Face Recognition System Security: Anti-spoofing and Template Protection

Pong C Yuen

Department of Computer Science
Hong Kong Baptist University

Outline

1. Background and Motivations
2. Face Anti-spoofing
3. Face Template Protection
4. Conclusions

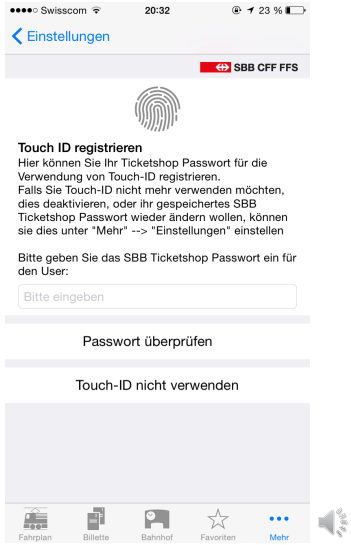
Biometrics

- 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

face-recognition payment Alipay

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

Source: china.com and iomniscient.com

Face Biometrics

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

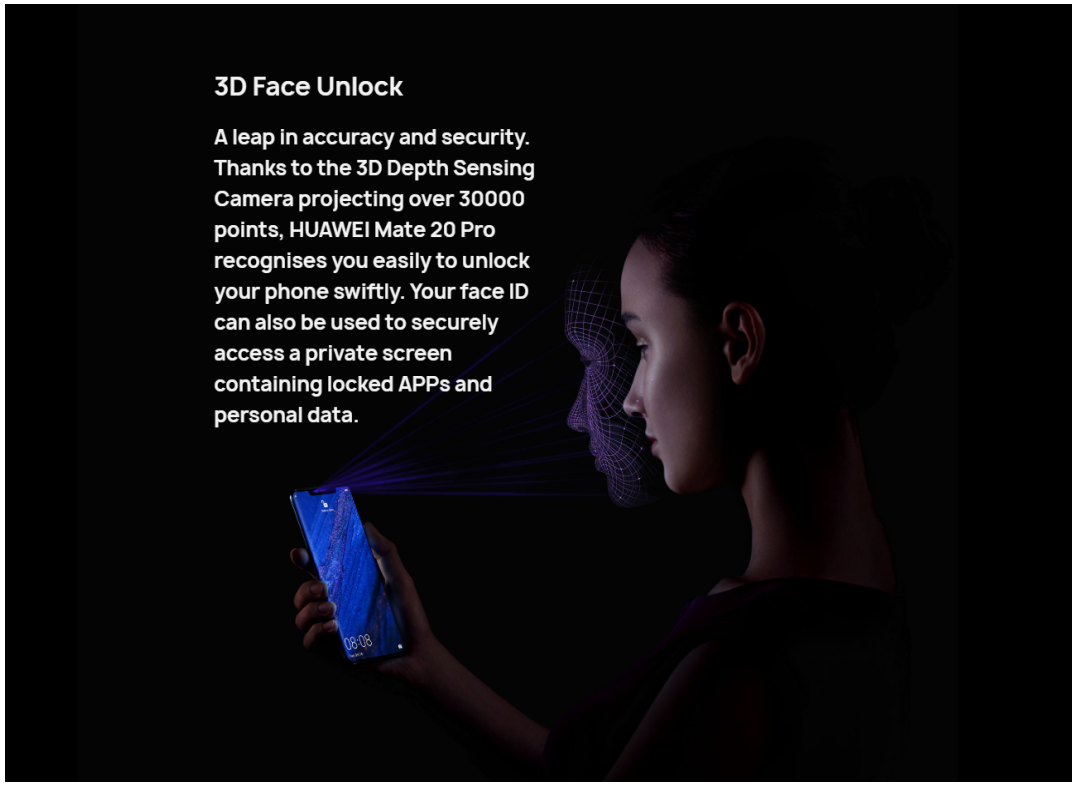
Face Biometrics

HUAWEI Mate 20 Pro

Nov 2018

Biometric Technology

Unlock Life's Possibilities

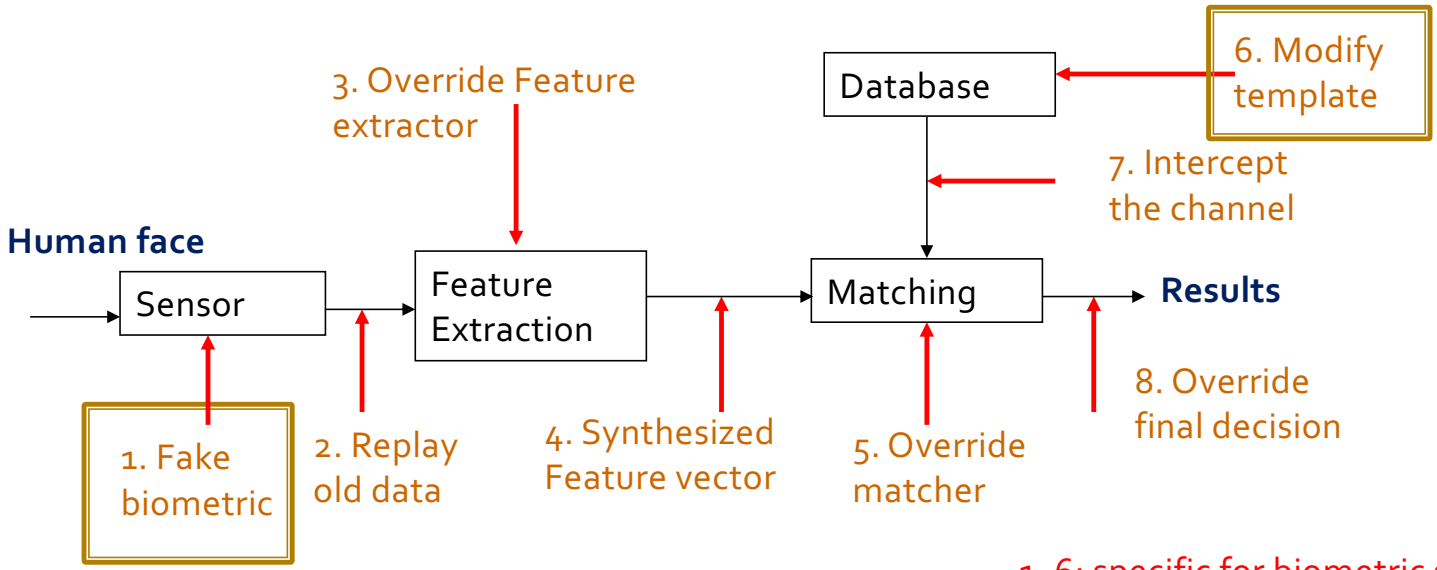


https://consumer.huawei.com/en/phones/mate20-pro/

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



Part I:
Face Anti-Spoofing

Mission Impossible - Rogue Nation (2015): Biometric Spoofing

Outline: Face Anti-spoofing: 3D Mask Attack

1. Background and Motivations
2. Related Work
3. rPPG Approach
4. Deep Learning Approach
5. Conclusions

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

Image and Video Face Anti-spoofing

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

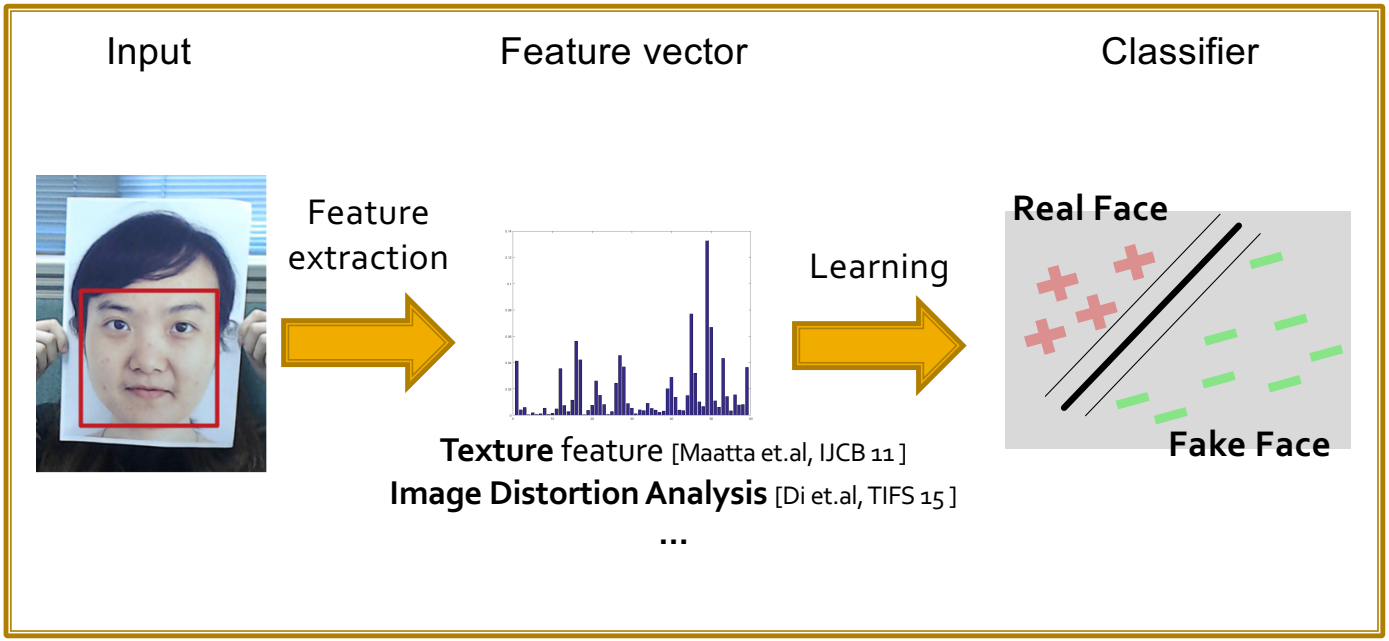
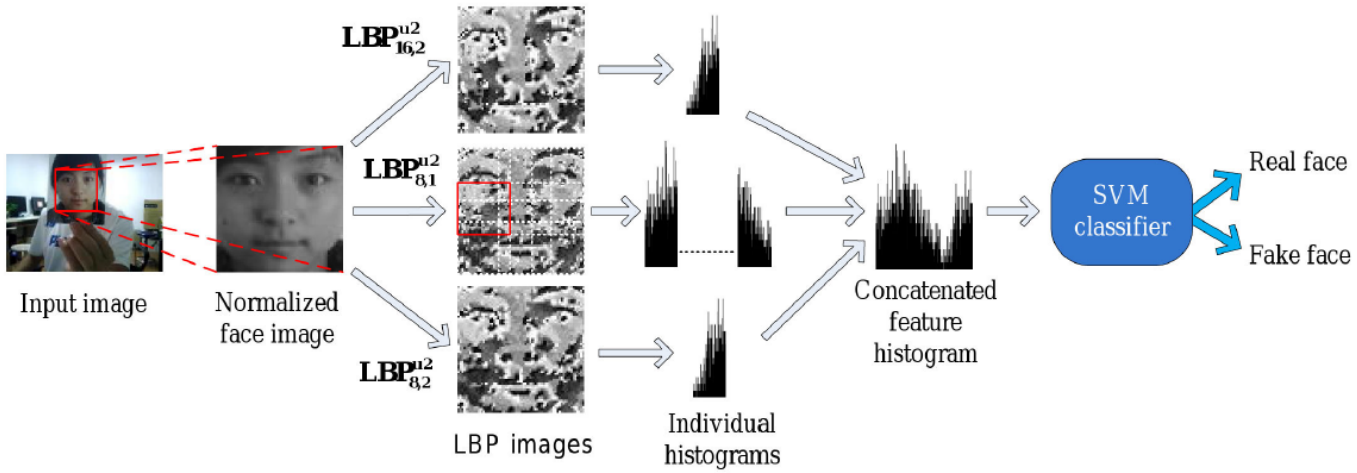


Image and Video Face Anti-spoofing

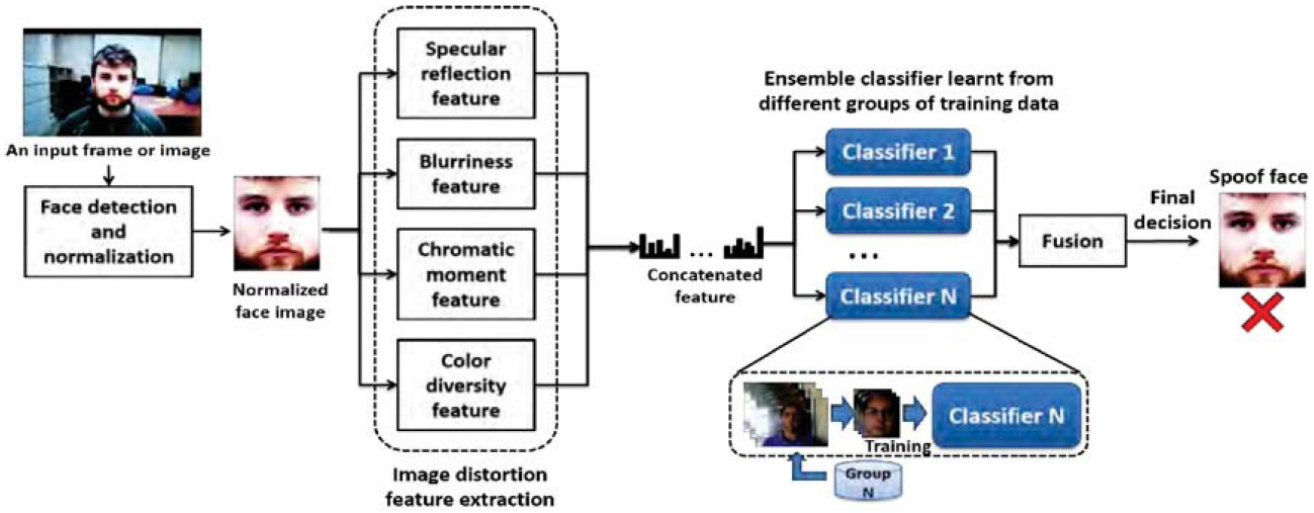
- Anti-spoofing approach: Appearance-based
  - Spoof media (Prints and screen) has different texture, comparing with genuine face



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

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

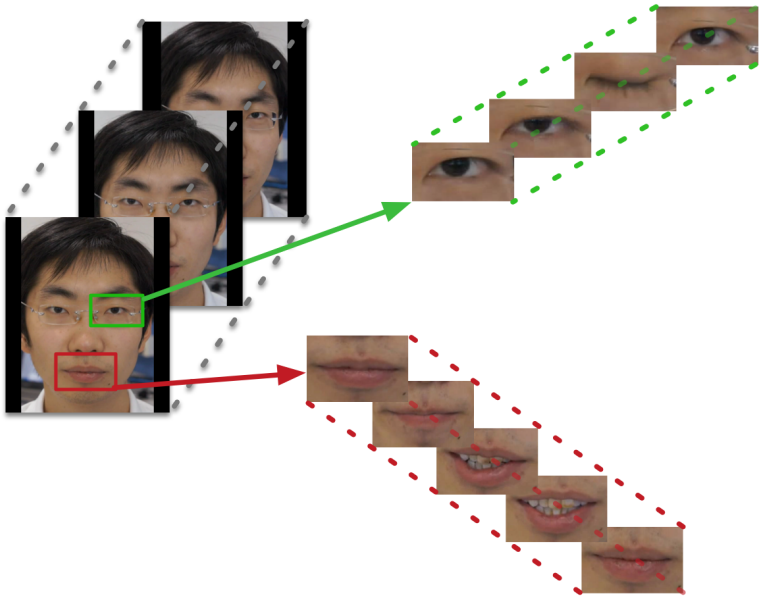
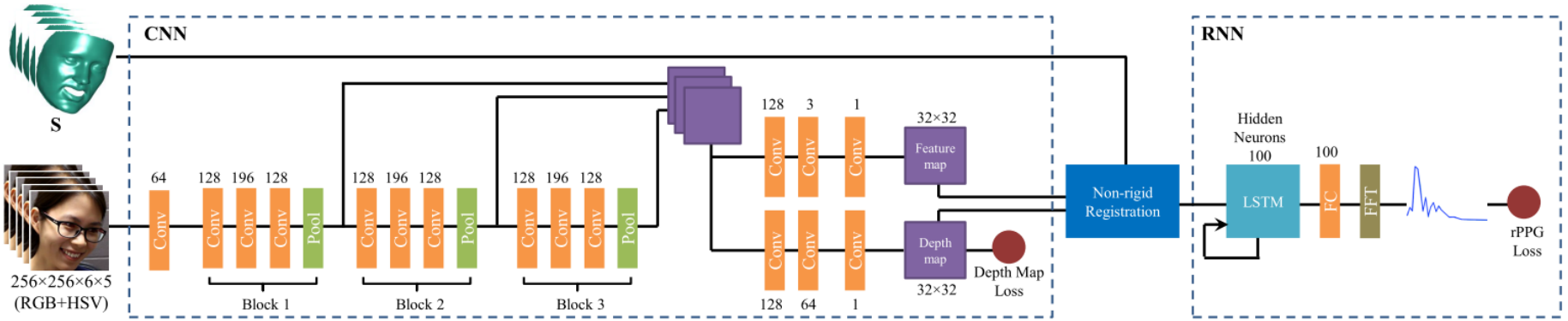


Image and Video Face Anti-spoofing

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

Background and Motivations

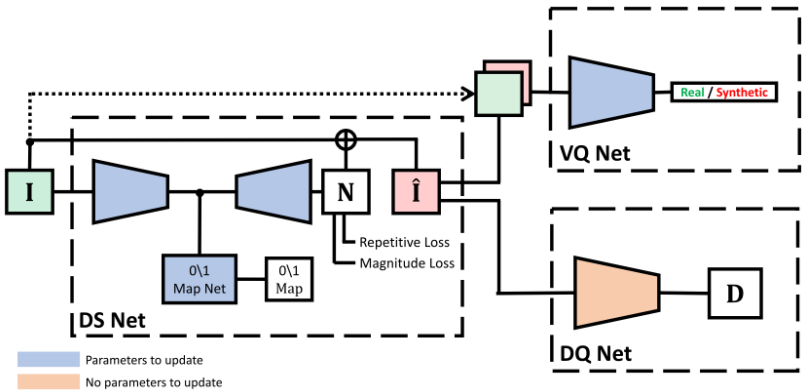
- Multiple modality approach
  - CNN: Learn different **face depth maps** at pixel-wise level +
  - RNN: Learn different **rPPG signals** with sequence-wise



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

Background and Motivations

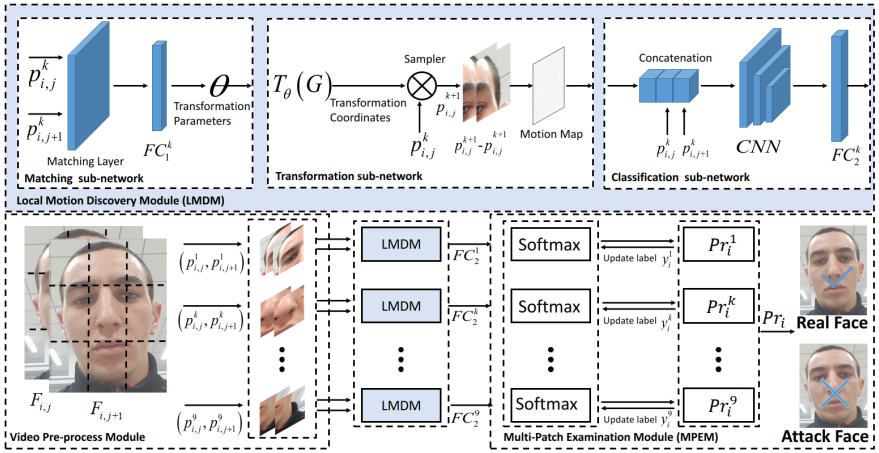
- Face de-spoofing approach
  - Inversely decompose a spoofed face into a spoof noise and a live face, and then utilizing the spoof noise for classification.
  - Real face: no spoof noise vs. Fake face: clear spoof noise



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

Background and Motivations

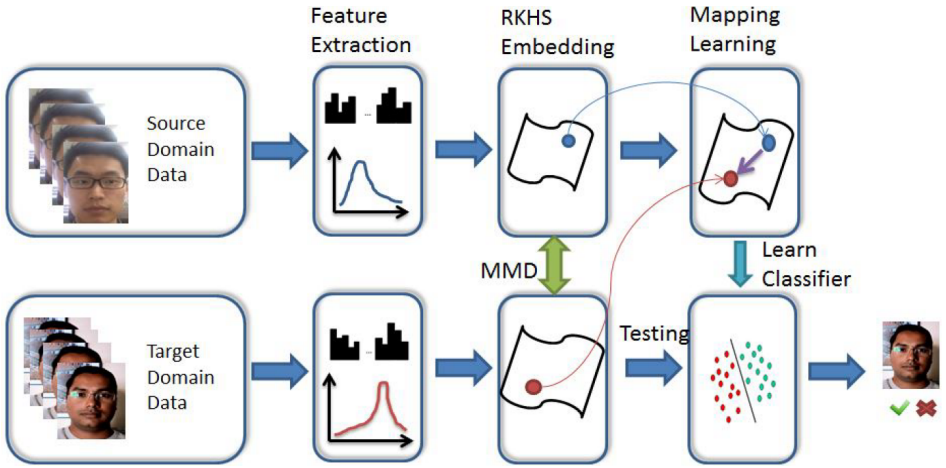
- Local homographic parameterization approach
  - Capture subtle motion difference between the facial movements from a planer screen and those from a real face
  - Multi-patch examination module enhances the recall rate of the attack videos



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

Background and Motivations

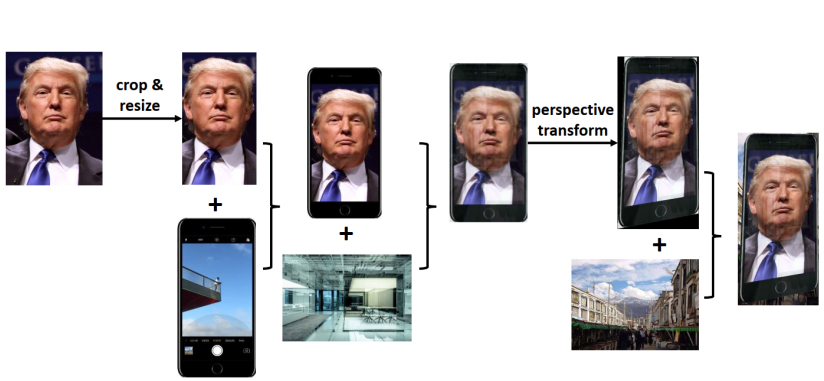
- Domain adaptation approach
  - An embedding function is imposed to map the data to a new space where source and target distribution similarity can be measured
  - Maximum Mean Discrepancy between the source and target latent features is minimized

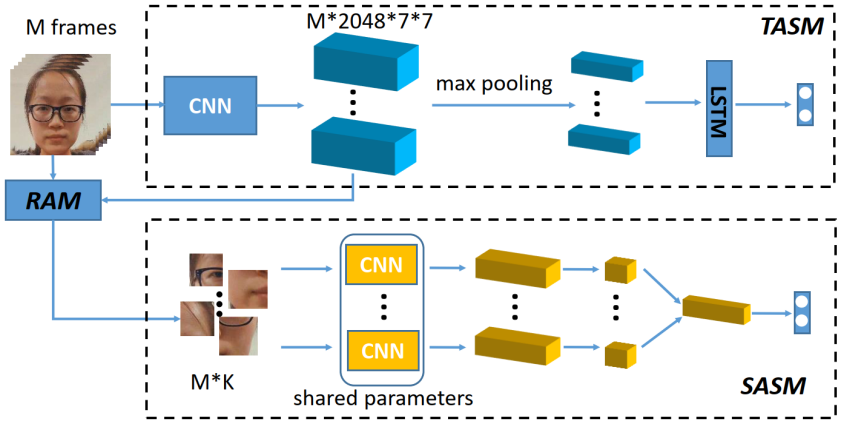


H Li, W Li, H Cao and et al. Unsupervised domain adaptation for face anti-spoofing, TIFS 2018

Background and Motivations

- 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

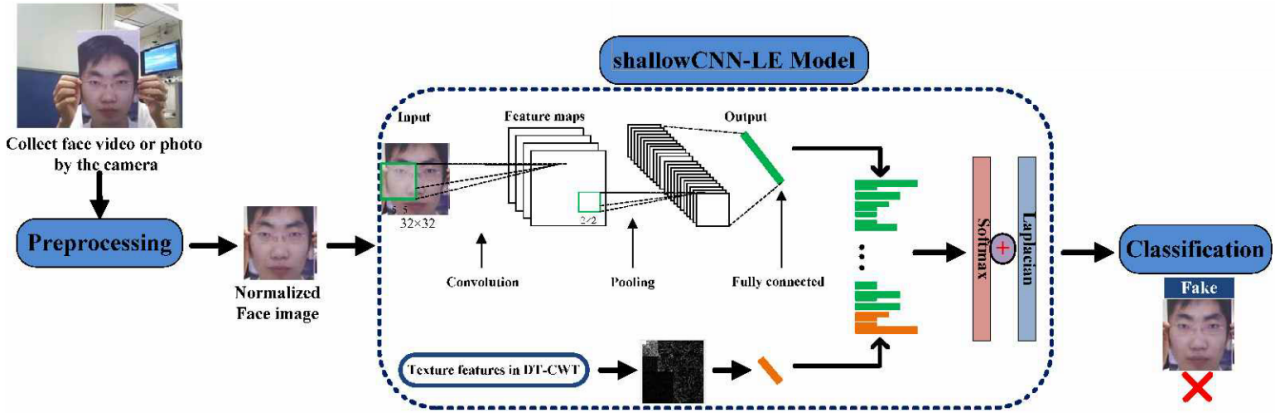




Yang X, Luo W, Bao L, et al. Face Anti-Spoofing: Model Matters, So Does Data, CVPR 2019

Background and Motivations

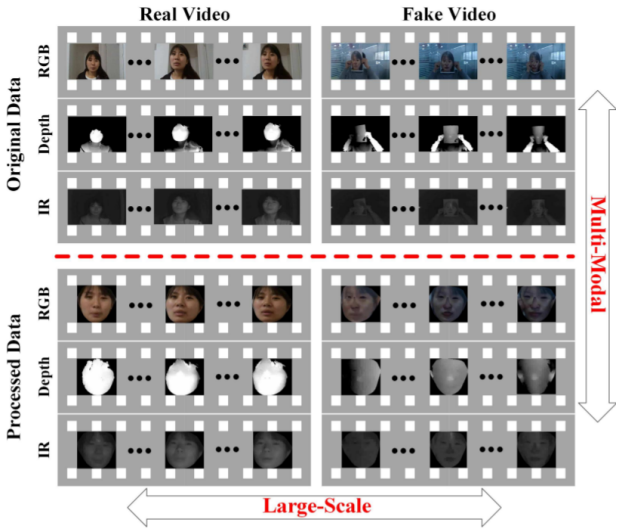
- Laplacian Embedding approach
  - Depth features and dynamic texture features are concatenated
  - A laplacian embedding algorithm is proposed to maintain the inter-class discrimination and penalize the distance of intra-class

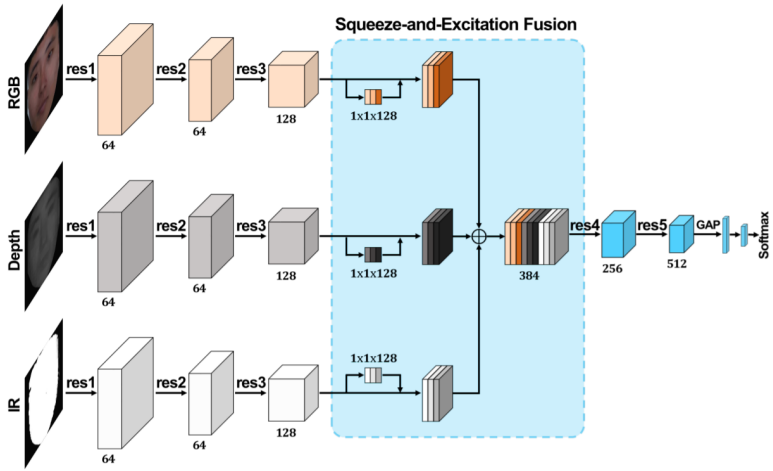


Qu X, Dong J, Niu S. shallowCNN-LE: A shallow CNN with Laplacian Embedding for face anti-spoofing, FG 2019

Background and Motivations

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





Zhang S, Wang X, Liu A, et al. A Dataset and Benchmark for Large-scale Multi-modal Face Anti-spoofing, CVPR 2019

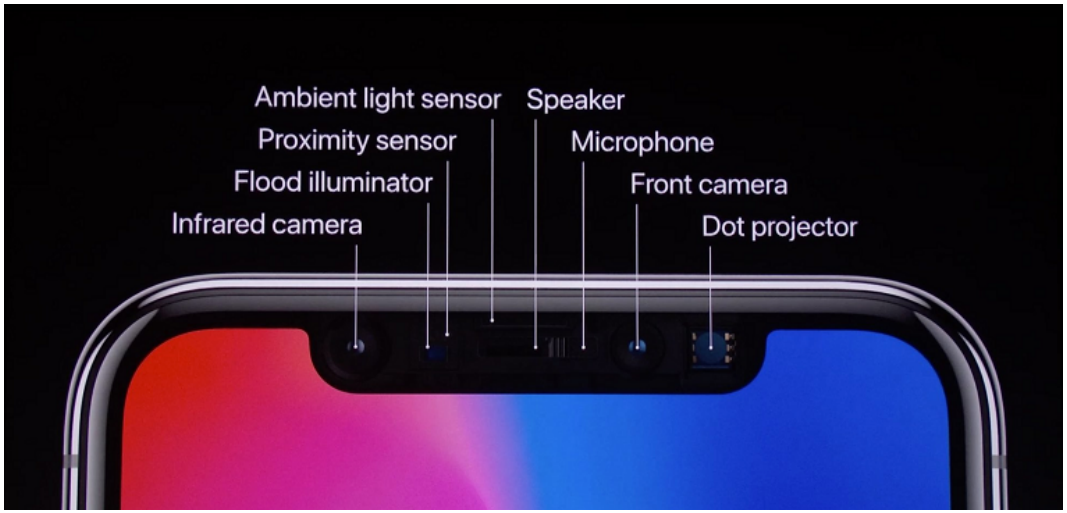
Image and Video Face Anti-spoofing

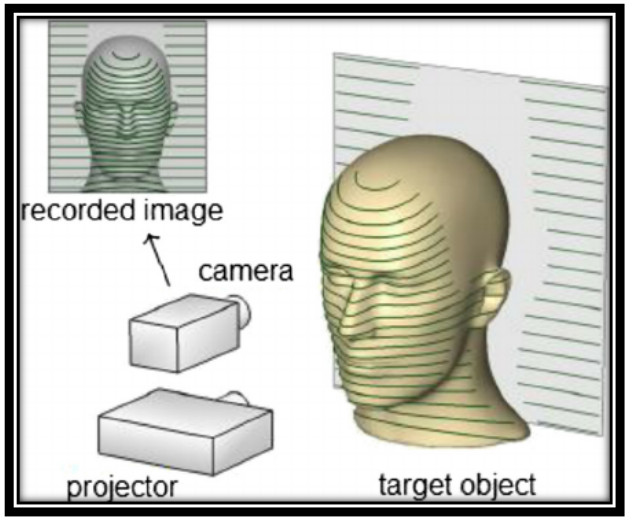
- Performance on traditional face spoofing attack

	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]

Structured-light 3D Technology

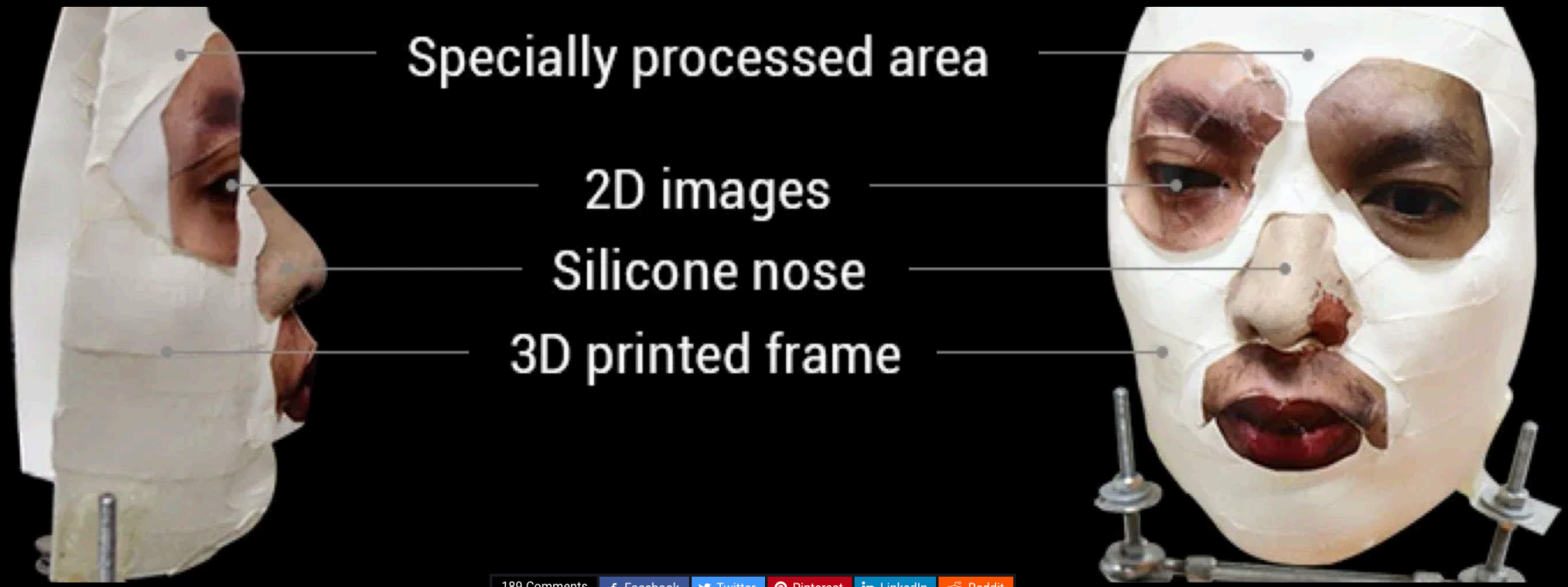




https://matterandform.net/blog/how-do-3d-scanners-work

Cybersecurity experts ‘beat’ Face ID with carefully constructed 3D mask

Benjamin Mayo - Nov. 13th 2017 4:08 am PT @bzamayo



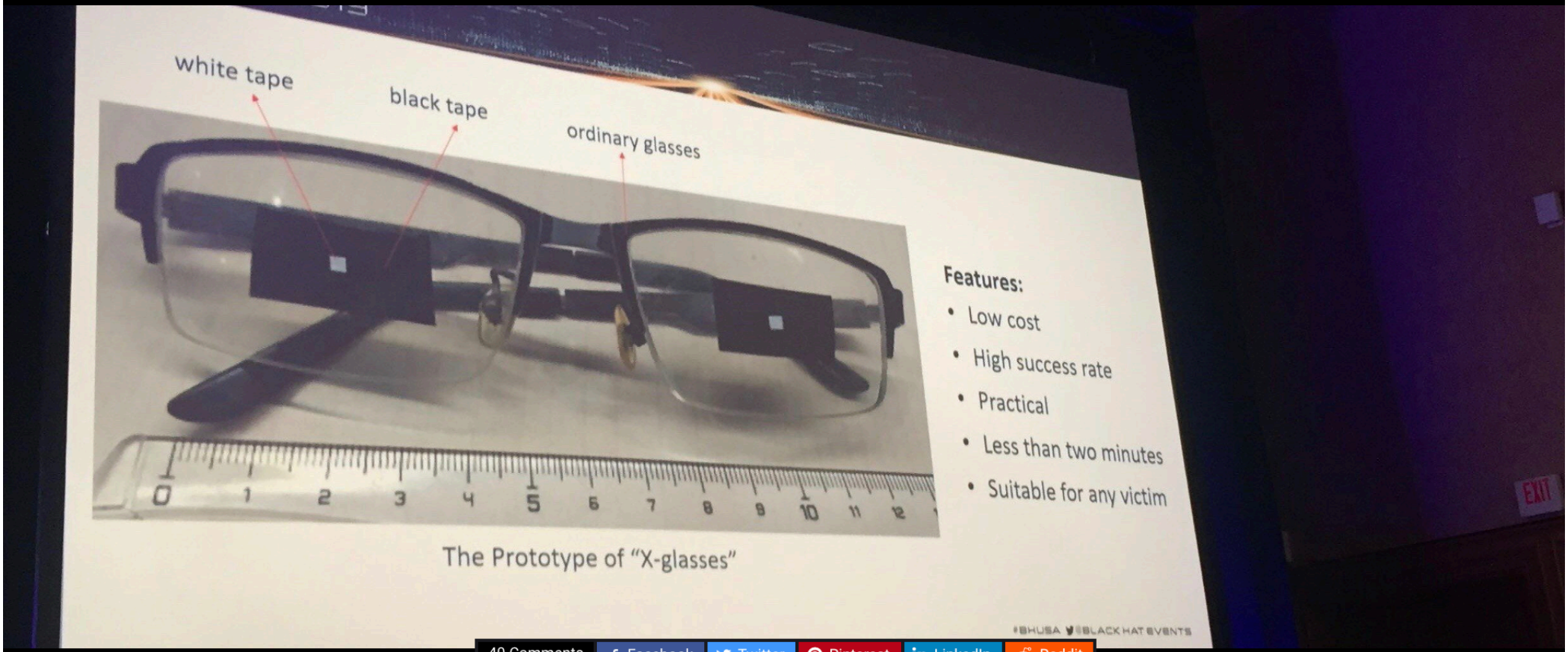
189 Comments Facebook Twitter Pinterest LinkedIn Reddit

Reminders

ity firm have apparently successfully tricked Face ID into unlocking with a specially made

Security researchers demonstrate how to bypass Face ID with glasses and tape

Chance Miller - Aug. 8th 2019 5:37 pm PT @ChanceHMiller

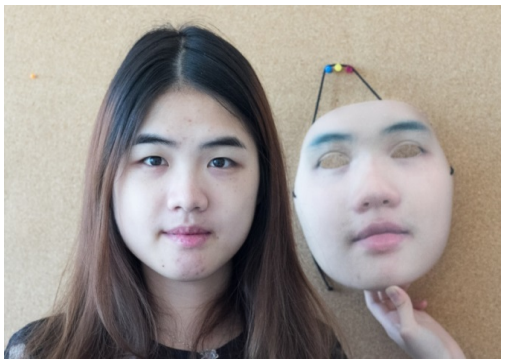


40 Comments Facebook Twitter Pinterest LinkedIn Reddit

At the Black Hat security conference today, researchers demonstrated a unique way to bypass Face ID

3D Mask Face Anti-spoofing

- **New Challenge**: 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 Anti-spoofing

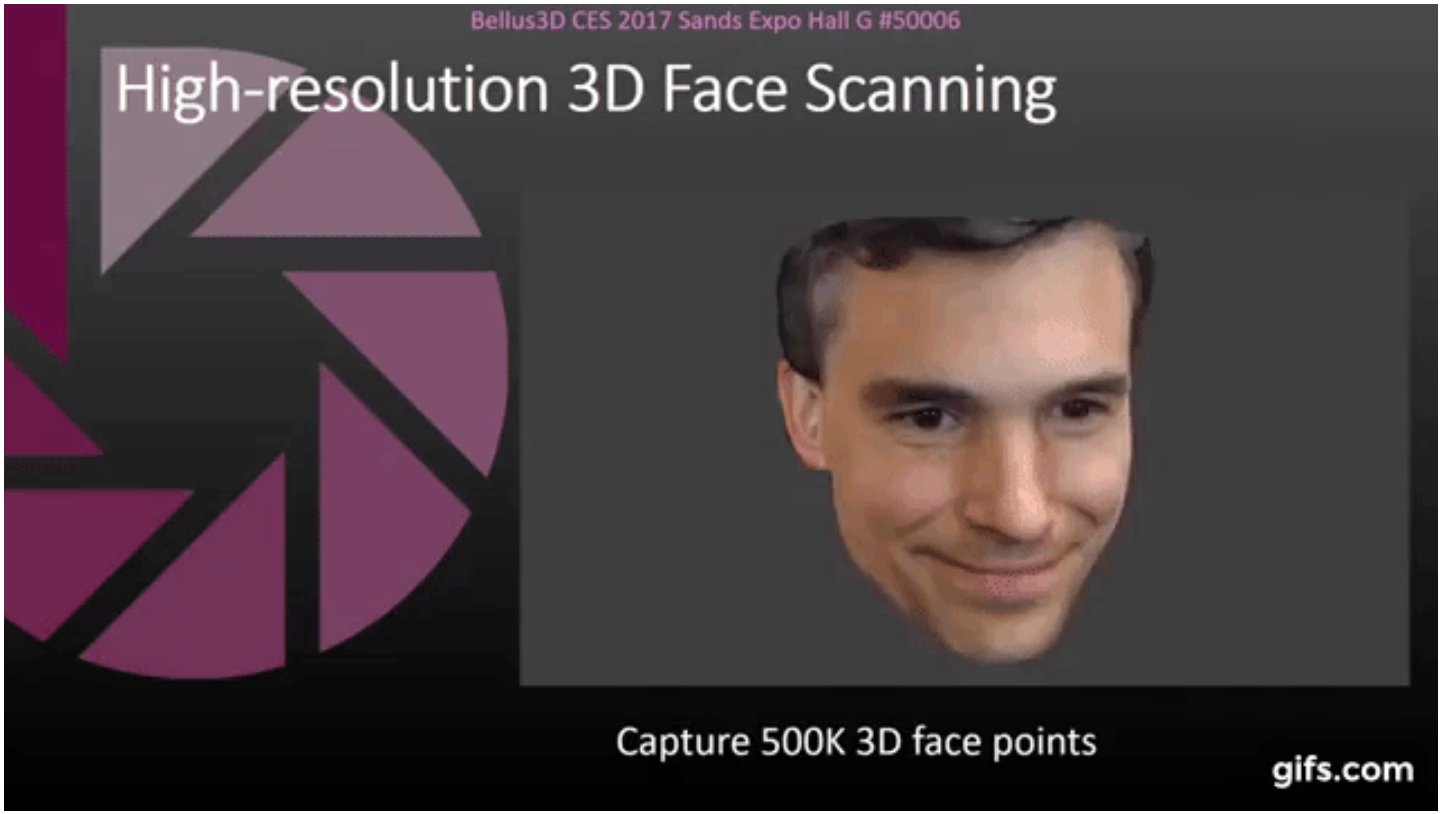
- **New Challenge**: Super-realistic 3D Mask

(a) Life face

(b) Real-F hyper real mask

Source: real-f.jp

3D Mobile Apps: Bellus3D



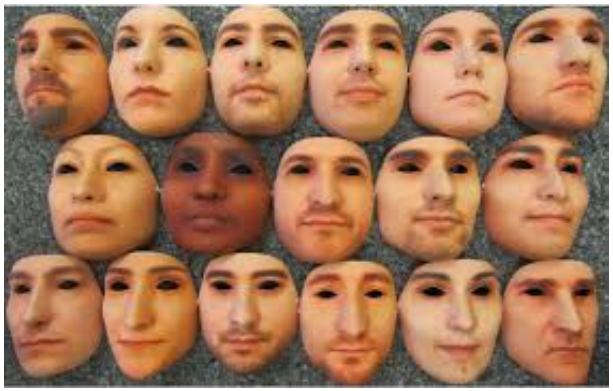
BBC NEWS

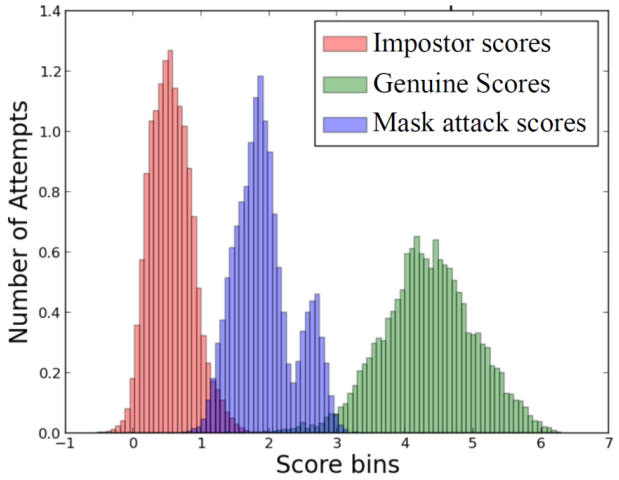
Brazil drug dealer dresses up as daughter in bungled jail escape

05 August 2019 | Latin America & Caribbean

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

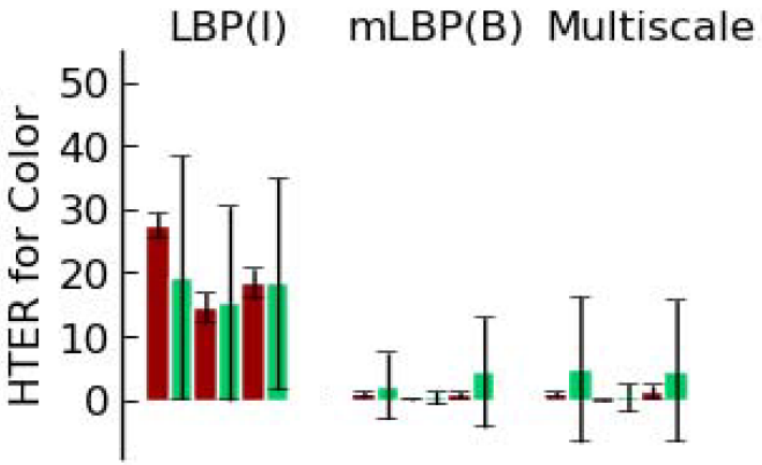


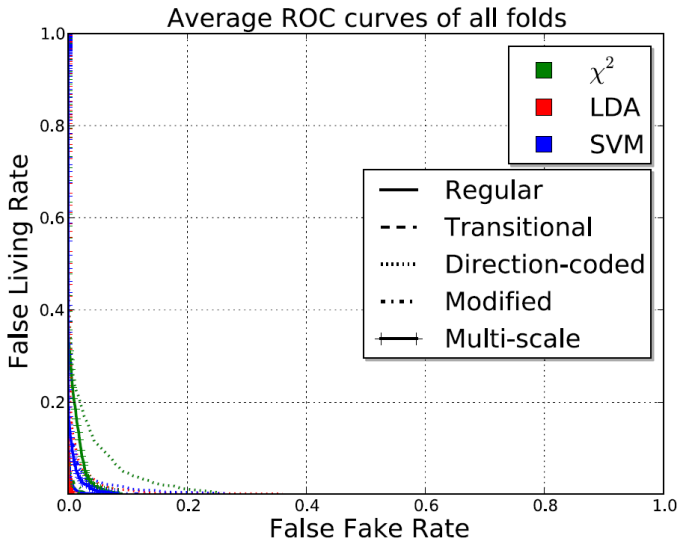


[Erdogmus et al., BTAS'13]

3D Mask Face Anti-spoofing

- LBP-based solution
  - The multi-scale LBP features yield to very good results on 3DMAD





[Erdogmus et al., TIFS'14]

Analysis of Existing Methods

- Pros and Cons

  √ Achieve high performance in 3DMAD dataset

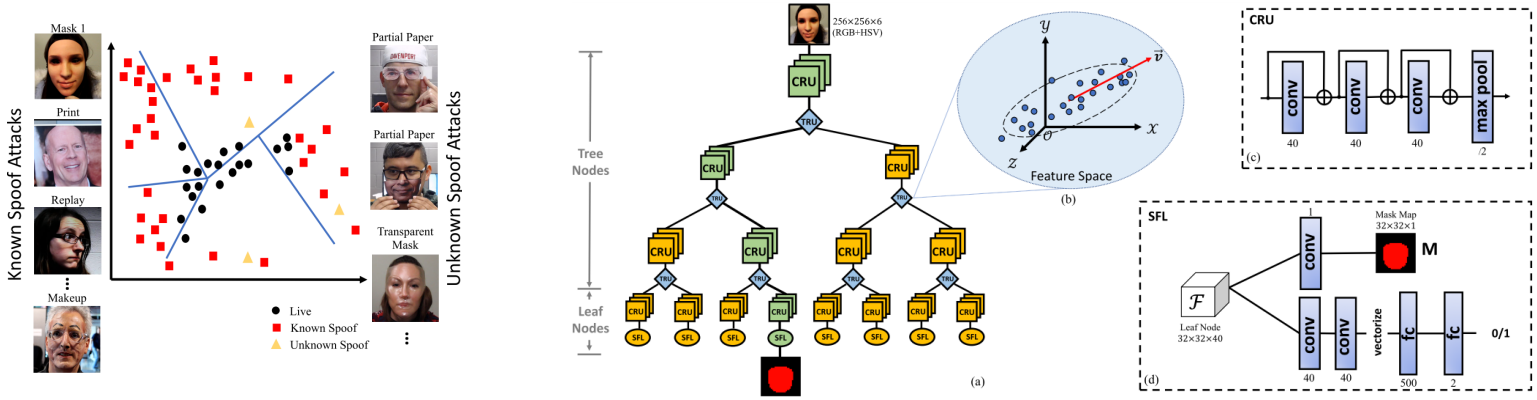
  × Hyperreal 3D mask may not have quality defects

  × LBP-based solution may not perform well under cross database scenario

- What do we need?
  - A new discriminative liveness cue
  - More 3D mask datasets for comprehensive experiments

Other recent works

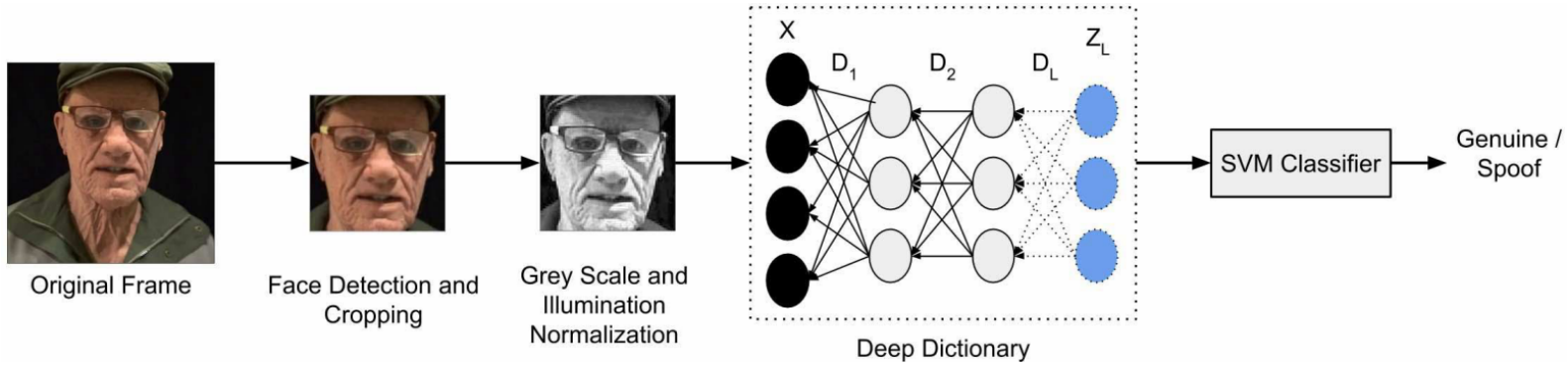
- Zero-shot Learning approach
  - Investigate the Zero-Shot Face Anti-spoofing problem in a wide range of 13 types of spoof attacks including 3D masks.
  - A novel Deep Tree Network is proposed to partition the spoof samples into semantic sub-groups



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

Other recent works

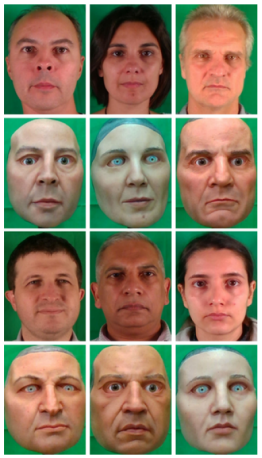
- Deep Dictionary Learning approach
  - Detecting Silicone Mask-Based Presentation Attack.
  - Multilevel deep dictionary learning-based presentation attack detection algorithm

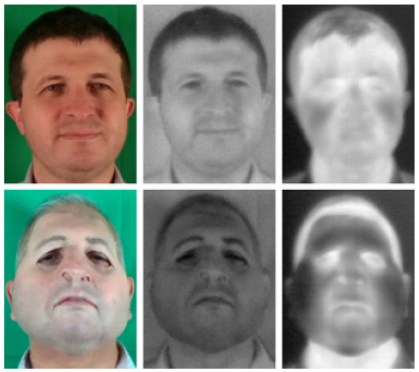


Manjani I, Tariyal S, Vatsa M, et al. Detecting silicone mask-based presentation attack via deep dictionary learning, TIFS 2017

Other recent works

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

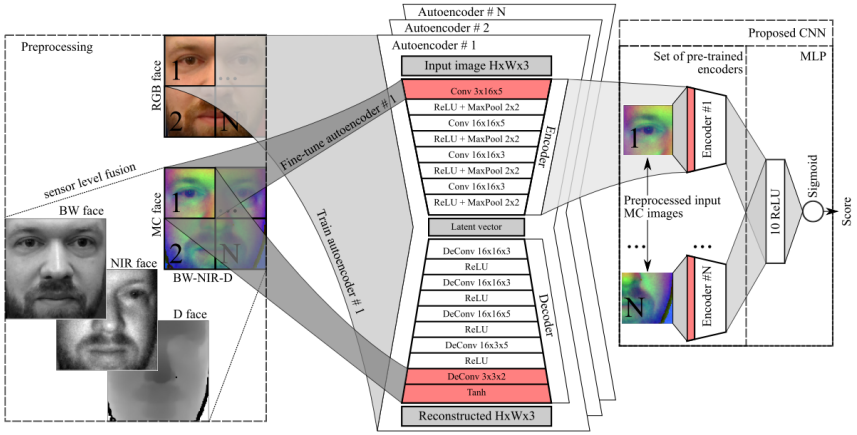


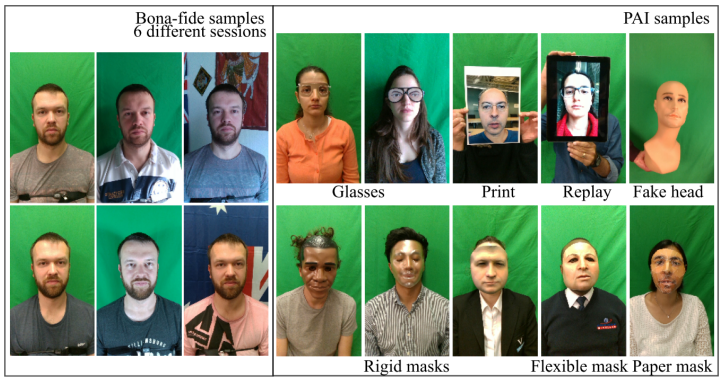


Bhattacharjee S, Mohammadi A, Marcel S. Spoofing deep face recognition with custom silicone masks, BTAS 2018

Other recent works

- 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

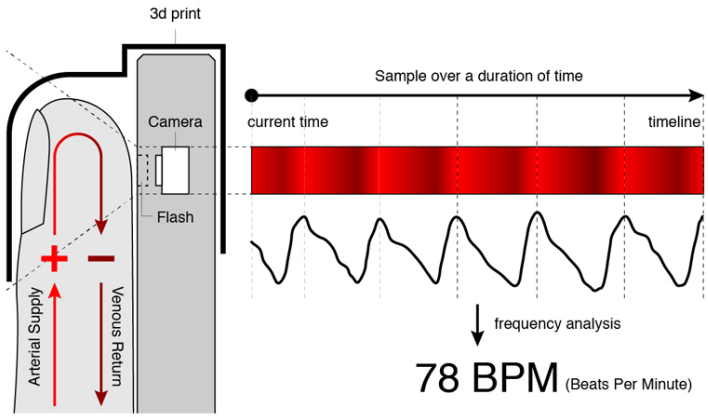
- PhotoPlethysmoGraphy based Approach
- Deep Dynamic Feature Approach
- Domain Generalization Approach

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

- Reference:

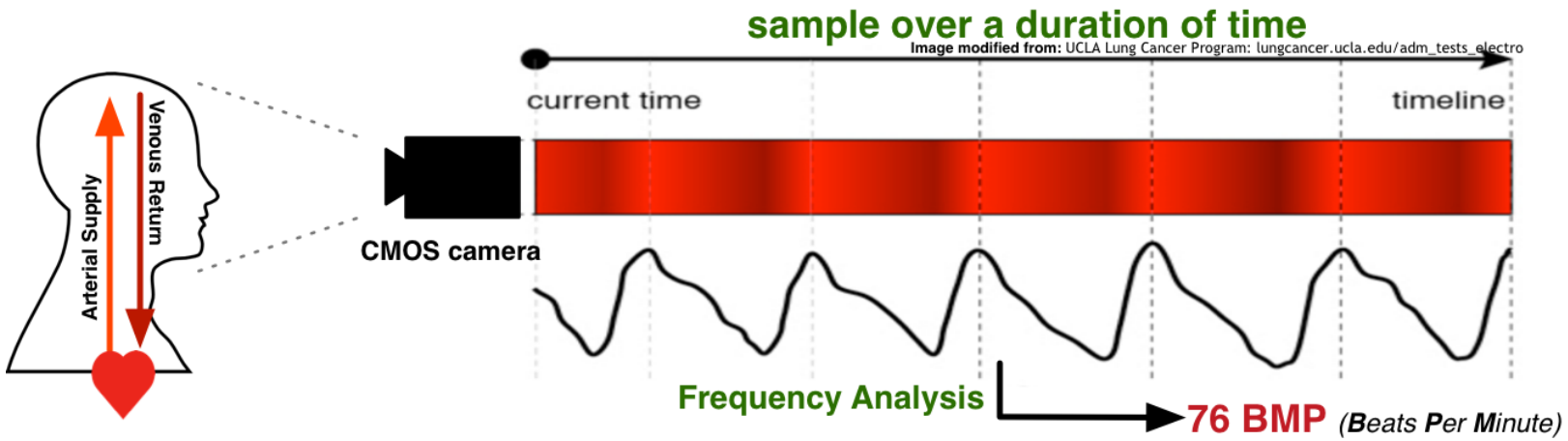
1. S Q Liu, X Lan, P C Yuen, "Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection", *Proceedings of the European Conference on Computer Vision (ECCV)*, pp. 558-573, Sept. 2018.
2. S Q Liu, P C Yuen, S Zhang and G Zhao, "3D Mask Face Anti-spoofing with Remote Photoplethysmography" *European Conference on Computer Vision (ECCV)*, Oct 2016.
3. 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)

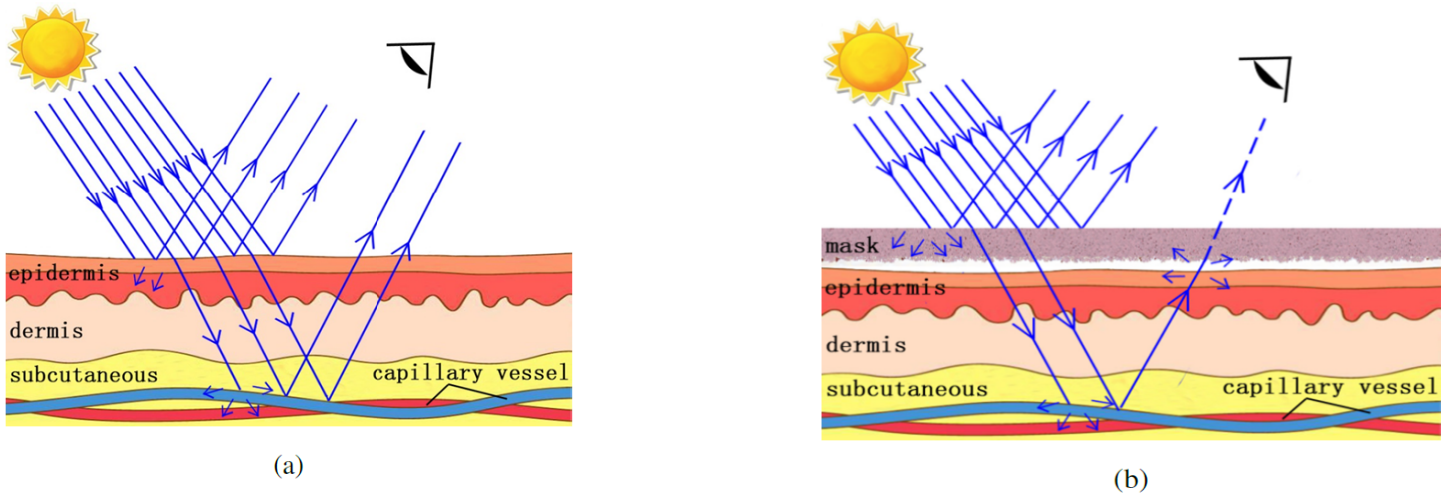


Pic. from UCLA Lung Cancer Program http://lungcancer.ucla.edu/adm_tests_electro.html

remote PhotoPlethysmoGraphy (rPPG)



Principle of rPPG Based Face Anti-Spoofing



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

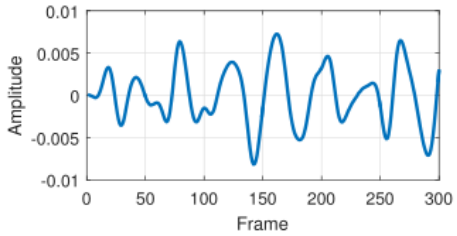
(b) rPPG signals will be **too weak** to be detected from a masked face.

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

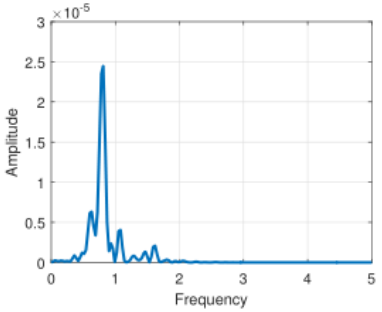
Principle of rPPG Based Face Anti-Spoofing

genuine face

(a)



(b)

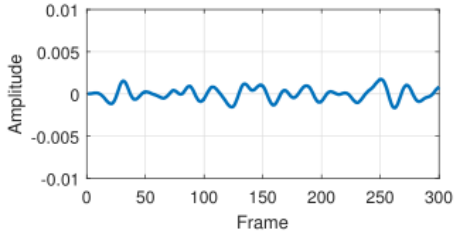


(c)

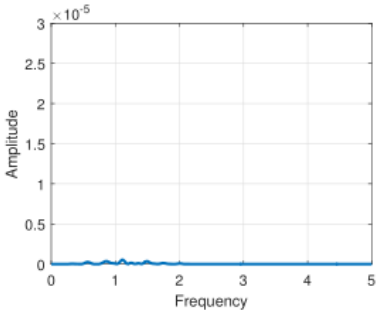
masked face

(d)

(a)

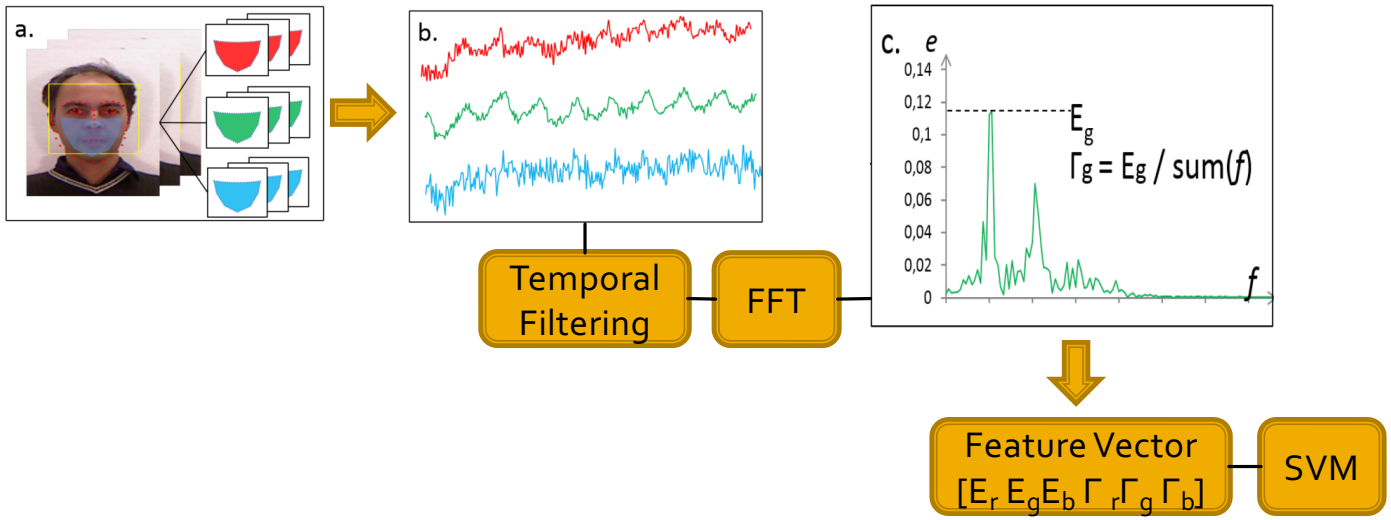


(e)



(f)

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

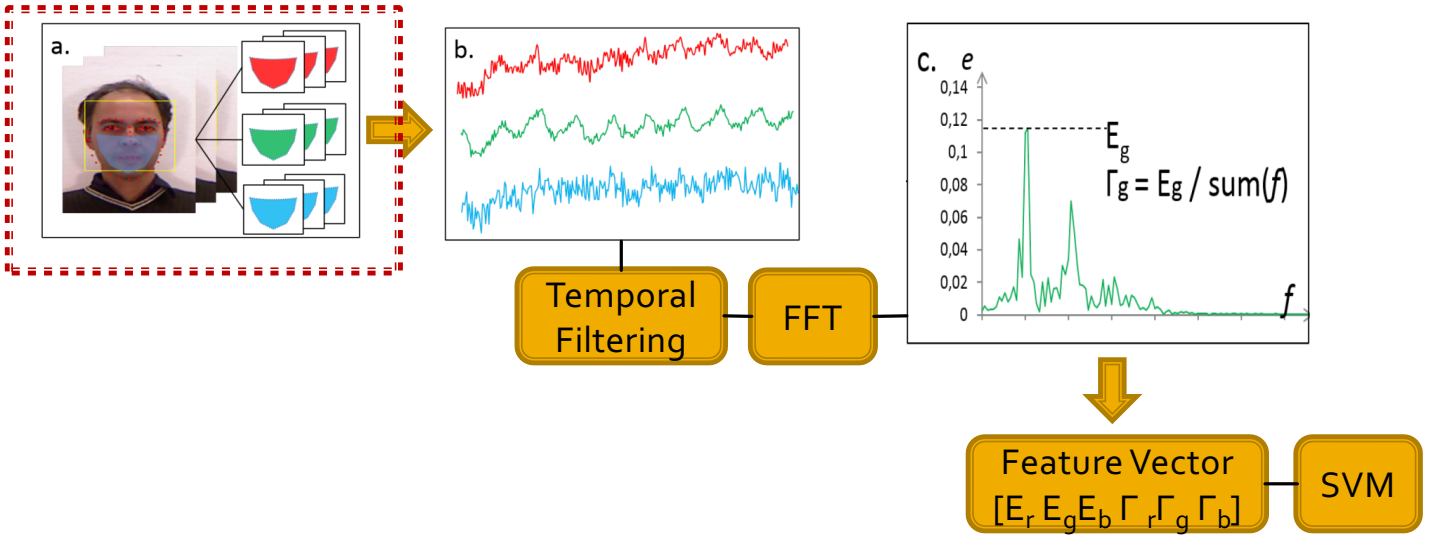


X Li, J Komulainen, G Zhao, P C Yuen and M Pietikainen,

"Generalized face anti-spoofing by detecting pulse from face videos"

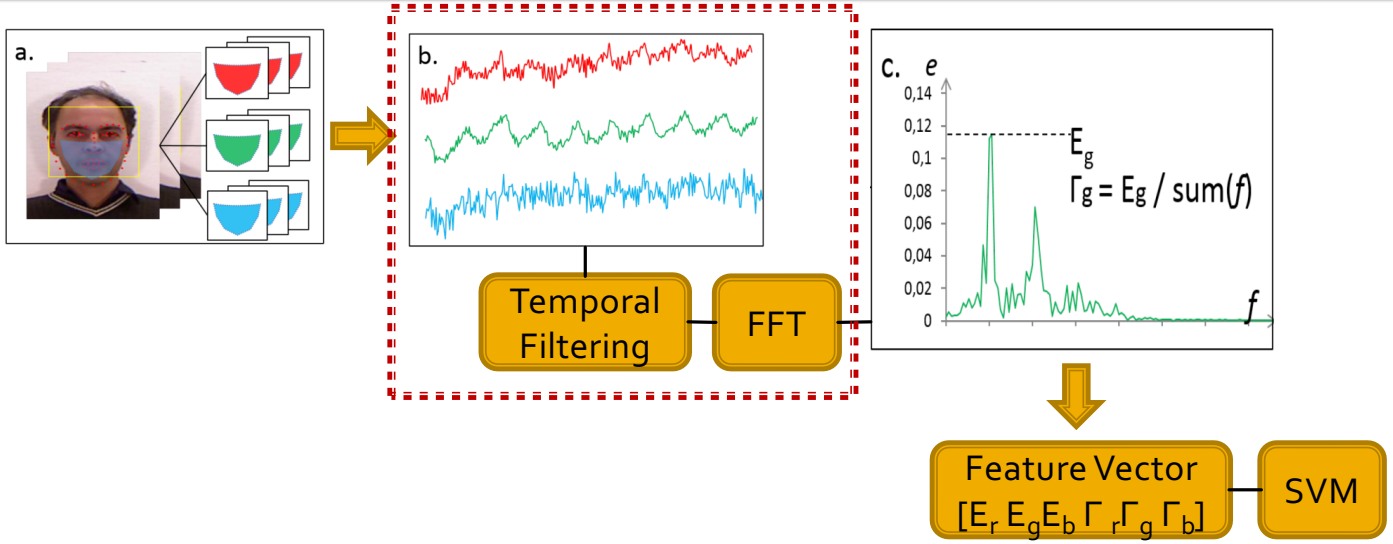
ICPR 2016

Global rPPG-based Face Anti-Spoofing



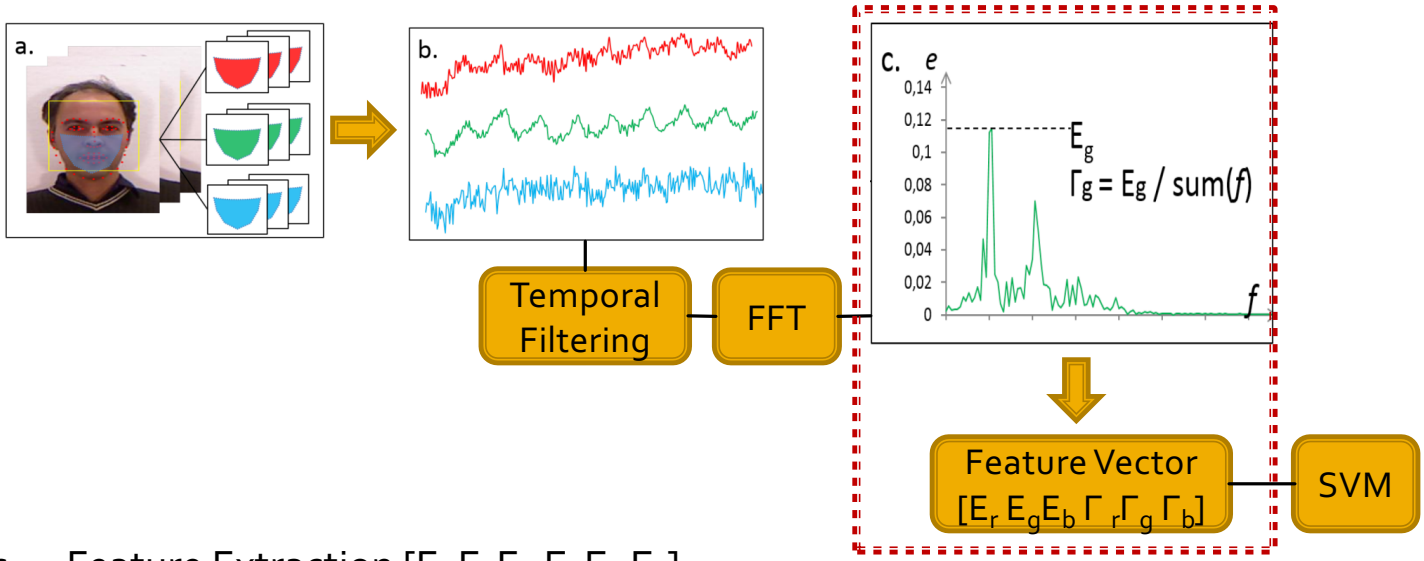
a. Face Detection and ROI tracking
   - Use Viola-Jones face detector on the first frame
   - Find 66 facial landmarks [CVPR'13 Asthana et.al] within the face bounding box. Use 9 of them to define the ROI
   - ROI is tracked through all frames using KLT

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-> 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 3DMAD
  - LOOCV protocol [Erdogmus *et.al* TIFS'14]

	3DMAD-dev	3DMAD-test	
Method	EER(%)	HTER(%)	EER(%)
Pulse (ours)	**2.31**	**7.94**	**4.17**
LBP-blk	0	0	0
LBP-blk-color	0	0	0
LBP-ms	0	0	0
LBP-ms-color	0	0	0

Note:

LBP-blk: $LBP_{8,1}$ extracted from 33 blocks of a gray-scale face

LBP-blk-color: LBP-blk extracted separately from each RGB color channel

LBP-ms: multi-scale LBP extracted from a whole gray-scale face image combining $LBP_{8,1}$, $LBP_{8,2}$, $LBP_{8,3}$, $LBP_{8,4}$, and $LBP_{16,2}$

LBP-ms-color: LBP-ms extracted separately from each RGB color channel

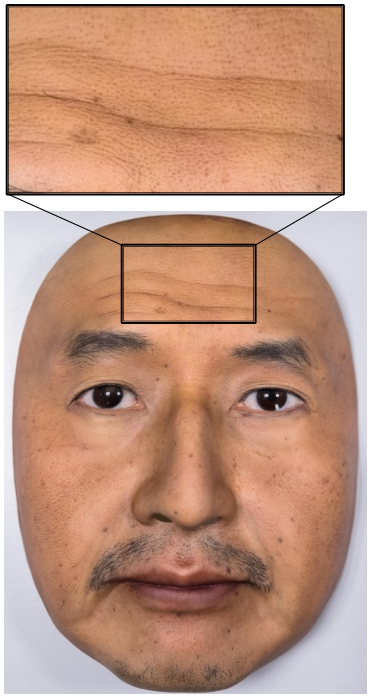
Experimental Results

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

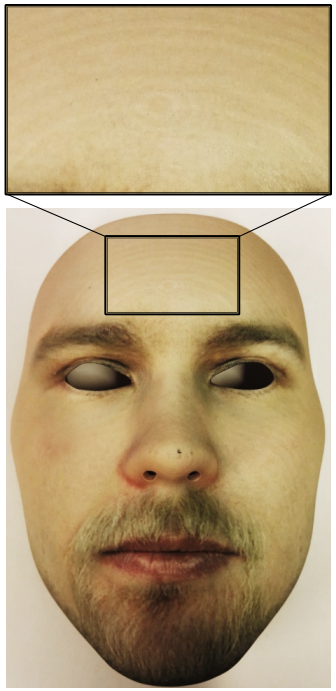
	REAL-F			
Method	HTER(%)	EER(%)	FPR (@FNR=0.1%)	FPR (@FNR=0.01%)
Pulse (ours)	**4.29**	**1.58**	**0.25**	**3.83**
LBP-blk	26.3	25.08	37.92	48.25
LBP-blk-color	25.92	20.42	31.5	48.67
LBP-ms	39.87	46.5	59.83	73.17
LBP-ms-color	47.38	46.08	86.5	95.08

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

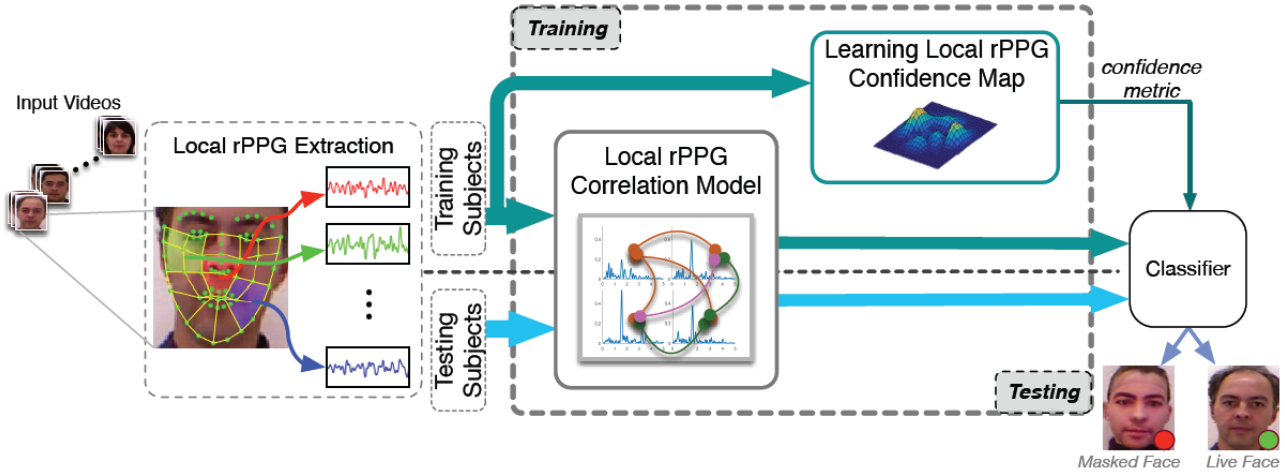
Limitations on Global rPPG method

- 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]

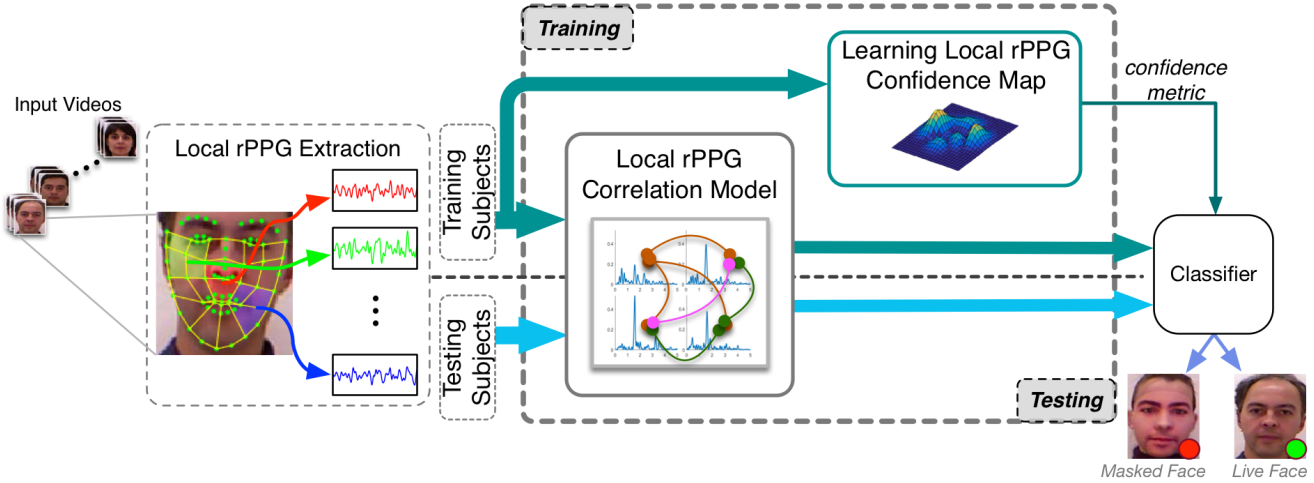


S Q Liu, P C Yuen, S P Zhang and G Y Zhao

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.

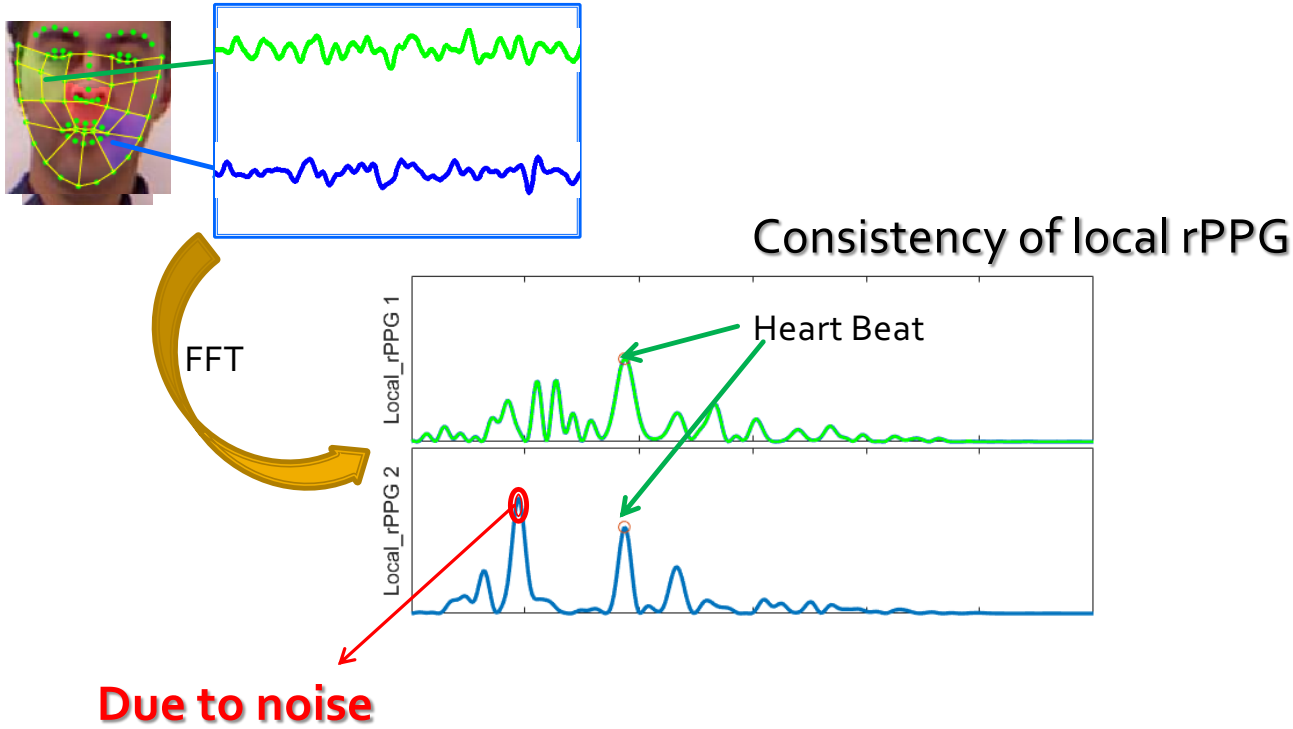
(b) Extract Local rPPG patterns through the proposed **local rPPG correlation model**.

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

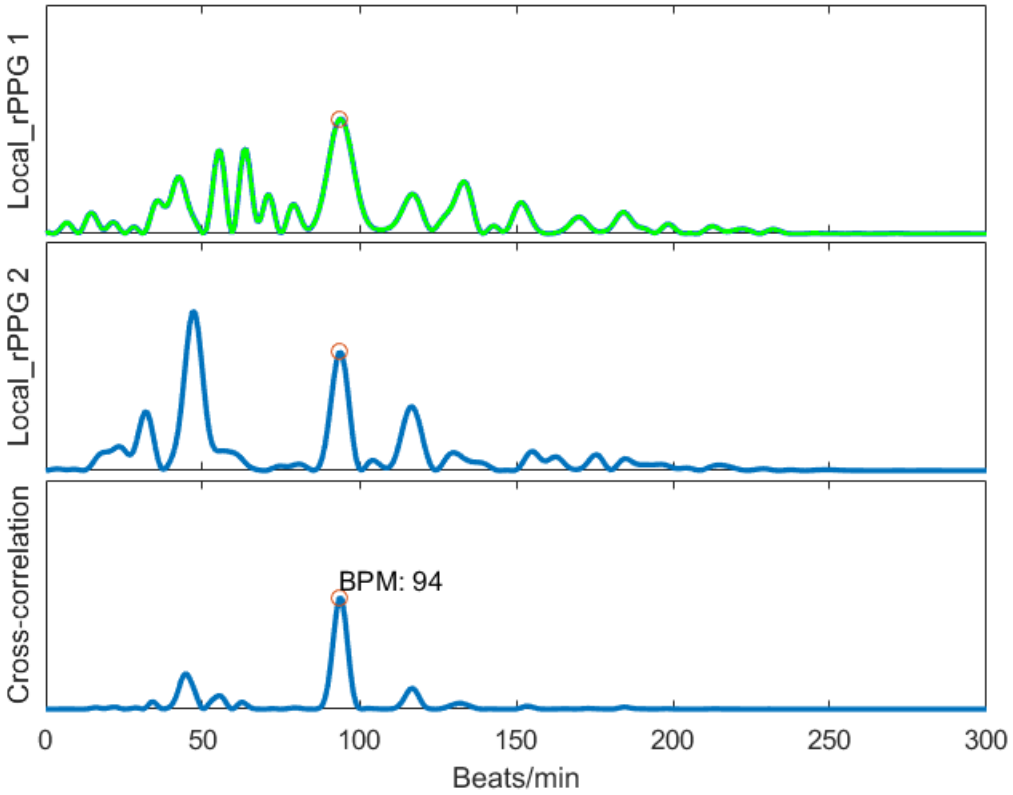
(d) Classifier: SVM

Contribution 1: Local rPPG Correlation Model

- Local rPPG on genuine face

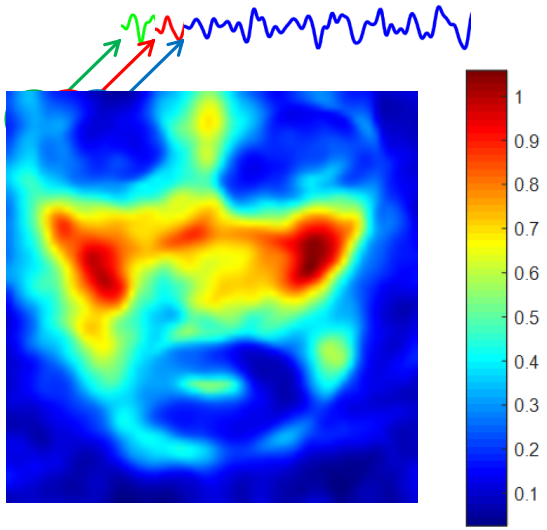


2. Local rPPG Correlation Model



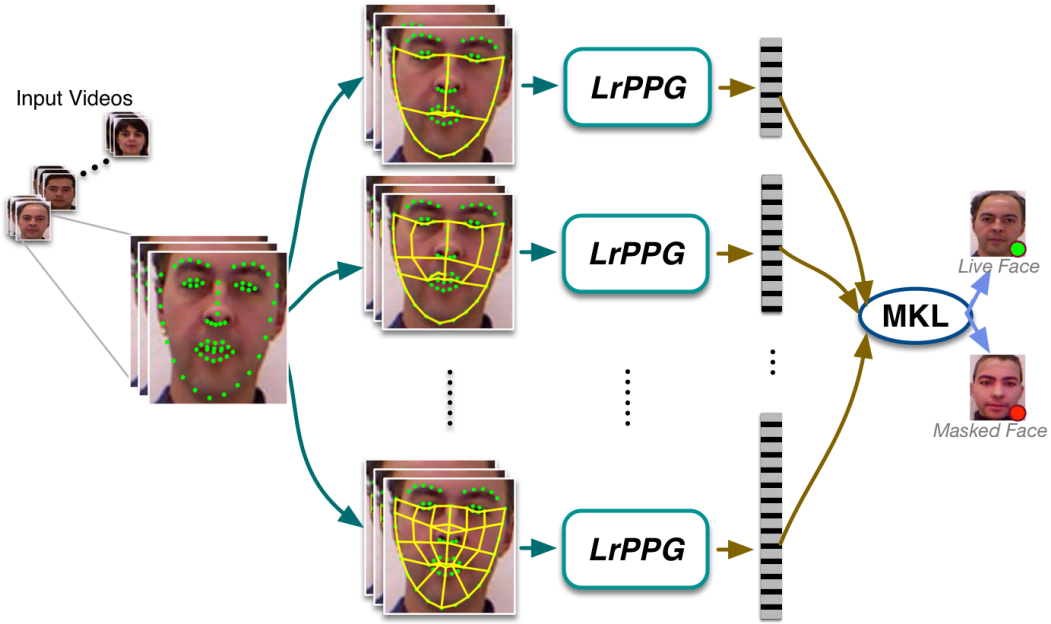
Contribution 2: Learning Local rPPG Confidence Map

Generic map of blood vessels on the face



The distribution of local rPPG signals should be considered

Multi-Scale Local rPPG Method



$$K_{\mathcal{MS}}(\boldsymbol{x}, \boldsymbol{x'}) = \sum_{m \in M} d_m K(\boldsymbol{x}_m, \boldsymbol{x'}_m)$$

$$s.t., d_m \geq 0, \sum_{m \in M} d_m = 1$$

M : number of scales

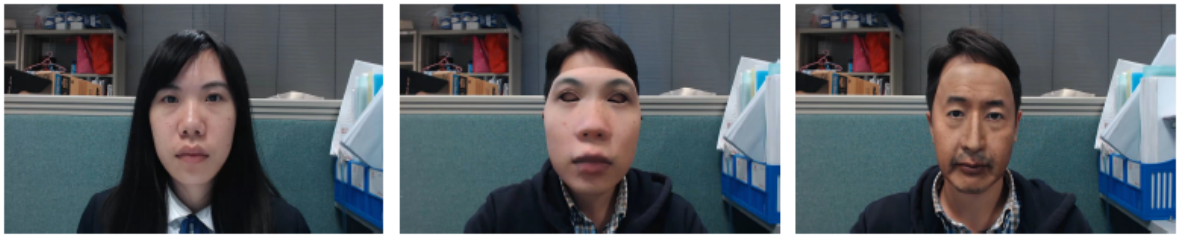
x_m: LrPPG feature extracted from of scale *m*

d_m: weight of scale *m*

Experimental Results

- **Datasets**
- 3DMAD [TIFS'14 Erdogmus et.al]
  - 255 videos recorded from 17 subjects
  - Masks made from ThatsMyFace.com

- HKBU MARs V2 Dataset:
  - 2 Mask types: **12** subjects: ThatsMyFace (6), REAL-F (**6**)
  - Captured by WebCam Logitech C920 (1280*720 RGB)



More details can be found: http://rds.comp.hkbu.edu.hk/mars/

Experimental Results

- Intra-Database Experiment (***LOOCV***)
  - 3DMAD, HKBU MARs V2, and Combined Dataset (3DMAD+HKBU MARs V2)
- Cross-Database Experiment
  - Training on 3DMAD, Test on HKBU MARs V2 dataset
  - Training on HKBU MARs V2 , Test on 3DMAD dataset
- Cross-Mask Experiment
  - Training and test using different mask types

Experimental Results

- Intra-database experiments (***LOOCV***)

Combined

	HTER_dev	HTER_test	EER	AUC	FFR@ FLR=0.1	FFR@ FLR=0.01
MS-LBP[2]	15.7 ± 4.2	7.93 ± 15.1	16.6	91.0	25.4	64.2
CTA [1]	18.4 ± 5.8	9.91 ± 14.1	18.9	87.7	42.9	95.7
CNN [6]	13.5 ± 5.9	6.97 ± 12.8	14.5	93.5	21.2	71.5
GrPPG	9.33 ± 2.5	5.22 ± 10.6	10.0	94.0	9.99	27.0
LrPPG [5]	8.69 ± 1.5	4.57 ± 9.8	9.21	95.7	8.79	29.4
MS-LrPPG	**7.30 ± 1.2**	**3.70 ± 9.5**	**7.90**	**96.3**	**6.67**	**25.8**

HKBU MARs V2

	HTER_dev	HTER_test	EER	AUC	FFR@ FLR=0.1	FFR@ FLR=0.01
MS-LBP[2]	20.5 ± 8.9	12.7 ± 17.2	22.5	85.8	48.6	95.1
CTA [1]	22.4 ± 10.4	11.7 ± 13.7	23.0	82.3	53.7	89.2
CNN [6]	15.0 ± 10.2	8.73 ± 15.4	16.4	90.9	30.4	79.5
GrPPG	**5.98 ± 2.9**	**3.85 ± 6.6**	**5.70**	97.9	**3.41**	37.3
LrPPG [5]	8.78 ± 2.3	5.06 ± 7.6	9.35	96.8	8.95	32.8
MS-LrPPG	6.84 ± 2.5	3.90 ± 6.7	7.31	**98.1**	5.64	**30.3**

1. Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face spoofing detection using colour texture analysis", *TIFS*, 2016

2. N. Erdogmus and S. Marcel, "Spoofing face recognition with 3d masks", TIFS, 2014

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

6. J. Yang, Z. Lei, and S. Z. Li, "Learn convolutional neural network for face anti-spoofing", arXiv, 2014.

Experimental Results

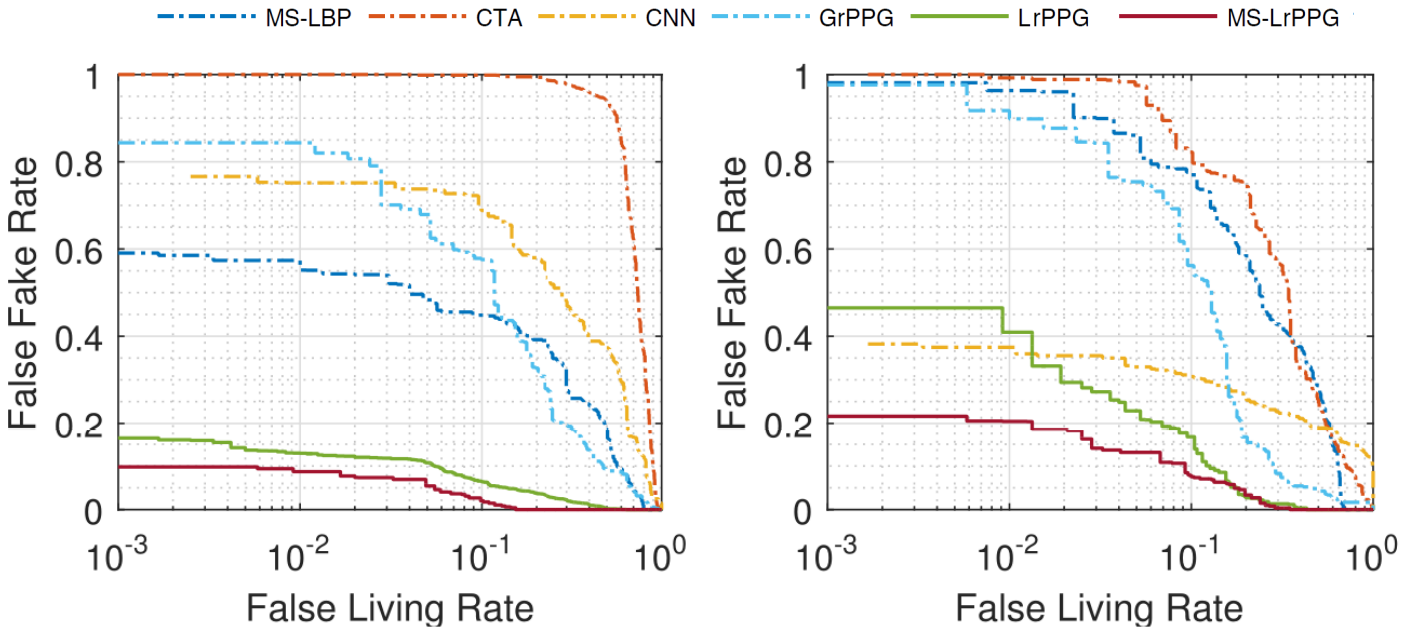
- Cross-database experiments

	3DMAD to MARsV2					MARsV2 to 3DMAD				
	HTER(%)	EER(%)	AUC(%)	FFR@ FLR=0.1	FFR@ FLR=0.01	HTER(%)	EER(%)	AUC(%)	FFR@ FLR=0.1	FFR@ FLR=0.01
MS-LBP[2]	19.0 ± 1.8	39.6	61.4	90.4	99.6	17.5 ± 6.8	35.7	70.8	73.9	94.3
CTA [1]	21.5 ± 5.5	47.3	53.7	93.2	99.4	18.0 ± 4.7	46.0	56.1	85.8	99.1
CNN [6]	24.3 ± 3.9	49.5	50.6	90.3	98.6	19.9 ± 6.4	49.3	50.8	90.0	99.5
GrPPG	15.1 ± 7.6	36.8	66.9	71.2	95.3	20.1 ± 13.8	42.3	59.7	99.4	99.7
LrPPG [5]	5.55 ± 0.9	10.9	95.6	12.4	61.7	7.36 ± 1.3	15.1	91.6	19.3	51.3
MS-LrPPG	**4.79 ± 0.8**	**9.08**	**97.6**	**7.42**	**33.3**	**4.75 ± 0.5**	**9.71**	**95.1**	**9.71**	**37.3**

• Our proposed method is robust encountering the cross-database scenario

• The appearance based method exposes the aforementioned drawbacks in the cross-database scenario

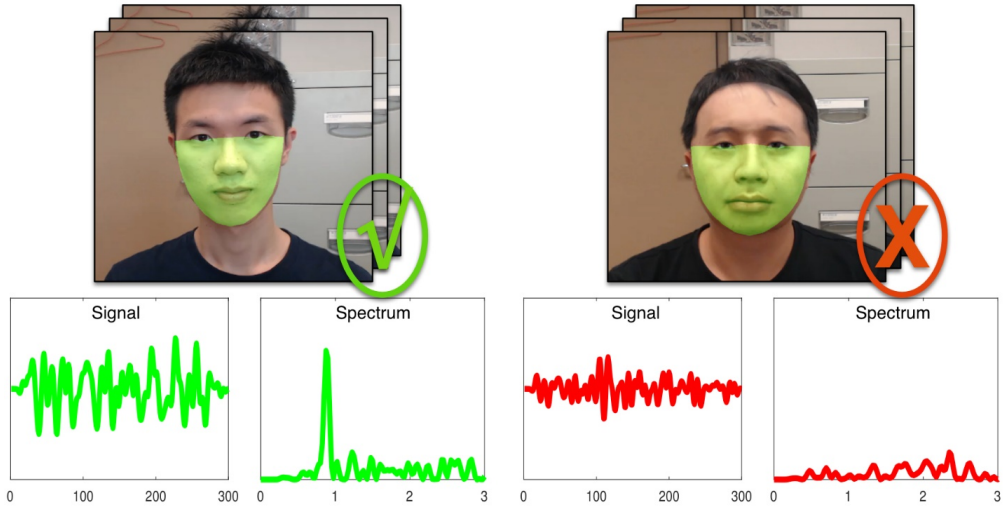
Experimental Results: Cross-mask



(a) TMF to RF (MARsV2)

(b) RF to TMF (MARsV2)

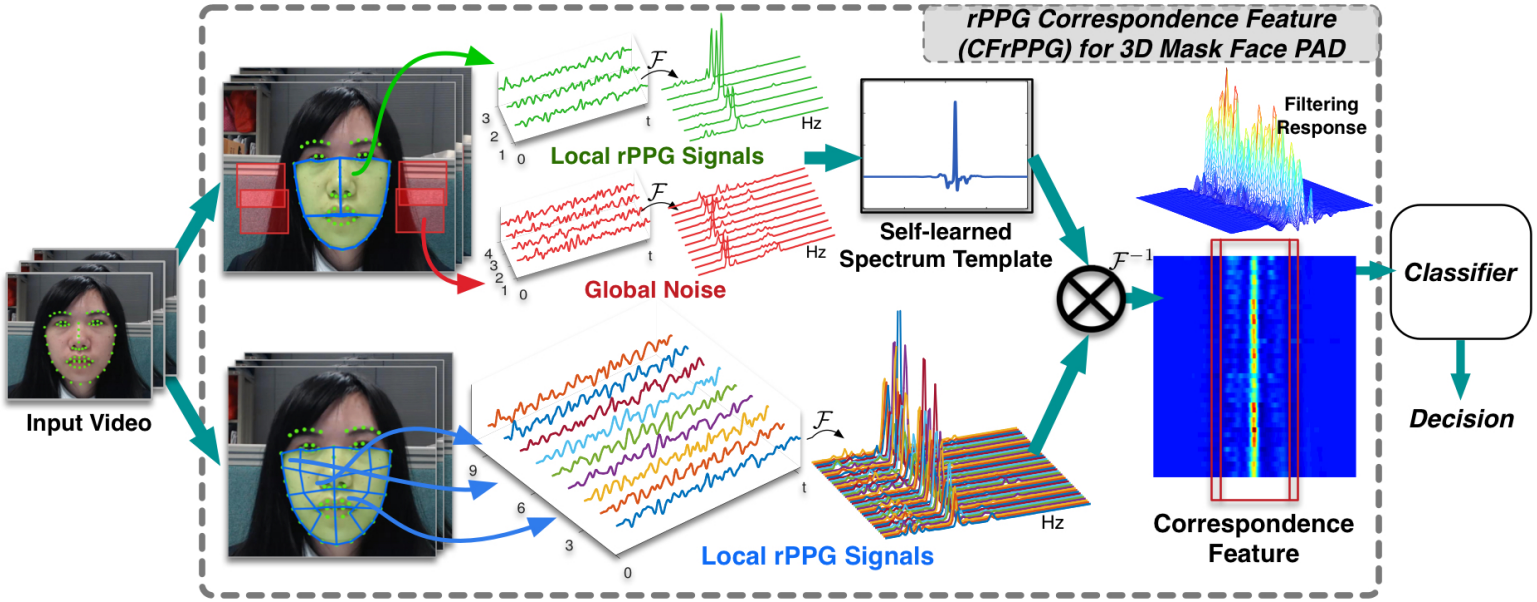
Limitation on Local rPPG Approach



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

Improved Method: rPPG Correspondence Feature

[ECCV 2018]

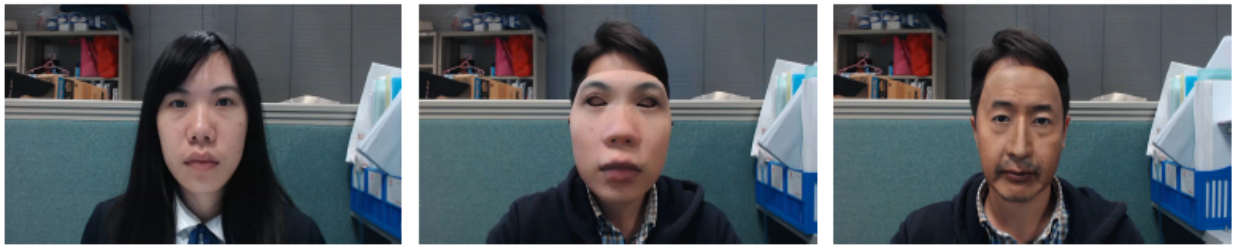


S Q Liu, X Y Lan and P C Yuen, "Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection", *ECCV* 2018

Experimental Results

- **Dataset**
- 3DMAD [TIFS'14 Erdogmus et.al]
  - 255 videos recorded from 17 subjects
  - Masks made from ThatsMyFace.com

- HKBU MARs V2 Dataset:
  - 2 Mask type: **12** subjects: ThatsMyFace (6), REAL-F (**6**)
  - Captured by WebCam Logitech C920 (1280*720 RGB)



Experimental Results

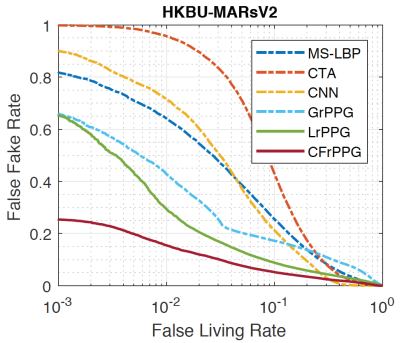
- Intra-database experiments (***LOOCV***)

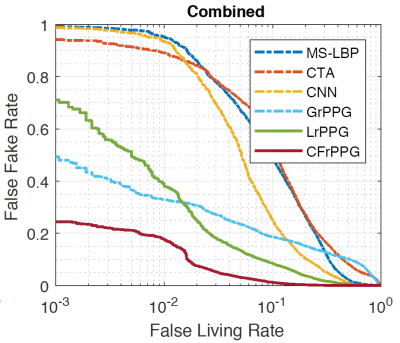
HKBU MARs V2

	HTER_dev(%)	HTER_test(%)	EER(%)	AUC	FFR@ FLR=0.1	FFR@ FLR=0.01
MS-LBP [3]	20.5 ± 8.9	24.0 ± 25.6	22.5	85.8	48.6	95.1
CTA [1]	22.4 ± 10.4	23.4 ± 20.5	23.0	82.3	53.7	89.2
CNN	13.7 ± 10.8	14.8 ± 22.2	15.2	91.4	25.1	93.5
GrPPG [4]	15.4 ± 6.7	16.1 ± 20.5	16.4	89.4	18.6	32.9
LrPPG [5]	8.43 ± 2.9	8.67 ± 8.8	9.07	97.0	8.51	38.9
CFrPPG	**3.24 ± 1.9**	**4.42 ± 5.1**	**4.04**	**99.3**	**1.24**	**17.8**

Combined

	HTER_dev(%)	HTER_test(%)	EER(%)	AUC	FFR@ FLR=0.1	FFR@ FLR=0.01
MS-LBP [3]	15.7 ± 4.2	16.2 ± 22.6	16.6	91.0	25.4	64.2
CTA [1]	18.4 ± 5.8	19.5 ± 21.5	18.9	87.7	42.9	95.7
CNN	13.5 ± 5.9	14.6 ± 20.6	14.5	93.5	21.2	71.5
GrPPG [4]	15.3 ± 2.9	15.5 ± 18.5	15.2	91.1	17.2	42.8
LrPPG [5]	8.69 ± 1.5	9.16 ± 11.9	9.21	95.7	8.79	29.4
CFrPPG						



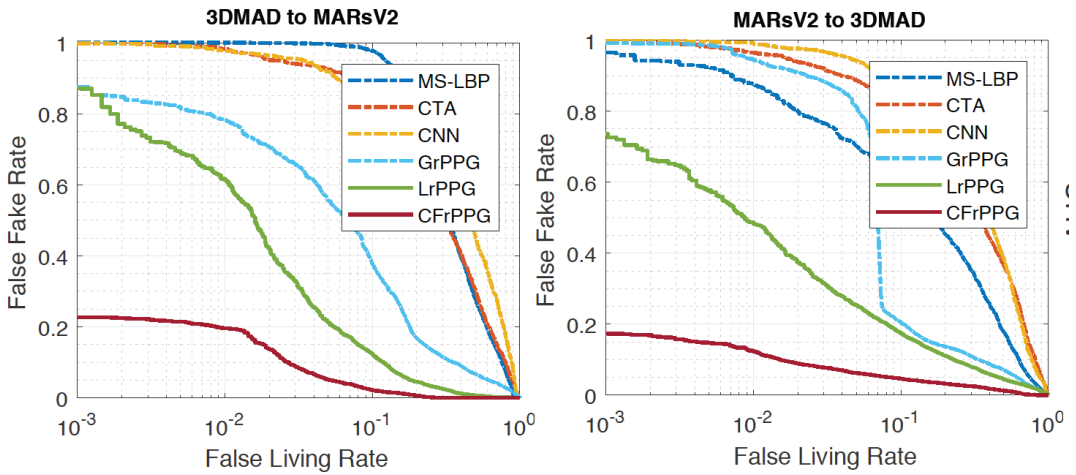


1. Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face spoofing detection using colour texture analysis", *TIFS*, 2016
3. N. Erdogmus and S. Marcel, "Spoofing face recognition with 3d masks", TIFS, 2014
4. X. Li, J. Komulainen, G. Zhao, P. C. Yuen, and M. Pietikainen, "Generalized face anti-spoofing by detecting pulse from face videos", ICPR, 2016.
5. S. Liu, P C. Yuen, S. Zhang, and G. Zhao, "3D Mask Face Anti-spoofing with Remote Photoplethysmography" , ECCV, 2016.

Experimental Results

- Cross-database experiments

	3DMAD to MARsV2					MARsV2 to 3DMAD				
	HTER(%)	EER(%)	AUC(%)	FFR@ FLR=0.1	FFR@ FLR=0.01	HTER(%)	EER(%)	AUC(%)	FFR@ FLR=0.1	FFR@ FLR=0.01
MS-LBP [3]	53.0 ± 3.6	39.8	60.4	97.8	100.0	32.8 ± 11.5	32.5	75.3	58.5	87.8
CTA [1]	40.1 ± 7.8	40.2	62.1	87.1	98.3	47.7 ± 5.4	42.5	60.5	81.2	96.5
CNN	50.0 ± 0.0	47.8	54.6	82.6	97.9	50.0 ± 0.0	44.3	58.6	87.3	99.3
GrPPG [4]	24.3 ± 7.1	18.5	86.7	37.8	78.5	15.7 ± 6.8	15.4	87.2	20.6	94.5
LrPPG [5]	16.8 ± 5.0	10.9	95.6	12.4	61.7	17.4 ± 4.4	14.0	92.3	17.4	48.7

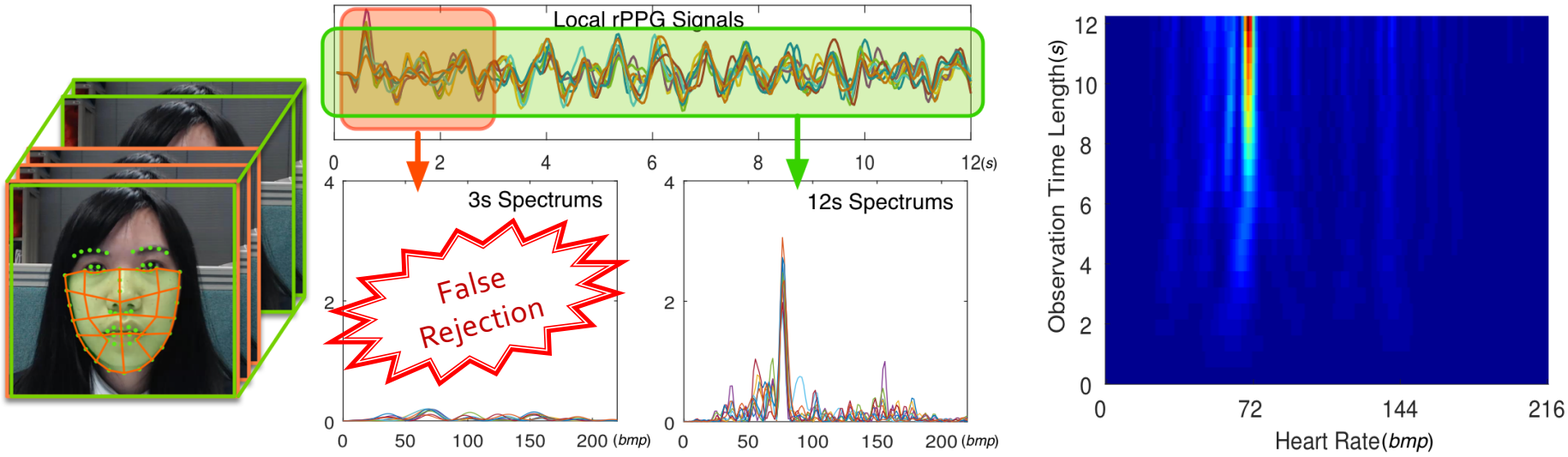


Temporal Similarity Analysis of rPPG (TSrPPG) for Fast 3D Mask Face PAD

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.

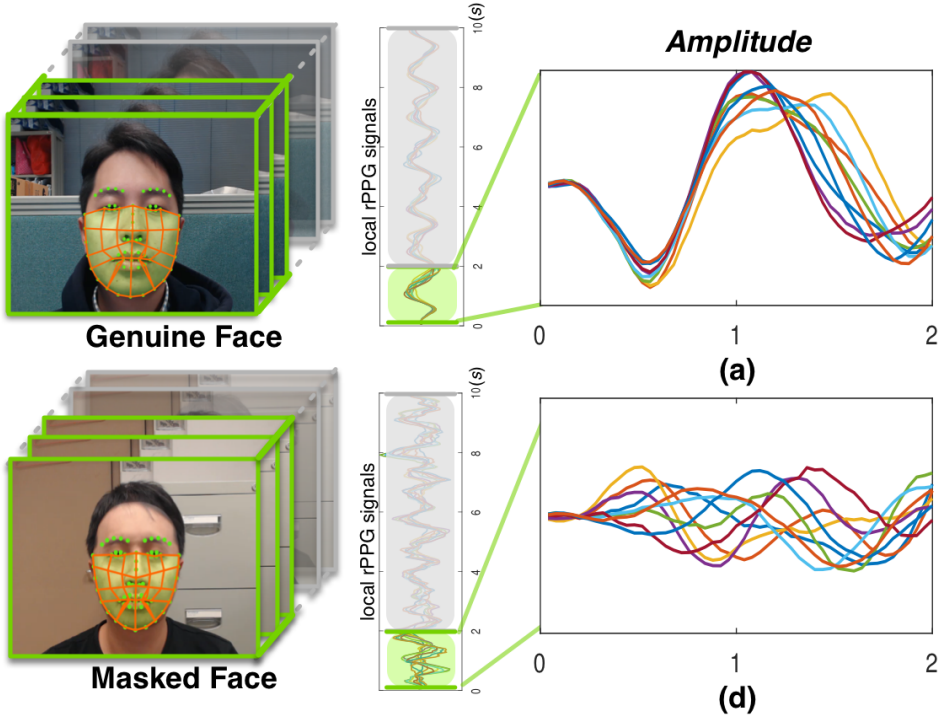
Limitations on existing rPPG Methods



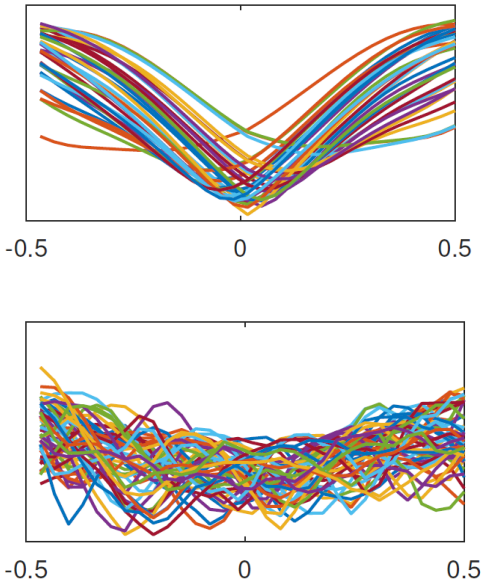
Existing rPPG-based 3D mask PAD methods are based on spectrum analysis

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

The proposed TSrPPG



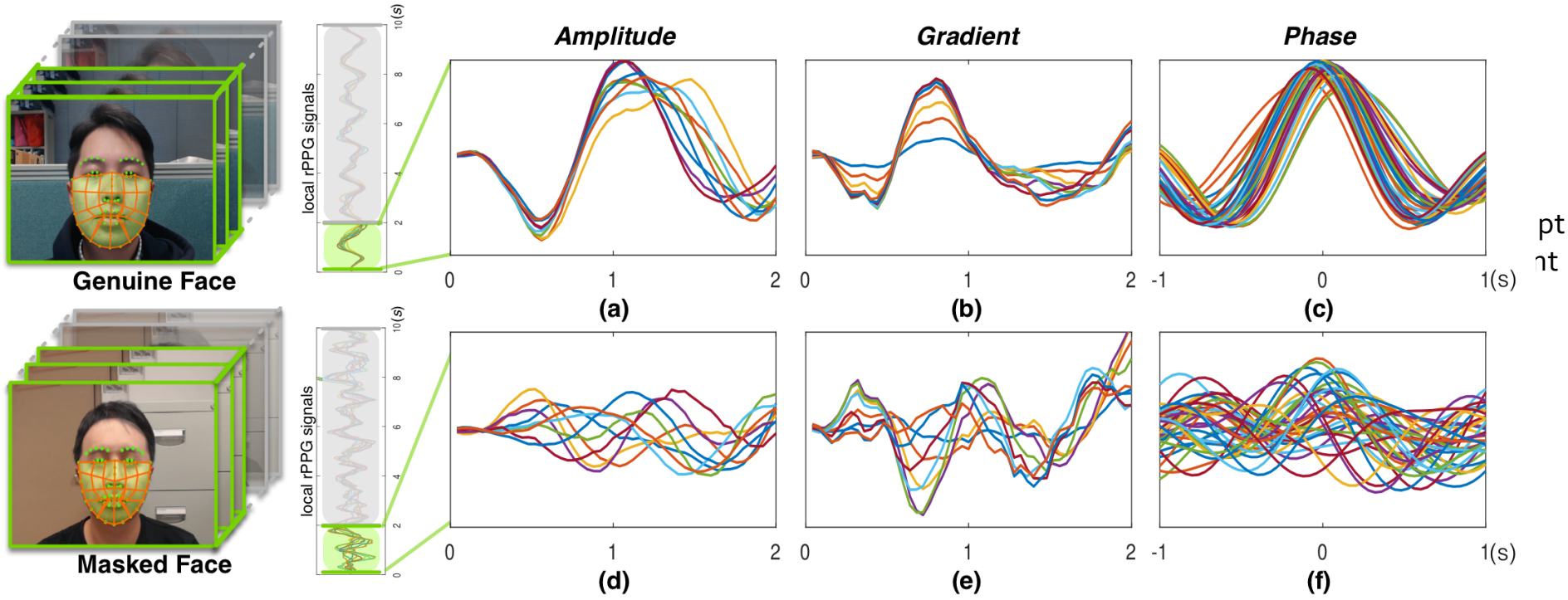
$$\boldsymbol{TSrPPG_{i,j}}[m] = \int_{-\infty}^{+\infty} \mathcal{D}(\boldsymbol{s}_i[t], \boldsymbol{s}_j[t+m])dt$$



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

The proposed TSrPPG

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



Final result is obtained through score-level-fusion

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

Deep Dynamic Feature Learning Approach

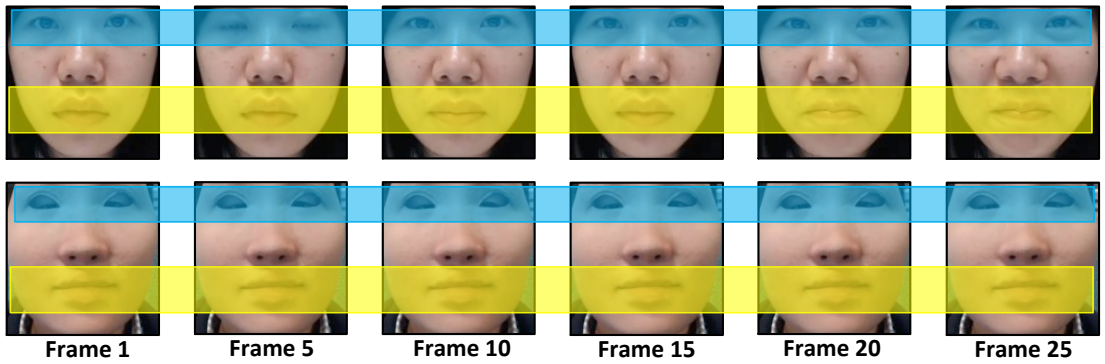
Reference:

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**

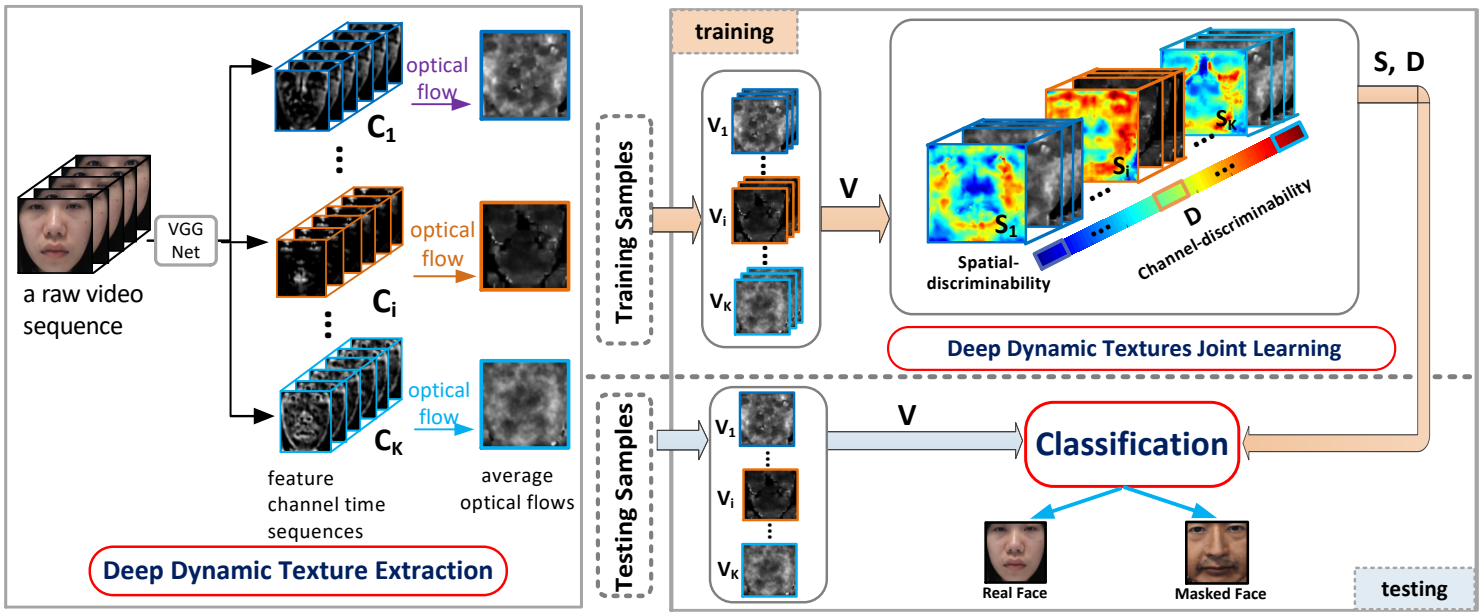


- Eye blinking
- Lip movements
- Some other facial components movements

} **Captured by dynamic textures**

Joint Discriminative Learning of Deep Dynamic Textures

[IJCB 2017, TIFS 2019]



Experimental Results

Dataset

- 3DMAD [TIFS'14 Erdogmus et.al]:
  - 255 videos recorded from 17 subjects
  - Masks made from ThatsMyFace.com

- Supplementary Dataset (SUP) [ECCV'16 Liu et.al]:
  - 120 videos recorded from 8 subjects
  - 2 Mask type: 8 subjects: ThatsMyFace (6), REAL-F (2)

- Silicone Mask Attack Dataset (SMAD) [TIFS'17 Manjani et.al]:
  - 130 videos recorded videos
    (65 genuine samples, and 65 masked samples.)
  - Silicone masks

Experimental Results

Protocols

- Intra-database Experiment (LOOCV) [TIFS'14 Erdogmus et.al]
  - 3DMAD Dataset
  - Supplementary (SUP) Dataset
  - SMAD Dataset

- Cross-database Experiment: [ECCV'16 Liu et.al] [TIFS'17 Manjani et.al]
  - Train on 3DMAD, Test on SUP dataset
  - Train on SUP, Test on 3DMAD dataset
  - Train on 3D masks datasets (3DMAD&SMAD)
    Test on 2D presentation datasets (CASIA&Replay Attack)
  - Train on 3D masks datasets (3DMAD&SMAD)
    Test on 2D presentation datasets (CASIA&Replay Attack)

- Evaluation metrics:
  - False Fake Rate (FFR)
  - False Liveness Rate (FLR)
  - Area Under Curve (AUC)
  - Equal Error Rates (EER)
  - Half Total Error Rates (HTER)

Experimental Results

Comparison features

- Appearance-based features:
  - Multi-scale LBP (**MS_LBP** for short) [1]
  - Color Texture (**CT** for short) [2]
  - Deep features from last fully connected layer of CNN (**fc_CNN** for short) [3]
  - Image distortion analysis features (**IDA** for short) [4]

- Motion-based features:
  - LBPTOP features (**LBPTOP** for short) [5]
  - Multifeature videolet aggregation (**Videolet** for short)[6]
  - Optical flow field (**OFF** for short) [7]
  - Optical flows on Gabor features [8](**OF_Gabor** for short)
  - Deep convolutional dynamic texture with adaptive channel-discriminability (Our conference version)[9] (**DTAC** for short)

- Other cues-based features:
  - rPPG features (**rPPG** for short) [10]

[1] "Spoofing face recognition with 3D masks", TIFS, 2014
[2] "Face spoofing detection using color texture analysis", TIFS, 2016
[3] "Learn convolutional neural network for face anti-spoofing", arXiv, 2014
[4] "Face spoof detection with image distortion analysis", TIFS, 2015
[5] "Face liveness detection using dynamic texture", EURASIP Journal on Image and Video Processing, 2014
[6] "Face anti-spoofing with multifeature videolet aggregation", ICPR, 2016
[7] "A liveness detection method for face recognition based on optical flow field", IASP, 2009
[8] "Nonlinear operator for oriented texture", TIP, 1999
[9] "Deep convolutional dynamic texture learning with adaptive channel-discriminability for 3D mask face anti-spoofing", IJCB 2017
[10] "3D mask face anti-spoofing with remote photoplethysmography", ECCV, 2016

Experimental Results

- **Intra-dataset Test**

TABLE I: Comparison of intra-dataset performance on 3DMAD and SUP datasets.

Method	3DMAD dataset						Supplementary dataset					
	EER(%)	AUC(%)	HTER(%)	FFR @FLR=0.001	FFR @FLR=0.01	FFR @FLR=0.1	EER(%)	AUC(%)	HTER(%)	FFR @FLR=0.001	FFR @FLR=0.01	FFR @FLR=0.1
MS_LBP[17]	9.14	96.71	12.29	42.11	21.08	9.01	21.17	80.29	22.81	94.60	85.66	46.00
CT[6]	2.92	99.74	5.24	11.37	4.45	0.24	27.00	81.40	23.12	93.05	87.93	65.44
fc_CNN[41]	1.77	99.82	2.06	26.77	3.98	0.03	21.98	89.17	21.41	27.53	25.79	24.51
IDA[39]	16.57	90.25	13.88	99.83	94.09	42.45	25.67	79.27	25.38	94.61	89.16	69.15
LBPTOP[14]	3.46	99.60	5.41	21.52	9.64	0.30	16.50	92.71	19.50	63.52	51.00	19.95
Videolet[9]	27.19	78.69	13.38	98.30	95.09	61.72	26.81	81.31	15.13	93.64	86.75	60.73
OFF[3]	33.43	70.72	33.79	97.89	95.18	64.13	52.31	46.54	52.12	99.34	95.47	87.69
rPPG[28]	8.59	96.81	8.59	28.76	20.15	7.97	15.38	92.03	14.81	75.73	58.13	22.08
DTAC[33]	2.66	99.69	3.29	28.34	7.86	0.20	12.54	95.94	14.75	63.06	39.96	14.16
OF_Gabor	3.29	99.66	2.82	19.64	6.25	0.39	14.33	91.66	17.87	39.23	34.33	14.66
Ours	**0**	**100**	**1.76**	**0**	**0**	**0**	**7.33**	**96.68**	**13.44**	**15.50**	**14.00**	**6.50**

TABLE III: Comparison of intra-dataset performance on SMAD datasets.

Method	SMAD dataset				
	HTER(%)	EER(%)	FFR @FLR=0.001	FFR @FLR=0.01	FFR @FLR=0.1
MS_LBP[17]	30.9	27.13	86.72	81.27	62.61
CT[6]	30.86	40.42	94.03	92.87	81.92
fc_CNN[41]	16.93	15.96	80.42	76.75	21.36
LBPTOP[14]	14.41	14.89	57.66	50.08	29.24
IDA[39]	46.31	52.13	100	99.07	88.71
Videolet[9]	20.4*	–	–	–	–
DDGL[30]	13.1*	–	–	–	–
Ours	**11.7**	**14.89**	**55.37**	**40.17**	**15.39**

- Hand-crafted appearance-based methods can achieve good results in 3DMAD dataset which are comparable with our method, but the performance of these methods drop a lot in supplementary dataset

  -> Appearance-based features are not discriminative enough to capture subtle texture differences when facing masks with good appearance quality

- The intrinsic limitation of the hand-crafted feature leads to the same degraded performance of motion-based features and other cues-based features

  -> Motion-based features and other cues-based features are not descriptive enough for subtle motion differentiation

Experimental Results

- **Cross-dataset Test**

TABLE II: Comparison of cross-dataset performance on 3DMAD and SUP datasets.

Method	3DMAD to SUP dataset						SUP to 3DMAD dataset					
	EER(%)	AUC(%)	HTER(%)	FFR @FLR=0.001	FFR @FLR=0.01	FFR @FLR=0.1	EER(%)	AUC(%)	HTER(%)	FFR @FLR=0.001	FFR @FLR=0.01	FFR @FLR=0.1
MS_LBP[17]	41.00	62.35	42.94	96.95	93.62	77.87	26.12	81.67	26.09	99.29	97.29	66.82
CT[6]	37.16	67.59	35.00	97.96	94.75	77.25	32.65	73.59	31.78	99.64	96.47	73.76
fc_CNN[41]	42.63	60.89	41.78	100	99.50	92.37	45.25	54.69	44.57	100	100	95.64
IDA[39]	44.38	57.82	18.16	97.61	94.00	85.62	25.82	80.05	21.47	99.82	97.94	54.64
LBPTOP[14]	24.97	84.99	14.50	89.44	77.12	48.12	31.06	77.67	26.29	99.31	96.47	64.23
Videolet[9]	44.88	55.83	51.51	100	100	97.62	43.58	55.60	54.40	100	100	94.35
rPPG[28]	**12.25**	94.89	**11.93**	79.32	61.62	16.47	17.67	91.83	17.38	72.94	**54.31**	25.97
DTAC[33]	13.03	94.98	17.31	70.77	55.37	18.37	18.00	90.21	11.63	83.63	74.76	36.64
OF_Gabor	18.59	90.04	16.44	60.48	52.62	27.62	35.18	68.88	33.53	100	99.05	82.00
Ours	12.75	**95.64**	13.16	**37.35**	**26.87**	**13.12**	**7.60**	**97.44**	**6.85**	**70.46**	56.43	**1.05**

TABLE IV: Comparison of the the HTER(%) in cross-dataset experiments between 3D masks and 2D presentation attacks.

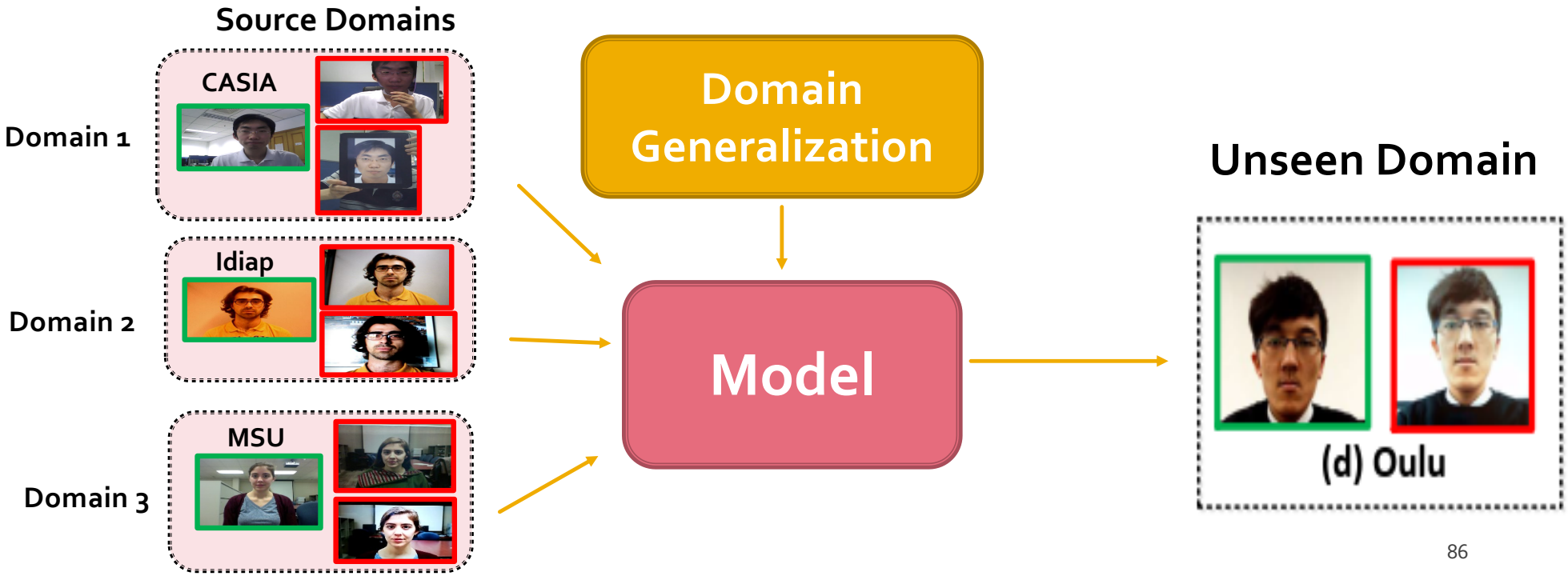
Train Dataset	Test Dataset	Ours	DDGL[30]	Videolet[9]
3DMAD	Repaly-Attack	**24.4**	40.9	49.4
	SMAD	**29.4**	29.9	44.8
	CASIA	**39.4**	42.8	48.1
SMAD	Repaly-Attack	**24.3**	42.6	50.1
	3DMAD	20.8	**14.1**	28.6
	CASIA	**40.5**	44.6	48.1
Replay-Attack	3DMAD	**16.4**	21.6	40.0
	SMAD	**31.7**	32.0	50.0
	CASIA	35.0	**27.4**	44.6
CASIA	3DMAD	**29.1**	30.2	46.4
	Repaly-Attack	**22.2**	22.8	35.4
	SMAD	**30.8**	31.2	48.0

- The proposed method **generalizes well** between different datasets.

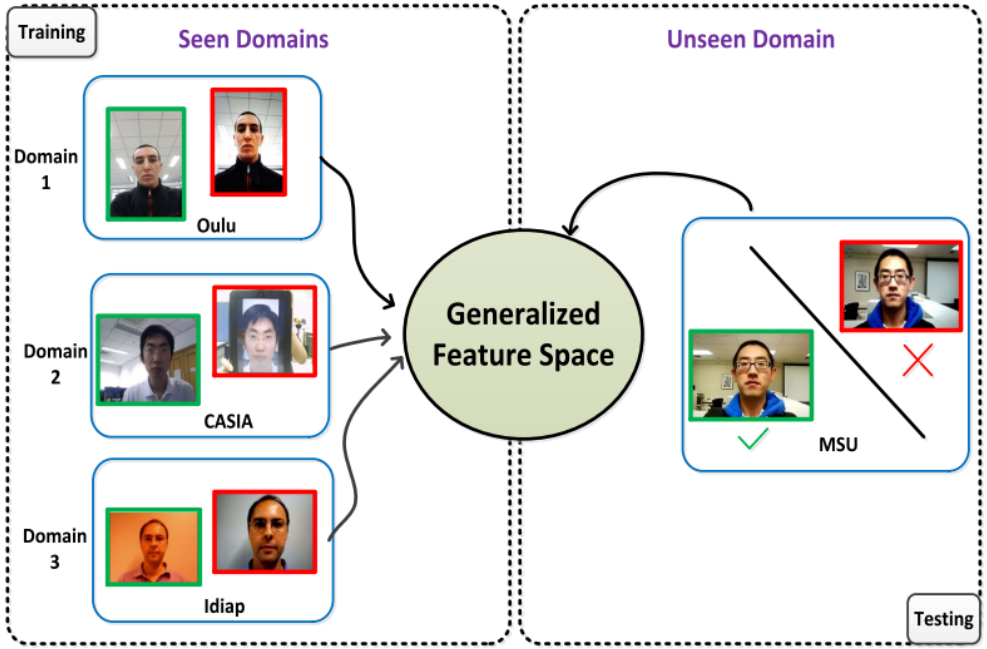
Can we develop a generalized detection method in which the attack type is not known?

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

- **Domain Generalization:**

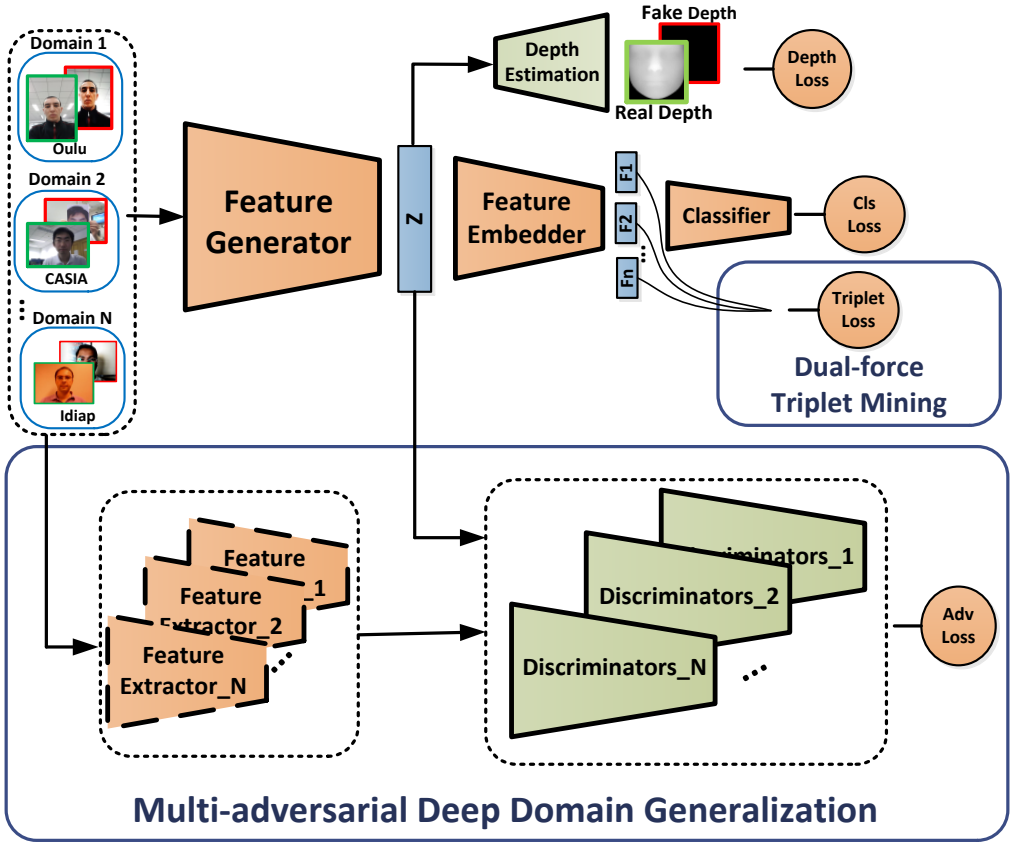


Multi-adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection [CVPR 2019]



- 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]



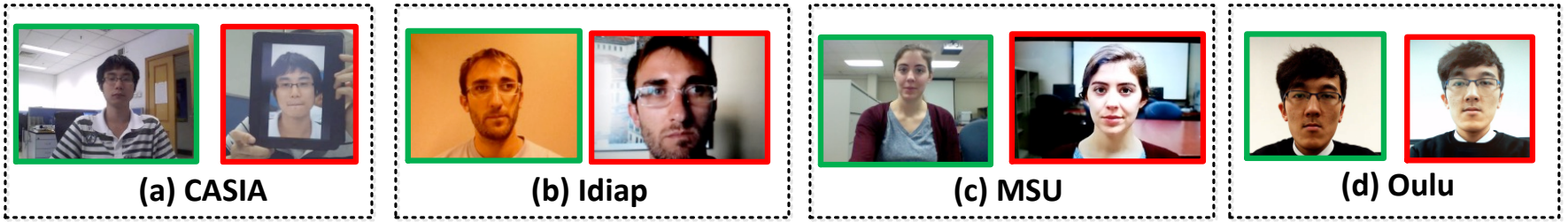
- A unified multi-adversarial discriminative deep domain generalization framework **(MADDG)**:

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

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

Experimental Results

- **Dataset**



[ICB'2012 Zhang et.al] [BIOSIG'2012 Chingovska et.al] [TIFS'2015 Wen et.al] [FG'2017 Zinelabinde et.al]

Table 1. Comparison of four experimental datasets.

Dataset	Extra light	Complex background	Attack type	Display devices
C	No	Yes	Printed photo Cut photo Replayed video	iPad
I	Yes	Yes	Printed photo Display photo Replayed video	iPhone 3GS iPad
M	No	Yes	Printed photo Replayed video	iPad Air iPhone 5S
O	Yes	No	Printed photo Display photo Replayed video	Dell 1905FP Macbook Retina

Experimental Results

- **Experimental Setting**
  - **One** dataset as **one domain** in our experiment.
  - **Three** datasets in four are randomly selected as source domains where we conduct the domain generalization, and the remaining **one** is the unseen domain for testing, which cannot be accessed in the training process.
  - Evaluation metrics:
    - **Half Total Error Rates (HTER)** (half of the summation of false acceptance rate and false rejection rate)
    - **Area Under Curve (AUC)**

Experimental Results

- **Baseline Methods**
  - Several state-of-the-art face anti-spoofing methods:
    - Multi-scale LBP [1]
    - Color Texture [2]
    - Binary CNN[3]
    - Image distortion analysis features [4]
    - LBPTOP features [5]
    - Auxiliary [6]
  - Domain generalization method based on adversarial learning:
    - MMD-AAE [7]

[1] Spoofing face recognition with 3D masks., 2014. IEEE transactions on information forensics and security, 2014

[2] Face spoofing detection using color texture analysis., 2016. IEEE Transactions on Information Forensics and Security, 2016

[3] Learn convolutional neural network for face anti-spoofing., 2014. arXiv

[4] Face spoof detection with image distortion analysis., 2015. IEEE Transactions on Information Forensics and Security

[5] Face liveness detection using dynamic texture., 2014. EURASIP Journal on Image and Video Processing, 2014

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

[7] Haoliang Li, Sinno Jialin Pan, Shiqi Wang, and Alex C. Kot. Domain generalization with adversarial feature learning. In CVPR, 2018

Experimental Results

- **Comparison Results with face anti-spoofing methods**

Table 3. Comparison to face anti-spoofing methods on four testing sets for domain generalization on face anti-spoofing.

Method	O&C&I to M		O&M&I to C		O&C&M to I		I&C&M to O	
	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)
MS_LBP	29.76	78.50	54.28	44.98	50.30	51.64	50.29	49.31
Binary CNN	29.25	82.87	34.88	71.94	34.47	65.88	29.61	77.54
IDA	66.67	27.86	55.17	39.05	28.35	78.25	54.20	44.59
Color Texture	28.09	78.47	30.58	76.89	40.40	62.78	63.59	32.71
LBPTOP	36.90	70.80	42.60	61.05	49.45	49.54	53.15	44.09
Auxiliary(Depth Only)	22.72	85.88	33.52	73.15	29.14	71.69	30.17	77.61
Auxiliary(All)	–	–	28.4	–	27.6	–	–	–
Ours (MADDG)	**17.69**	**88.06**	**24.5**	**84.51**	**22.19**	**84.99**	**27.98**	**80.02**

Experimental Results

- **Comparison Results with adversarial domain generalization method**

Table 4. Comparison to adversarial domain generalization method on four testing sets for domain generalization on face anti-spoofing

Method	O&C&I to M		O&M&I to C		O&C&M to I		I&C&M to O	
	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)
MMD-AAE	27.08	83.19	44.59	58.29	31.58	75.18	40.98	63.08
Ours (MADDG)	**17.69**	**88.06**	**24.5**	**84.51**	**22.19**	**84.99**	**27.98**	**80.02**

Experimental Results

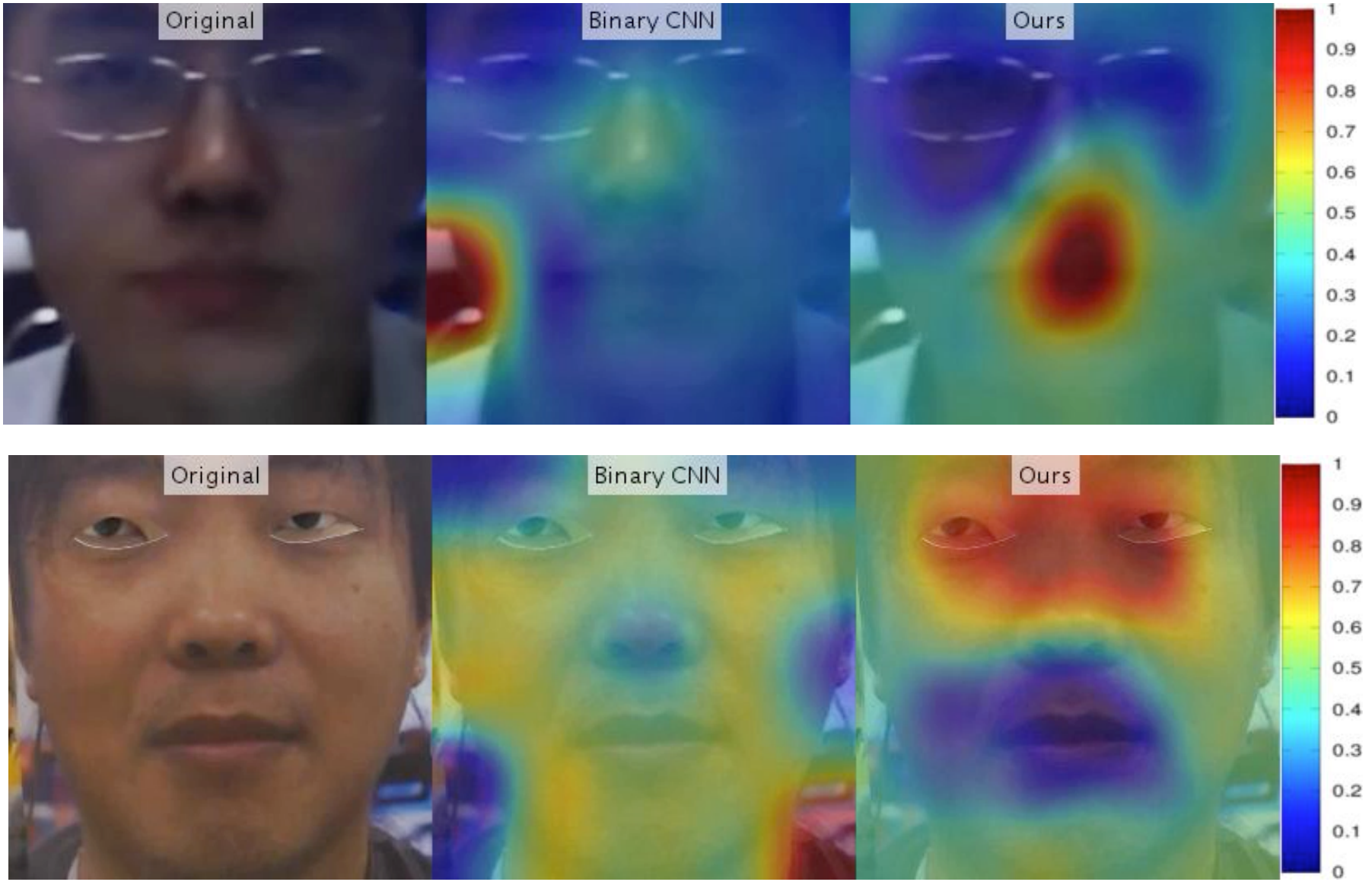
- **Fusion strategies comparison**

Table 6. Comparison to fusion strategies on four testing sets for domain generalization on face anti-spoofing.

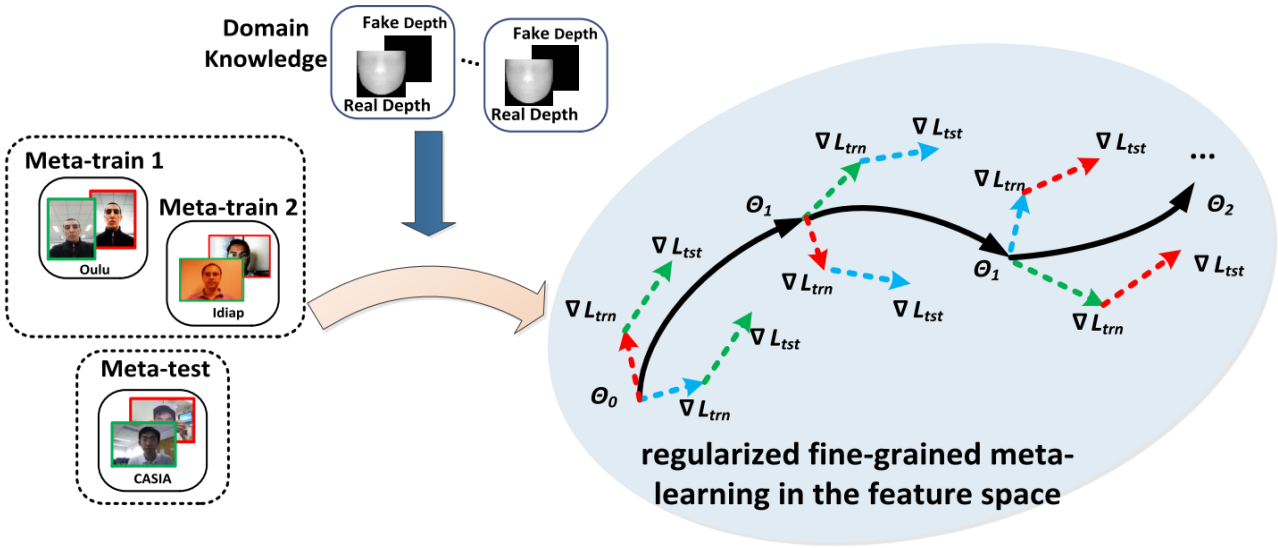
Method	O&C&I to M		O&M&I to C		O&C&M to I		I&C&M to O	
	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)
Score_Fusion	21.00	86.18	46.62	57.05	34.17	71.53	31.12	76.42
Feature_Fusion	25.62	74.57	52.32	48.23	46.29	52.71	32.56	76.01
Ours (MADDG)	**17.69**	**88.06**	**24.5**	**84.51**	**22.19**	**84.99**	**27.98**	**80.02**

- Simple fusion strategies cannot cope with various cross-domain scenarios so that in some scenarios such as O&M&I to C, the performance of both baseline methods drop significantly.

- Our method is robust in all scenarios.


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 DG 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]

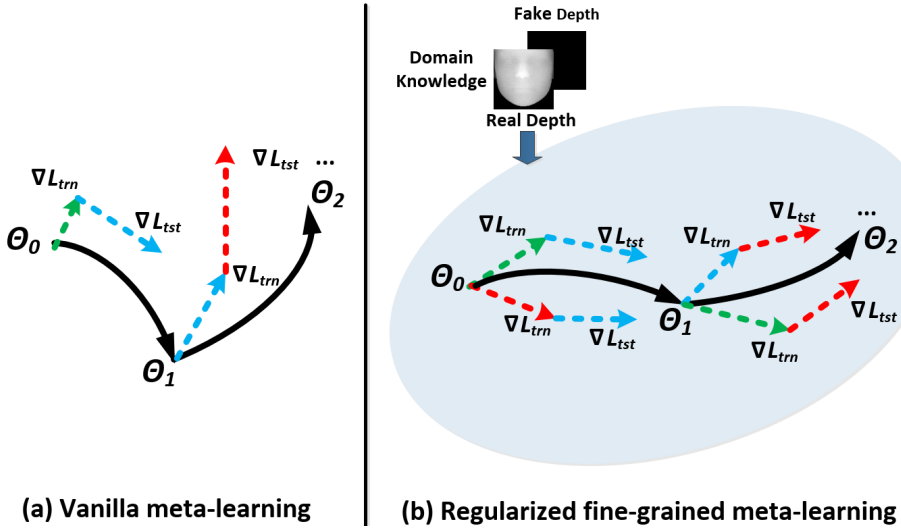
- Two issues if directly applying existing vanilla meta-learning for DG algorithms on face anti-spoofing ：
  - Second issue:

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:

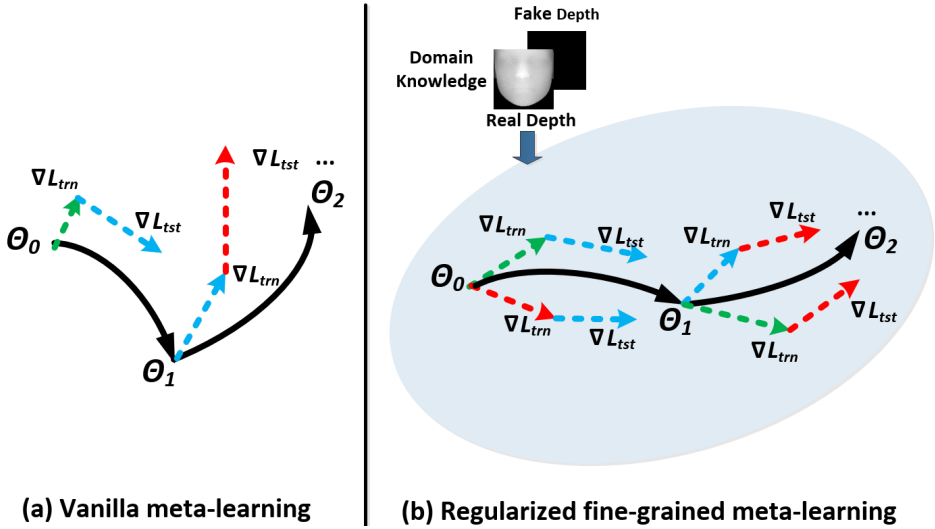
Incorporate the domain knowledge of face anti-spoofing as regularization into feature learning process

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 :



(a) Vanilla meta-learning

(b) Regularized fine-grained meta-learning

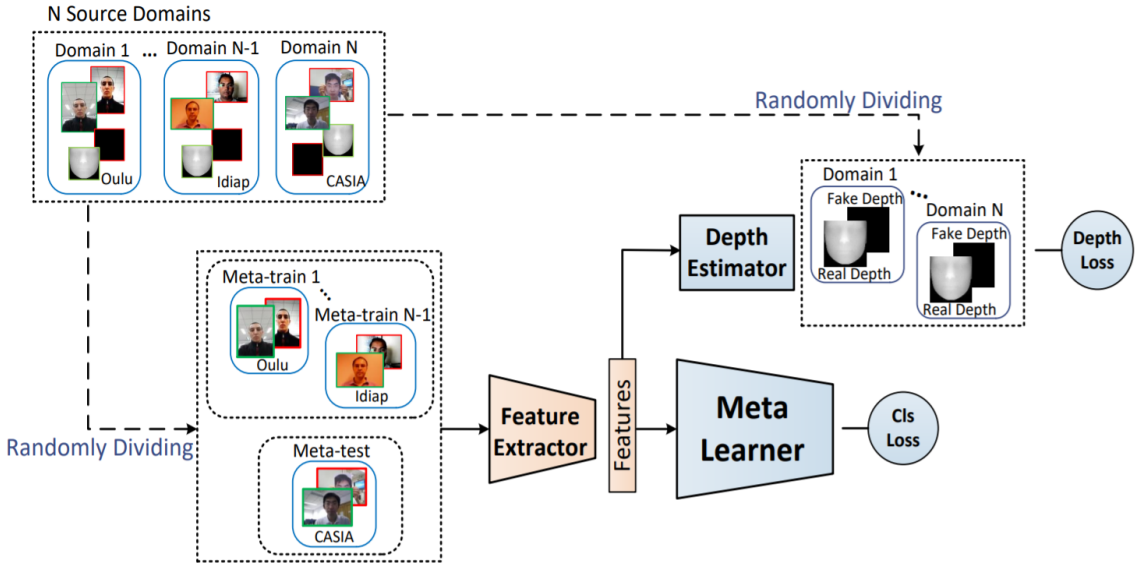
- For second issue:

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

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

- Method :



Algorithm 1 Regularized Fine-grained Meta Face Anti-spoofing

Require:
Input: N source domains $D = [D_1, D_2, ..., D_N]$,
Initialization: Model parameters $\theta_F, \theta_D, \theta_M$. Hyperparameters α, β

while not done **do**
  Randomly select $(N-1)$ source domains in D as D_{trn}, and the remaining one as D_{val}
  Meta-train: Sampling batch in each domain in D_{trn} as $\widehat{\mathcal{T}}_i$ $(i = 1, ..., N-1)$
  for each $\widehat{\mathcal{T}}_i$ **do**
    $\mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_M) = \sum_{(x,y)\sim\widehat{\mathcal{T}}_i} ylogM(F(x)) + (1-y)log(1-M(F(x)))$
    $\theta_{M_i}{}' = \theta_M - \alpha\nabla_{\theta_M}\mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_M)$
    $\mathcal{L}_{Dep(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_D) = \sum_{(x,I)\sim\widehat{\mathcal{T}}_i} \|D(F(x)) - I\|^2$
  end for
  Meta-test: Sampling batch in D_{val} as $\widetilde{\mathcal{T}}$
  $\sum_{i=1}^{N-1} \mathcal{L}_{Cls(\widetilde{\mathcal{T}})}(\theta_F, \theta_{M_i}{}') = \sum_{i=1}^{N-1} \sum_{(x,y)\sim\widetilde{\mathcal{T}}} ylogM_i{}'(F(x)) + (1-y)log(1-M_i{}'(F(x)))$
  $\mathcal{L}_{Dep(\widetilde{\mathcal{T}})}(\theta_F, \theta_D) = \sum_{(x,I)\sim\widetilde{\mathcal{T}}} \|D(F(x)) - I\|^2$
  Meta-optimization:
  $\theta_M \leftarrow \theta_M - \beta\nabla_{\theta_M}(\sum_{i=1}^{N-1}(\mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_M) + \mathcal{L}_{Cls(\widetilde{\mathcal{T}})}(\theta_F, \theta_{M_i}{}')))$
  $\theta_F \leftarrow \theta_F - \beta\nabla_{\theta_F}(\mathcal{L}_{Dep(\widetilde{\mathcal{T}})}(\theta_F, \theta_D) + \sum_{i=1}^{N-1}(\mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_M) + \mathcal{L}_{Dep(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_D) + \mathcal{L}_{Cls(\widetilde{\mathcal{T}})}(\theta_F, \theta_{M_i}{}')))$
  $\theta_D \leftarrow \theta_D - \beta\nabla_{\theta_D}(\mathcal{L}_{Dep(\widetilde{\mathcal{T}})}(\theta_F, \theta_D) + \sum_{i=1}^{N-1}(\mathcal{L}_{Dep(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_D)))$
end while
return Model parameters $\theta_F, \theta_D, \theta_M$

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

- Analysis :
  - The objective of meta-optimization is as follows:

$$\min_{\theta_M} = \sum_{i=1}^{N-1} (\mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_M) + \mathcal{L}_{Cls(\widetilde{\mathcal{T}})}(\theta_{M_i}{}'))$$

Do the first order Taylor expansion on the second term as follows:

$$\mathcal{L}_{Cls(\widetilde{\mathcal{T}})}(\theta_{M_i}{}') = \mathcal{L}_{Cls(\widetilde{\mathcal{T}})}(\theta_M - \alpha \nabla_{\theta_M} \mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_M)) =$$
$$\mathcal{L}_{Cls(\widetilde{\mathcal{T}})}(\theta_M) + \nabla_{\theta_M} \mathcal{L}_{Cls(\widetilde{\mathcal{T}})}(\theta_M)^T(-\alpha \nabla_{\theta_M} \mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_M))$$

$$\min_{\theta_M} = \sum_{i=1}^{N-1} (\mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_M) + \mathcal{L}_{Cls(\widetilde{\mathcal{T}})}(\theta_M)$$
$$- \alpha(\nabla_{\theta_M} \mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_M)^T \cdot \nabla_{\theta_M} \mathcal{L}_{Cls(\widetilde{\mathcal{T}})}(\theta_M)))$$

- Above objective is conducted **in feature space regularized by the domain knowledge supervision**, learning directions of meta-train and meta-test **more likely to be coordinated in the task of face anti-spoofing (in the above third term)**

- Above objective is simultaneously conducted between **multiple (N – 1) pairs** of meta-train and meta-test domains in each iteration. Our model can be trained to generalize well to unseen attacks of **various scenarios** in each iteration.

Experimental Results

- **Comparison Results with face anti-spoofing methods**

Table 1: Comparison to face anti-spoofing methods on four testing sets for domain generalization on face anti-spoofing.

Method	O&C&I to M		O&M&I to C		O&C&M to I		I&C&M to O	
	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)
MS_LBP	29.76	78.50	54.28	44.98	50.30	51.64	50.29	49.31
Binary CNN	29.25	82.87	34.88	71.94	34.47	65.88	29.61	77.54
IDA	66.67	27.86	55.17	39.05	28.35	78.25	54.20	44.59
Color Texture	28.09	78.47	30.58	76.89	40.40	62.78	63.59	32.71
LBPTOP	36.90	70.80	42.60	61.05	49.45	49.54	53.15	44.09
Auxiliary(Depth Only)	22.72	85.88	33.52	73.15	29.14	71.69	30.17	77.61
Auxiliary(All)	–	–	28.4	–	27.6	–	–	–
MMD-AAE	27.08	83.19	44.59	58.29	31.58	75.18	40.98	63.08
MADDG	17.69	88.06	24.5	84.51	22.19	84.99	27.98	80.02
Ours	**13.89**	**93.98**	**20.27**	**88.16**	**17.3**	**90.48**	**16.45**	**91.16**

Experimental Results

- **Comparison Results with meta-learning for DG method**

Table 2: Comparison to meta-learning for DG methods on four testing sets for domain generalization on face anti-spoofing.

Method	O&C&I to M		O&M&I to C		O&C&M to I		I&C&M to O	
	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)
Reptile	23.64	85.06	30.38	78.10	36.13	69.01	22.88	82.22
MLDG	23.91	84.81	32.75	74.51	36.55	68.54	25.75	79.52
MetaReg	21.17	86.11	35.66	70.83	32.28	67.48	37.72	68.71
Ours	**13.89**	**93.98**	**20.27**	**88.16**	**17.3**	**90.48**	**16.45**	**91.16**

Experimental Results

- **Ablation study**

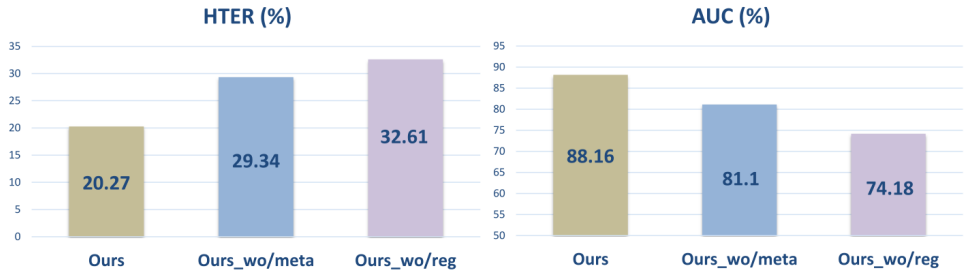


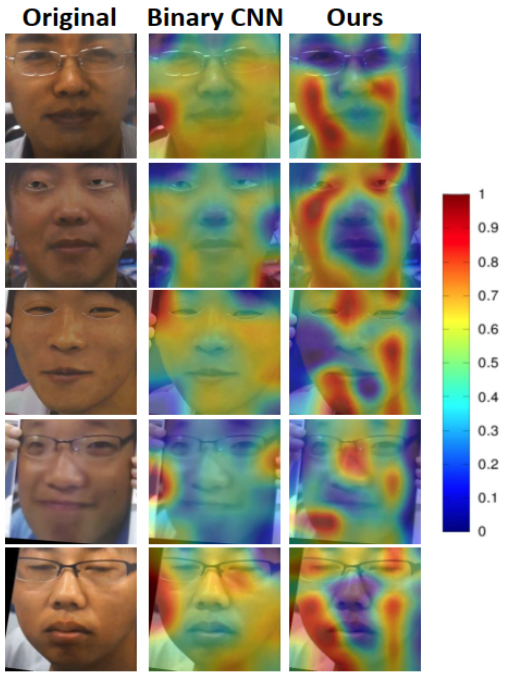
Figure 5: Evaluation of different components of proposed method in O&M&I to C set for face anti-spoofing.

Table 3: Effectiveness of fine-grained learning strategy and second-order derivative information

Method	O&C&I to M		O&M&I to C		O&C&M to I		I&C&M to O	
	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)
Ours (Aggregation)	14.54	92.87	24.28	85.29	20.07	88.13	17.94	90.69
Ours (First-order)	17.93	87.36	27.47	82.17	26.24	79.32	19.24	87.82
Ours	**13.89**	**93.98**	**20.27**	**88.16**	**17.3**	**90.48**	**16.45**	**91.16**

Experimental Results

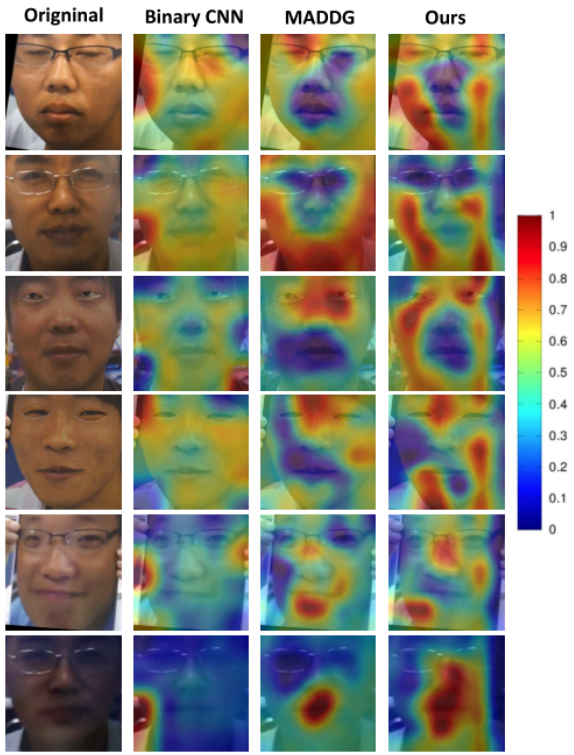
- **Visualization**



- Bianry_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 focuses on the region of internal face for searching generalized differentiation cues.

Experimental Results

- **Visualization (Contain comparison with MADDA (Our CVPR19))**



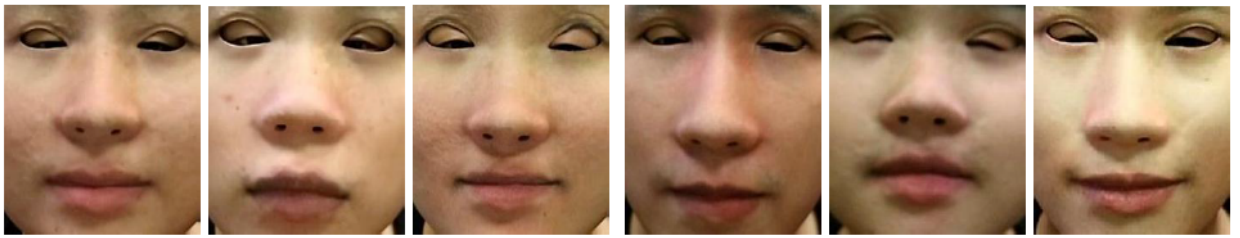
- Our method is more able to focus on the region of internal face for searching generalized differentiation cues.

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



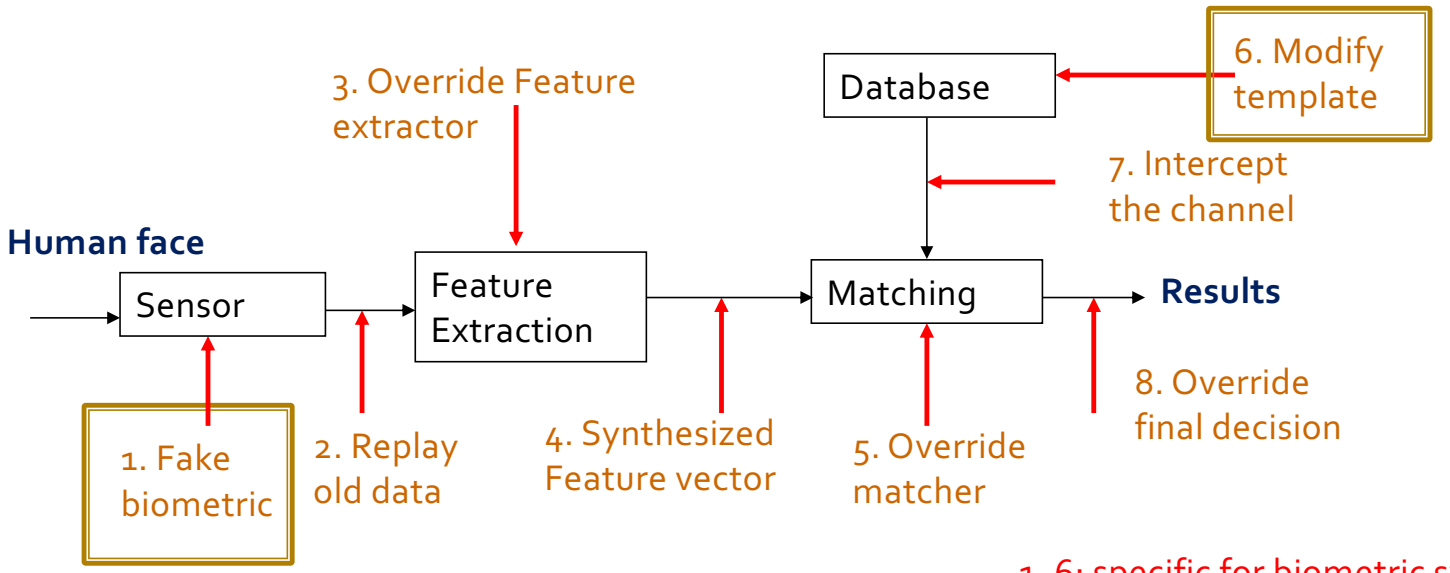
(a) (b) (c) (d) (e) (f)

(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



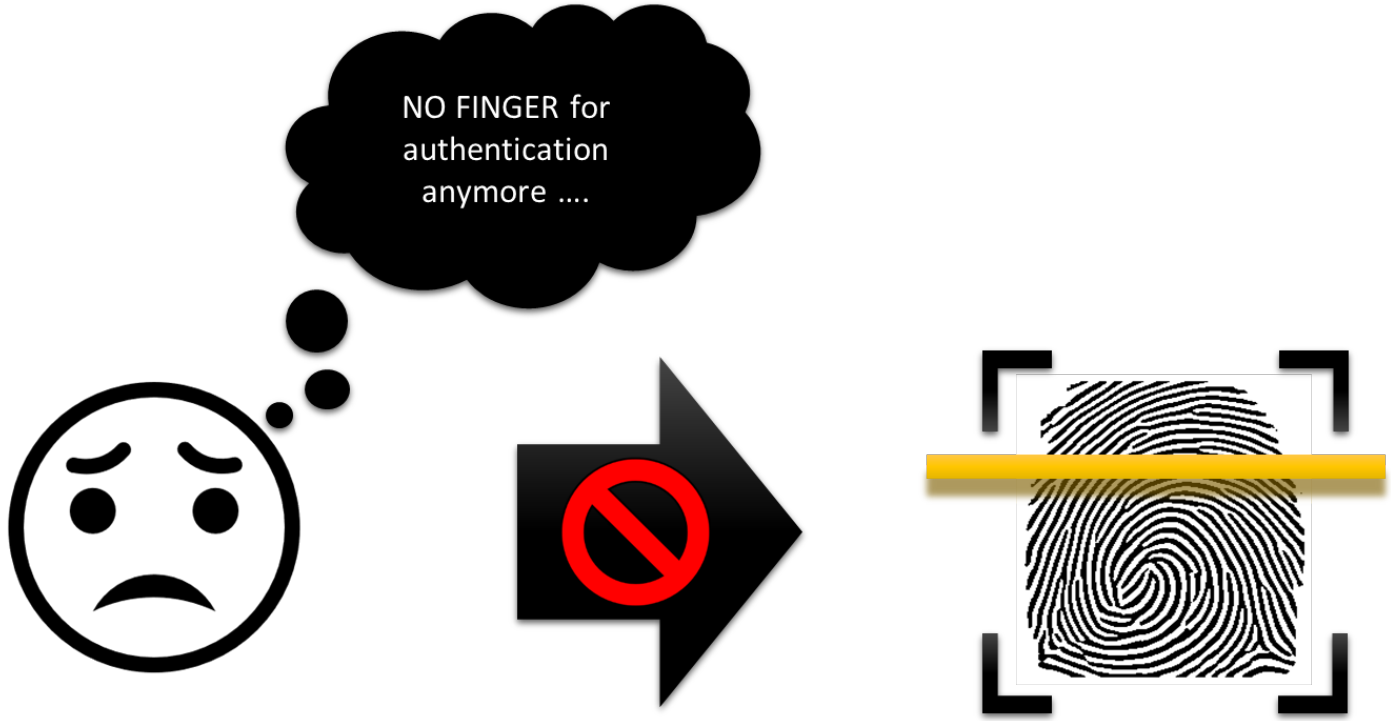
1, 6: specific for biometric systems

The Consequences of Template Attack

The stolen biometric template
= Identity Theft

Courtesy of Andrew Teoh

The Consequences of Template Attack



Limited Biometrics and Irrevocable

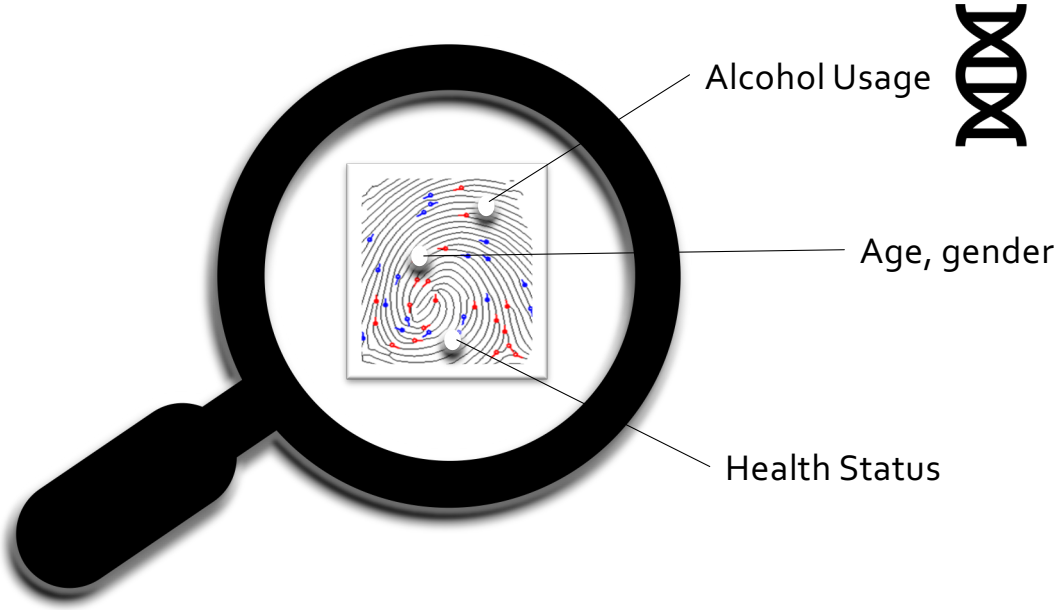
Courtesy of Andrew Teoh

The Consequences of Template Attack

Cross-matching

Courtesy of Andrew Teoh

The Consequences of Template Attack



Privacy Leakage

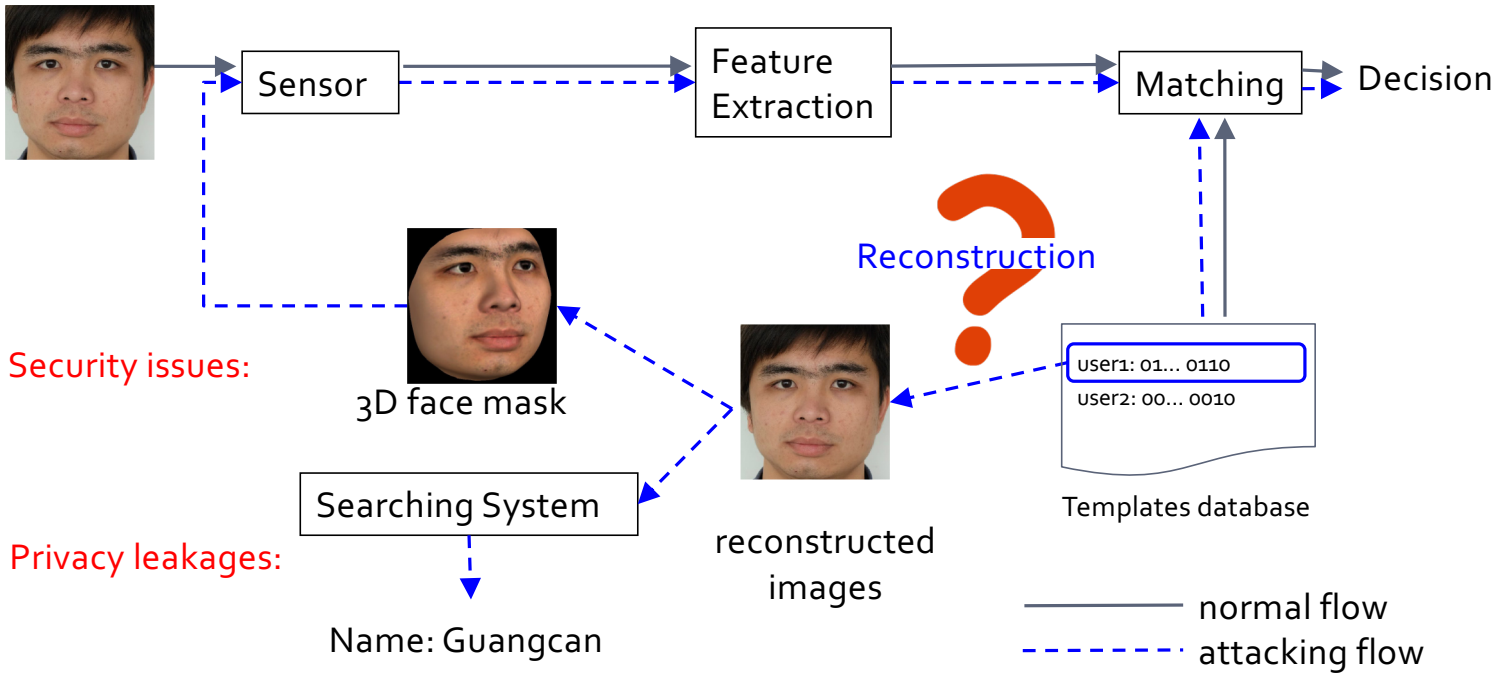
Courtesy of Andrew Teoh

Outline: Face Template Protection

1. Can we reconstruct a fake face from templates?
2. Review on existing techniques in protecting face templates
3. Our work
   a. Hybrid approach
   b. Binary Discriminative Analysis for binary template generation
   c. Binary template fusion for multi-biometric cryptosystems

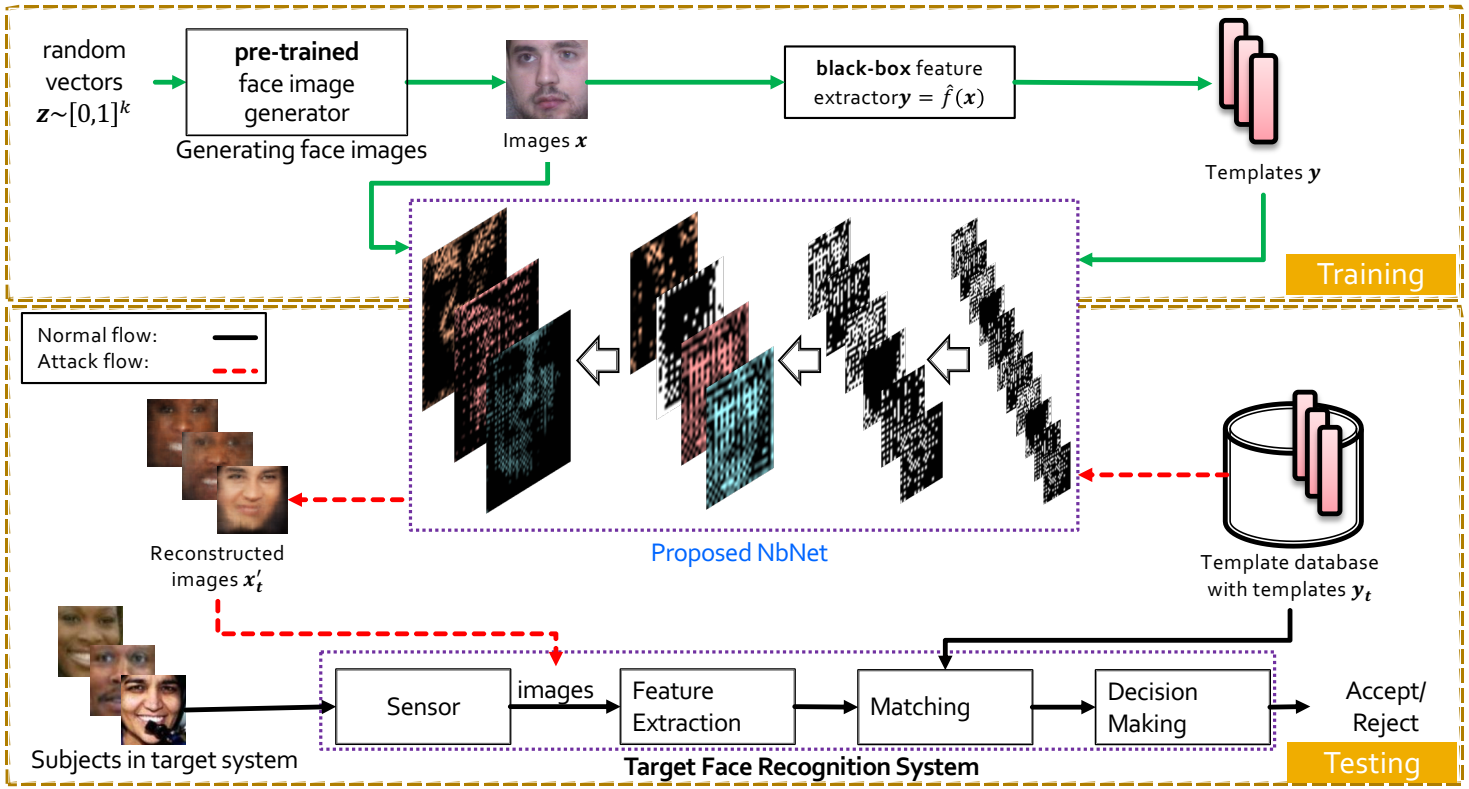
Can we reconstruct a fake face from templates?

Image Reconstruction Attack [TPAMI 2019]

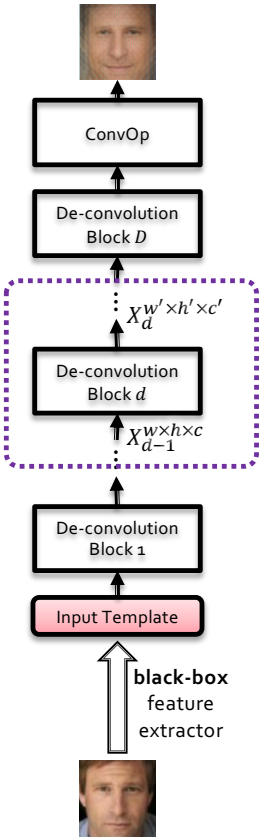


G. Mai, Kai Cao, P. C. Yuen and Anil K. Jain, On the Reconstruction of Deep Face Templates, *IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI)*, 2019

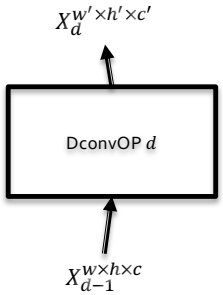
Proposed Reconstruction- Overview



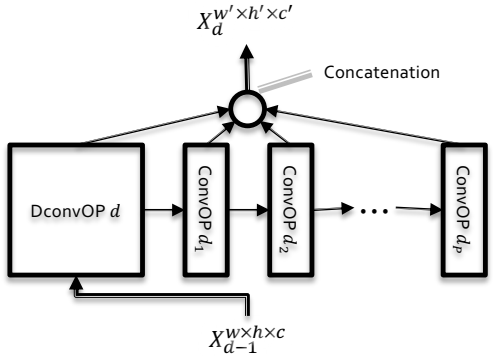
Proposed NbNet for Reconstruction



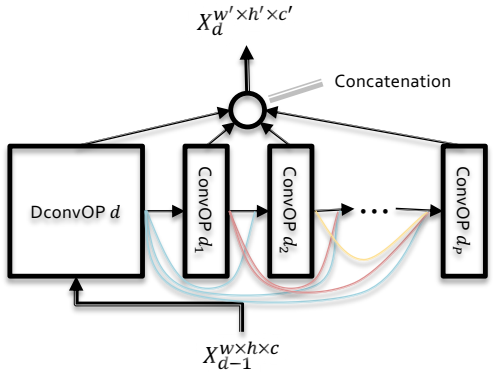
(a) Overview



(b) Naïve de-convolution block
Design for Building D-CNN (**Dn**)



(c) Neighborly de-convolution block A
Design for building our NbNet-A (**NbA**)



(d) Neighborly de-convolution block B
Design for building our NbNet-B (**NbB**)

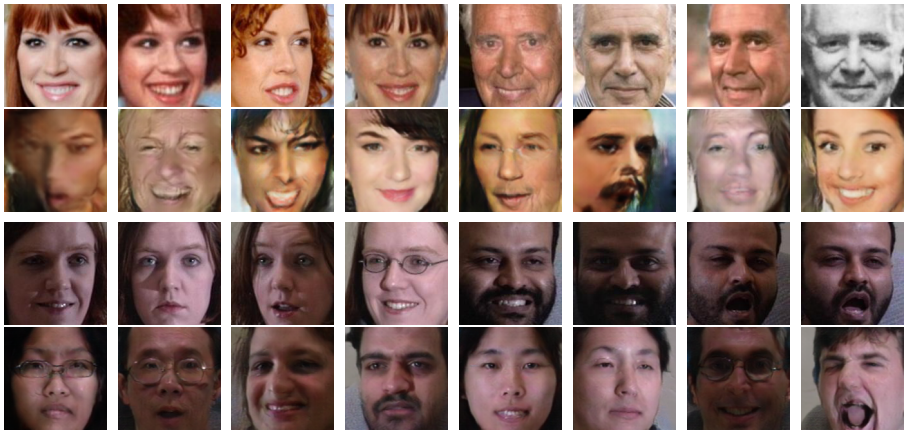
Network Details

Layer name	Output size ($c \times w \times h$)	D-CNN	NbNet-A, NbNet-B
input layer	$128 \times 1 \times 1$		
De-convolution Block (1)	$512 \times 5 \times 5$	$[5 \times 5, 512]$ DconvOP, stride 2	$[5 \times 5, 256]$ DconvOP, stride 2 $\{[3 \times 3, 8]$ ConvOP, stride $1\} \times 32$
De-convolution Block (2)	$256 \times 10 \times 10$	$[3 \times 3, 256]$ DconvOP, stride 2	$[3 \times 3, 128]$ DconvOP, stride 2 $\{[3 \times 3, 8]$ ConvOP, stride $1\} \times 16$
De-convolution Block (3)	$128 \times 20 \times 20$	$[3 \times 3, 128]$ DconvOP, stride 2	$[3 \times 3, 64]$ DconvOP, stride 2 $\{[3 \times 3, 8]$ ConvOP, stride $1\} \times 8$
De-convolution Block (4)	$64 \times 40 \times 40$	$[3 \times 3, 64]$ DconvOP, stride 2	$[3 \times 3, 32]$ DconvOP, stride 2 $\{[3 \times 3, 8]$ ConvOP, stride $1\} \times 4$
De-convolution Block (5)	$32 \times 80 \times 80$	$[3 \times 3, 32]$ DconvOP, stride 2	$[3 \times 3, 16]$ DconvOP, stride 2 $\{[3 \times 3, 8]$ ConvOP, stride $1\} \times 2$
De-convolution Block (6)	$16 \times 160 \times 160$	$[3 \times 3, 16]$ DconvOP, stride 2	$[3 \times 3, 8]$ DconvOP, stride 2 $\{[3 \times 3, 8]$ ConvOP, stride $1\} \times 1$
ConvOP	$3 \times 160 \times 160$	$[3 \times 3, 3]$ ConvOP, stride 1	
Loss layer	$3 \times 160 \times 160$	Pixel difference or perceptual loss [36]	

$[k_1 \times k_2, c]$ DconvOP (ConvOP), stride s denotes cascade of a de-convolution (convolutionan) layer with c channels, kernel size $(k_1 \times k_2)$, and stride s, batch normalization and ReLU (tanh for the bottom ConvOP) activation layer

Experiments - Training

- **Feature extractor** [1], an implementation of FaceNet [2]
- **Network arichitecture**: D-CNN (Dn), NbNet-A (NbA), NbNet-B (NbB)
- **Training approach**: Generated images & Raw images (r)
- **Loss function**: Pixel difference (M) & Perceptual Loss [3] (P)
- **Training datasets:**



VGG Raw Images:	1.94 M
VGG Gen Images:	19.2 M
Multi-PIE Raw Images:	150,760
Multi-PIE Gen Images:	19.2 M

1. https://github.com/davidsandberg/facenet (model: 20170512-110547)
2. Schroff, Florian et al. "Facenet: A unified embedding for face recognition and clustering." *CVPR2015*
3. *Johnson et. al., "Perceptual losses for real-time style transfer and super-resolution", ECCV2016*

Experiments

- Verification (protocol: BLUFR[1], comparison: RBF [2])
  - Type-I attack: match the reconstructed image against the same one from which representation was extracted
  - Type-II attack: match the reconstructed image against a different one of the same subject
- Identification (Rank-one identification rate)
  - Type-I attack: identify the images reconstructed from the gallery set
  - Type-II attack: identify the images reconstructed from the probe set
- Testing datasets

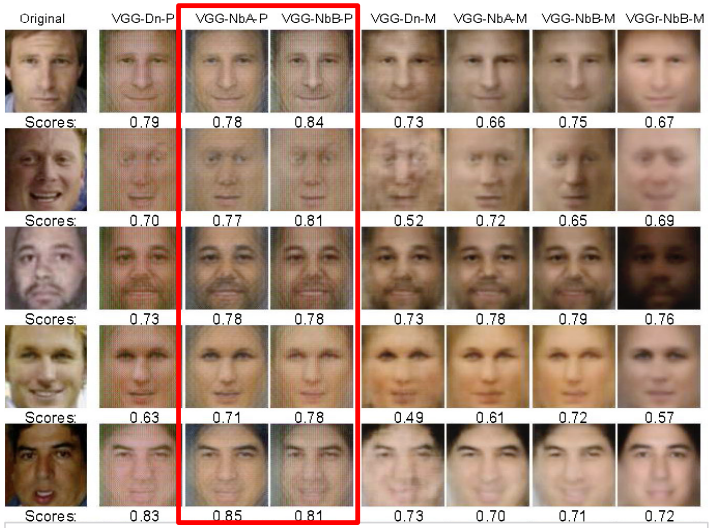
(a) LFW (Verification)

(b) FRGC V2.0 (Verification)

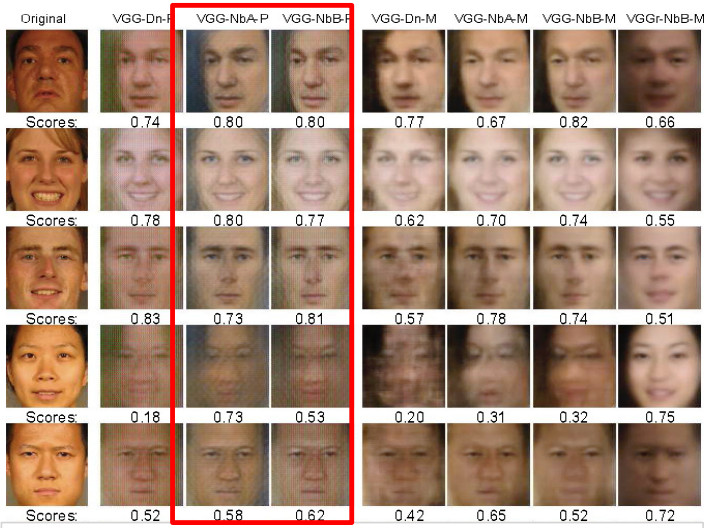
(c) Color FERET (Identification)

1. Shengcai Liao, Zhen Lei, Dong Yi, Stan Z. Li, "A Benchmark Study of Large-scale Unconstrained Face Recognition." , IJCB2014
2. Mignon, Alexis, and Frédéric Jurie. "Reconstructing Faces from their Signatures using RBF Regression." *BMVC2013*

Reconstruction of First 5 Subjects*



LFW Thresholds:
@(FAR=0.1%) = 0.51 @ (FAR=1%) = 0.38

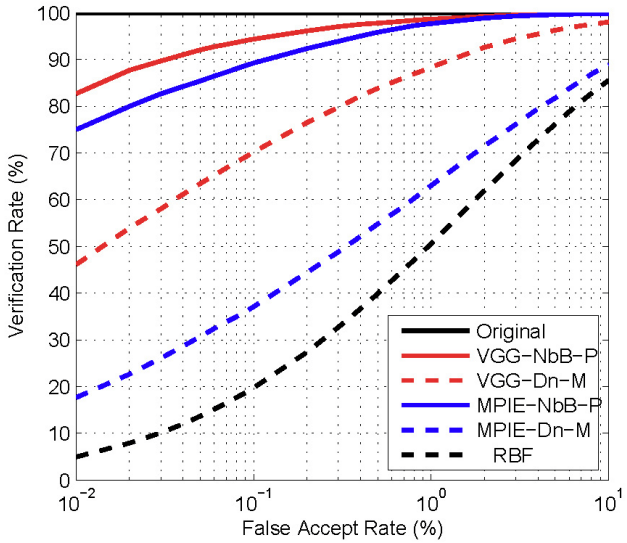


FRGC v2.0 Thresholds:
@(FAR=0.1%) = 0.80 @ (FAR=1%) = 0.64

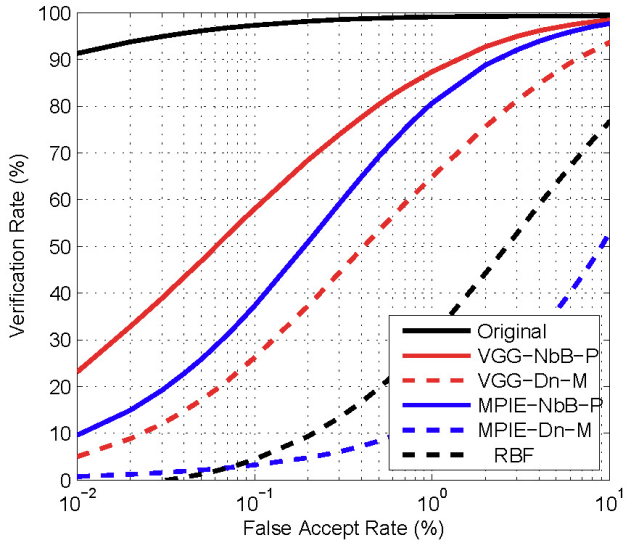
- * As specified in the image list of the BLUFR protocol [1]
- 'VGG-' , 'MPIE-' denotes the face image generator is pretrained by the VGG-Face (2.6M) and MultiPIE (fontal images, 150K)
- 'VGGr-' denotes the NbNet directly trained by the raw images in VGG-Face, no face image generator is used.
- '-Dn-', '-NbA-', '-NbB-' denote the network architecture, i.e., D-CNN, NbNet-A and NbNet-B
- '-P' trained with perceptual loss
- '-M' trained with pixel-wise mean absolute error

1. Shengcai Liao, Zhen Lei, Dong Yi, Stan Z. Li, "A Benchmark Study of Large-scale Unconstrained Face Recognition." , IJCB2014

Experiments – Verification on LFW



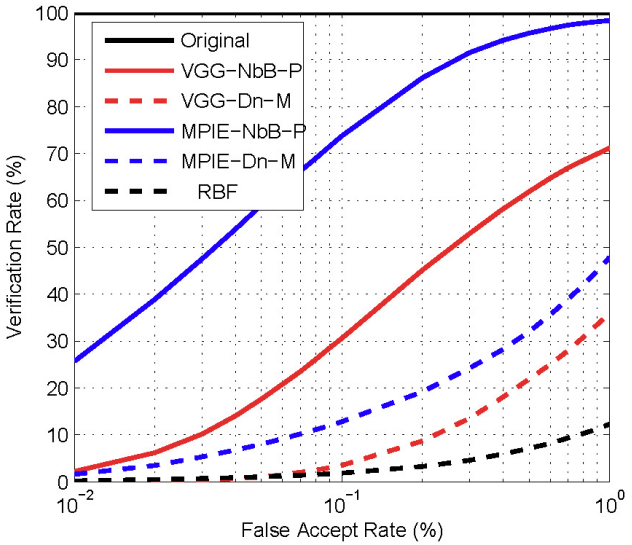
(a) Type-I attack on LFW



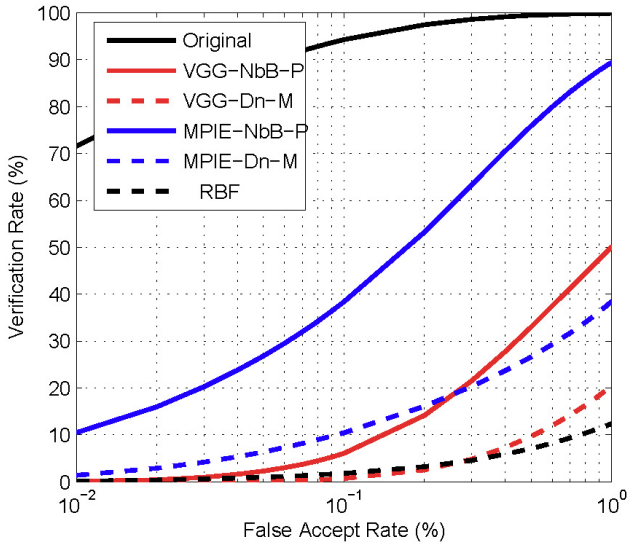
(b) Type-II attack on LFW

- Type-I attack: match the reconstructed image against the same one from which representation was extracted
- Type-II attack: match the reconstructed image against a different one of the same subject

Experiments – Verification on FRGC



(a) Type-I attack on FRGC



(b) Type-II attack on FRGC

- Type-I attack: match the reconstructed image against the same one from which representation was extracted
- Type-II attack: match the reconstructed image against a different one of the same subject

Identification with Reconstructed Images on Color FERET

Probe (partition specified by protocol)	Type-I	Type-II		
	fa	fb	dup1	dup2
Original	100.00	98.89	97.96	99.12
VGG-Dn-P	89.03	86.59	76.77	78.51
VGG-NbA-P	94.87	90.93	80.30	81.58
VGG-NbB-P	95.57	**92.84**	*84.78*	84.65
VGG-Dn-M	80.68	74.40	62.91	65.35
VGG-NbA-M	86.62	80.44	64.95	66.67
VGG-NbB-M	92.15	87.00	75	75.44
VGGr-NbB-M	81.09	74.29	61.28	62.28
MPIE-Dn-P	*96.07*	91.73	84.38	*85.53*
MPIE-NbA-P	93.86	90.22	79.89	79.82
MPIE-NbB-P	**96.58**	**92.84**	**86.01**	**87.72**
MPIE-Dn-M	73.54	64.11	53.26	49.12
MPIE-NbA-M	72.23	64.01	51.09	44.74
MPIE-NbB-M	85.61	78.22	71.06	68.42
MPIEr-NbB-M	63.88	54.54	44.57	35.96
Mixedr-NbB-M	82.19	76.11	62.09	58.77

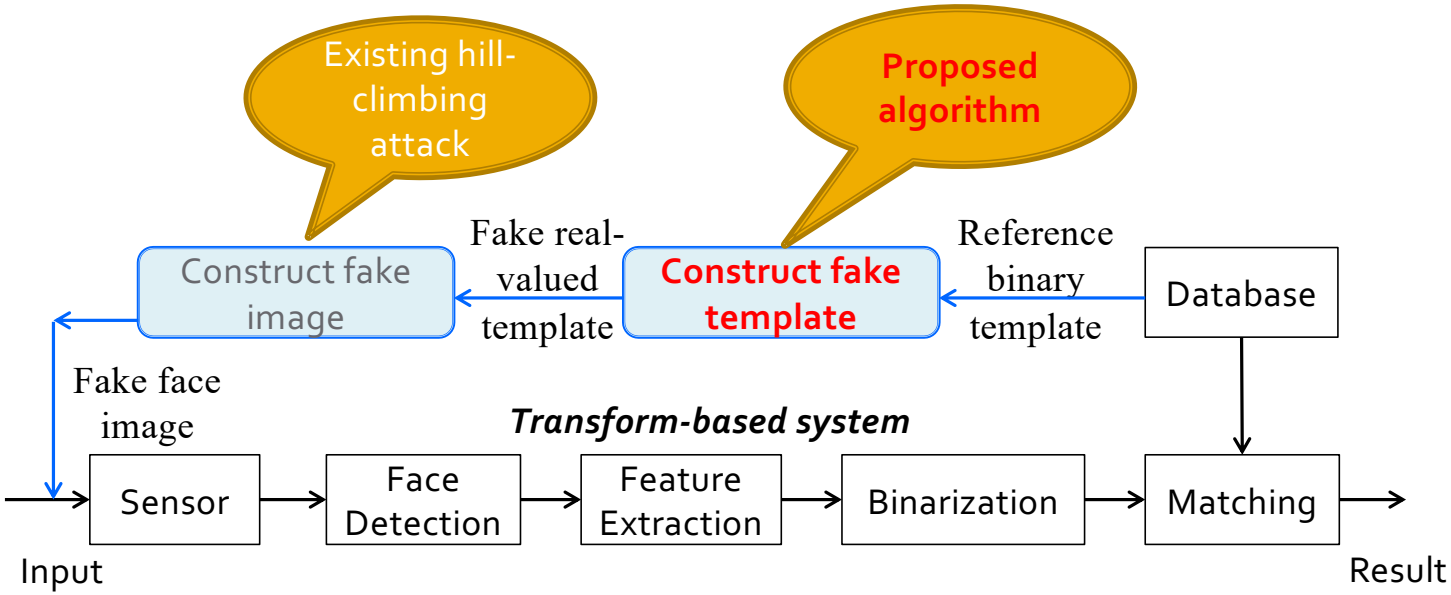
Best:
boldface
Second best:
underline

Type-I attack:
identify the images reconstructed from the gallery set (partition *fa*)

Type-II attack:
identify the images reconstructed from the images which not used in the gallery set (partition *fb*, *dup1*, *dup2*)

Binary Template is INSECURE too! [PR2014]

- Attack a transform-based system (partially protected, will be introduced later) with two steps



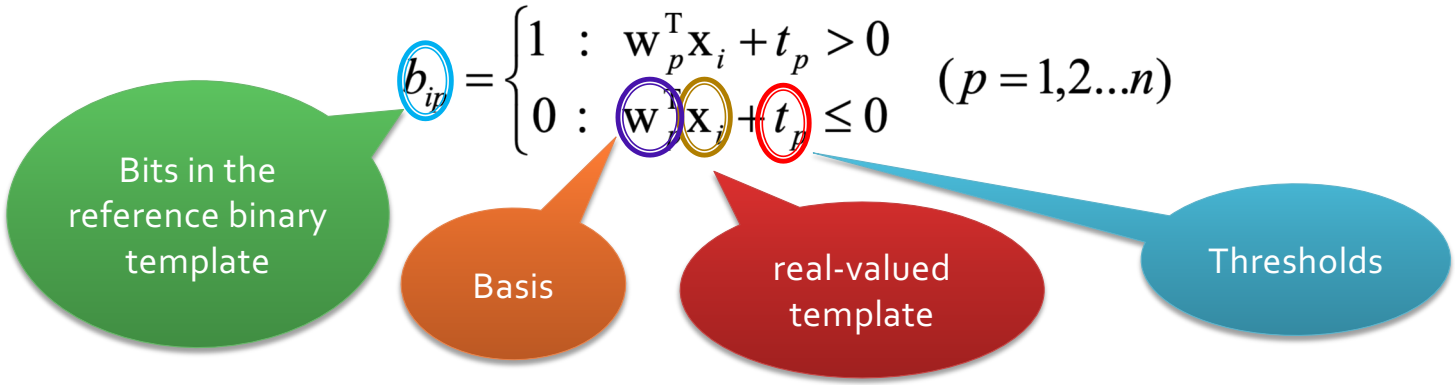
Y C Feng, M H Lim and P C Yuen, Masquerade attack on transform-based binary-template protection based on perceptron learning, *Pattern Recognition*, 2014.

From Binary Templates to Faces

- Consider two scenarios
  - The binarization scheme is understood by the attacker
  - The binarization scheme is unknown to the attacker
- Assumptions

Scenario One

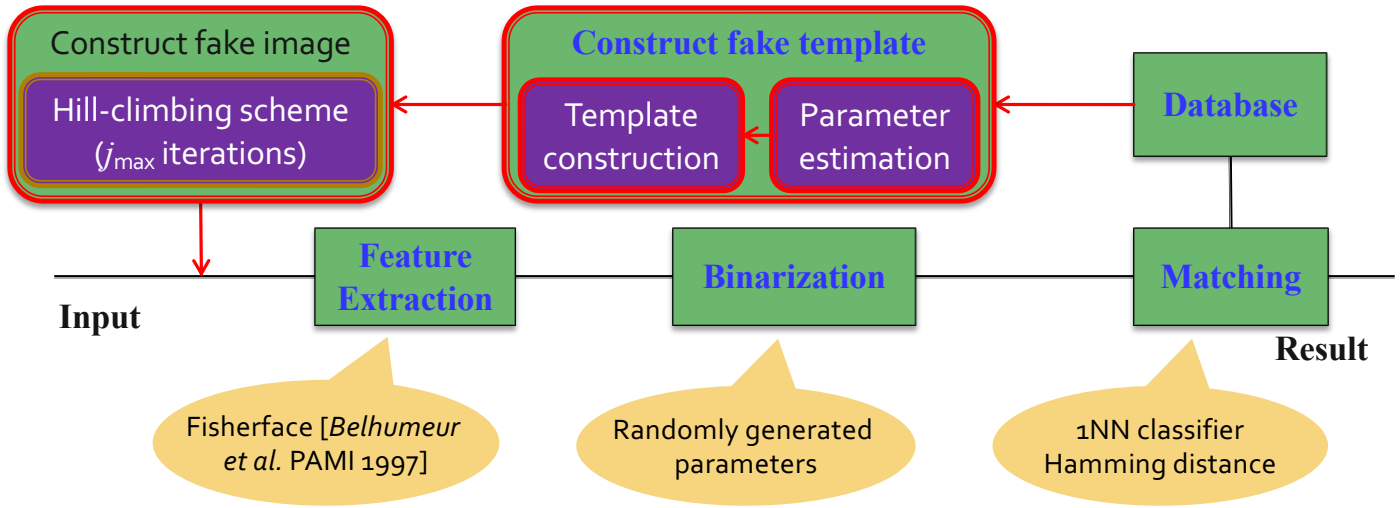
- Understand the binarization scheme
  - Most schemes follow "projection + thresholding" approach



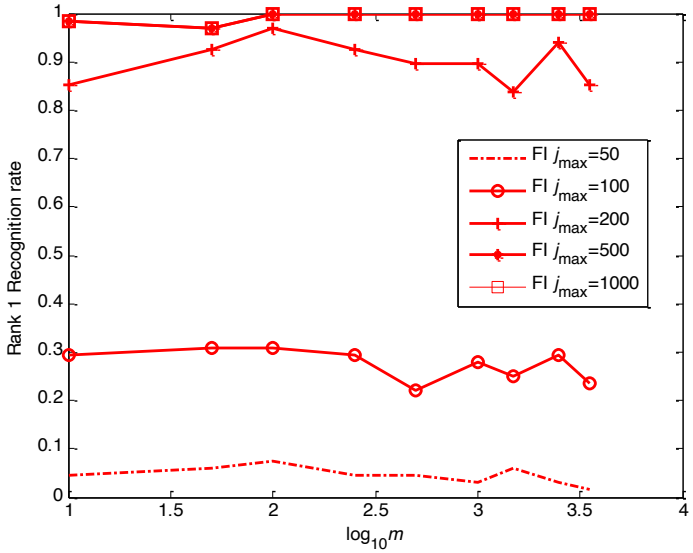
  - Two steps to construct fake template
    - Binarization parameters estimation
    - Construct fake template with estimated parameters

Scenario One

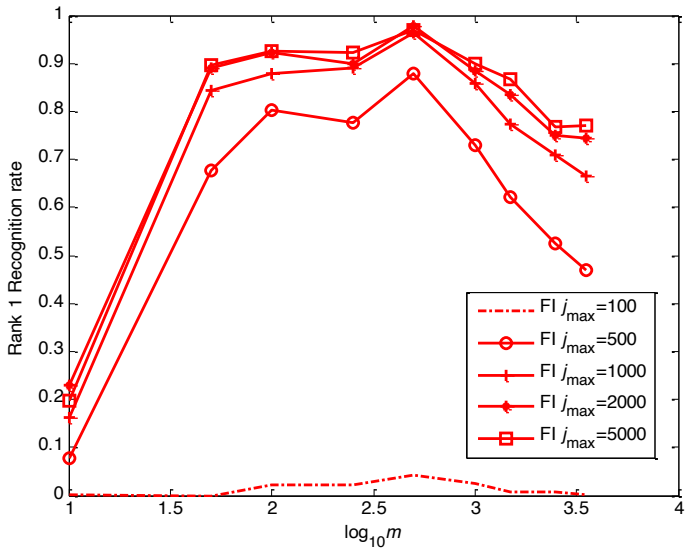
- Experimental results
  - Experiment settings
    - CMU PIE & FRGC databases employed
    - Choose different *m* (No. of local faces) in testing



Scenario One – Results



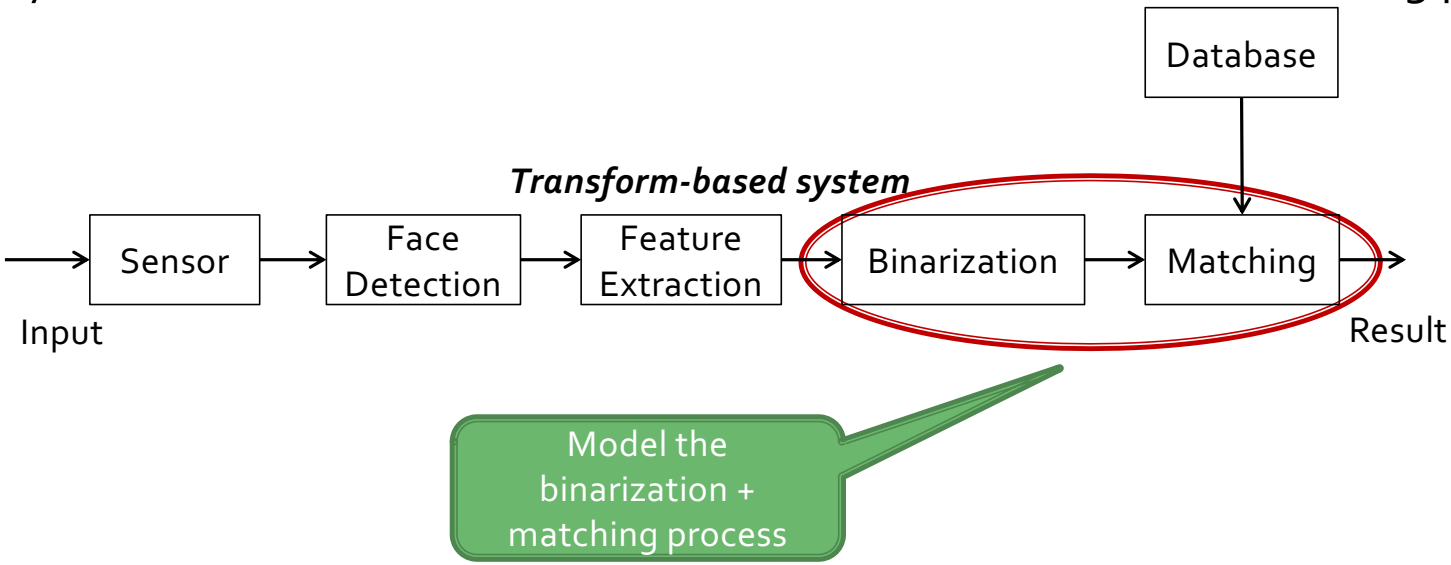
CMU PIE



FRGC

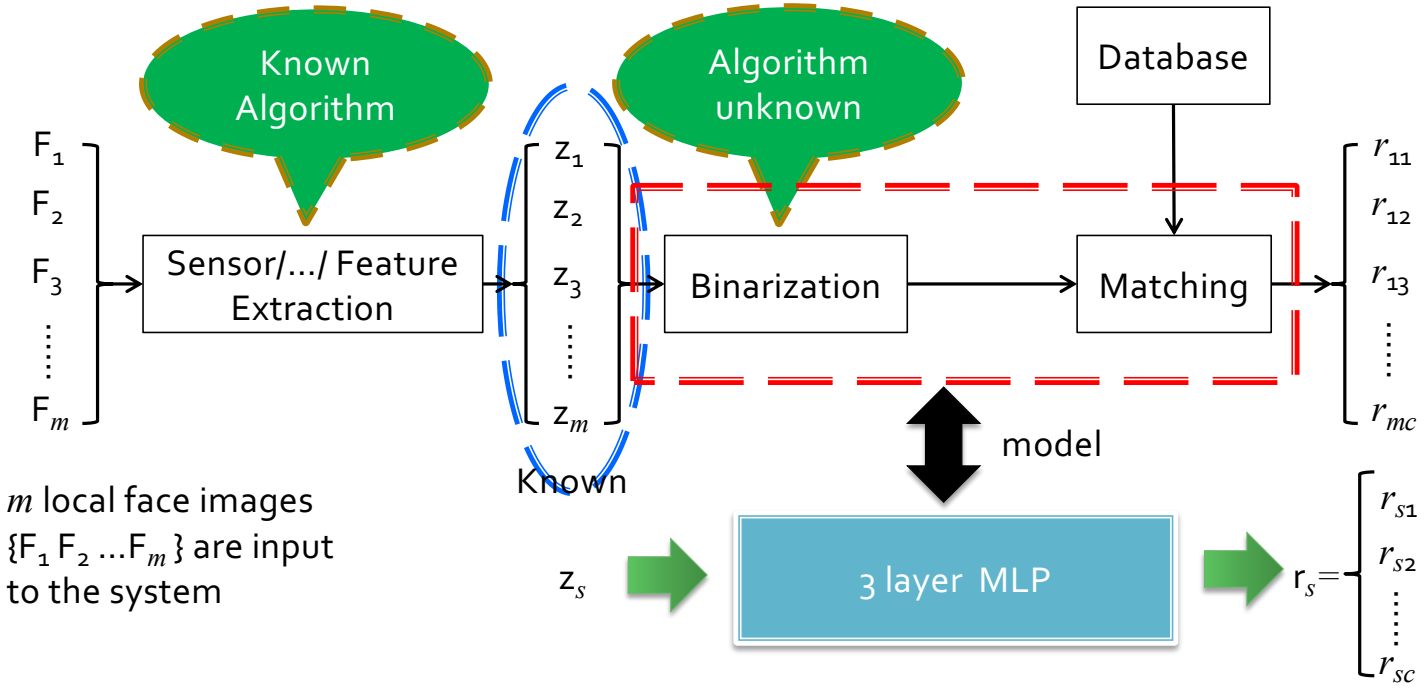
Scenario Two

- Since the attacker does not understand the binarization algorithm, the binarization process needs to be modeled.
- Employ artificial neural networks to model the binarization and matching process



Scenario Two

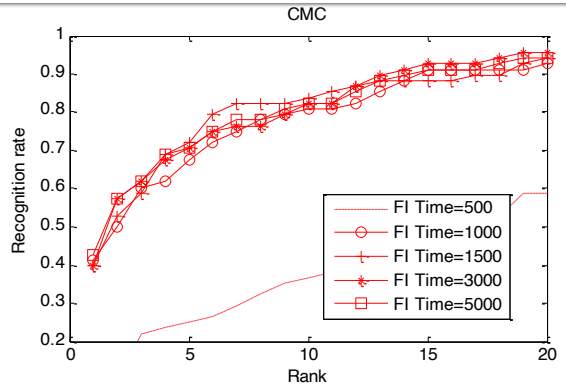
- Use local faces for modeling



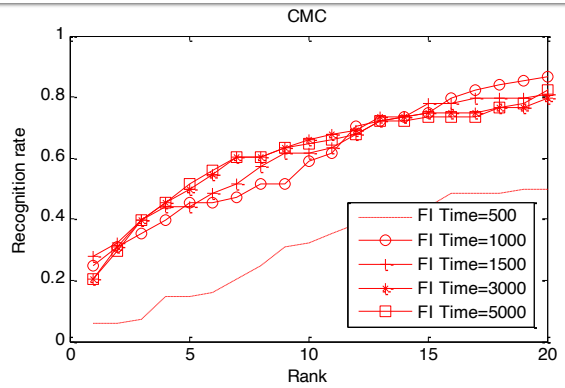
Scenario Two

- Experimental results
  - Experiment settings
    - Follow the settings in scenario one
    - Implement the proposed attack in different binarization schemes
      - Biohashing (BH)
      - Multi-stage biohashing (MBH)
      - Feature binarization (FB)
      - Discriminability-preserving transform (DP)

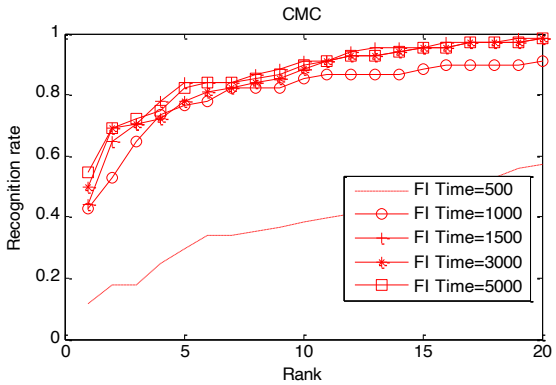
Scenario Two – CMU-PIE Results



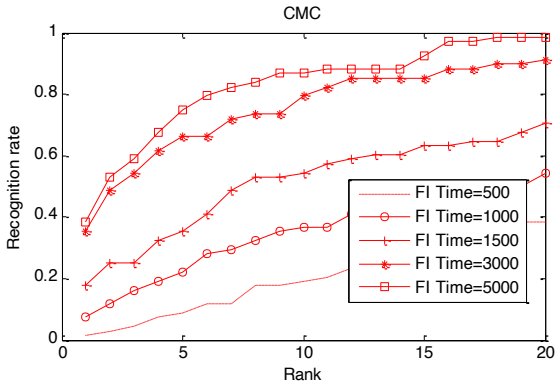
BH



MBH

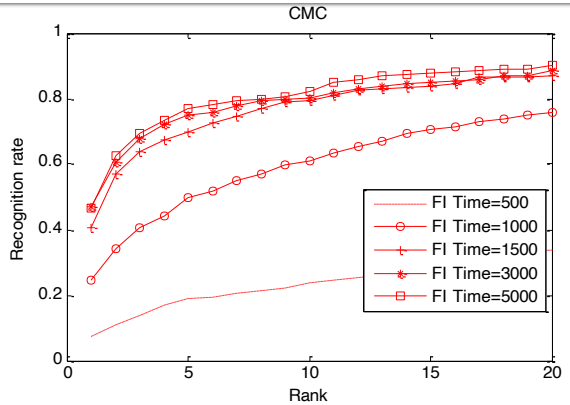


FB

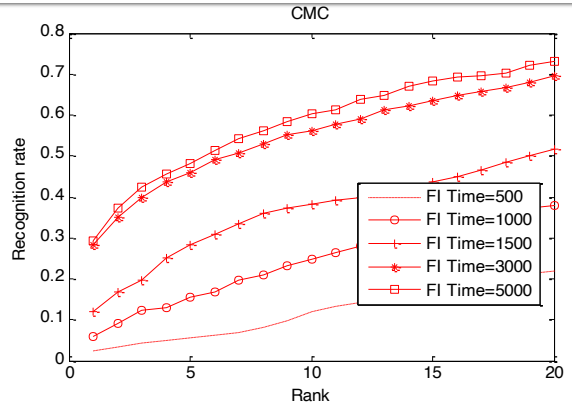


DP

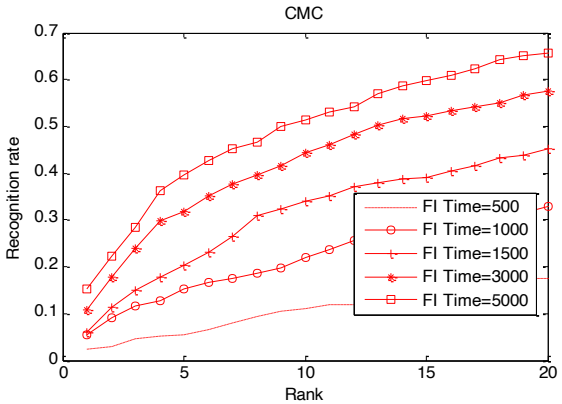
Scenario Two – FRGC Results



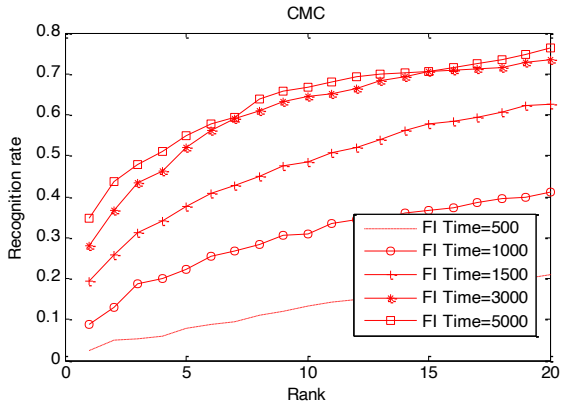
BH



MBH



FB



DP

Review on Existing Techniques for Face Template Protection

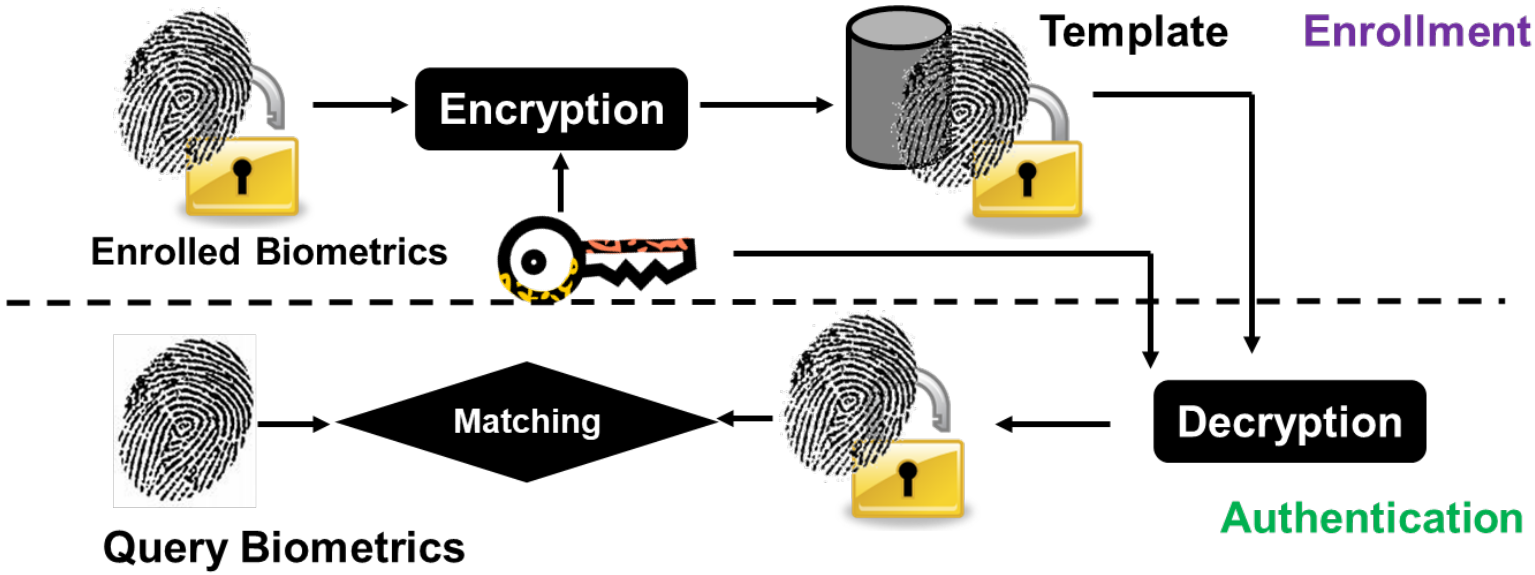
Requirements

Security	Discriminability	Cancelability
• Computationally hard to reconstruct the original template from the secure template.	• 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.	• The secure template can be canceled and re-issued from original template if it is stolen or lost.

Basic Idea

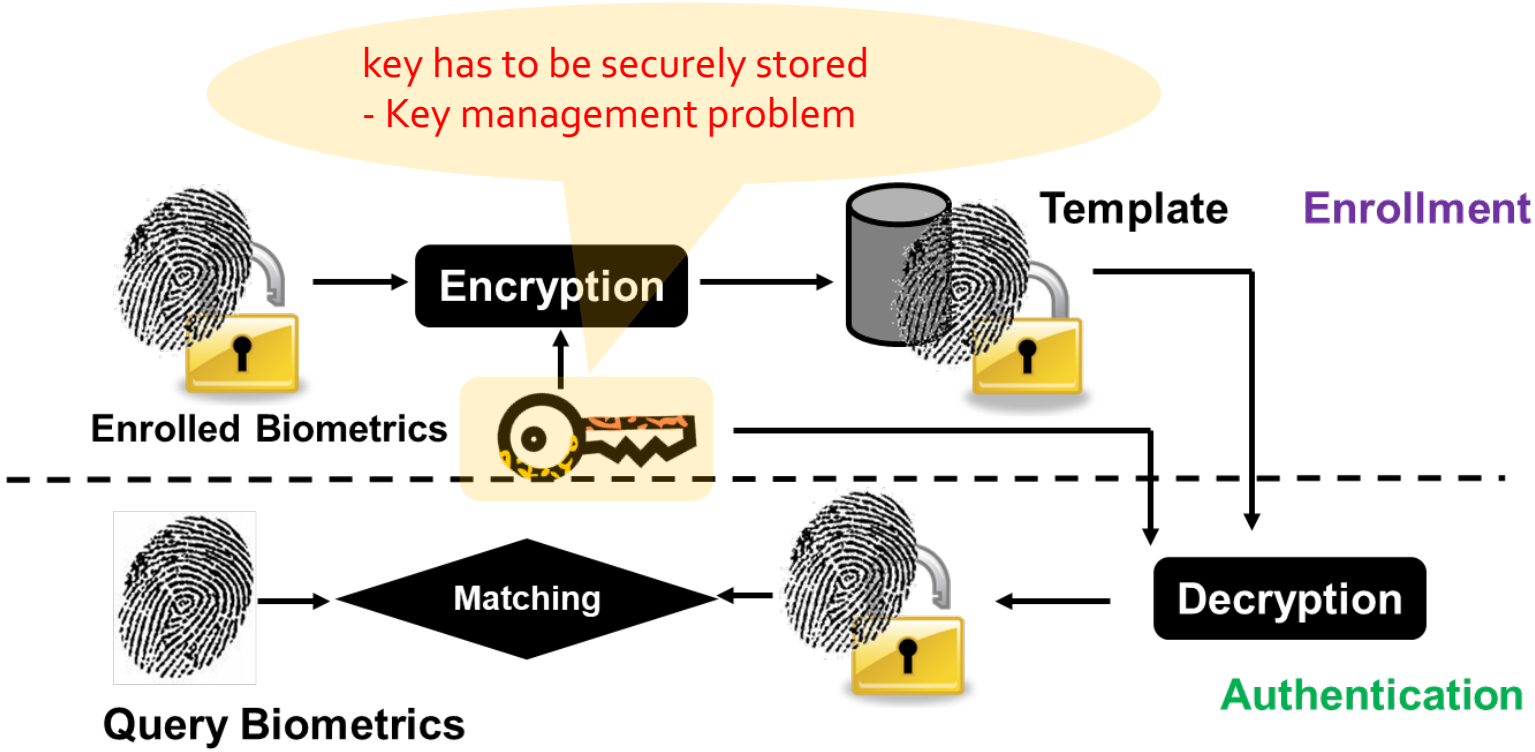
- General approach: *Never* store the original raw biometric template
- Straightforward method: Protection with traditional encryption/hashing methods (e.g. DES, MD5)
  - Small change in input cause large change in output
  - Intra-class variations => not good for matching
  - Not feasible

Present Commercial Solution



Courtesy of Andrew Teoh

Not an Ideal Solution



Courtesy of Andrew Teoh

Existing Approaches

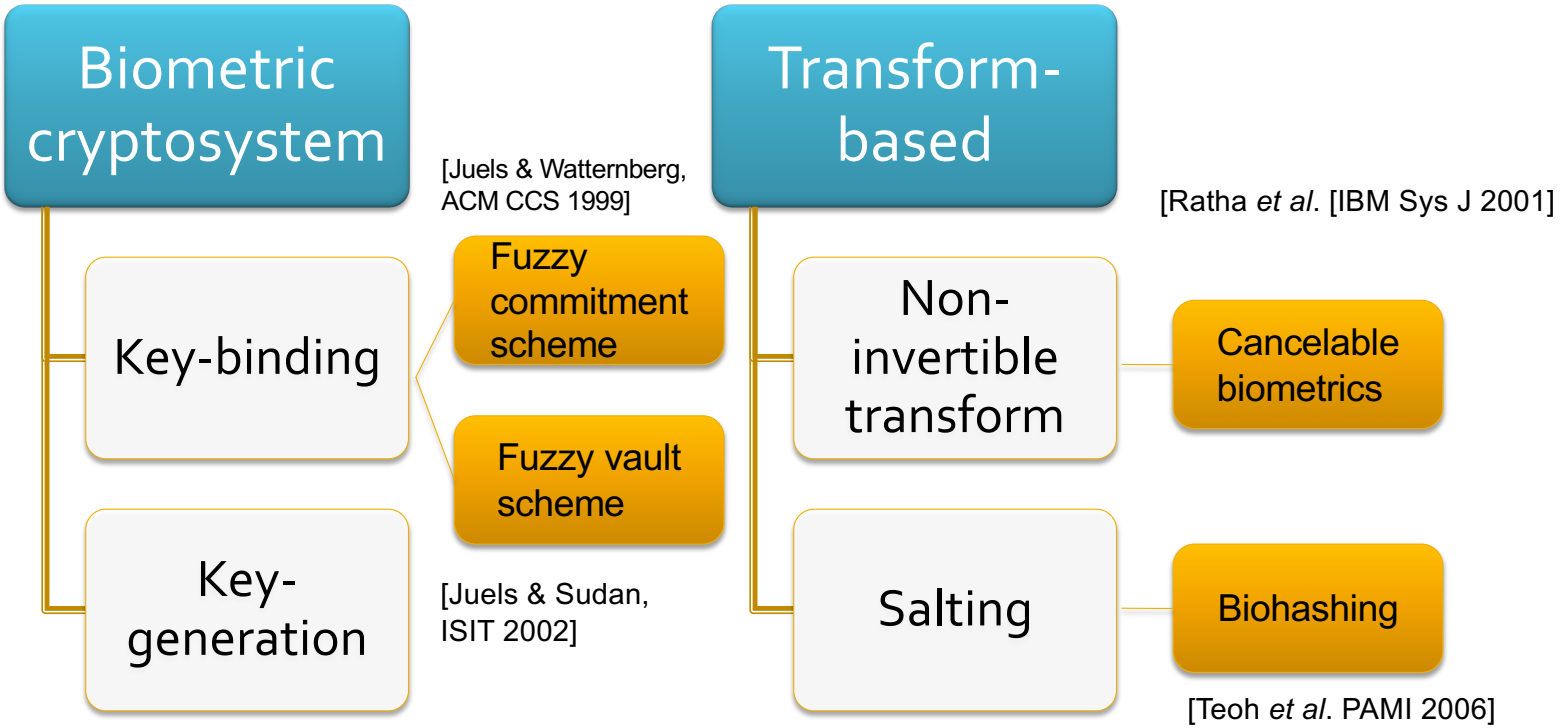
Biometric cryptosystem

- 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

Existing Approaches



Biometric Cryptosystems

Key-binding

- The cryptographic key is independent from biometric data.
- ***Advantage***: Tolerance of intra-class variations
- ***Disadvantage***: Require finite field input & Not for cancelability purpose

Key generation

- The cryptographic key is directly generated from the biometric data.
- ***Advantage***: Direct key generation
- ***Disadvantage***: Hard to generate secure and variance-tolerant key

Transform-based Approach

Non-invertible transform

- The transform is non-invertible. Even if K and $f(\mathrm{T},\mathrm{K})$ are known, T can not be retrieved.
- ***Advantage***: High security
- ***Disadvantage:*** Trade-off between security & discriminability

Salting

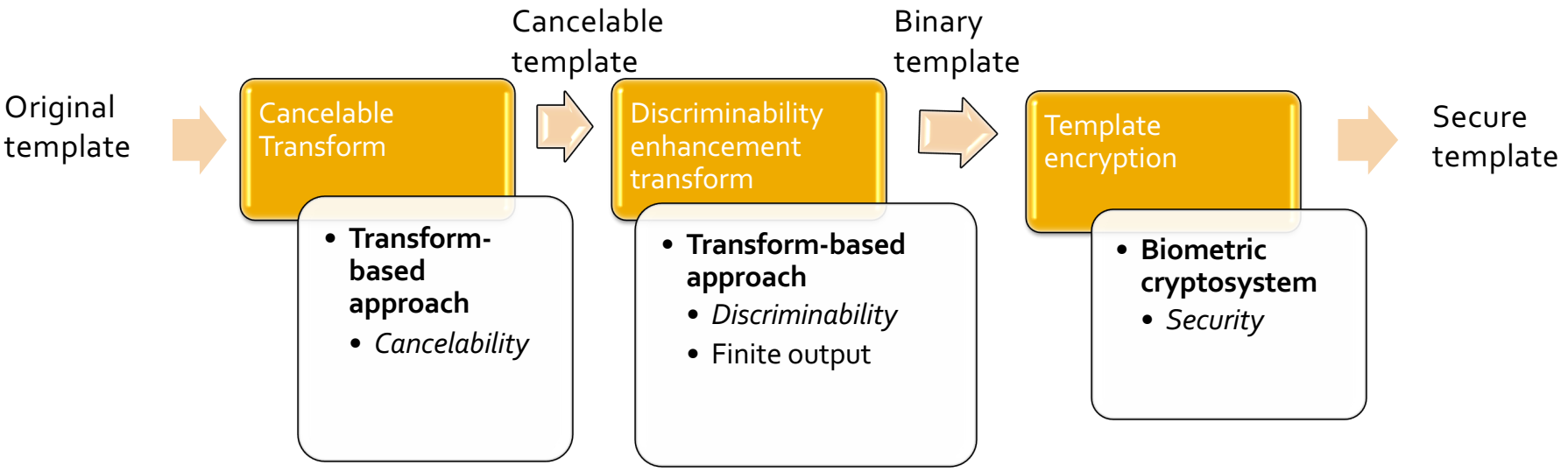
- A user-specific key is applied in transform to diverge the outputs, resulting in high performance
- ***Advantage***: Cancelable & High performance
- ***Disadvantage***: Unsecure user-specific key & invertible transform

Our Works

a. Hybrid Approach [TIFS 2010]
b. Binary Discriminative Analysis for binary template generation [TIFS 2012]
c. Binary template fusion for multi-biometric cryptosystems [IVC 2017]

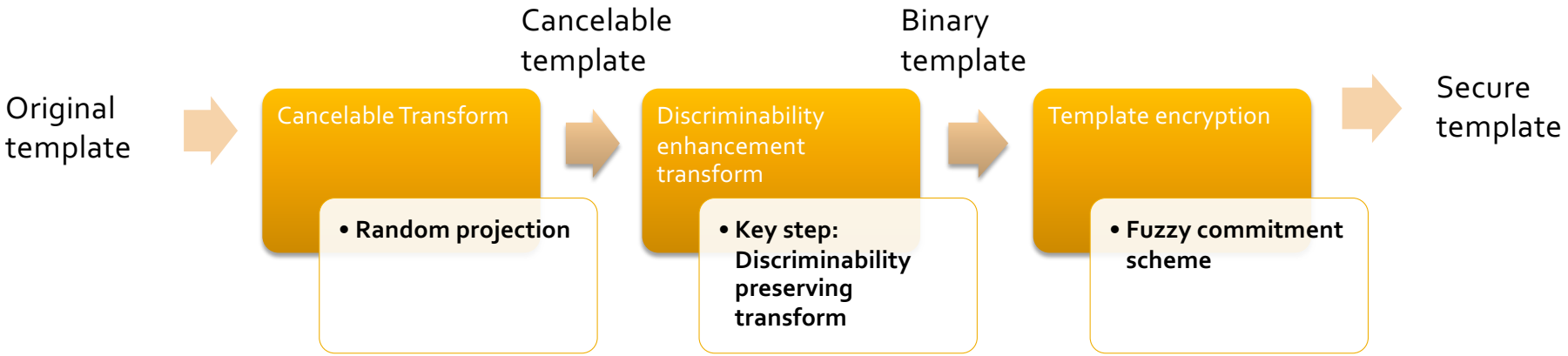
Proposed Hybrid Framework [TIFS 2010]

- One single approach cannot achieve all security, discriminability and cancelability requirements
- A three-step hybrid approach: transformation-based biometric cryptosystem



3-step Algorithm

- The three-step hybrid algorithm



- The discriminability preserving transform should
  - Convert the cancelable template into binary template
  - Preserve the discriminability via transform.

Experimental Results

- Experiment settings:
  - Database:

c : No. of individuals.
m: No. of samples for each individual.
q : No. of training samples per individual

CMU PIE

FERET

FRGC

Database	c	m	q	Variations
CMU PIE	68	105	10	Illumination, pose, expression
FERET	250	4	2	Mild expression, illumination
FRGC	350	40	5	expression, illumination, mild pose

Experimental Results

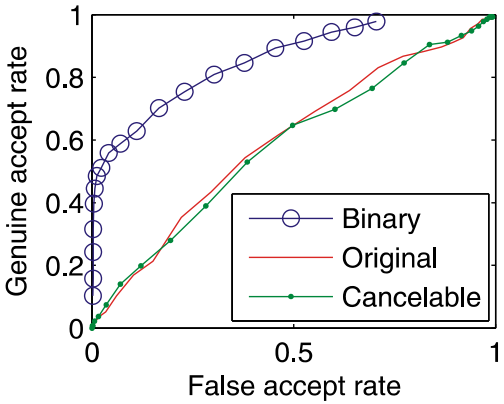
- Experiment settings
  - Fisherface [Belhumeur *et al.* PAMI 1997] applied for feature extraction
  - Experiments
    - Template discriminability
    - Recognition accuracy
    - Cancelability

Template Discriminability

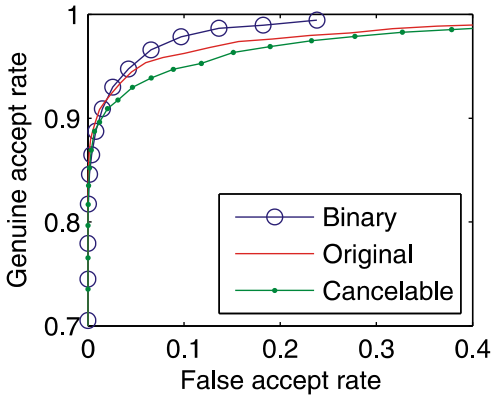
- Experimental settings
  - Choose three subsets from the CMU PIE database for experiments.
  - kr: length of the cancelable templates
  - kc: length of the binary templates

Database	c	m	q	kr	kc	Variations
CMU PIE-1	68	4	2	40	56	Pose
CMU PIE-2	250	21	4	40	84	Illumination
CMU PIE-3	350	105	10	40	210	Pose & illumination

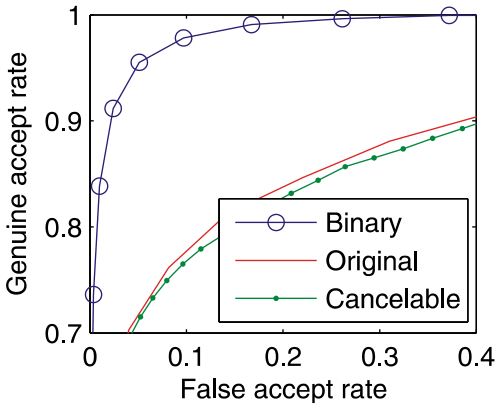
Template Discriminability



(a) Pose



(b) Illumination



(c) Pose &Illumination

- Observations
  - Overlapping rate increased: Cancelable templates lightly degrade some discriminability
  - Overlapping rate significantly decreased: binary templates enhance discriminability.
  - The recognition performance conforms it.

Recognition Accuracy

- Experimental settings
  - CMU PIE, FERET, FRGC databases used.

Database	c	m	q	kr	kc
CMU PIE	68	105	10	40	120, 150, 180, 210
FERET	250	4	2	150	120, 150, 180, 210
FRGC	350	40	5	250	150, 200, 250, 350

- Implement authentication with different kc. And comparing the performance with the
  - Original fisherface algorithm ("Original")
  - Random multispace quantization scheme ("RMQ-S") [Teoh *et al*. PAMI 2006]

Recognition Accuracy

- In the transformed-based scheme (random projection), keys can be issued in two ways.

- Experiments are done in two scenarios
  - Common key scenario ("SRC")
  - User-specified key scenario ("DRC")

Common-key Scenario

- Observation
  - The proposed hybrid algorithm outperforms the original fisherface and the RMQ algorithm

EER(%)	Fisherface	*kc*-1	*kc*-2	*kc*-3	*kc*-4	RMQ
CMU PIE	18.18	7.61	7.30	6.95	6.81	11.93
FERET	12.58	9.52	8.86	8.61	8.55	12.83
FRGC	31.75	17.93	17.40	16.70	16.68	21.87

kc: length of the binary templates

User-specified Key Scenario

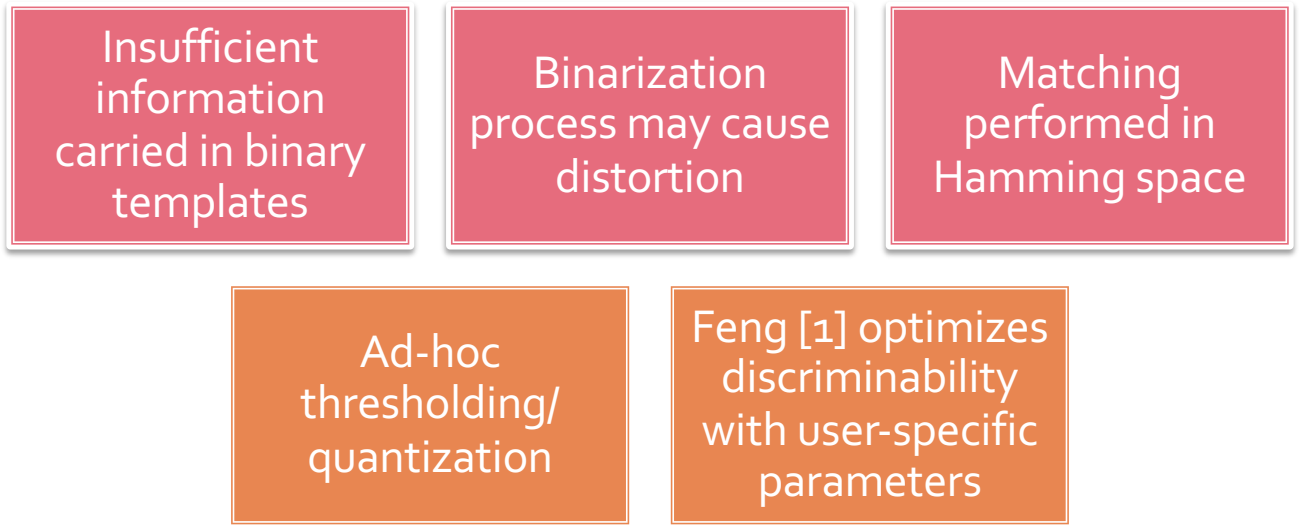
- Observation
  - The proposed hybrid algorithm outperforms the original fisherface and the RMQ algorithm

EER(%)	Fisherface	*kc*-1	*kc*-2	*kc*-3	*kc*-4	RMQ
CMU PIE	18.18	9.41	8.41	8.70	8.26	11.68
FERET	21.66	3.38	3.36	3.34	3.62	4.49
FRGC	31.75	9.03	9.18	9.08	9.13	11.03

kc: length of the binary templates

Binary Template Generation [TIFS 2012]

- The discriminability of the binary templates receives little attention



Y C Feng and P C Yuen, "Binary Discriminant Analysis for Generating Binary Face Template ," *IEEE Transactions on Information Forensics and Security (TIFS), vol.* 7, no. 2, pp.613-624, 2012.

Background

- Existing schemes lack of discriminability evaluations of the binary templates
- Traditional discriminability optimization methods are not effective
  - Employ differentiation
  - Differentiation is not feasible in Hamming space
- Propose a **binary discriminant analysis (BDA)** to optimize the discriminability of the binary templates

Rationale

- Use a series of linear discriminant functions (LDF) to form a binary template $\mathrm{b}=(b_1,b_2\ldots b_i\ldots b_k)$ from input sample x.

$$b_i(x) = \begin{cases} 0 \text{ if } & w_i^T x + t_i > 0 \\ & 1 \text{ if else} \end{cases}$$

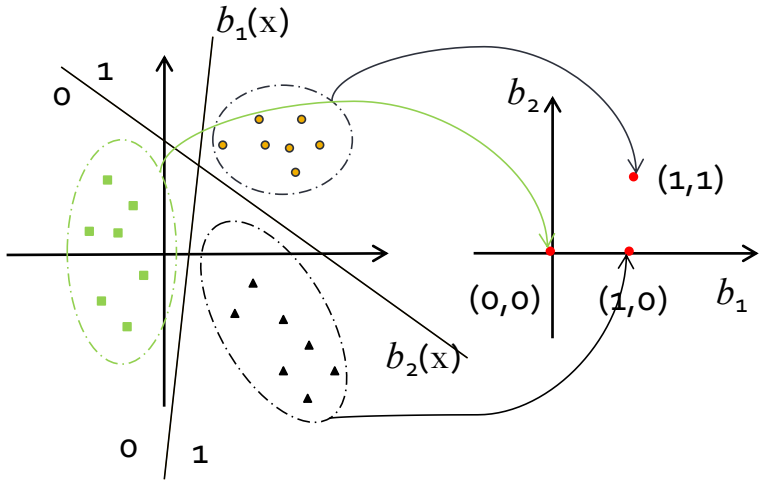
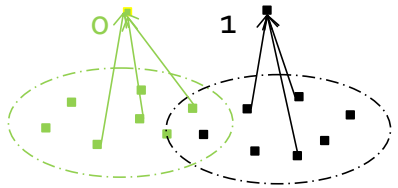


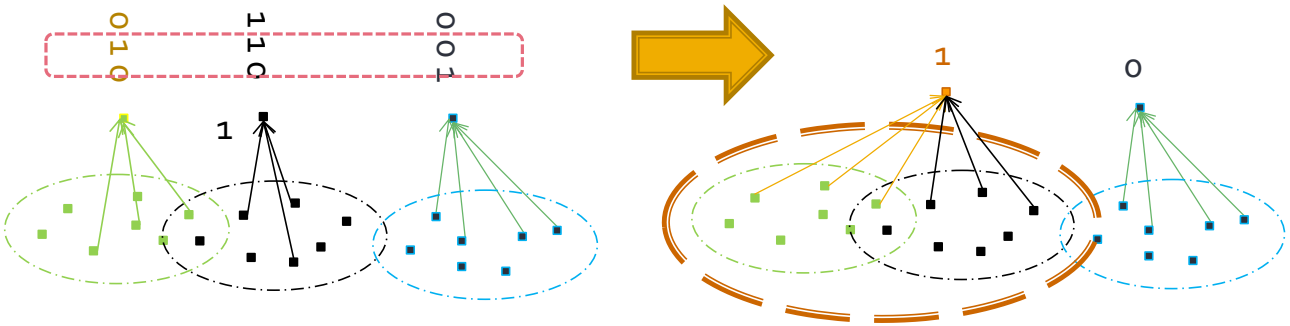
Illustration in 2-D space

Rationale

- Inspired by perceptron
  - Find a LDF to classify two classes

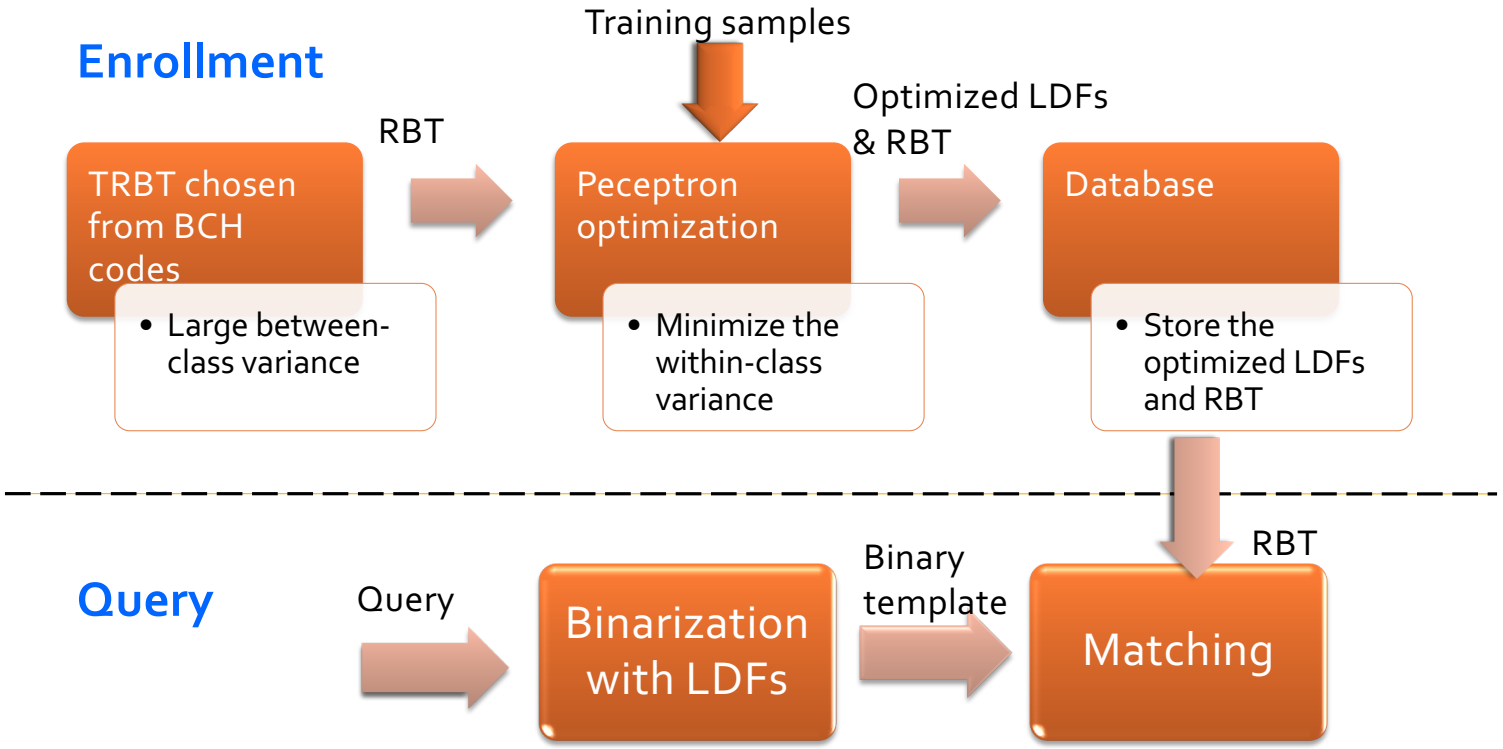


  - Construct a continuous perceptron criteria function to find optimal (w , t)
    - Can be extended to multiple classes with labels of multiple bits, just like binarization



Detailed Algorithm

- The whole procedure of the algorithm



Experimental Results

- Experiment settings

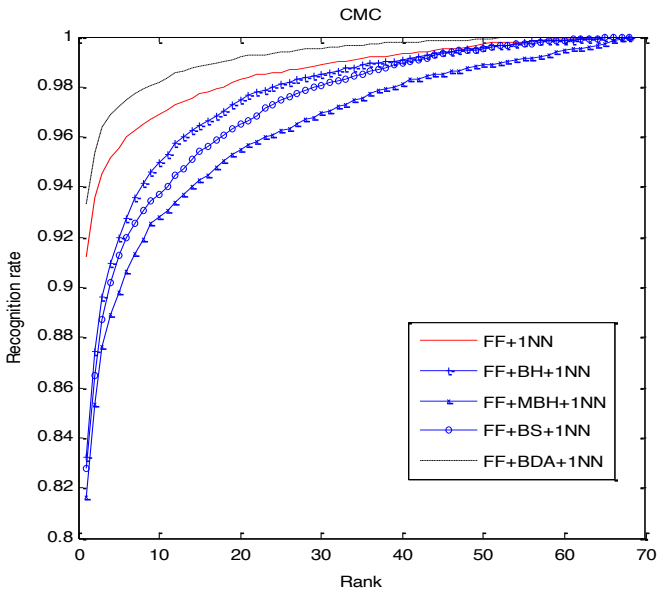
CMU PIE

FRGC

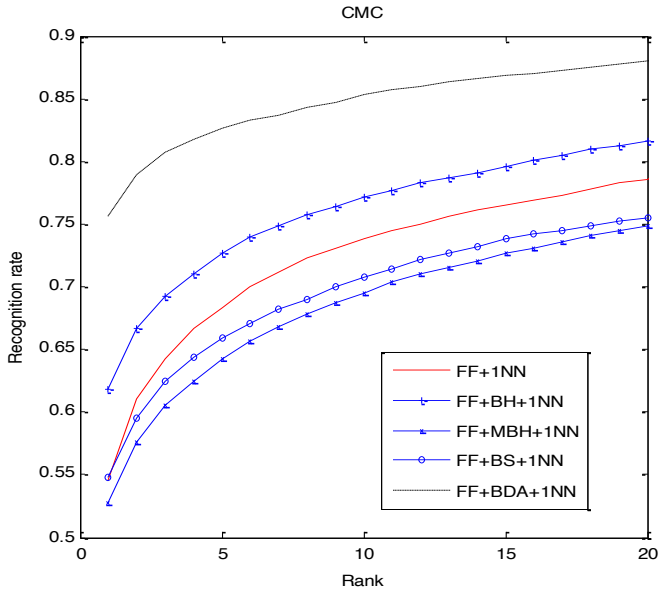
c : No. of individuals.
N_p: No. of samples for each individual.
N_t : No. of training samples per individual

Database	c	N_p	N_t	Variations
CMU PIE	68	105	10	Illumination, pose, expression
FRGC	350	40	5	expression, illumination, mild pose

Experimental Results

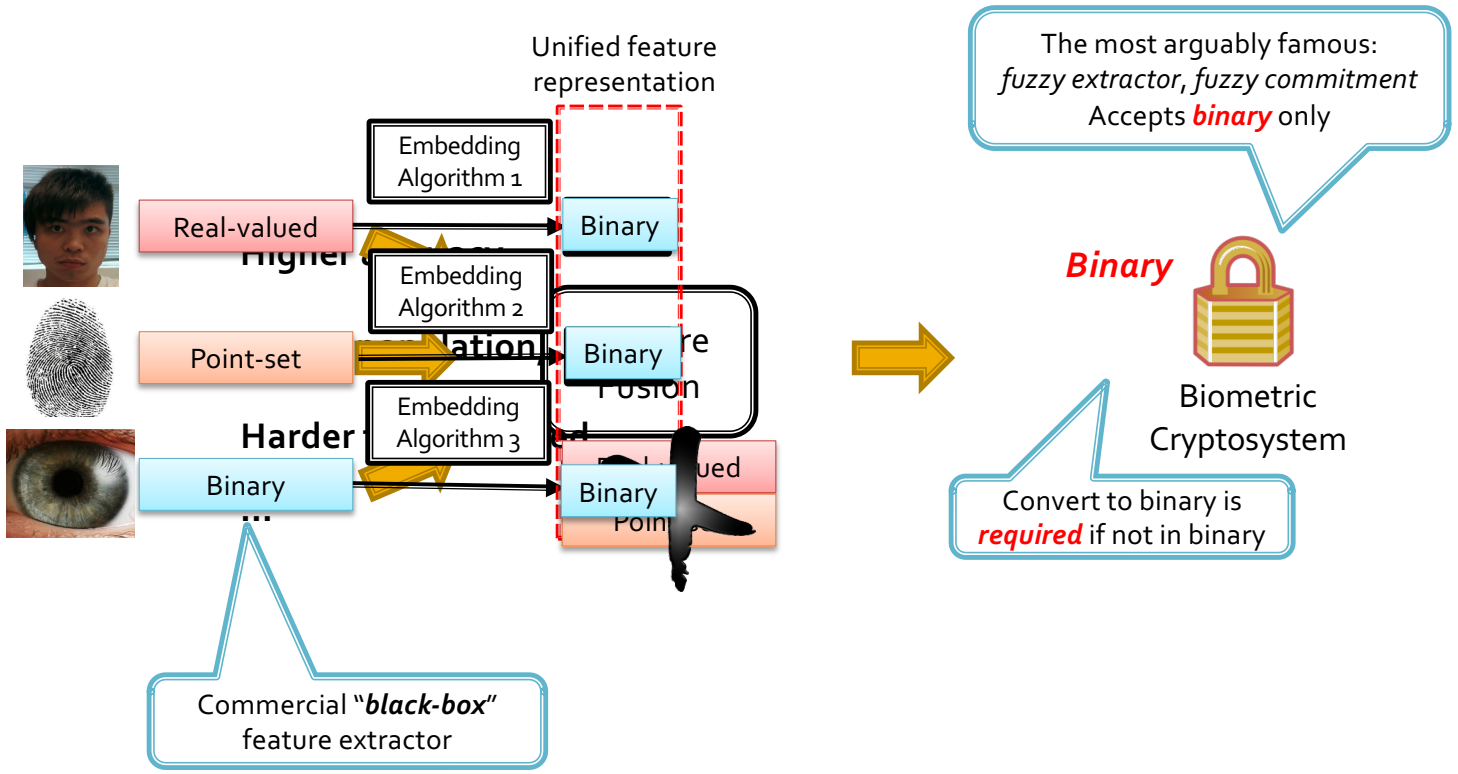


(a) CMU PIE



(b) FRGC

Binary Template Fusion for Multi-biometric Cryptosystem [IVC 2017]

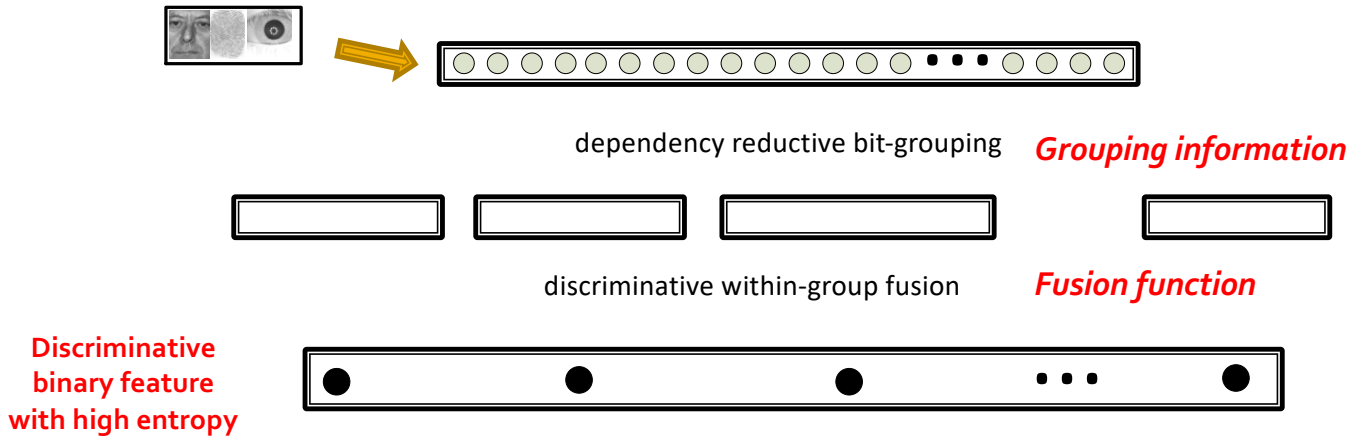


Criteria for Binary Template Fusion

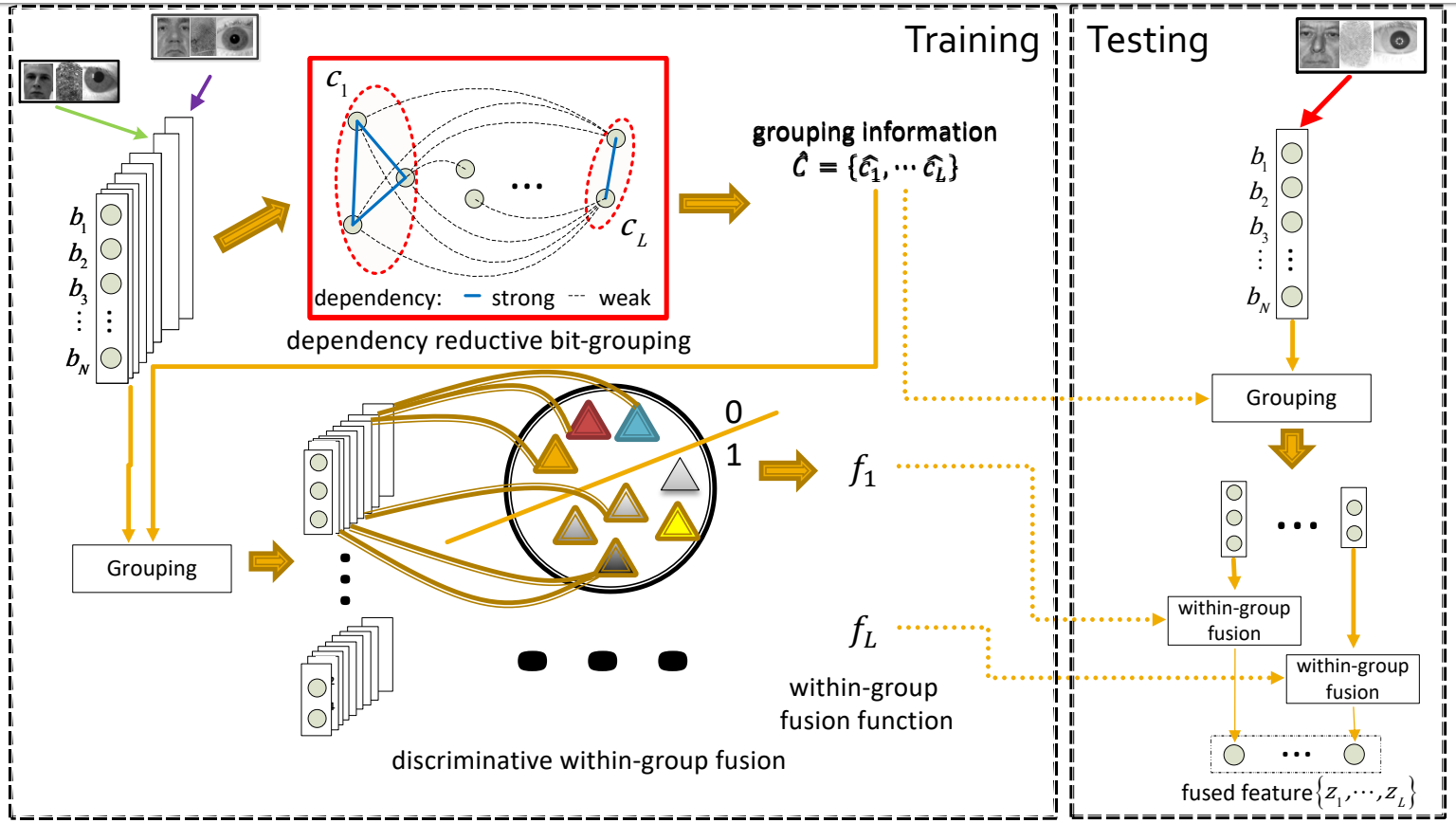
- Discriminability
  - Small intra-user variations ***of*** feature bits
  - Large inter-user variations ***of*** feature bits
- Security (high-entropy)
  - Low dependency ***among*** bits
  - High uniformity ***of*** feature bits
- Privacy
  - No information leakage from helper data

Proposed Binary Template Fusion

- Stage one: dependency-reductive bit grouping
  - Dependency among bits (**security**)
- Stage two: discriminative within-group fusion
  - Bit-uniformity (**security**), intra-user variations (**discriminability**), inter-user variations (**discriminability**)



Proposed Binary Template Fusion

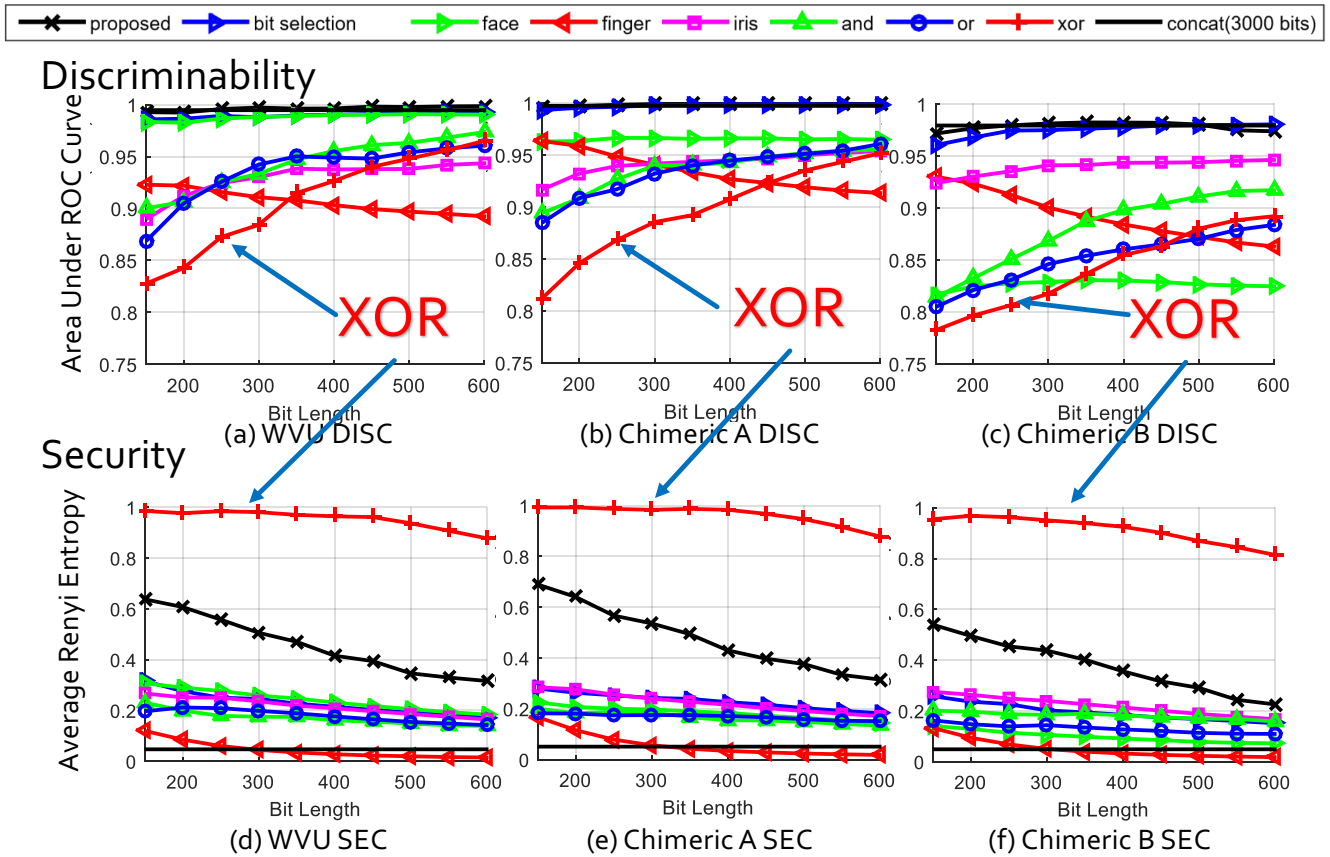


Experiments

- Evaluation
  - Discriminability (Area under ROC curve)
  - Security (average Renyi entropy, Hidano et al. BIOSIG2012)
- Experimental setting

Multimodal Database	WVU	Chimeric A (FVC2000DB2 + FERET + CASIA)	Chimeric B (FVC2002DB2 + FRGC + ICE2006)
Subjects	106	100	100
Training Sample	3	4	4
Testing Sample	2	4	4

Experimental Results



- Related work:

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

Conclusion

- 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 Template Protection)

1. 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
2. G. Mai, M H Lim and P C Yuen, "Binary Feature Fusion for Discriminative and Secure Multi-biometric Cryptosystems", *Image and Vision Computing*, 2016
3. M H Lim and P C Yuen, "Entropy Measurement for Biometric Verification Systems", *IEEE Transactions on Cybernetics*, 2016
4. 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
5. 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
6. YC Feng & PC Yuen, "Binary discriminant analysis for generating binary face template", *IEEE Transactions on Information Forensics and Security*, 2012
7. YC Feng, PC Yuen, AK Jain, "A hybrid approach for generating secure and discriminating face template", *IEEE Transactions on Information Forensics and Security*, 2010

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. "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 (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, 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 (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.