anti-Spoofing

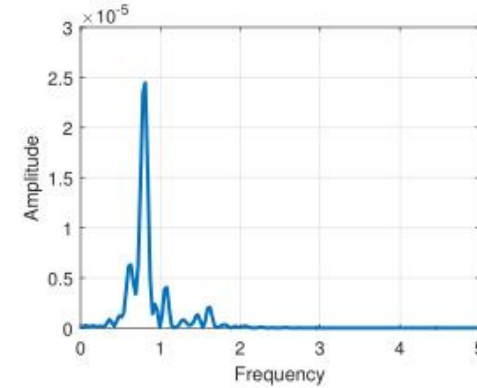
genuine face



(a)



(b)



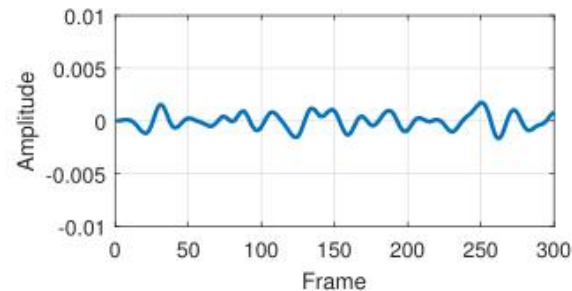
(c)

masked face

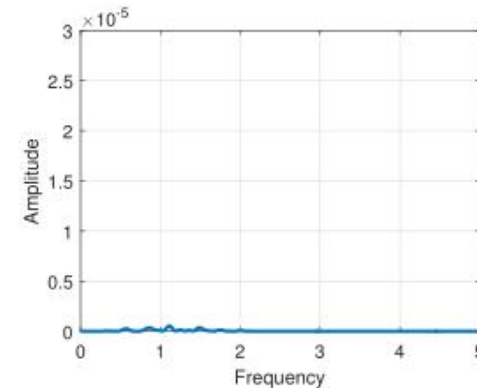


(d)

(a)

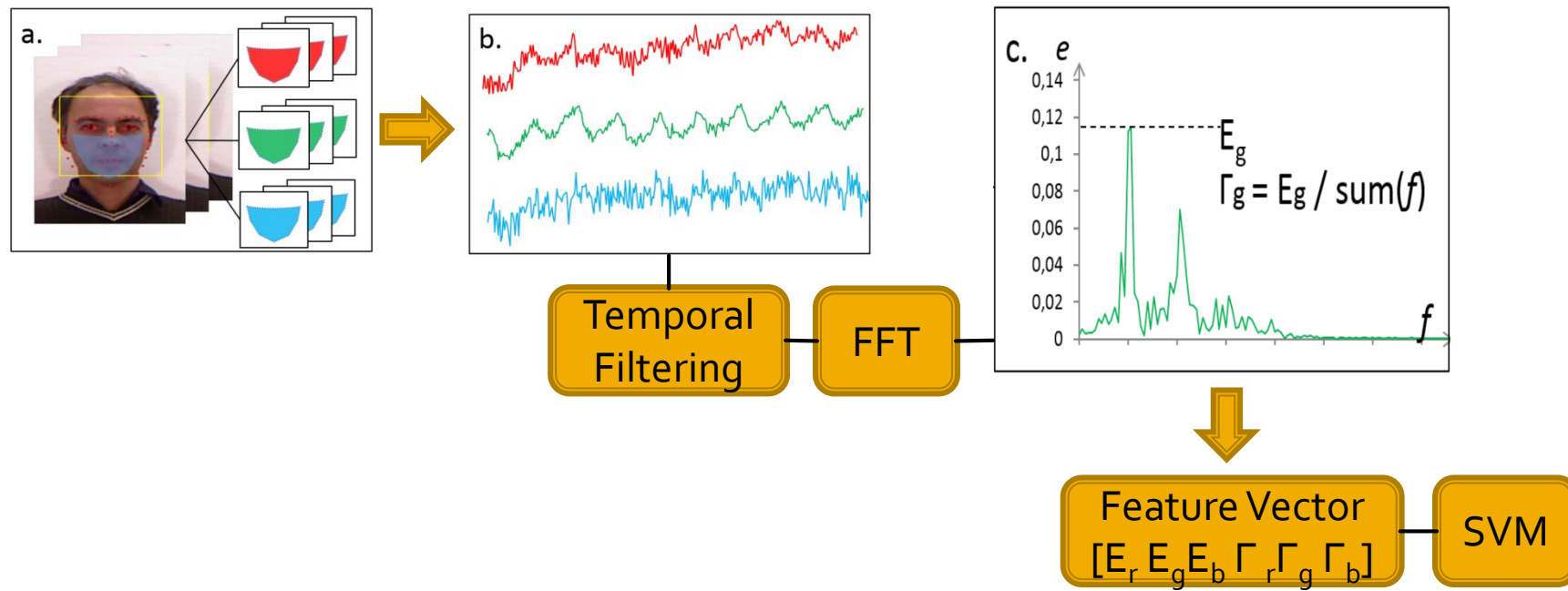


(e)



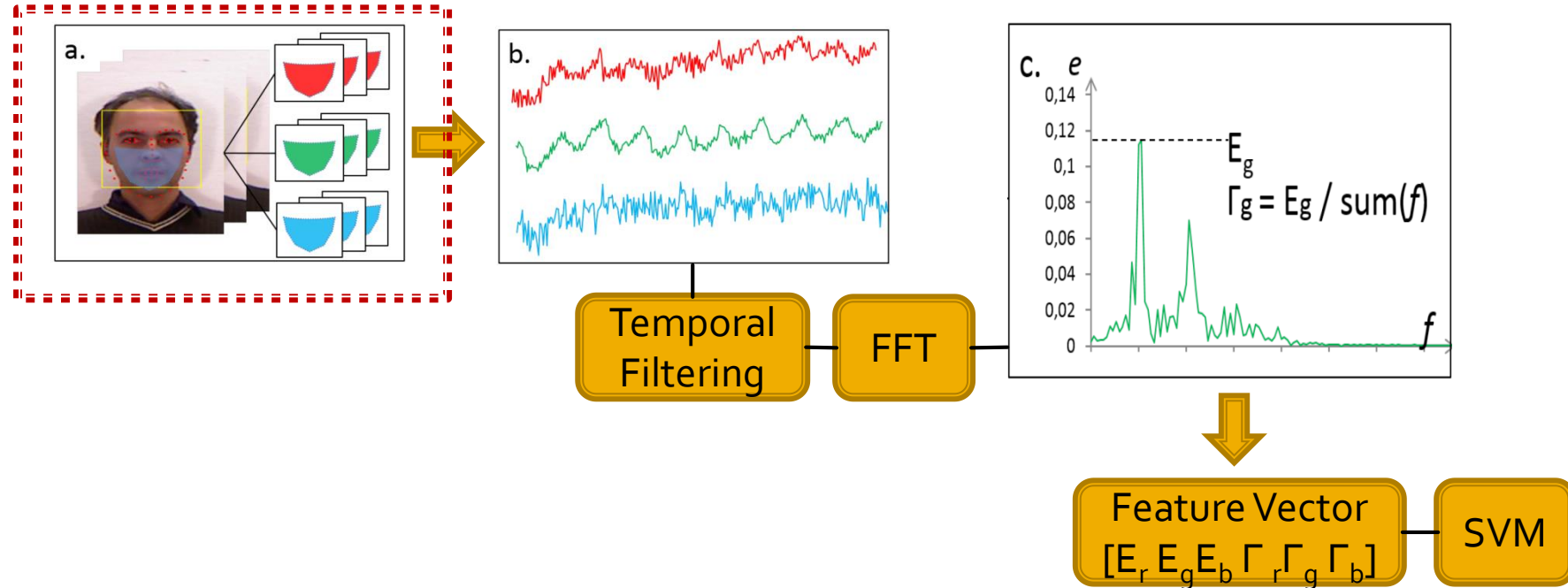
(f)

# 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

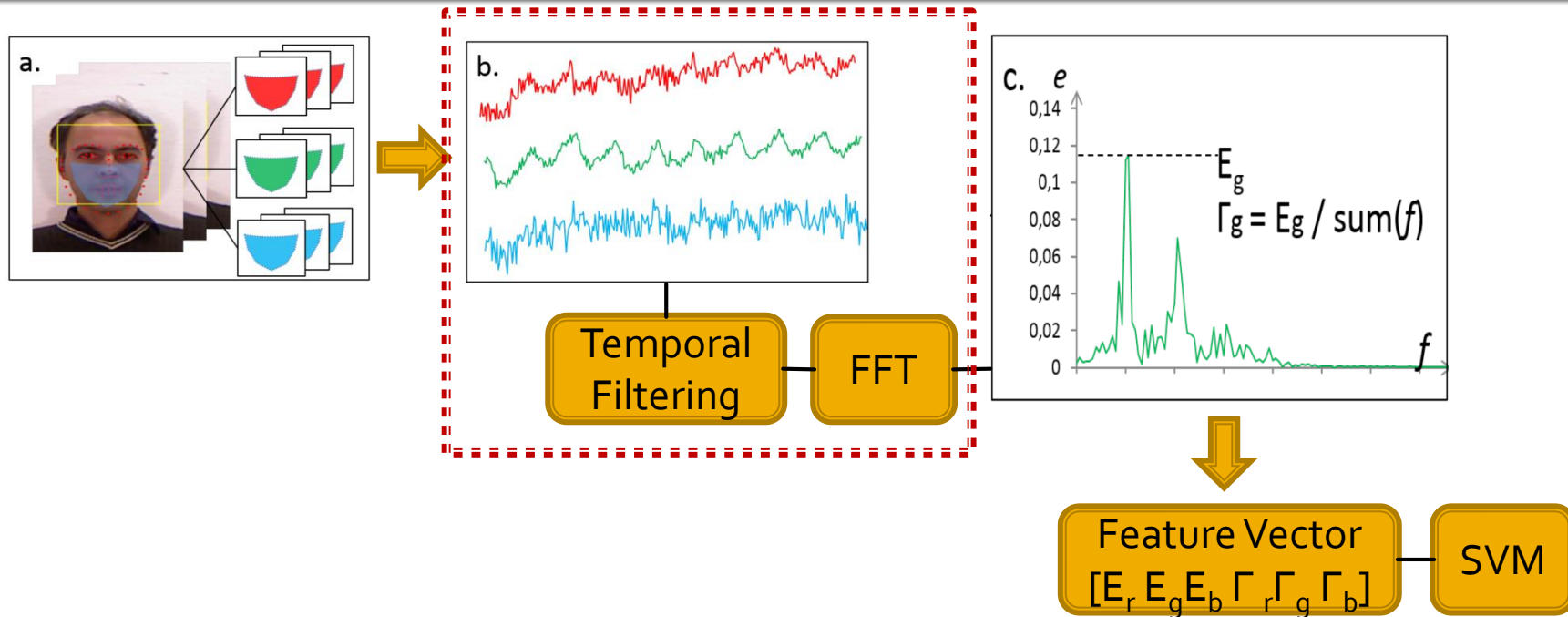
# Global rPPG-based Face Anti-Spoofing



- 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

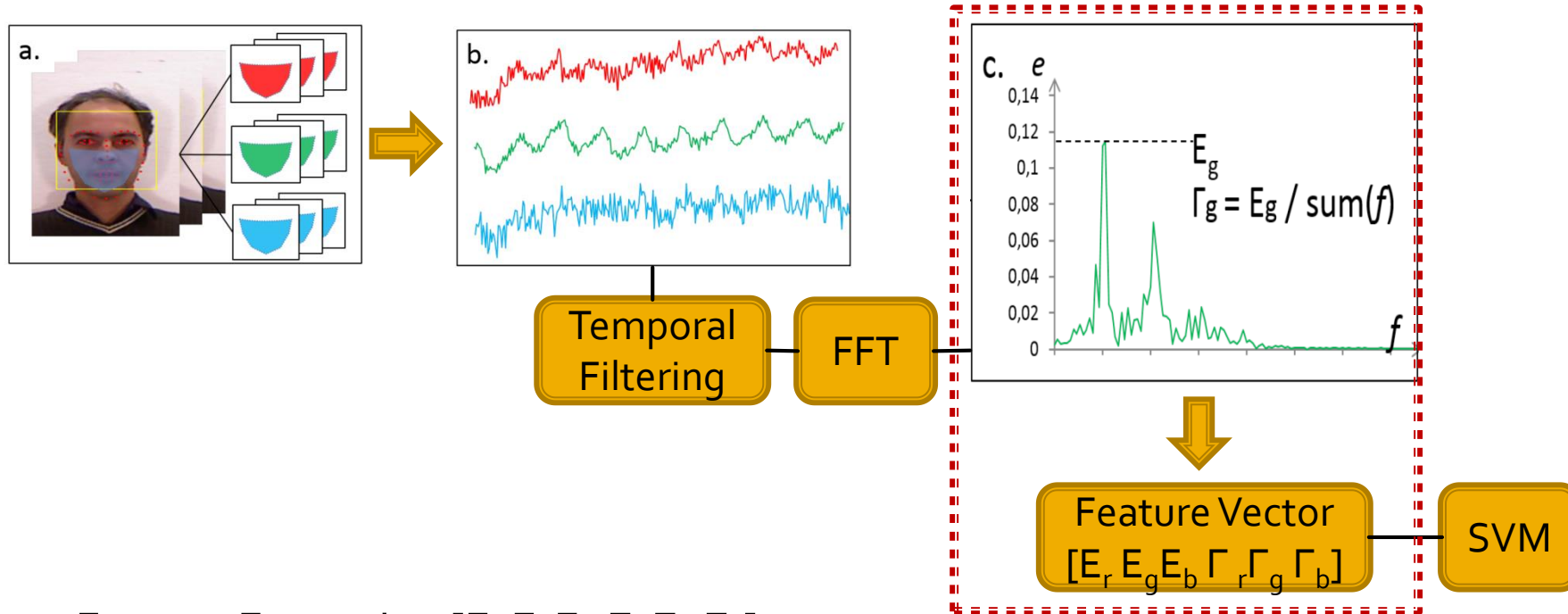


# Global rPPG-based Face Anti-Spoofing



- 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  $\rightarrow$  PSD curve:  $f$

# Global rPPG-based Face Anti-Spoofing



- c. Feature Extraction [E<sub>r</sub> E<sub>g</sub> E<sub>b</sub> Γ<sub>r</sub> Γ<sub>g</sub> Γ<sub>b</sub>]
- $E = \max(e(f))$
  - $\Gamma = \frac{E}{\sum_{\forall f \in [0.7, 4]} e(f)}$

# 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

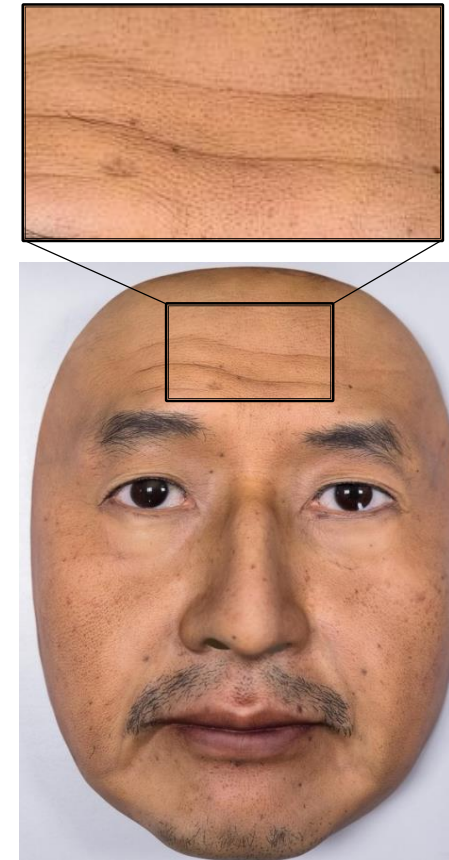
## ■ Results on REAL-F

- Randomly select 8 subjects from 3DMAD for training and the other 8 subjects as the development set

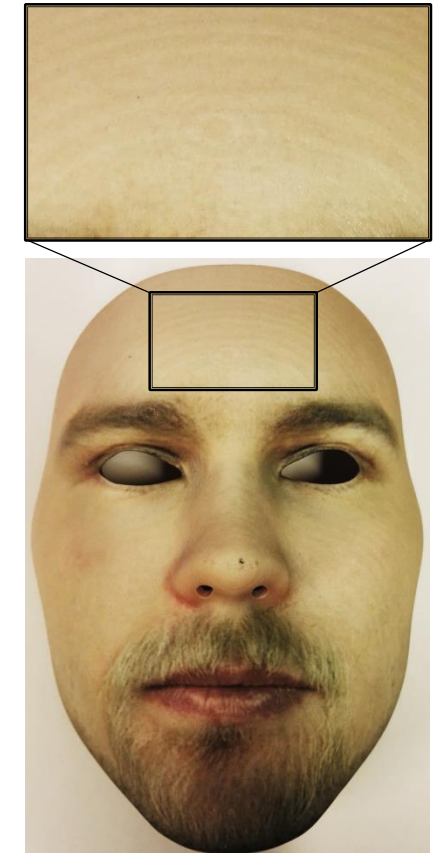
	REAL-F			
Method	HTER(%)	EER(%)	FPR (@FNR=0.1%)	FPR (@FNR=0.01%)
<b>Pulse (ours)</b>	<b>4.29</b>	<b>1.58</b>	<b>0.25</b>	<b>3.83</b>
LBP-blk	26.3	25.08	37.92	48.25
LBP-blk-color	25.92	20.42	31.5	48.67
LBP-ms	39.87	46.5	59.83	73.17
LBP-ms-color	47.38	46.08	86.5	95.08

# 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

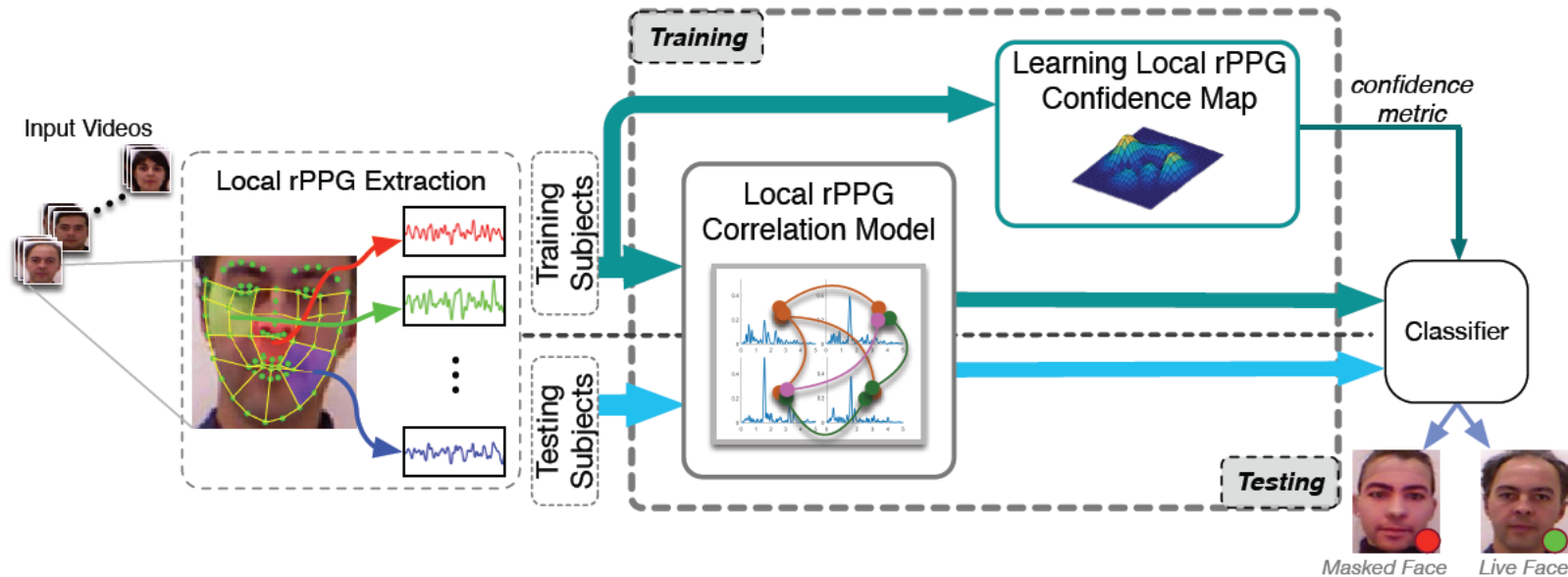
- Global rPPG signal is sensitive to certain variations such as illuminations, head motion and video quality
- rPPG signal strength may vary with different subjects



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

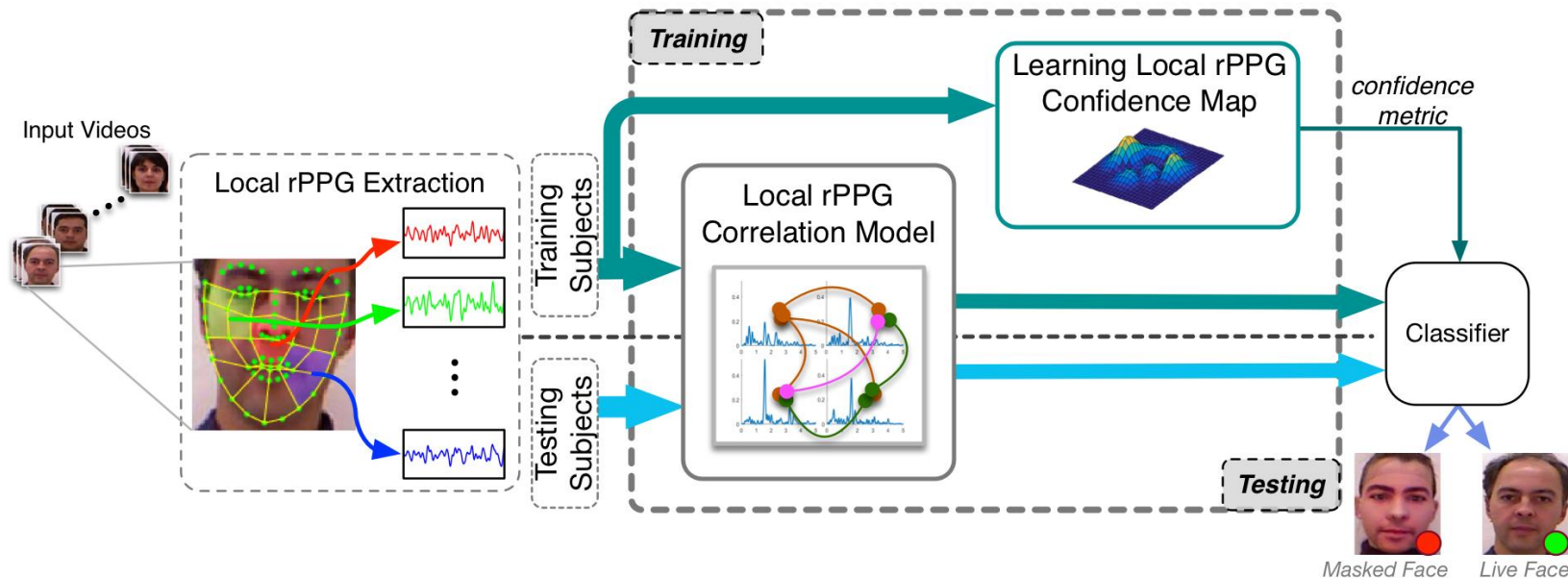
# Local rPPG based Face Anti-Spoofing Method

[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*

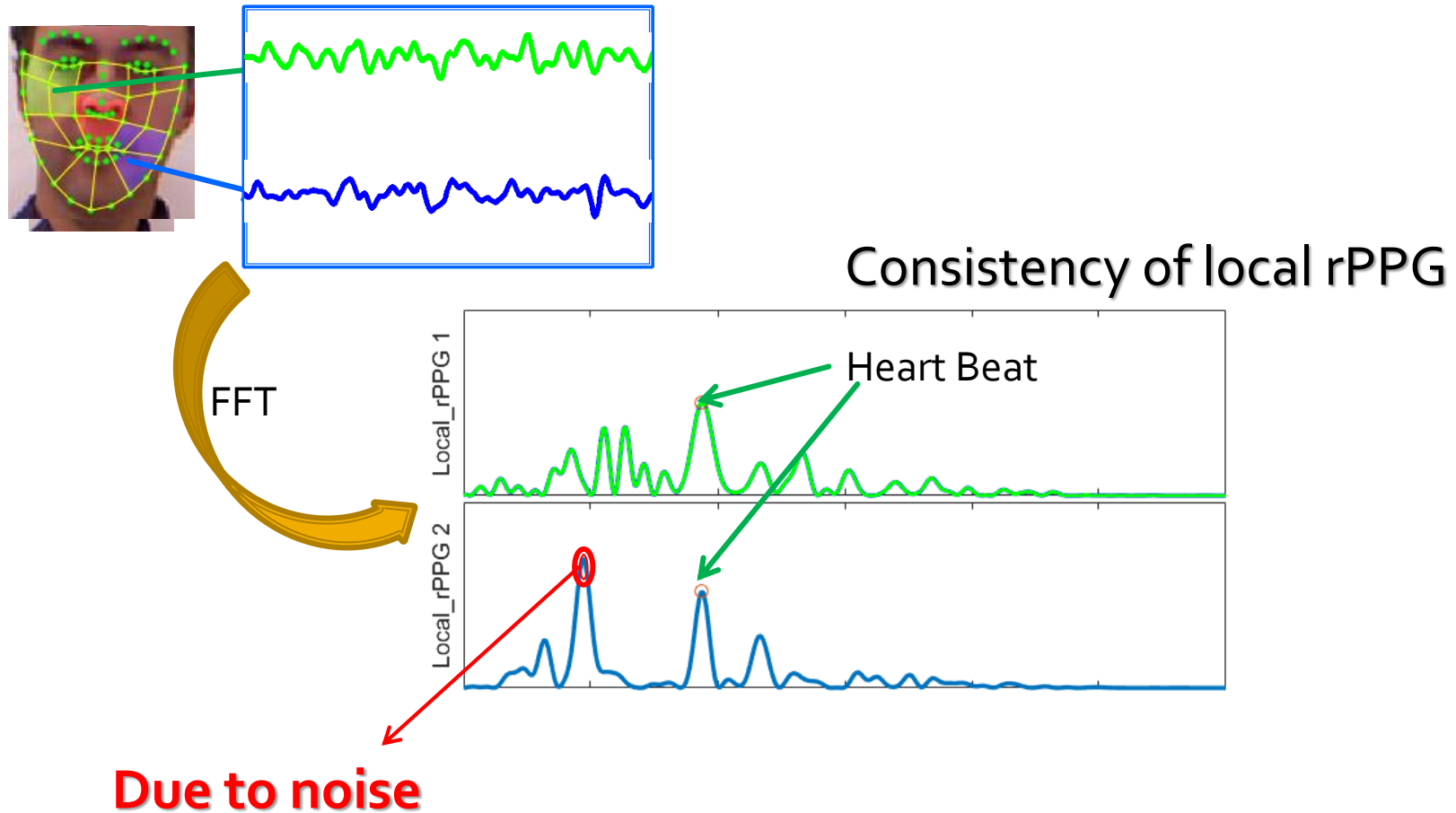
# Local rPPG based Face Anti-Spoofing Method



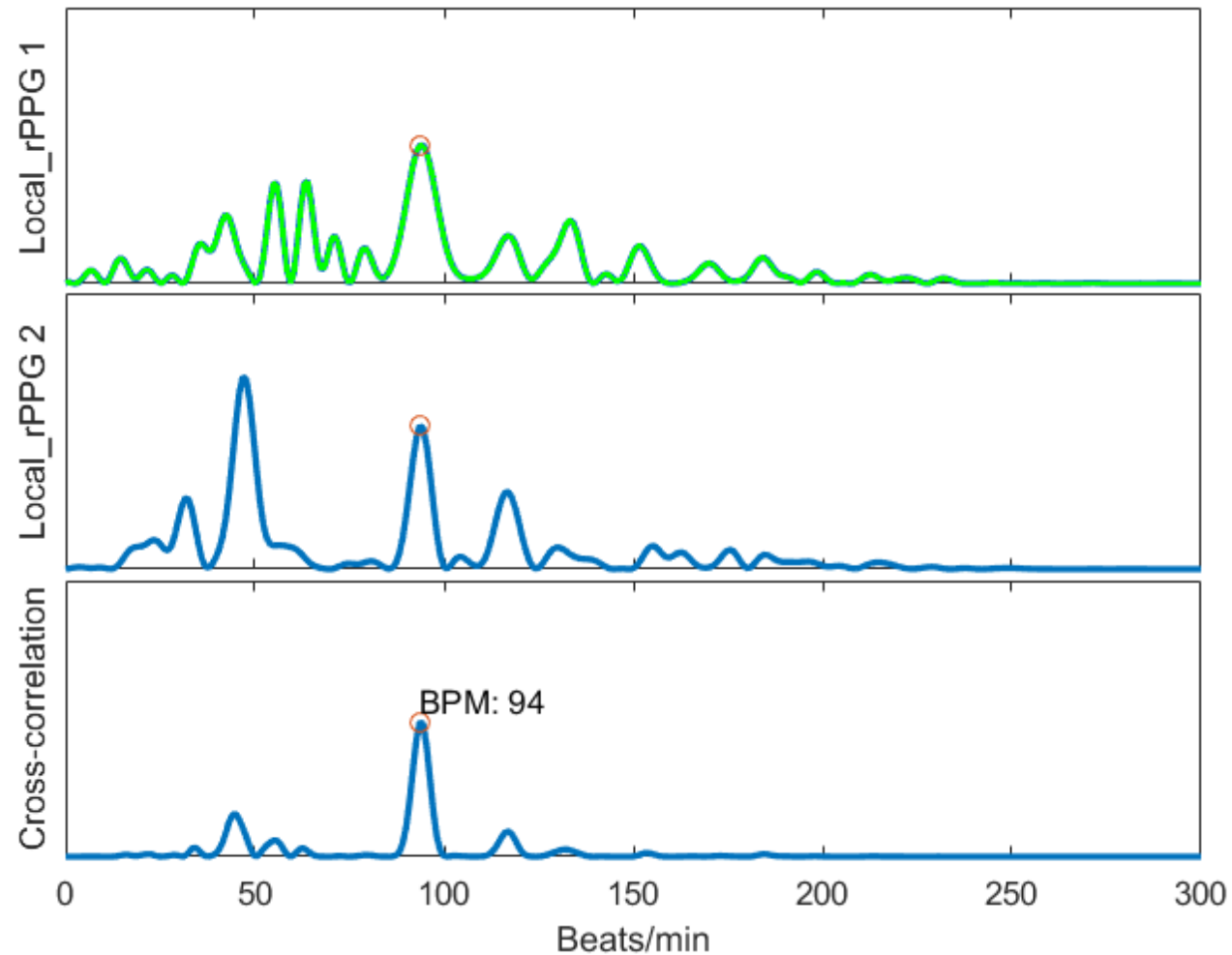
- (a) Local ROIs are pre-defined based on the facial landmarks. Local rPPG signals are extracted from these local face regions.
- (b) Extract Local rPPG patterns through the proposed **local rPPG correlation model**.
- (c) Training stage: local rPPG confidence map is learned, and then transformed into distance metric for classification.
- (d) Classifier: SVM

# Contribution 1: Local rPPG Correlation Model

- Local rPPG on genuine face



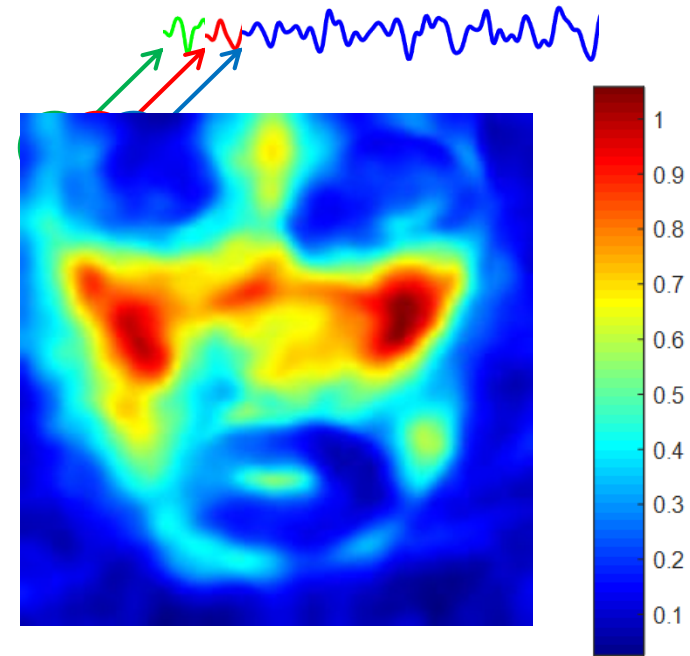
## 2. Local rPPG Correlation Model



# Contribution 2: Learning Local rPPG Confidence Map



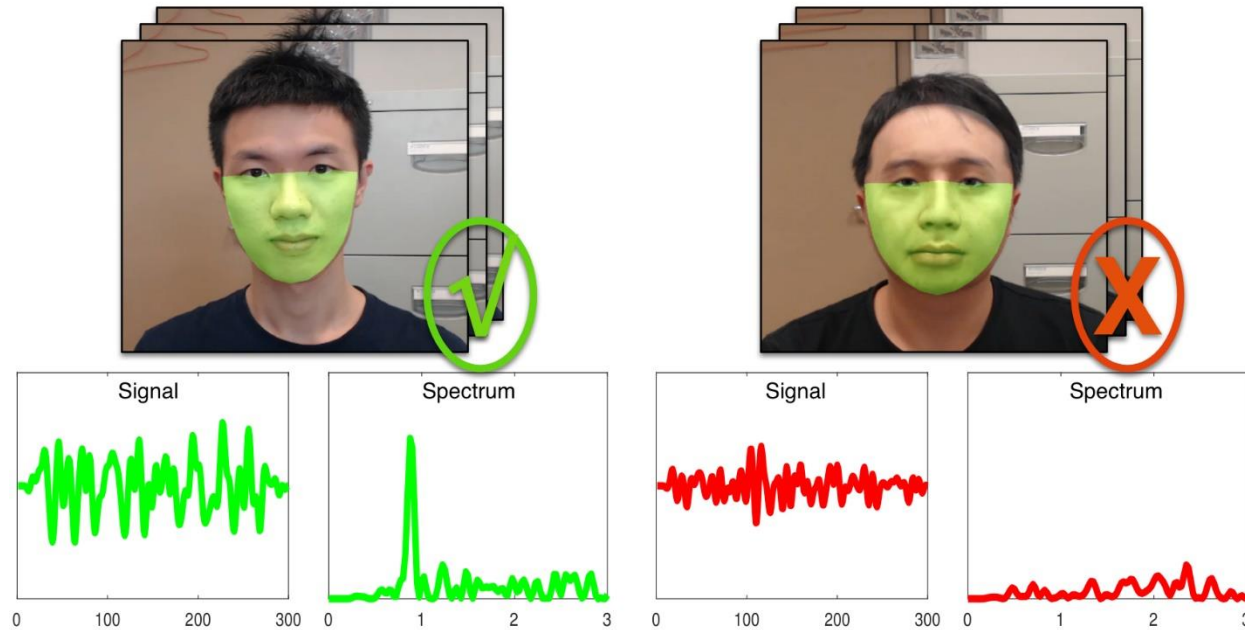
Generic map of blood vessels on the face



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



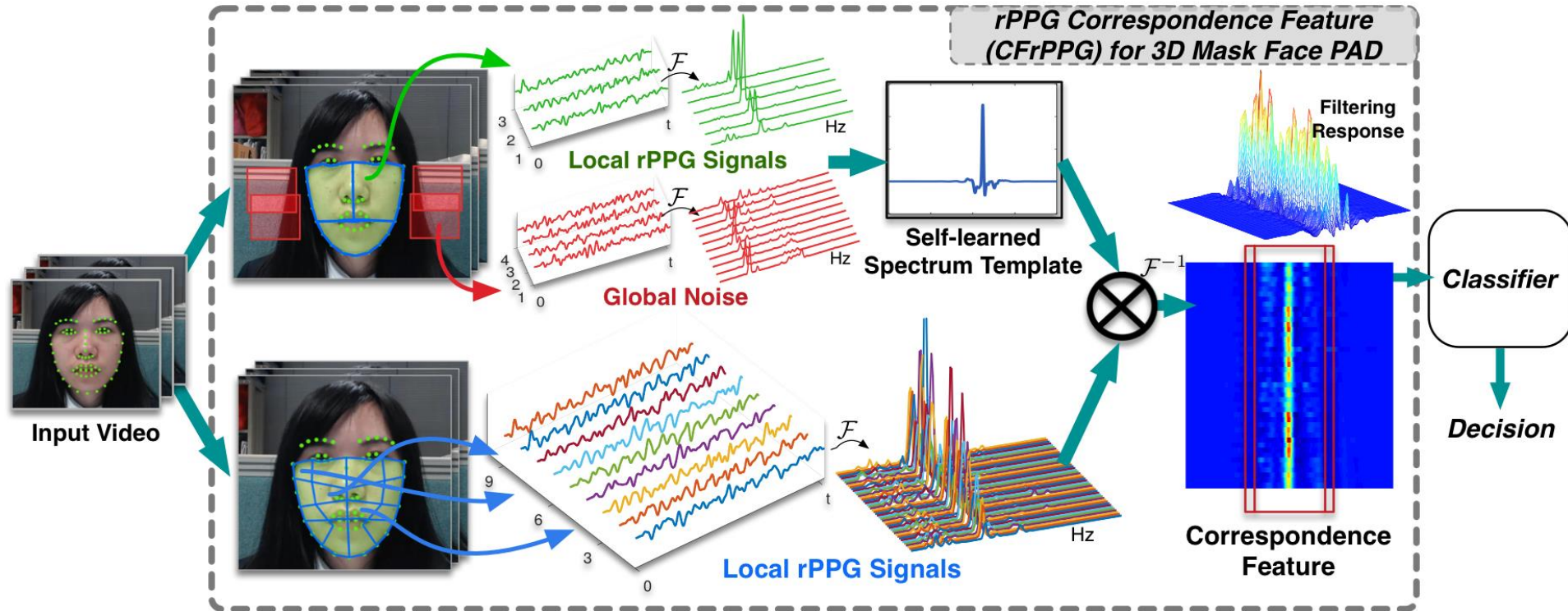
# Limitation on Local rPPG Approach



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

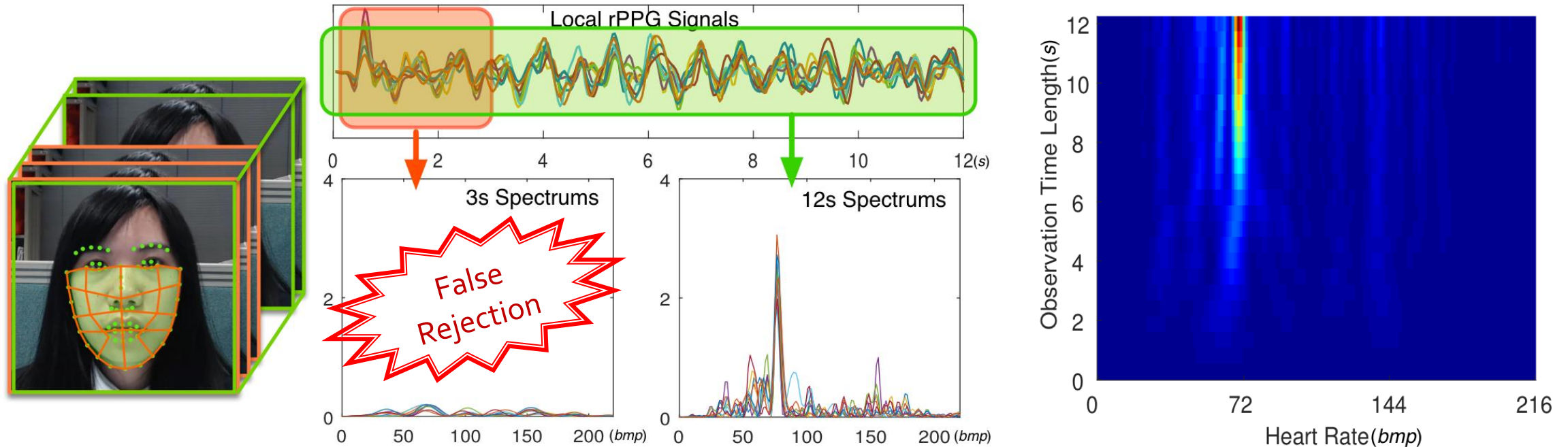
# Improved Method: rPPG Correspondence Feature

[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)*, In press 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*

# Limitations on existing rPPG Methods



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

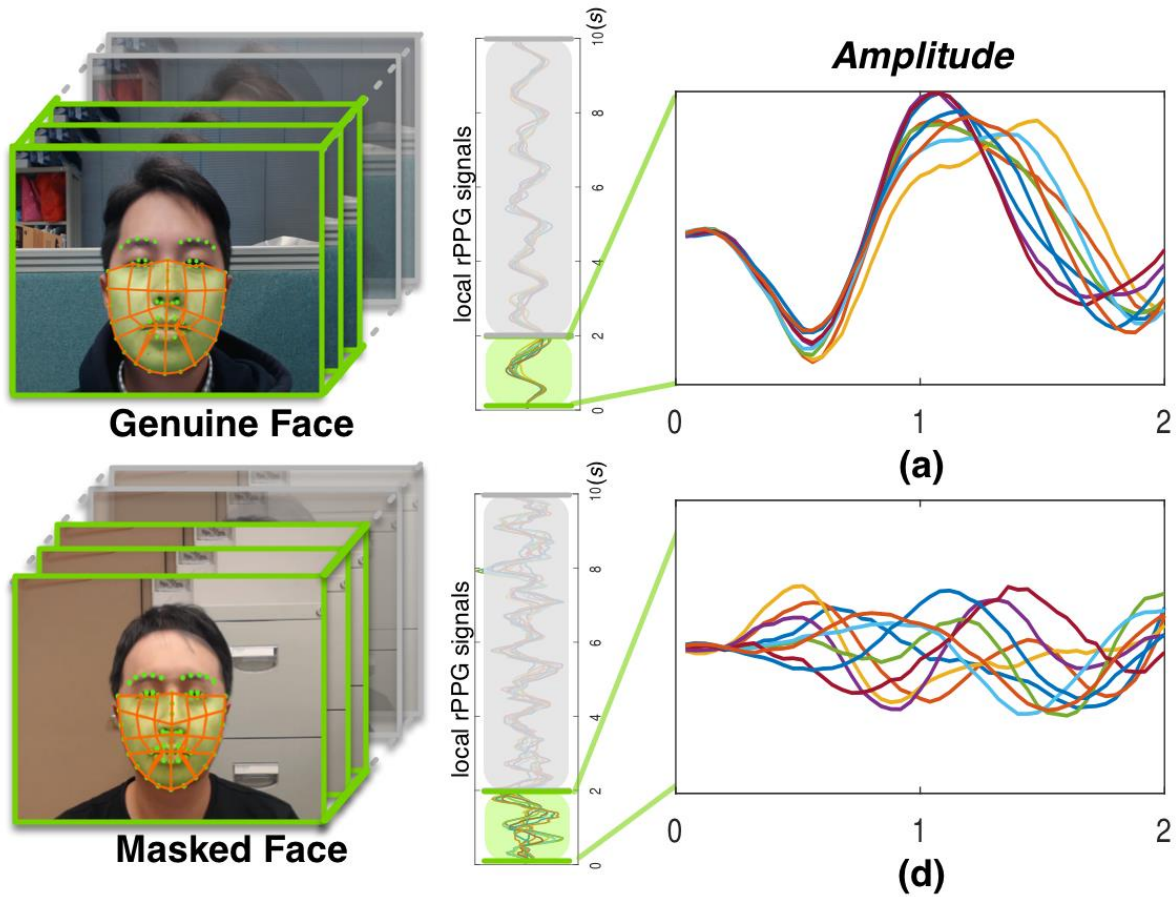
→ Require long observation time (8-10 seconds) to identify heartbeat information

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

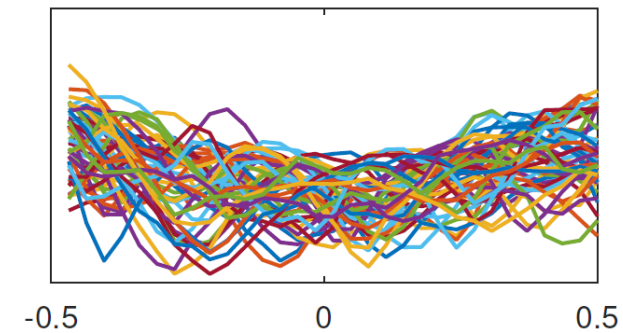
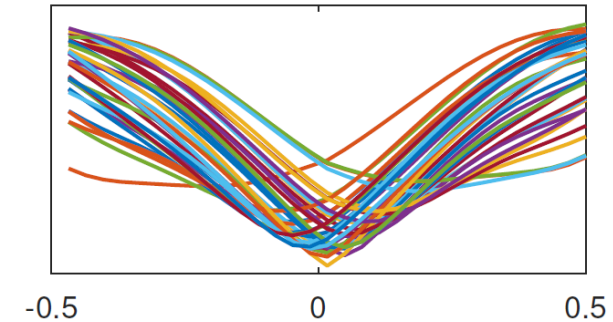
Reference:

S Q Liu, XY 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



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

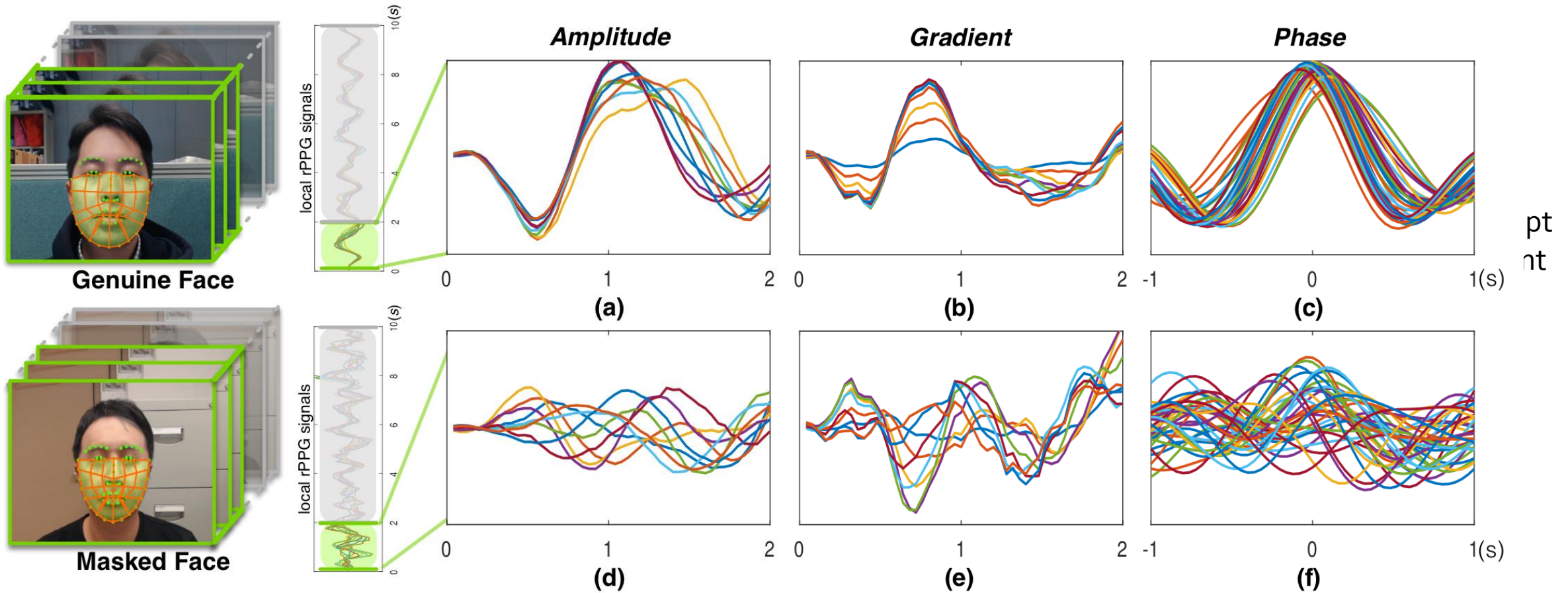


Extract features on the result pattern  
→ Min, Mean, Std (... etc.)



# The proposed TSrPPG

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



Final result is obtained through score-level-fusion



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



# Deep Dynamic Feature Learning Approach

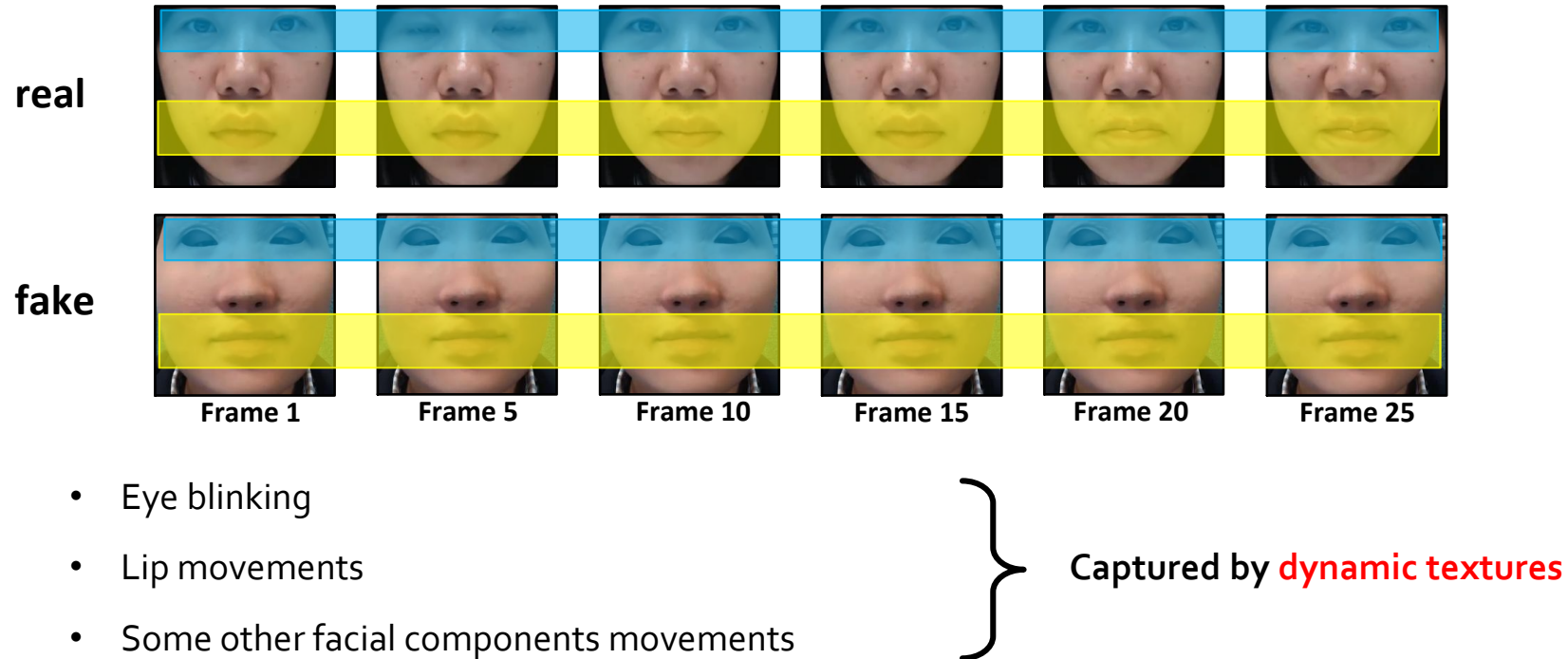
## Reference:

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]

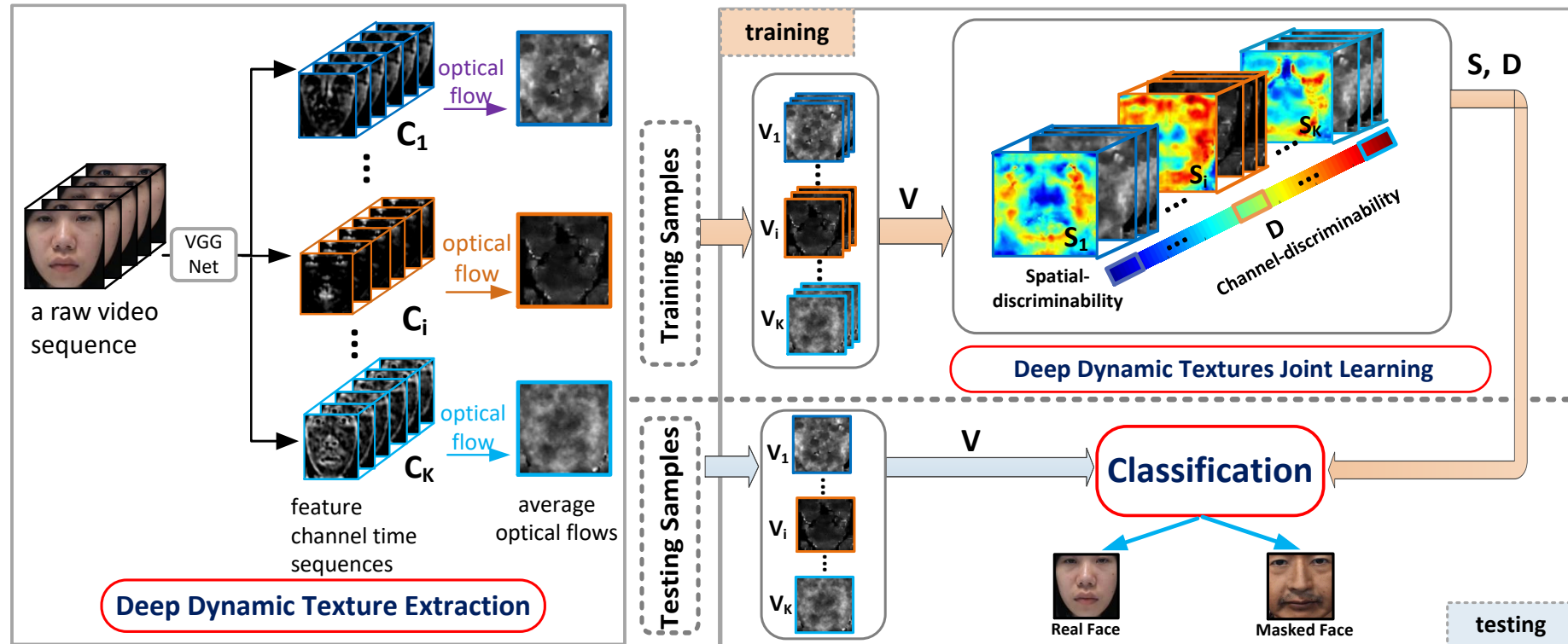
## Basic Idea





# 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?



✓ Real Face



✗ Prints Attack



✗ Replay Attack



✗ 3D Mask Attack

# Domain Generalization Approach

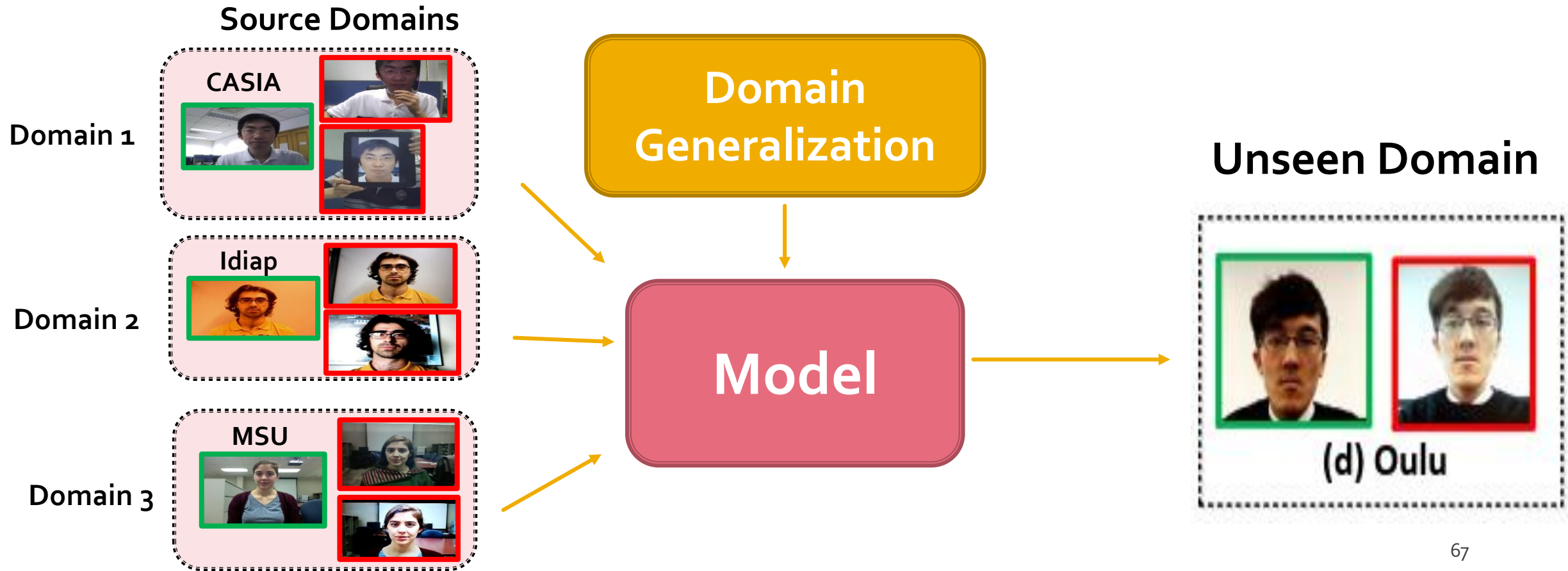
## Reference:

1. R Shao, XY Lan, JW 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.

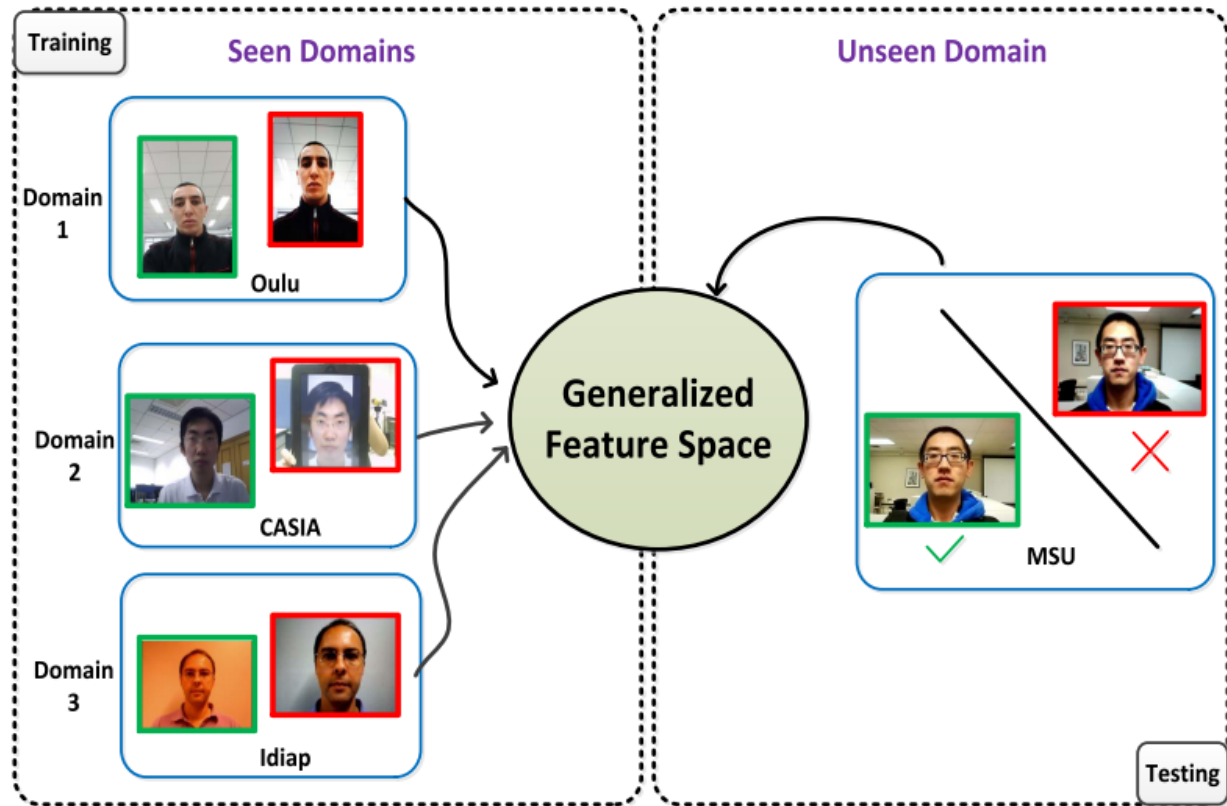


# Multi-adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection [CVPR2019]

- Domain Generalization:

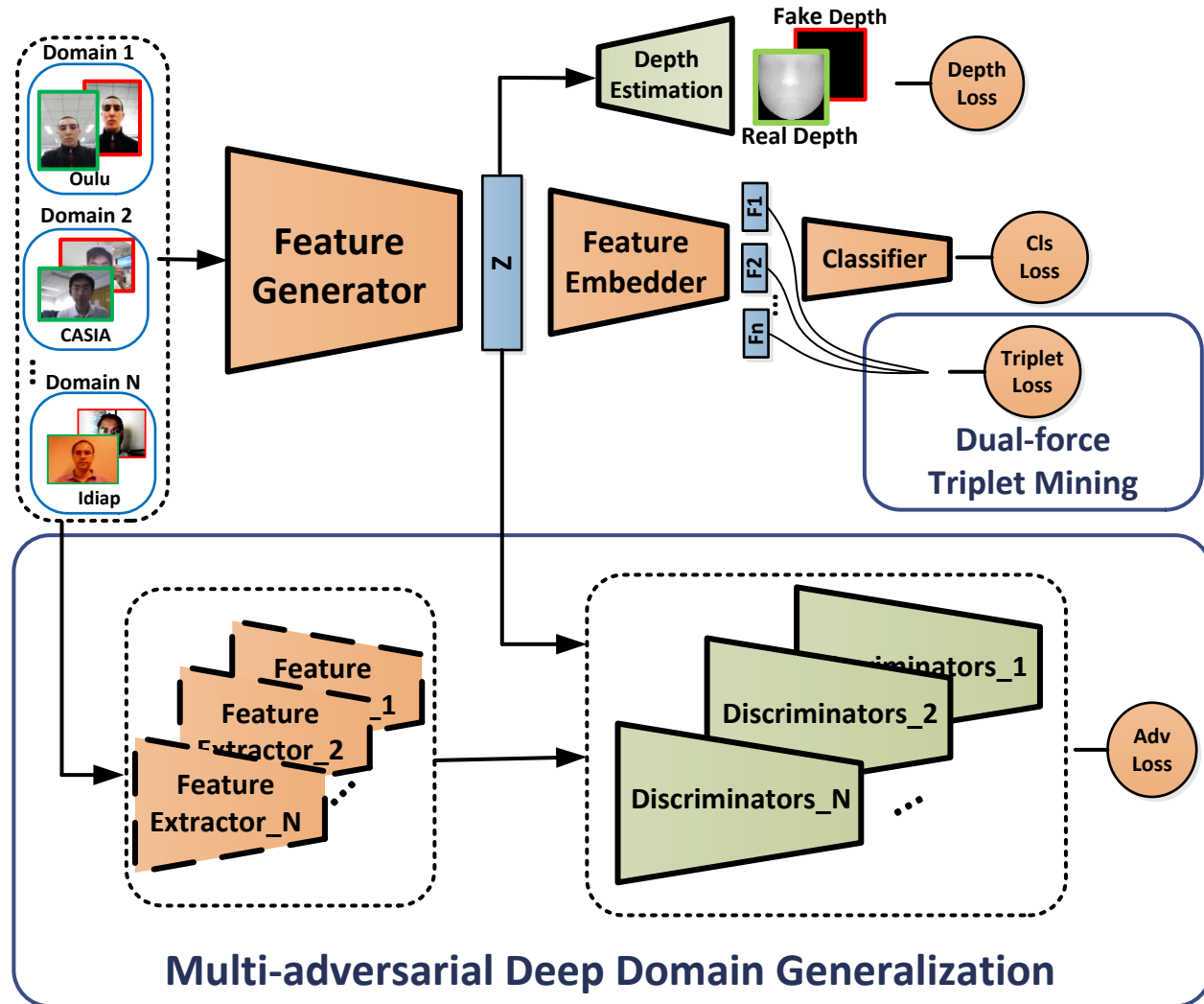


# Multi-adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection [CVPR 2019]



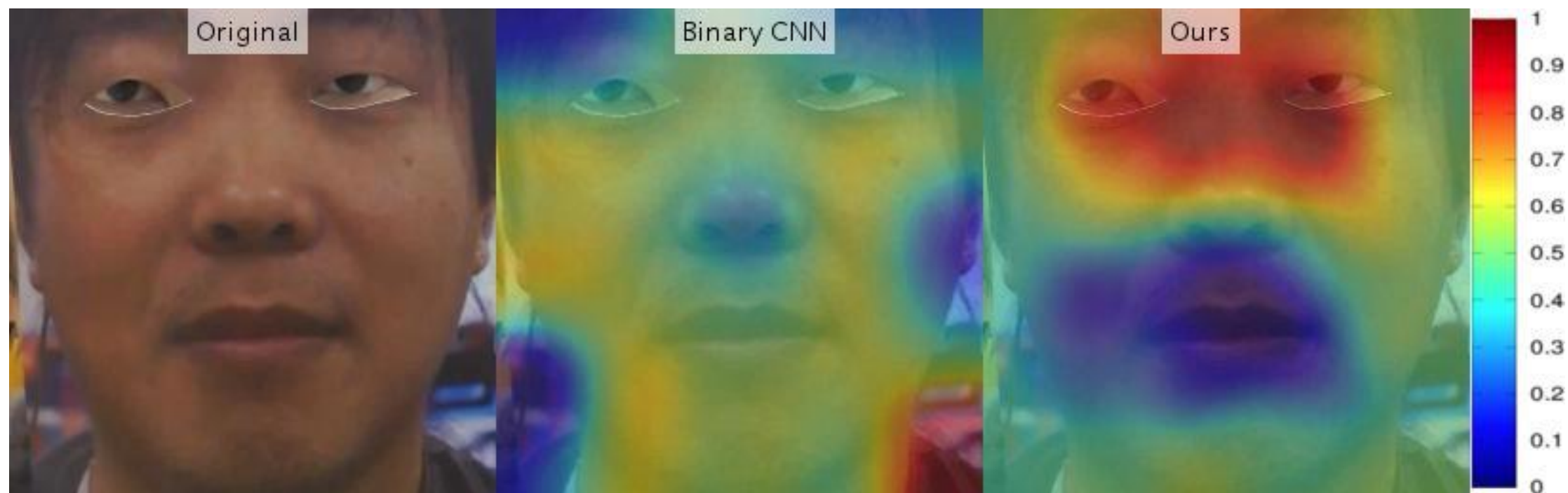
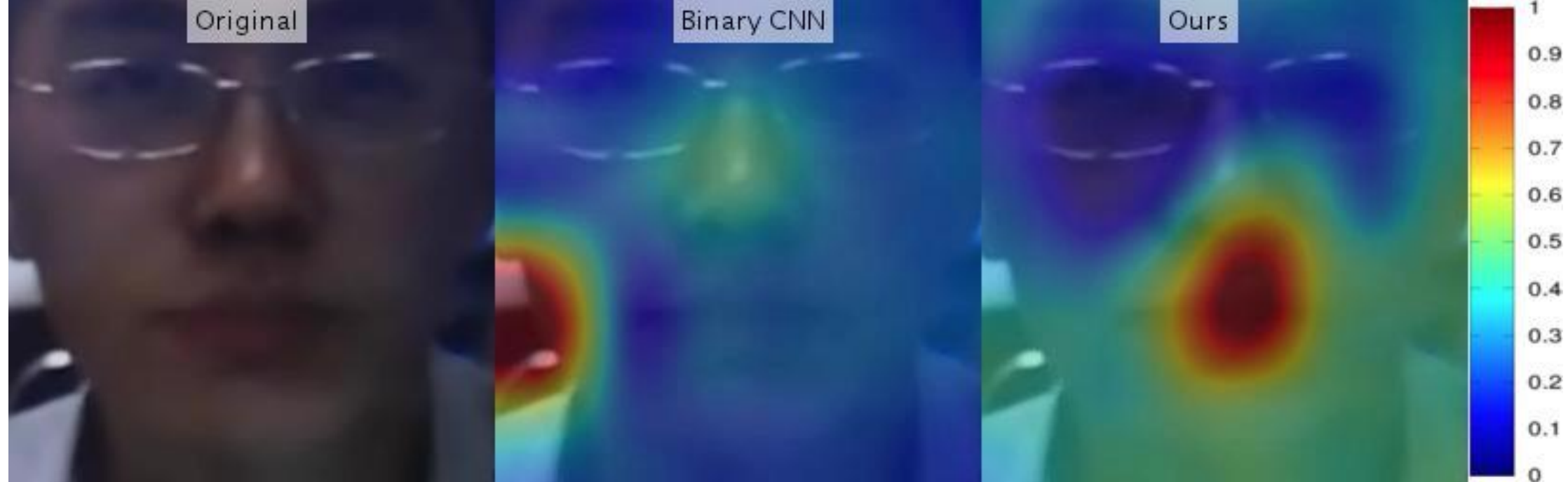
- The **generalized feature space** learned by the domain generalization approach should be:
  - **Shared** by multiple source domains
  - **Discriminative**

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

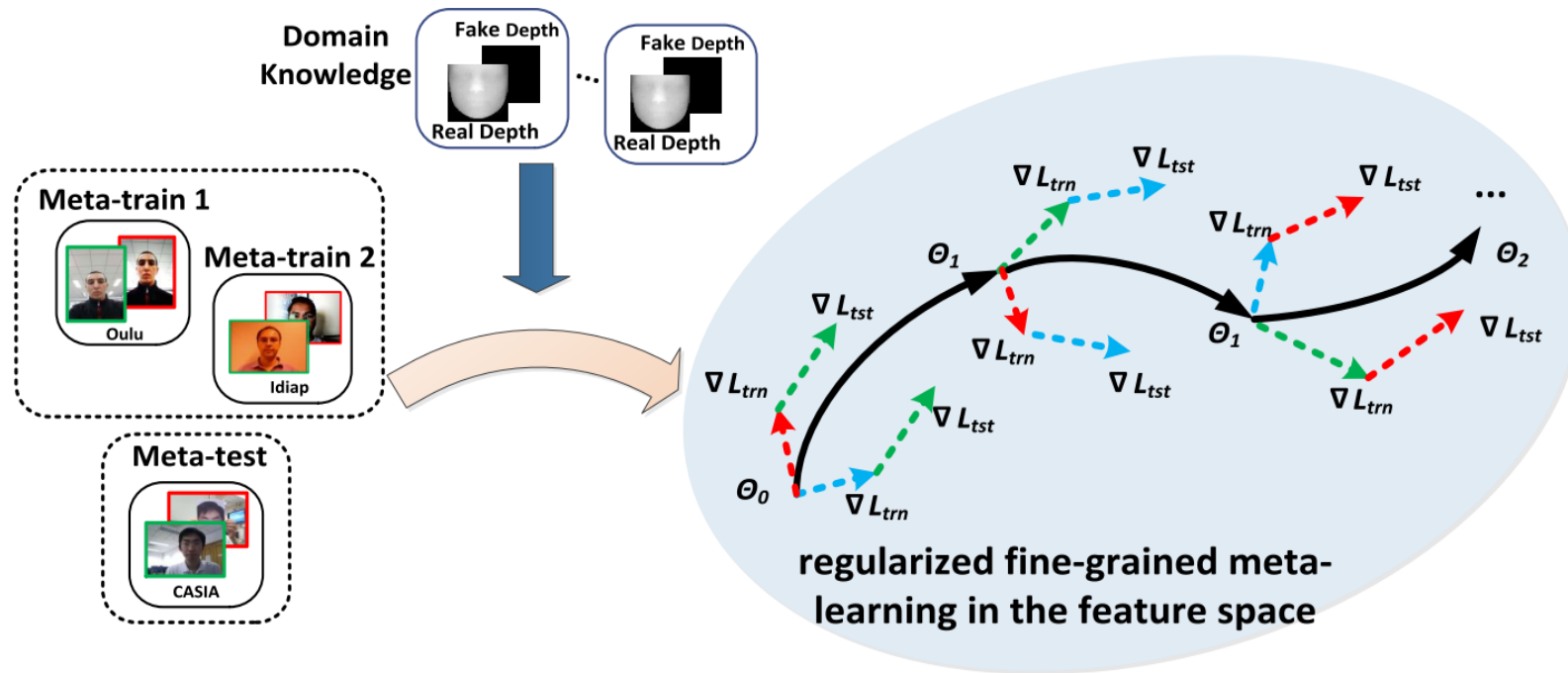


- A unified multi-adversarial discriminative deep domain generalization framework (**MADDG**):

$$\min_{G,E,C,Dep} \max_{D_1,D_2,\dots,D_N} \mathcal{L}_{MADDG} = \mathcal{L}_{DG} + \mathcal{L}_{Trip} + \mathcal{L}_{Dep} + \mathcal{L}_{Cls}$$



# 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**.

# 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.

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



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

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

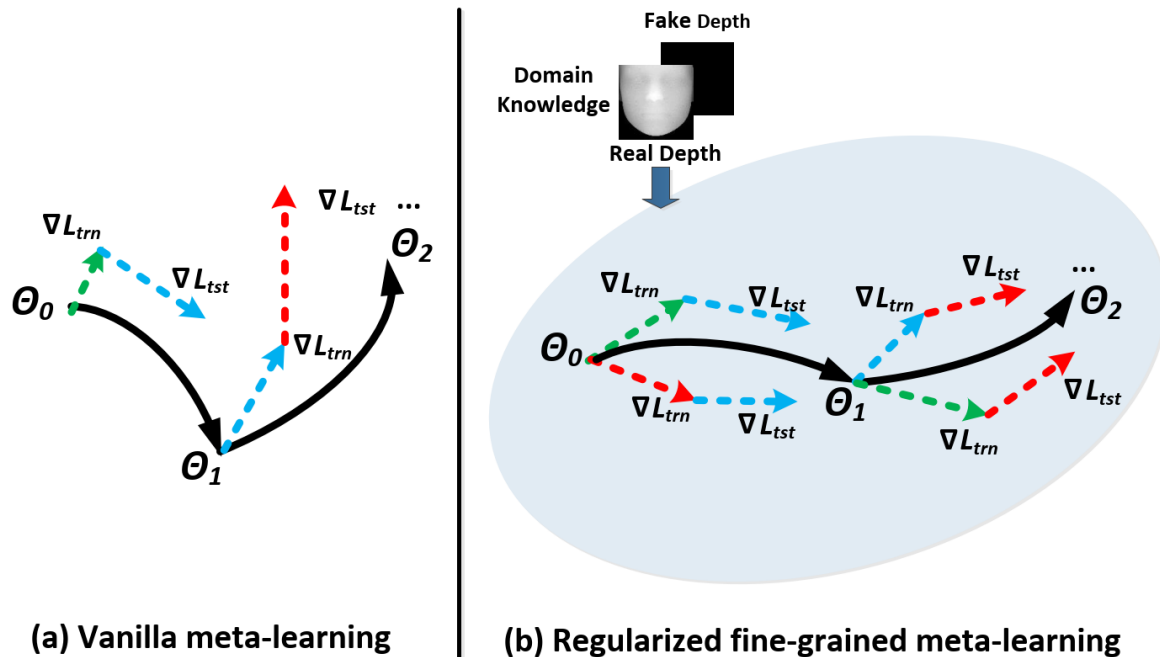
- Second issue:

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

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

## ■ Idea :



## ■ For first issue:

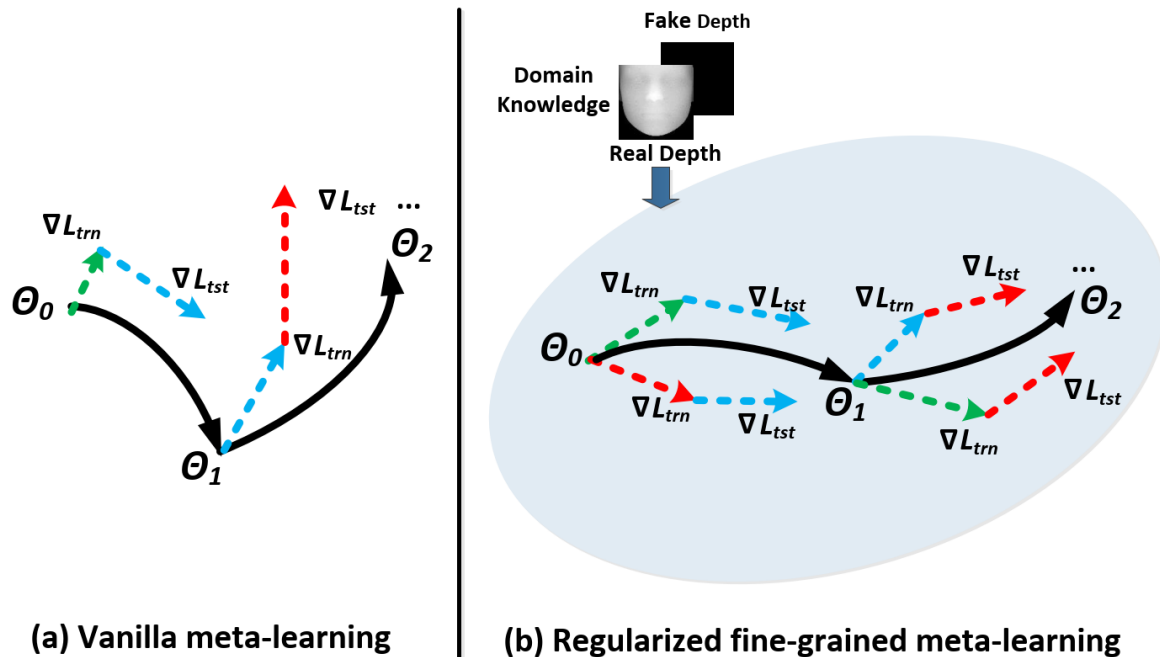
Incorporate the domain knowledge of face anti-spoofing as regularization into feature learning process

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

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

## ■ Idea :

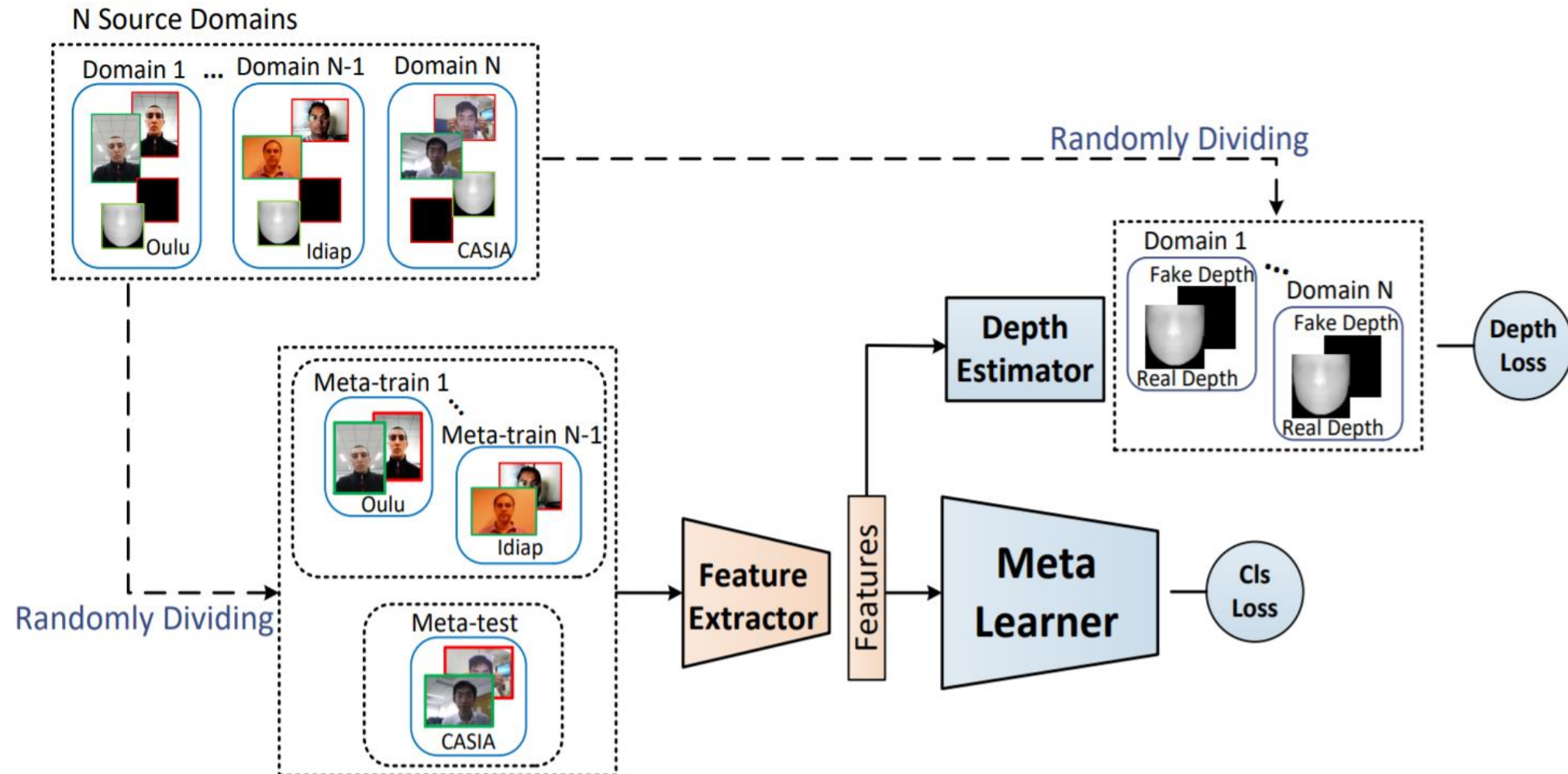


## ■ For second issue:

**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.

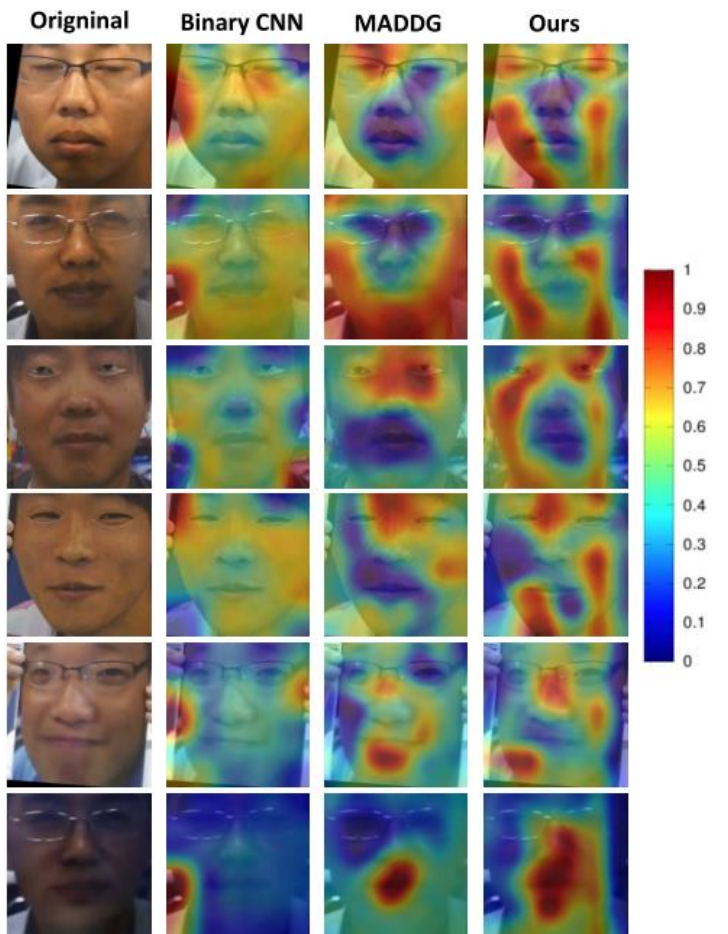
A **variety of domain shift scenarios** are **simultaneously** simulated and thus more abundant domain shift information can be exploited

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



# 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.



# New dataset: HKBU-MARs

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



(a) Room light

(b) Low light

(c) Bright light



(d) Warm light

(e) side light

(f) Up side light



(a)

(b)

(c)

(d)

(e)

(f)



(g)

(h)

(i)

(j)

(k)

(l)

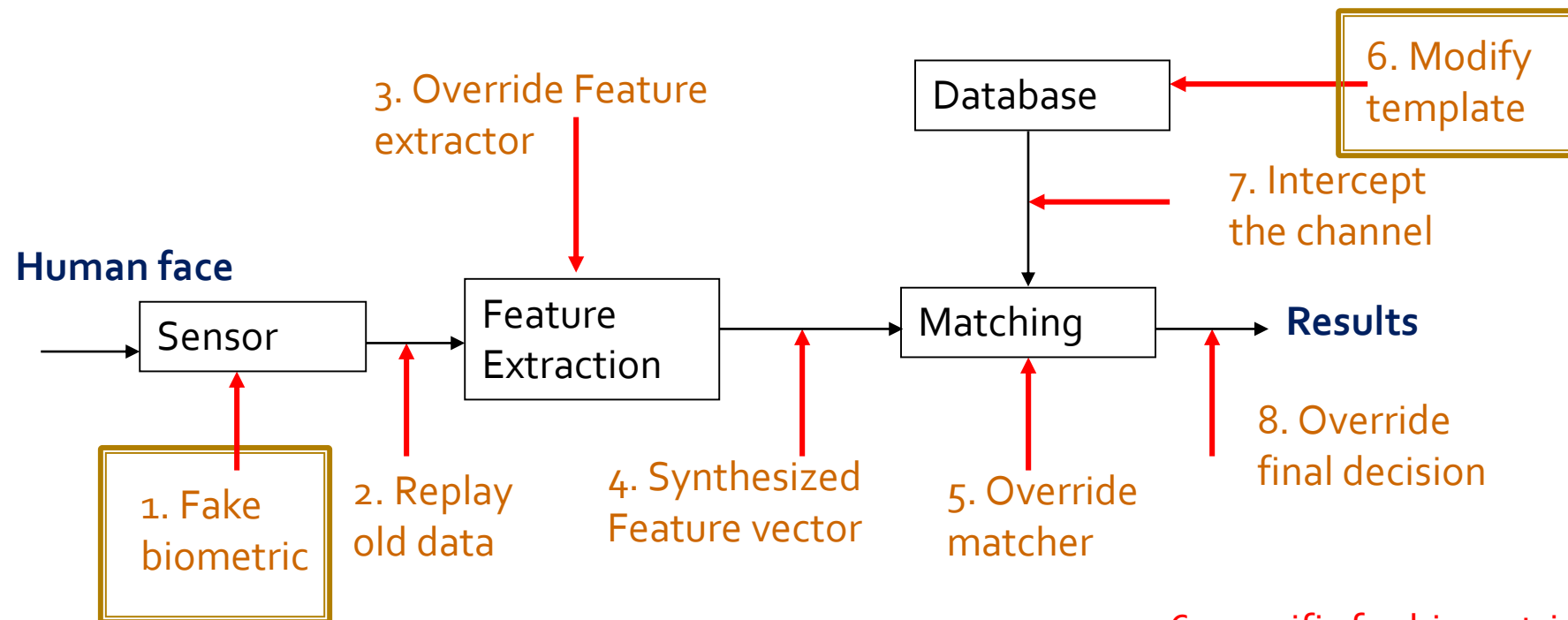
# Part II:

# Face Template Protection



# Biometric Systems are INSECURE!

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



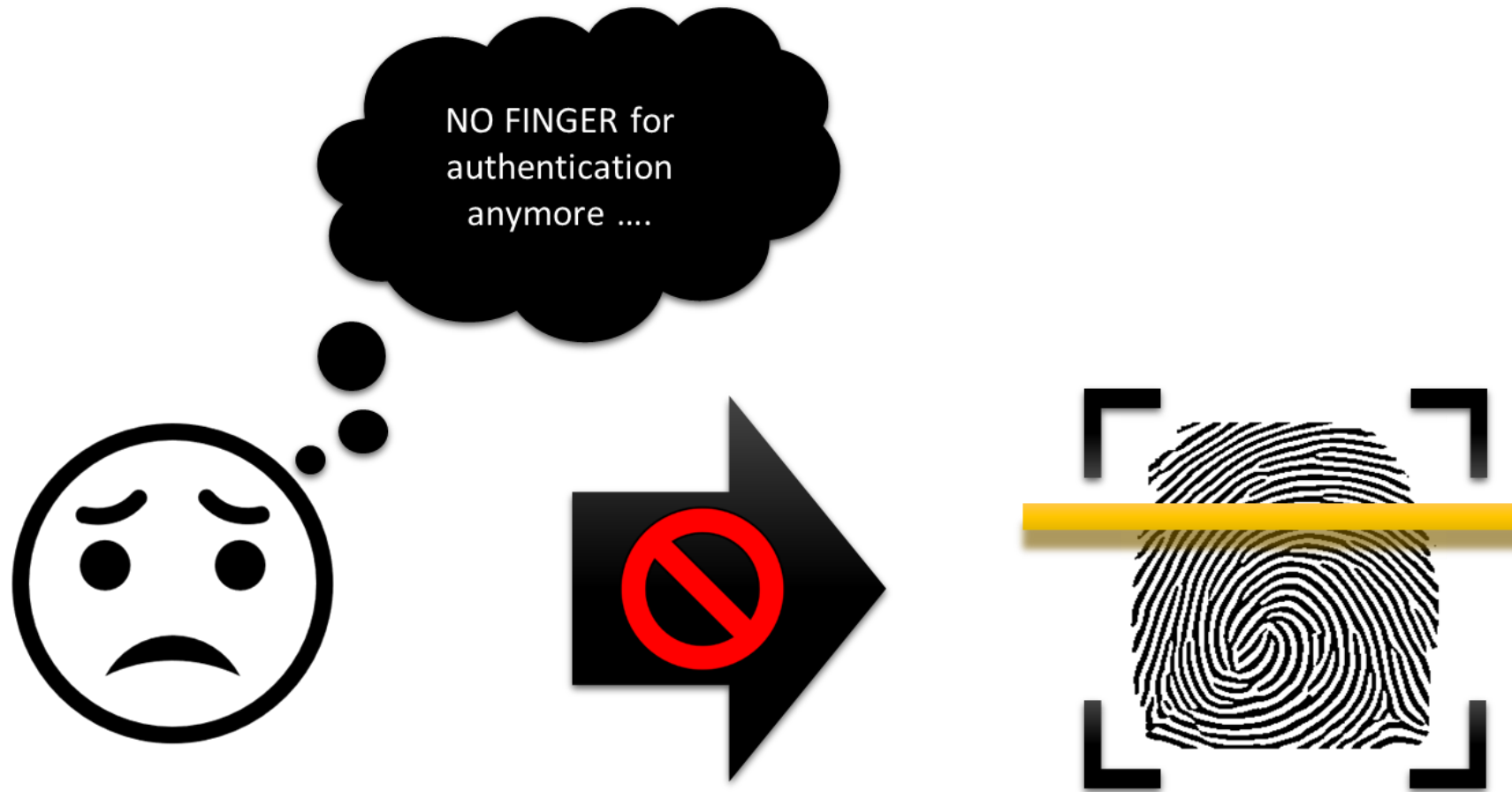
1, 6: specific for biometric systems

# The Consequences of Template Attack



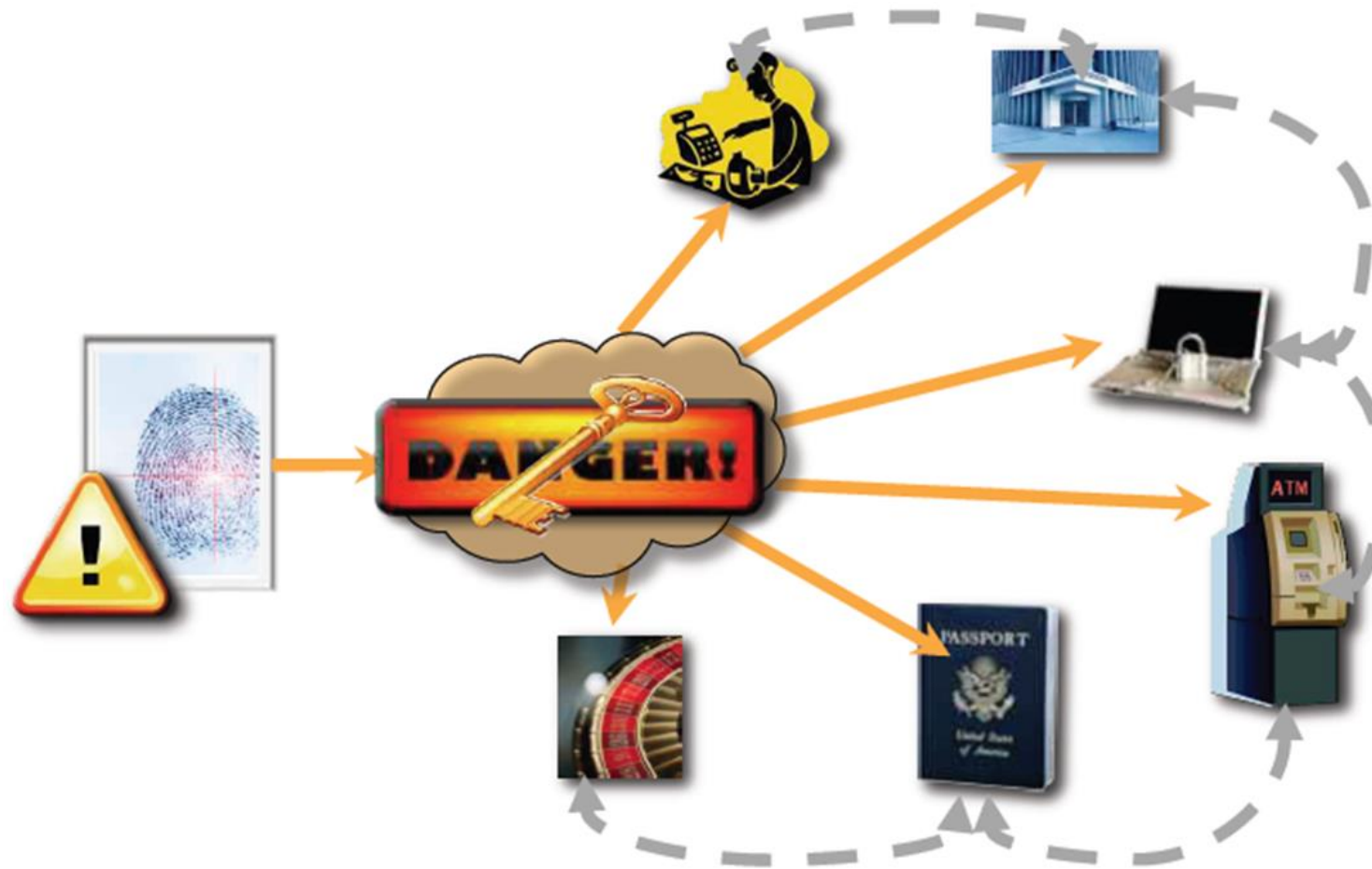
The stolen biometric template  
= Identity Theft

# The Consequences of Template Attack



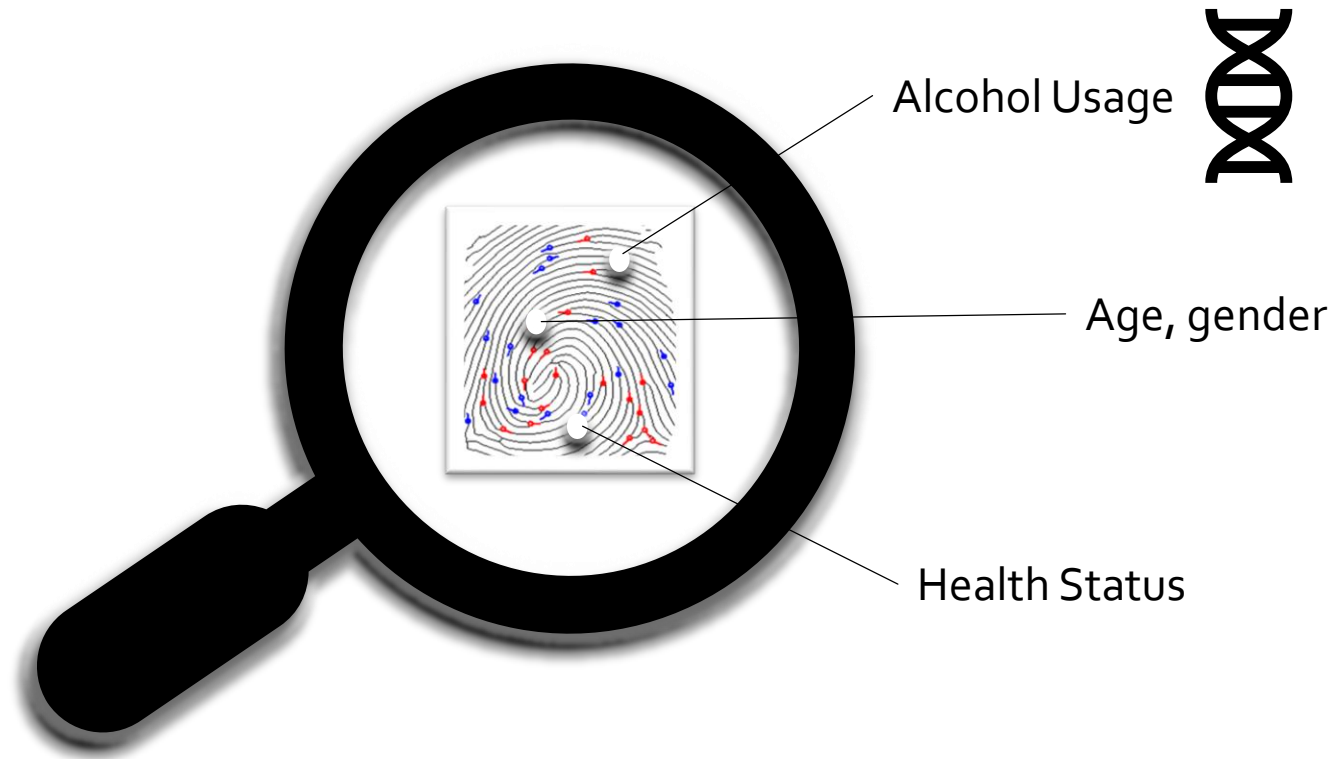
Limited Biometrics and Irrevocable

# The Consequences of Template Attack



Cross-matching

# The Consequences of Template Attack



Privacy Leakage

# Requirements

## Security

- Computationally hard to reconstruct the original template from the secure template.

## Discriminability

- The discriminative power of the secure template should be as good as that of the original face template so that system performance will not be affected.

## Cancelability

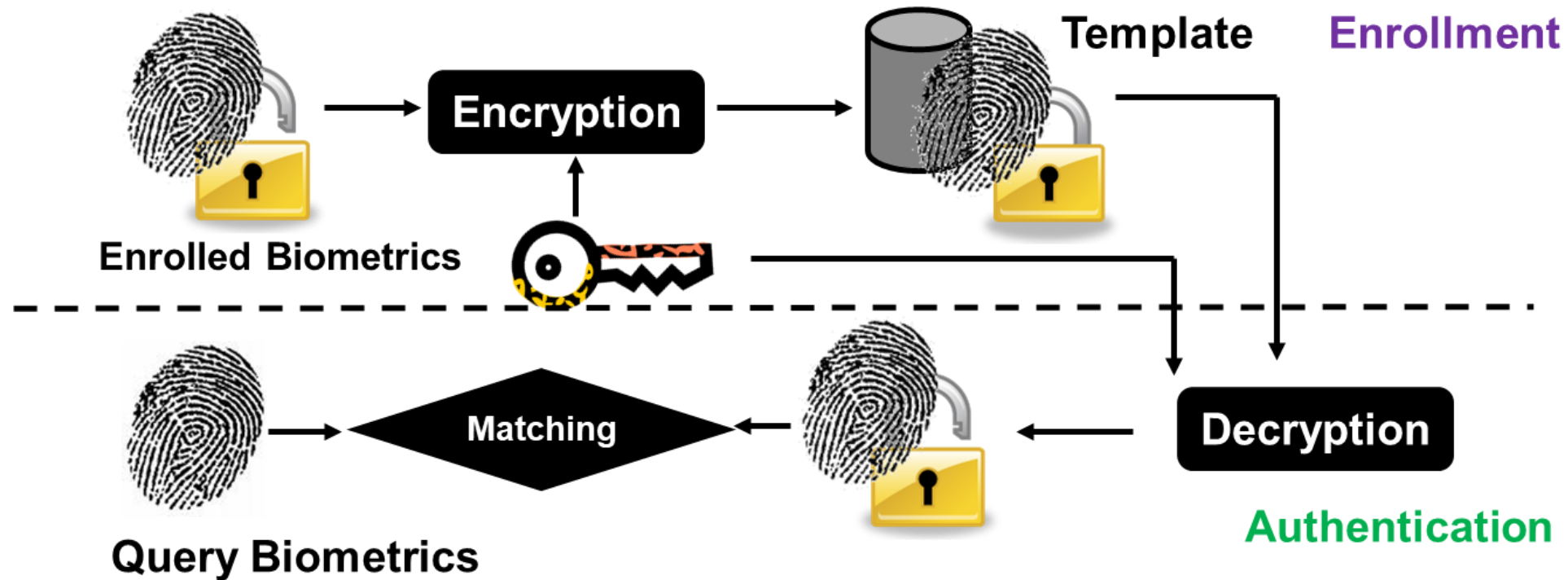
- The secure template can be canceled and re-issued from original template if it is stolen or lost.



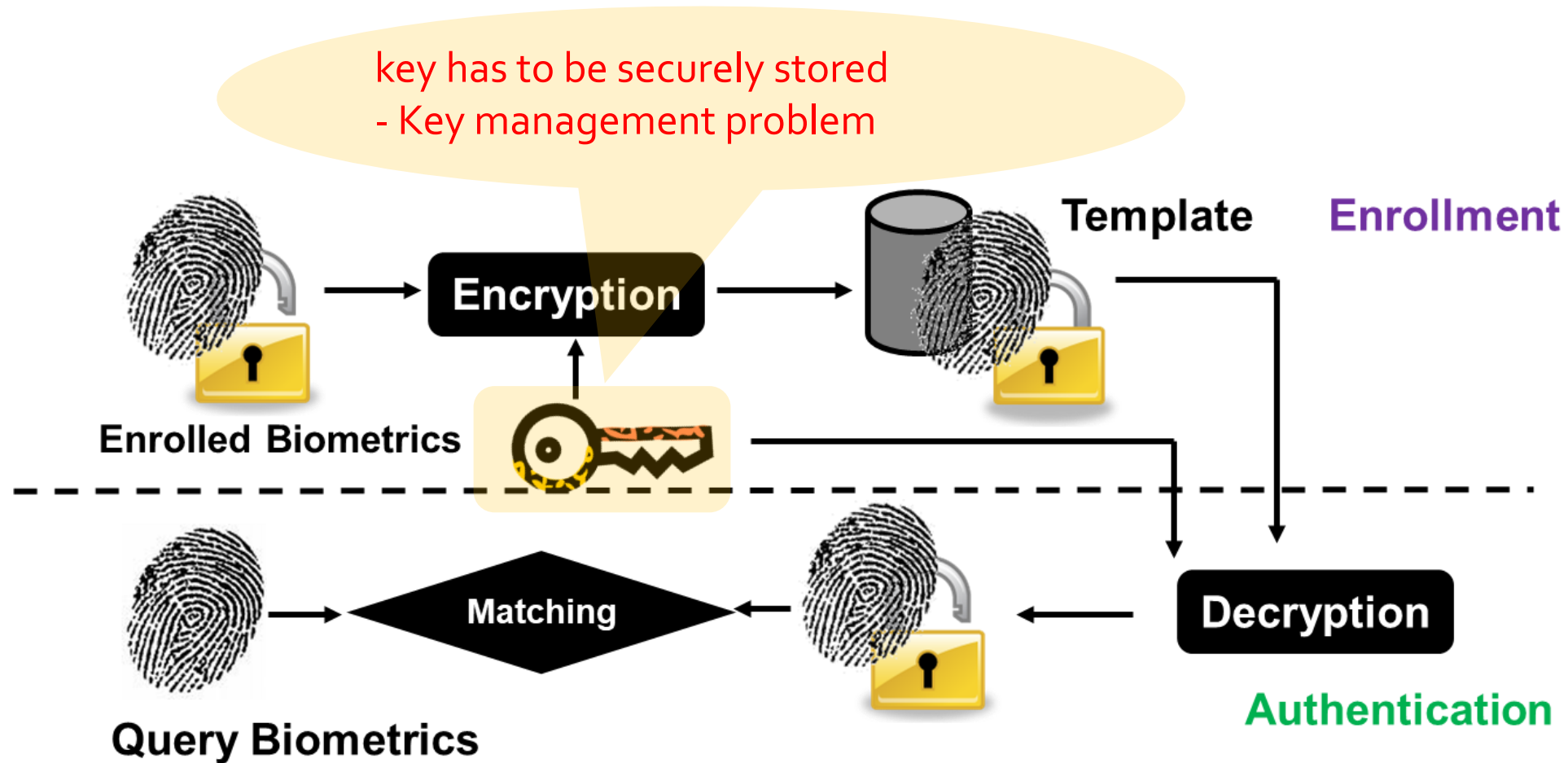
# Basic Idea

- General approach: *Never* store the original raw biometric template
- Straightforward method: Protection with traditional encryption/hashing methods (e.g. DES, MD5)
  - Small change in input cause large change in output
  - Intra-class variations => not good for matching
  - Not feasible

# Present Commercial Solution



# Not an Ideal Solution



# Existing Approaches

## Biometric cryptosystem

- Encrypt the original templates to a helper data
- Apply error-correcting coding methods to handle intra-class variance
- Require input in finite fields

## Transform-based

- Transform the original templates into a new domain
- Apply one-way transforms
- Cancelable
- High trade-off between discriminability and security

# Our Works

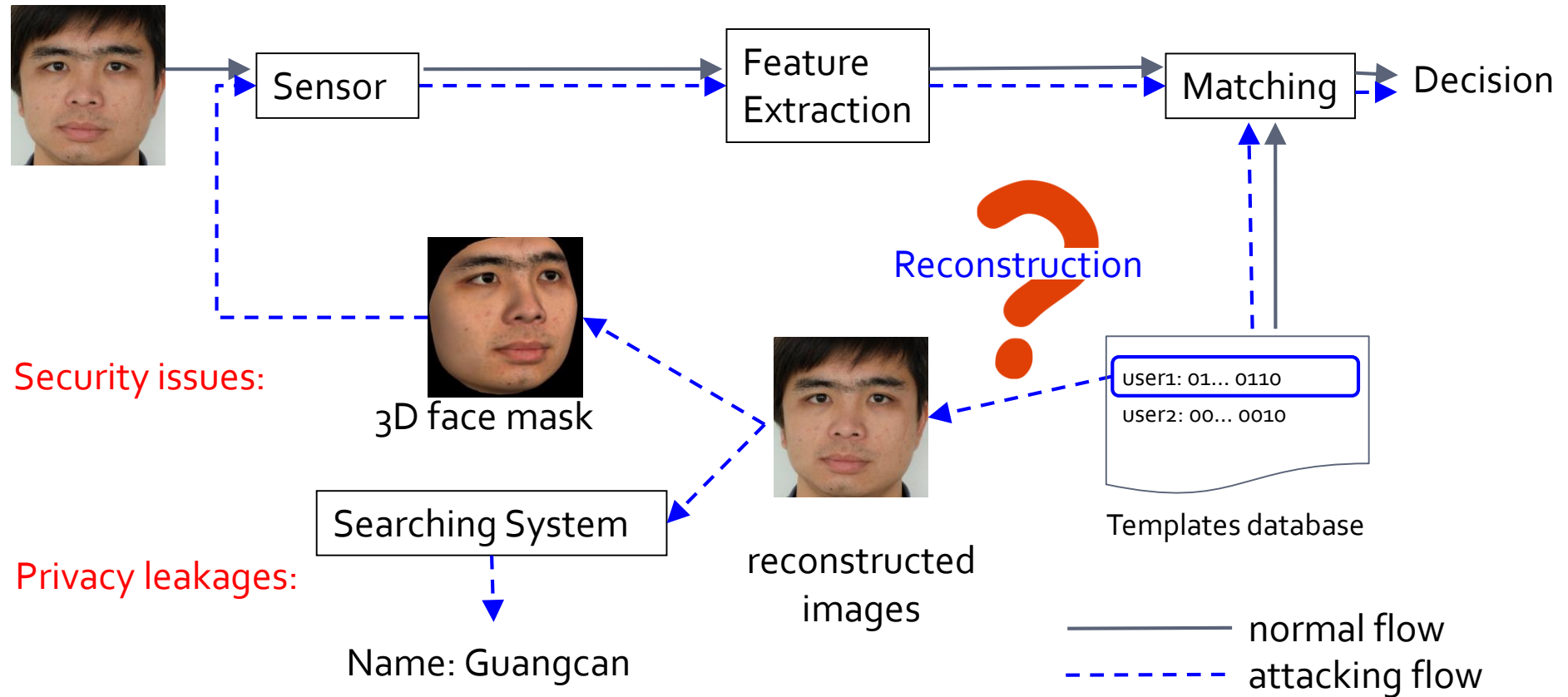
## Previous Work on Template Protection

- Hybrid Approach [TIFS 2010]
- Binary Discriminative Analysis for binary template generation [TIFS 2012]
- Unordered features for multibiometric feature-fused template protection, [PR 2016]
- Binary template fusion for multi-biometric cryptosystems [IVC 2017]

## Recent Work on Template Protection using deep learning approach

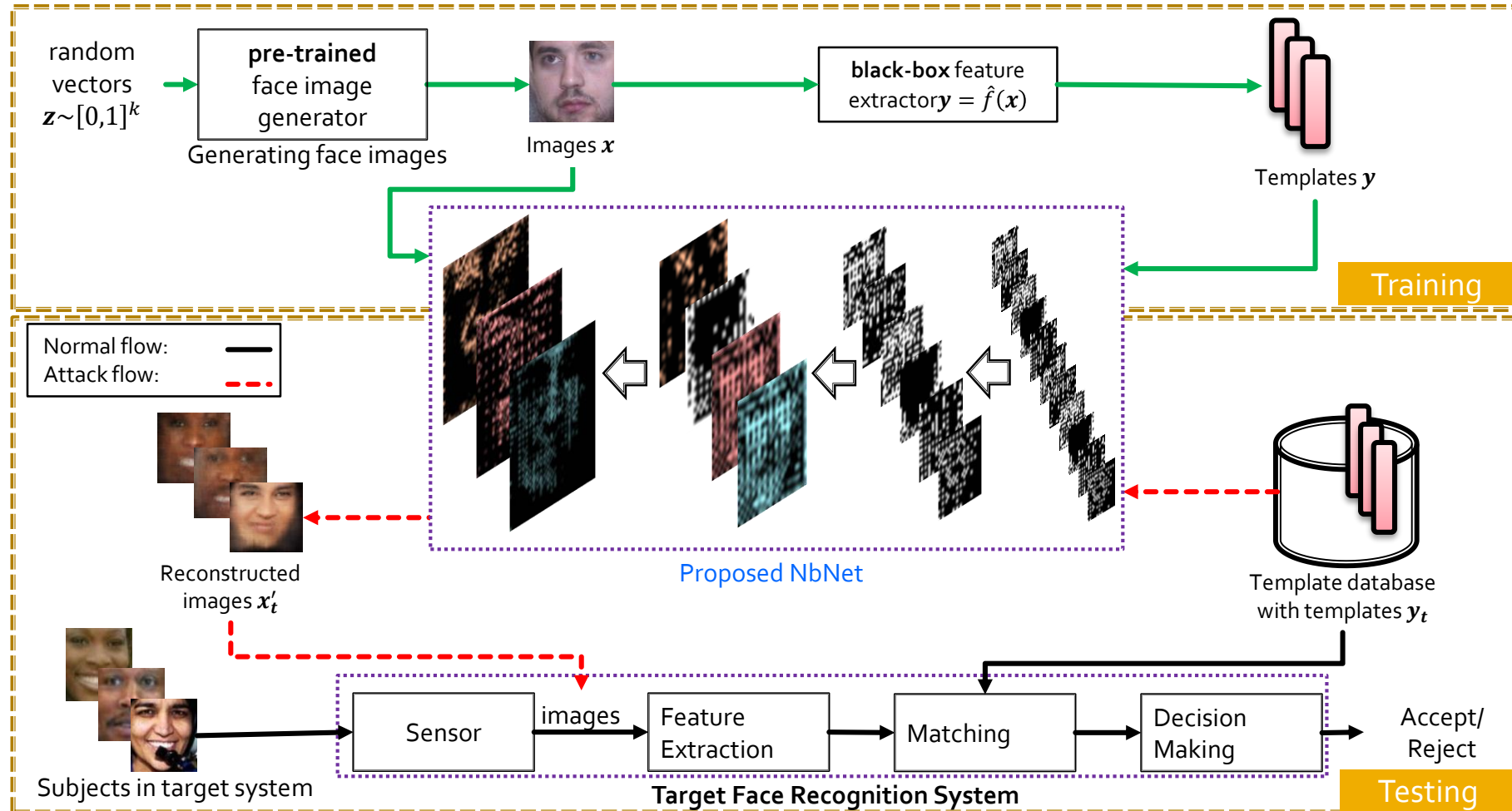
- On the Reconstruction of Deep Face Templates[*TPAMI* 2019]
- SecureFace [TIFS 2021]

# Image Reconstruction Attack [TPAMI 2019]

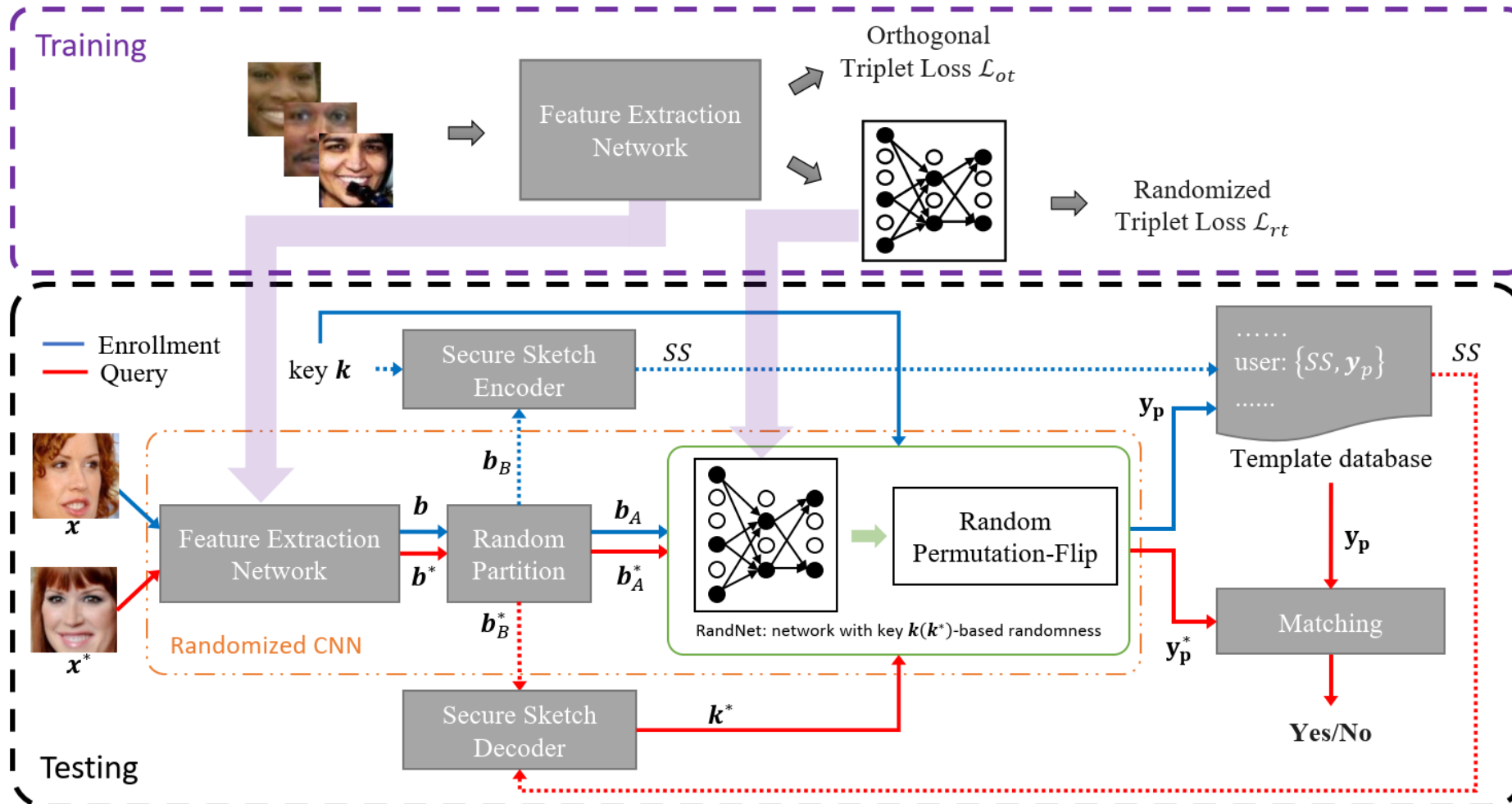




# Proposed Reconstruction- Overview



# SecureFace [TIFS 2021]



# Conclusions

- Biometrics security and privacy is an important issue for practical biometrics systems
- Research work in fake biometrics detection and biometrics template protection are discussed
- Security like a “cat and mouse” game
- More and continuous efforts are required

**Thank you!**

# References (Face Anti-spoofing)

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. "Eyeblick-based antispoofing in face recognition from a generic webcam", *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 (Face Anti-spoofing)

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, XY Lan and P CYuen, "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. XYang, 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 (Face Anti-spoofing)

- 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 (Face Anti-spoofing)

- 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 (Face Template Protection)

1. G C Mai, K Cao, X Y Lan and P C Yuen, "SecureFace: Face template protection", *IEEE Transactions on Information Forensics and Security*, In press, 2021
2. G. Mai, Kai Cao, P. C. Yuen and Anil K. Jain, "On the Reconstruction of Deep Face Templates", *IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI)*, 2019
3. G. Mai, M H Lim and P C Yuen, "Binary Feature Fusion for Discriminative and Secure Multi-biometric Cryptosystems", *Image and Vision Computing*, 2016
4. M H Lim and P C Yuen, "Entropy Measurement for Biometric Verification Systems", *IEEE Transactions on Cybernetics*, 2016
5. M H Lim, S Verma, G C Mai and P C Yuen, "Learning discriminability-preserving histogram representation from unordered features for multibiometric feature-fused template protection", *Pattern Recognition*, 2016
6. Y C Feng, M H Lim and P C Yuen, "Masquerade attack on transform-based binary-template protection based on perceptron learning", *Pattern Recognition*, 2014
7. YC Feng & PC Yuen, "Binary discriminant analysis for generating binary face template", *IEEE Transactions on Information Forensics and Security*, 2012
8. YC Feng, PC Yuen, AK Jain, "A hybrid approach for generating secure and discriminating face template", *IEEE Transactions on Information Forensics and Security*, 2010