BTAS 2019

Session II: Deep Learning Approaches for Face Anti-spoofing

Host: Yaojie Liu

MICHIGAN STATE UNIVERSITY

Computer Vision Lab

Outline

- Vanilla CNNs
- Patch-based CNN methods
- CNN methods with auxiliary supervisions
- GAN-based noise modeling
- Data augmentation

Outline

BTAS 2019

- **Vanilla CNN**
- Patch-based CNN methods
- CNN methods with auxiliary supervisions
- GAN-based noise modeling
- Data Augmentation

Vanilla CNNs

BTAS 2019

CNN is trained to do a binary classification: live vs spoof

Live Face

Presentation Attack

0

1

Binary Supervision

Vanilla CNNs

BTAS 2019

Learn Convolutional Neural Network for Face Anti-Spoofing, ArXiv, 2014

Learning temporal features using LSTM-CNN architecture for face anti-spoofing, ACPR, 2015

Integration of image quality and motion cues for face anti-spoofing: A neural network approach, JVCI, 2016

An Original Face Anti-spoofing Approach using Partial Convolutional Neural Network, IPTA, 2016

Cross-database face antispoofing with robust feature representation. CCBR, 2016

Vanilla CNNs

BTAS 2019

Learn Convolutional Neural Network for Face Anti-Spoofing, ArXiv, 2014

Learning temporal features using LSTM-CNN architecture for face anti-spoofing, ACPR, 2015

Integration of image quality and motion cues for face anti-spoofing: A neural network approach, JVCI, 2016

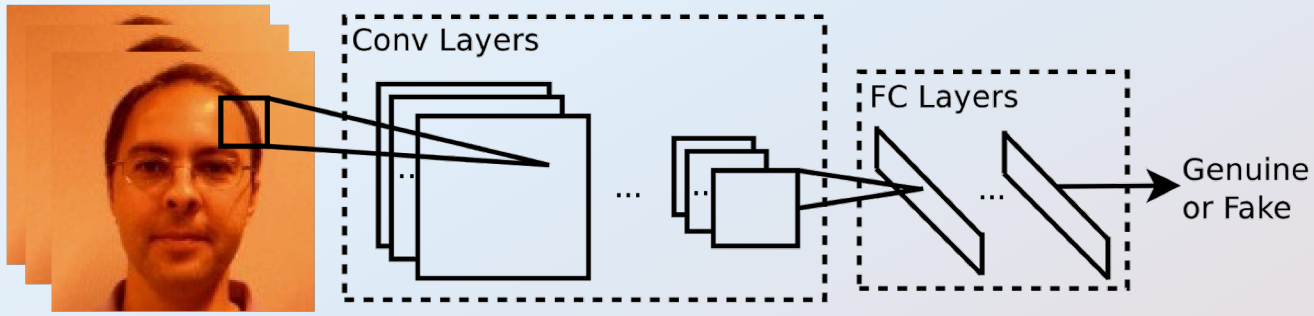
An Original Face Anti-spoofing Approach using Partial Convolutional Neural Network, IPTA, 2016

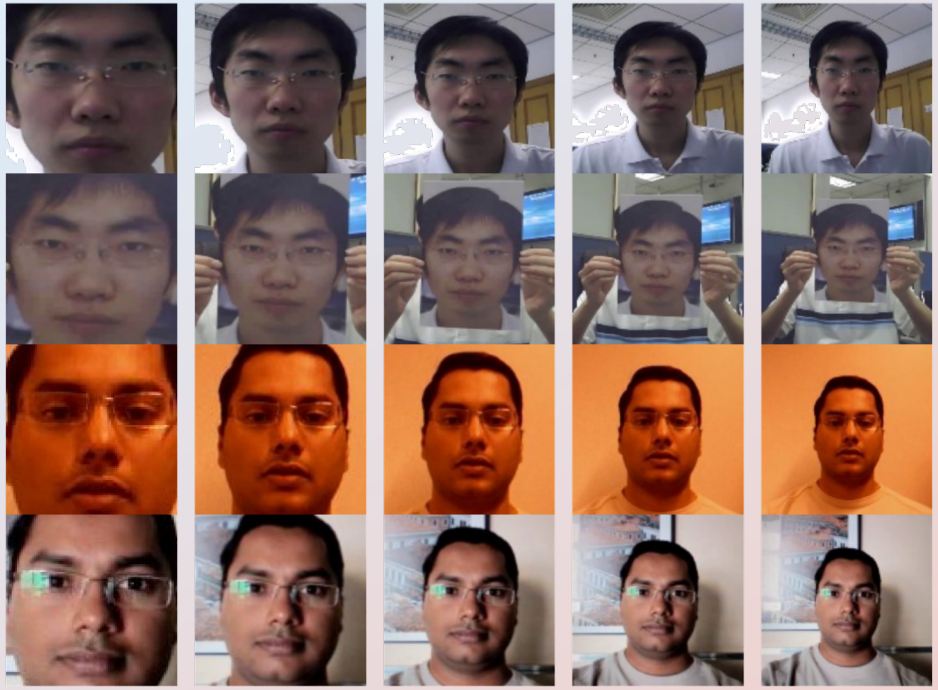
Cross-database face antispoofing with robust feature representation. CCBR, 2016

Learn Convolutional Neural Network for Face Anti-spoofing

BTAS 2019

- CNN feature + SVM classifier
- Examine the influence of face scale





Yang et. al., Learn Convolutional Neural Network for Face Anti-Spoofing. arXiv 2014.

Conclusion of Face Scales

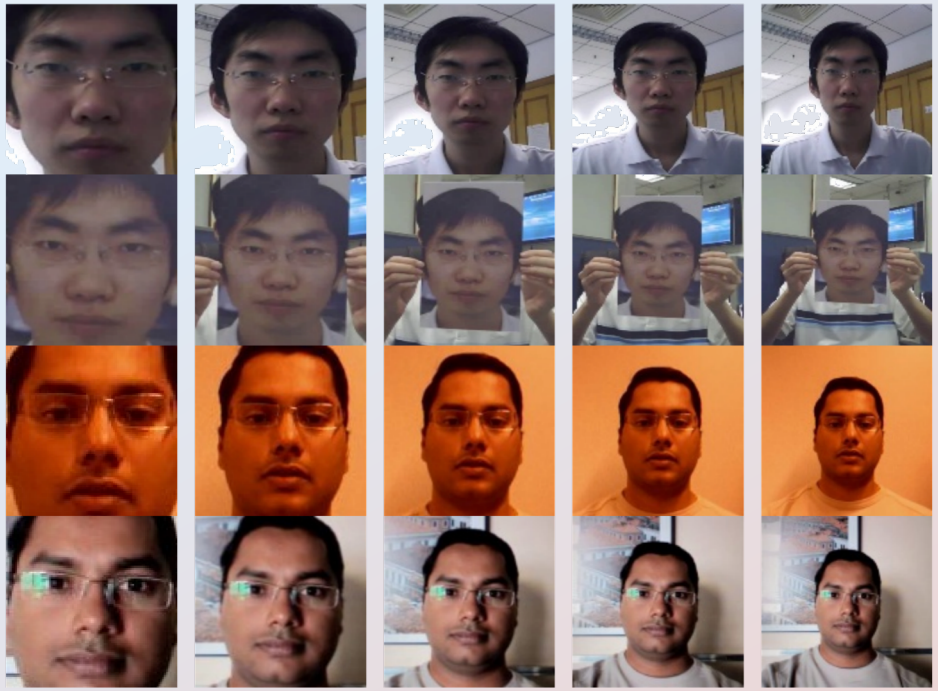
BTAS 2019

- Too small: very limited information

  →worse performance

- Too big: too much information → worse performance

- Varies from case to case
  - CASIA is best at medium res.
  - Replay is best at the largest res.

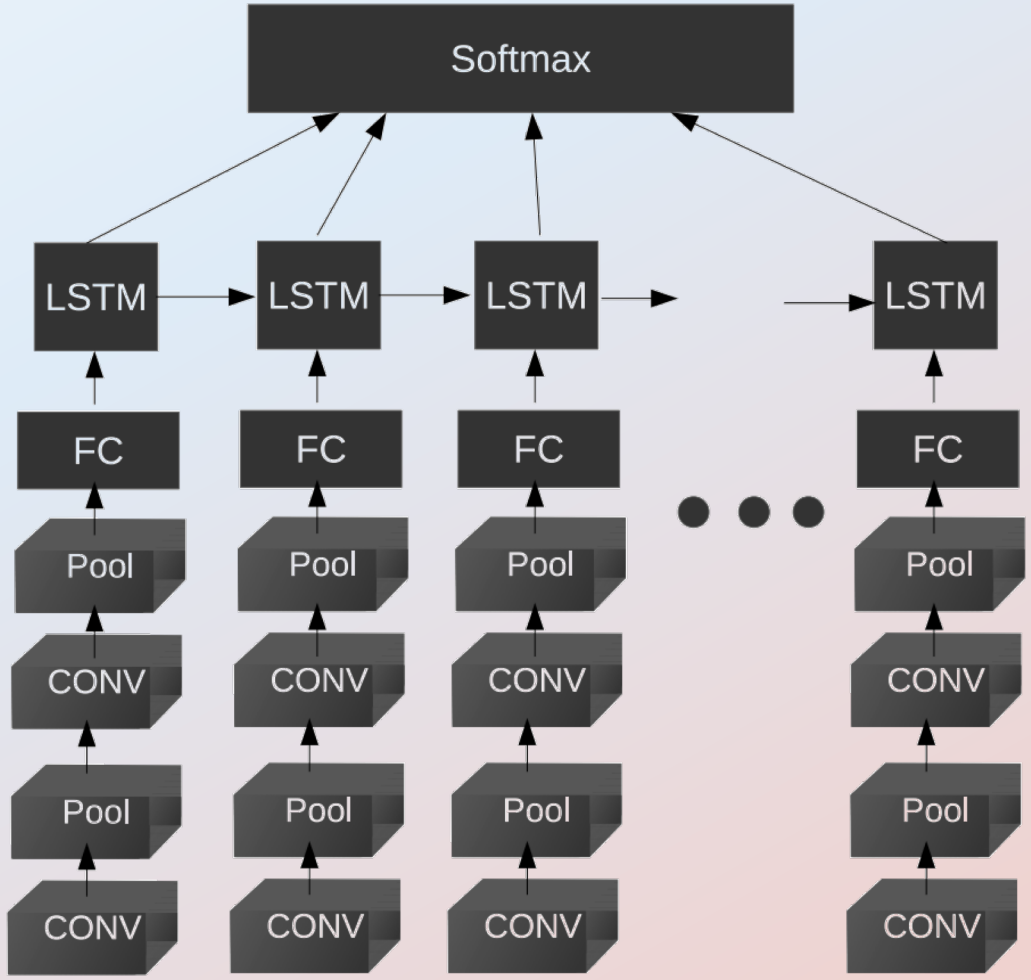


Yang et. al., Learn Convolutional Neural Network for Face Anti-Spoofing. arXiv 2014.

Learning Temporal Features using LSTM-CNN Architecture for Face Anti-spoofing

BTAS 2019

- CNN + LSTM
- Consider temporal information

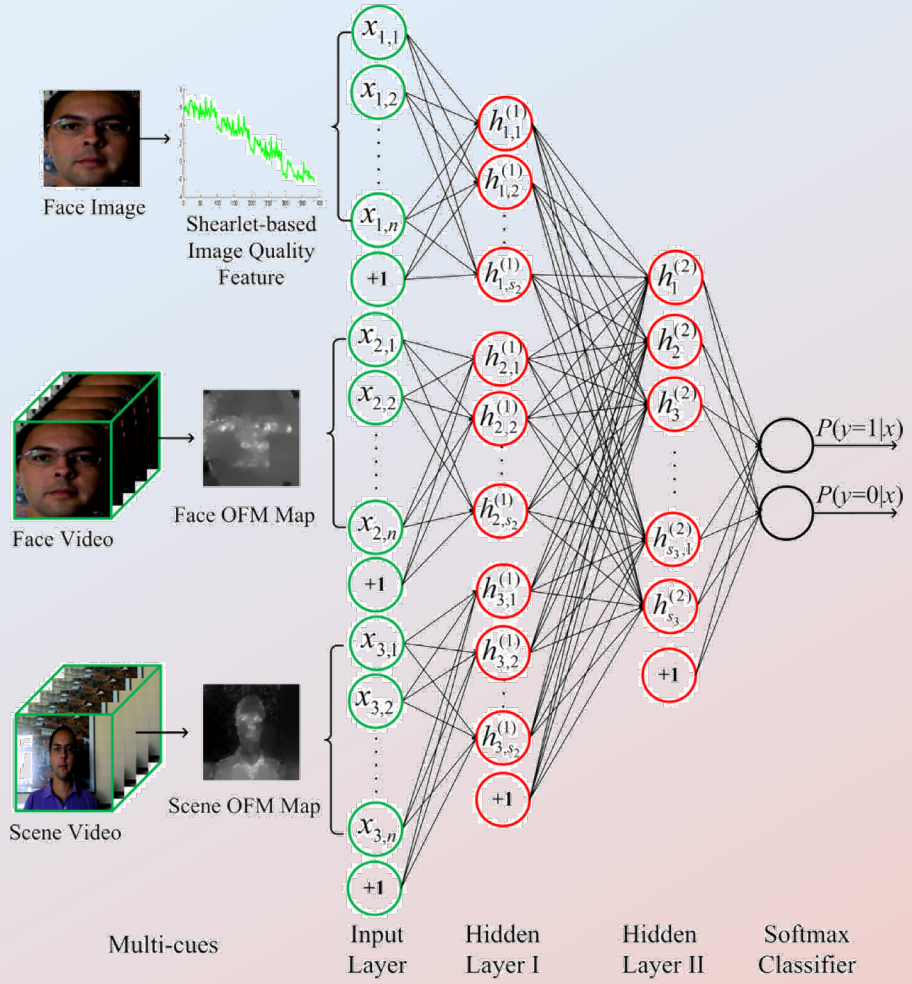


Xu et. al., Learning temporal features using LSTM-CNN architecture for face anti-spoofing. ACPR 2015.

Integration of Image Quality and Motion Cues for Face Anti-spoofing: A Neural Network Approach

BTAS 2019

- Use handcrafted features as input
  - Shearlet-based image quality
  - Face optical flow
  - Scene optical flow



Feng et. al., Integration of image quality and motion cues for face anti-spoofing: A neural network approach. JVCI 2016.

Experiment Results

BTAS 2019

CASIA Dataset	EER	HTER
Color LBP[1]	6.2	-
CNN + SVM[2]	-	6.25
CNN + LSTM[3]	-	5.93
Multi-cue CNN[4]	5.83	-

Replay Dataset	EER	HTER
Color LBP[1]	0.4	2.9
CNN + SVM[2]	-	2.68
CNN + LSTM[3]	-	-
Multi-cue CNN[4]	-	0

[1] Boulkenafet et. al., Face antispoofing based on color texture analysis. ICIP 2015
[2] Yang et. al., Learn Convolutional Neural Network for Face Anti-Spoofing. arXiv 2014.
[3] Xu et. al., Learning temporal features using LSTM-CNN architecture for face anti-spoofing. ACPR 2015.
[4] Feng et. al., Integration of image quality and motion cues for face anti-spoofing: A neural network approach. JVCI 2016.

Summary

BTAS 2019

- Fusing inputs (scale, handcrafted features, etc.) can help
- Improve the overall performance compared to non-CNN methods
- Binary classifier might lead to overfitting

Outline

BTAS 2019

- Vanilla CNNs
- **Patch-based CNN methods**
- CNN methods with auxiliary supervisions
- GAN-based noise modeling
- Data Augmentation

Patch-based CNNs

BTAS 2019

Face Anti-Spoofing Using Patch and Depth-Based CNNs, IJCB, 2017

On the Learning of Deep Local Features for Robust Face Spoofing Detection, SIBGRAPI, 2018

Face Anti-Spoofing: Model Matters, So Does Data, CVPR, 2019

Patch-based CNNs

BTAS 2019

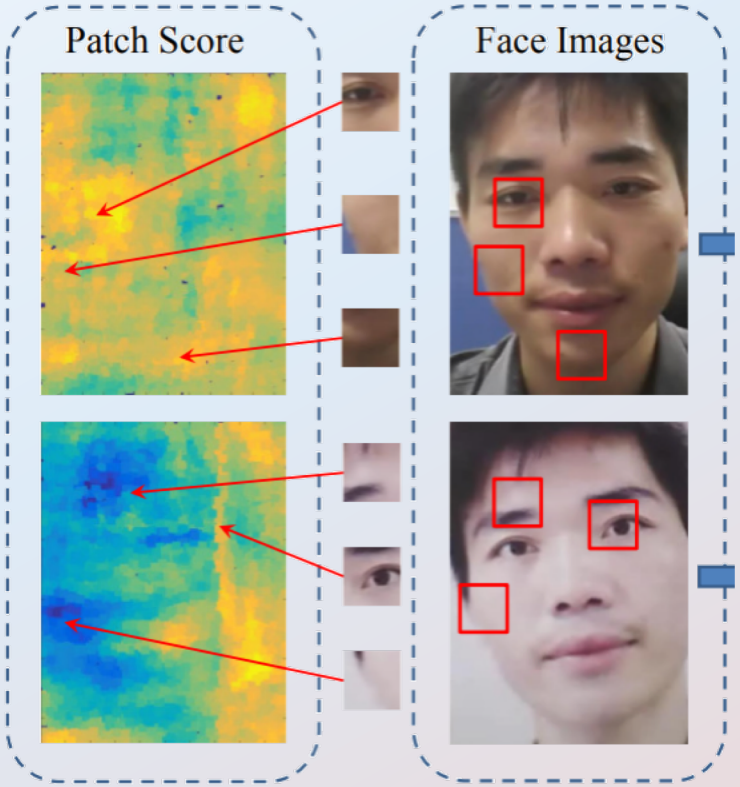
Face Anti-Spoofing Using Patch and Depth-Based CNNs, IJCB, 2017

On the Learning of Deep Local Features for Robust Face Spoofing Detection, SIBGRAPI, 2018

Face Anti-Spoofing: Model Matters, So Does Data, CVPR, 2019

Motivation

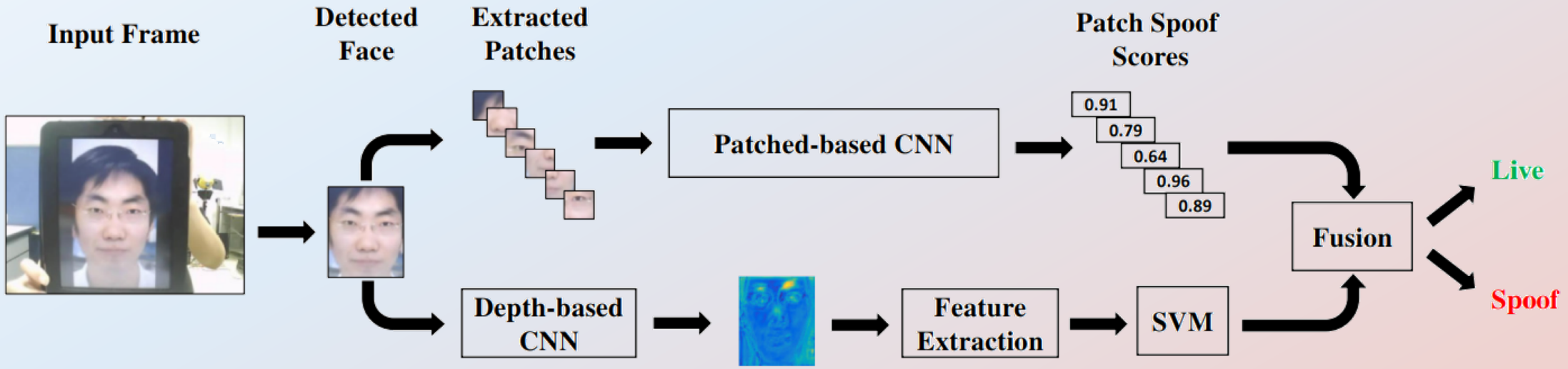
- Prevent overfitting
  - Increase the number of training samples



Yousef Atoum, Yaojie Liu, Amin Jourabloo, and Xiaoming Liu, Face anti-spoofing using patch and depth-based CNNs. IJCB 2017.

Patch CNN

- Input face: RGB+HSV, patch size 96*96
- Patch CNN: classify each patch as a live or spoof patch
- Fuse the score by average



Yousef Atoum, Yaojie Liu, Amin Jourabloo, and Xiaoming Liu, Face anti-spoofing using patch and depth-based CNNs. IJCB 2017.

Experiment Results

BTAS 2019

CASIA Dataset	EER	HTER
Color LBP[1]	6.2	-
CNN + SVM[2]	-	6.25
CNN + LSTM[3]	-	5.93
Multi-cue CNN[4]	5.83	-
Patch CNN + Depth CNN[5]	2.67	2.27

Replay Dataset	EER	HTER
Color LBP[1]	0.4	2.9
CNN + SVM[2]	-	2.68
CNN + LSTM[3]	-	-
Multi-cue CNN[4]	-	0
Patch CNN + Depth CNN[5]*	0.79	0.72

* Only use tight cropped face

[1] Boulkenafet et. al., Face antispoofing based on color texture analysis. ICIP 2015
[2] Yang et. al., Learn Convolutional Neural Network for Face Anti-Spoofing. arXiv 2014.
[3] Xu et. al., Learning temporal features using LSTM-CNN architecture for face anti-spoofing. ACPR 2015.
[4] Feng et. al., Integration of image quality and motion cues for face anti-spoofing: A neural network approach. JVCI 2016.
[5] Yousef Atoum, Yaojie Liu, Amin Jourabloo, and Xiaoming Liu, Face anti-spoofing using patch and depth-based CNNs. IJCB 2017.

Patch-based CNNs

BTAS 2019

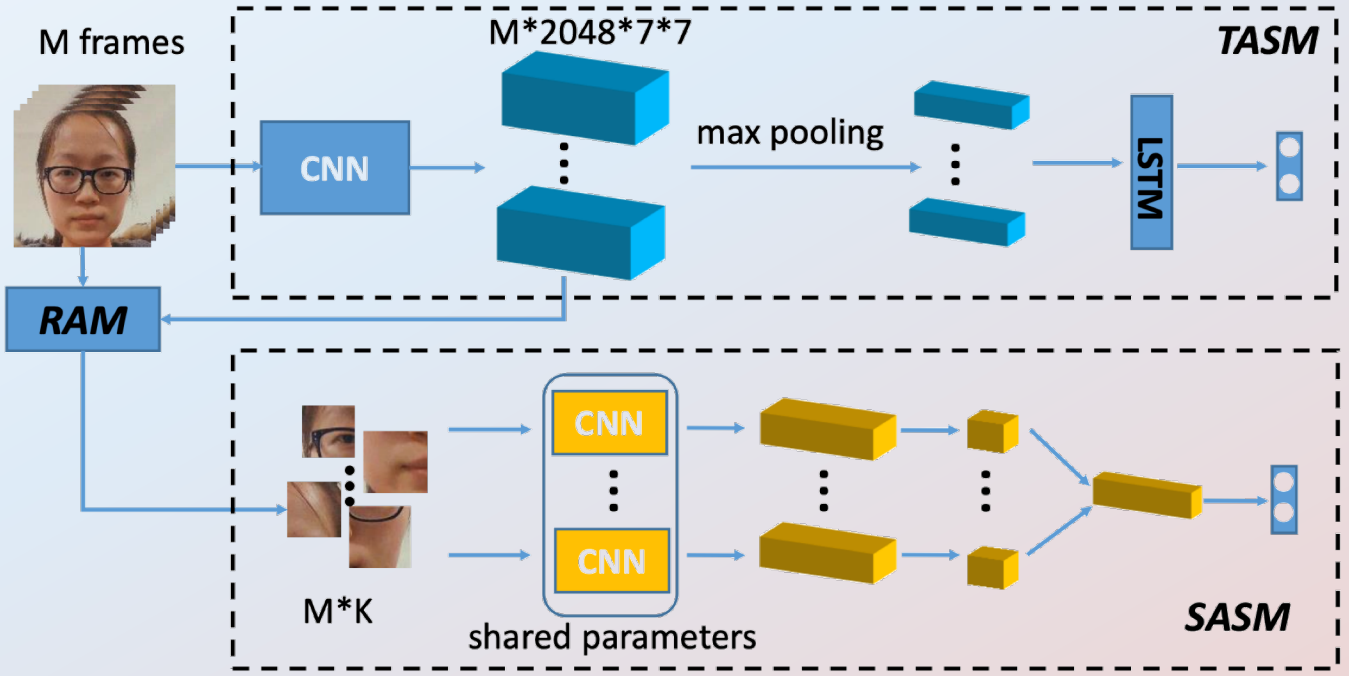
Face Anti-Spoofing Using Patch and Depth-Based CNNs, IJCB, 2017

On the Learning of Deep Local Features for Robust Face Spoofing Detection, SIBGRAPI, 2018

Face Anti-Spoofing: Model Matters, So Does Data, CVPR, 2019

STASN

- Temporal Anti-Spoofing Module (TASM): conv-LSTM
- Region Attention Module (RAM): locating the discriminative and significant sub-regions
- Spatial Anti-Spoofing Module (SASM): patch CNN



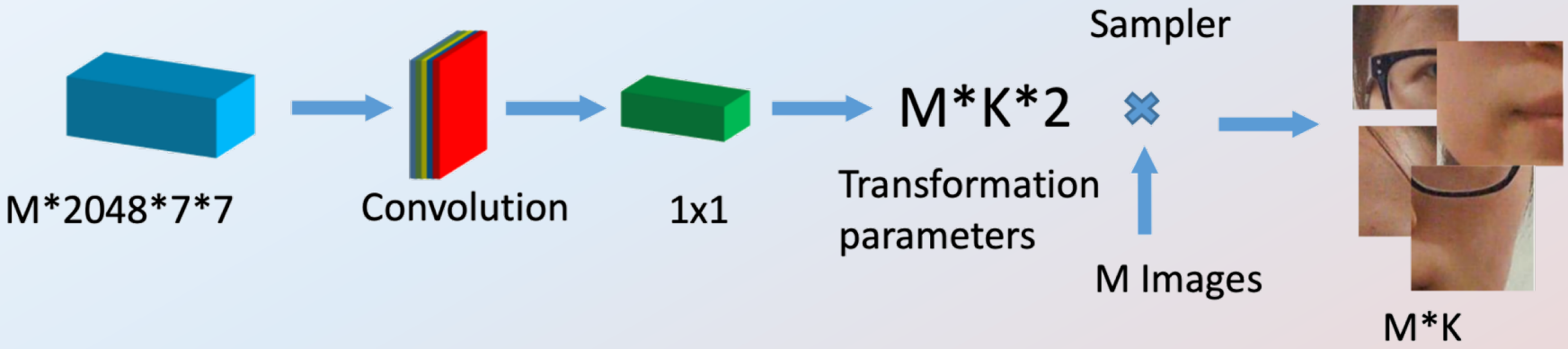
Yang et. al., Face Anti-Spoofing: Model Matters, So Does Data, CVPR 2019

Region Attention Module (RAM)

BTAS 2019

Locates the discriminative and significant sub-regions

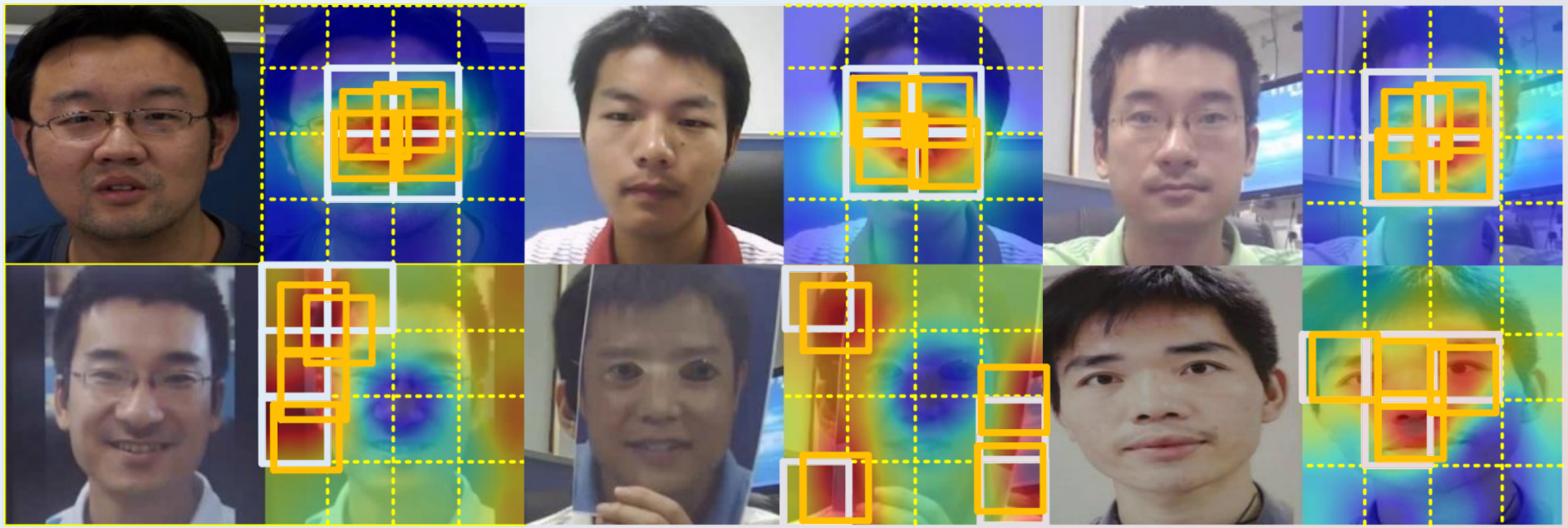
- RAM output 2*K parameters: offsets and translation of K patches



Yang et. al., Face Anti-Spoofing: Model Matters, So Does Data, CVPR 2019

Examples of Attention

- Live attentions are on face
- Spoof attentions are diverse



Yang et. al., Face Anti-Spoofing: Model Matters, So Does Data, CVPR 2019

Drawbacks

- Trade-off between efficiency and performance (more patches or less?)
- Not end-to-end training
- Patch scale

Outline

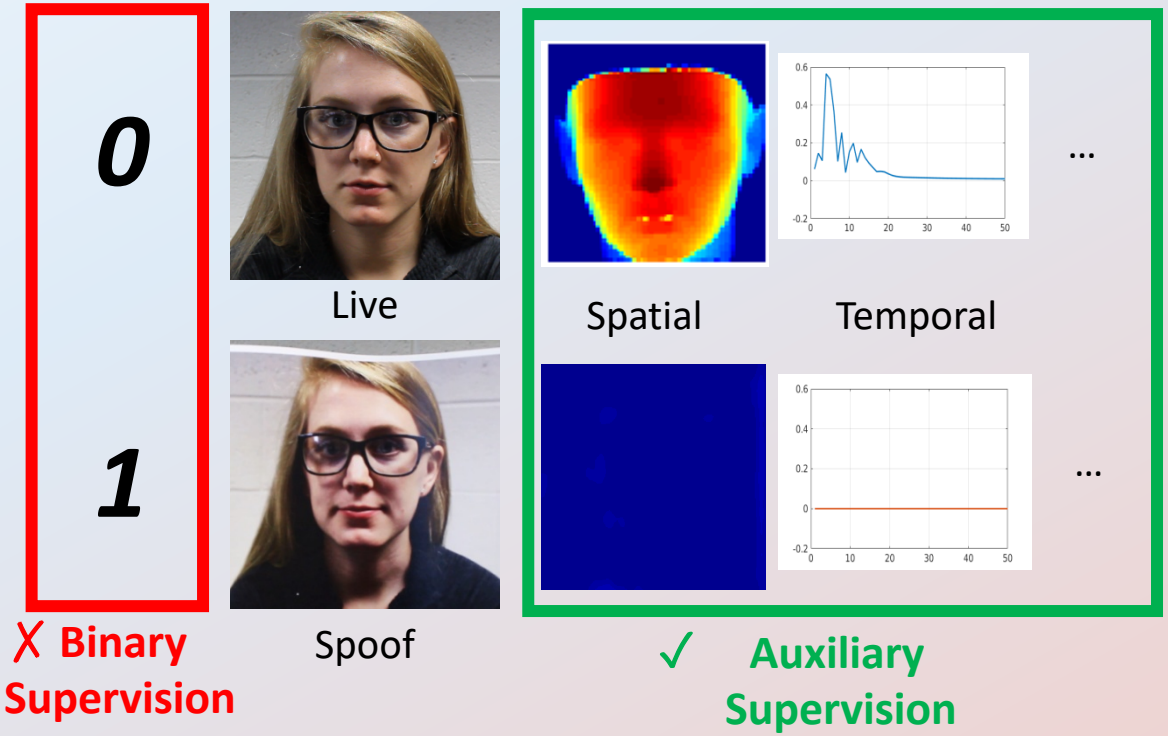
- Vanilla CNNs
- Patch-based CNN methods
- **CNN methods with auxiliary supervisions**
- GAN-based noise modeling
- Data Augmentation

CNN Methods with Auxiliary Supervisions

BTAS 2019

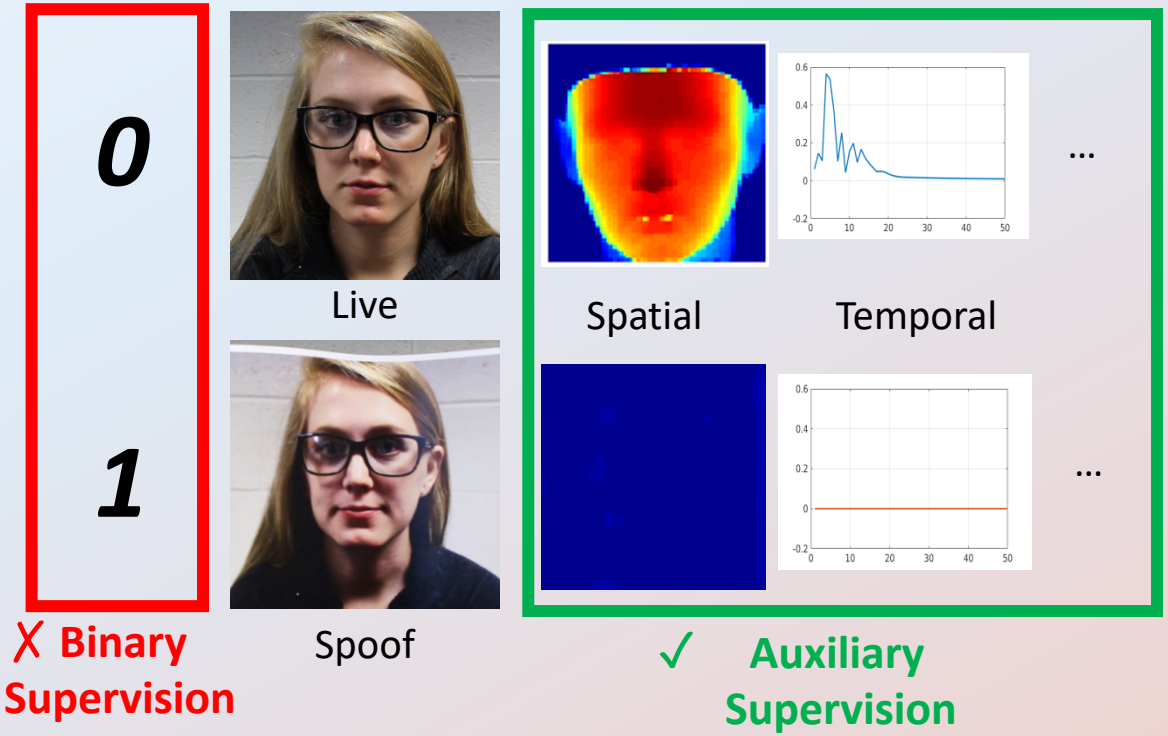
Auxiliary information: signals/biometric features with distinctive difference between live and spoof

- Depth map
- Heart beat signal (rPPG)
- Optical flow
- …



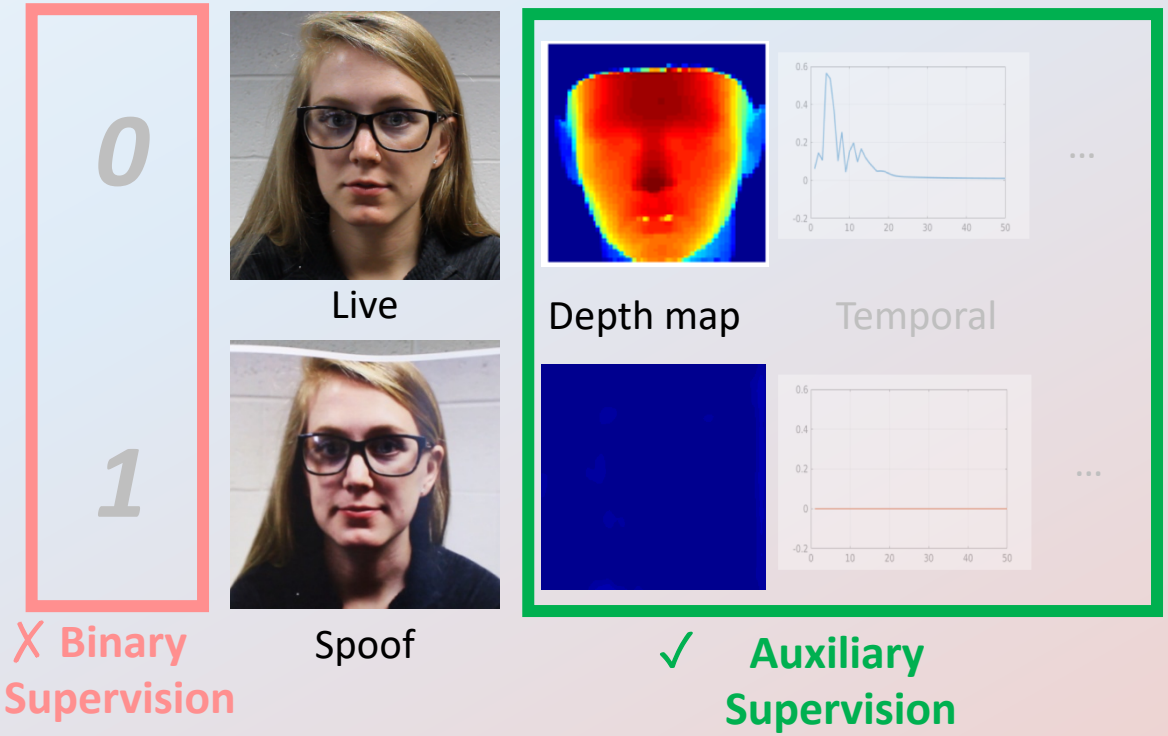
Why Auxiliary Supervision?

- Provide specific attention for CNN
- Make CNN explainable



Depth Map

- Provide specific attention for CNN
- Make CNN explainable



Methods using Depth Map

BTAS 2019

Face anti-spoofing using patch and depth-based CNNs. IJCB 2017.

Learning deep models for face anti-spoofing: binary or auxiliary supervision. *CVPR 2018.*

Face de-spoofing: anti-spoofing via noise modeling. *ECCV* 2018.

Exploiting temporal and depth information for multi-frame face anti-spoofing, arXiv 2019

Aurora guard: real-time face anti-spoofing via light reflection, arXiv 2019

Meta Anti-spoofing: Learning to Learn in Face Anti-spoofing, arXiv 2019

Multi-adversarial discriminative deep domain generalization for face presentation attack detection. CVPR 2019

Deep tree learning for zero-shot face anti-spoofing. CVPR 2019

Methods using Depth Map

BTAS 2019

Face anti-spoofing using patch and depth-based CNNs. IJCB 2017.

Learning deep models for face anti-spoofing: binary or auxiliary supervision. *CVPR 2018.*

Face de-spoofing: anti-spoofing via noise modeling. *ECCV* 2018.

Exploiting temporal and depth information for multi-frame face anti-spoofing, arXiv 2019

Aurora guard: real-time face anti-spoofing via light reflection, arXiv 2019

Meta Anti-spoofing: Learning to Learn in Face Anti-spoofing, arXiv 2019

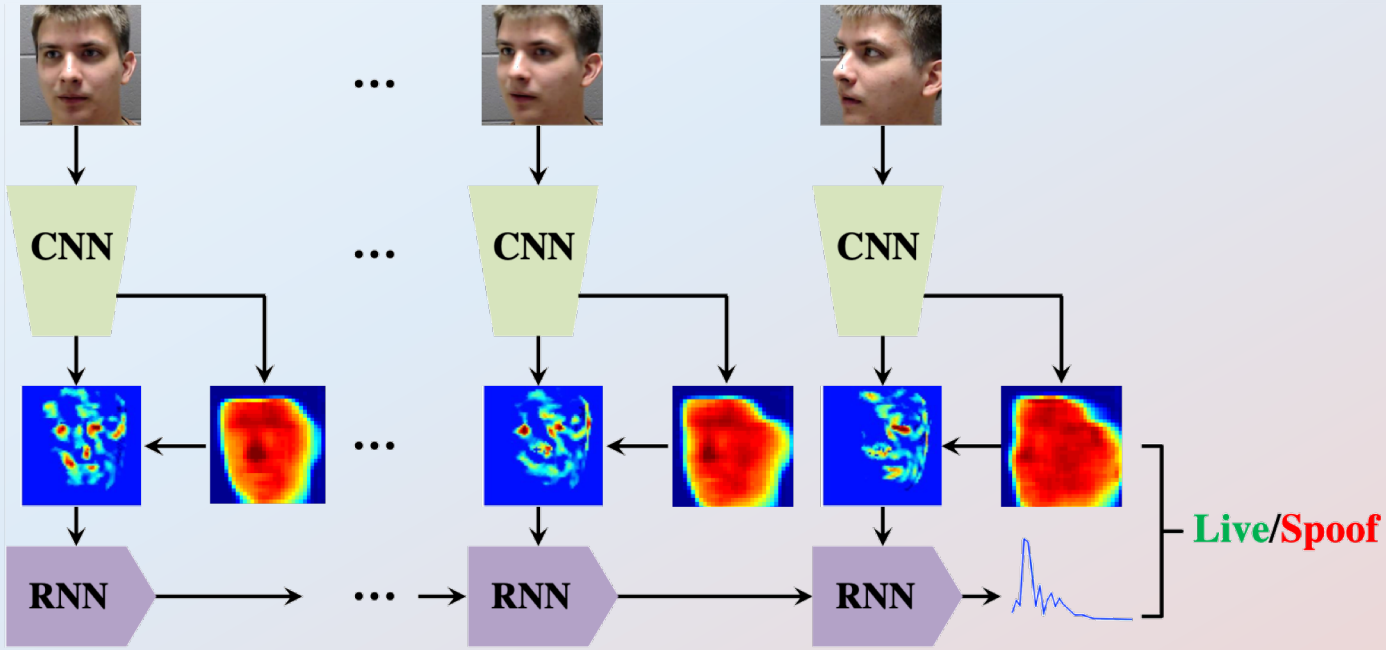
Multi-adversarial discriminative deep domain generalization for face presentation attack detection. CVPR 2019

Deep tree learning for zero-shot face anti-spoofing. CVPR 2019

…

Overall Architecture

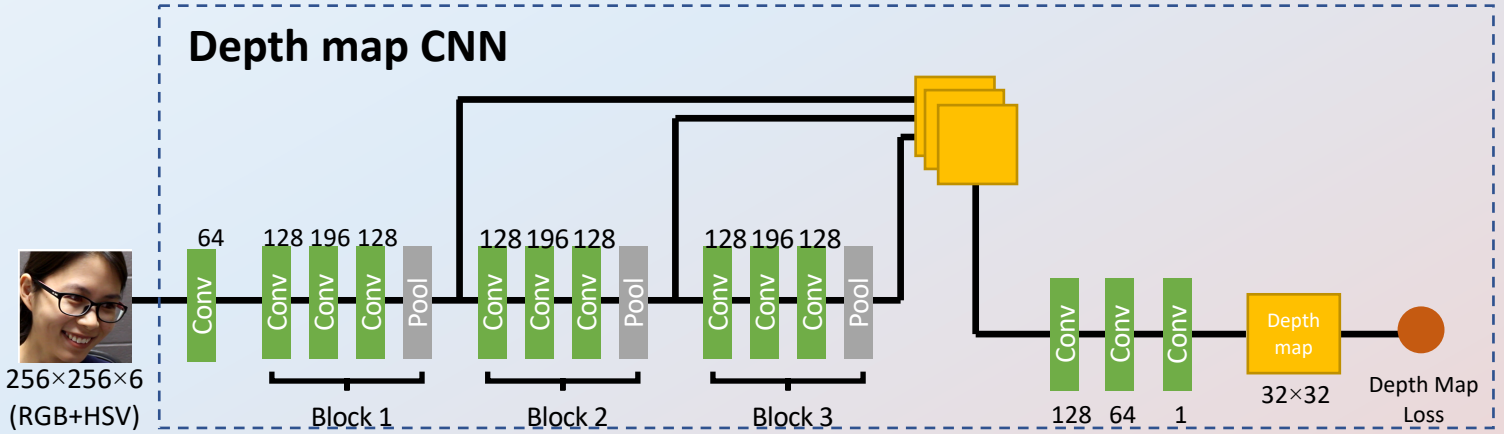
- Spatial supervision: depth map
- Temporal supervision: rPPG signal



Yaojie Liu, Amin Jourabloo, and Xiaoming Liu. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. *CVPR 2018.*

Depth Map CNN

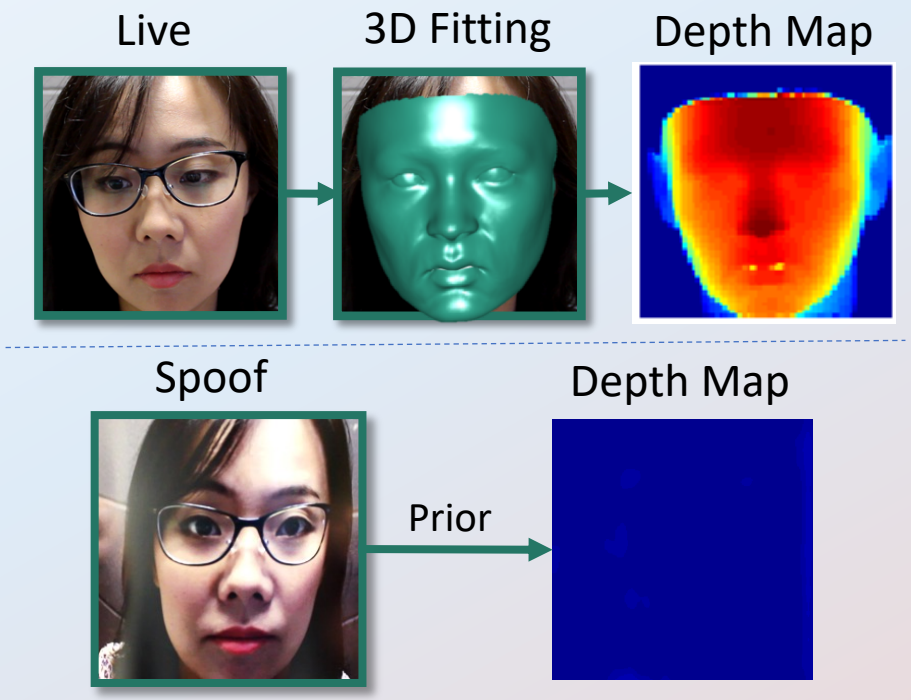
- RGB+HSV as input
- Fully convolutional network
- Short-cut connection to fuse multi-scale features
- Depth map regression loss: $\mathcal{L}_{depth} = \left\| D_{pred} - D_0 \right\|_F^1$



Yaojie Liu, Amin Jourabloo, and Xiaoming Liu. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. *CVPR 2018.*

How to Obtain Depth Map Label?

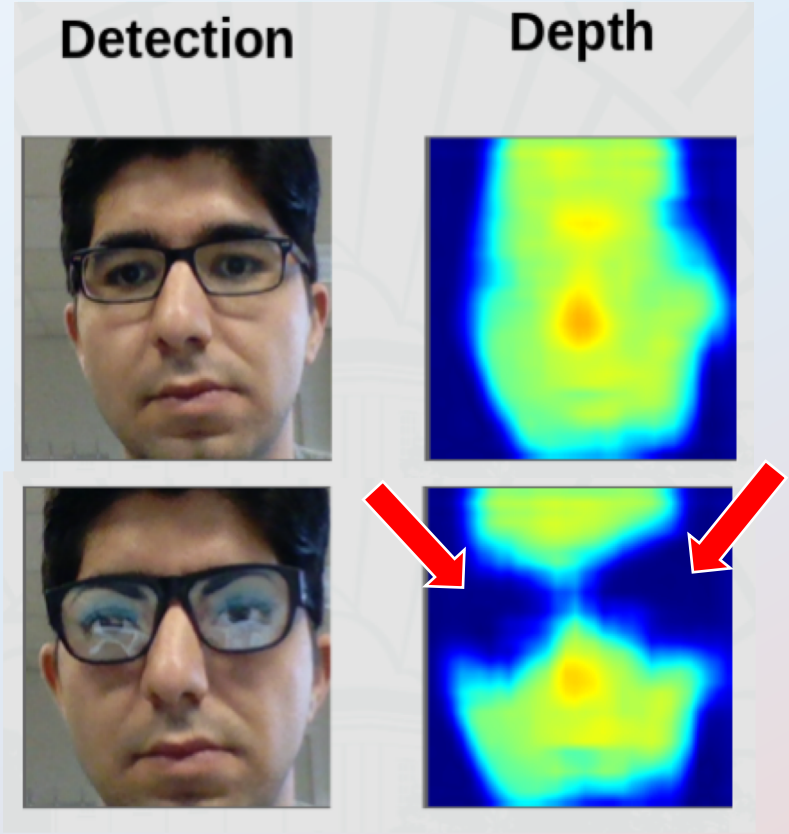
- Depth for live faces: 3D face fitting* + z-buffering rendering
- Depth for spoof faces: zero maps



Yaojie Liu, Amin Jourabloo, and Xiaoming Liu. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. *CVPR 2018.*
*Yaojie Liu, Amin Jourabloo, William Ren, and Xiaoming Liu. Dense Face Alignment. *ICCVW 2017.*

Explainablity

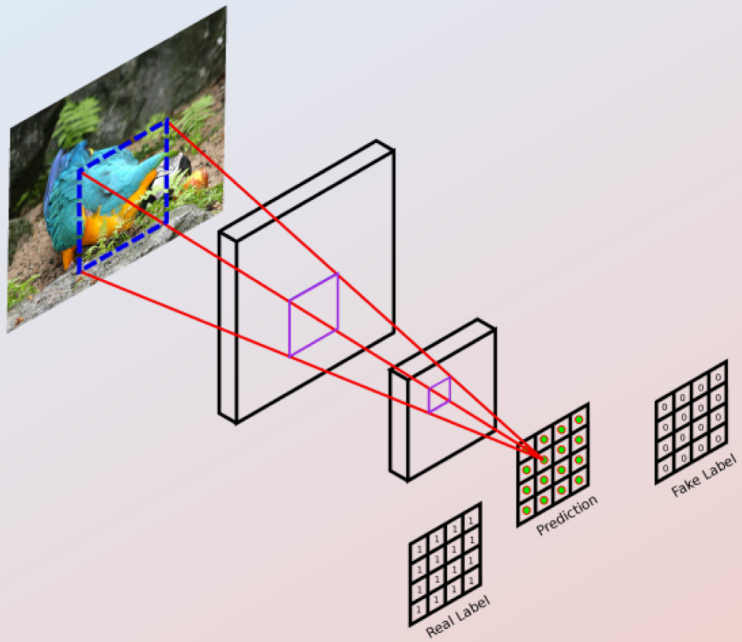
- Indicate the regions of spoof material



Yaojie Liu, Amin Jourabloo, and Xiaoming Liu. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. *CVPR 2018.*

Why Depth Maps Work?

- Local response (same rationale with Patch GAN)
- More elegant than patch-based CNNs (even multiscales!)
- Depth map vs. zero/one map
  - Focus on the face region
  - Noisy background may lead to a worse convergence

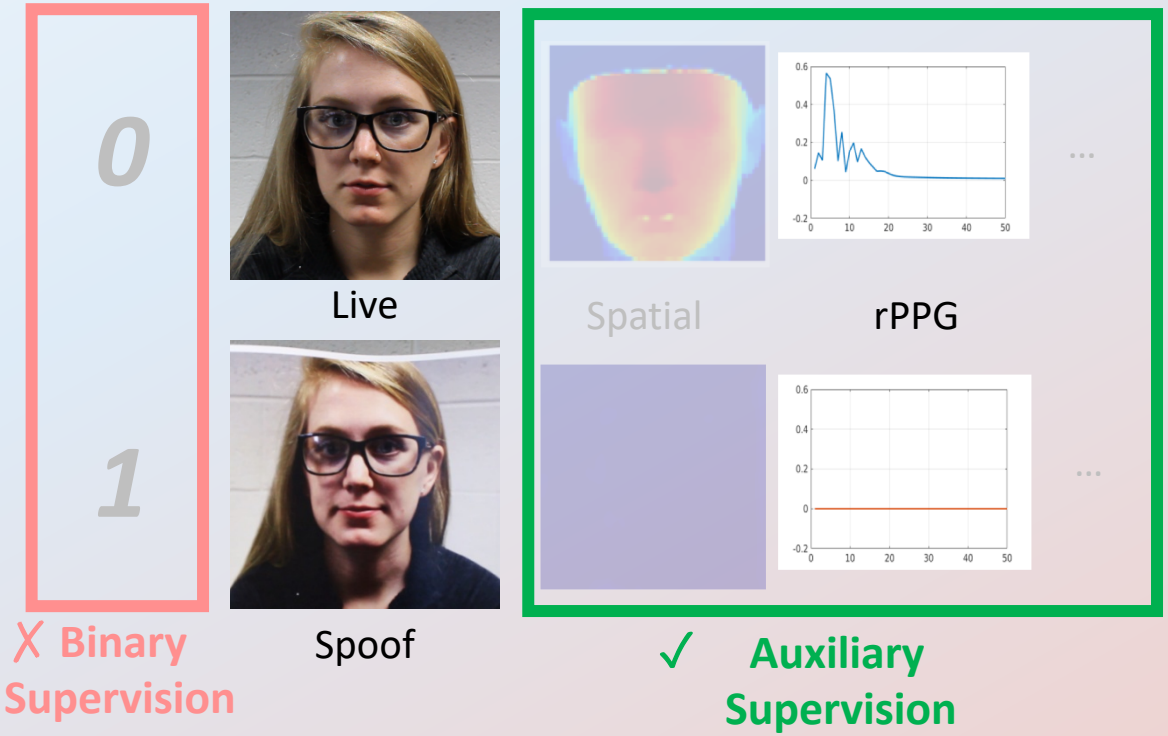


Yaojie Liu, Amin Jourabloo, and Xiaoming Liu. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. *CVPR 2018.*

rPPG Temporal Signal

BTAS 2019

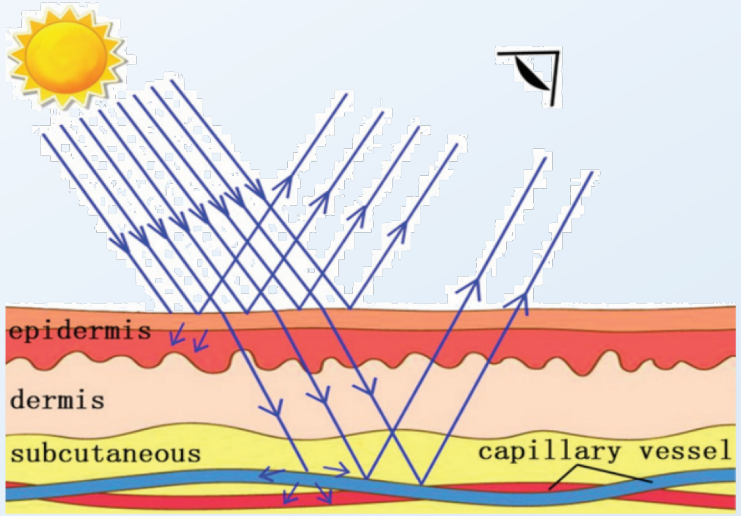
- Provide specific attention for CNN
- Make CNN explainable



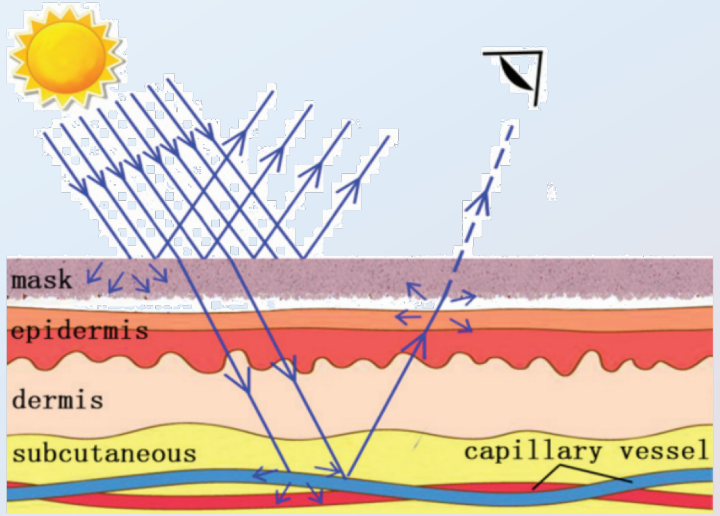
What is rPPG?

BTAS 2019

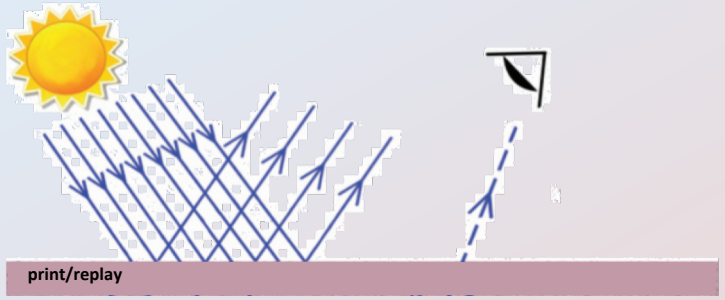
- Remote photoplethysmography: heart beat measurement from human skin using a non-contact camera



Live Face



3D Mask Spoof Face



Print/Replay Spoof Face

Methods using rPPG

BTAS 2019

3D Mask Face Anti-spoofing with Remote Photoplethysmography, ECCV 2016

Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection, ECCV 2018

Learning deep models for face anti-spoofing: binary or auxiliary supervision. *CVPR 2018.*

Methods using rPPG

BTAS 2019

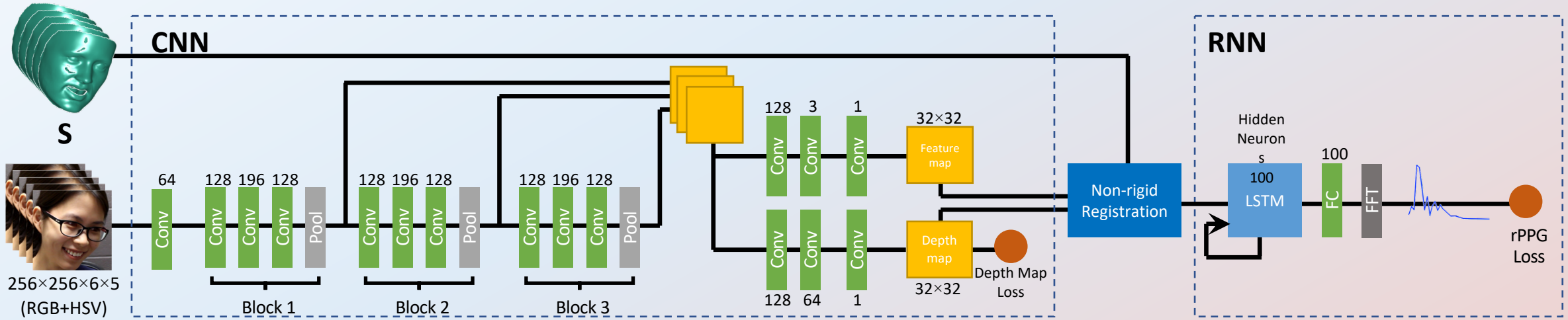
3D Mask Face Anti-spoofing with Remote Photoplethysmography, ECCV 2016

Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection, ECCV 2018

Learning deep models for face anti-spoofing: binary or auxiliary supervision. *CVPR 2018.*

Overall Architecture

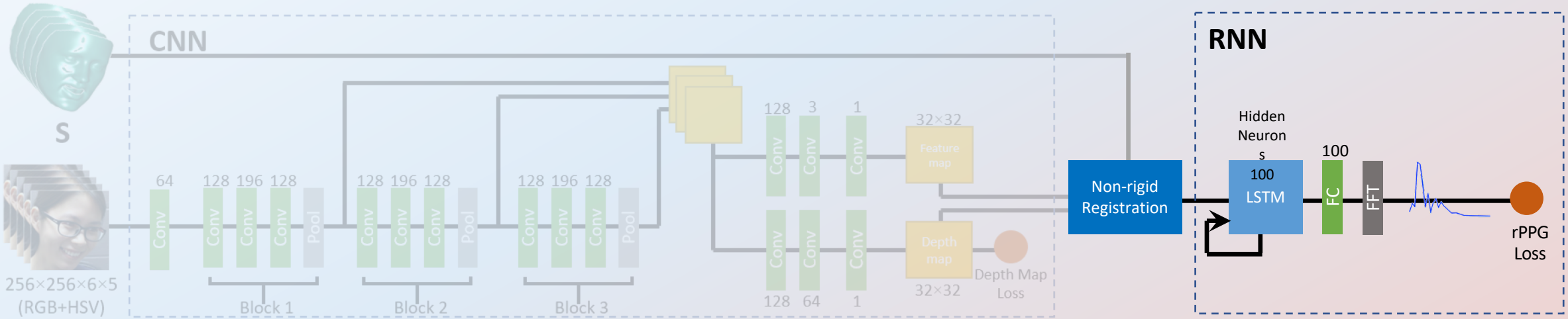
- Spatial supervision: depth map
- Temporal supervision: rPPG signal



Yaojie Liu, Amin Jourabloo, and Xiaoming Liu. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. *CVPR 2018.*

Overall RNN Architecture

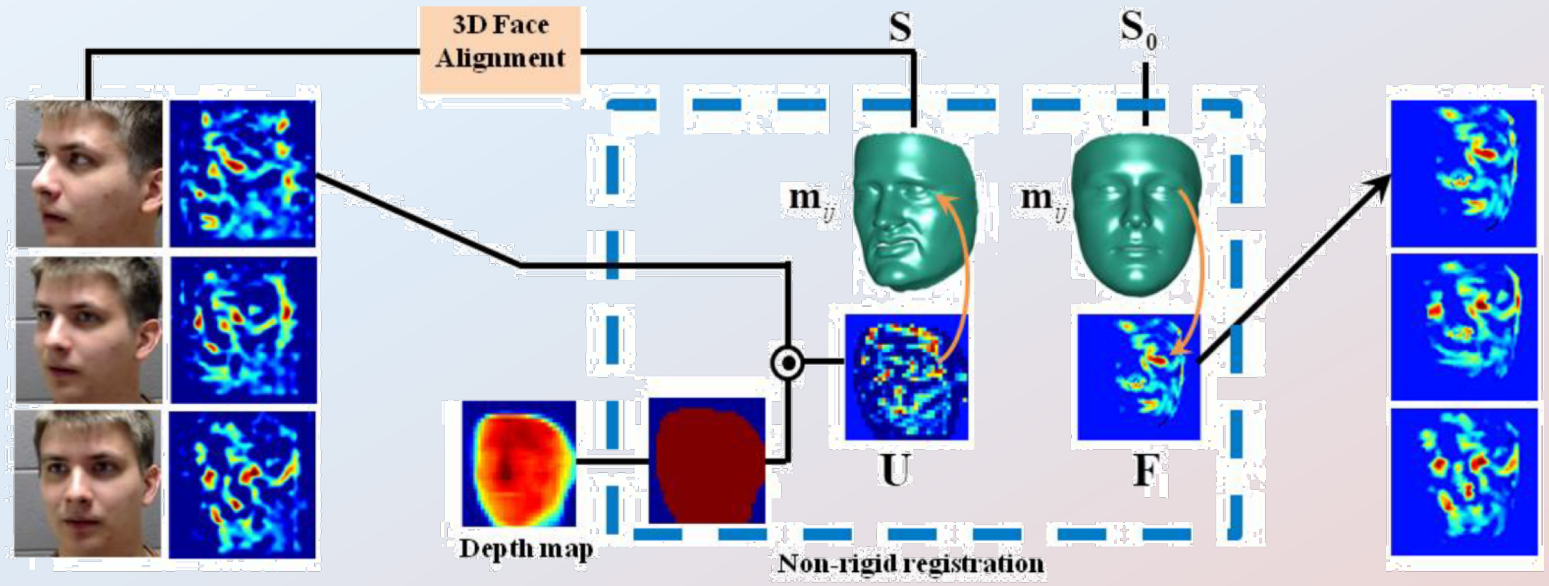
- CNN features as input
- Use non-rigid registration layer to align the features
- LSTM + FFT to predict rPPG



Yaojie Liu, Amin Jourabloo, and Xiaoming Liu. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. *CVPR 2018.*

Non-rigid Registration Layer

- Use 3D shape to compute offset
- Use offset to deform the features
- Differentiable



Yaojie Liu, Amin Jourabloo, and Xiaoming Liu. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. *CVPR 2018.*

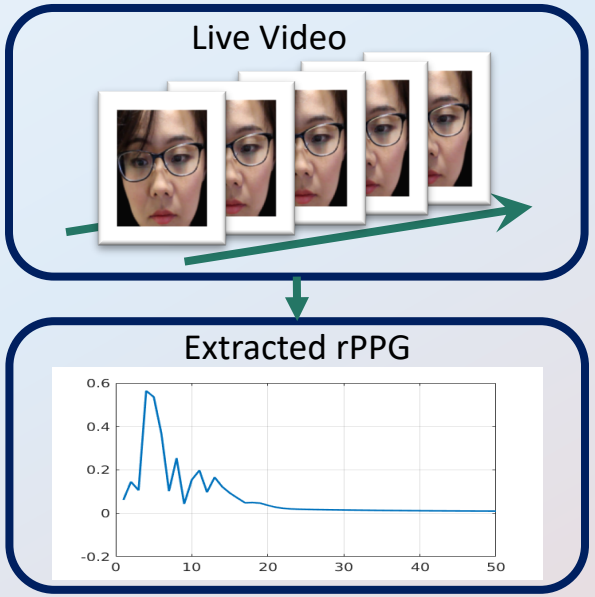
How to Obtain rPPG Label?

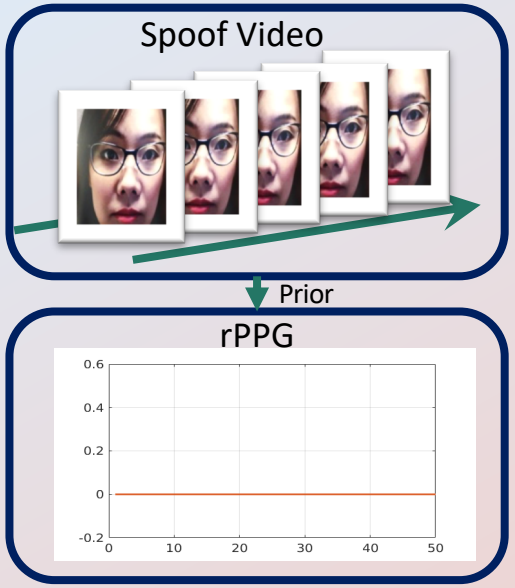
- Live faces: from off-the-shelf method*

$$S = c_1 R_n + c_2 G_n + c_3 B_n$$

$$C_{ni} = \frac{C_i}{\mu(C_i)}$$

- Spoof faces: Direct assignment as zero





Liu et. al., Learning deep models for face anti-spoofing: Binary or auxiliary supervision. *CVPR 2018.*
*Haan et. al., Robust pulse-rate from chrominance-based rPPG, IEEE Transactions on biomedical engineering

Oulu NPU Dataset

BTAS 2019

Protocol	Method	APCER	BPCER	ACER
P1	CPqD	2.9%	10.8%	6.9%
	GRADIANT	**1.3%**	12.5%	6.9%
	Auxiliary	1.6%	**1.6%**	**1.6%**
P2	MixedFASNet	9.7%	2.5%	6.1%
	Auxiliary	**2.7%**	2.7%	2.7%
	GRADIANT	3.1%	**1.9%**	**2.5%**
P3	MixedFASNet	5.3±6.7%	7.8±5.5%	6.5±4.6%
	GRADIANT	**2.6±3.9%**	5.0±5.3%	3.8±2.4%
	Auxiliary	2.7±1.3%	**3.1±1.7%**	**2.9±1.5%**
P4	Massy_HNU	35.8±35.3	**8.3±4.1%**	22.1±17.6%
	GRADIANT	**5.0±4.5%**	15.0±7.1%	10.0±5.0%
	Auxiliary	9.3±5.6%	10.4±6.0%	**9.5±6.0%**

Yaojie Liu, Amin Jourabloo, and Xiaoming Liu. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. *CVPR 2018.*

Oulu NPU Dataset

- Cross-test on CASIA and IDIAP (HTER)

Method	Train	Test	Train	Test
	CASIA MFSD	Replay Attack	Replay Attack	CASIA MFSD
Motion	50.2%		47.9%	
LBP	55.9%		57.6%	
LBP-TOP	49.7%		60.6%	
Motion-Mag	50.1%		47.0%	
Spectral cubes	34.4%		50.0%	
CNN	48.5%		45.5%	
LBP	47.0%		39.6%	
Color Texture	30.3%		37.7%	
Proposed method	**27.6%**		**28.4%**	

Yaojie Liu, Amin Jourabloo, and Xiaoming Liu. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. *CVPR 2018.*

Methods using Depth Map

BTAS 2019

Face anti-spoofing using patch and depth-based CNNs. IJCB 2017.

Learning deep models for face anti-spoofing: binary or auxiliary supervision. *CVPR 2018.*

Face de-spoofing: anti-spoofing via noise modeling. *ECCV* 2018.

Exploiting temporal and depth information for multi-frame face anti-spoofing, arXiv 2019

Aurora guard: real-time face anti-spoofing via light reflection, arXiv 2019

Meta Anti-spoofing: Learning to Learn in Face Anti-spoofing, arXiv 2019

Multi-adversarial discriminative deep domain generalization for face presentation attack detection. CVPR 2019

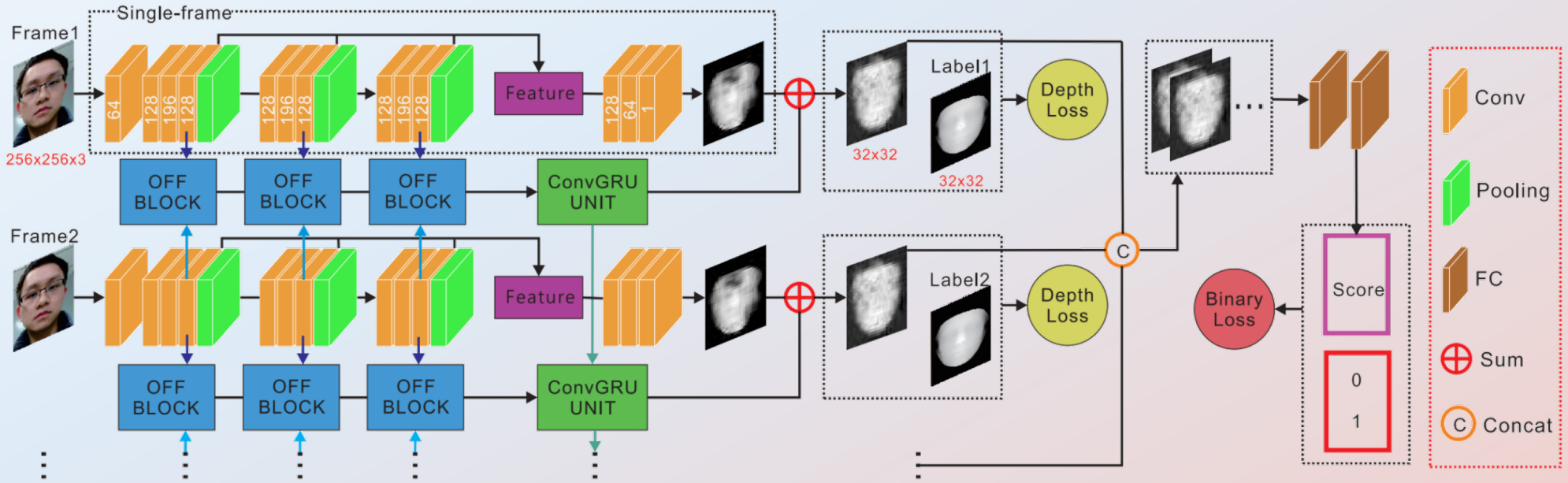
Deep tree learning for zero-shot face anti-spoofing. CVPR 2019

…

Exploiting Temporal and Depth Information for Multi-frame Face Anti-spoofing

BTAS 2019

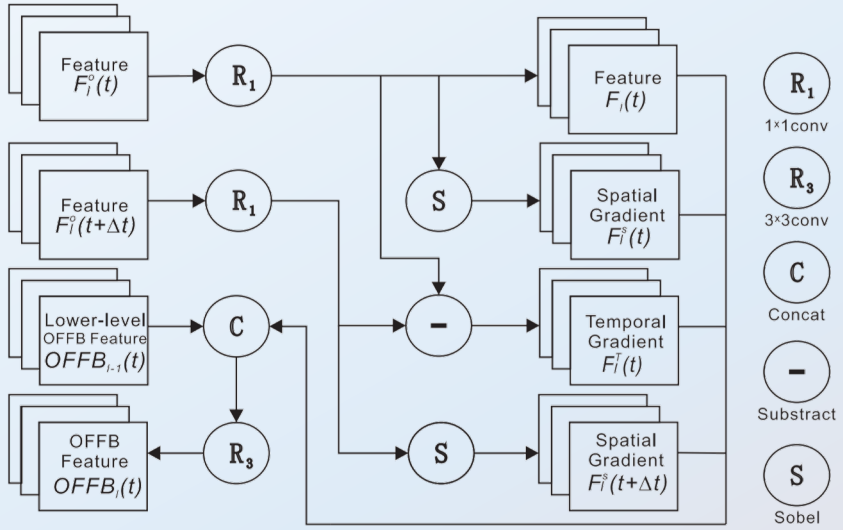
- Map single frame to depth map
- Introduce frame-to-frame motion to complete depth map
- Concat all maps to get a final score

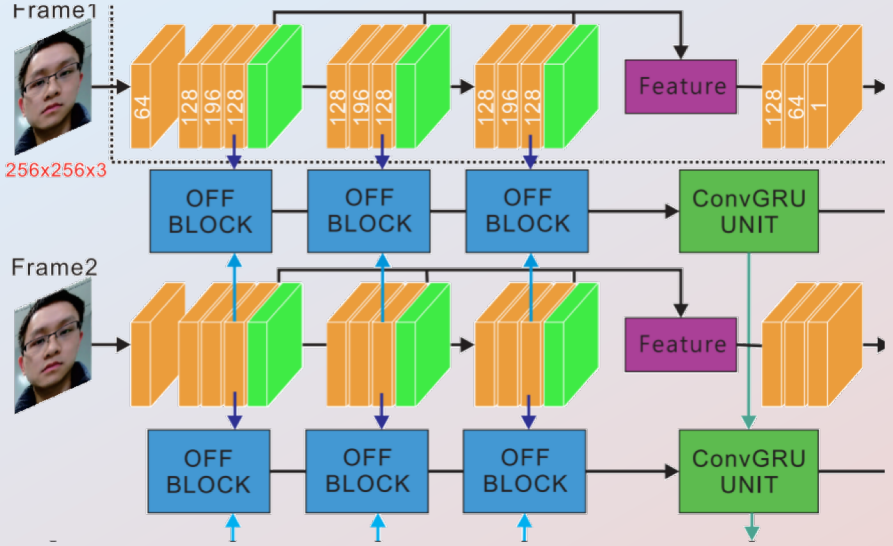


Wang et. al., Exploiting temporal and depth information for multi-frame face anti-spoofing, arXiv 2019

Temporal Blocks

- Short-term motion: OFF Block
- Long-term motion: multi-scale OFF feature to Conv Gated Recurrent Unit (GRU)





Wang et. al., Exploiting temporal and depth information for multi-frame face anti-spoofing, arXiv 2019

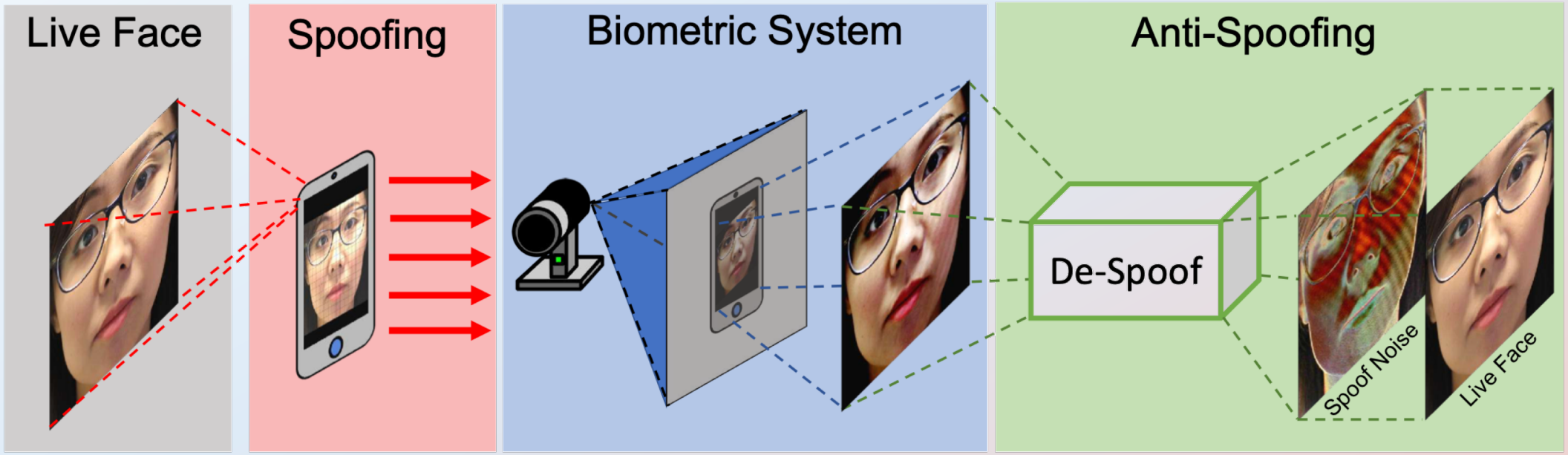
Outline

BTAS 2019

- Vanilla CNNs
- Patch-based CNN methods
- CNN methods with auxiliary supervisions
- **GAN-based noise modeling**
- Data Augmentation

Motivations

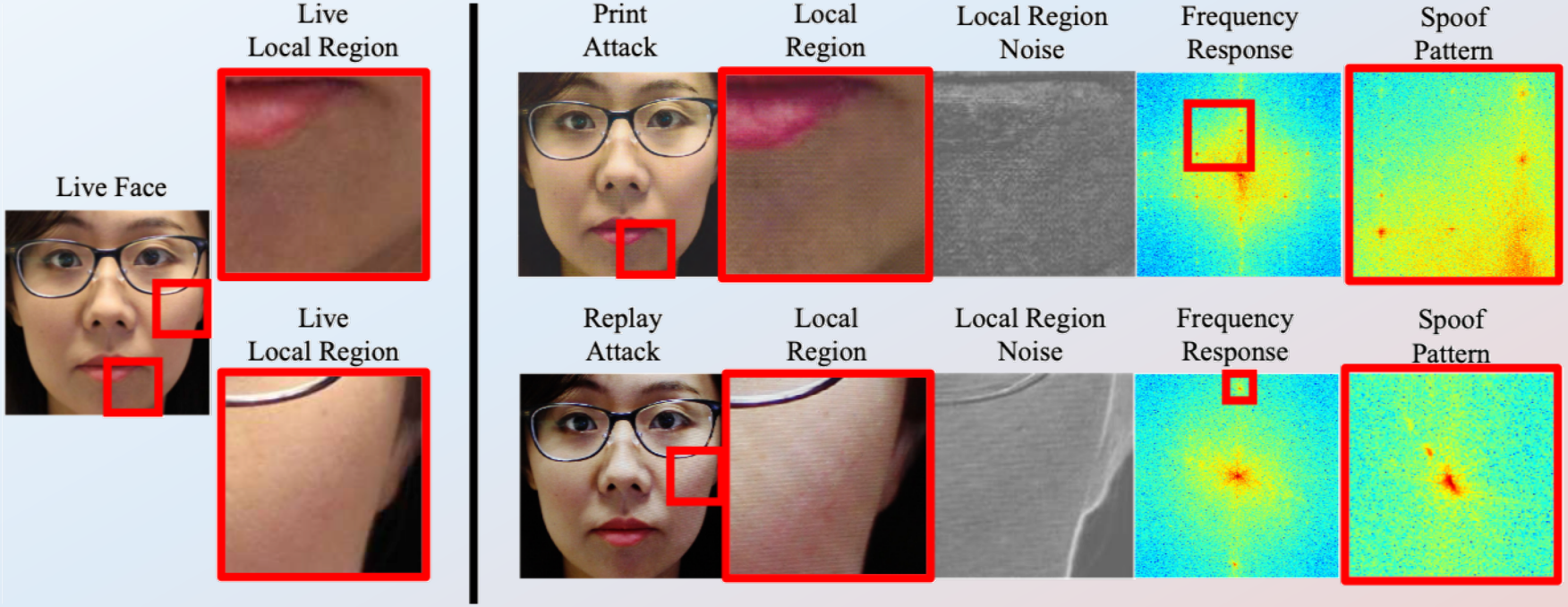
- Model the spoof patterns as noise
- De-spoofing: Decompose the spoof noise for face anti-spoofing.



Amin Jourabloo, Yaojie Liu, and Xiaoming Liu. Face De-spoofing: Anti-spoofing via noise modeling. *ECCV* 2018.

A Case Study

- Careful alignment the spoof with the live
- Subtraction live from spoof
- FFT analysis

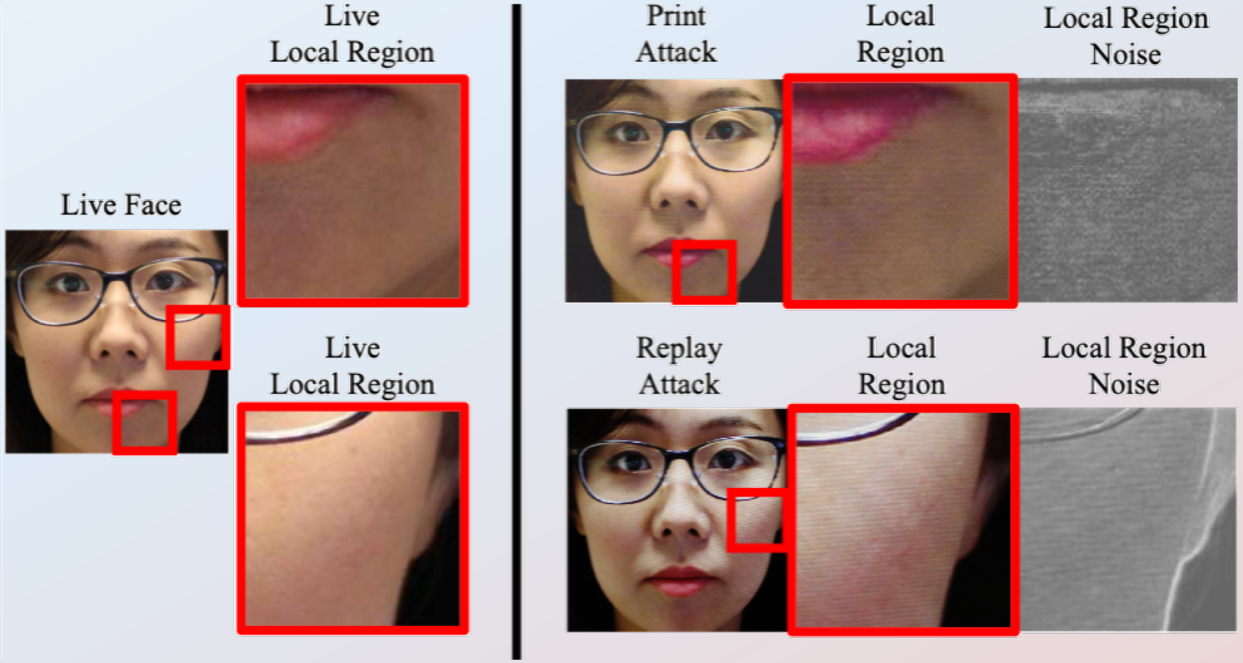


Amin Jourabloo, Yaojie Liu, and Xiaoming Liu. Face De-spoofing: Anti-spoofing via noise modeling. *ECCV* 2018.

The Cause of Spoof Noise Pattern?

BTAS 2019

- Color distortion
- Display artifacts
- Presenting artifacts
- Imaging artifacts



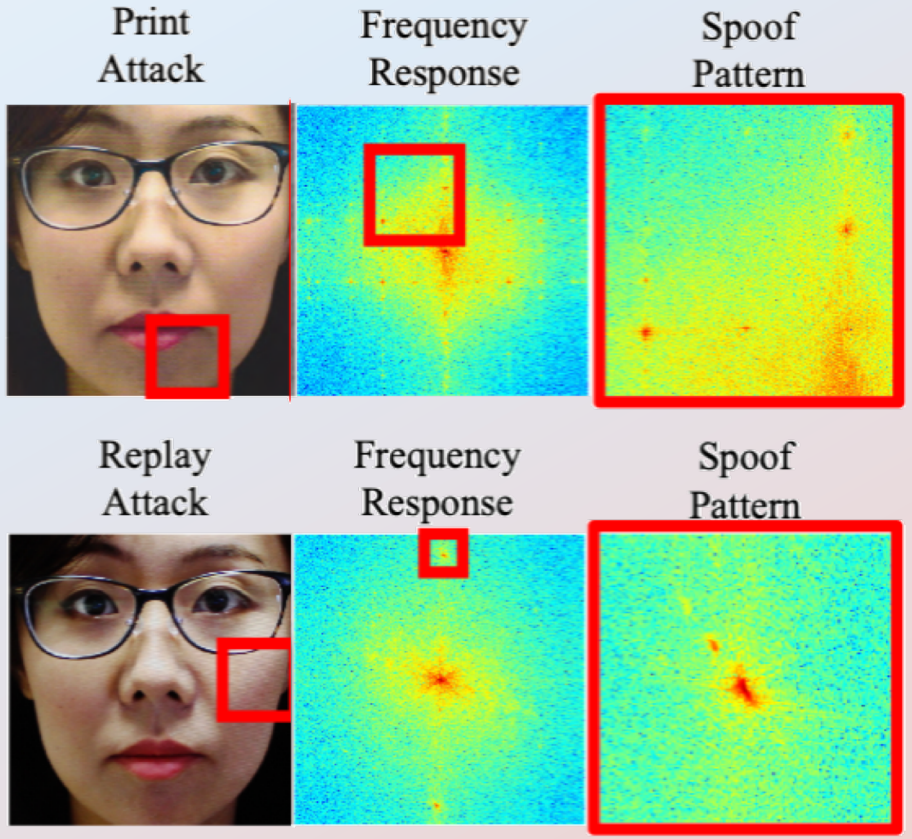
Amin Jourabloo, Yaojie Liu, and Xiaoming Liu. Face De-spoofing: Anti-spoofing via noise modeling. *ECCV* 2018.

Properties of the Spoof Noise Pattern

BTAS 2019

- Repetitive
- Ubiquitous

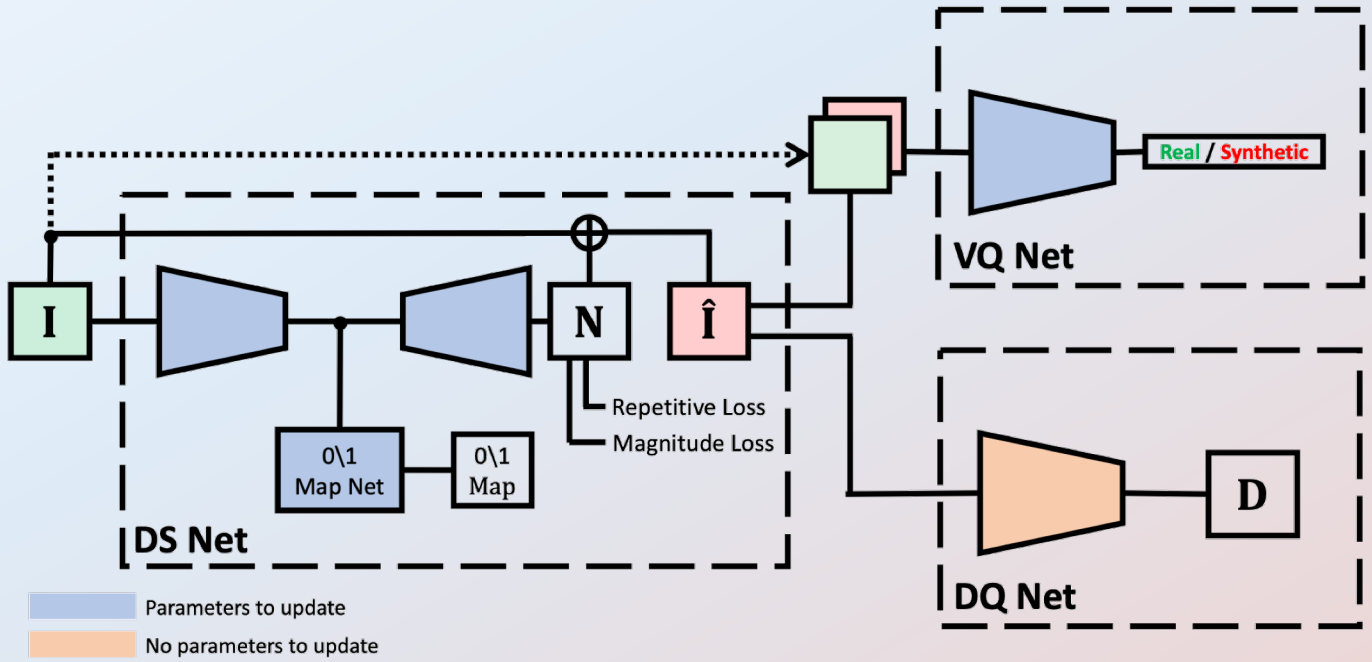
$$\mathbf{x} = \mathbf{A}\hat{\mathbf{x}} + \mathbf{n} = \hat{\mathbf{x}} + (\mathbf{A} - \mathbb{I})\hat{\mathbf{x}} + \mathbf{n} = \hat{\mathbf{x}} + N(\hat{\mathbf{x}})$$



Amin Jourabloo, Yaojie Liu, and Xiaoming Liu. Face De-spoofing: Anti-spoofing via noise modeling. *ECCV* 2018.

Overall Architecture

- **De-Spoofing Net**: estimate spoof noise pattern N and reconstruct live image I
- **Discriminative Quality Net**: guarantee reconstructed I is live
- **Visual Quality Net**: guarantee reconstructed I is photorealistic



Amin Jourabloo, Yaojie Liu, and Xiaoming Liu. Face De-spoofing: Anti-spoofing via noise modeling. *ECCV* 2018.

Training

De-Spoofing Net: Estimate spoof noise pattern N and reconstruct live image I

- Repetitive loss

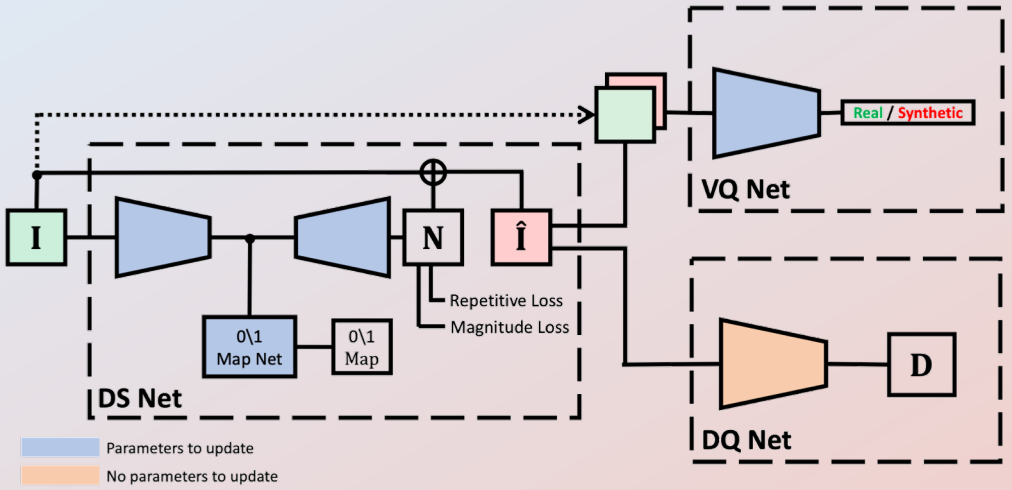
$$J_r = \begin{cases} -\max(H(\mathcal{F}(\mathbf{N}), k)), & \mathbf{I} \in Spoof \\ \|\max(H(\mathcal{F}(\mathbf{N}), k))\|_1, & \mathbf{I} \in Live \end{cases}$$

- Ubiquitous loss: zero/one map loss

$$J_z = \|\mathrm{CNN}_{01map}(\mathbf{F}; \Theta) - \mathbf{M}\|_1$$

- Magnitude loss

$$J_m = \|\mathbf{N}\|_1 \text{ , for live}$$



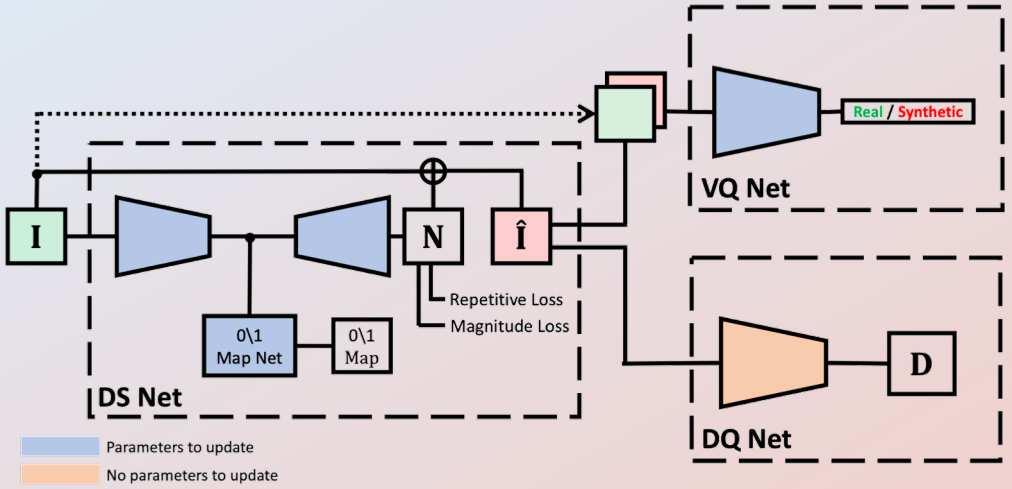
Amin Jourabloo, Yaojie Liu, and Xiaoming Liu. Face De-spoofing: Anti-spoofing via noise modeling. *ECCV* 2018.

Training

Discriminative Quality Net: guarantee reconstructed I is live

- Depth map loss

$$J_{DQ} = \left\| \mathrm{CNN}_{DQ}(\hat{\mathbf{I}}) - \mathbf{D} \right\|_1$$



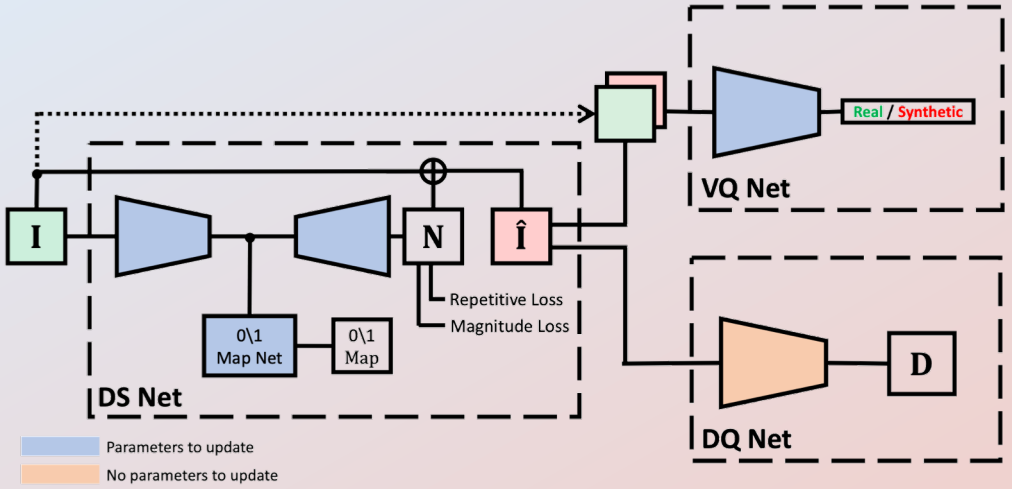
Amin Jourabloo, Yaojie Liu, and Xiaoming Liu. Face De-spoofing: Anti-spoofing via noise modeling. *ECCV* 2018.

Training

Visual Quality Net: guarantee reconstructed I is photorealistic

- GAN loss

$$J_{VQ_{train}} = -\mathbb{E}_{\mathbf{I}\in\mathcal{R}} \log(\mathrm{CNN}_{VQ}(\mathbf{I})) - \mathbb{E}_{\mathbf{I}\in\mathcal{S}} \log(1 - \mathrm{CNN}_{VQ}(\mathrm{CNN}_{DS}(\mathbf{I})))$$

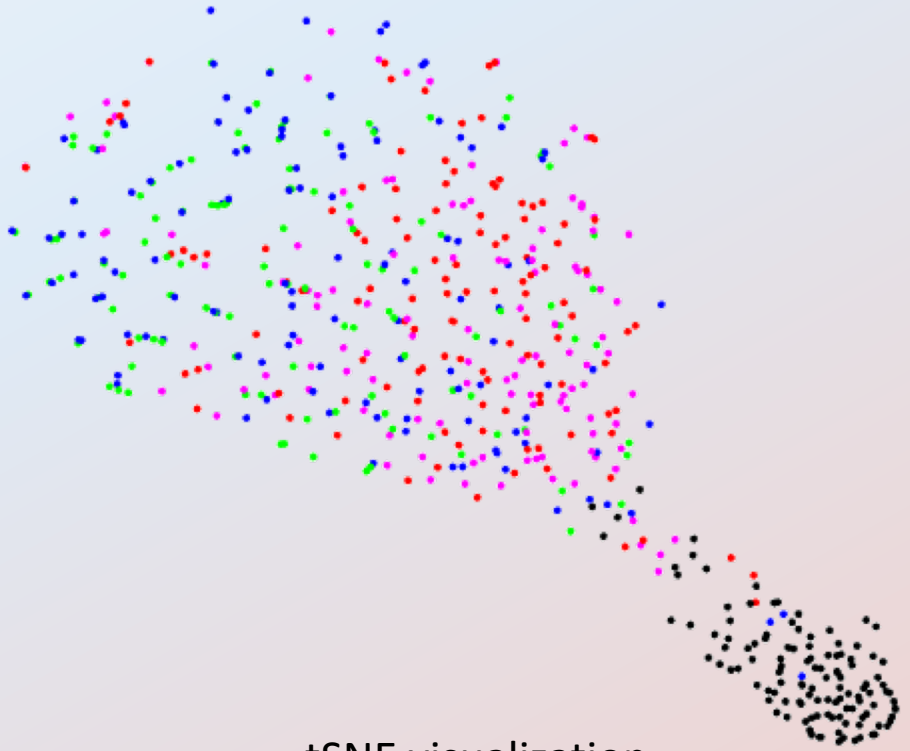


Amin Jourabloo, Yaojie Liu, and Xiaoming Liu. Face De-spoofing: Anti-spoofing via noise modeling. *ECCV* 2018.

Noise Classification

Actual \ Predicted	live	print	display
live	59	1	0
print	0	88	32
display	13	8	99

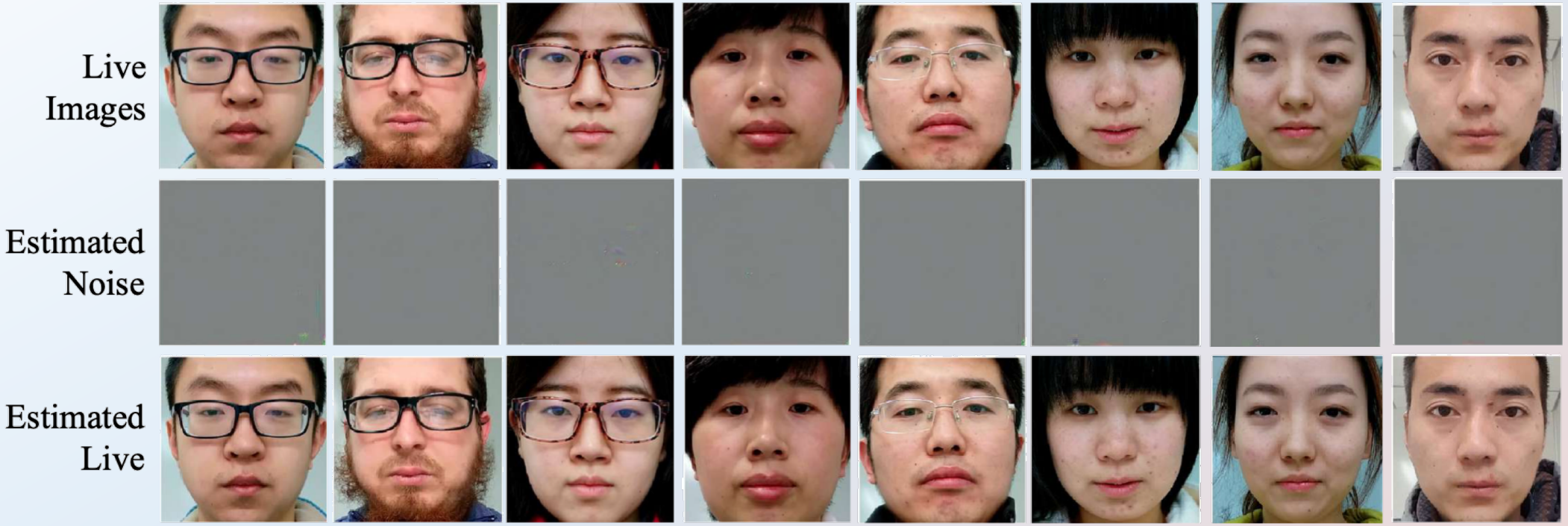
Actual \ Predicted	live	print1	print2	display1	display2
live	59	0	1	0	0
print1	0	41	2	11	6
print2	0	34	11	9	6
display1	10	6	0	13	31
display2	8	7	0	6	39



tSNE visualization

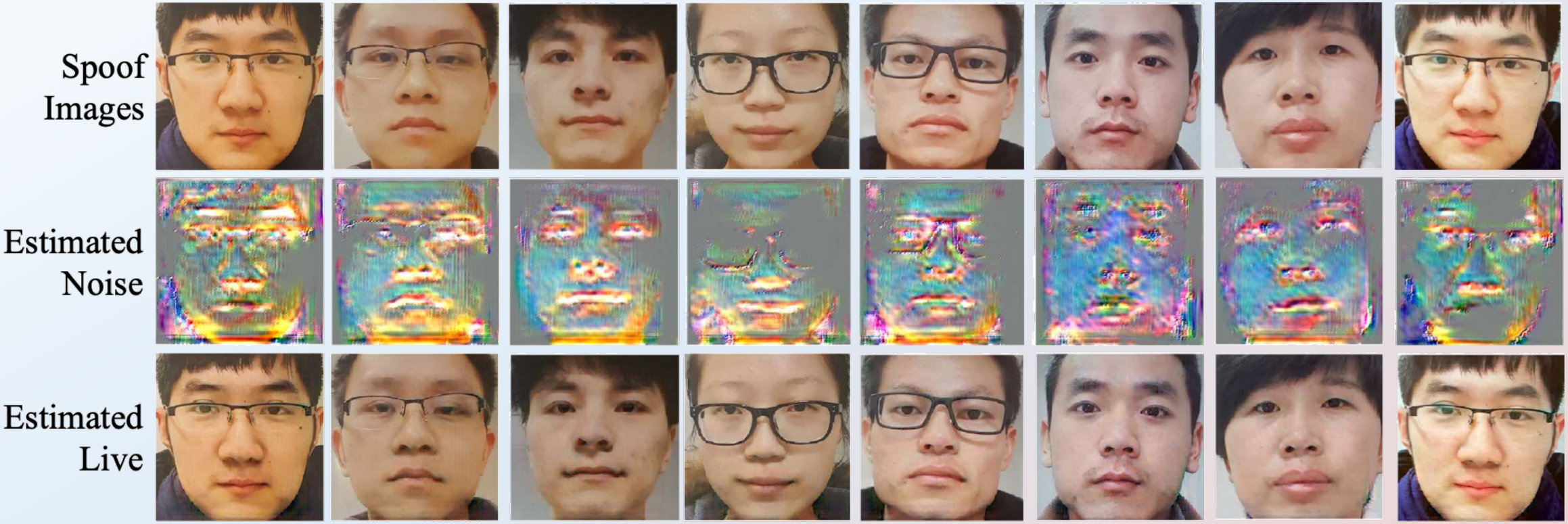
Amin Jourabloo, Yaojie Liu, and Xiaoming Liu. Face De-spoofing: Anti-spoofing via noise modeling. *ECCV* 2018.

Results of Live



Amin Jourabloo, Yaojie Liu, and Xiaoming Liu. Face De-spoofing: Anti-spoofing via noise modeling. *ECCV* 2018.

Results of Spoof



Amin Jourabloo, Yaojie Liu, and Xiaoming Liu. Face De-spoofing: Anti-spoofing via noise modeling. *ECCV* 2018.

Testing on Oulu

BTAS 2019

Protocol	Method	APCER	BPCER	ACER
P1	CPqD	2.9%	10.8%	6.9%
	GRADIANT	1.3%	12.5%	6.9%
	Auxiliary	1.6%	**1.6%**	1.6%
	DS Net	**1.2%**	1.7%	**1.5%**
P2	MixedFASNet	9.7%	2.5%	6.1%
	Auxiliary	**2.7%**	2.7%	2.7%
	GRADIANT	3.1%	**1.9%**	**2.5%**
	DS Net	4.2%	4.4%	4.3%
P3	MixedFASNet	5.3±6.7%	7.8±5.5%	6.5±4.6%
	GRADIANT	**2.6±3.9%**	5.0±5.3%	3.8±2.4%
	Auxiliary	2.7±1.3%	**3.1±1.7%**	**2.9±1.5%**
	DS Net	4.0±1.8%	3.8±1.2%	3.6±1.6%
P4	Massy_HNU	35.8±35.3	8.3±4.1%	22.1±17.6%
	GRADIANT	**5.0±4.5%**	15.0±7.1%	10.0±5.0%
	Auxiliary	9.3±5.6%	10.4±6.0%	9.5±6.0%
	DS Net	5.1±6.3%	**6.1±5.0%**	**5.6±5.7%**

Amin Jourabloo, Yaojie Liu, and Xiaoming Liu. Face De-spoofing: Anti-spoofing via noise modeling. *ECCV* 2018.

Outline

BTAS 2019

- Vanilla CNNs
- Patch-based CNN methods
- CNN methods with auxiliary supervisions
- GAN-based noise modeling
- **Data Augmentation**

Data Augmentations

BTAS 2019

Face Anti-Spoofing: Model Matters, So Does Data, CVPR, 2019

Presentation Attack Detection for Face in Mobile Phones, Selfie Biometrics, 2019

Style Transfer Applied to Face Liveness Detection with User-Centered Models, arXiv, 2019

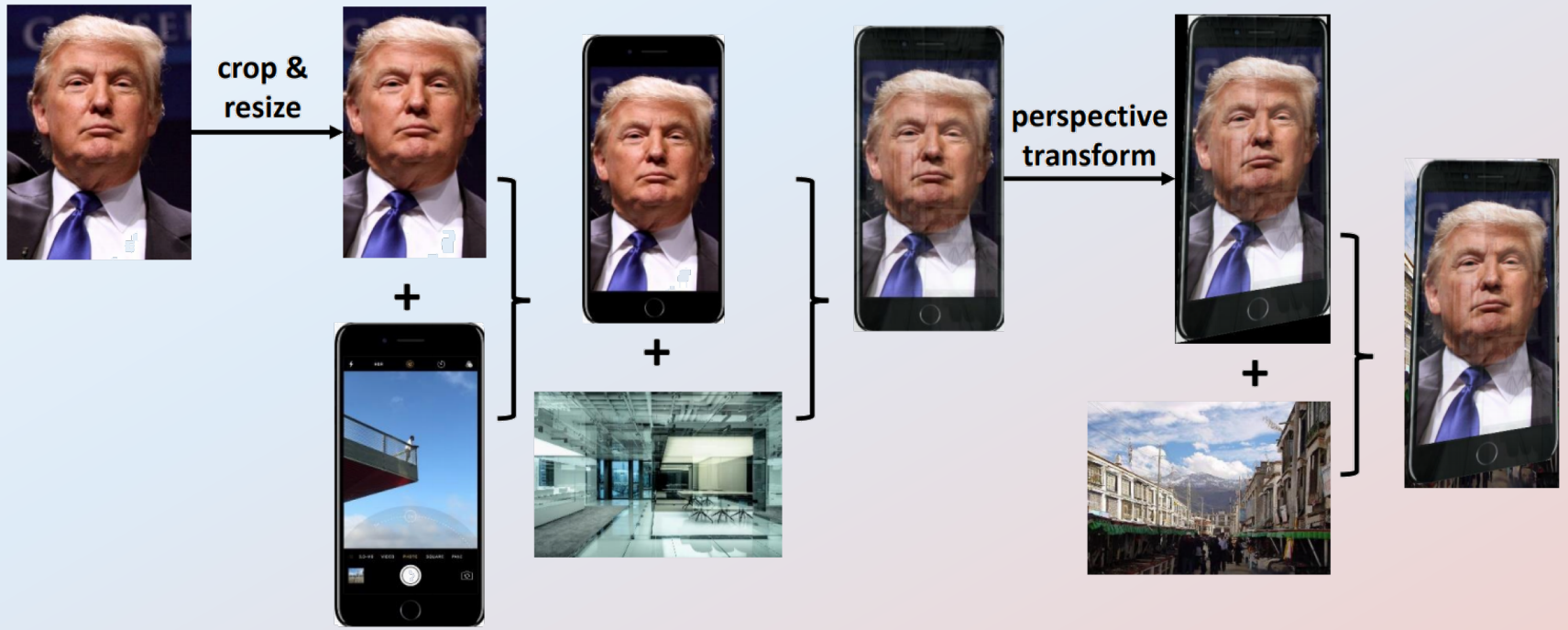
Improving Face Anti-Spoofing by 3D Virtual Synthesis, arXiv, 2019

Face Anti-Spoofing: Model Matters, So Does Data

BTAS 2019

Synthesize

- Blurriness: random strength Gaussian blurring
- Reflection: $\mathbf{X}'_r = (1-\alpha)\,\mathbf{X}' + \alpha\mathbf{X}_r$
- Distortion: Perspective projection



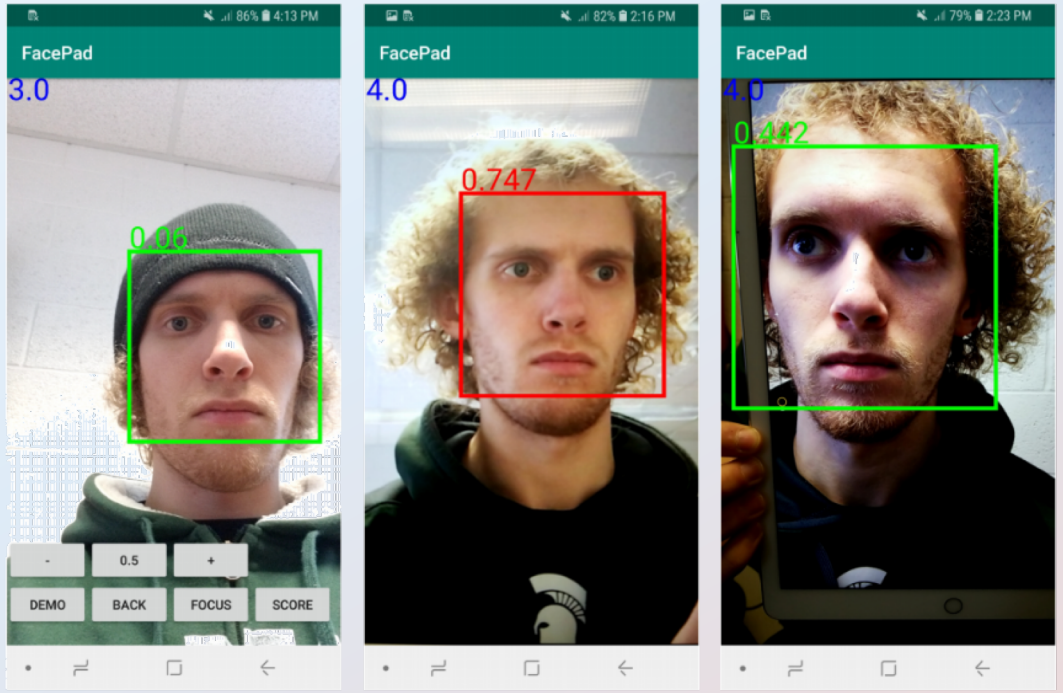
Yang et. al., Face Anti-Spoofing: Model Matters, So Does Data, CVPR 2019

Presentation Attack Detection for Face in Mobile Phones

BTAS 2019

Random perturbation:

- Contrast
- Lightness

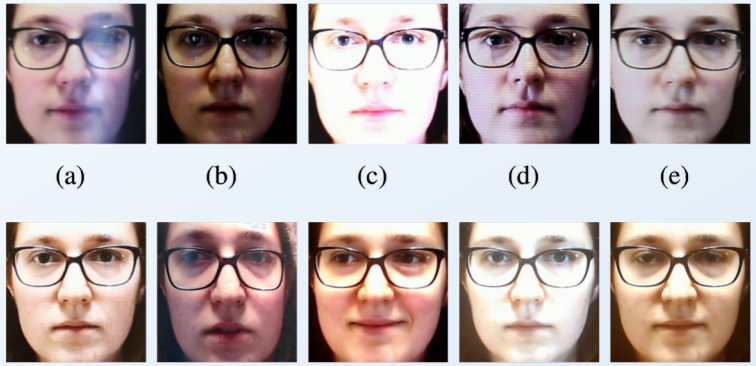


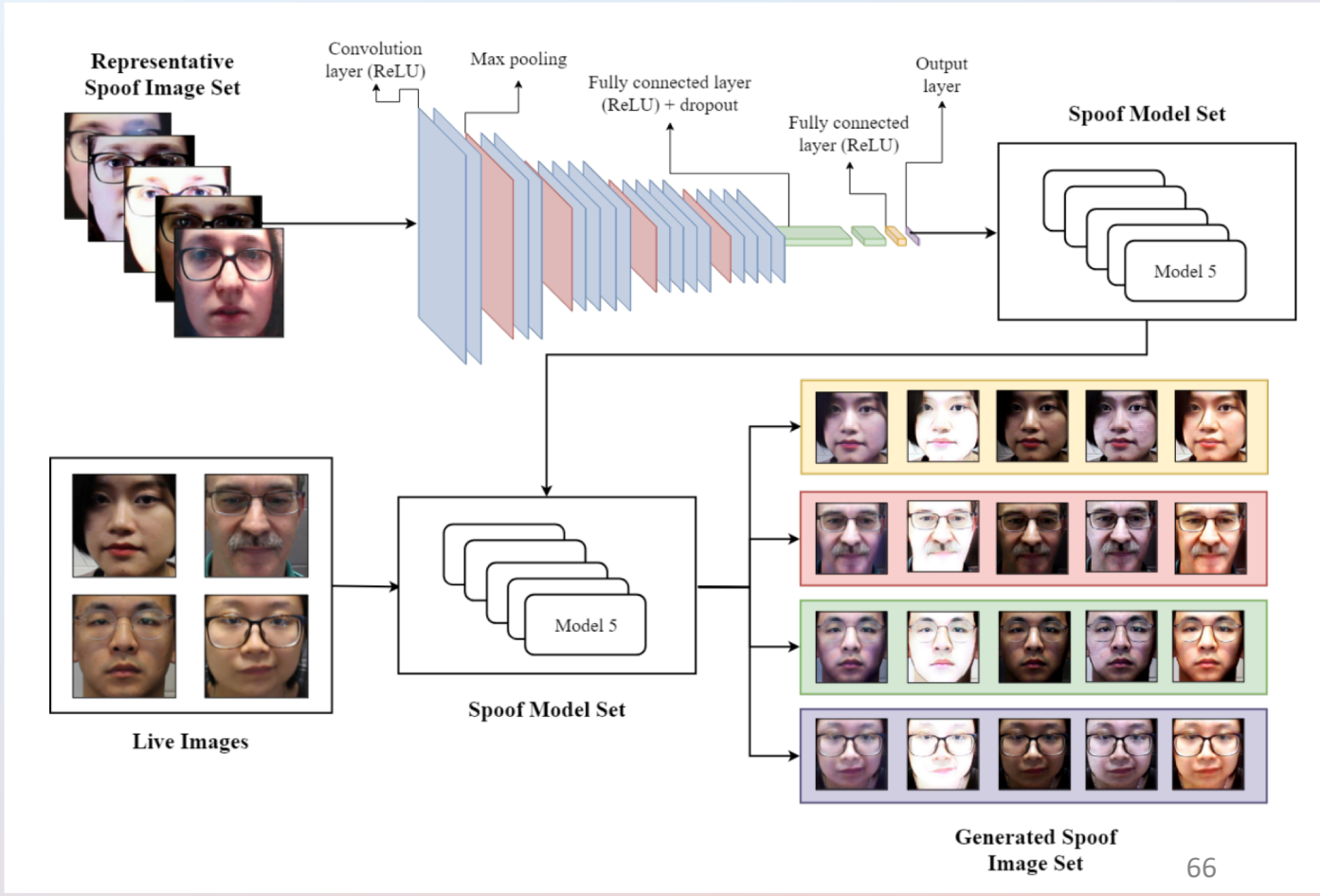
Liu et. al., Presentation Attack Detection for Face in Mobile Phones, Selfie Biometrics, 2019

Style Transfer

BTAS 2019

Use CNN for data augmentation

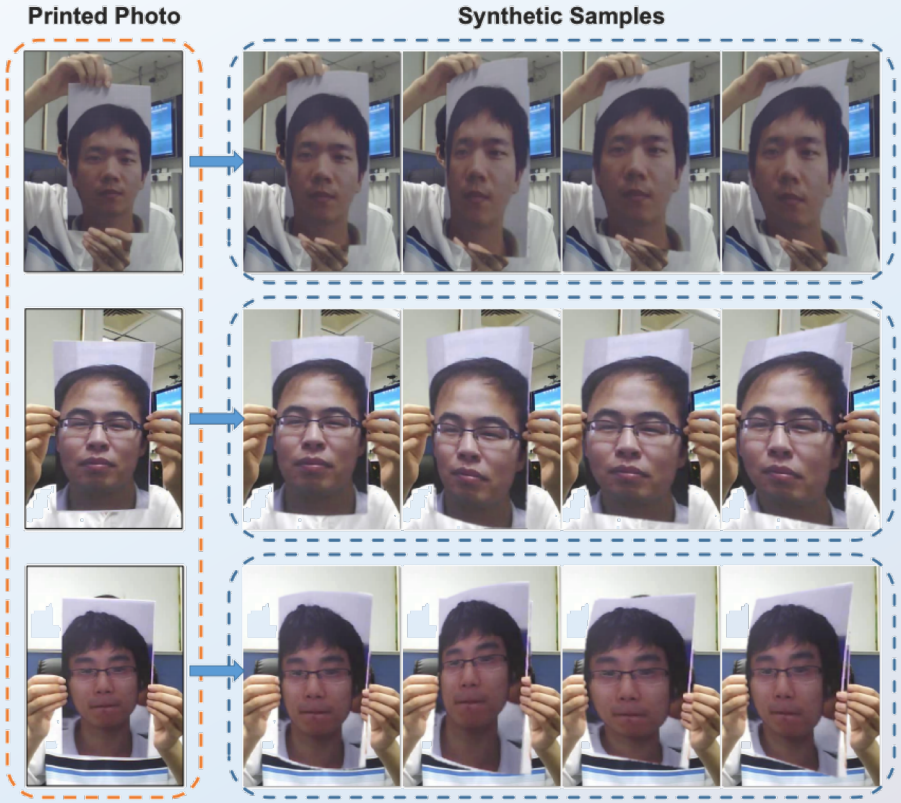


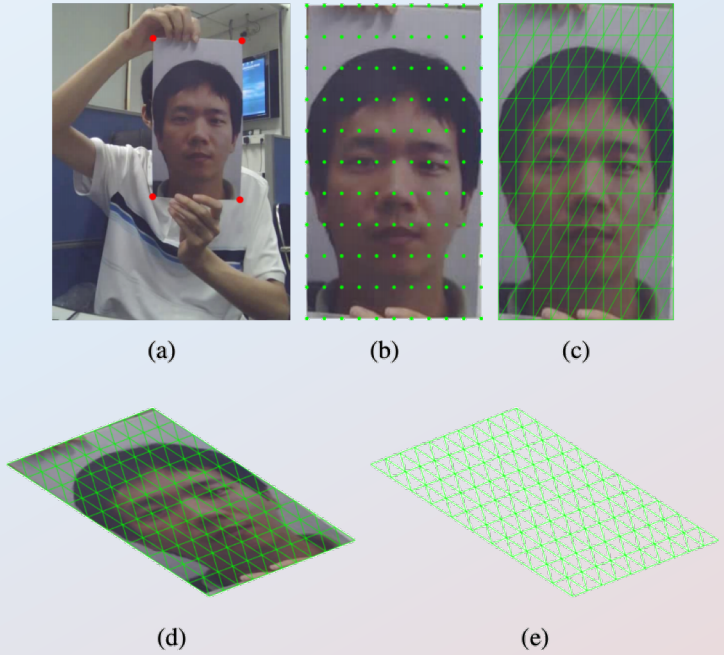


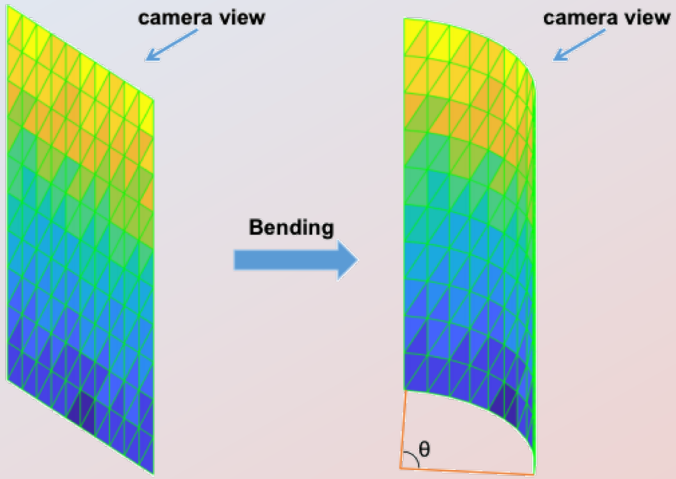
Laurensi et. al., Style Transfer Applied to Face Liveness Detection with User-Centered Models, arXiv, 2019

3D Synthesis

Use CNN to deform the face based on 3D shape







Guo et. al., Improving Face Anti-Spoofing by 3D Virtual Synthesis, arXiv, 2019

Summary

- We review deep learning based methods
- Binary CNN may lead to overfitting
- Advanced design is required
  - Multiple input features
  - Auxiliary supervision
  - Noise modeling
  - Data augmentation

BTAS 2019

End of Session II

Q & A

MICHIGAN STATE UNIVERSITY

Computer Vision Lab

BTAS 2019

End of Session II

15 Minutes Break.

MICHIGAN STATE UNIVERSITY

Computer Vision Lab