Secure the Face Analysis System

Recent Advances on Detecting Face Presentation Attacks and Digital Manipulation

MICHIGAN STATE UNIVERSITY

Computer Vision Lab

IJCB 2020

Outline

Session 1: Face Anti-Spoofing: Detection and Visualization

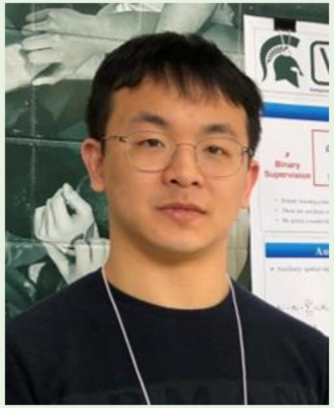
Break: 7 mins

Session 2: Face Anti-Spoofing Generalization

Break: 7 mins

Session 3: Digital Face Manipulation

Introduction



Yaojie Liu

liuyaoj1@msu.edu

Dr. Xiaoming Liu

liuxm@cse.msu.edu

1. http://cvlab.cse.msu.edu/pages/presentation.html

Acknowledgement

Joel Stehouwer

Amin Jourabloo

Yousef Atoum

Feng Liu

Xiaohong Liu

Vishal Asnani

Acknowledgement

The research of face presentation attack detection is based upon work supported by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA), via IARPA R&D Contract No. 2017-17020200004. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the ODNI, IARPA, or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon.

IARPA
BE THE FUTURE

Session I
Face Anti-Spoofing: Detection and Visualization

Host: Yaojie Liu

MICHIGAN STATE UNIVERSITY

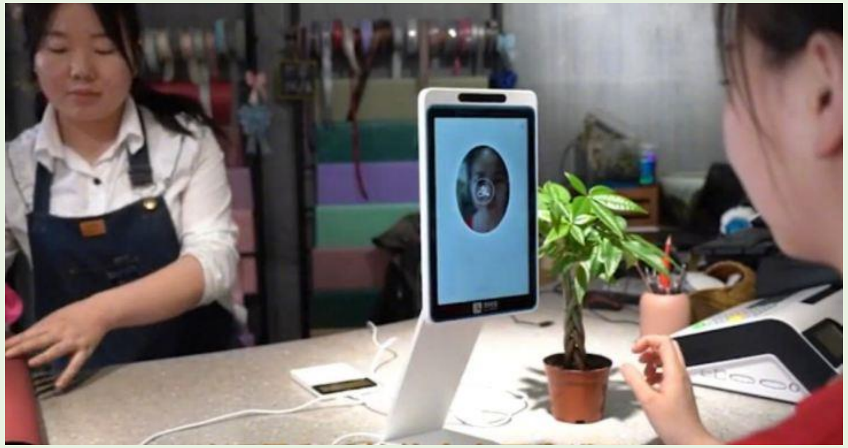
Computer Vision Lab

IJCB 2020

Face: Easy-to-use Biometric Modality

Public Security

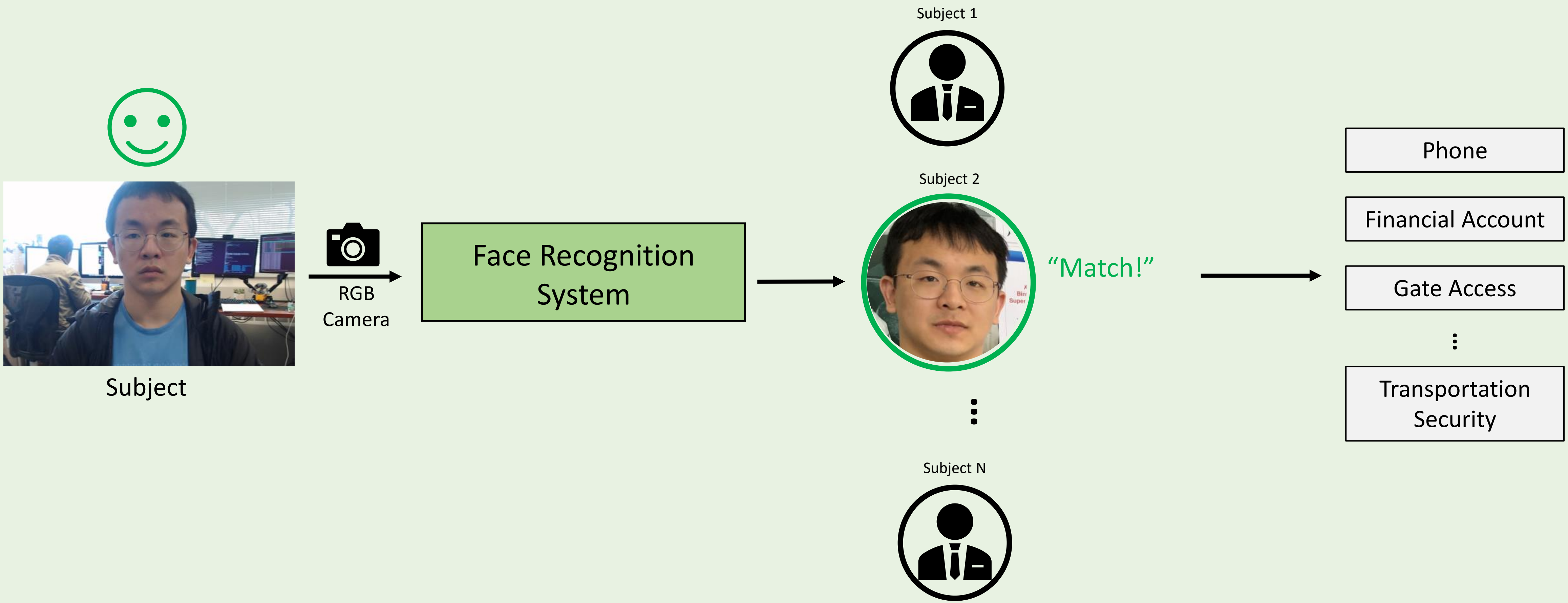
Border Control



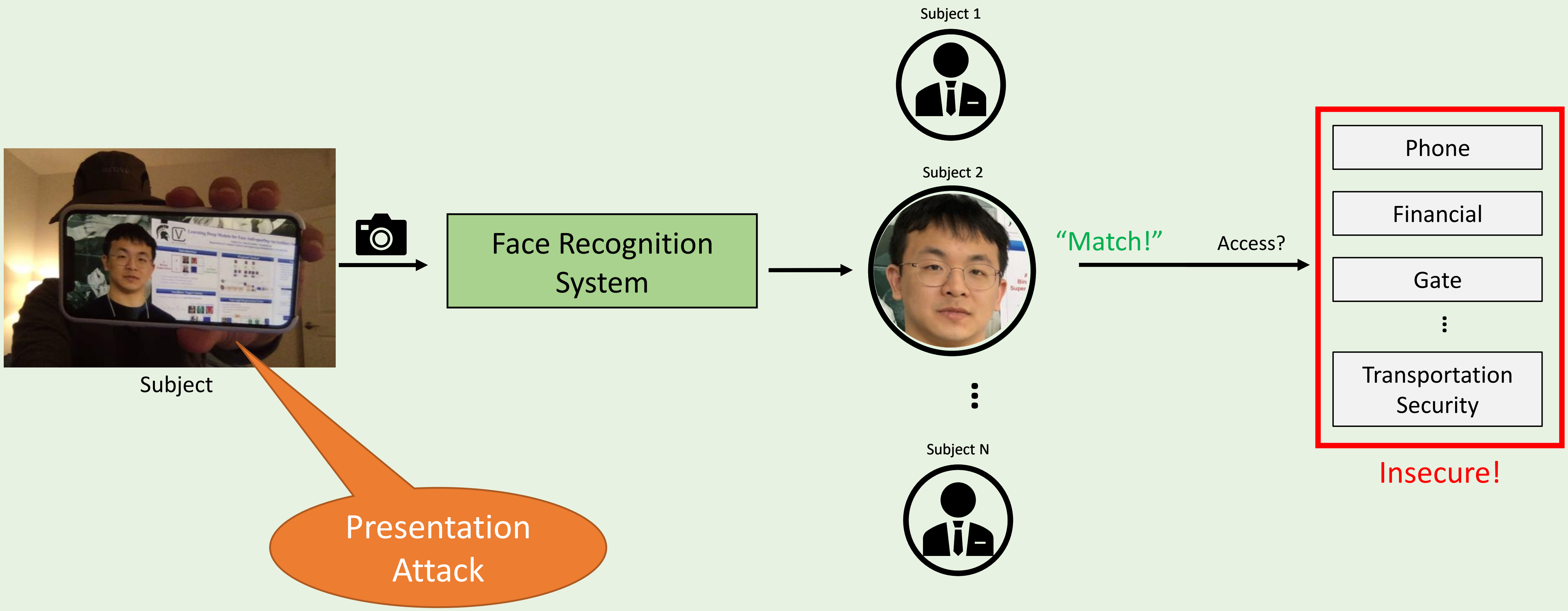
Quick Purchase

Building Access

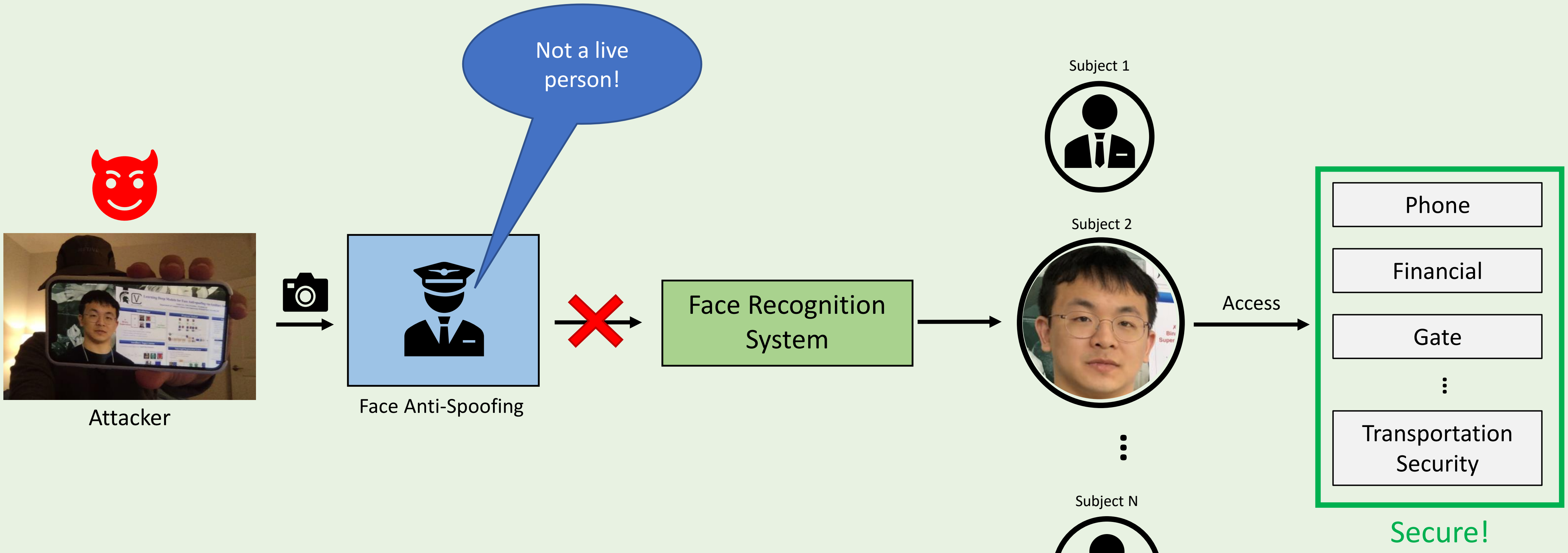
A General Face Recognition Flow



Is This Secure?



Face Anti-Spoofing



The Development

- Interaction-based methods (2006-2010)
- Texture-based methods (2010-2017)
- Deep-learning-based methods (2017-2020)

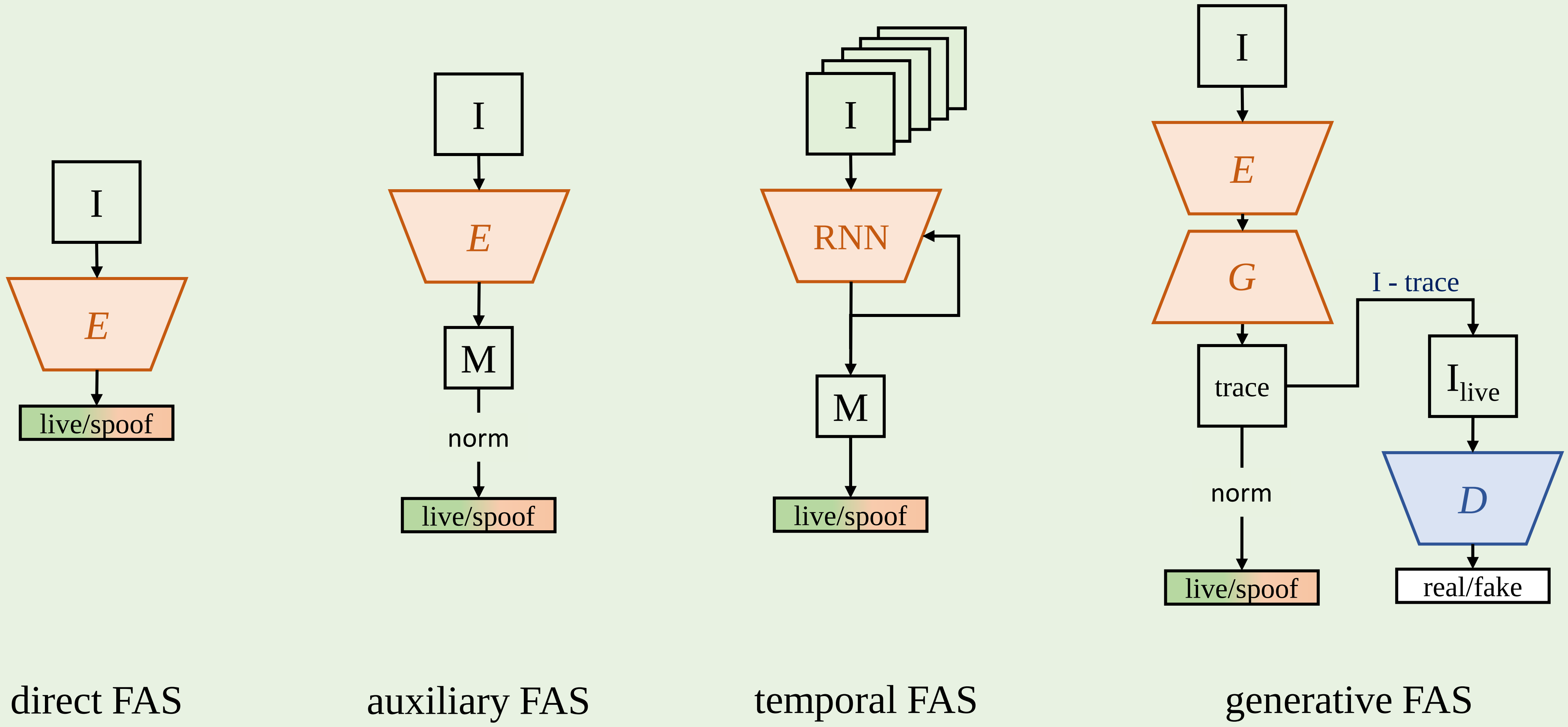
Texture-based Methods

- J. Maatta, et. al., Face Spoofing Detection from Single Images using Micro-Texture Analysis, *IJCB*, 2011.
- J. Galbally, et. al., Face Anti-Spoofing Based on General Image Quality Assessment, *ICPR*, 2014.
- Z. Boulkenafet, et. al., Face Anti-Spoofing Based on Color Texture Analysis, *ICIP*, 2015
- S. Liu, et. al., 3D Mask Face Anti-Spoofing with Remote Photoplethysmography, *ECCV*, 2016.
- Z. Boulkenafet, et. al., Face Anti-Spoofing Using Speeded Up Robust Features and Fisher Vector Encoding, *IEEE Signal Processing Letters*, 2017.
- A. Agarwal, et. al., Face anti-spoofing using Haralick features, *BTAS*, 2016.
- K. Patel, et. al., Secure face unlock: Spoof detection on smartphones, *TIFS*, 2016.
- K. Patel, et. al., Live face video vs. spoof face video: Use of moire patterns to detect replay video attacks, *ICB*, 2015.

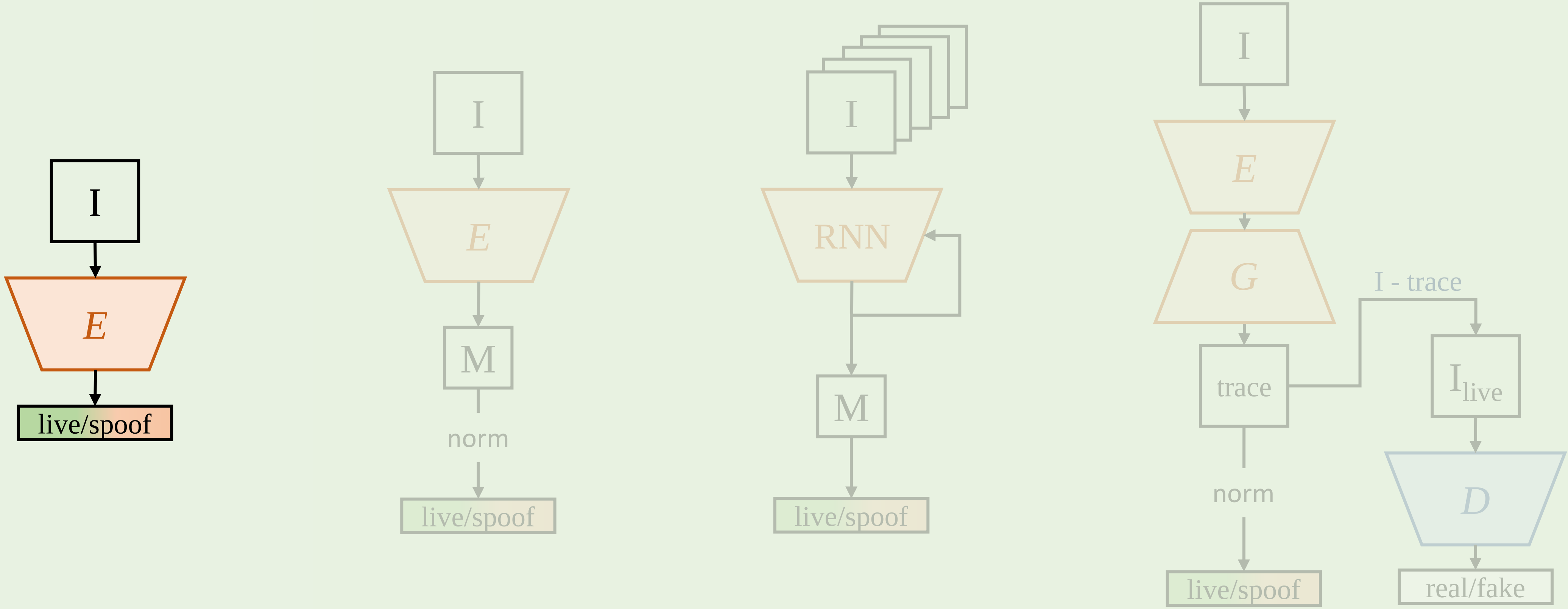
The Development

- Interaction-based methods (2006-2010)
- Texture-based methods (2010-2017)
- **Deep-learning-based methods (2017-2020)**

Deep-Learning-Based Methods



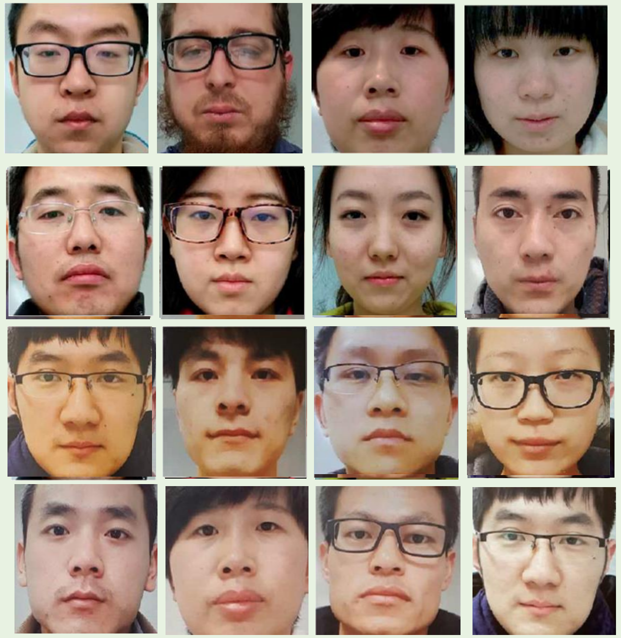
Deep-Learning-Based Methods

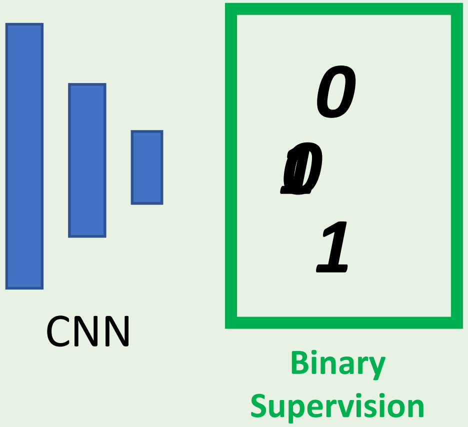


direct FAS auxiliary FAS temporal FAS generative FAS

Direct FAS

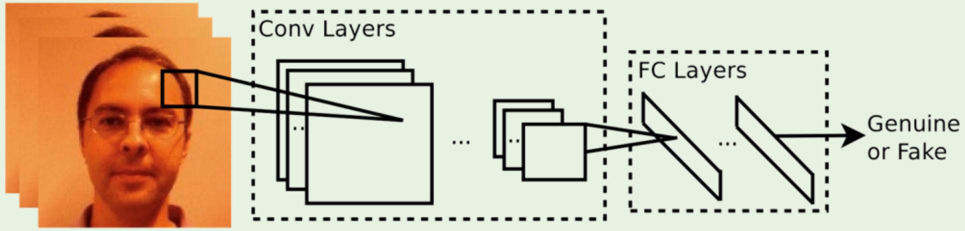
- CNN is trained to do a binary classification: live vs spoof

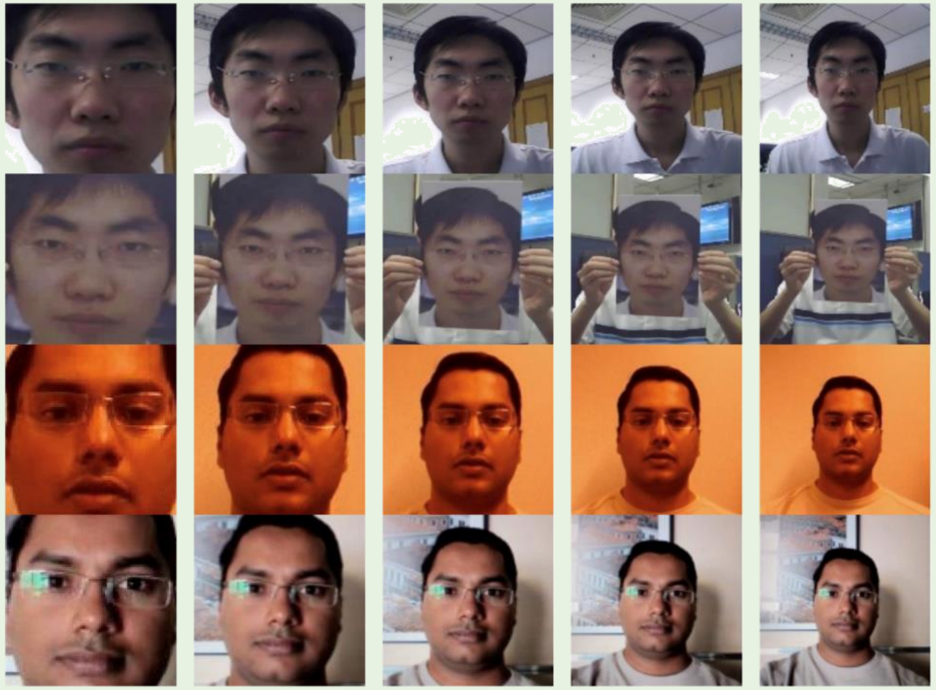




Direct FAS

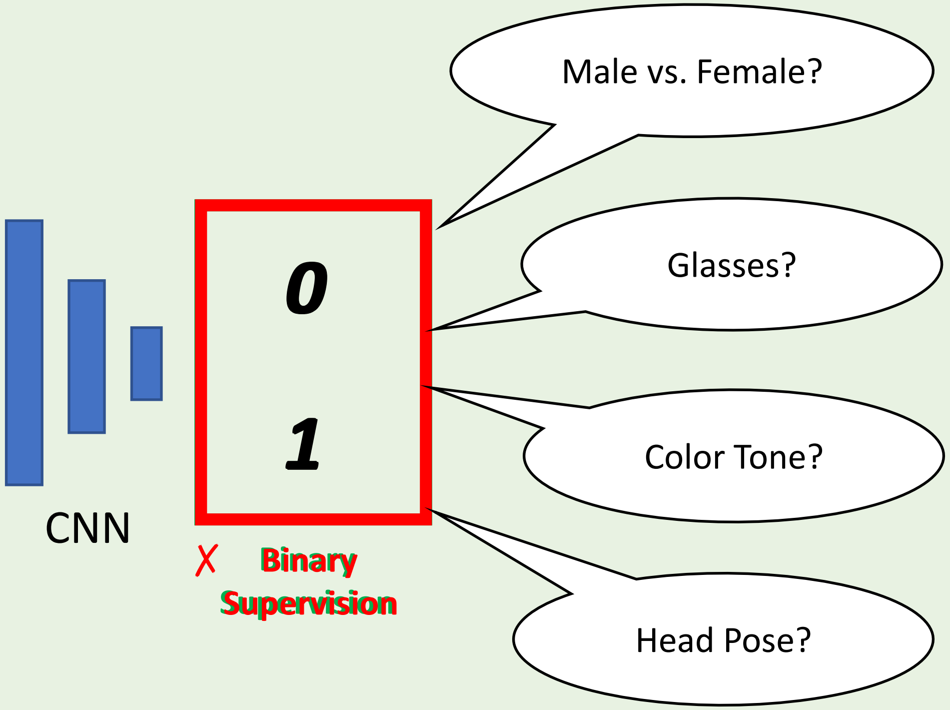
- MLP / CNN feature + SVM classifier
- Search different input to improve performance
  - Features (LBP, IQM)
  - Face scales
  - Color spaces (RGB, HSV, YCbCr)





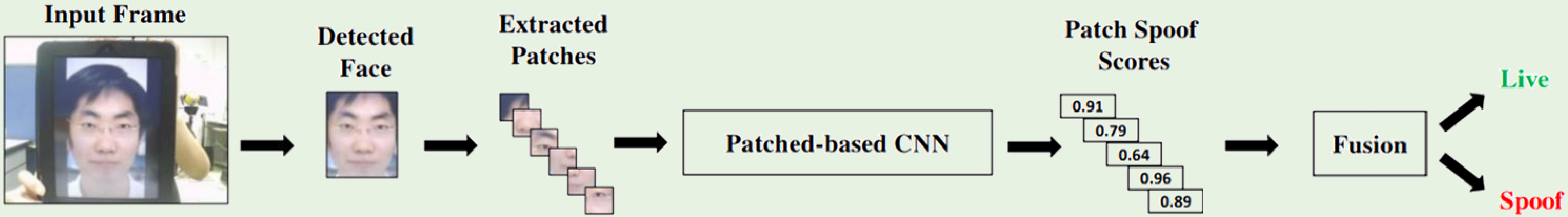
1. Yang et. al., Learn Convolutional Neural Network for Face Anti-Spoofing. arXiv 2014.
2. Xu et. al., Learning temporal features using LSTM-CNN architecture for face anti-spoofing. ACPR 2015.

Drawbacks


CNN
0
1
✗ Binary Supervision
Male vs. Female?
Glasses?
Color Tone?
Head Pose?

Patch-based CNNs

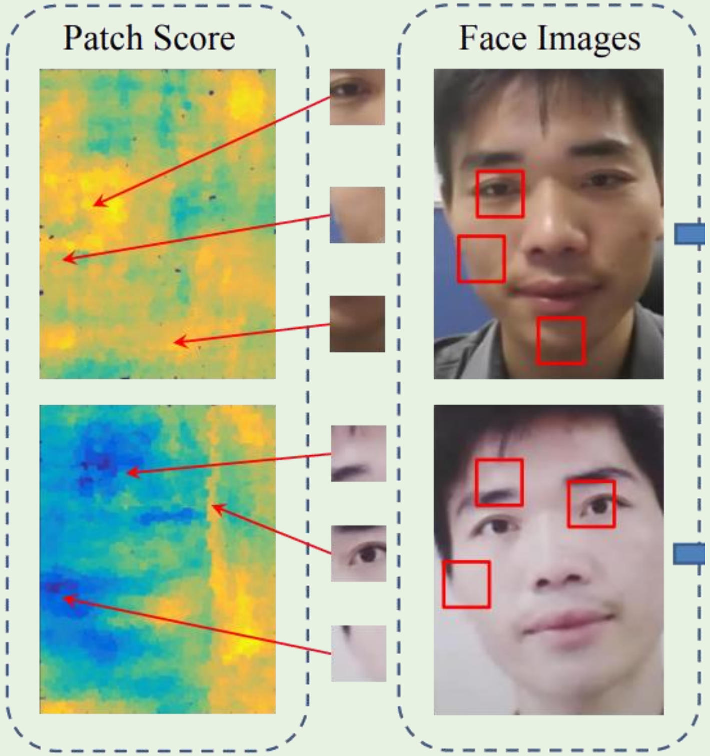
- CNN is trained to do a binary classification for each face patch



1. Yousef Atoum et. al., Face Anti-Spoofing Using Patch and Depth-Based CNNs, IJCB, 2017
2. Gustavo Botelho de Souza et. al., On the Learning of Deep Local Features for Robust Face Spoofing Detection, SIBGRAPI, 2018
3. Xiao Yang et. al., Face Anti-Spoofing: Model Matters, So Does Data, CVPR, 2019
4. DRL-FAS: A Novel Framework Based on Deep Reinforcement Learning for Face Anti-Spoofing , arXiv, 2020
5. Look Locally Infer Globally: A Generalizable Face Anti-Spoofing Approach, arXiv, 2020

Patch-based CNNs

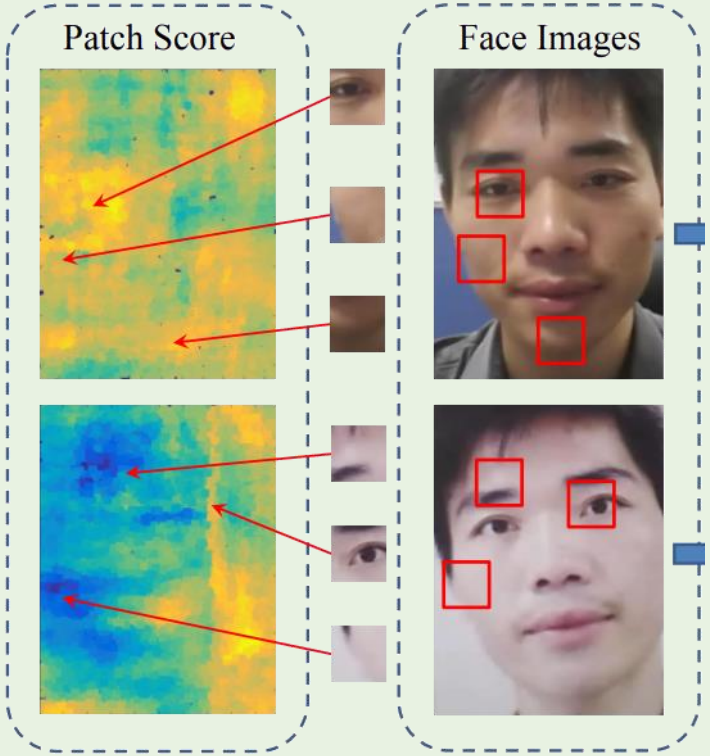
- Benefits
  - Mitigate overfitting (+ training samples)
  - Light-weight network
- Challenges
  - Efficiency *v.s.* performance?
  - End-to-end training
  - Patch scales



1. Yousef Atoum et. al., Face Anti-Spoofing Using Patch and Depth-Based CNNs, IJCB, 2017

Patch-based CNNs

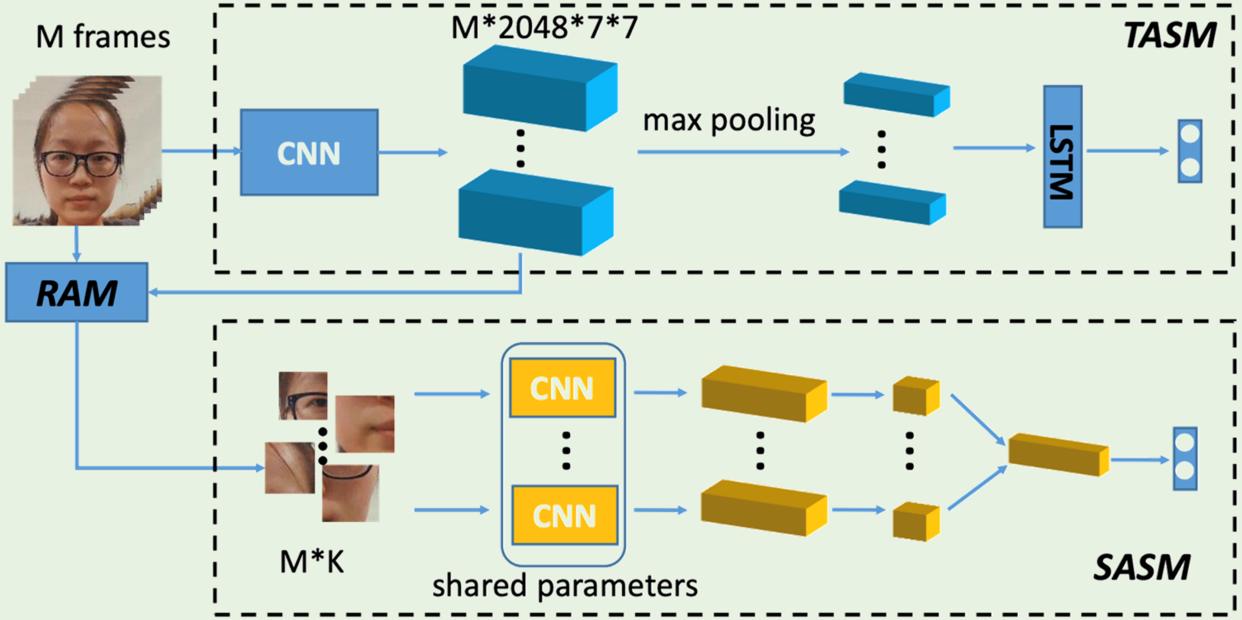
- Benefits
  - Mitigate overfitting (+ training samples)
  - Light-weight network
- Challenges
  - Efficiency *v.s.* performance?
  - End-to-end training
  - Patch scales



1. Yousef Atoum et. al., Face Anti-Spoofing Using Patch and Depth-Based CNNs, IJCB, 2017

Global + Patch CNN

- Stage 1: global face training (TASM)
  - Learn features for RAM
- Stage 2: local region training (RAM+SASM)
  - RAM: region proposals
  - SASM: patch-based CMM
- Testing: TASM+RAM+SASM

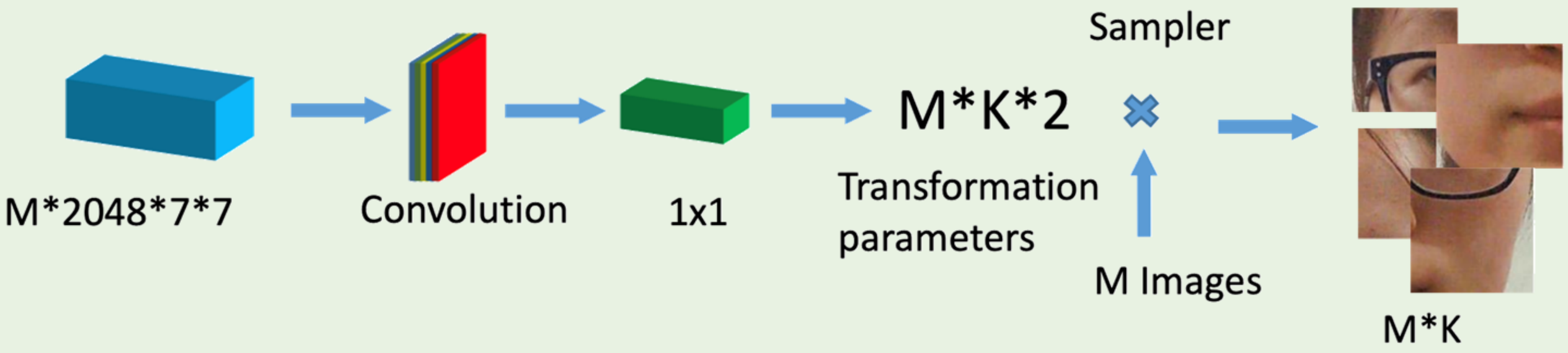


1. Yang et. al., Face Anti-Spoofing: Model Matters, So Does Data, CVPR 2019

Region Attention Module (RAM)

Locates the discriminative and significant sub-regions

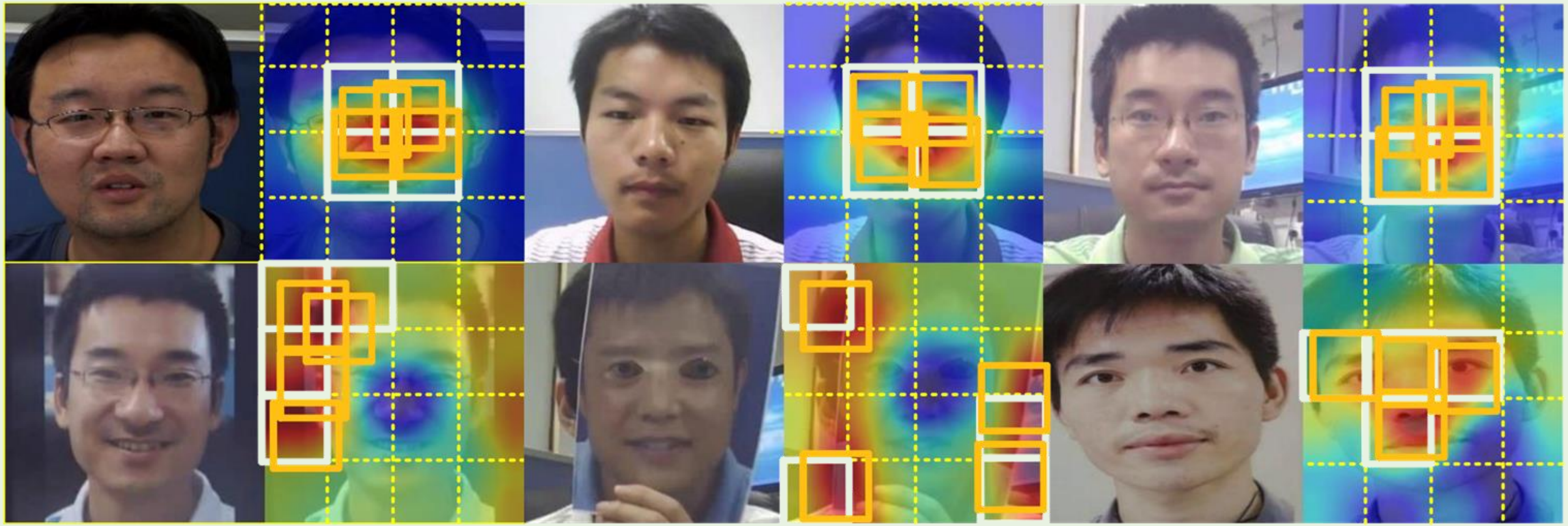
- RAM output 2*K parameters: offsets and translation of K patches



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

Examples of Attention

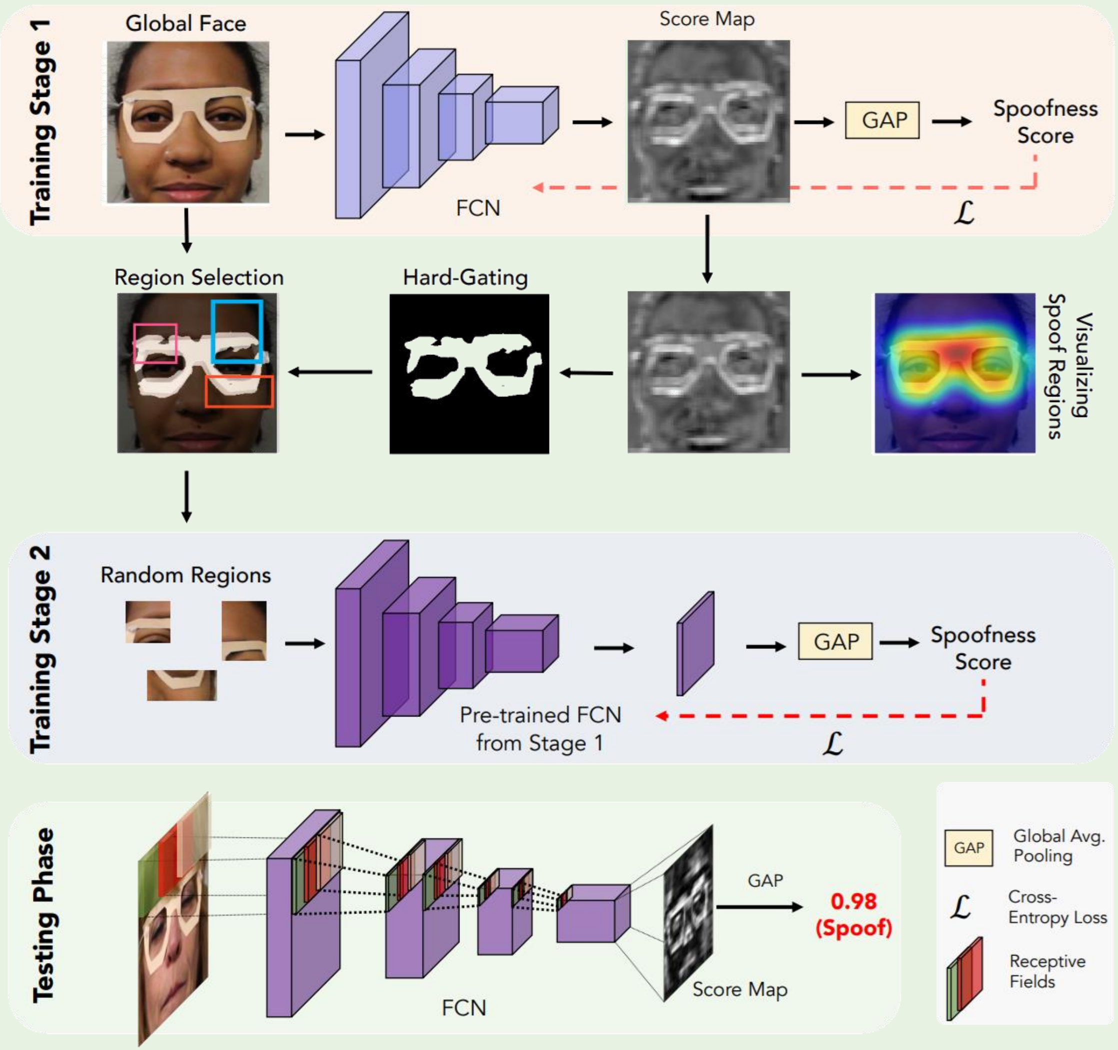
- Live attentions are on face
- Spoof attentions are diverse



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

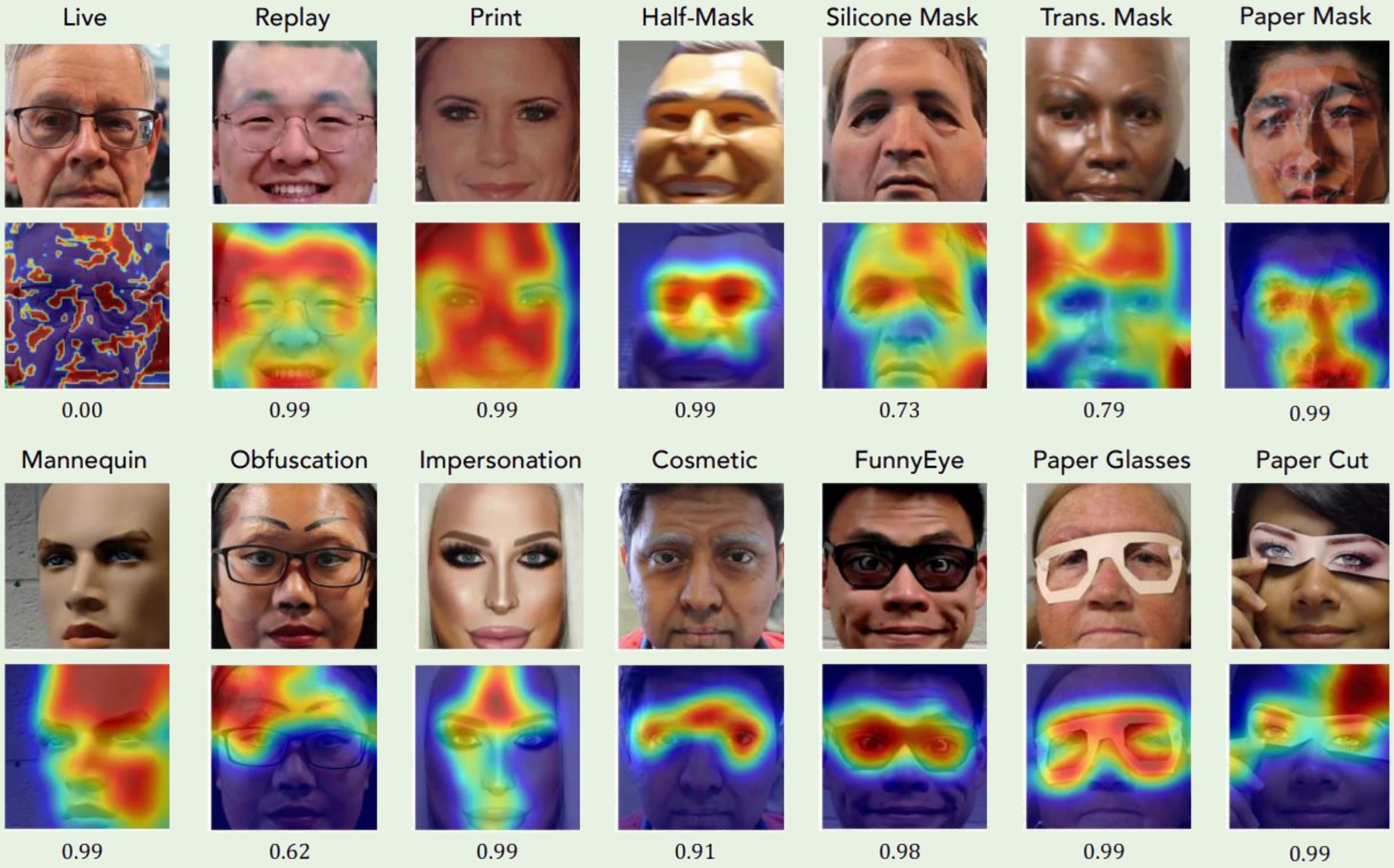
Global + Patch CNN 2

- Apply fully convolutional network (FCN)
- Stage 1: global face training
  - Provide better locations to crop patches
- Stage 2: local region training
  - Random sizes/scales
- Testing: Global face
  - Improve efficiency with GPU testing



1. Look Locally Infer Globally: A Generalizable Face Anti-Spoofing Approach, arXiv, 2020

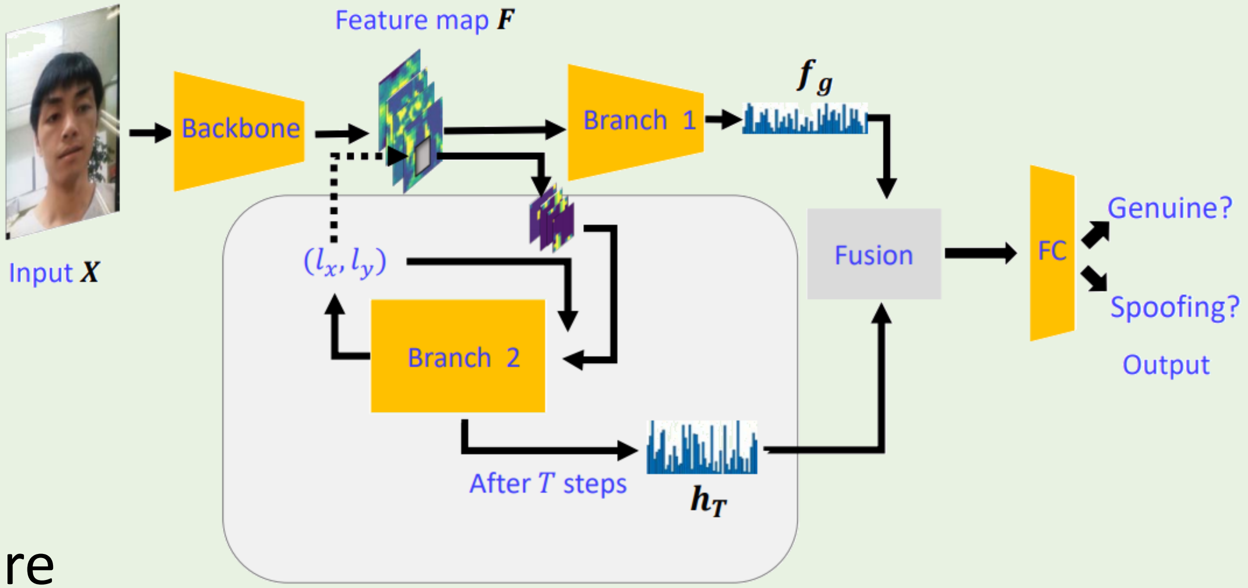
Global + Patch CNN 2



1. Look Locally Infer Globally: A Generalizable Face Anti-Spoofing Approach, arXiv, 2020

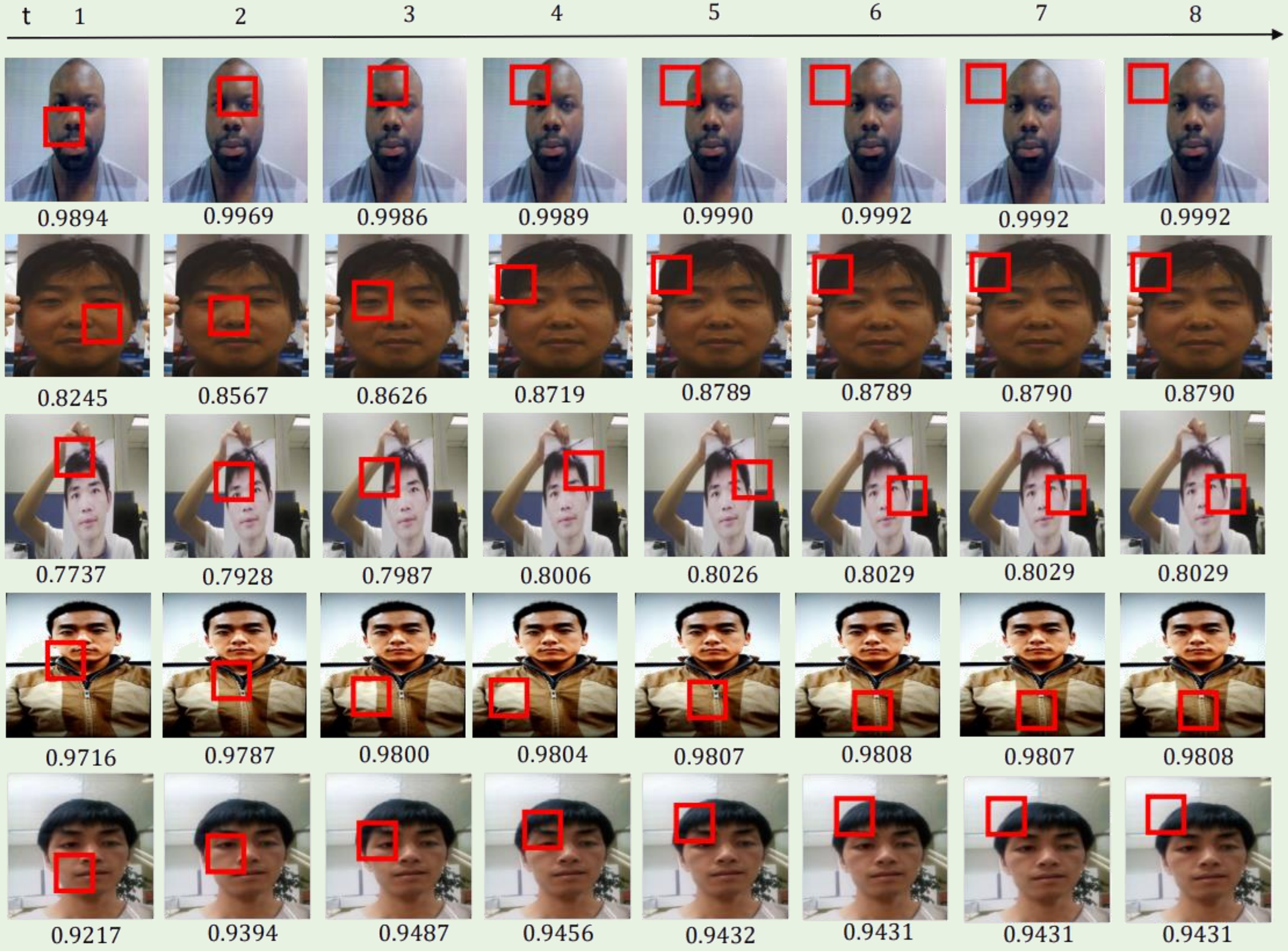
Global + Patch CNN 3

- Apply deep reinforcement learning to choose the best patch for decision
- Stage 1: global feature training
- Stage 2: find the best local patch
  - Via RNN
  - Trained by DRL as finding patch w/ higher score
- Testing: Global feature + best local feature



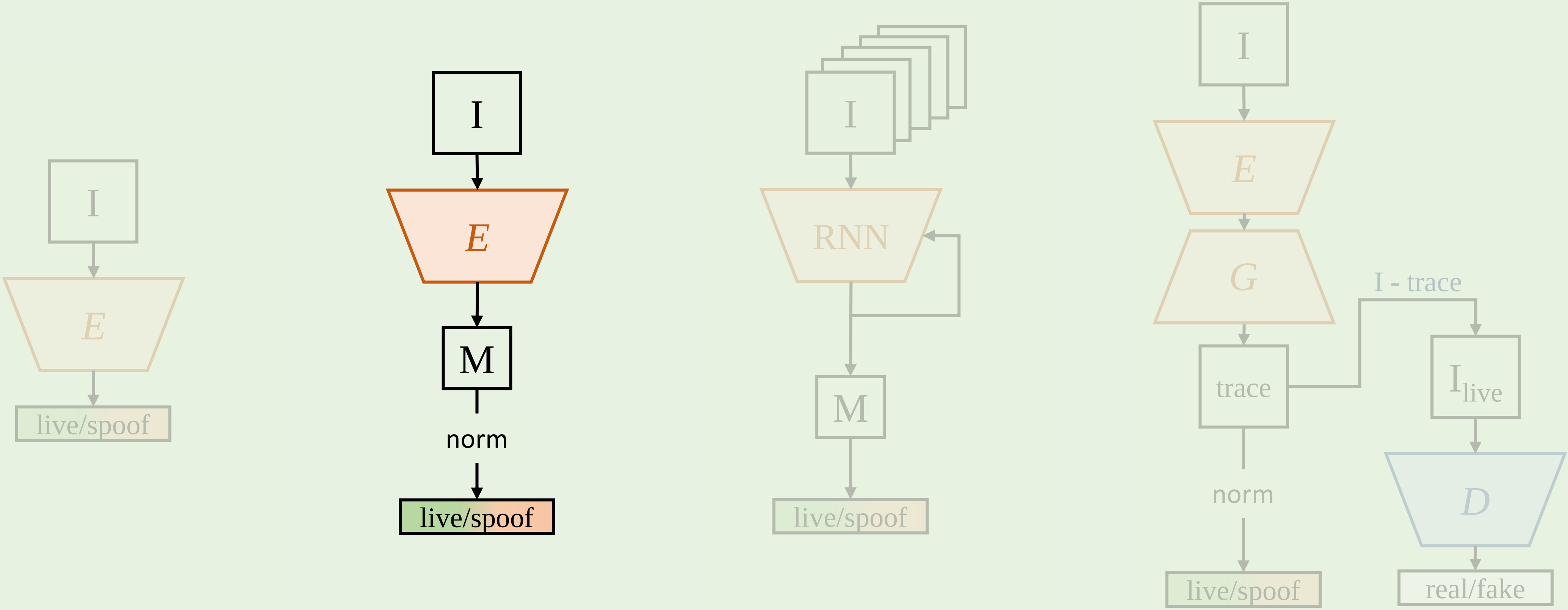
1. DRL-FAS: A Novel Framework Based on Deep Reinforcement Learning for Face Anti-Spoofing , arXiv, 2020

Global + Patch CNN 3



1. DRL-FAS: A Novel Framework Based on Deep Reinforcement Learning for Face Anti-Spoofing , arXiv, 2020

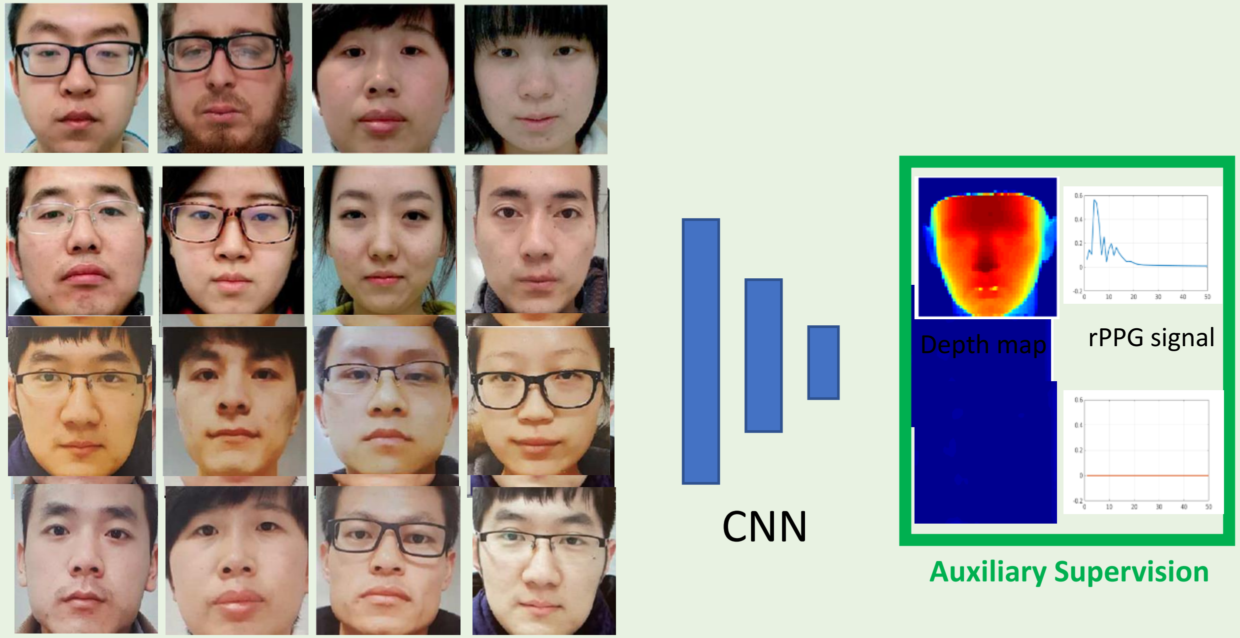
Deep-Learning-Based Methods



direct FAS auxiliary FAS temporal FAS generative FAS

Auxiliary FAS

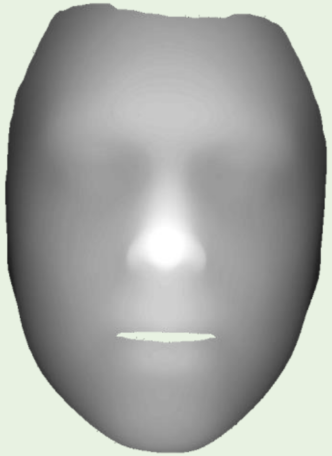
- CNN is trained to do auxiliary tasks, which can help face anti-spoofing



1. Face anti-spoofing using patch and depth-based CNNs. IJCB 2017.
2. Learning deep models for face anti-spoofing: binary or auxiliary supervision. *CVPR 2018.*
3. Face de-spoofing: anti-spoofing via noise modeling. *ECCV* 2018.
4. Exploiting temporal and depth information for multi-frame face anti-spoofing, arXiv 2019
5. Aurora guard: real-time face anti-spoofing via light reflection, arXiv 2019
6. Meta Anti-spoofing: Learning to Learn in Face Anti-spoofing, arXiv 2019
7. Multi-adversarial discriminative deep domain generalization for face presentation attack detection. CVPR 2019
8. Deep tree learning for zero-shot face anti-spoofing. CVPR 2019

Depth Estimation

- Can CNN learn specific tasks that contain anti-spoofing information?



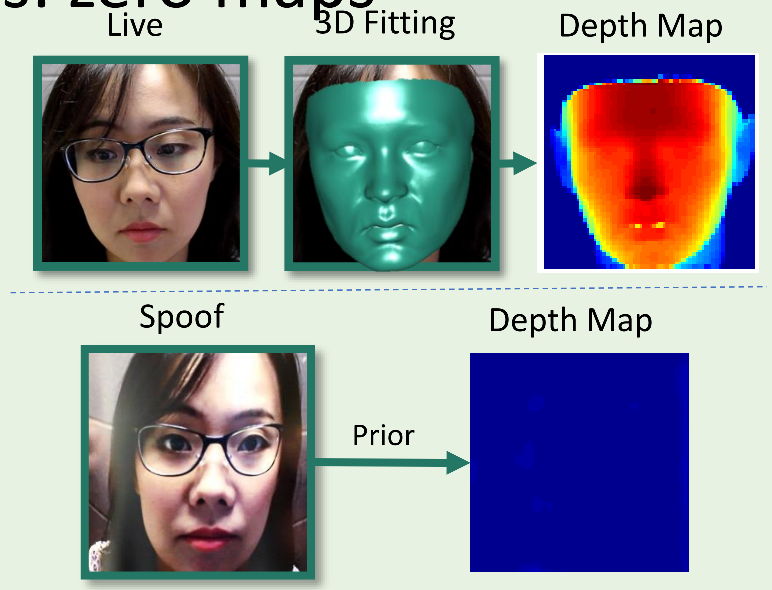
Rich Depth Information

Flat Surface

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

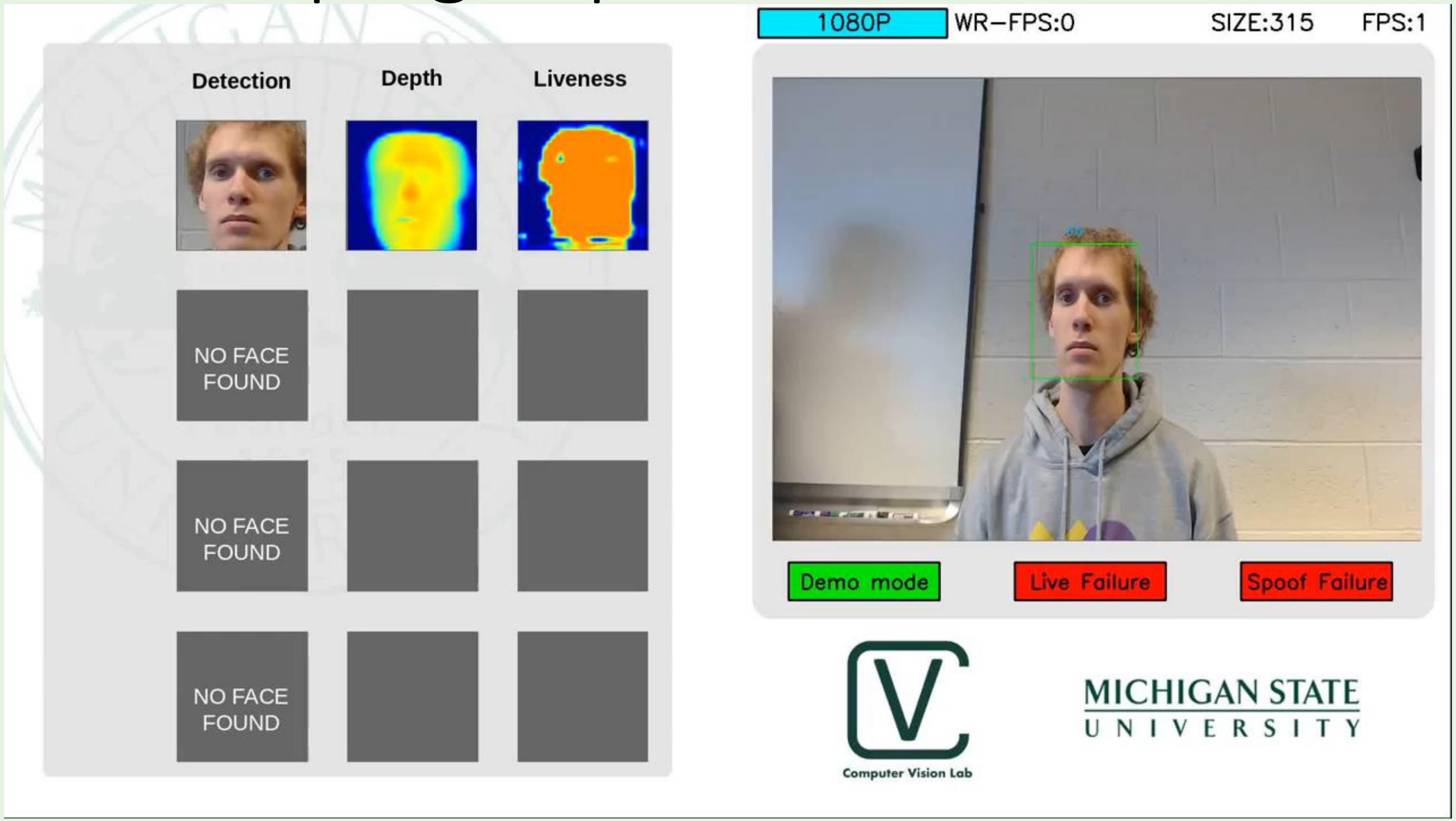
How to Obtain Depth Map Label?

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



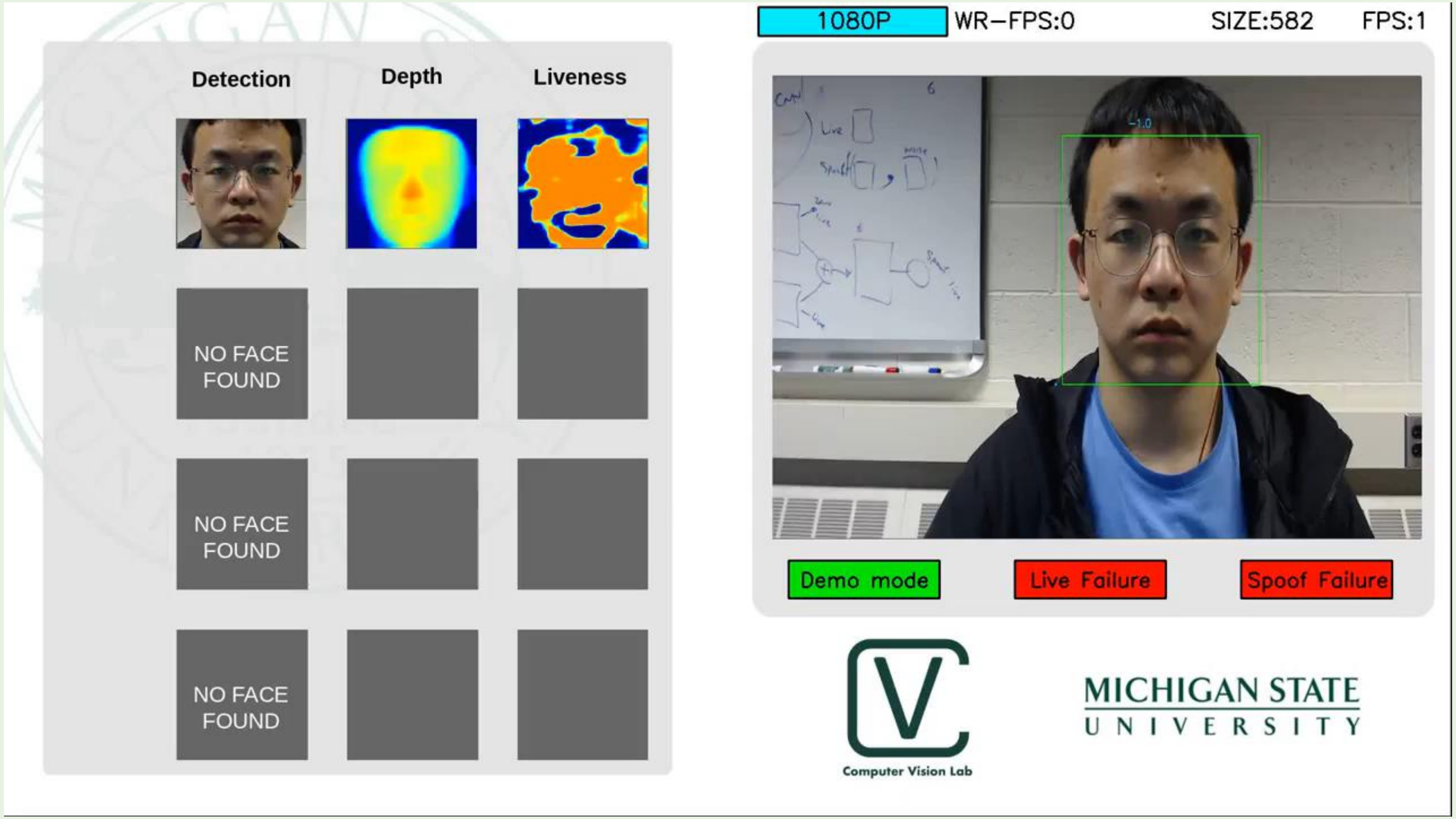
1. Y. Liu, A. Jourabloo, and X. Liu. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. *CVPR 2018*
2. Y. Liu, A. Jourabloo, W. Ren, and X. Liu. Dense Face Alignment. *ICCVW 2017.*

What If Warping Paper?



1. https://www.youtube.com/watch?v=b3gUwkJJuRs

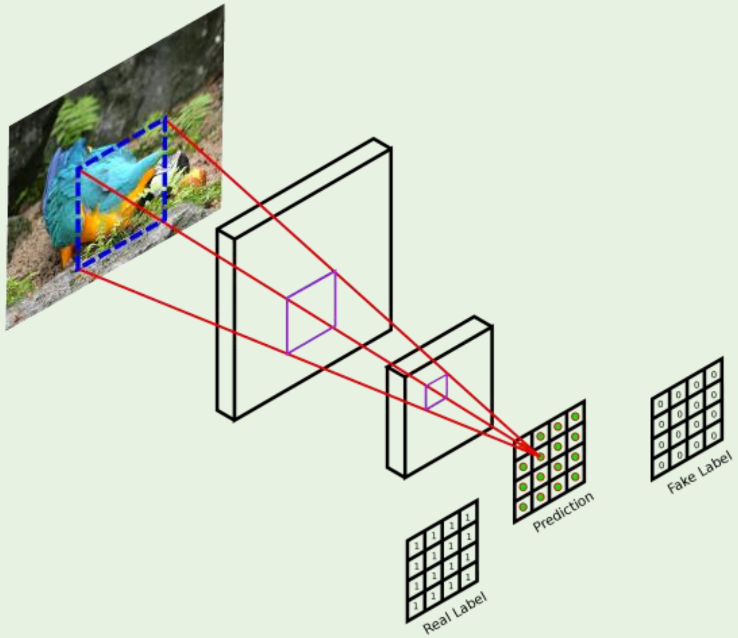
What If Warping Paper?



1. https://www.youtube.com/watch?v=OQN0VUWUxyc

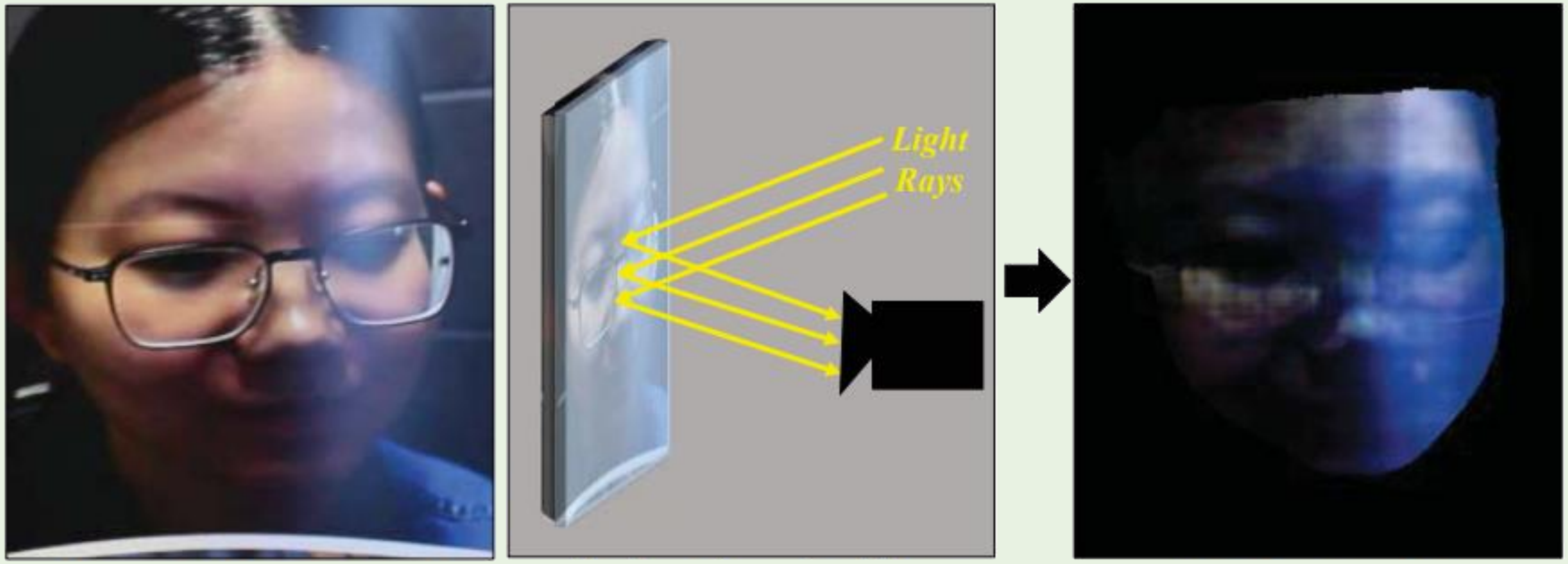
Why It Works?

- Local responses
- Multi-scale features
- Addition knowledge (> 0/1 map)



Reflection Estimation

- Can CNN learn specific tasks that contain anti-spoofing information?

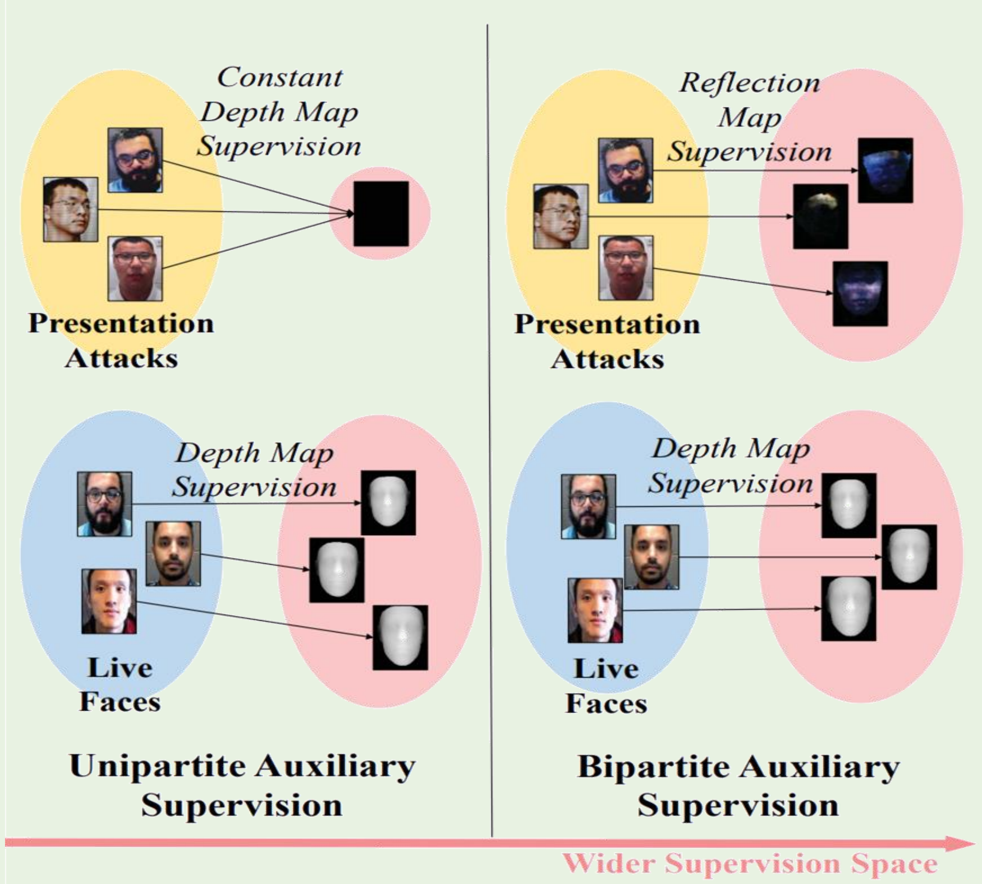


Presentation Attack Reflection Artifact Reflection Map

1. T. Kim. BASN: Enriching Feature Representation Using Bipartite Auxiliary Supervisions for Face Anti-Spoofing. *ICCVW 2019*
2. Z. Yu, et. al., Face Anti-Spoofing with Human Material Perception*, ECCV 2020*

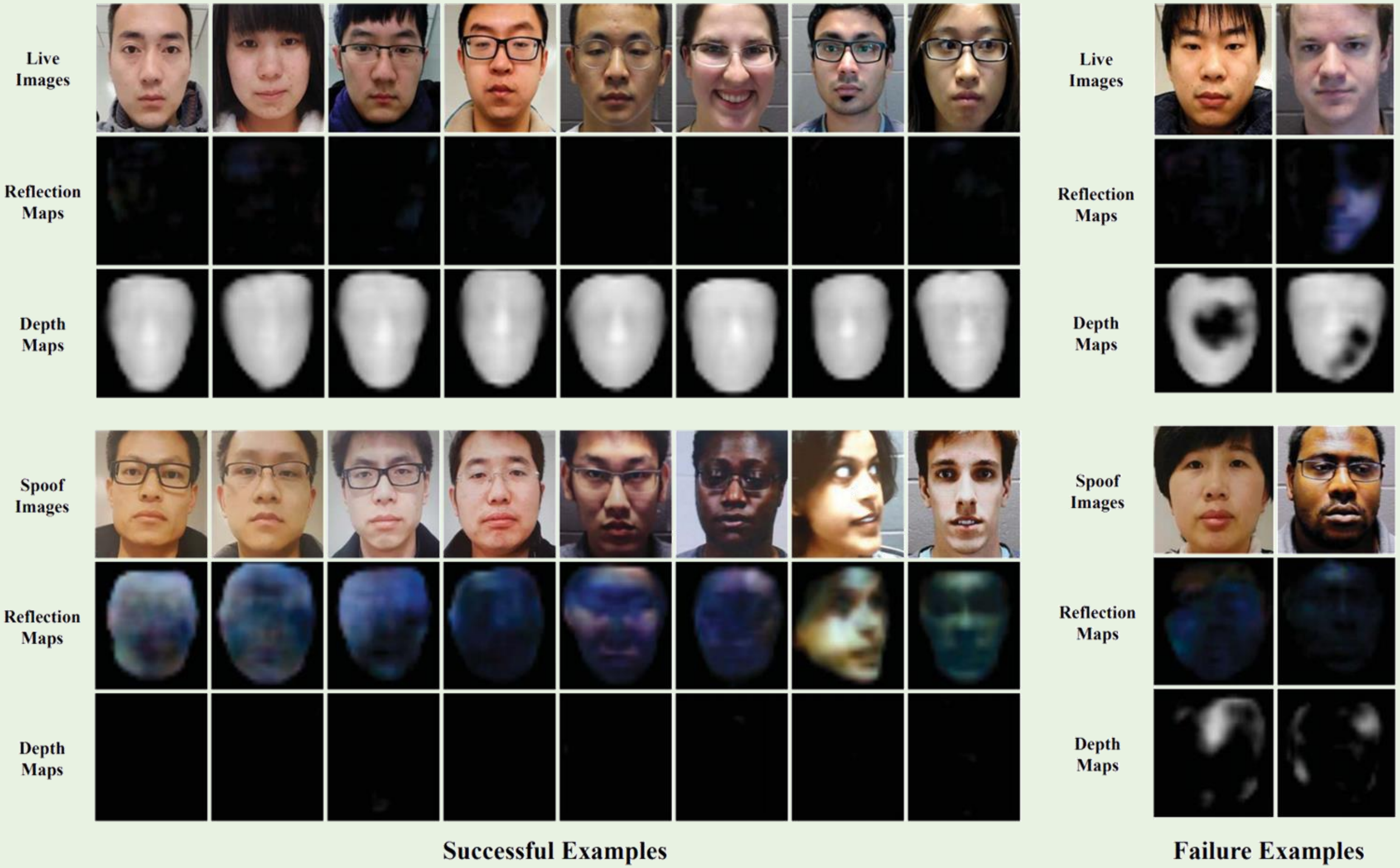
Reflection Estimation

- Depth map: unipartite supervision
- Depth + reflection: bipartite supervision
- Reflection ground truth provided by [2]



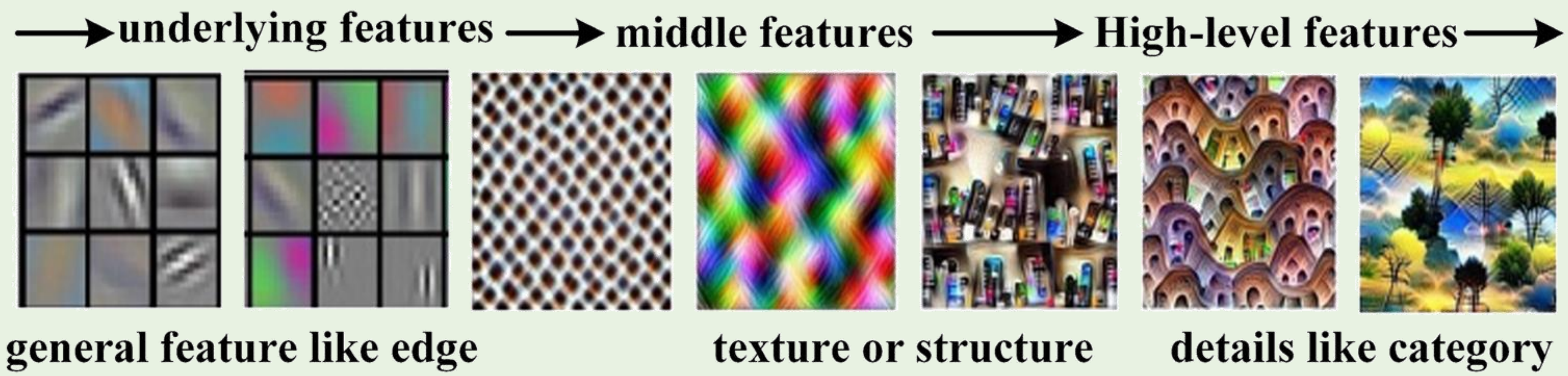
1. T. Kim. BASN: Enriching Feature Representation Using Bipartite Auxiliary Supervisions for Face Anti-Spoofing. *ICCVW 2019*
2. X. Zhang, et. al., Single image reflection separation with perceptual losses. CVPR, 2018.
3. Z. Yu, et. al., Face Anti-Spoofing with Human Material Perception*, ECCV 2020*

Reflection Estimation



1. T. Kim. BASN: Enriching Feature Representation Using Bipartite Auxiliary Supervisions for Face Anti-Spoofing. *ICCVW 2019*

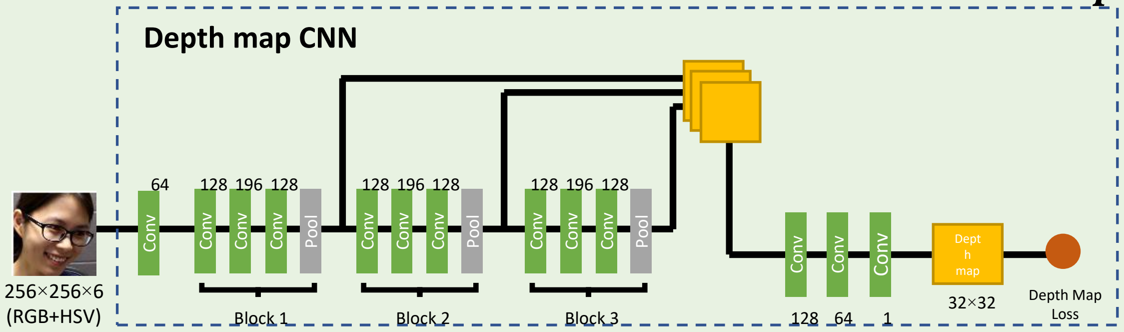
Network Designs



1. Y. Liu, A. Jourabloo, and X. 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: $\mathcal{L}_{depth} = \left\| D_{pred} - D_0 \right\|_F^1$

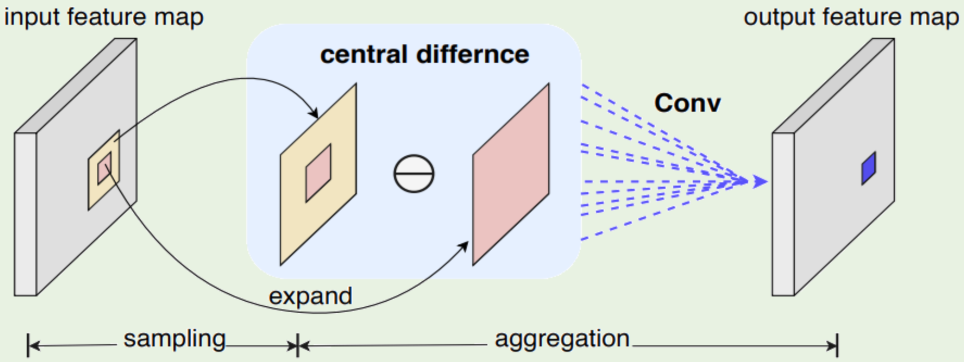


1. Y. Liu, A. Jourabloo, and X. Liu. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. *CVPR 2018*

Central Difference Conv

- Vanilla conv: $y(p_0) = \sum_{p_n \in \mathcal{R}} w(p_n) \cdot x(p_0 + p_n)$
- Central difference conv: $y(p_0) = \sum_{p_n \in \mathcal{R}} w(p_n) \cdot (x(p_0 + p_n) - x(p_0))$
- Final design:

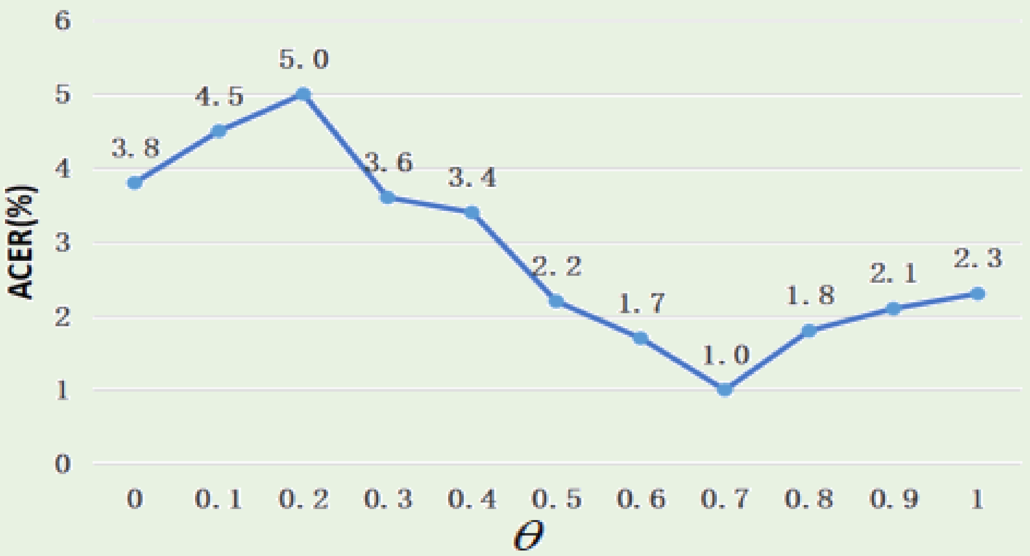
$$y(p_0) = \underbrace{\theta \cdot \sum_{p_n \in \mathcal{R}} w(p_n) \cdot (x(p_0 + p_n) - x(p_0))}_{\text{central difference convolution}} + (1-\theta) \cdot \underbrace{\sum_{p_n \in \mathcal{R}} w(p_n) \cdot x(p_0 + p_n)}_{\text{vanilla convolution}},$$

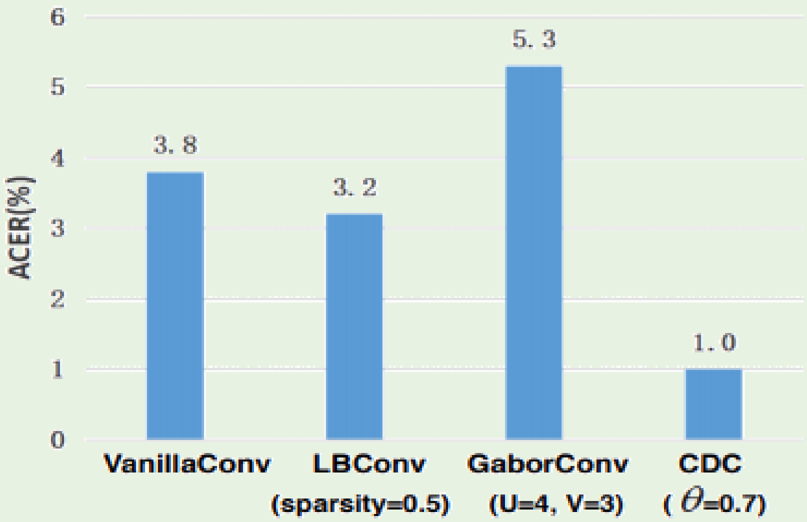


1. Zitong Yu et al., Searching Central Difference Convolutional Networks for Face Anti-Spoofing, CVPR2020

Central Difference Conv

- Different theta
- Different various convolution

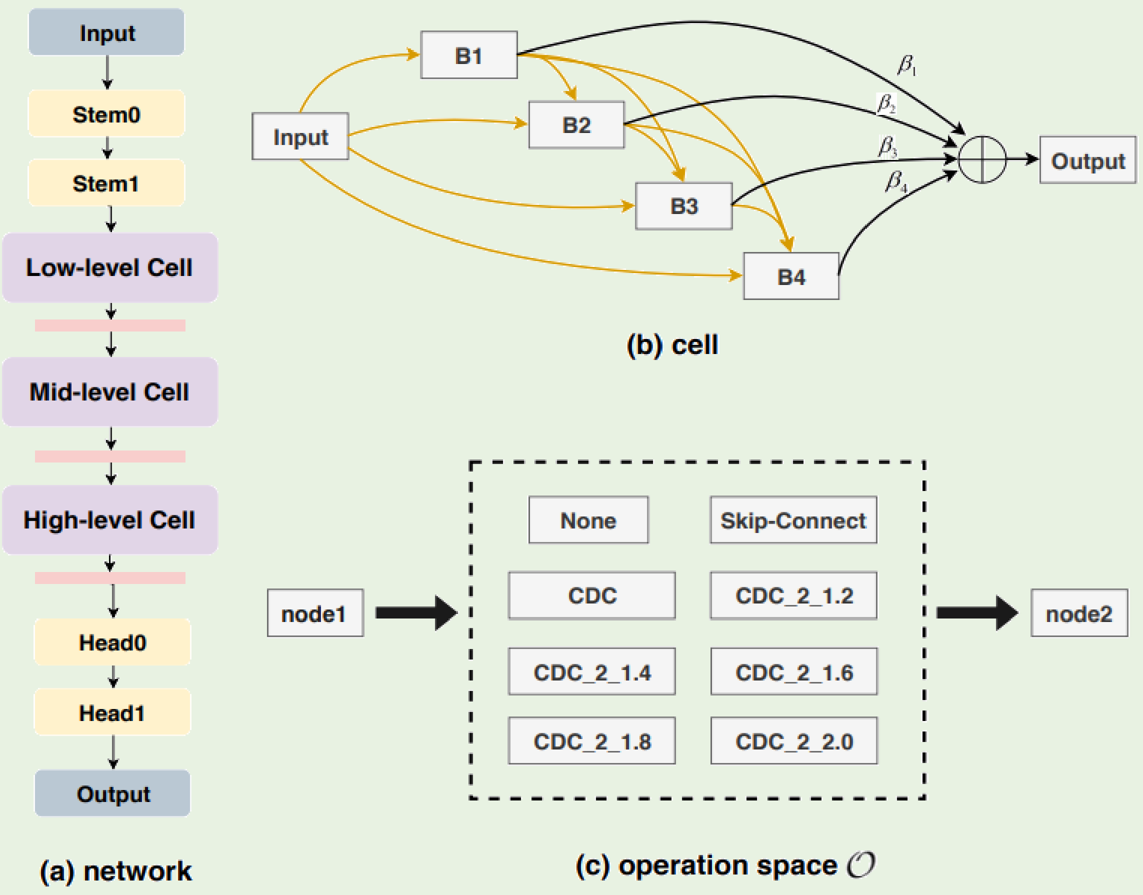




1. Zitong Yu et al., Searching Central Difference Convolutional Networks for Face Anti-Spoofing, CVPR2020

Network Architecture Search

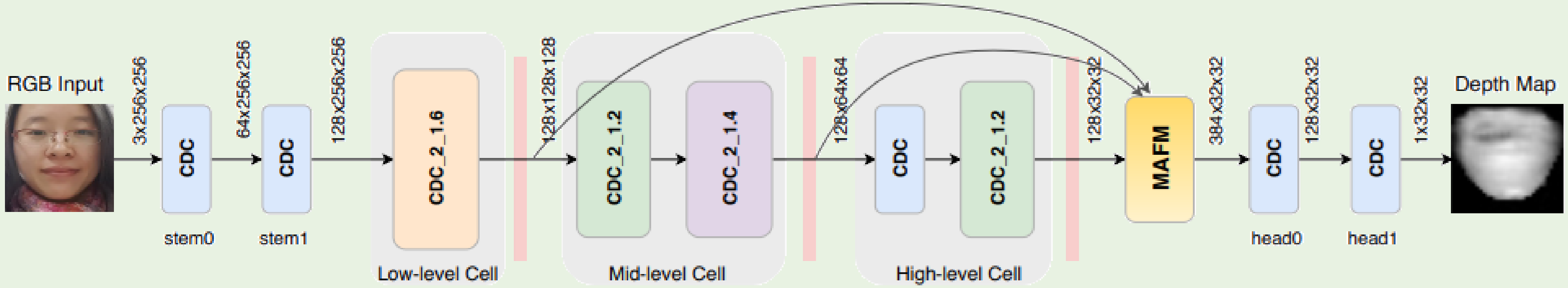
- (a) net frame
- (b) cell structure
- (c) node search space



1. Zitong Yu et al., Searching Central Difference Convolutional Networks for Face Anti-Spoofing, CVPR2020

NAS Result

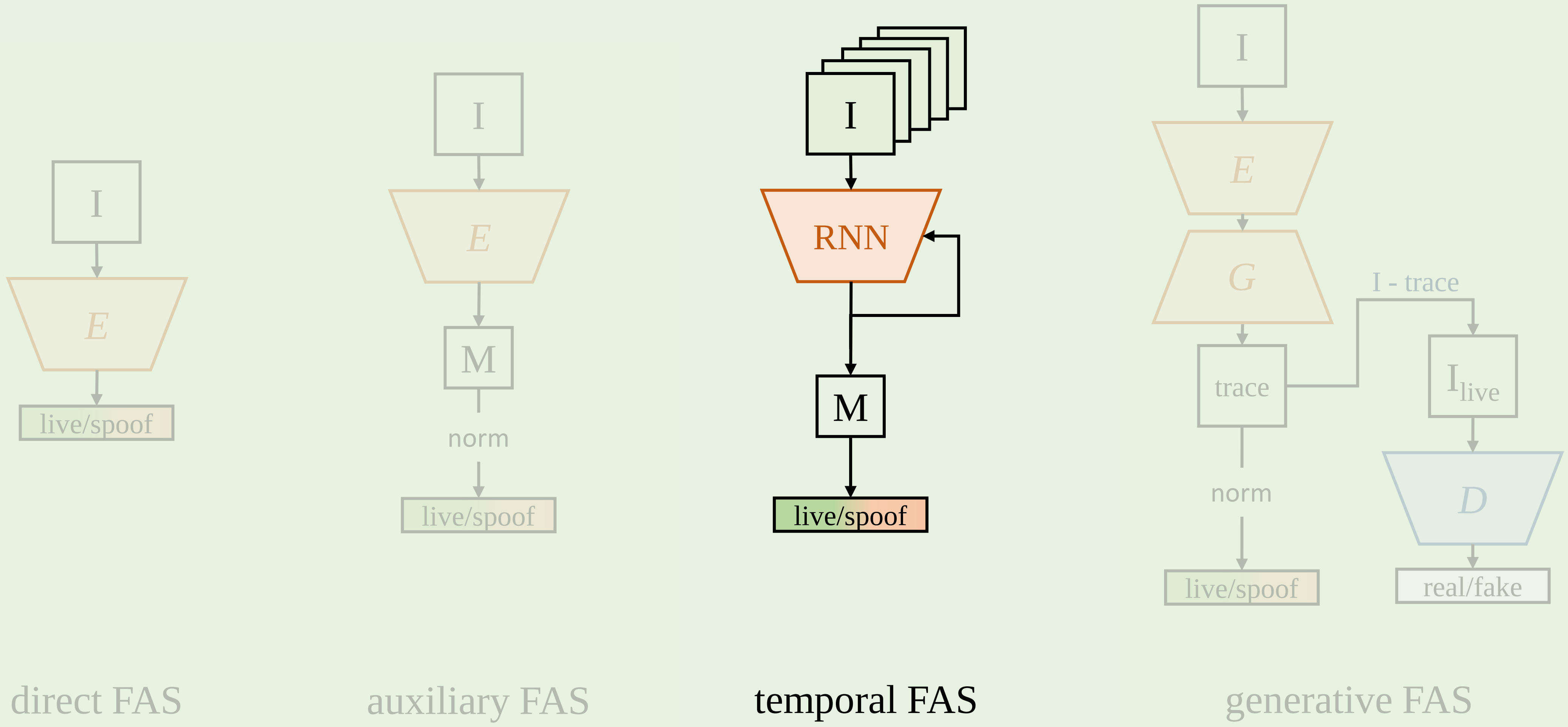
- (a) net frame
- (b) cell structure
- (c) node search space



Prot.	Method	APCER(%)	BPCER(%)	ACER(%)
1	GRADIANT [6]	1.3	12.5	6.9
	STASN [62]	1.2	2.5	1.9
	Auxiliary [36]	1.6	1.6	1.6
	FaceDs [26]	1.2	1.7	1.5
	FAS-TD [56]	2.5	0.0	1.3
	DeepPixBiS [20]	0.8	0.0	0.4
	CDCN (Ours)	0.4	1.7	1.0
	CDCN++ (Ours)	0.4	0.0	**0.2**
2	DeepPixBiS [20]	11.4	0.6	6.0
	FaceDs [26]	4.2	4.4	4.3
	Auxiliary [36]	2.7	2.7	2.7
	GRADIANT [6]	3.1	1.9	2.5
	STASN [62]	4.2	0.3	2.2
	FAS-TD [56]	1.7	2.0	1.9
	CDCN (Ours)	1.5	1.4	1.5
	CDCN++ (Ours)	1.8	0.8	**1.3**
3	DeepPixBiS [20]	11.7±19.6	10.6±14.1	11.1±9.4
	FAS-TD [56]	5.9±1.9	5.9±3.0	5.9±1.0
	GRADIANT [6]	2.6±3.9	5.0±5.3	3.8±2.4
	FaceDs [26]	4.0±1.8	3.8±1.2	3.6±1.6
	Auxiliary [36]	2.7±1.3	3.1±1.7	2.9±1.5
	STASN [62]	4.7±3.9	0.9±1.2	2.8±1.6
	CDCN (Ours)	2.4±1.3	2.2±2.0	2.3±1.4
	CDCN++ (Ours)	1.7±1.5	2.0±1.2	**1.8±0.7**
4	DeepPixBiS [20]	36.7±29.7	13.3±14.1	25.0±12.7
	GRADIANT [6]	5.0±4.5	15.0±7.1	10.0±5.0
	Auxiliary [36]	9.3±5.6	10.4±6.0	9.5±6.0
	FAS-TD [56]	14.2±8.7	4.2±3.8	9.2±3.4
	STASN [62]	6.7±10.6	8.3±8.4	7.5±4.7
	FaceDs [26]	1.2±6.3	6.1±5.1	5.6±5.7
	CDCN (Ours)	4.6±4.6	9.2±8.0	6.9±2.9
	CDCN++ (Ours)	4.2±3.4	5.8±4.9	**5.0±2.9**

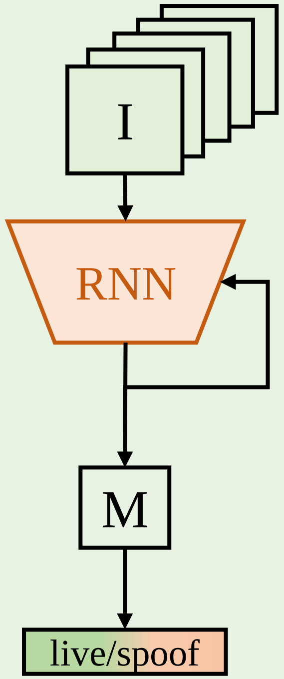
1. Zitong Yu et al., Searching Central Difference Convolutional Networks for Face Anti-Spoofing, CVPR2020

Deep-Learning-Based Methods



Temporal FAS

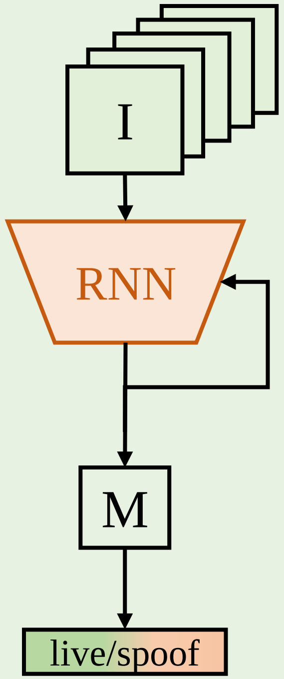
- CNN is trained to leverage temporal information with spatial information



1. Xu et. al., Learning temporal features using LSTM-CNN architecture for face anti-spoofing. ACPR 2015.
2. Gan et. al., 3D Convolutional Neural Network Based on Face Anti-spoofing, ICMIP 2017
3. Yang et. al., Face Anti-Spoofing: Model Matters, So Does Data, CVPR 2019
4. Feng et. al., Integration of image quality and motion cues for face anti-spoofing: A neural network approach. JVCI 2016.
5. Liu et. al., Learning deep models for face anti-spoofing: binary or auxiliary supervision. CVPR 2018.
6. Zhang et. al., Exploiting temporal and depth information for multi-frame face anti-spoofing, arXiv 2019
7. Liu et. al., 3D Mask Face Anti-spoofing with Remote Photoplethysmography, ECCV 2016
8. Liu et. al., Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection, ECCV 2018
9. Xu et. al., On Improving Temporal Consistency for Online Face Liveness Detection System. arXiv 2020

Temporal FAS

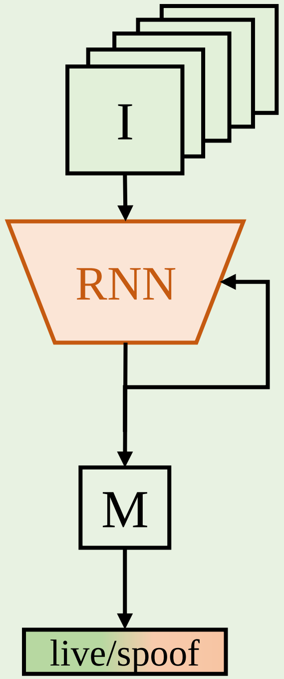
- Vanilla RNN [1,2,3]
- Temporal features [4]
- Auxiliary temporal tasks [5,7,8]
- Temporal consistency [6,9]



1. Xu et. al., Learning temporal features using LSTM-CNN architecture for face anti-spoofing. ACPR 2015.
2. Gan et. al., 3D Convolutional Neural Network Based on Face Anti-spoofing, ICMIP 2017
3. Yang et. al., Face Anti-Spoofing: Model Matters, So Does Data, CVPR 2019
4. Feng et. al., Integration of image quality and motion cues for face anti-spoofing: A neural network approach. JVCI 2016.
5. Liu et. al., Learning deep models for face anti-spoofing: binary or auxiliary supervision. CVPR 2018.
6. Zhang et. al., Exploiting temporal and depth information for multi-frame face anti-spoofing, arXiv 2019
7. Liu et. al., 3D Mask Face Anti-spoofing with Remote Photoplethysmography, ECCV 2016
8. Liu et. al., Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection, ECCV 2018
9. Xu et. al., On Improving Temporal Consistency for Online Face Liveness Detection System. arXiv 2020

Temporal FAS

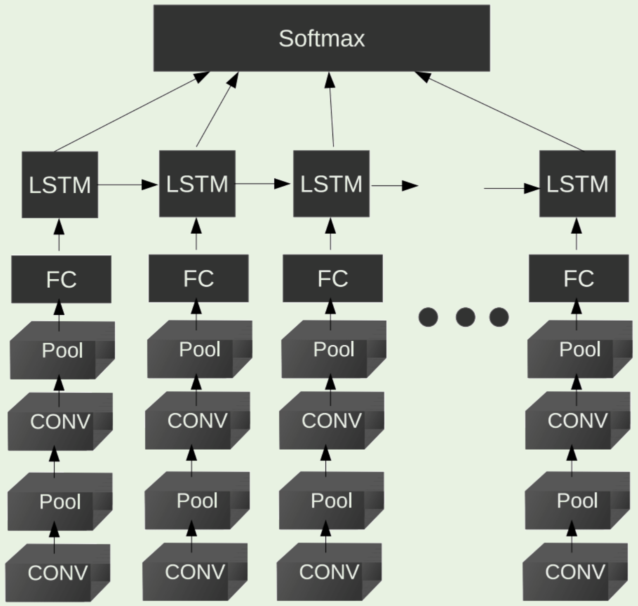
- Vanilla RNN [1,2,3]
- Temporal features [4]
- Auxiliary temporal tasks [5,7,8]
- Temporal consistency [6,9]

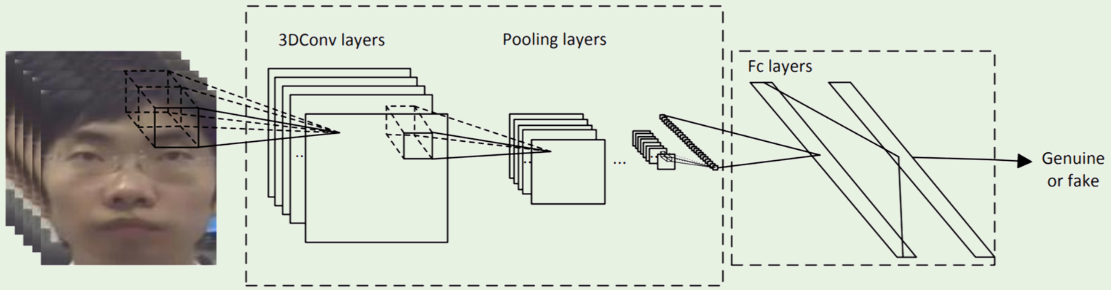


1. Xu et. al., Learning temporal features using LSTM-CNN architecture for face anti-spoofing. ACPR 2015.
2. Gan et. al., 3D Convolutional Neural Network Based on Face Anti-spoofing, ICMIP 2017
3. Yang et. al., Face Anti-Spoofing: Model Matters, So Does Data, CVPR 2019
4. Feng et. al., Integration of image quality and motion cues for face anti-spoofing: A neural network approach. JVCI 2016.
5. Liu et. al., Learning deep models for face anti-spoofing: binary or auxiliary supervision. CVPR 2018.
6. Zhang et. al., Exploiting temporal and depth information for multi-frame face anti-spoofing, arXiv 2019
7. Liu et. al., 3D Mask Face Anti-spoofing with Remote Photoplethysmography, ECCV 2016
8. Liu et. al., Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection, ECCV 2018
9. Xu et. al., On Improving Temporal Consistency for Online Face Liveness Detection System. arXiv 2020

Vanilla RNN

- Directly feed multiple frames to network
  - RNN, LSTM → binary classification
  - 3D Convolution
  - Concatenation

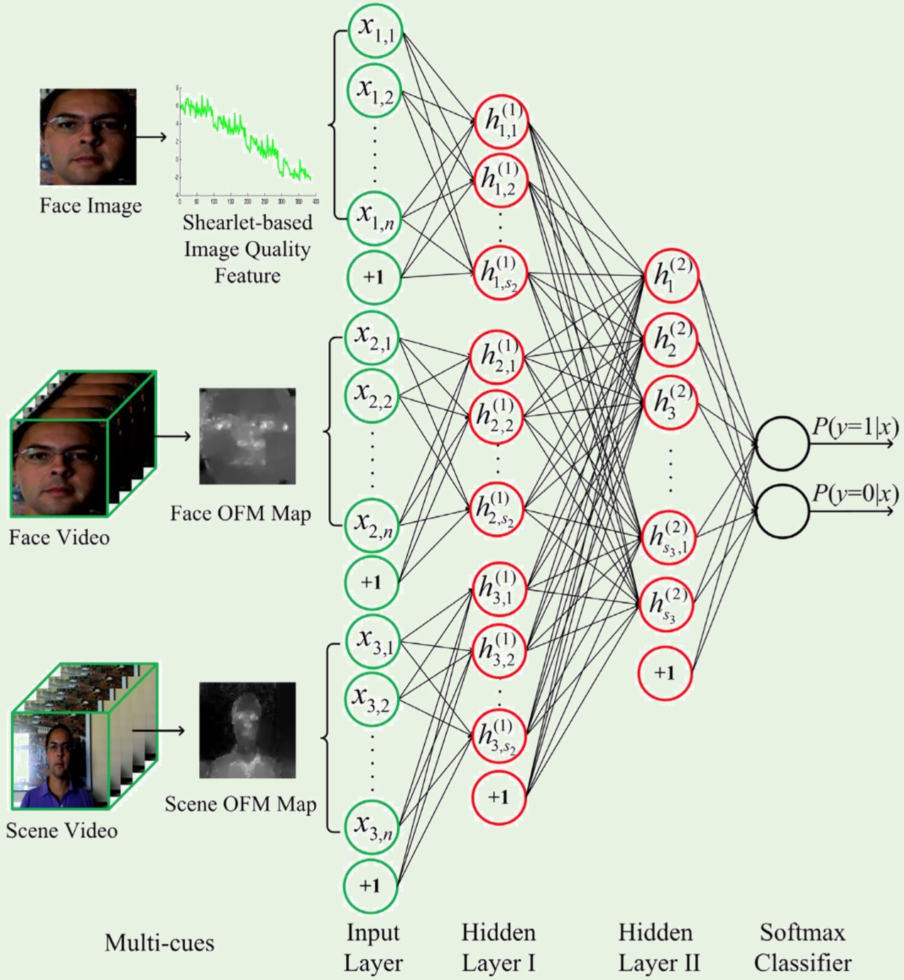




1. Xu et. al., Learning temporal features using LSTM-CNN architecture for face anti-spoofing. ACPR 2015.
2. Gan et. al., 3D Convolutional Neural Network Based on Face Anti-spoofing, ICMIP 2017
3. Yang et. al., Face Anti-Spoofing: Model Matters, So Does Data, CVPR 2019

Temporal Features

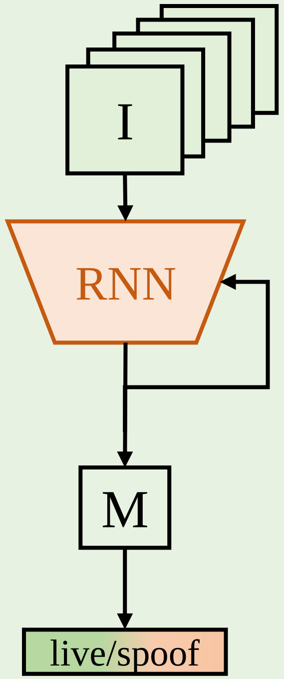
- Use temporal features as input
  - Face optical flow
  - Scene optical flow



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

Temporal FAS

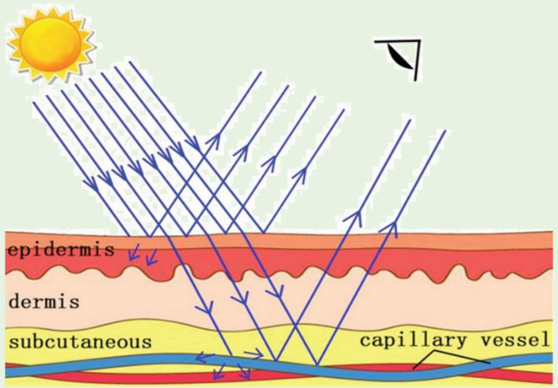
- Vanilla RNN [1,2,3]
- Temporal features [4]
- Auxiliary temporal tasks [5,7,8]
- Temporal consistency [6,9]



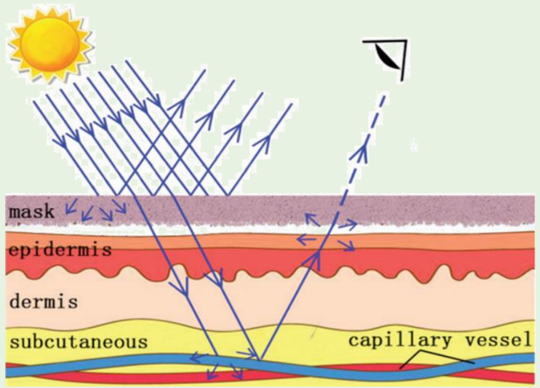
1. Xu et. al., Learning temporal features using LSTM-CNN architecture for face anti-spoofing. ACPR 2015.
2. Gan et. al., 3D Convolutional Neural Network Based on Face Anti-spoofing, ICMIP 2017
3. Yang et. al., Face Anti-Spoofing: Model Matters, So Does Data, CVPR 2019
4. Feng et. al., Integration of image quality and motion cues for face anti-spoofing: A neural network approach. JVCI 2016.
5. Liu et. al., Learning deep models for face anti-spoofing: binary or auxiliary supervision. CVPR 2018.
6. Zhang et. al., Exploiting temporal and depth information for multi-frame face anti-spoofing, arXiv 2019
7. Liu et. al., 3D Mask Face Anti-spoofing with Remote Photoplethysmography, ECCV 2016
8. Liu et. al., Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection, ECCV 2018
9. Xu et. al., On Improving Temporal Consistency for Online Face Liveness Detection System. arXiv 2020

rPPG Estimation

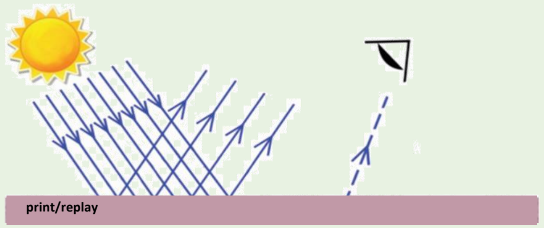
- Remote photoplethysmography: heartbeat measurement from human skin using a non-contact camera



Live Face



3D Mask Spoof Face

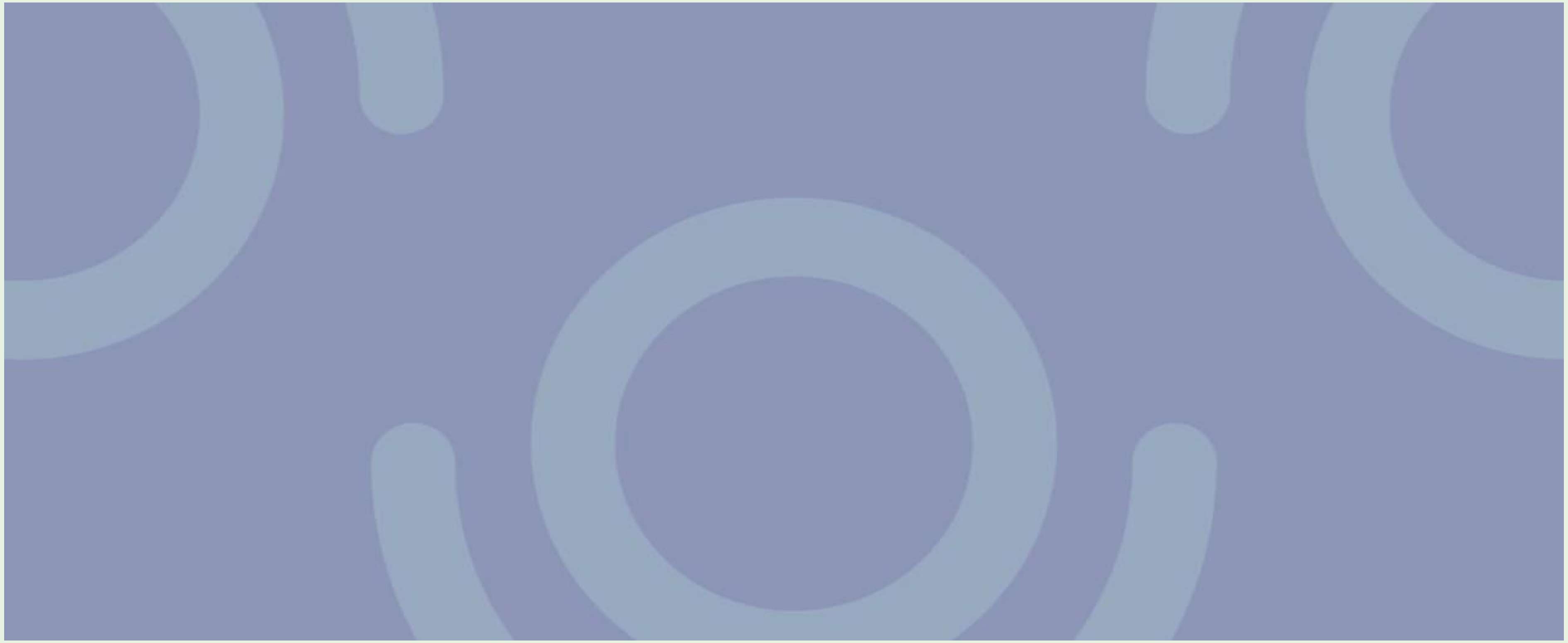


Print/Replay Spoof Face

1. Liu et. al., Learning deep models for face anti-spoofing: binary or auxiliary supervision. CVPR 2018.
2. Liu et. al., 3D Mask Face Anti-spoofing with Remote Photoplethysmography, ECCV 2016
3. Liu et. al., Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection, ECCV 2018

What is rPPG?

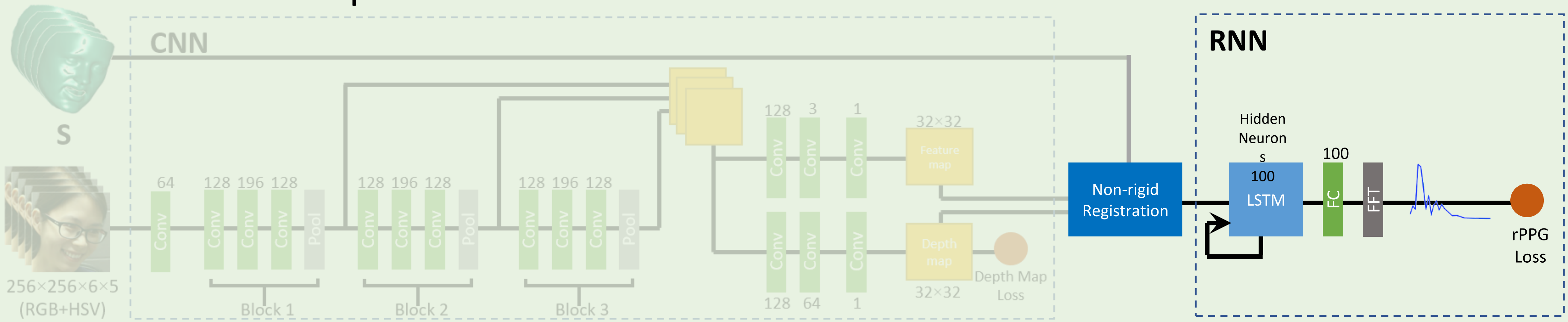
- Remote photoplethysmography: heart beat measurement from human skin using a non-contact camera



1. https://www.youtube.com/watch?v=Lazr_5Yfm-w

RNN Architecture

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



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

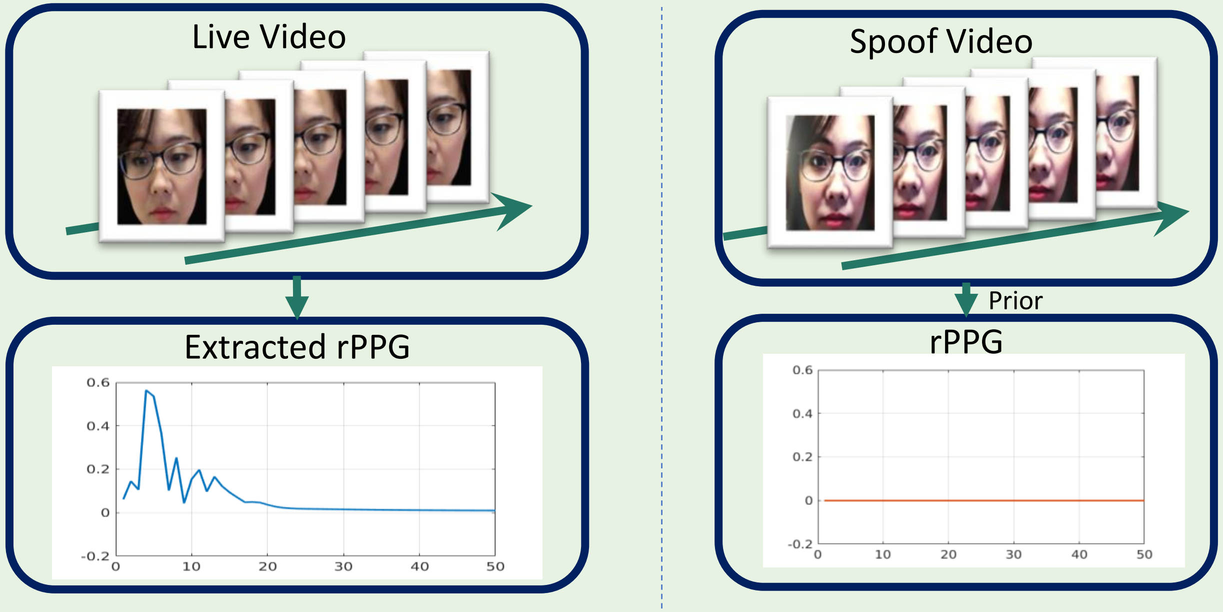
How to Obtain rPPG Label?

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

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

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

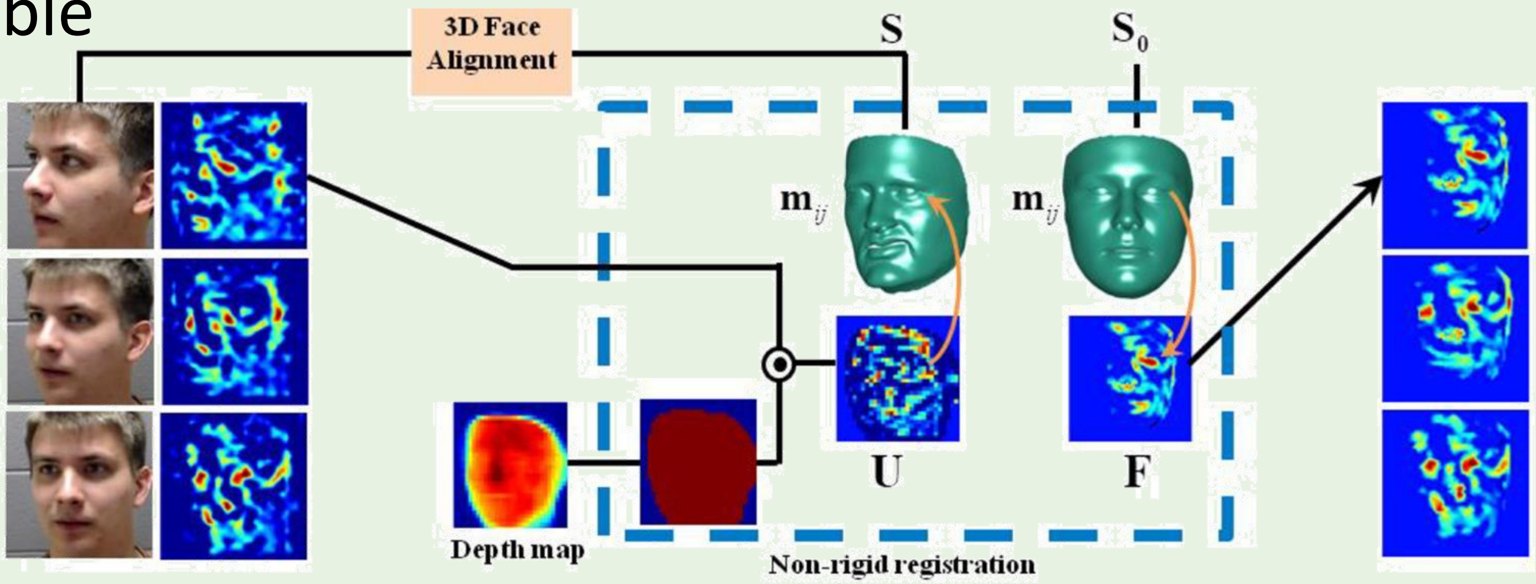
- Spoof faces: Direct assignment as zero



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

Non-rigid Registration Layer

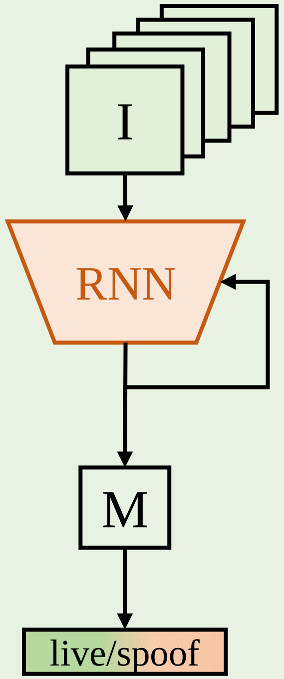
- Use 3D shape to compute offset
- Use offset to deform the features
- Differentiable



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

Temporal FAS

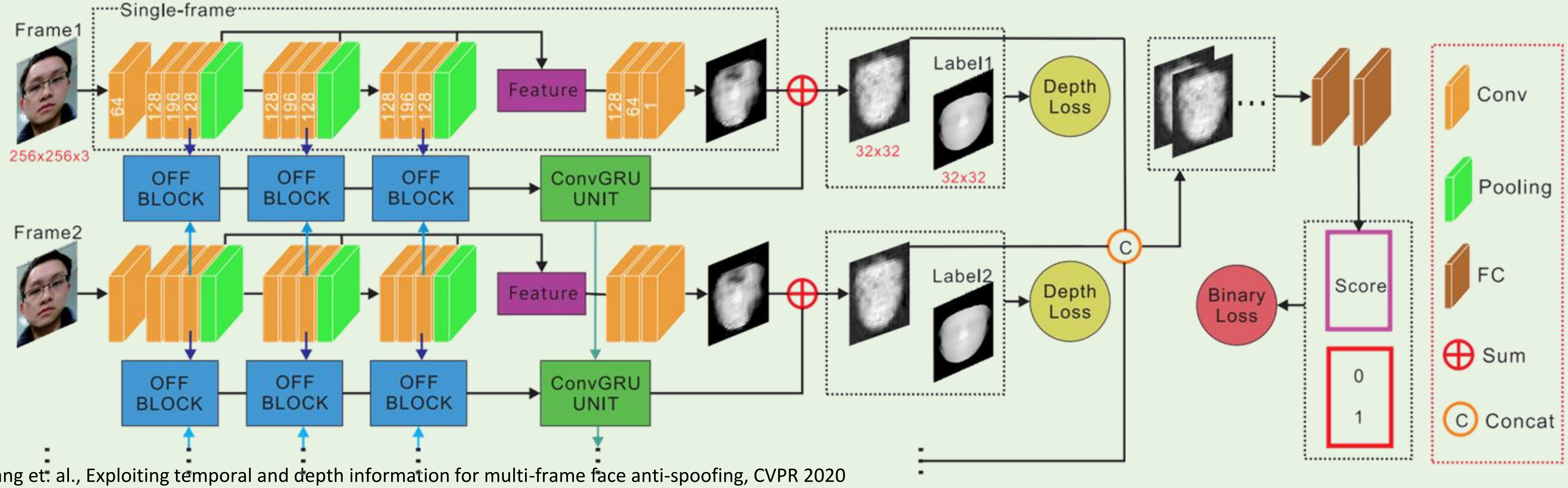
- Vanilla RNN [1,2,3]
- Temporal features [4]
- Auxiliary temporal tasks [5,7,8]
- Temporal consistency [6,9]



1. Xu et. al., Learning temporal features using LSTM-CNN architecture for face anti-spoofing. ACPR 2015.
2. Gan et. al., 3D Convolutional Neural Network Based on Face Anti-spoofing, ICMIP 2017
3. Yang et. al., Face Anti-Spoofing: Model Matters, So Does Data, CVPR 2019
4. Feng et. al., Integration of image quality and motion cues for face anti-spoofing: A neural network approach. JVCI 2016.
5. Liu et. al., Learning deep models for face anti-spoofing: binary or auxiliary supervision. CVPR 2018.
6. Zhang et. al., Exploiting temporal and depth information for multi-frame face anti-spoofing, arXiv 2019
7. Liu et. al., 3D Mask Face Anti-spoofing with Remote Photoplethysmography, ECCV 2016
8. Liu et. al., Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection, ECCV 2018
9. Xu et. al., On Improving Temporal Consistency for Online Face Liveness Detection System. arXiv 2020

Temporal Consistency

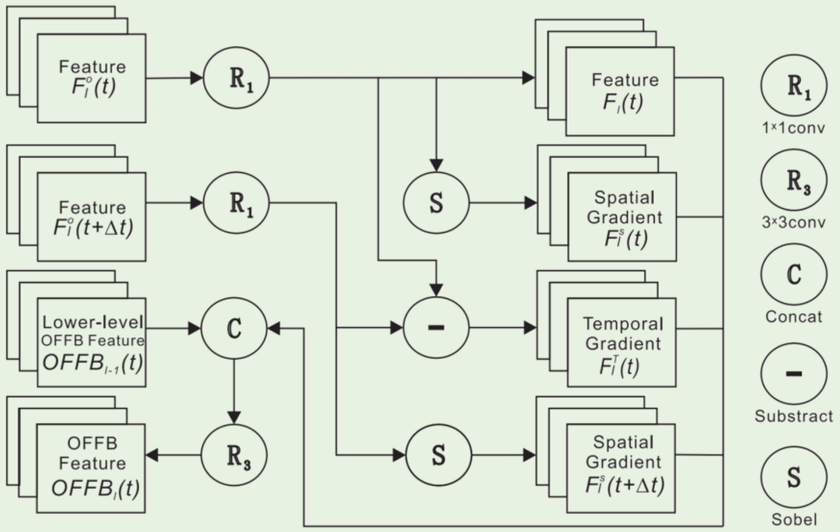
- Map single frame to depth map
- Introduce frame-to-frame motion to complete depth map
- Concat all maps to get a final score

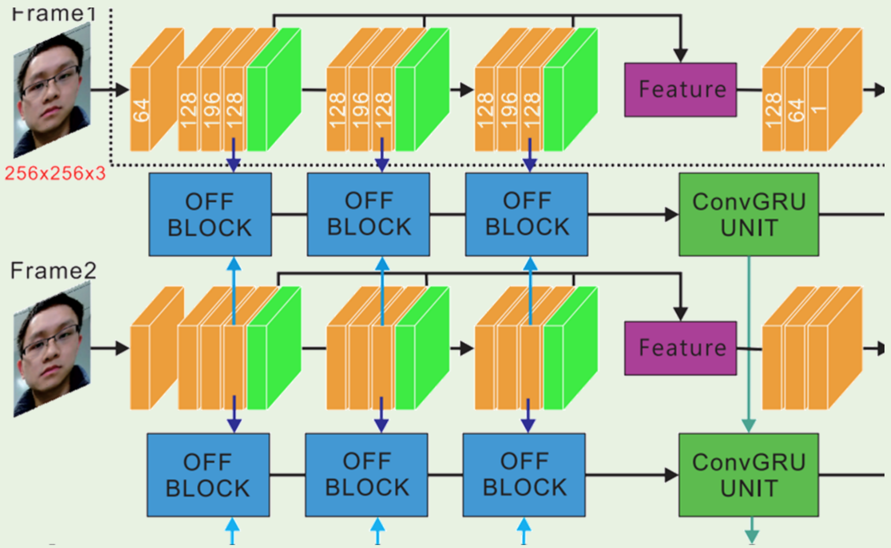


1. Wang et. al., Exploiting temporal and depth information for multi-frame face anti-spoofing, CVPR 2020

Temporal Blocks

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





1. Wang et. al., Exploiting temporal and depth information for multi-frame face anti-spoofing, CVPR 2020

Temporal Consistency

- Classification supervision (Le):

$$L_c = -\frac{1}{m}\sum_{i=0}^{m} \log p_{y_i},$$

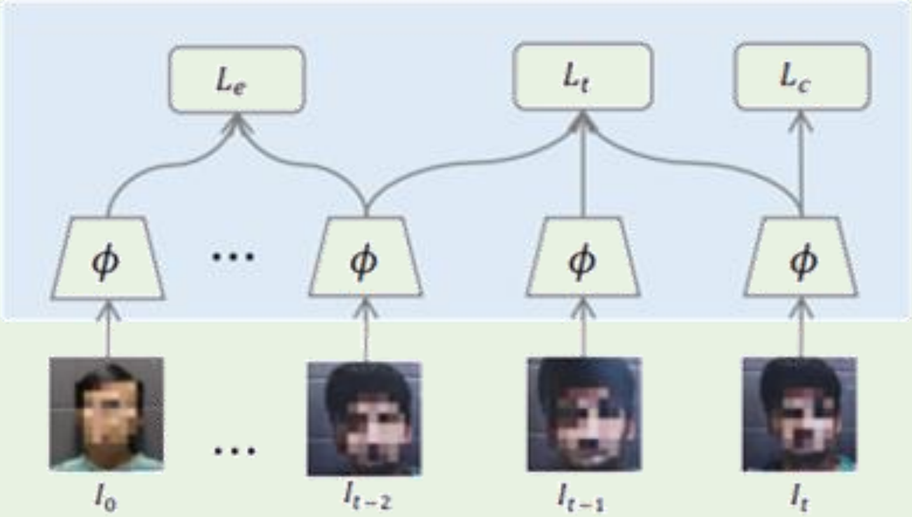
- Temporal consistency supervision (Lt):

$$L_t = \frac{1}{m}\sum_{i=0}^{m} \max_{i,j \in v} ||x_i - x_j||_2^2,$$

  - x is the feature representation of each frame

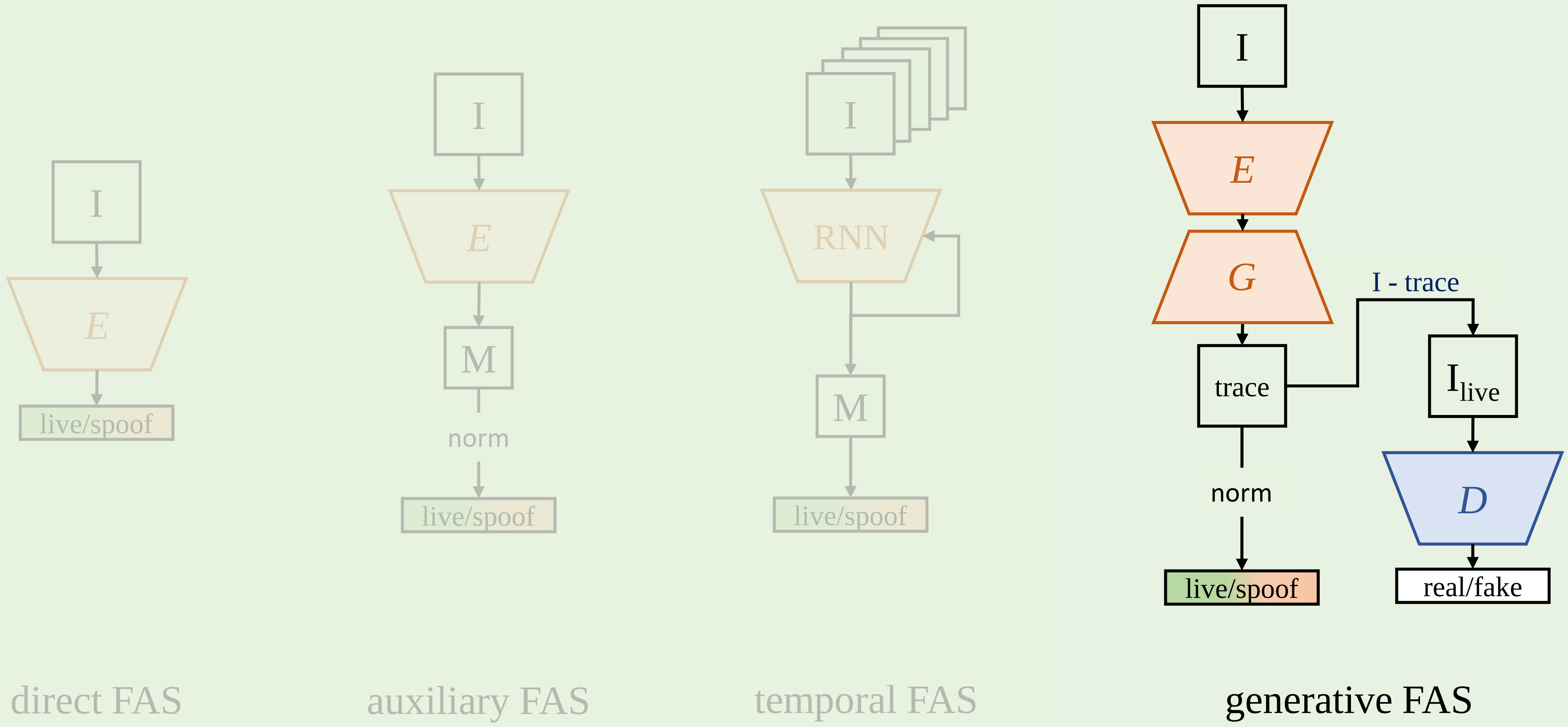
- Class consistency supervision (Lc):

$$L_e = \frac{1}{m}\sum_{i=0}^{m} \max y_{ij} ||x_i - x_j||_2^2,$$



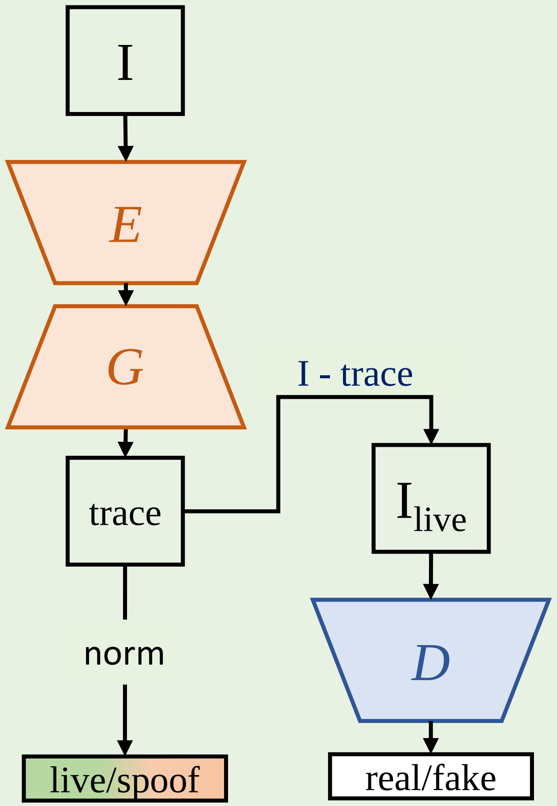
1. Xu et. al., On Improving Temporal Consistency for Online Face Liveness Detection System, arXiv 2020

Deep-Learning-Based Methods



Generative FAS

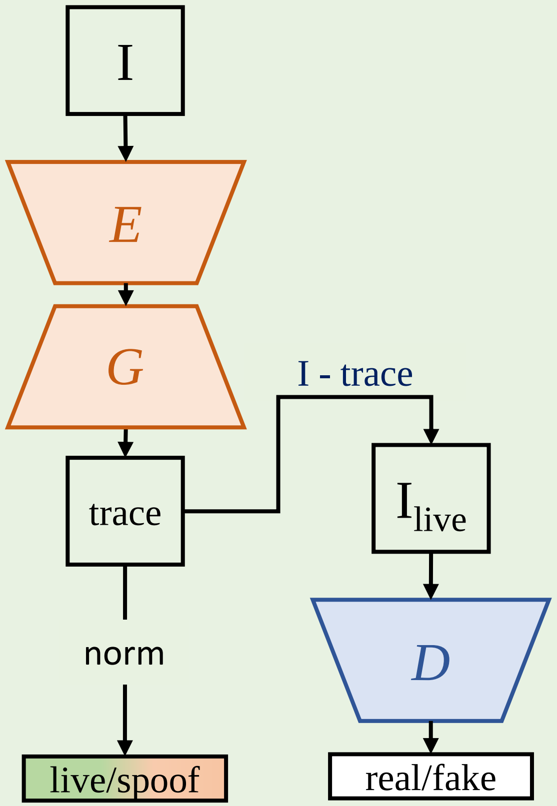
- CNN is trained to generate some type of image to extract FAS feature
- Generate:
  - Data augmentation
  - Some "spoof patterns"[5]
  - Disentangling reconstruction[3]
  - Spoof trace[1,2,4]



1. Y. Liu, et. al. "On Disentangling Spoof Traces for Generic Face Anti-Spoofing", ECCV 2020
2. A. Jourabloo, et. al. "Face De-Spoofing: Anti-Spoofing via Noise Modeling", ECCV 2018
3. K. Zhang, et. al., "Face Anti-Spoofing via Disentangled Representation Learning ", ECCV 2020
4. J. Stehouwer, et. al., "Noise Modeling, Synthesis and Classification for Generic Object Anti-Spoofing", CVPR 2020
5. H. Feng, et. al., "Learning Generalized Spoof Cues for Face Anti-spoofing", arXiv, 2020

Generative FAS

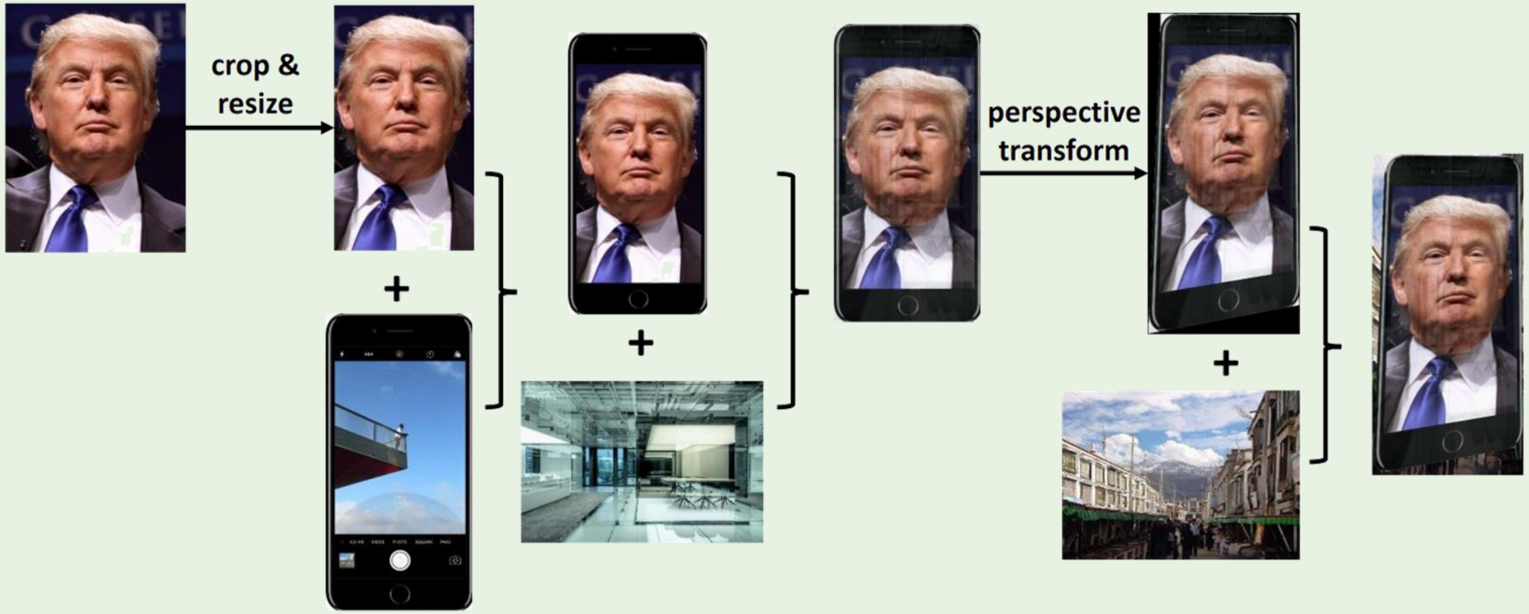
- CNN is trained to generate some type of image to extract FAS feature
- Generate:
  - Data augmentation
  - Some "spoof patterns"[5]
  - Disentangling reconstruction[3]
  - Spoof trace[1,2,4]



1. Y. Liu, et. al. "On Disentangling Spoof Traces for Generic Face Anti-Spoofing", ECCV 2020
2. A. Jourabloo, et. al. "Face De-Spoofing: Anti-Spoofing via Noise Modeling", ECCV 2018
3. K. Zhang, et. al., "Face Anti-Spoofing via Disentangled Representation Learning ", ECCV 2020
4. J. Stehouwer, et. al., "Noise Modeling, Synthesis and Classification for Generic Object Anti-Spoofing", CVPR 2020
5. H. Feng, et. al., "Learning Generalized Spoof Cues for Face Anti-spoofing", arXiv, 2020

Data Augmentation

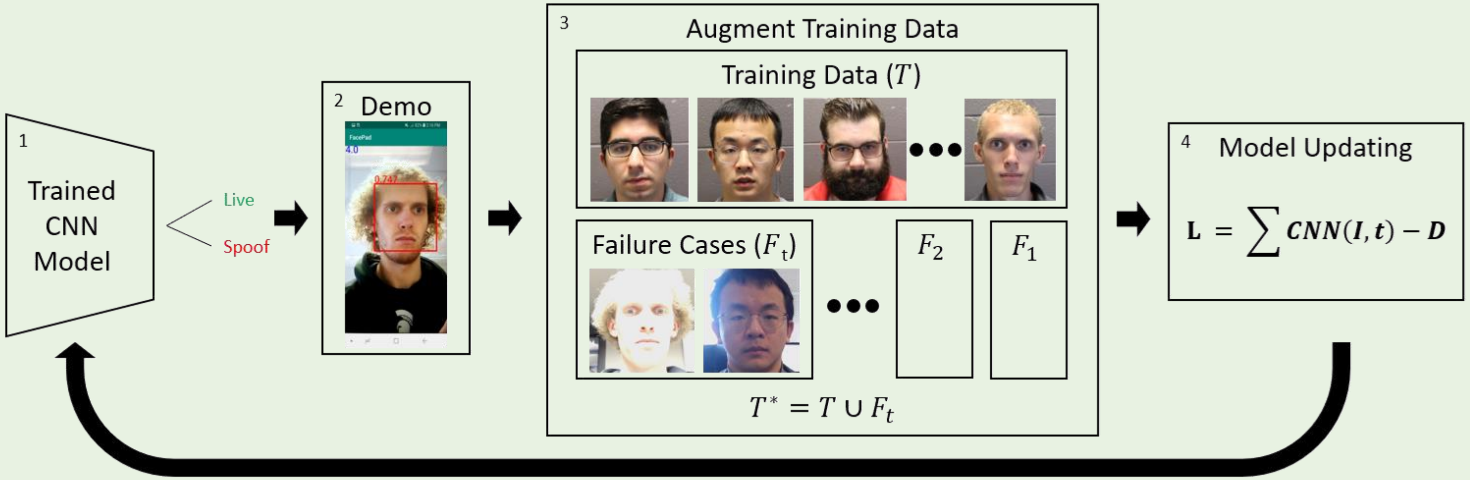
- Blurriness: random strength Gaussian blurring
- Reflection: $\mathbf{X}_r' = (1-\alpha)\,\mathbf{X}' + \alpha\mathbf{X}_r$
- Distortion: Perspective projection



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

Data Augmentation

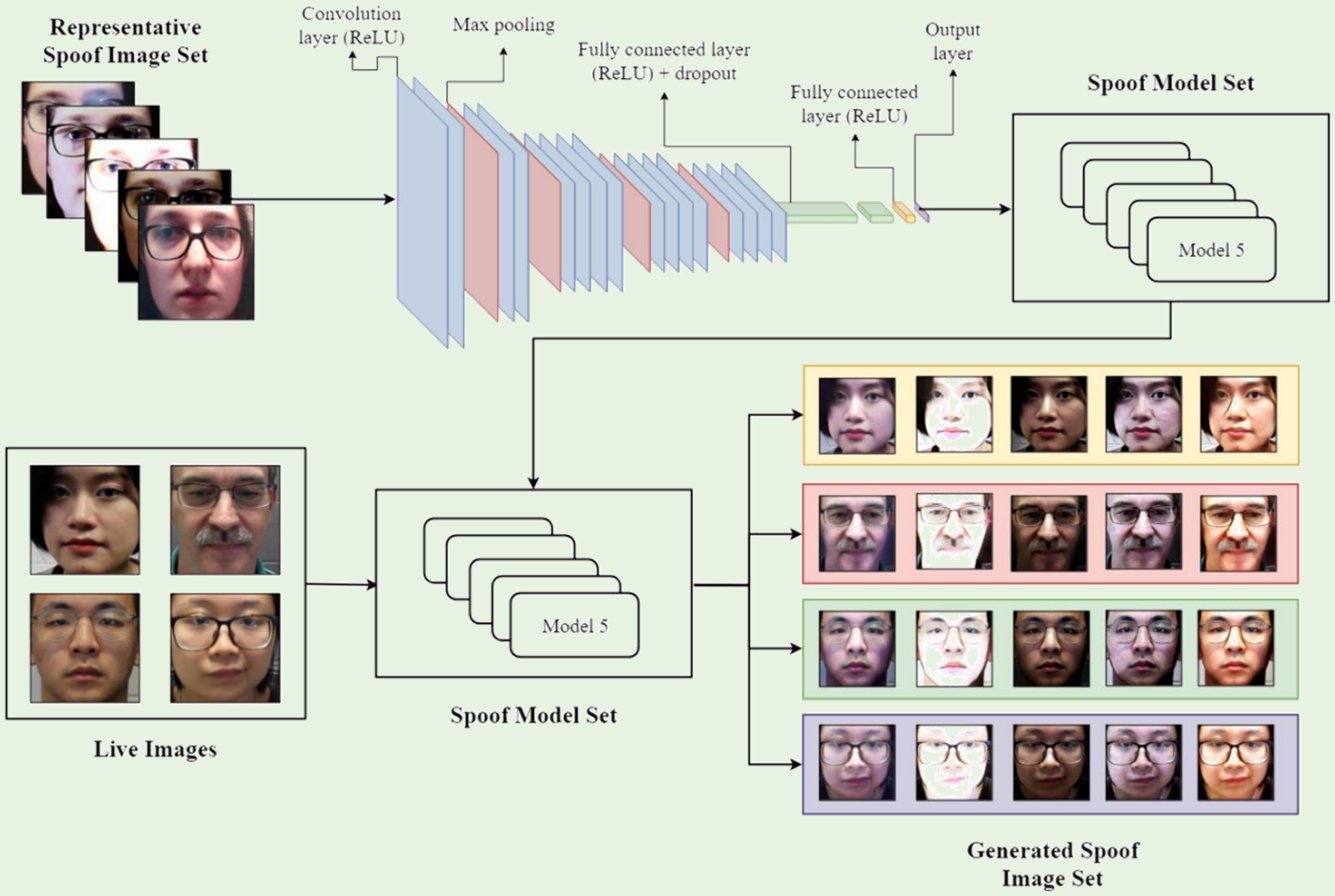
- Random perturbation
  - Contrast
  - Lightness
- Data Updating
  - Use current model to collect failure cases
  - Add failure cases to training set to fine-tune the model
  - Update the current model
  - Repeat several times



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

Data Augmentation

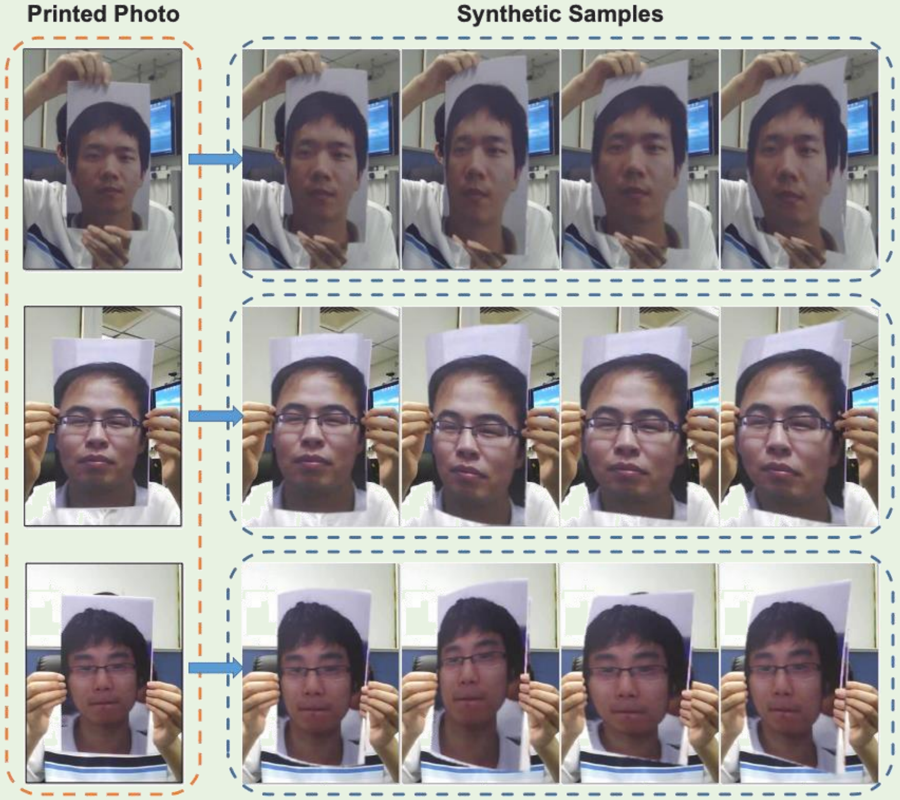
Use style transfer for data augmentation

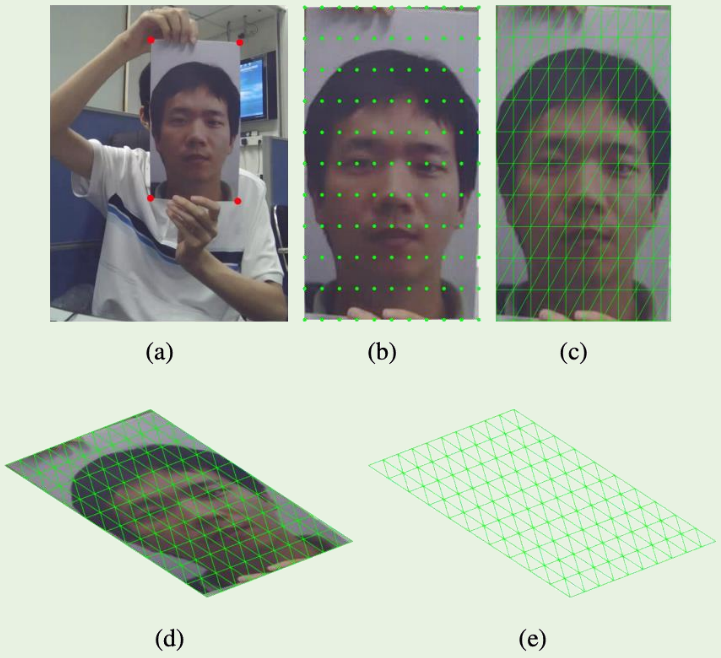


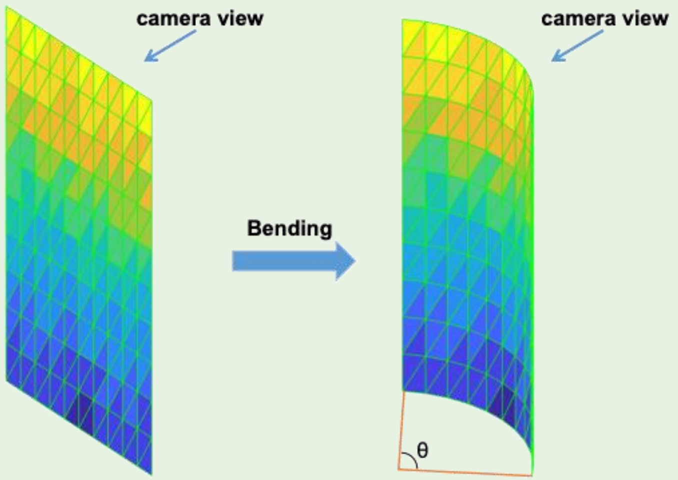
1. Laurensi et. al., Style Transfer Applied to Face Liveness Detection with User-Centered Models, arXiv, 2019

Data Augmentation: 3D Synthesis

Use CNN to deform the face based on 3D shape



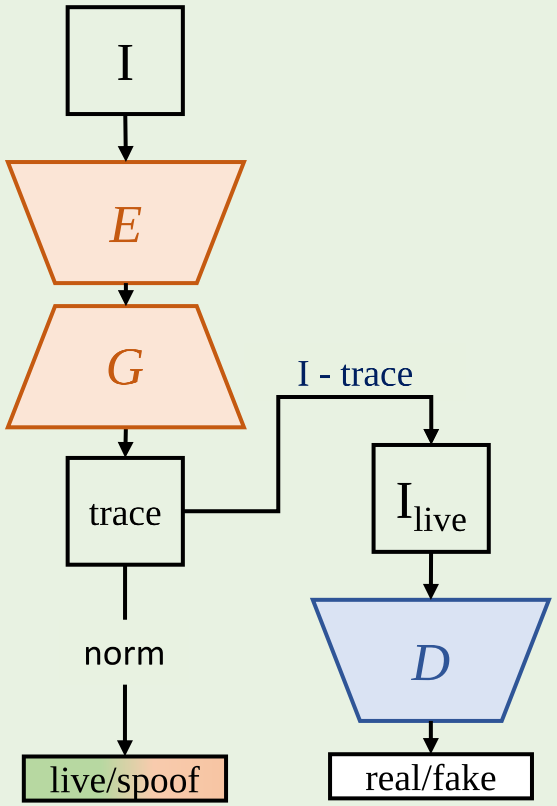




1. Guo et. al., Improving Face Anti-Spoofing by 3D Virtual Synthesis, arXiv, 2019

Generative FAS

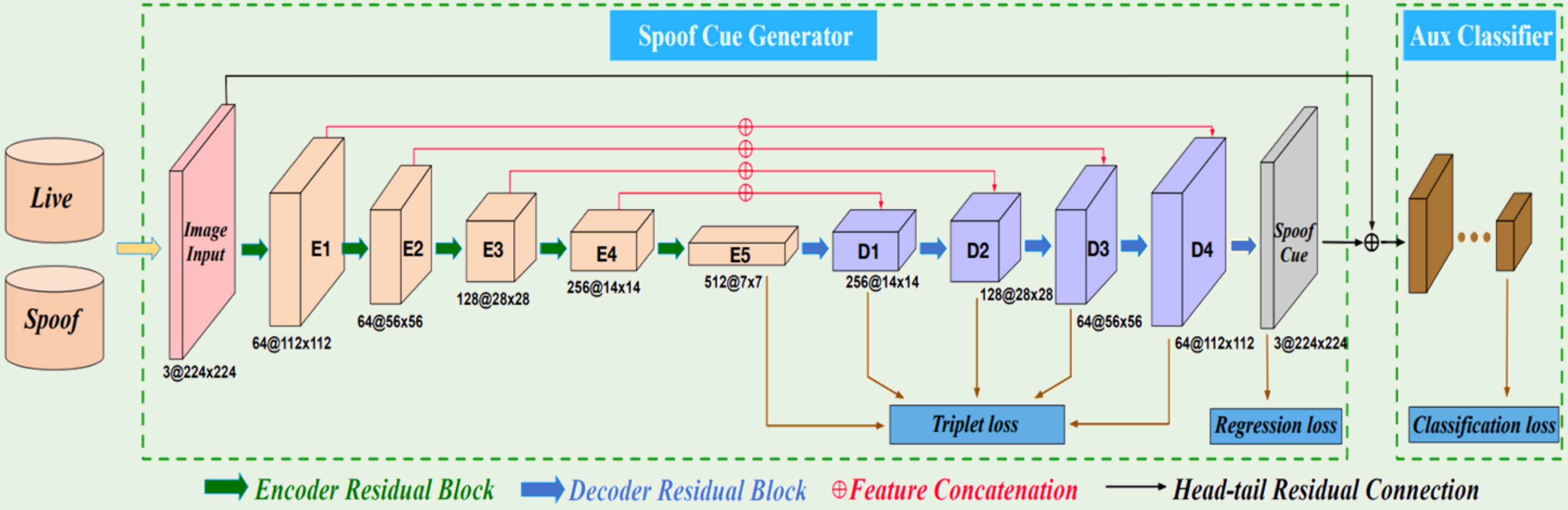
- CNN is trained to generate some type of image to extract FAS feature
- Generate:
  - Data augmentation
  - Some “spoof patterns”[5]
  - Disentangling reconstruction[3]
  - Spoof trace[1,2,4]



1. Y. Liu, et. al. “On Disentangling Spoof Traces for Generic Face Anti-Spoofing”, ECCV 2020
2. A. Jourabloo, et. al. “Face De-Spoofing: Anti-Spoofing via Noise Modeling”, ECCV 2018
3. K. Zhang, et. al., “Face Anti-Spoofing via Disentangled Representation Learning ”, ECCV 2020
4. J. Stehouwer, et. al., “Noise Modeling, Synthesis and Classification for Generic Object Anti-Spoofing”, CVPR 2020
5. H. Feng, et. al., “Learning Generalized Spoof Cues for Face Anti-spoofing”, arXiv, 2020

Spoof Pattern Motivation

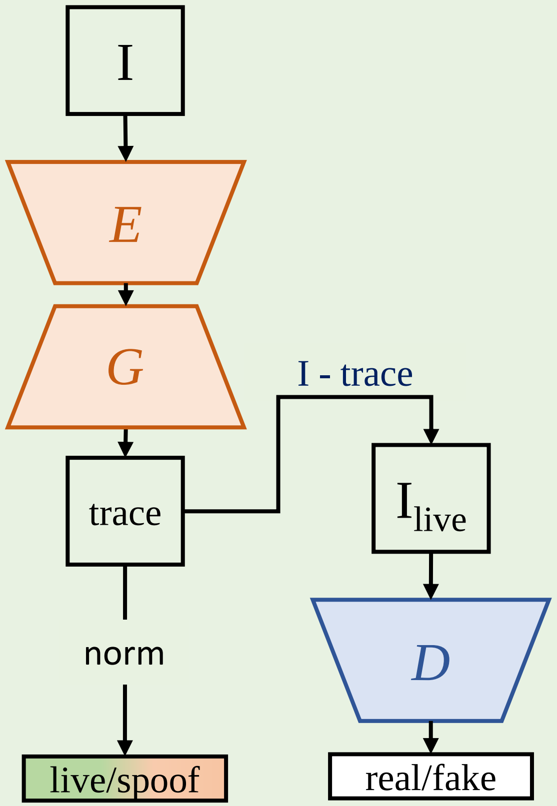
- Augment the spoof cue for classification
- Triplet learning for spoof cue features



1. H. Feng, et. al., "Learning Generalized Spoof Cues for Face Anti-spoofing", arXiv, 2020

Generative FAS

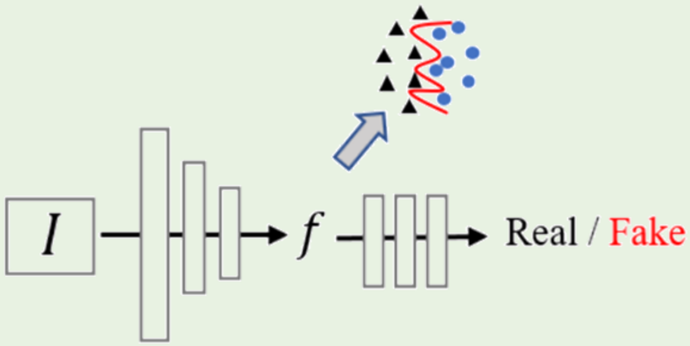
- CNN is trained to generate some type of image to extract FAS feature
- Generate:
  - Data augmentation
  - Some “spoof patterns”[5]
  - Disentangling reconstruction[3]
  - Spoof trace[1,2,4]

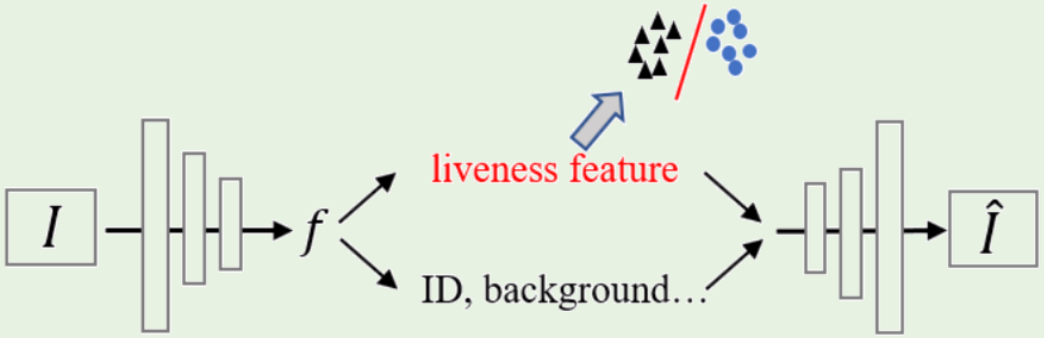


1. Y. Liu, et. al. “On Disentangling Spoof Traces for Generic Face Anti-Spoofing”, ECCV 2020
2. A. Jourabloo, et. al. “Face De-Spoofing: Anti-Spoofing via Noise Modeling”, ECCV 2018
3. K. Zhang, et. al., “Face Anti-Spoofing via Disentangled Representation Learning ”, ECCV 2020
4. J. Stehouwer, et. al., “Noise Modeling, Synthesis and Classification for Generic Object Anti-Spoofing”, CVPR 2020
5. H. Feng, et. al., “Learning Generalized Spoof Cues for Face Anti-spoofing”, arXiv, 2020

Disentangling Reconstruction Motivation

- Disentangling spoof-related features and spoof-unrelated features (face content)

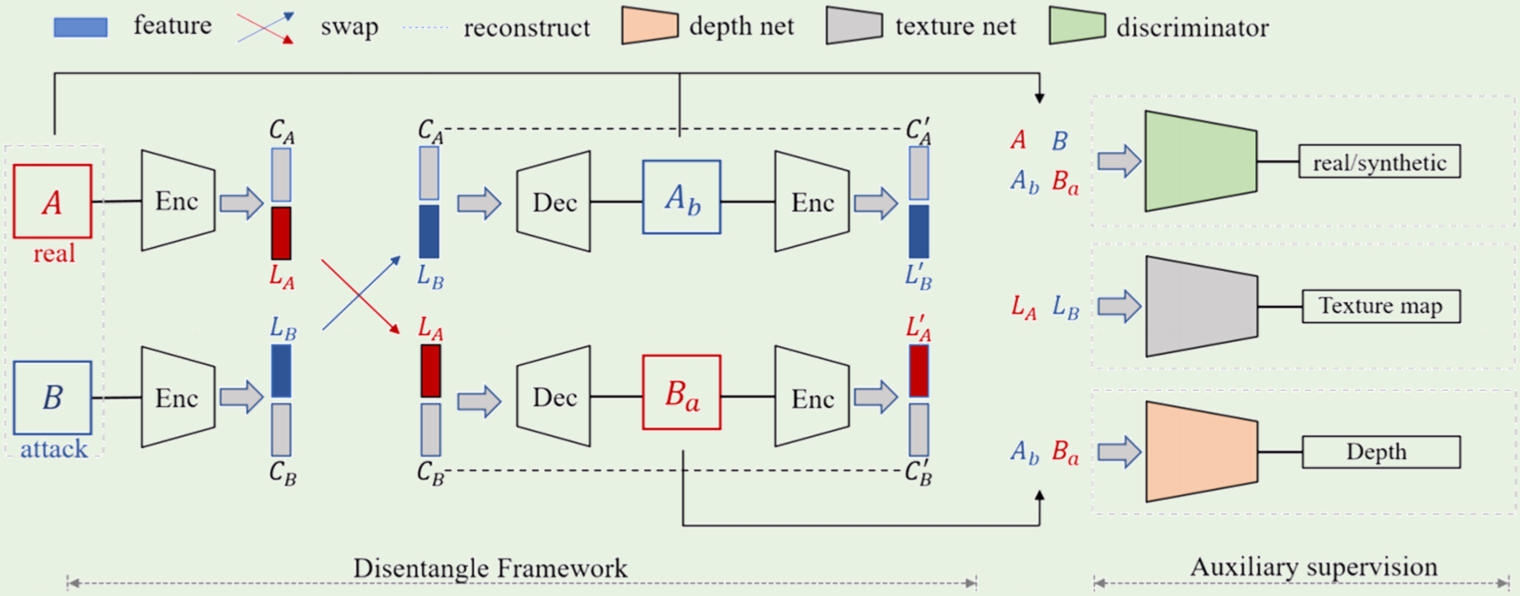




1. K. Zhang, et. al., “Face Anti-Spoofing via Disentangled Representation Learning ”, ECCV 2020

Disentangling Reconstruction Motivation

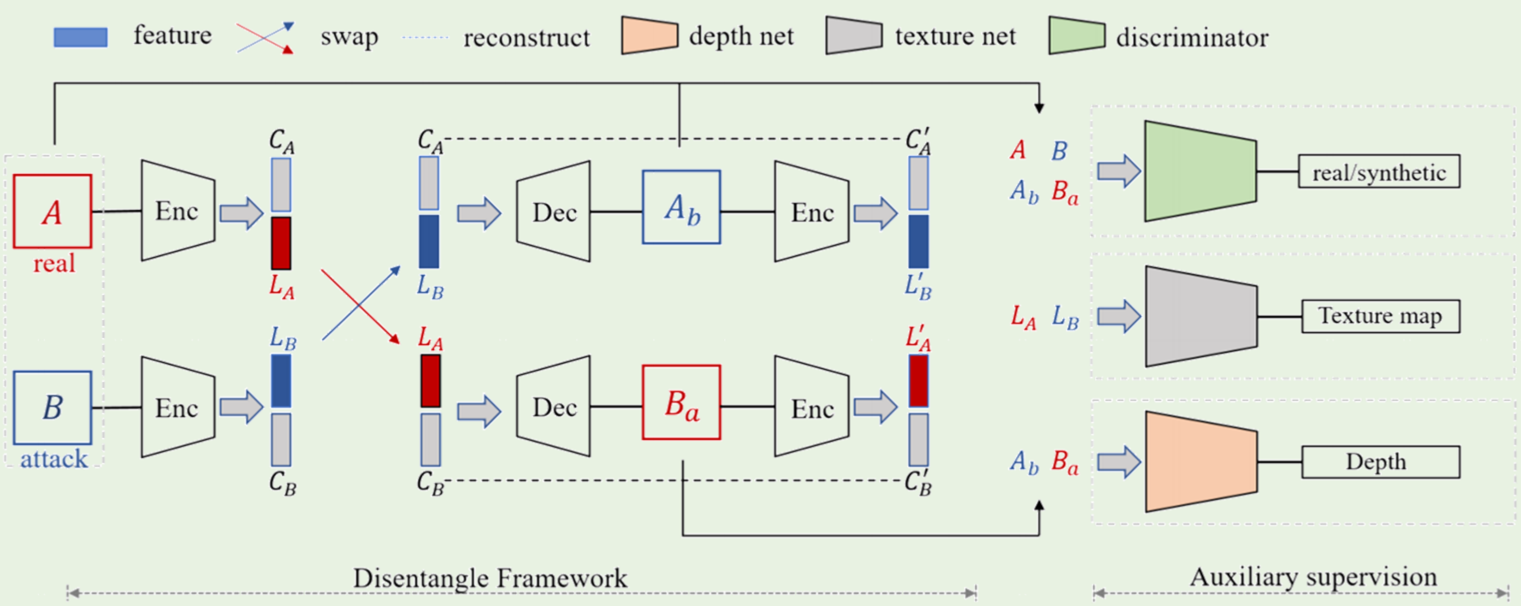
- Generator
  - Disentangle the content feature with liveness feature
- Discriminators
  - #1 distinguish real v.s. synthetic
  - #2 auxiliary lbp supervision for latent code
  - #3 auxiliary depth supervision for face



1. K. Zhang, et. al., “Face Anti-Spoofing via Disentangled Representation Learning ”, ECCV 2020

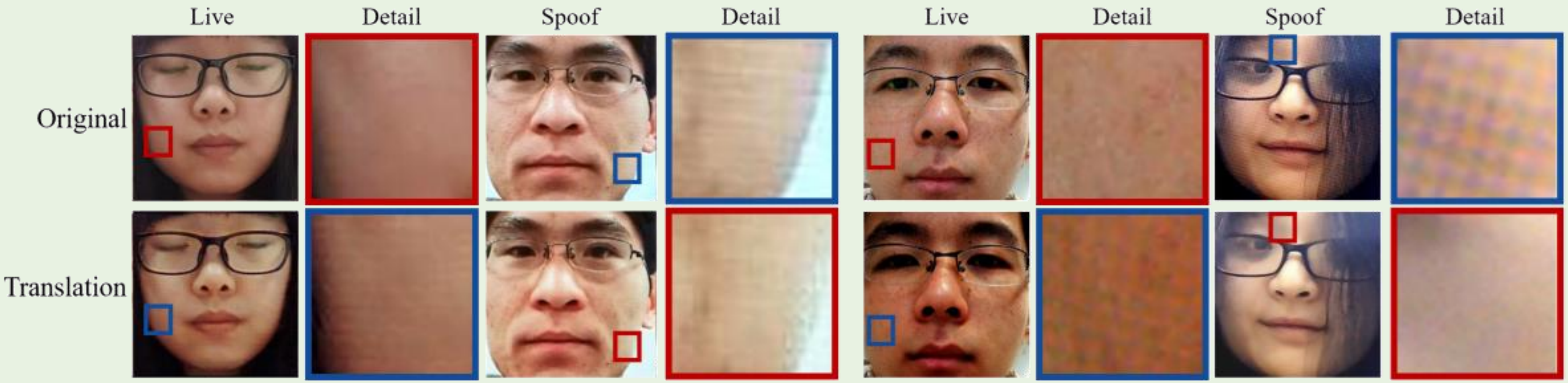
Losses

- Generator
  - image reconstruction
  - code reconstruction
  - GAN loss
- Discriminators
  - GAN loss
  - depth supervision
  - Lbp supervision



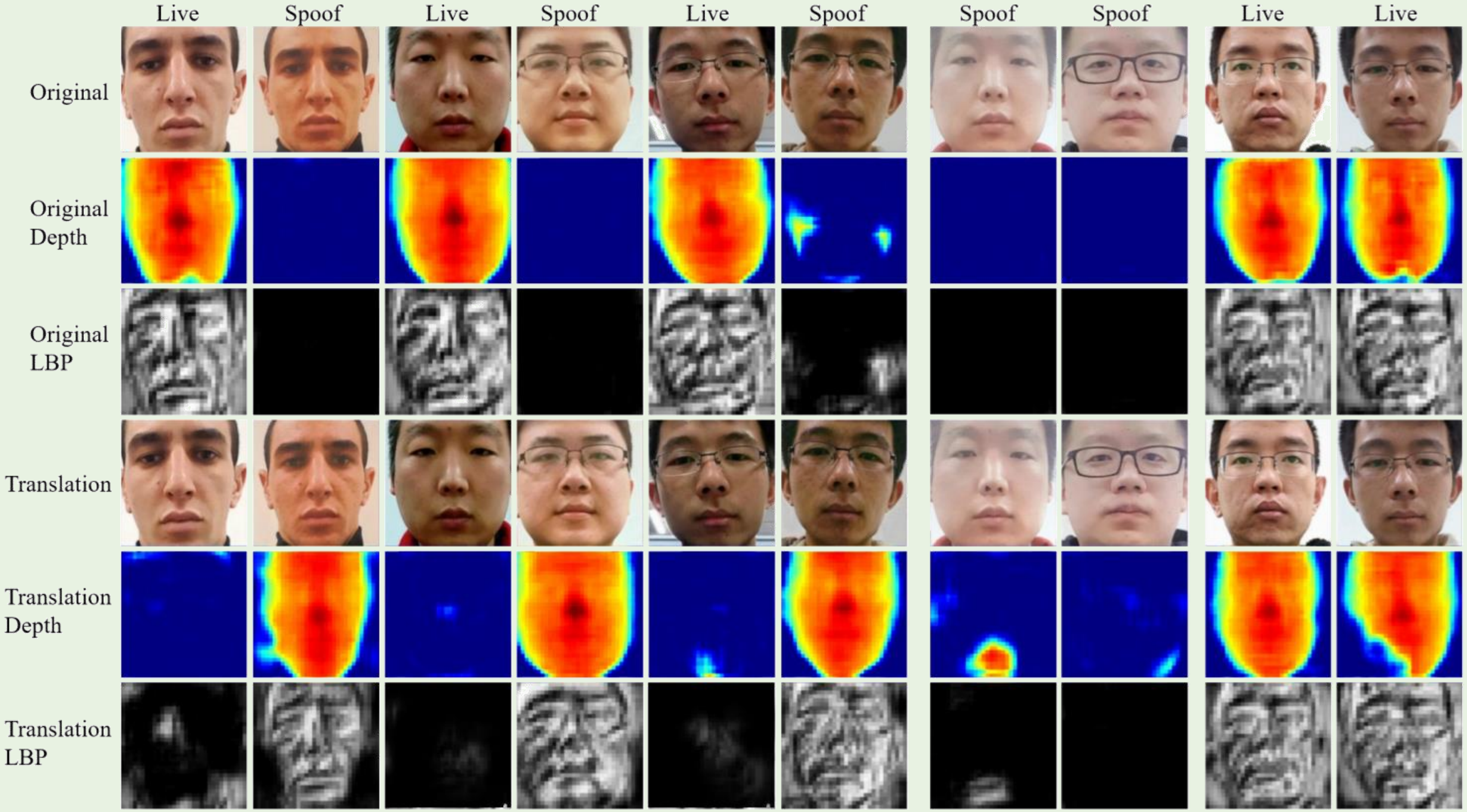
1. K. Zhang, et. al., "Face Anti-Spoofing via Disentangled Representation Learning ", ECCV 2020

Disentangling Results



1. K. Zhang, et. al., “Face Anti-Spoofing via Disentangled Representation Learning ”, ECCV 2020

Disentangling Results

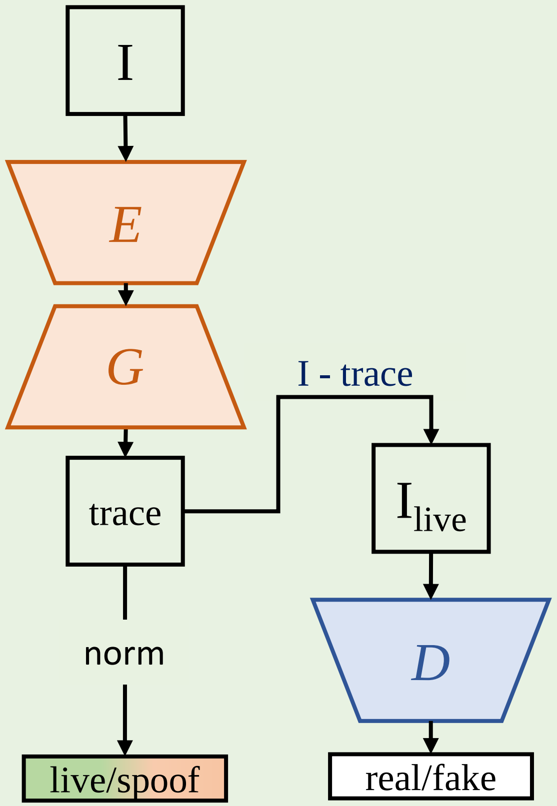


(a) live_spoof group (b) spoof_spoof group (c) live_live group

1. K. Zhang, et. al., "Face Anti-Spoofing via Disentangled Representation Learning ", ECCV 2020

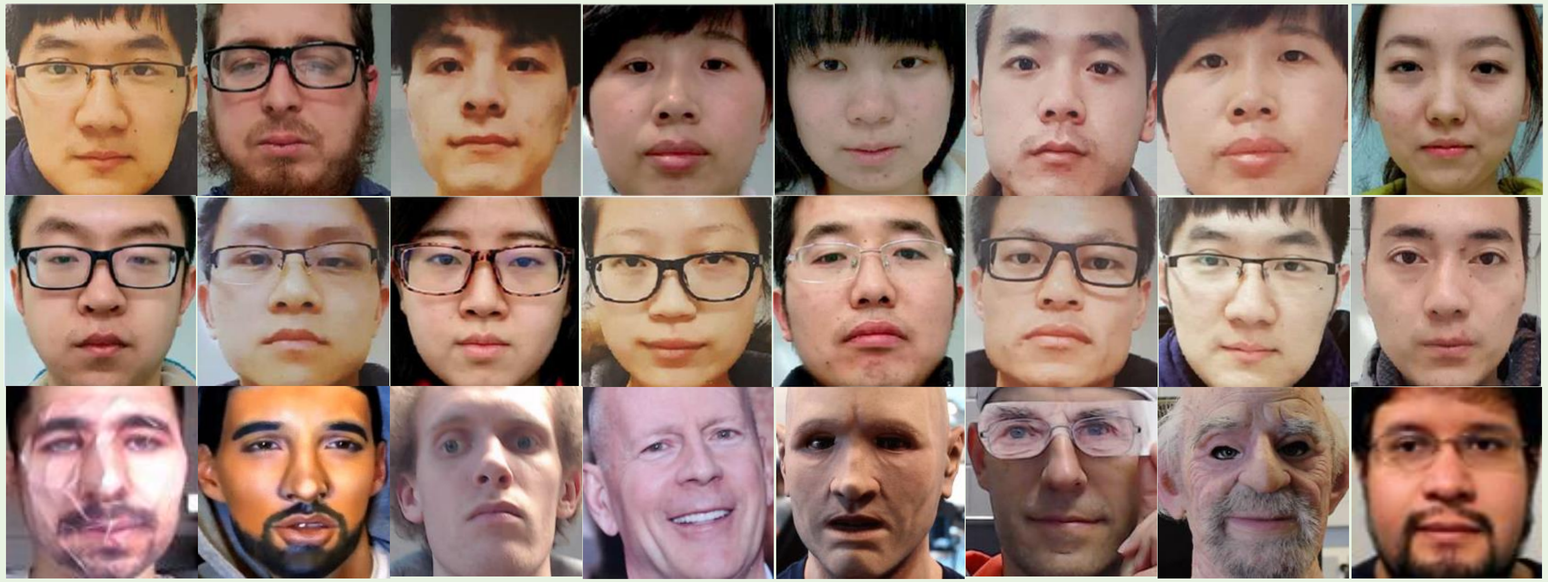
Generative FAS

- CNN is trained to generate some type of image to extract FAS feature
- Generate:
  - Data augmentation
  - Some "spoof patterns"[5]
  - Disentangling reconstruction[3]
  - Spoof trace[1,2,4]



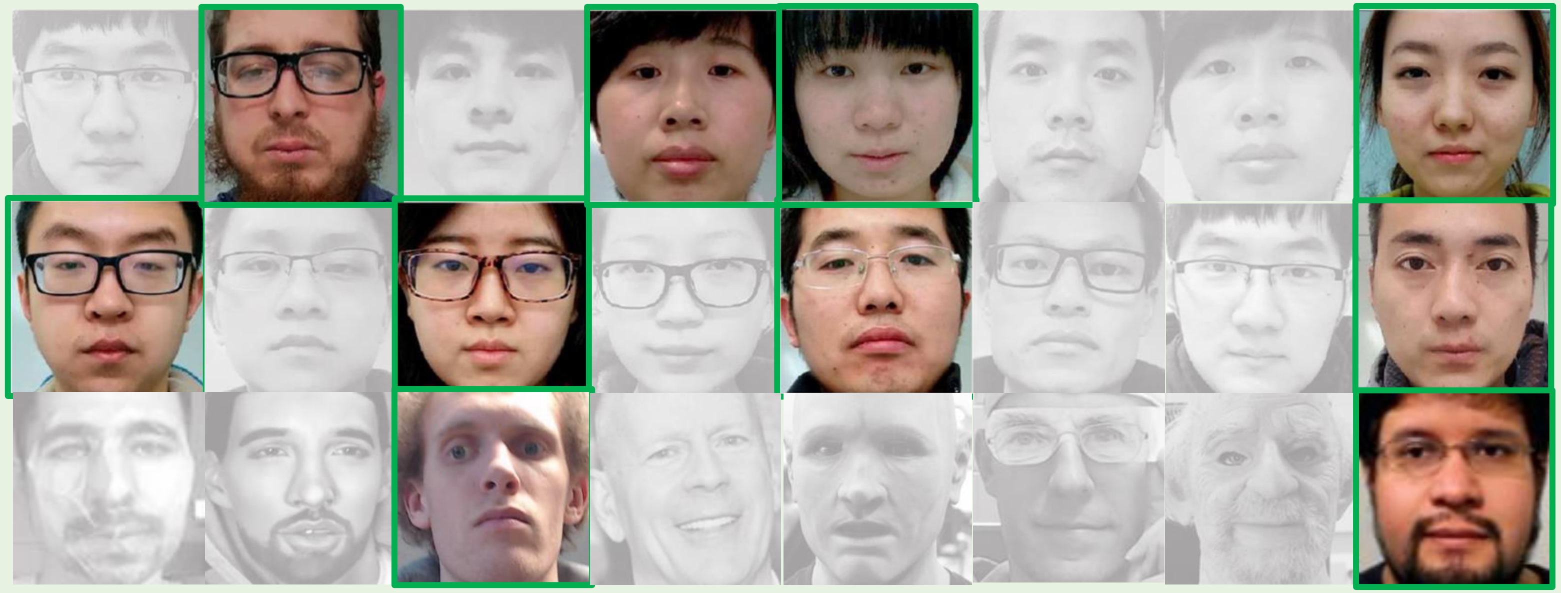
1. Y. Liu, et. al. "On Disentangling Spoof Traces for Generic Face Anti-Spoofing", ECCV 2020
2. A. Jourabloo, et. al. "Face De-Spoofing: Anti-Spoofing via Noise Modeling", ECCV 2018
3. K. Zhang, et. al., "Face Anti-Spoofing via Disentangled Representation Learning ", ECCV 2020
4. J. Stehouwer, et. al., "Noise Modeling, Synthesis and Classification for Generic Object Anti-Spoofing", CVPR 2020
5. H. Feng, et. al., "Learning Generalized Spoof Cues for Face Anti-spoofing", arXiv, 2020

Spoof Trace Motivation



Which are live faces? Which are spoof faces?

Spoof Trace Motivation



- Can we train a model to recognize all those attacks?
- Why the spoof faces are different from the live faces?

Spoof Trace

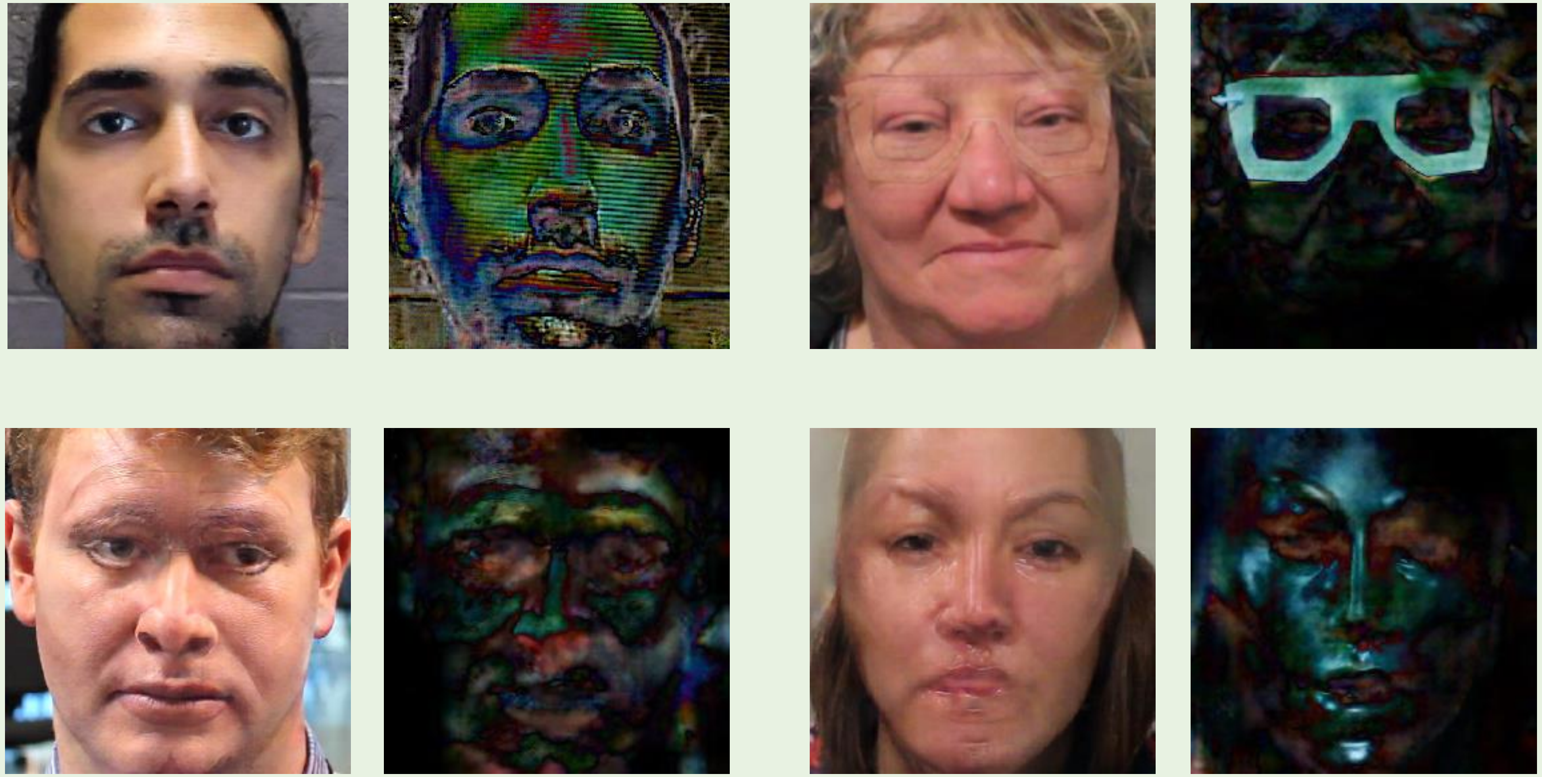
- The exact pattern introduced by spoof mediums
- Transfer the spoof to the closest live




1. Y. Liu, et. al. “On Disentangling Spoof Traces for Generic Face Anti-Spoofing”, ECCV 2020
2. A. Jourabloo, et. al. “Face De-Spoofing: Anti-Spoofing via Noise Modeling”, ECCV 2018
3. J. Stehouwer, et. al., “Noise Modeling, Synthesis and Classification for Generic Object Anti-Spoofing”, CVPR 2020

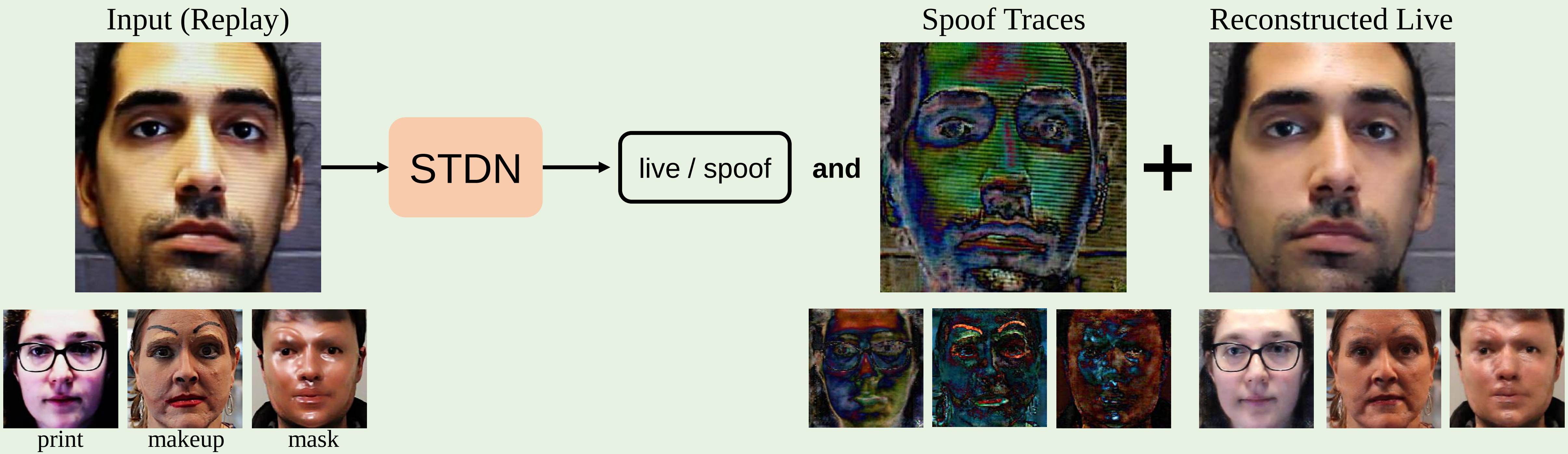
Spoof Trace Motivation

- Explainable AI
- Data limitation
    a. constrained environment
    b. long tail



1. Y. Liu, et. al. “On Disentangling Spoof Traces for Generic Face Anti-Spoofing”, ECCV 2020
2. A. Jourabloo, et. al. “Face De-Spoofing: Anti-Spoofing via Noise Modeling”, ECCV 2018
3. J. Stehouwer, et. al., “Noise Modeling, Synthesis and Classification for Generic Object Anti-Spoofing”, CVPR 2020

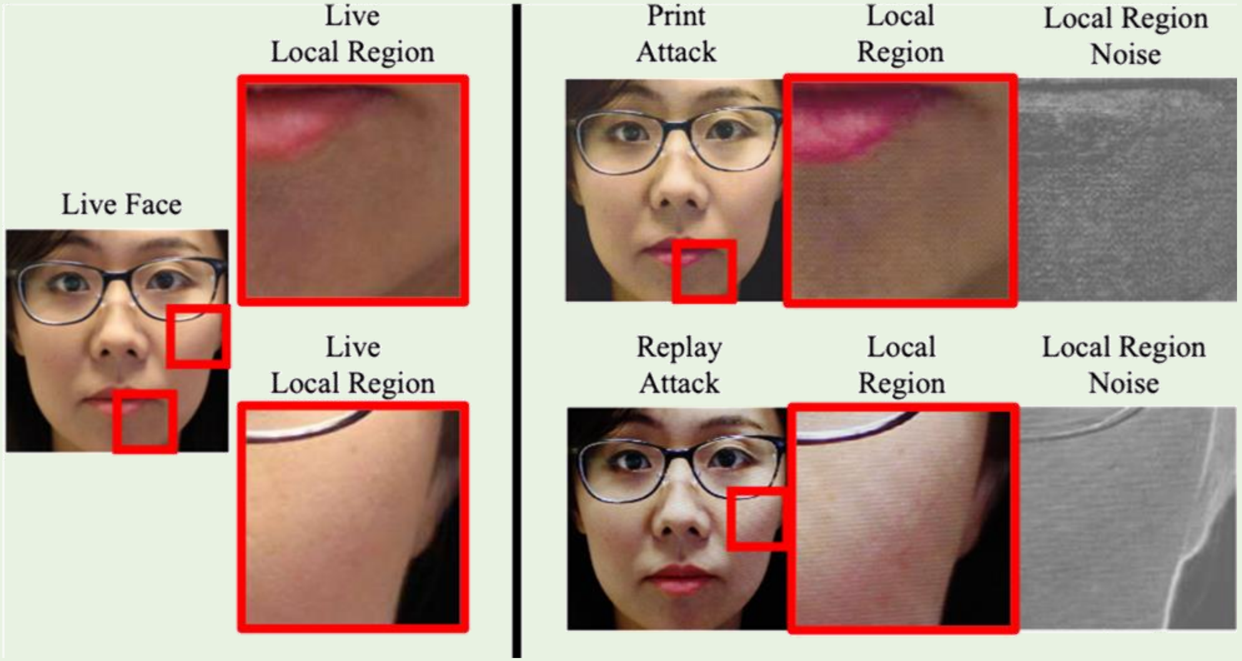
Spoof Trace Disentangling Network



1. Y. Liu, et. al. “On Disentangling Spoof Traces for Generic Face Anti-Spoofing”, ECCV 2020
2. A. Jourabloo, et. al. “Face De-Spoofing: Anti-Spoofing via Noise Modeling”, ECCV 2018
3. J. Stehouwer, et. al., “Noise Modeling, Synthesis and Classification for Generic Object Anti-Spoofing”, CVPR 2020

The Cause of Spoof Noise Pattern?

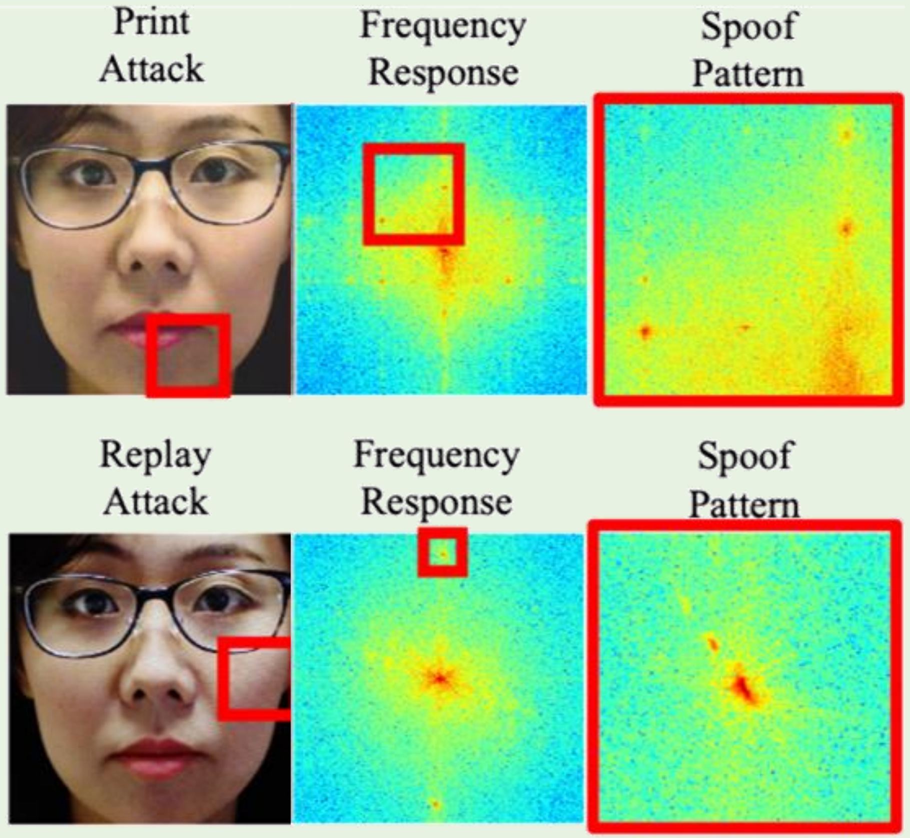
- Color distortion (Low)
- Display artifacts (Mid-High)
- Presenting artifacts (Mid-High)
- Imaging artifacts (High)



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

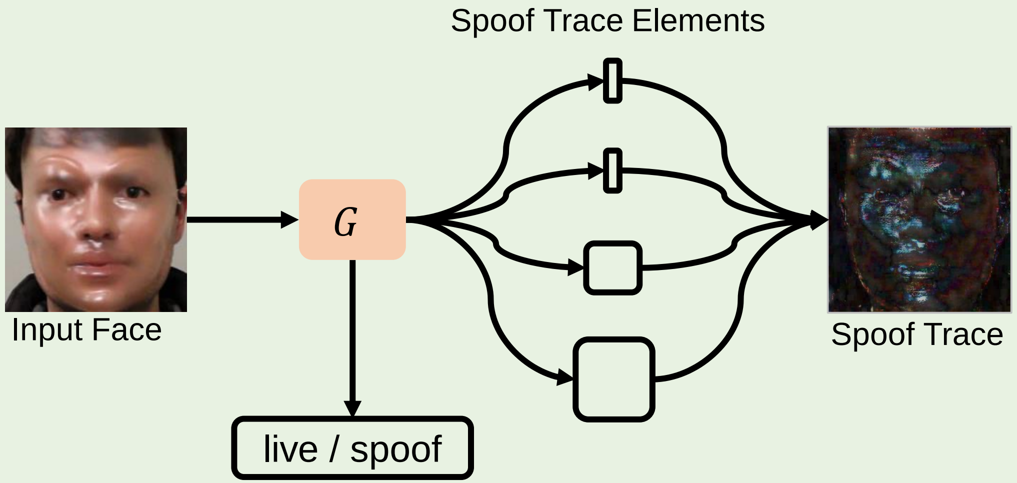
The Cause of Spoof Noise Pattern?

- Color distortion (Low)
- Display artifacts (Mid-High)
- Presenting artifacts (Mid-High)
- Imaging artifacts (High)



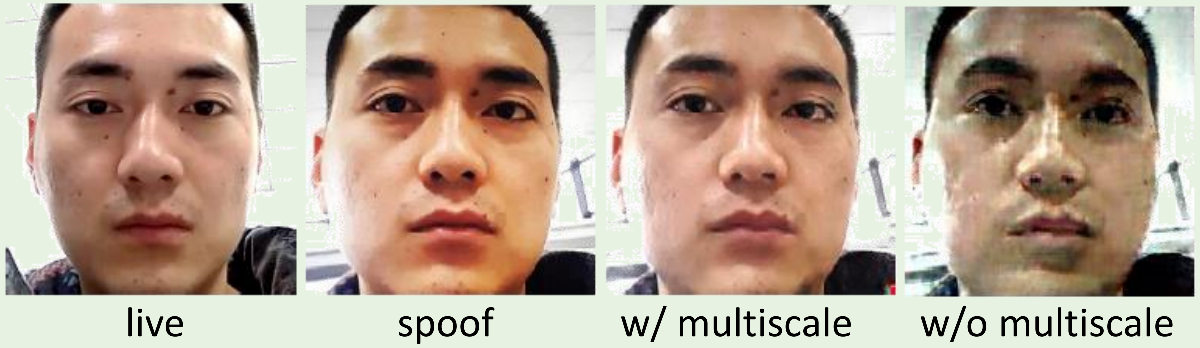
1. Amin Jourabloo, Yaojie Liu, and Xiaoming Liu. Face De-spoofing: Anti-spoofing via noise modeling. *ECCV* 2018.

Generator

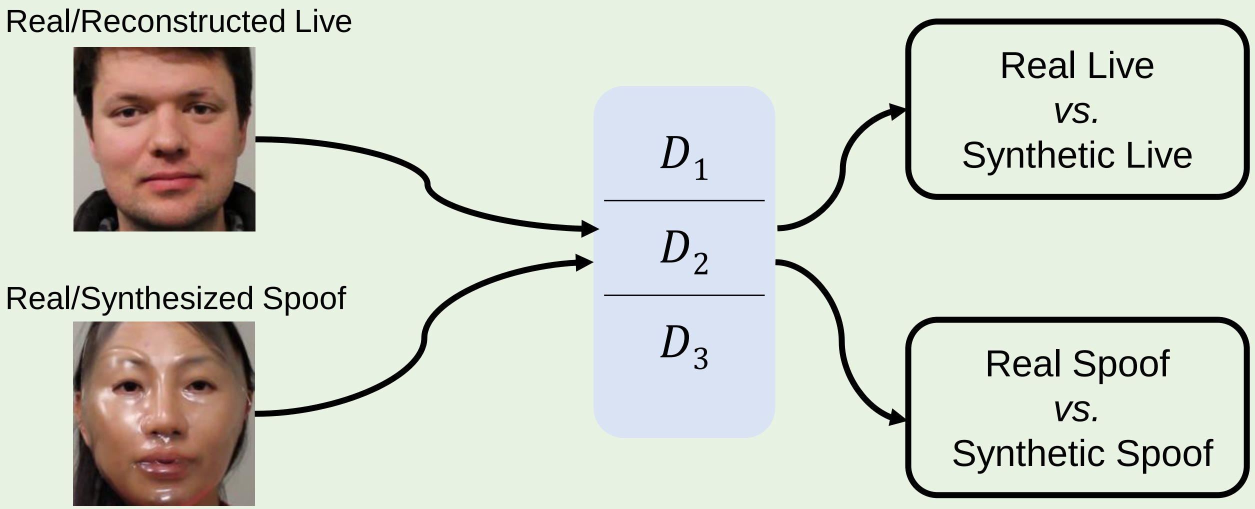


$$
\begin{aligned}
G(\mathbf{I}) &= \mathbf{I} - \hat{\mathbf{I}} \\
&= \mathbf{I} - ((1 - \mathbf{s})\mathbf{I} - \mathbf{b} - \lfloor \mathbf{C} \rceil_N - \mathbf{T}) \\
&= \mathbf{s}\mathbf{I} + \mathbf{b} + \lfloor \mathbf{C} \rceil_N + \mathbf{T},
\end{aligned}
$$

Generator
1. U-Net
2. Disentangle traces into multiscale elements
   - Color distortion
   - Content distortion
   - Texture distortion
3. Auxiliary depth estimation

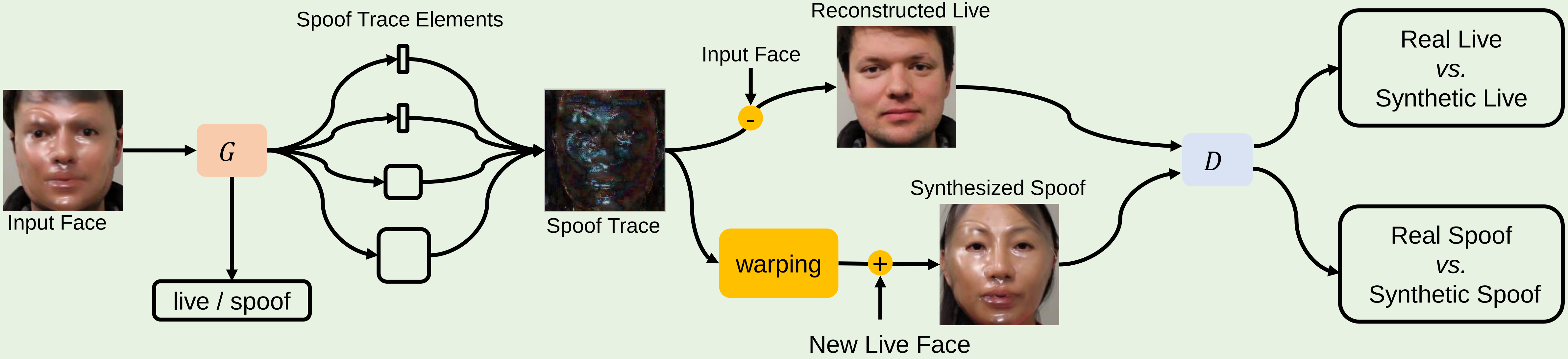


Discriminators



Discriminators
1. Multi-scale discriminators
2. LS-GAN

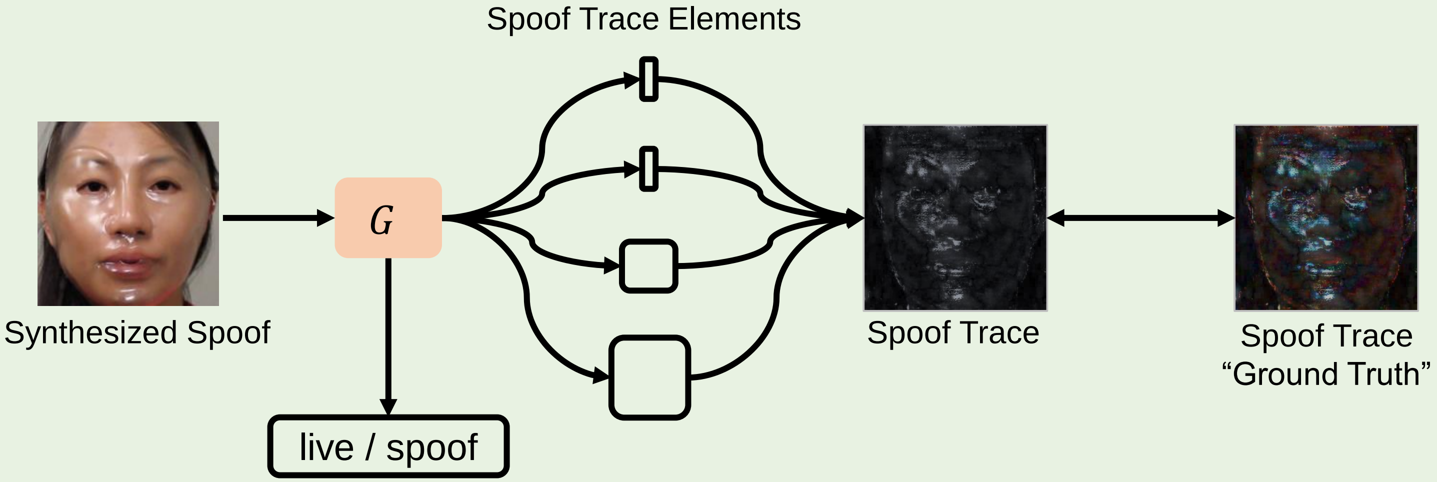
Training



G Step
1. Estimate the spoof trace
2. Estimate the spoofness map
3. Step1 trained with GAN loss and L2 regularization
4. Step2 trained with ground truth

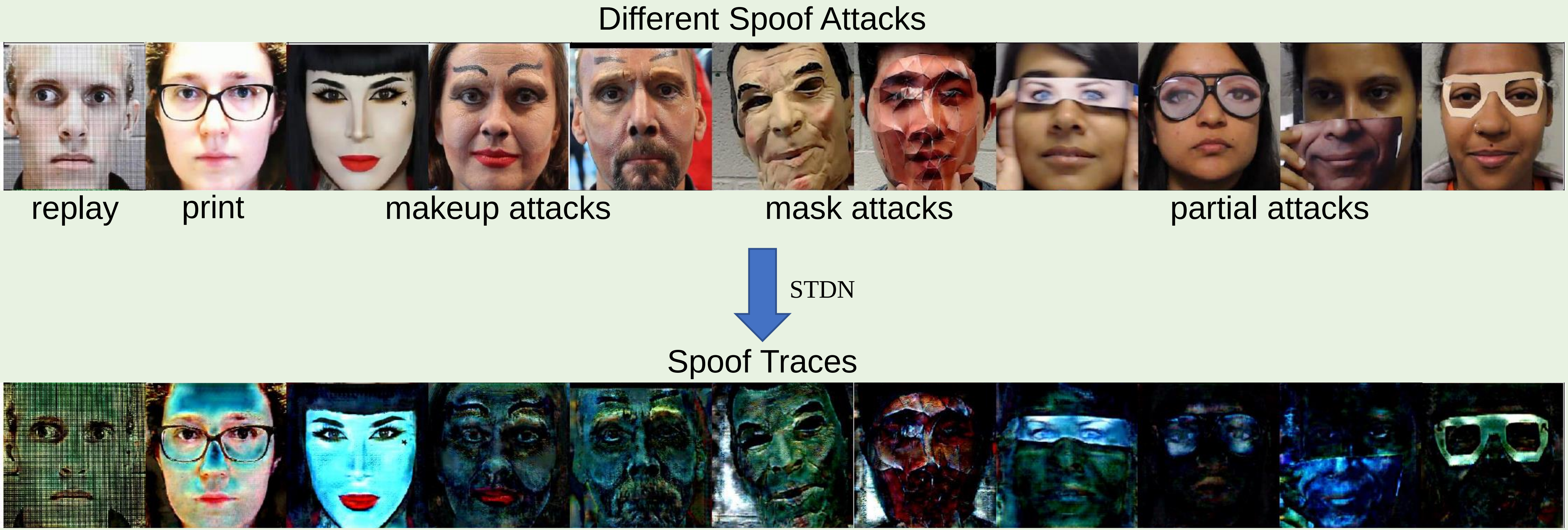
D Step
1. Reconstruct the live counterpart
2. Warp trace and synthesize new spoof faces
3. Step1&2 trained with multi-scale discriminators

Addition Training Step



A Step
1. Estimate the spoofness
2. Estimate the spoof trace
3. Step1&2 trained with ground truth

Visualization



Visualization

New Live Faces

+

Spoof Traces

=

New Spoof Faces

Summary

- Direct FAS
  - Vanilla CNN
  - Patch-based CNN
- Auxiliary FAS
  - Auxiliary tasks
  - Advanced architecture
- Temporal FAS
  - Temporal auxiliary tasks
  - Temporal consistency
- Generative FAS
  - Data augmentation
  - Spoof patterns

End of Session I

7 Minutes Break

MICHIGAN STATE UNIVERSITY

Computer Vision Lab

IJCB 2020