Session II
Face Anti-Spoofing Generalization

Host: Yaojie Liu

MICHIGAN STATE UNIVERSITY

Computer Vision Lab

IJCB 2020

Training-Testing Difference

The testing scenarios are different with the training phase.

- Environment (Lighting, Indoor/outdoor, etc.)
- Camera/Image quality
- Subjects (Age, Race, etc.)
- Spoof types

Training-Testing Difference

The testing scenarios are different with the training phase.

- Environment (Lighting, Indoor/outdoor, etc.)
- Camera/Image quality
- Subjects (Age, Race, etc.)

Cross-database Domain Adaption

- Spoof types

Training-Testing Difference

The testing scenarios are different with the training phase.

- Environment (Lighting, Indoor/outdoor, etc.)
- Camera/Image quality
- Subjects (Age, Race, etc.)
- Spoof types → Unknown Spoof Detection

Outline

- Cross-database domain adaption
- Unknown attack detection
- Testing protocols & evaluation metrics

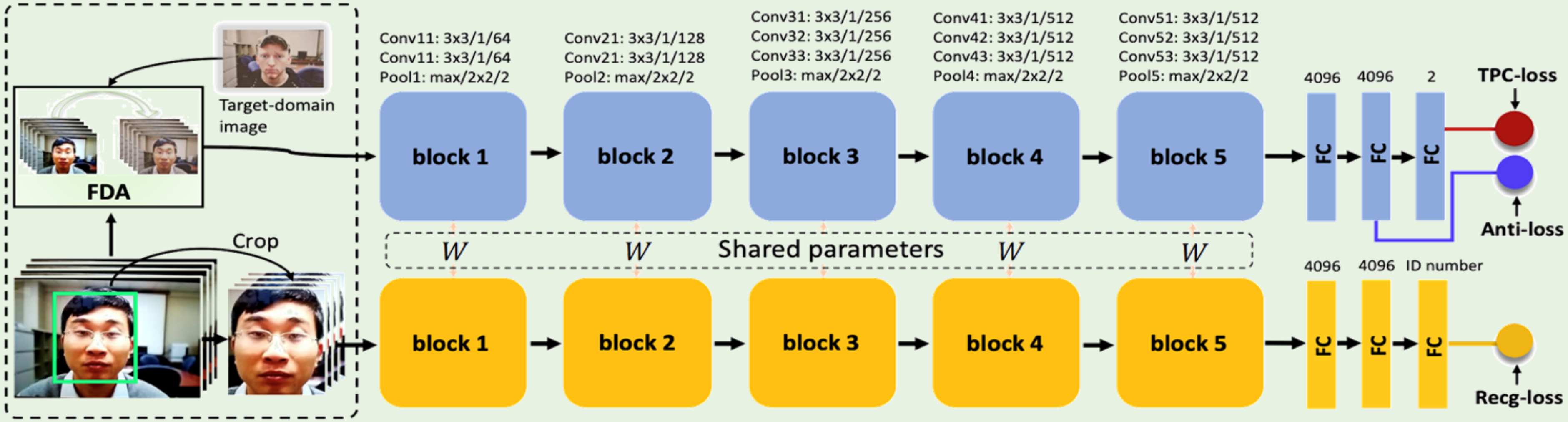
Cross-database Domain Adaption

- Enforce features to be domain-invariant
  - Domain adaption [1,2]
  - Metric learning [3,5,6]
  - Meta learning [7,8]

1. Learning Generalizable and Identity-Discriminative Representations for Face Anti-Spoofing, TIFS, 2018
2. Unsupervised Domain Adaptation for Face Anti-Spoofing, TIFS 2018
3. Multi-adversarial Discriminative Deep Domain Generalization, CVPR, 2019
4. Domain Adaptation in Multi-Channel Autoencoder based Features for Robust Face Anti-Spoofing, ICB 2019
5. Improving Cross-database Face Presentation Attack Detection via Adversarial Domain Adaptation, ICB 2019
6. Single-Side Domain Generalization for Face Anti-Spoofing, CVPR 2020
7. Regularized Fine-grained Meta Face Anti-spoofing, AAAI 2020
8. Learning Meta Model for Zero- and Few-shot Face Anti-spoofing, AAAI 2020

Learning Generalizable and Identity-Discriminative Representations for Face Anti-Spoofing

- Learn face anti-spoofing and face recognition at the same time
- Apply a Fast Domain Adaption (FDA) to remove the bias of different domain
- Share the weights of face anti-spoofing and face recognition



1. Li et. al., Learning Generalizable and Identity-Discriminative Representations for Face Anti-Spoofing, TIFS, 2018

Learning Generalizable and Identity-Discriminative Representations for Face Anti-Spoofing

- Fast Domain Adaption (FDA)
  - Style transfer network
  - Content loss + Style (domain) loss

$$\mathcal{L}_{\text{content}} = \frac{1}{C_j H_j W_j} ||\varphi_j(y) - \varphi_j(x)||_2^2$$

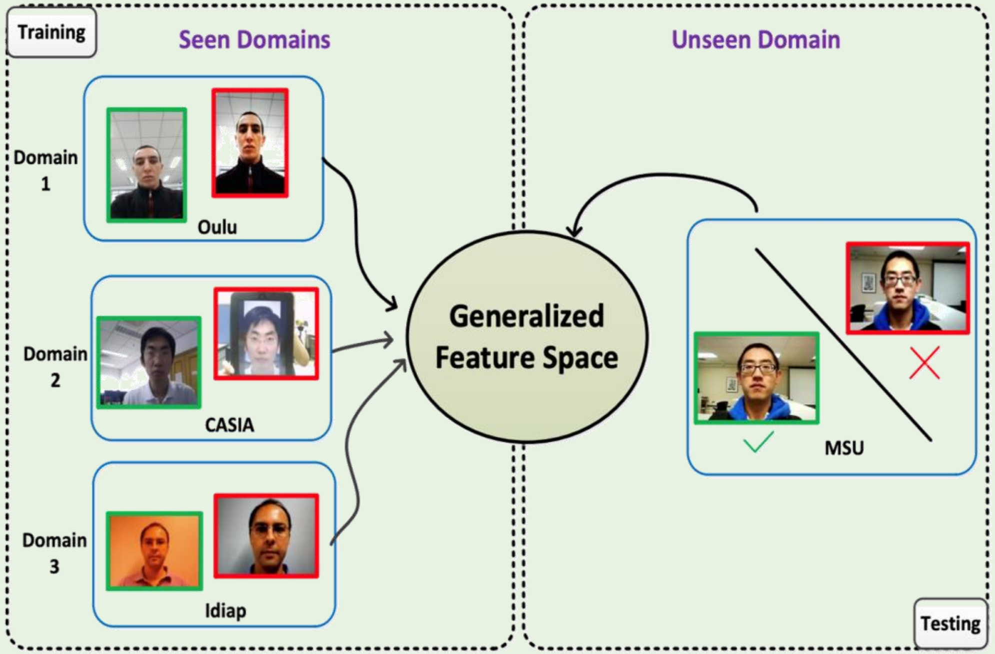
$$\mathcal{L}_{\text{domain}} = \frac{1}{C_j H_j W_j} ||G_j(y) - G_j(y_d)||_F^2$$

$$\hat{y} = \arg\min_P (\lambda_c \mathcal{L}_{\text{content}}(y, x) + \lambda_s \mathcal{L}_{\text{domain}}(y, y_d))$$

1. Li et. al., Learning Generalizable and Identity-Discriminative Representations for Face Anti-Spoofing, TIFS, 2018

Metric learning

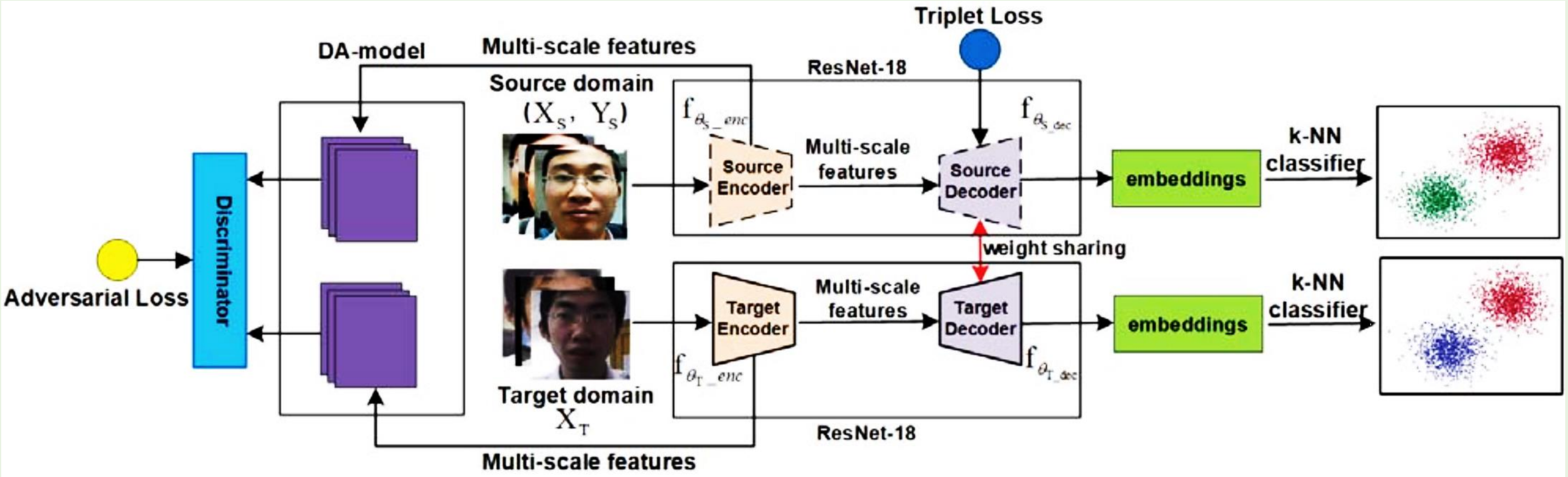
- Adversarial learning
  - learn target features such that discriminator cannot correctly predict the domain
  - remove unrelated features
- Triplet loss
  - learn target features such that live samples from different domains are similar
  - find shared features



1. Multi-adversarial Discriminative Deep Domain Generalization, CVPR, 2019
2. Improving Cross-database Face Presentation Attack Detection via Adversarial Domain Adaptation, ICB 2019
3. Single-Side Domain Generalization for Face Anti-Spoofing, CVPR 2020

Improving Cross-database Face Presentation Attack Detection via Adversarial Domain Adaptation

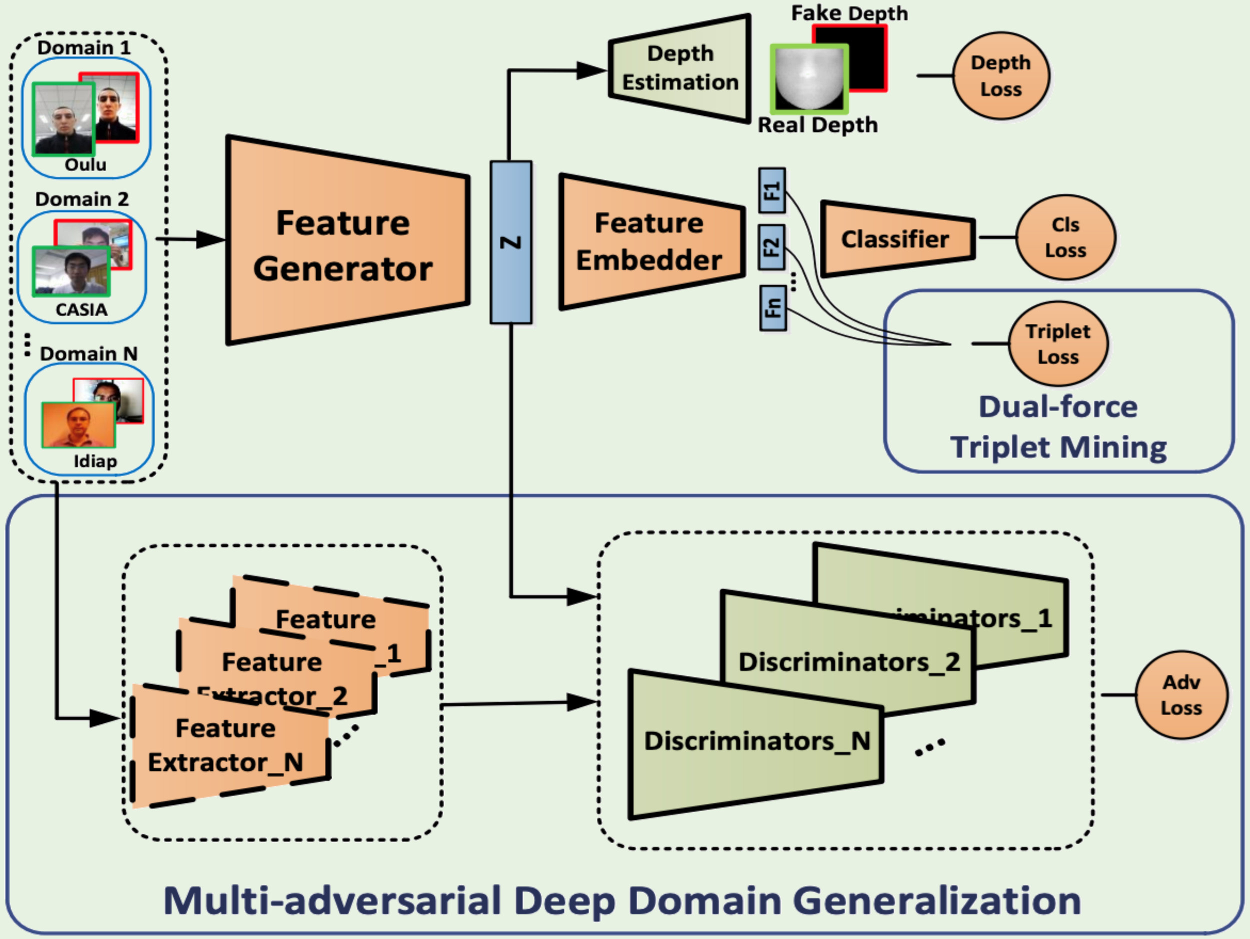
- Pretrain a source encoder/decoder
- Classify with k-NN classifier



1. Wang et. al., Improving Cross-database Face Presentation Attack Detection via Adversarial Domain Adaptation, ICB, 2019

Multi-adversarial Deep Domain Generalization for Face Presentation Attack Detection

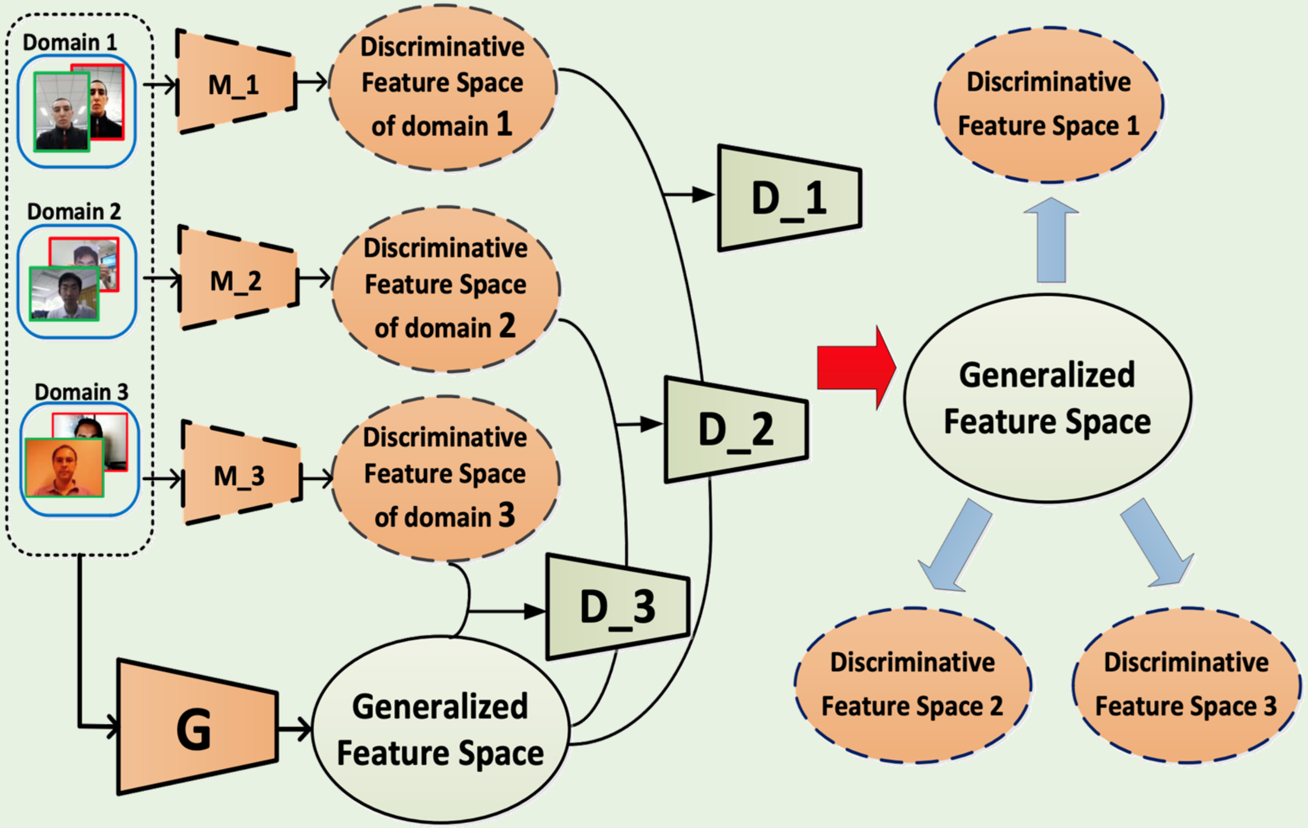
- Feature generator
  - extract features for face anti-spoofing
  - adversarial-trained to remove domain information
- Depth estimation
  - improve the discriminativeness
- Dual-force triplet mining
  - enforce a smaller intra-class distance
  - enforce a larger inter-class distance
  - cross domain



1. Shao et. al., Multi-adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection, CVPR, 2019

Multi-adversarial Deep Domain Generalization for Face Presentation Attack Detection

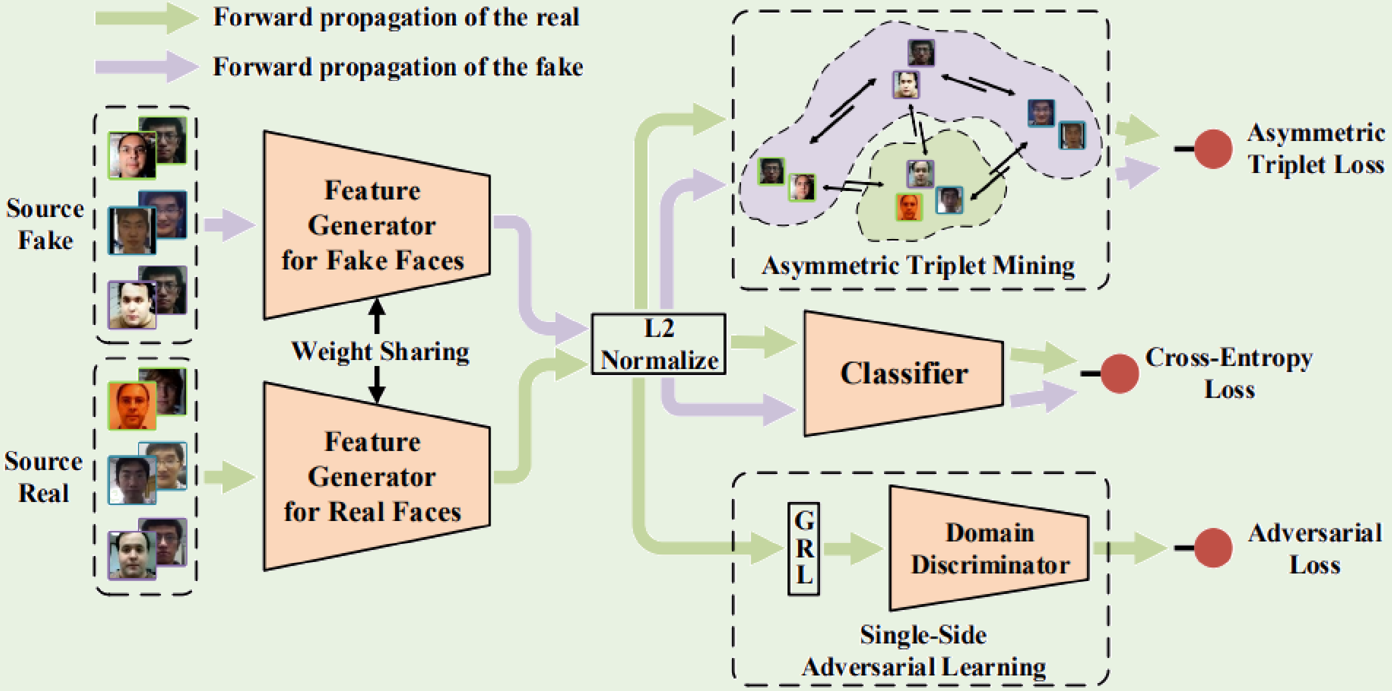
- M1, M2, M3: domain specified features
- G: generalized features
- G and D1, D2, D3 compete



1. Shao et. al., Multi-adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection, CVPR, 2019

Single-Side Domain Generalization for Face Anti-Spoofing

- The parameter sharing feature generator is trained to make the feature distributions of different domains undistinguishable **for the real faces** but not for the fake ones under the single-side adversarial learning.



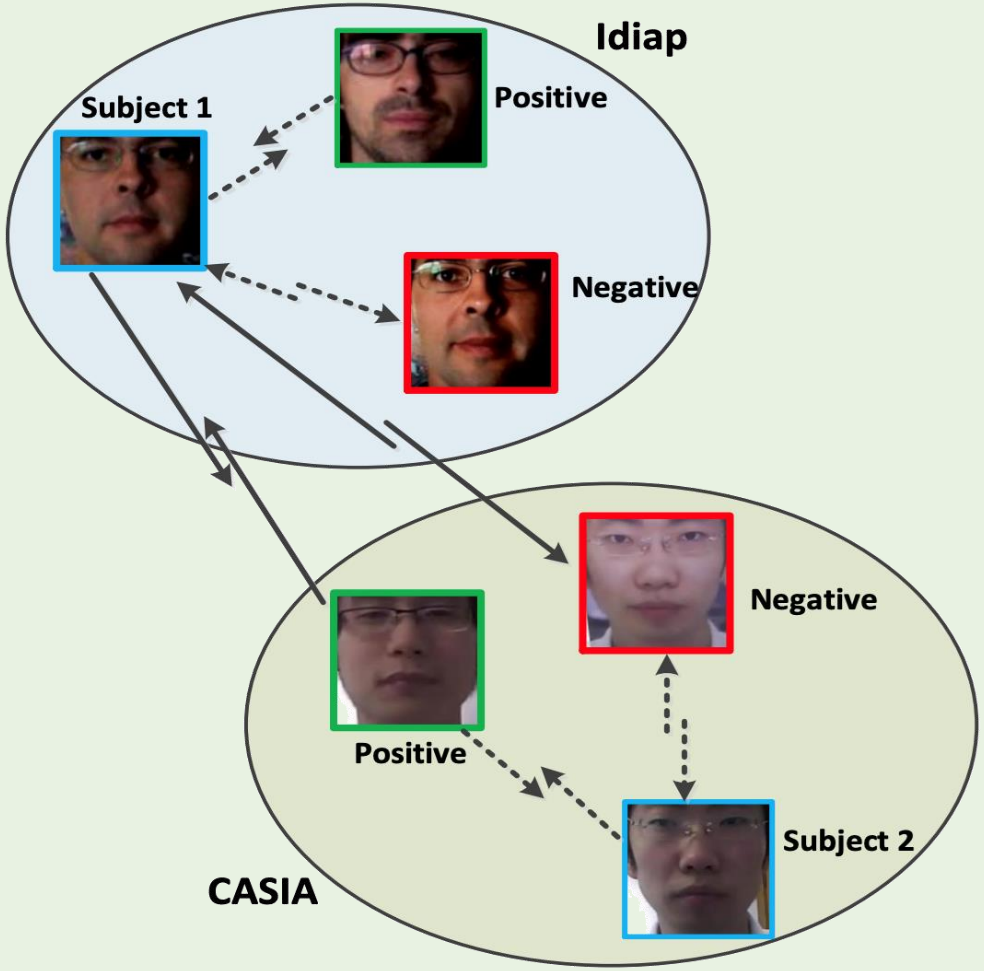
1. Single-Side Domain Generalization for Face Anti-Spoofing, CVPR 2020

Dual-force Triplet Mining

- In one domain
  - Minimize live-to-live distance between different subjects
  - Maximize live-to-spoof distance between different subjects

- Cross domains
  - Minimize live-to-live distance between different subjects
  - Maximize live-to-spoof distance between different subjects

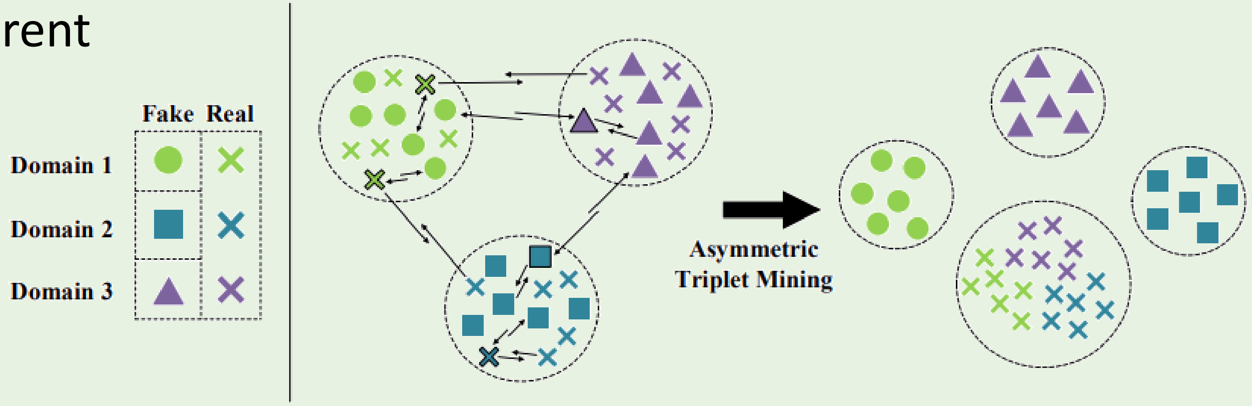
- Anchor as live



1. Shao et. al., Multi-adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection, CVPR, 2019

Dual-force Triplet Mining

- In one domain
  - Minimize live-to-live distance between different subjects
  - Maximize live-to-spoof distance between different subjects



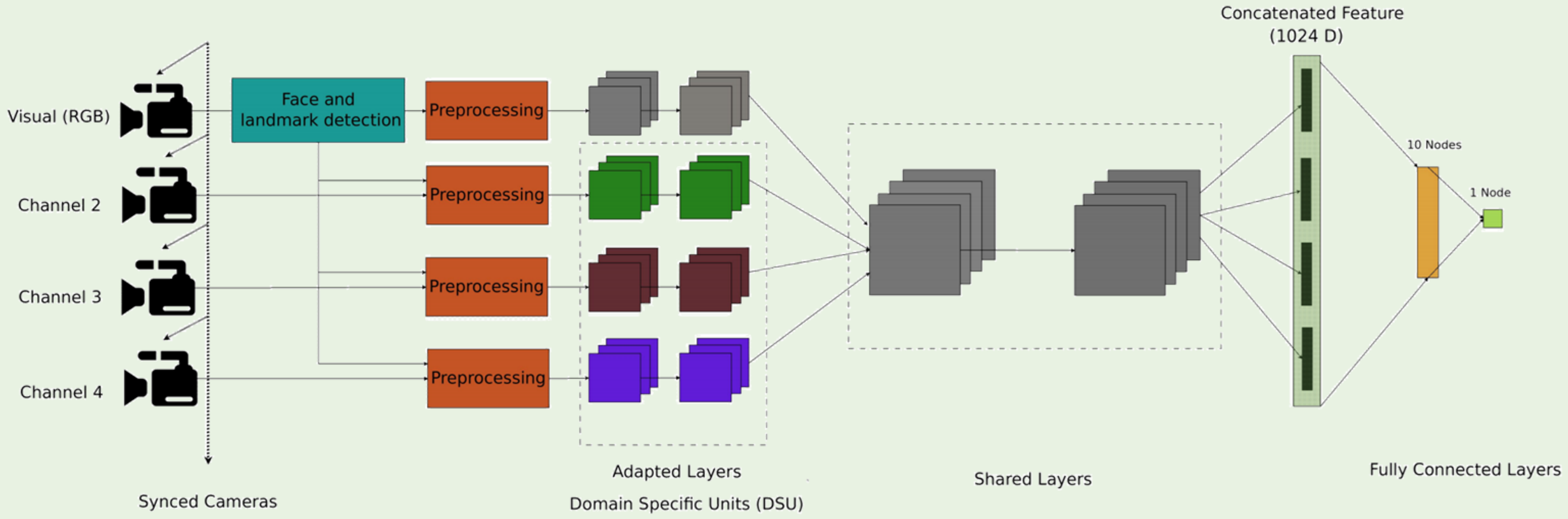
- Cross domains
  - Minimize live-to-live / spoof-to-spoof distance between different subjects only
  - Maximize live-to-spoof / spoof-to-spoof distance between different domains

- Triplet with live (d1,d2,d3), spoof (d1), spoof (d2), spoof(d3)

1. Single-Side Domain Generalization for Face Anti-Spoofing, CVPR 2020

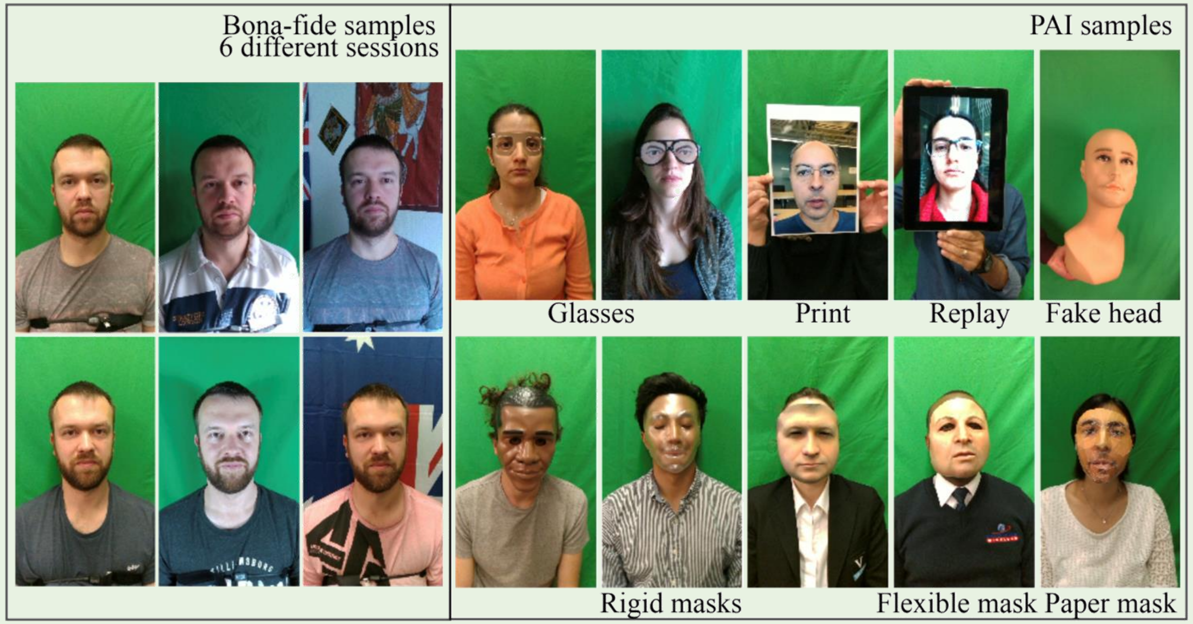
Domain Adaptation in Multi-Channel Autoencoder based Features for Robust Face Anti-Spoofing

- Use multi-modality data (RGB, NIR, and Depth) instead of RGB only
- Domain Adaption: fine-tuning (RGB → NIR-Depth)



1. George et. al., Biometric Face Presentation Attack Detection with Multi-Channel Convolutional Neural Network, TIFS 2019

Domain Adaptation in Multi-Channel Autoencoder based Features for Robust Face Anti-Spoofing

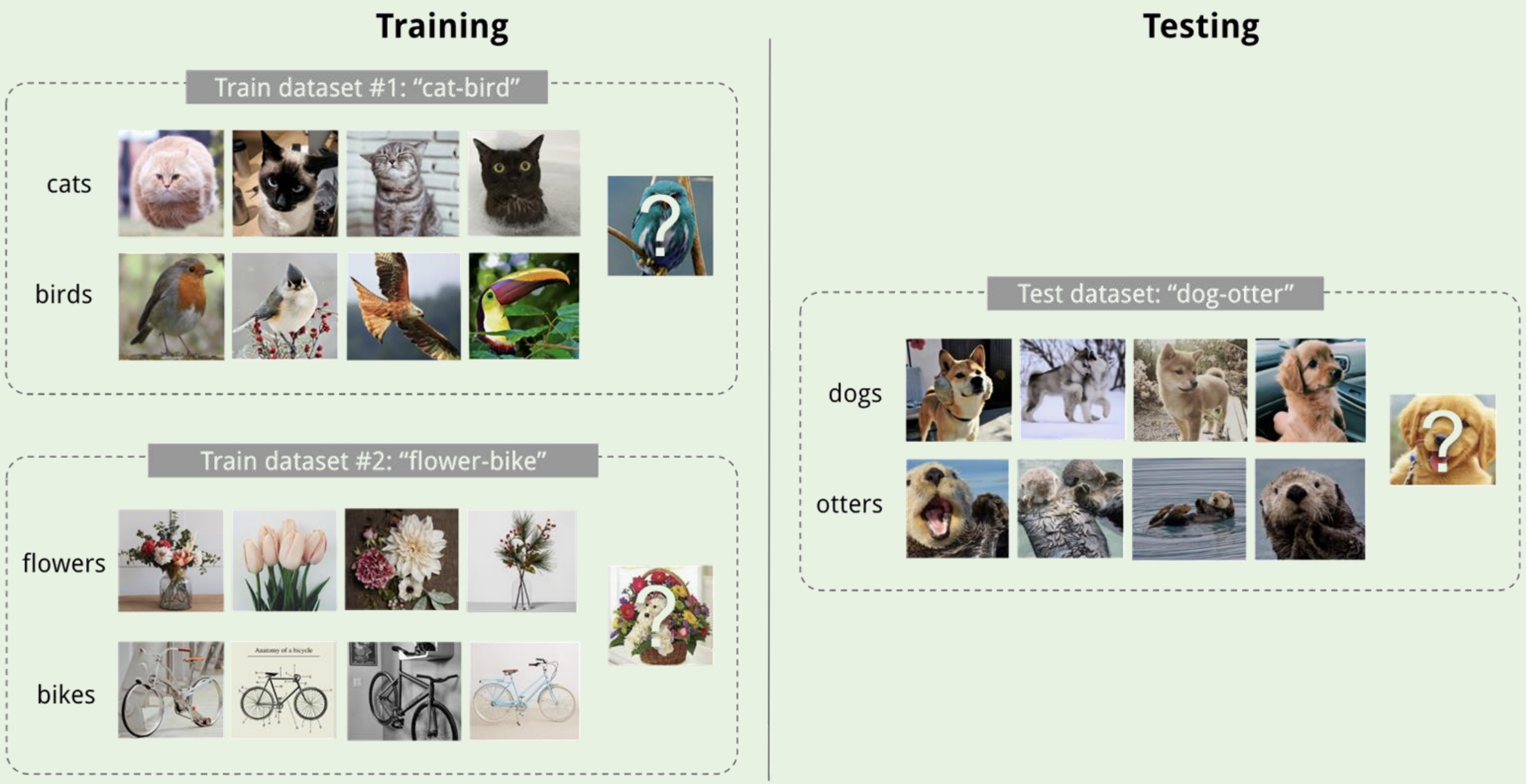


Method	dev (%)		test (%)		
	APCER	ACER	APCER	BPCER	ACER
Color (IQM-LR)	76.58	38.79	87.49	0	43.74
Depth (LBP-LR)	57.71	29.35	65.45	0.03	32.74
Infrared (LBP-LR)	32.79	16.9	29.39	1.18	15.28
Thermal (LBP-LR)	11.79	6.4	16.43	0.5	8.47
Score fusion (IQM-LBP-LR Mean fusion)	10.52	5.76	13.92	1.17	7.54
Color (RDWT-Haralick-SVM)	36.02	18.51	35.34	1.67	18.5
Depth (RDWT-Haralick-SVM)	34.71	17.85	43.07	0.57	21.82
Infrared (RDWT-Haralick-SVM)	14.03	7.51	12.47	0.05	6.26
Thermal (RDWT-Haralick-SVM)	21.51	11.26	24.11	0.85	12.48
Score fusion (RDWT-Haralick-SVM Mean fusion)	6.2	3.6	6.39	0.49	3.44
FASNet	18.89	9.94	17.22	5.65	11.44

1. George et. al., Biometric Face Presentation Attack Detection with Multi-Channel Convolutional Neural Network, TIFS 2019

Meta Learning

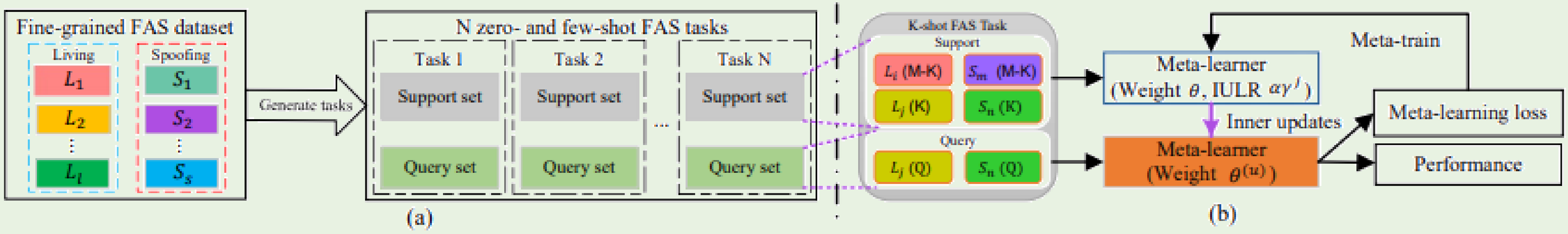
- Meta-learning, also known as “learning to learn”, intends to design models that can learn new skills or adapt to new environments rapidly with a few training examples.



1. Regularized Fine-grained Meta Face Anti-spoofing, AAAI 2020
2. Learning Meta Model for Zero- and Few-shot Face Anti-spoofing, AAAI 2020

Meta Learning for FAS

- Tackle cross-database testing: Train on multiple domains, test on one domain



1. Regularized Fine-grained Meta Face Anti-spoofing, AAAI 2020
2. Learning Meta Model for Zero- and Few-shot Face Anti-spoofing, AAAI 2020

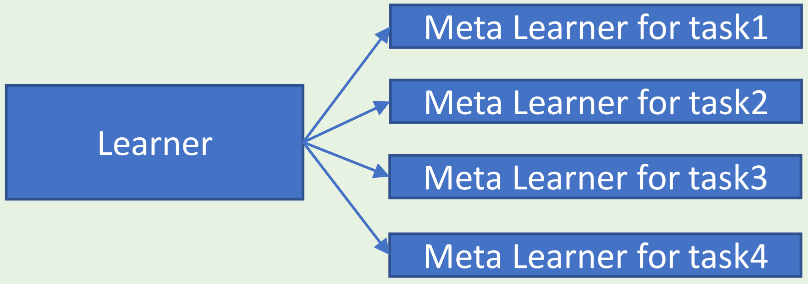
Meta Learning

- A learner to handle all meta learning tasks
- **Training set** (meta-train set +meta-test set), **testing set**
  - E.g., domain 1,2,3 → train, domain 4 → test
    - Meta-task 1: domain 1,2 → meta-train, domain 3 → meta-test
    - Meta-task 2: domain 1,3 → meta-train, domain 2 → meta-test
    - Meta-task 3: domain 2,3 → meta-train, domain 1 → meta-test

Algorithm 1 AIM-FAS in training stage

input: K-shot ($K >= 0$) FAS training tasks Ψ_t, learning rate β, number of inner-update steps u, initial value of AIU parameters α and γ.
output: Meta-learner's weight θ, AIU parameters α and γ.

initialize θ and AIU parameters α and γ.
pre-train the meta-learner on the train set.
while not done **do**
  sample batch tasks $\tau_i \in \Psi_t$
  for each of τ_i **do**
    $\theta_i^{(0)} = \theta$
    for $j < u$ **do**
      $\mathcal{L}_{s(\tau_i)}(\theta_i^{(j)}) \leftarrow \frac{1}{\|s(\tau_i)\|} \sum_{x,y \in s(\tau_i)} l(f_{\theta_i^{(j)}}(x), y)$
      $\theta_i^{(j+1)} \leftarrow \theta_i^{(j)} - \alpha \cdot \gamma^j \cdot \nabla_{\theta_i^{(j)}} \mathcal{L}_{s(\tau_i)}(\theta_i^{(j)})$
      $\mathcal{L}_{q(\tau_i)}(\theta_i^{(j+1)}) \leftarrow \frac{1}{\|q(\tau_i)\|} \sum_{x,y \in q(\tau_i)} l(f_{\theta_i^{(j+1)}}(x), y)$
      $j = j + 1$
    end
  end
  $(\theta, \alpha, \gamma) \leftarrow (\theta, \alpha, \gamma)$ - $\beta \cdot \nabla_{(\theta,\alpha,\gamma)} \sum_{\tau_i} \mathcal{L}_{q(\tau_i)}(\theta_i^{(u)})$
end



1. Learning Meta Model for Zero- and Few-shot Face Anti-spoofing, AAAI 2020

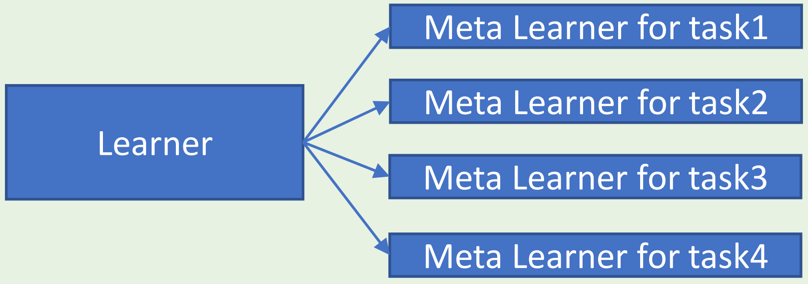
Meta Learning

- A learner to handle all meta learning tasks
- **Training set** (meta-train set +meta-test set), **testing set**
- Choose meta tasks
- Update meta learner (inner update) ← meta-train losses
- Compute meta-test losses
- Update learner with meta-test losses

Algorithm 1 AIM-FAS in training stage

input: K-shot ($K >= 0$) FAS training tasks Ψ_t, learning rate β, number of inner-update steps u, initial value of AIU parameters α and γ.
output: Meta-learner's weight θ, AIU parameters α and γ.

```
initialize θ and AIU parameters α and γ.
pre-train the meta-learner on the train set.
while not done do
    sample batch tasks τ_i ∈ Ψ_t
    for each of τ_i do
        θ_i^(0) = θ
        for j < u do
            L_s(τ_i)(θ_i^(j)) ← 1/||s(τ_i)|| Σ_{x,y∈s(τ_i)} l(f_{θ_i^(j)}(x), y)
            θ_i^(j+1) ← θ_i^(j) − α · γ^j · ∇_{θ_i^(j)} L_s(τ_i)(θ_i^(j))
            L_q(τ_i)(θ_i^(j+1)) ← 1/||q(τ_i)|| Σ_{x,y∈q(τ_i)} l(f_{θ_i^(j+1)}(x), y)
            j = j + 1
        end
    end
    (θ, α, γ) ← (θ, α, γ) - β · ∇_(θ,α,γ) Σ_{τ_i} L_q(τ_i)(θ_i^(u))
end
```



1. Learning Meta Model for Zero- and Few-shot Face Anti-spoofing, AAAI 2020

Meta Learning

- A learner to handle all meta learning tasks
- **Training set** (meta-train set +meta-test set), **testing set**
- Choose meta tasks
- Update meta learner (inner update) ← meta-train losses
- Compute meta-test losses
- Update learner with meta-test losses + meta-train losses

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 T̂_i (i = 1, ..., N − 1)
    for each T̂_i do
        [line 5]
        [line 6]
        [line 7]
    end for
    Meta-test: Sampling batch in D_val as T̃
        [line 10]
        [line 11]
    Meta-optimization:
        [lines 13–15]
end while
return Model parameters θ_F, θ_D, θ_M
```

$$\mathcal{L}_{Cls(\hat{\mathcal{T}}_i)}(\theta_F, \theta_M) = \sum_{(x,y)\sim\hat{\mathcal{T}}_i} ylogM(F(x)) + (1-y)log(1-M(F(x)))$$

$$\theta_{M_i}{}' = \theta_M - \alpha\nabla_{\theta_M}\mathcal{L}_{Cls(\hat{\mathcal{T}}_i)}(\theta_F, \theta_M)$$

$$\mathcal{L}_{Dep(\hat{\mathcal{T}}_i)}(\theta_F, \theta_D) = \sum_{(x,I)\sim\hat{\mathcal{T}}_i} \|D(F(x)) - I\|^2$$

$$\sum_{i=1}^{N-1}\mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_F, \theta_{M_i}{}') = \sum_{i=1}^{N-1}\sum_{(x,y)\sim\tilde{\mathcal{T}}} ylogM_i{}'(F(x)) + (1-y)log(1-M_i{}'(F(x)))$$

$$\mathcal{L}_{Dep(\tilde{\mathcal{T}})}(\theta_F, \theta_D) = \sum_{(x,I)\sim\tilde{\mathcal{T}}} \|D(F(x)) - I\|^2$$

$$\theta_M \leftarrow \theta_M - \beta\nabla_{\theta_M}\Big(\sum_{i=1}^{N-1}\big(\mathcal{L}_{Cls(\hat{\mathcal{T}}_i)}(\theta_F, \theta_M) + \mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_F, \theta_{M_i}{}')\big)\Big)$$

$$\theta_F \leftarrow \theta_F - \beta\nabla_{\theta_F}\Big(\mathcal{L}_{Dep(\tilde{\mathcal{T}})}(\theta_F, \theta_D) + \sum_{i=1}^{N-1}\big(\mathcal{L}_{Cls(\hat{\mathcal{T}}_i)}(\theta_F, \theta_M) + \mathcal{L}_{Dep(\hat{\mathcal{T}}_i)}(\theta_F, \theta_D) + \mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_F, \theta_{M_i}{}')\big)\Big)$$

$$\theta_D \leftarrow \theta_D - \beta\nabla_{\theta_D}\Big(\mathcal{L}_{Dep(\tilde{\mathcal{T}})}(\theta_F, \theta_D) + \sum_{i=1}^{N-1}\big(\mathcal{L}_{Dep(\hat{\mathcal{T}}_i)}(\theta_F, \theta_D)\big)\Big)$$

1. Regularized Fine-grained Meta Face Anti-spoofing, AAAI 2020

Cross-database Domain Adaption

- Enforce features to be domain-invariant
  - Domain adaption [1,2]
  - Metric learning [3,5,6]
  - Meta learning [7,8]

1. Learning Generalizable and Identity-Discriminative Representations for Face Anti-Spoofing, TIFS, 2018
2. Unsupervised Domain Adaptation for Face Anti-Spoofing, TIFS 2018
3. Multi-adversarial Discriminative Deep Domain Generalization, CVPR, 2019
4. Domain Adaptation in Multi-Channel Autoencoder based Features for Robust Face Anti-Spoofing, ICB 2019
5. Improving Cross-database Face Presentation Attack Detection via Adversarial Domain Adaptation, ICB 2019
6. Single-Side Domain Generalization for Face Anti-Spoofing, CVPR 2020
7. Regularized Fine-grained Meta Face Anti-spoofing, AAAI 2020
8. Learning Meta Model for Zero- and Few-shot Face Anti-spoofing, AAAI 2020

Unknown Attack Detection

- One-class classifier
  - One-class SVM
  - Gaussian Mixture Model
  - AutoEncoder
- Zero-shot learning

1. An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol, IEEE Access, 2017
2. Unknown Presentation Attack Detection with Face RGB Images, ICB, 2018
3. Deep Anomaly Detection for Generalized Face Anti-Spoofing, CVPRW, 2019
4. Deep Tree Learning for Zero-shot Face Anti-Spoofing, CVPR 2019

An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol

A very comprehensive study on various hand-crafted feature and classifiers.

- Feature: LBP-TOP, LPQ-TOP, BSIF-TOP, Image quality measures
- Classifier: SVM1, SVM2, LDA2, Sparse representation classifier (SRC)1, SRC 2
- Dataset: CASIA-FASD, Replay-attack, MSU-MFSD

1. Arashlool et. al., An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol, 2017

An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol

A very comprehensive study on various hand-crafted feature and classifiers.

- Feature: LBP-TOP, LPQ-TOP, BSIF-TOP, Image quality measures
- Classifier: SVM1, SVM2, LDA2, Sparse representation classifier (SRC)1, SRC 2
- Dataset: CASIA-FASD, Replay-attack, MSU-MFSD

- Conclusion: neither the two-class systems nor the one-class approaches perform well enough

1. Arashlool et. al., An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol, 2017

Unknown Presentation Attack Detection with Face RGB Images

A very comprehensive study on various hand-crafted feature and classifiers.

- Feature: Color LBP
- Classifier: SVM1, Auto Encoder, GMM
- Dataset: CASIA-FASD, Replay-attack, MSU-MFSD

1. Xiong et. al., Unknown Presentation Attack Detection with Face RGB Images, ICB, 2018

Unknown Presentation Attack Detection with Face RGB Images

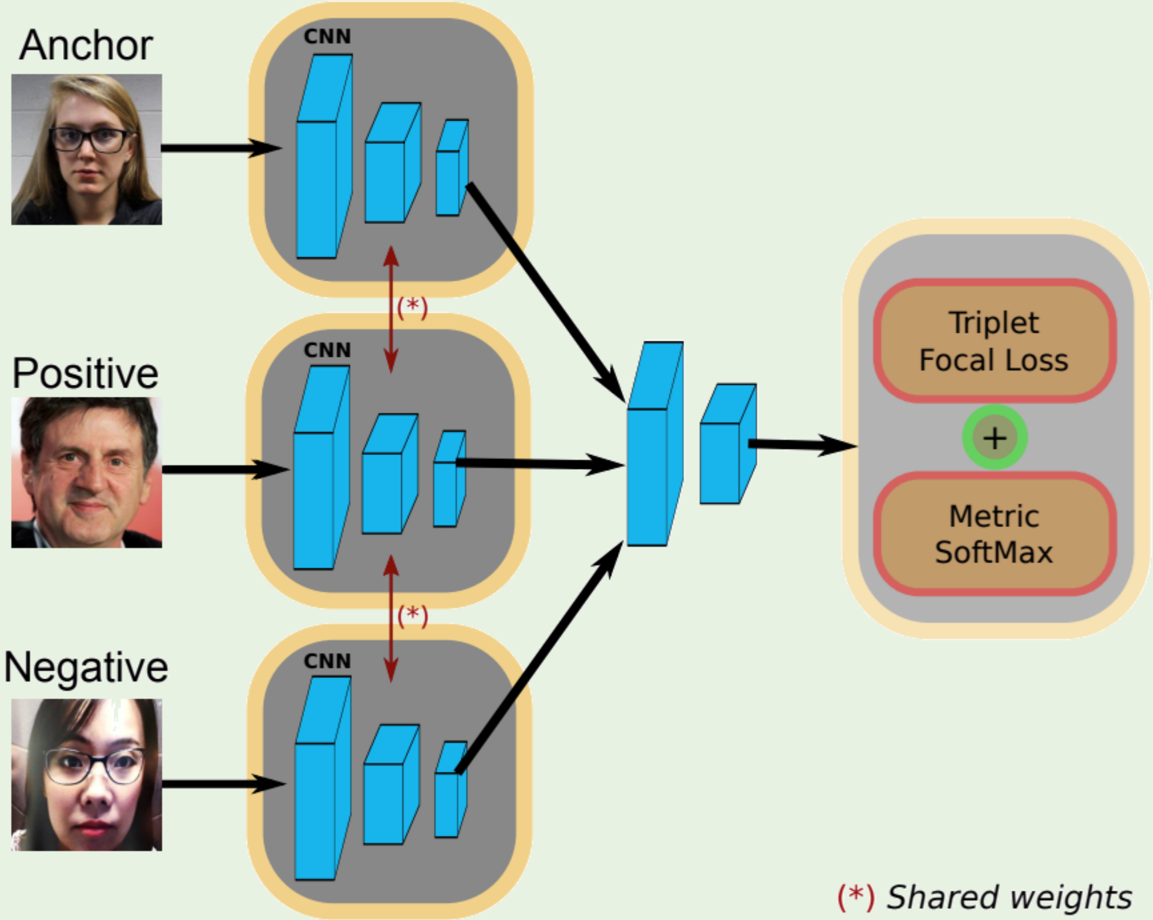
	CASIA			Replay-Attack			MSU			All	
	Video	Cut Photo	Warped Photo	Video	Digital Photo	Printed Photo	Printed Photo	HR Video	Mobile Video	Mean	Std
OC-SVM$_{RBF}$ + IMQ[1]	68.89	61.95	74.80	98.24	90.82	53.23	63.94	63.00	76.38	72.80	14.48
OC-SVM$_{RBF}$ + BSIF[1]	70.74	60.73	95.90	84.03	88.14	73.66	64.81	87.44	74.69	78.68	11.74
SVM$_{RBF}$ + LBP[5]	91.49	91.70	84.47	99.08	98.17	87.28	47.68	99.50	97.61	88.55	16.25
NN + LBP	94.16	88.39	79.85	99.75	95.17	78.86	50.57	99.93	93.54	86.69	15.56
GMM + LBP	90.91	77.52	62.61	93.20	87.80	89.19	68.18	91.21	94.04	83.85	11.60
OC-SVM$_{RBF}$ + LBP	91.21	82.32	65.58	91.55	84.97	87.19	71.46	96.89	93.57	84.97	10.42
AE + LBP	87.00	80.48	65.84	88.62	84.67	85.09	71.25	96.00	95.64	83.84	10.10

- Dataset: CASIA-FASD, Replay-attack, MSU-MFSD

- Conclusion: improve the performance
  - NN+LBP works best on C+R+M protocols
  - AE+LBP works best on Oulu protocols

Deep Anomaly Detection for Generalized Face Anti-Spoofing

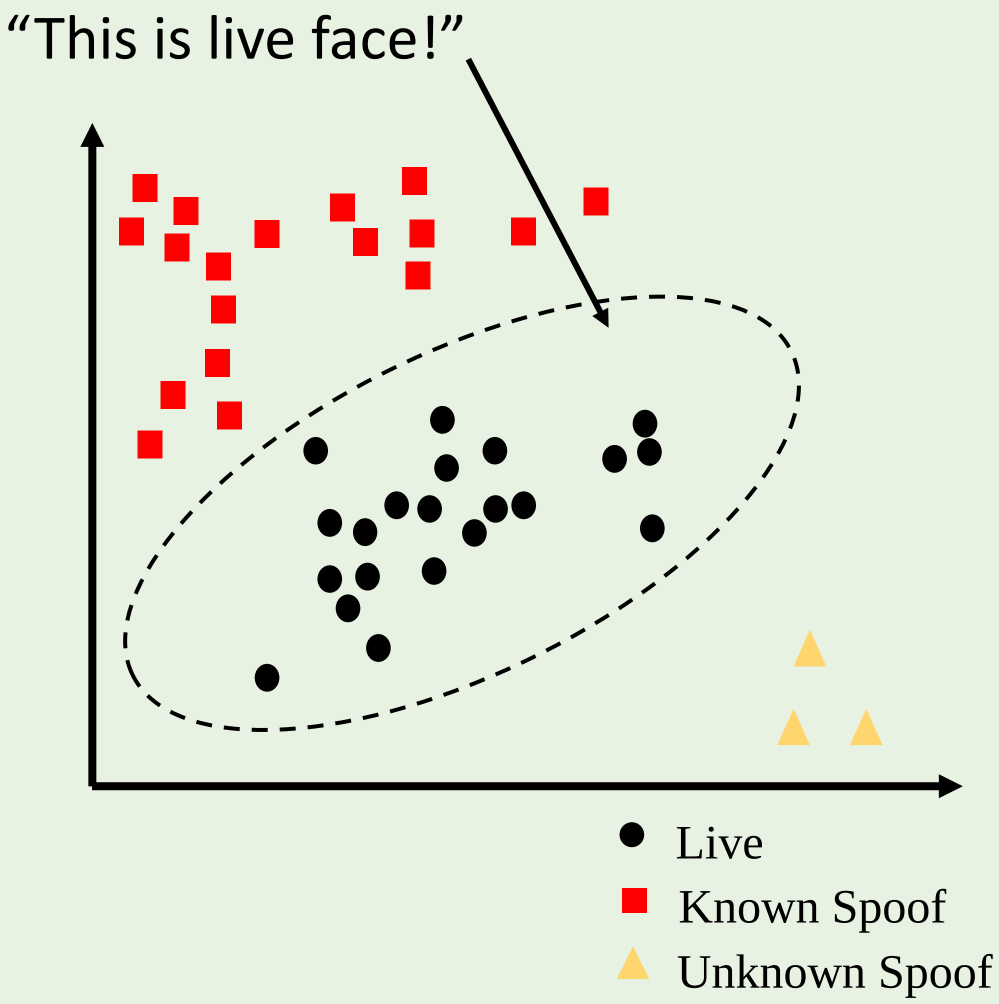
- Deep metric learning
- Triplet Focal loss
  - Focus on the harder cases



1. Perez-Cabo et. al., Deep Anomaly Detection for Generalized Face Anti-Spoofing, CVPRW, 2019

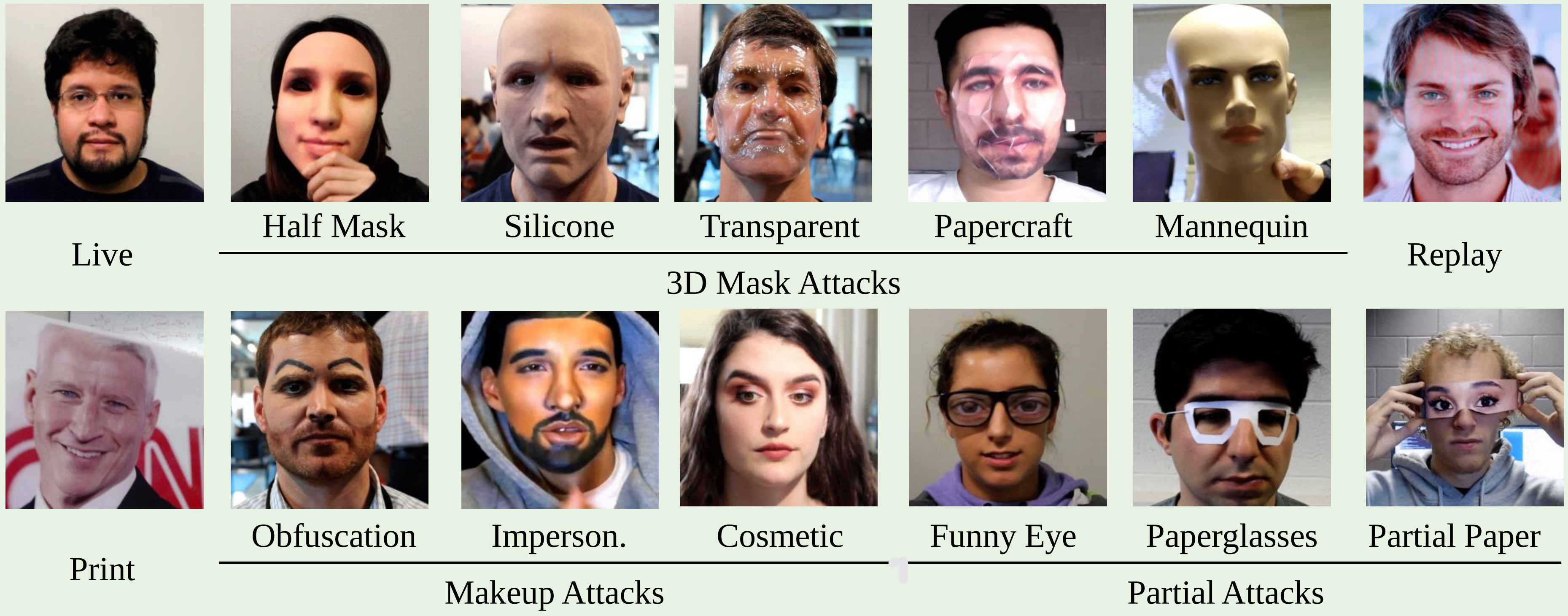
Literature and Issues

- Limited Spoof Types[1,2]
- Only model the live distribution[1,2]



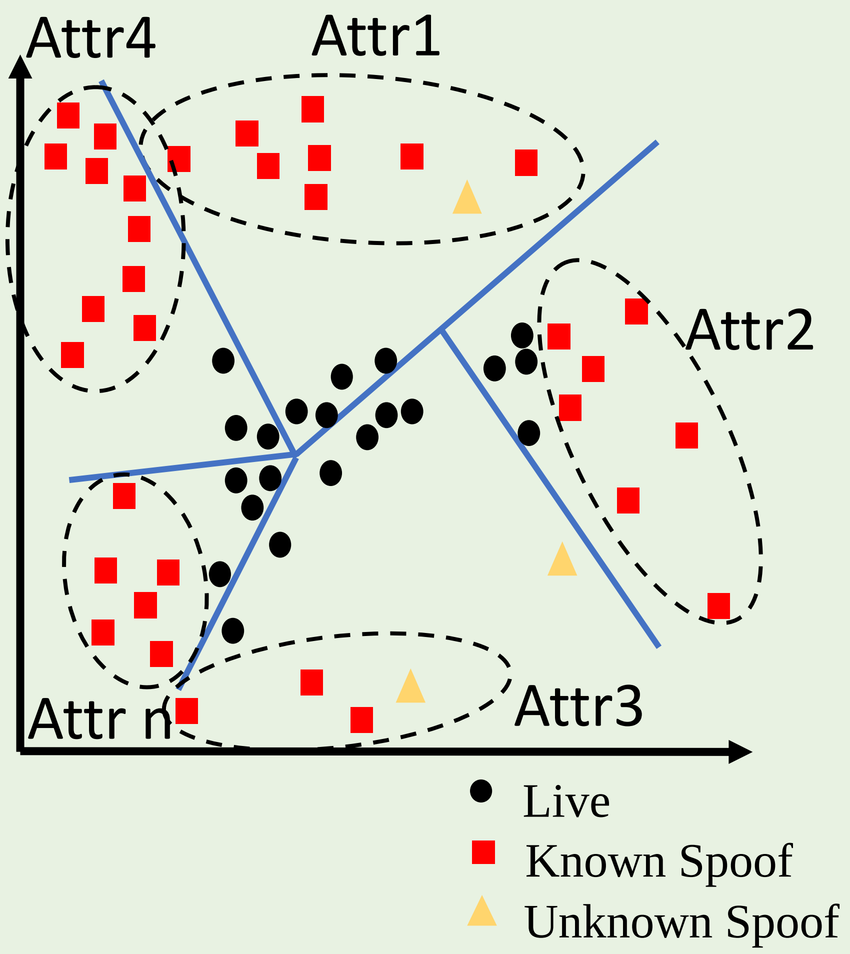
1. S. R. Arashloo et. al. An anomaly detection approach to face spoofing detection: a new formulation and evaluation protocol.
2. F. Xiong and W. Abdalmageed. Unknown presentation attack detection with face RGB images. BTAS 2018

What if More Spoof Types?



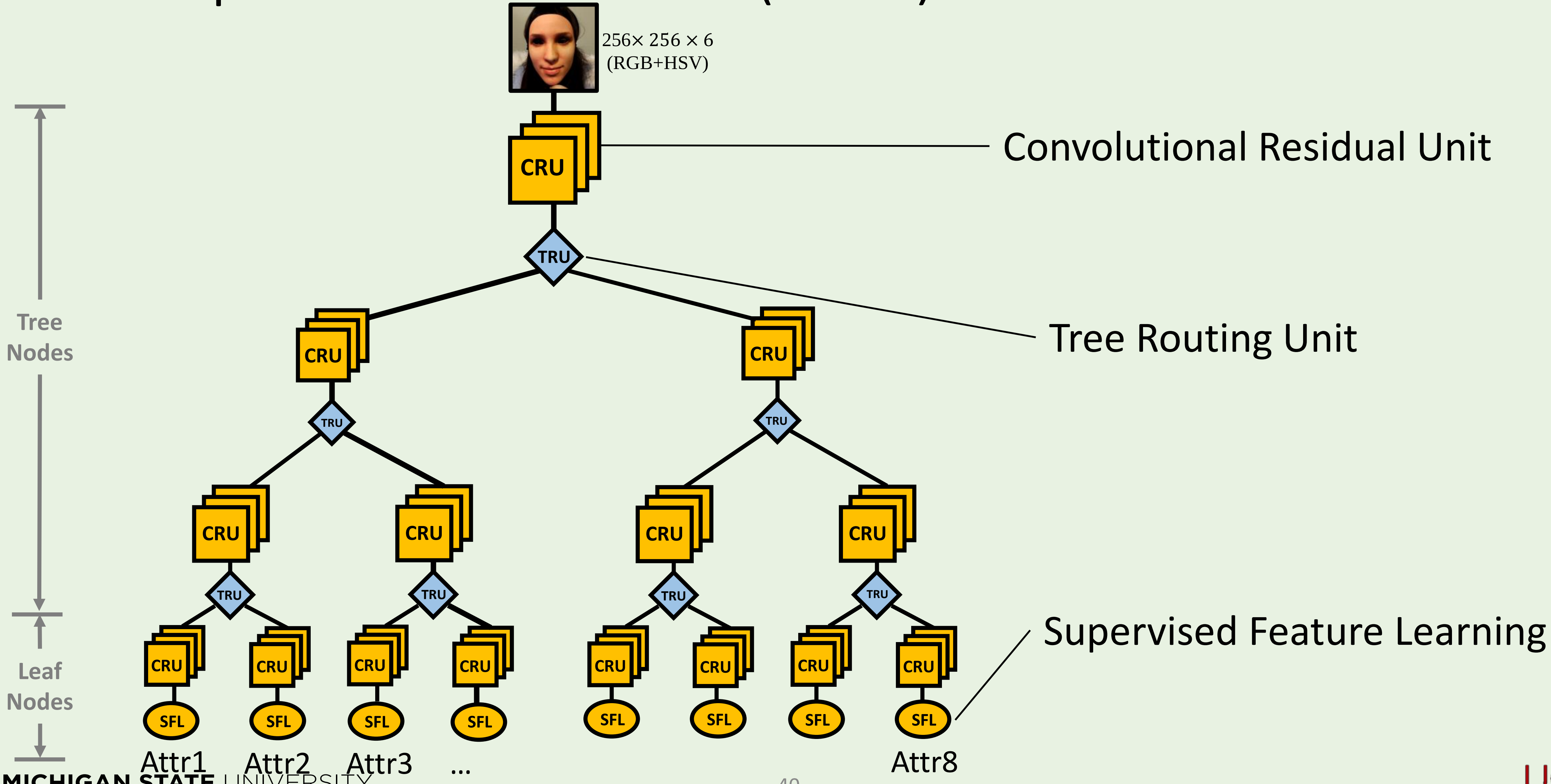
Deep Tree Learning for Zero-shot Face Anti-Spoofing

- Previous methods only model the live
- Learning semantic spoof attributes

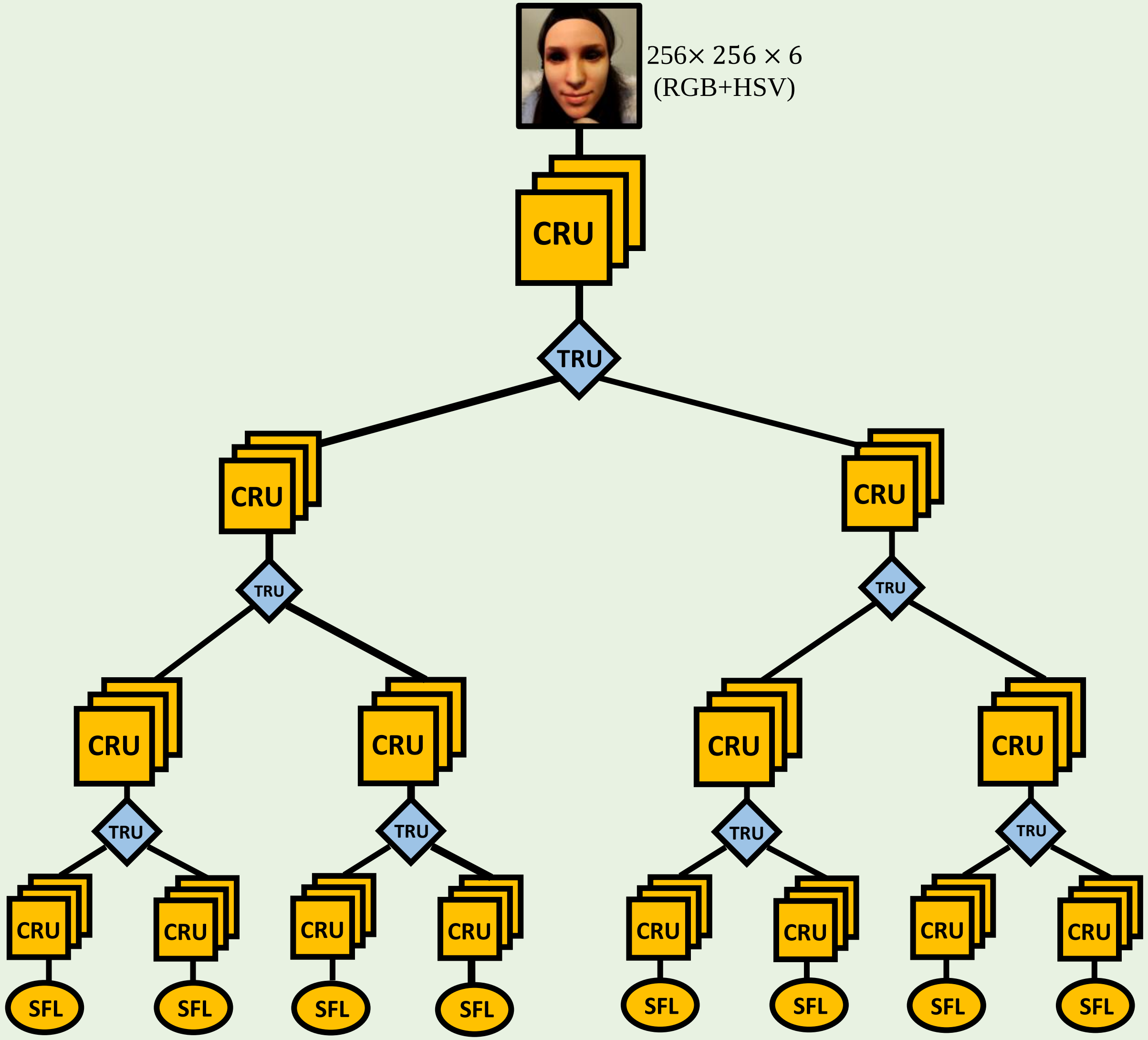


1. Liu et. al., Deep Tree Learning for Zero-shot Face Anti-Spoofing, CVPR 2019

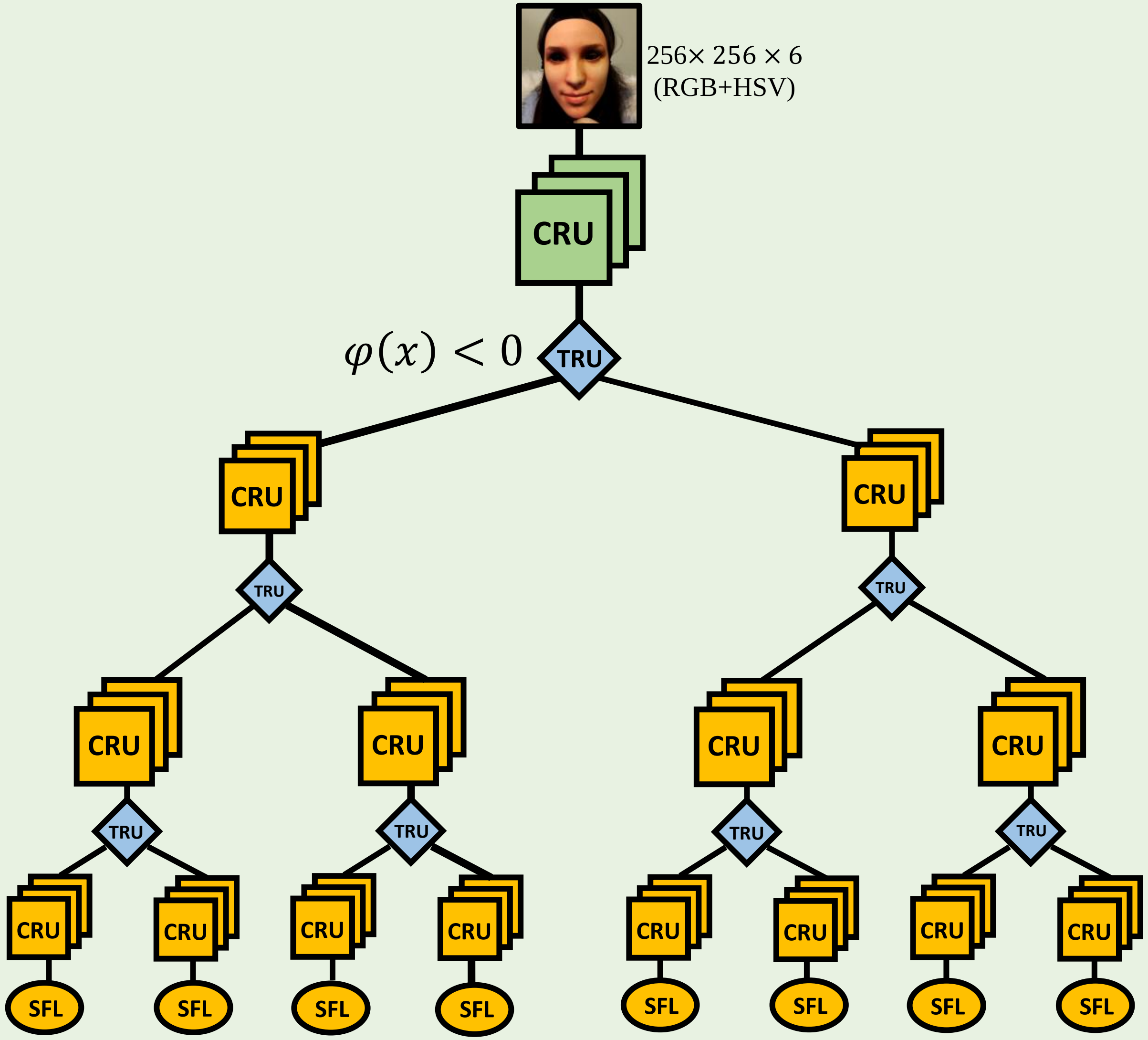
Deep Tree Networks (DTN)



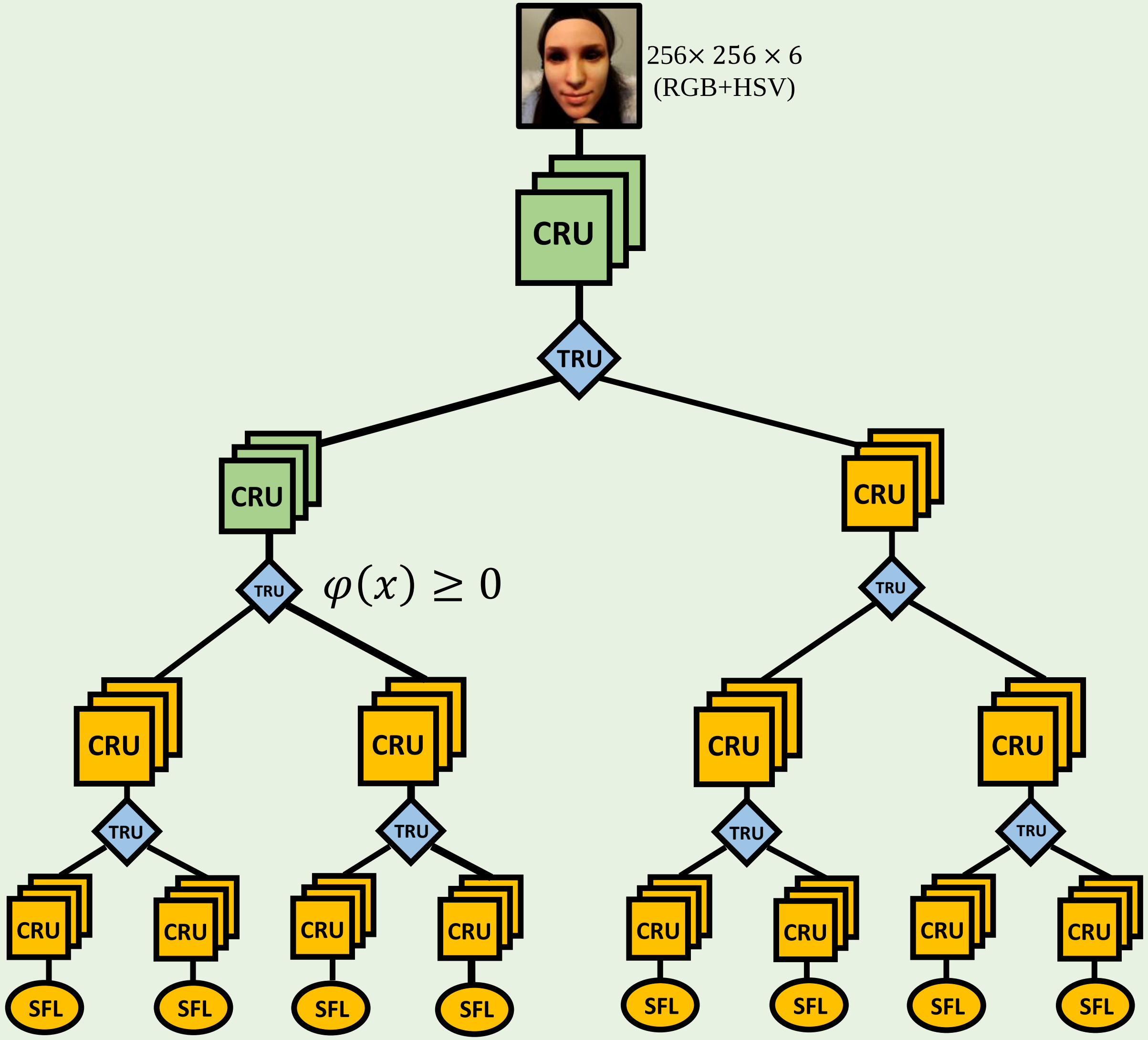
Deep Tree Networks (DTN)



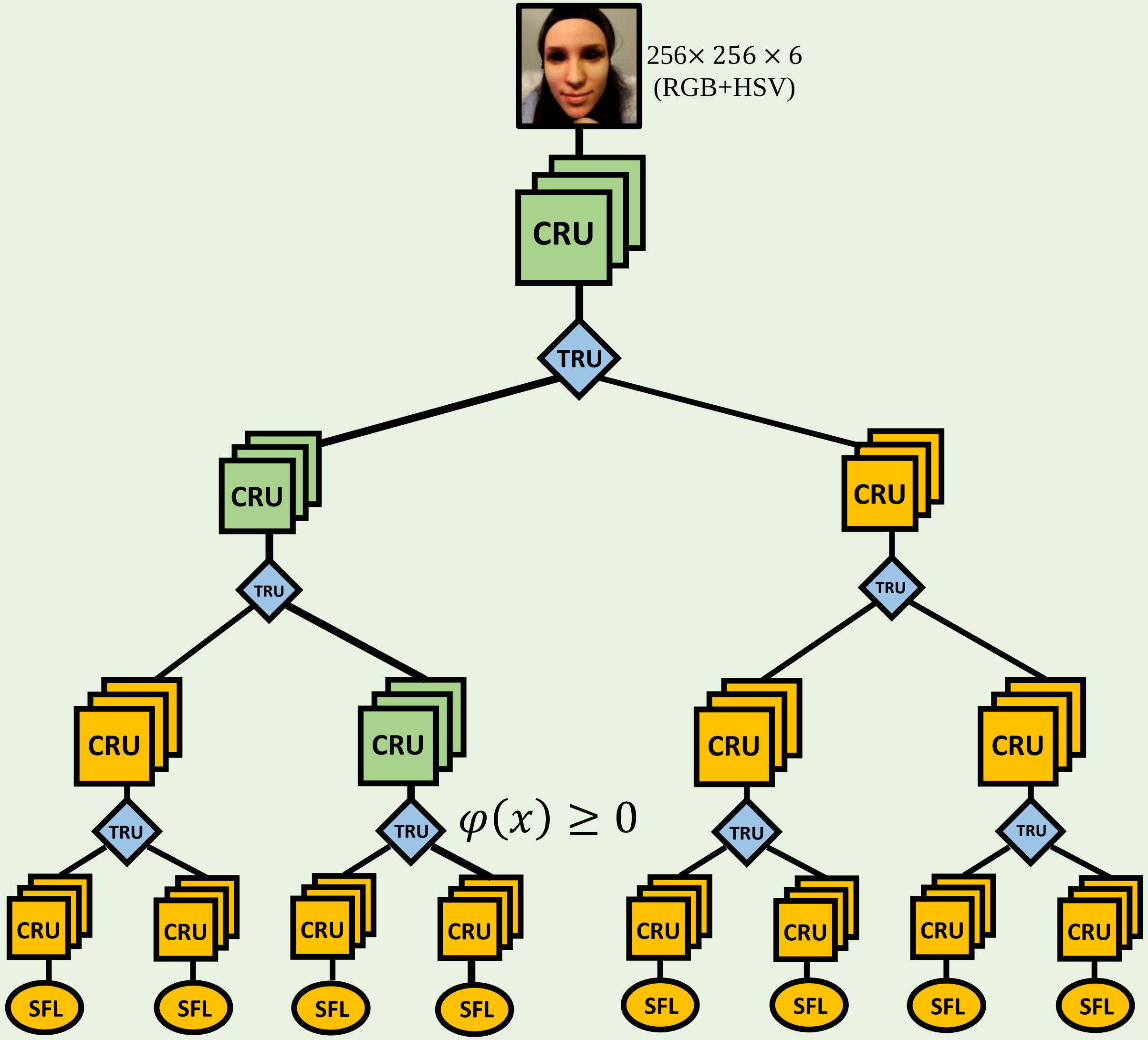
Deep Tree Networks (DTN)



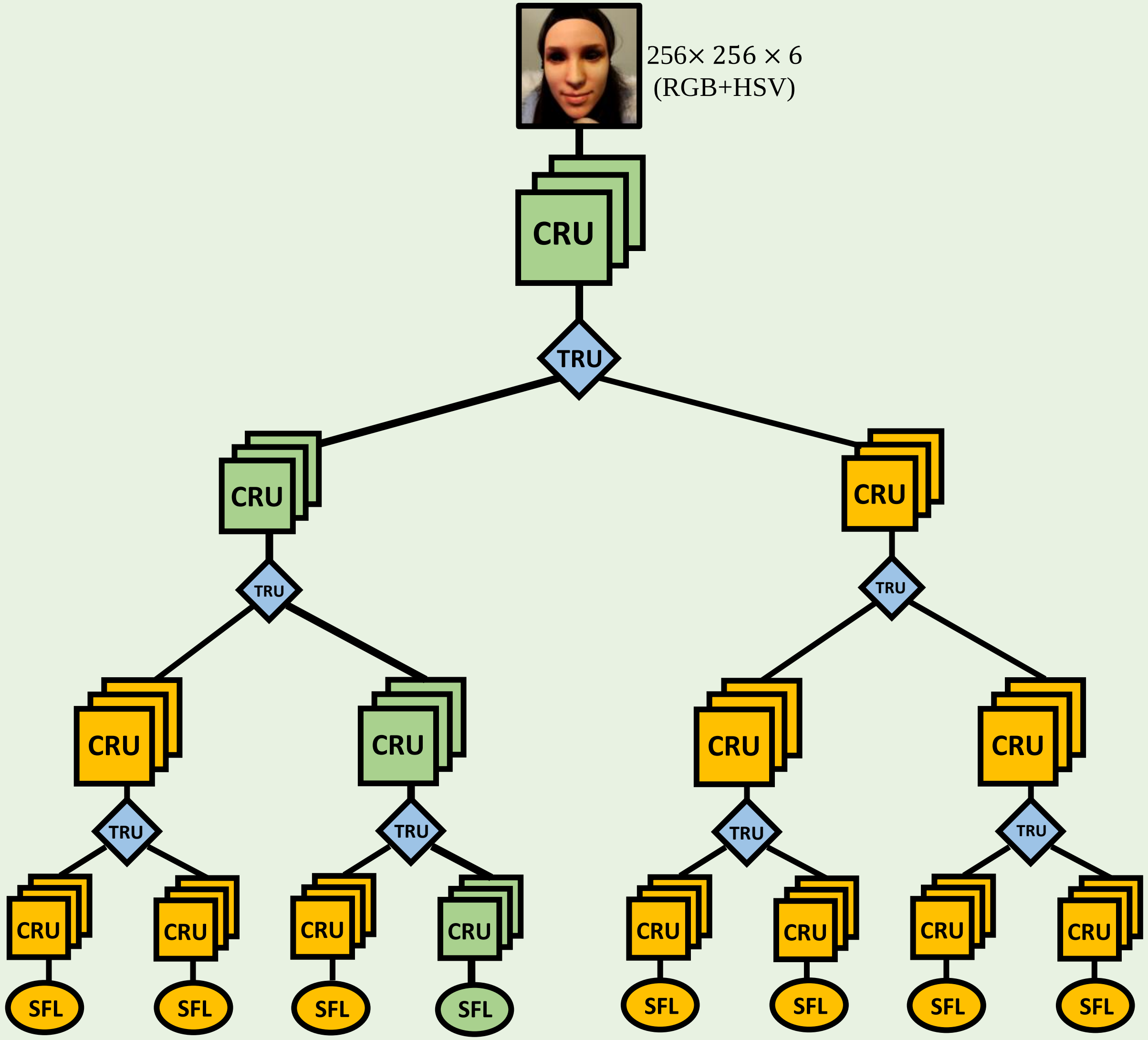
Deep Tree Networks (DTN)



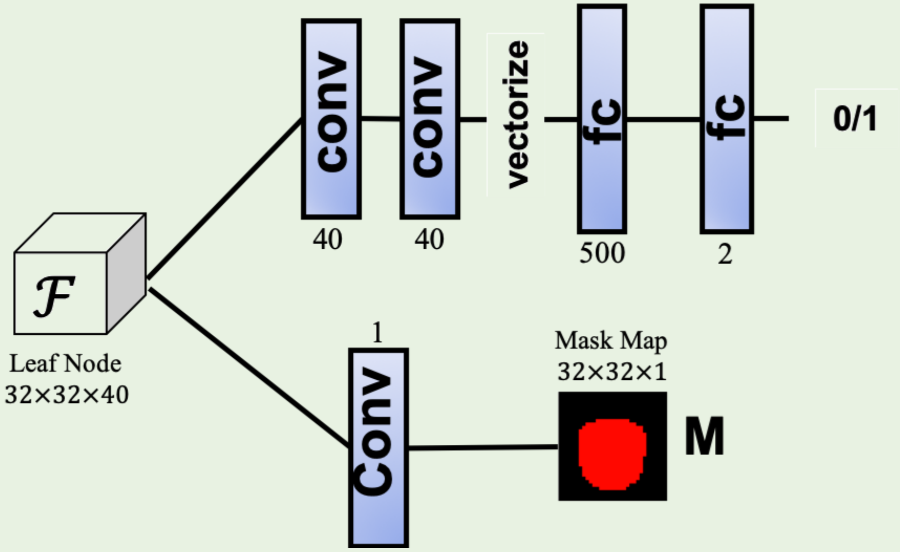
Deep Tree Networks (DTN)

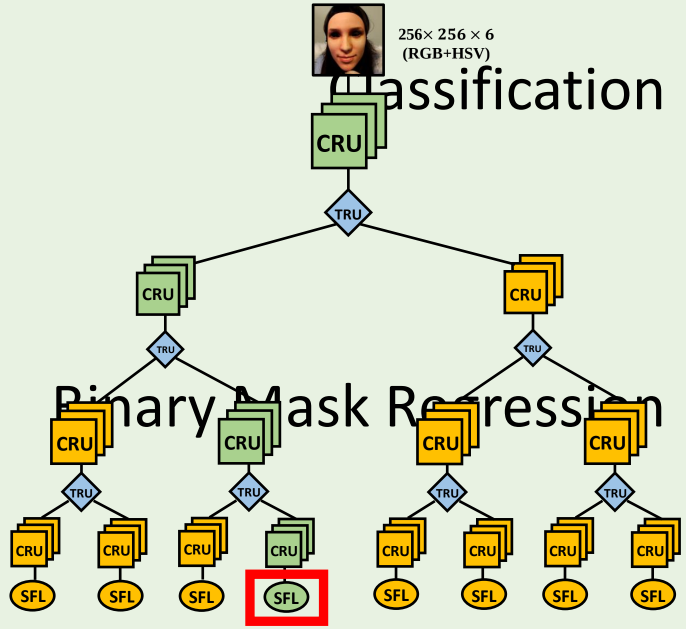


Deep Tree Networks (DTN)

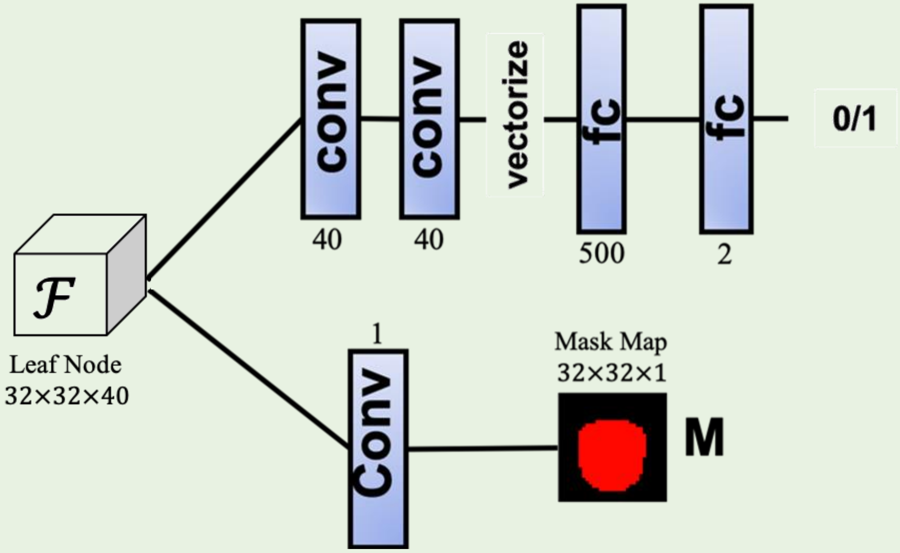


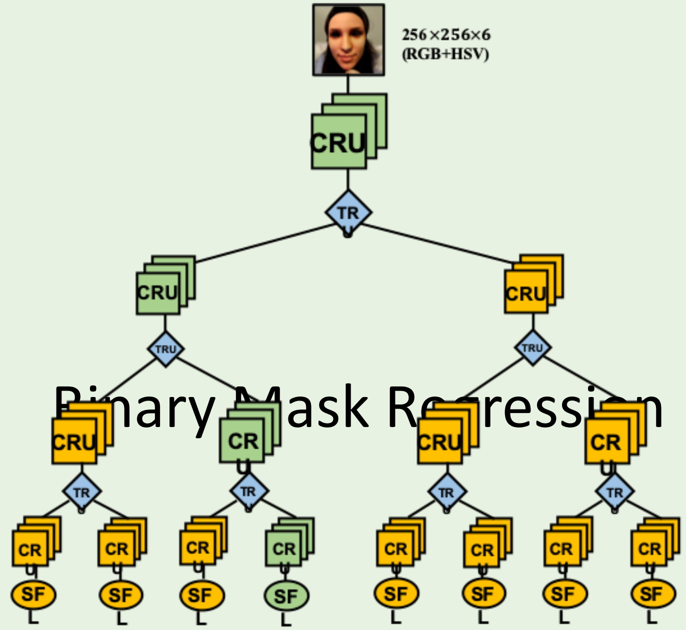
Supervised Feature Learning



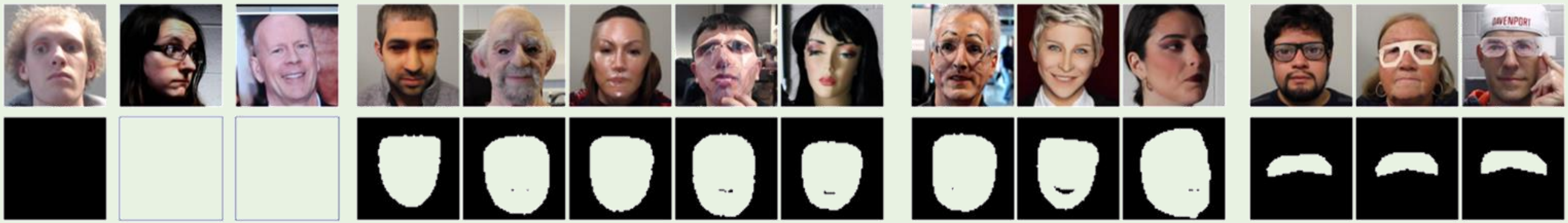


Supervised Feature Learning

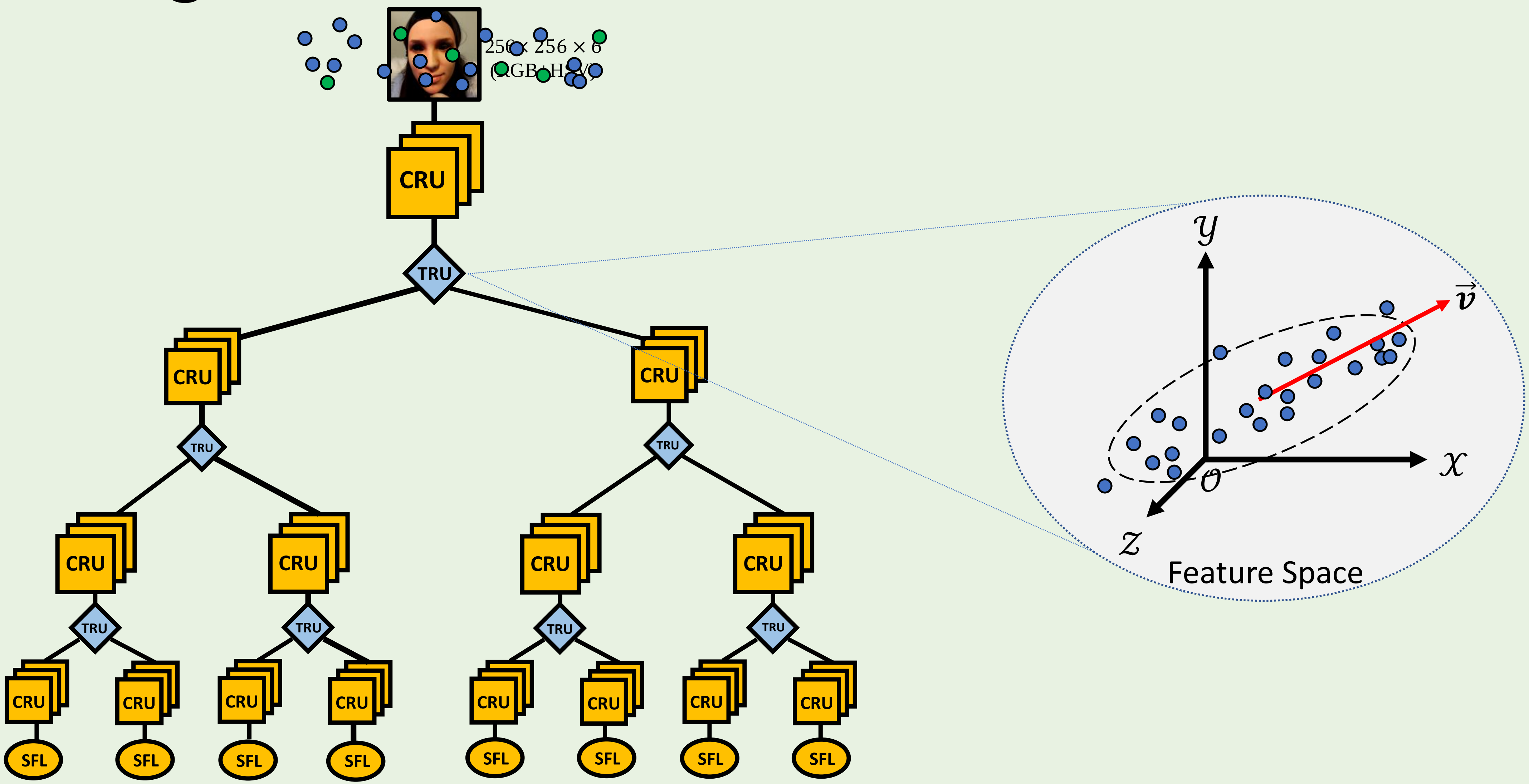




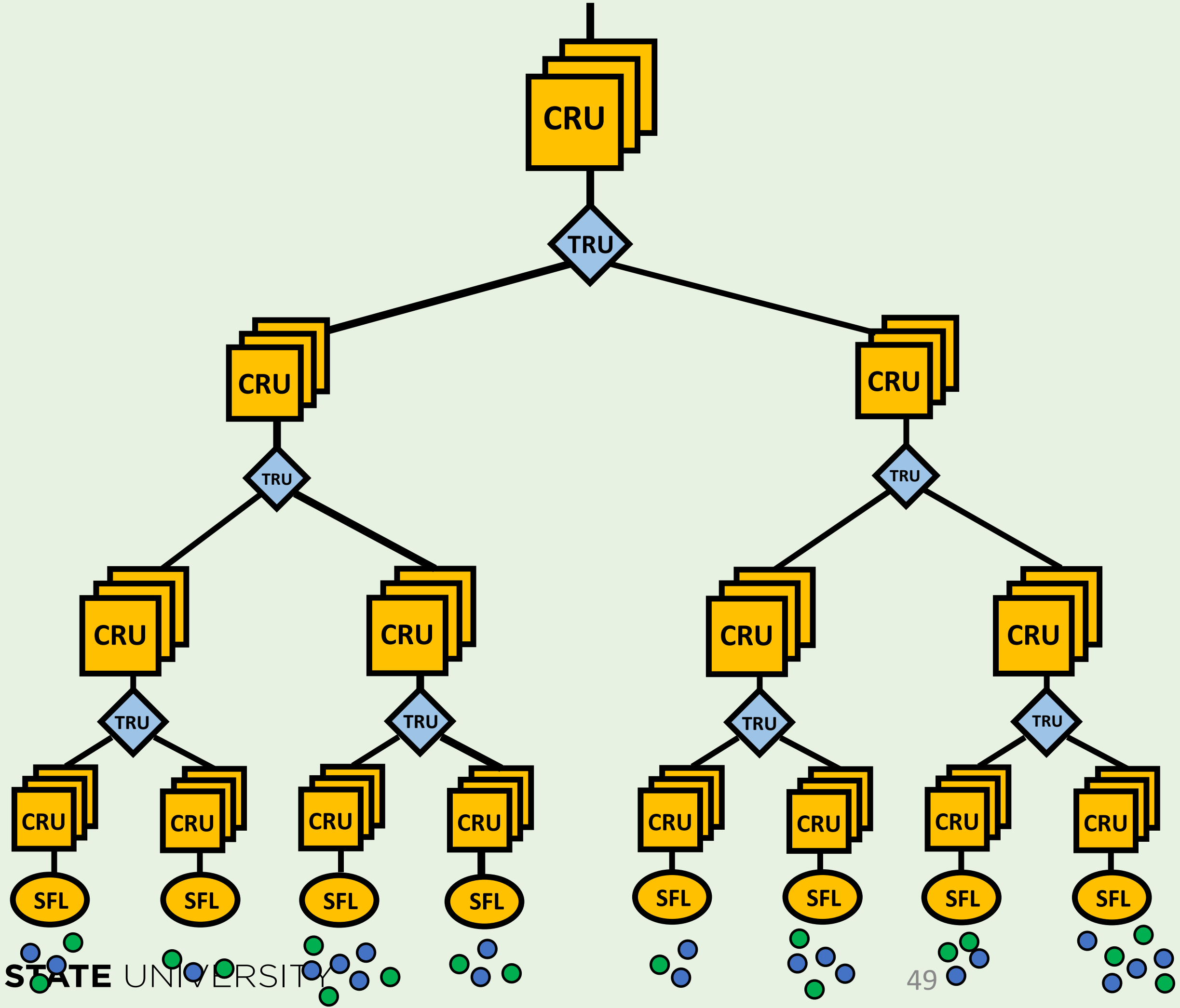
Binary Mask Regression



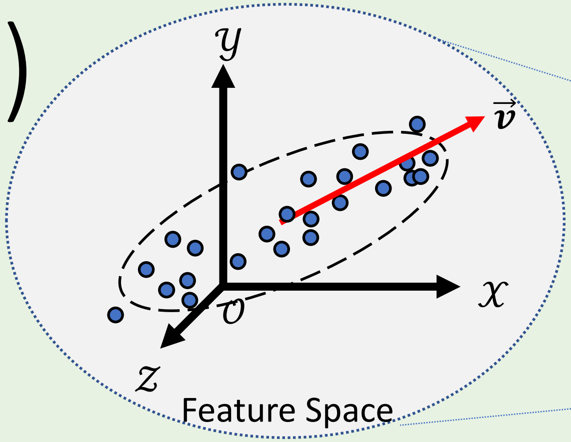
Training TRU

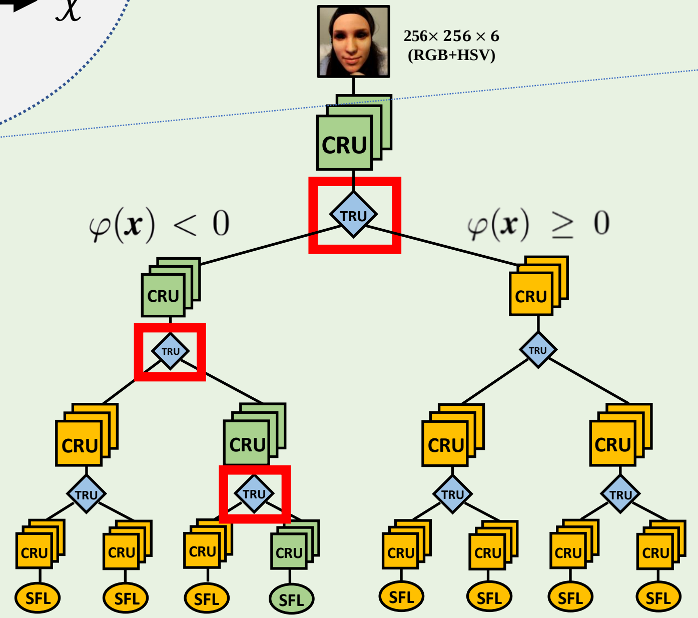


Training TRU



Tree Routing Unit (TRU)





- Routing Function

$$\varphi(\boldsymbol{x}) = (\boldsymbol{x} - \boldsymbol{\mu})^T \cdot \boldsymbol{v}, \quad \|\boldsymbol{v}\| = 1$$

- Based on eigen-analysis of visiting set

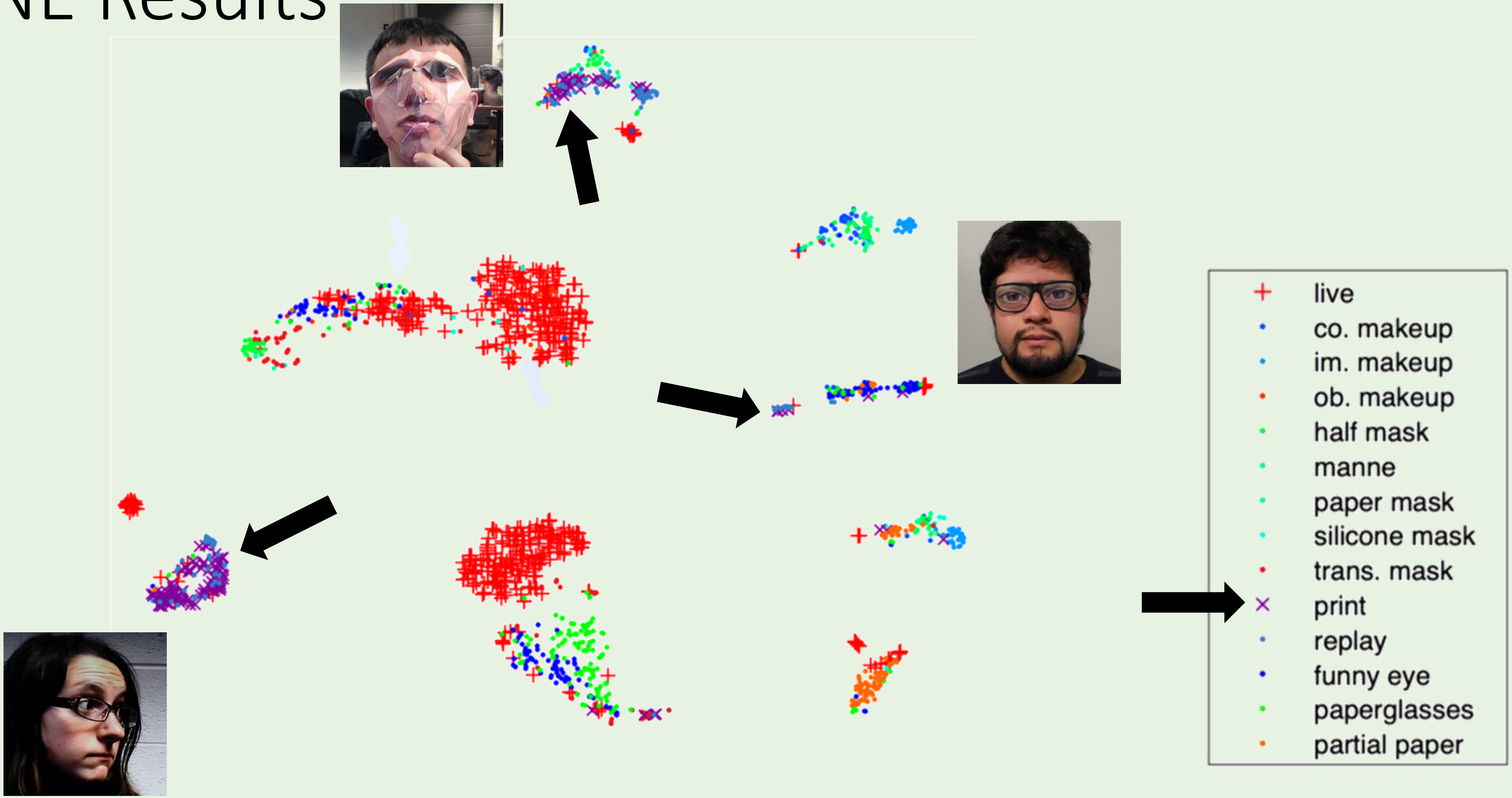
$$\bar{\boldsymbol{X}}_{\mathcal{S}} = \boldsymbol{X}_{\mathcal{S}} - \boldsymbol{\mu}$$

- We optimize:

$$\bar{\boldsymbol{X}}_{\mathcal{S}}^T \bar{\boldsymbol{X}}_{\mathcal{S}} \boldsymbol{v} = \lambda \boldsymbol{v}$$

$$\underset{\boldsymbol{v},\theta}{\arg\max}\ \lambda = \underset{\boldsymbol{v},\theta}{\arg\max}\ \boldsymbol{v}^T \bar{\boldsymbol{X}}_{\mathcal{S}}^T \bar{\boldsymbol{X}}_{\mathcal{S}} \boldsymbol{v}$$

t-SNE Results



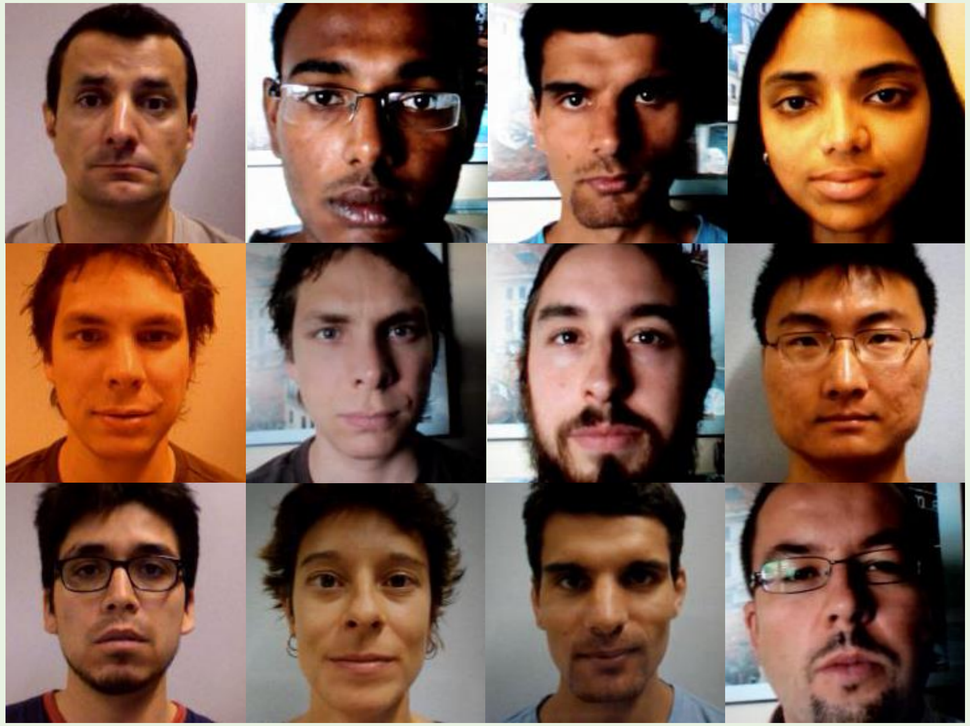
Databases and testing protocols

Database	Sensors	Print/Replay	Mask	Makeup	# Spoof Type	# Subjects	# Videos	Year
Replay-Attack	RGB	X			3	50	1200	2012
CASIA-FASD	RGB	X			3	50	600	2012
3DMAD	RGB, Depth		X		1	17	510	2014
MSU-MFSD	RGB	X			3	55	280	2015
MSU-USSA	RGB	X			8	1000	9,000 (I)	2016
HKBU MAR	RGB		X		2	35	1008	2016
MiW	RGB			X	3	434	1604	2017
OULU-NPU	RGB	X			4	55	4950	2017
SiW	RGB	X			6	165	4478	2018
SiW-M	RGB	X	X	X	13	493	1630	2019
CASIA-SURF	RGB, NIR, Depth	X				1000	21000	2019
WMCA	RGB, NIR, Depth, Thermal	X	X		7	72	1679	2019
CelebA-Spoof	RGB	X	X		4	10,177	625,537 (I)	2020

Replay Attack Database

Database	Sensors	Print/Replay	Mask	Makeup	# Spoof Type	# Subjects	# Videos	Year
Replay-Attack	RGB	X			3	50	1200	2012

- Controlled/adverse sessions

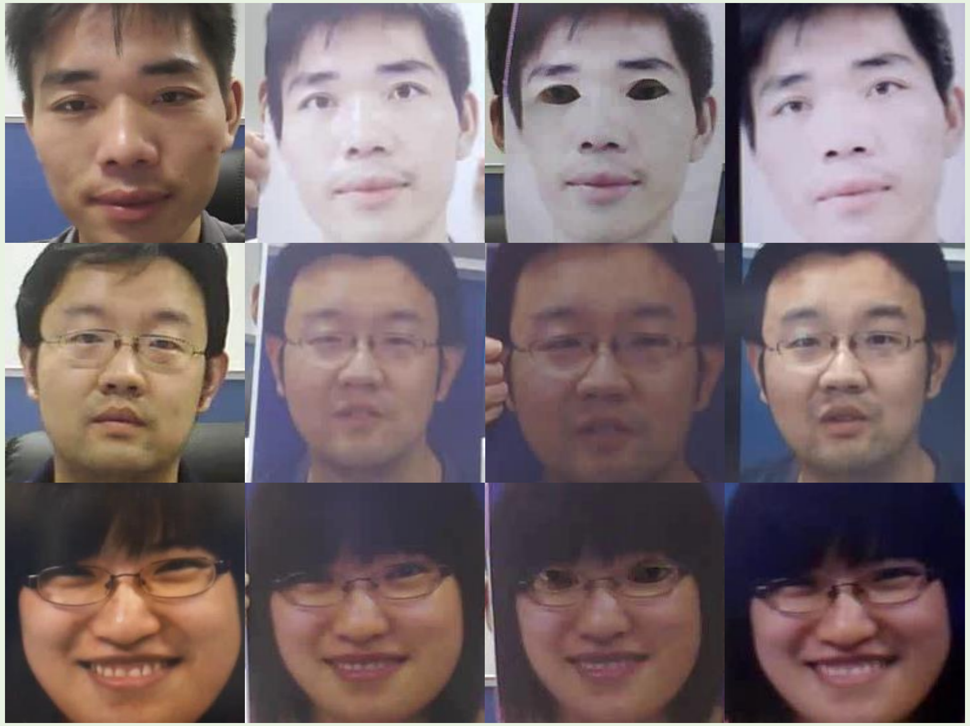


Chingovska et. al., On the Effectiveness of Local Binary Patterns in Face Anti-spoofing, BIOSIG, 2012

CASIA-FASD Database

Database	Sensors	Print/Replay	Mask	Makeup	# Spoof Type	# Subjects	# Videos	Year
CASIA-FASD	RGB	X			3	50	600	2012

- Three different image quality
- Eye cut to counter the eye-blinking methods
- Warp paper to counter the motion methods

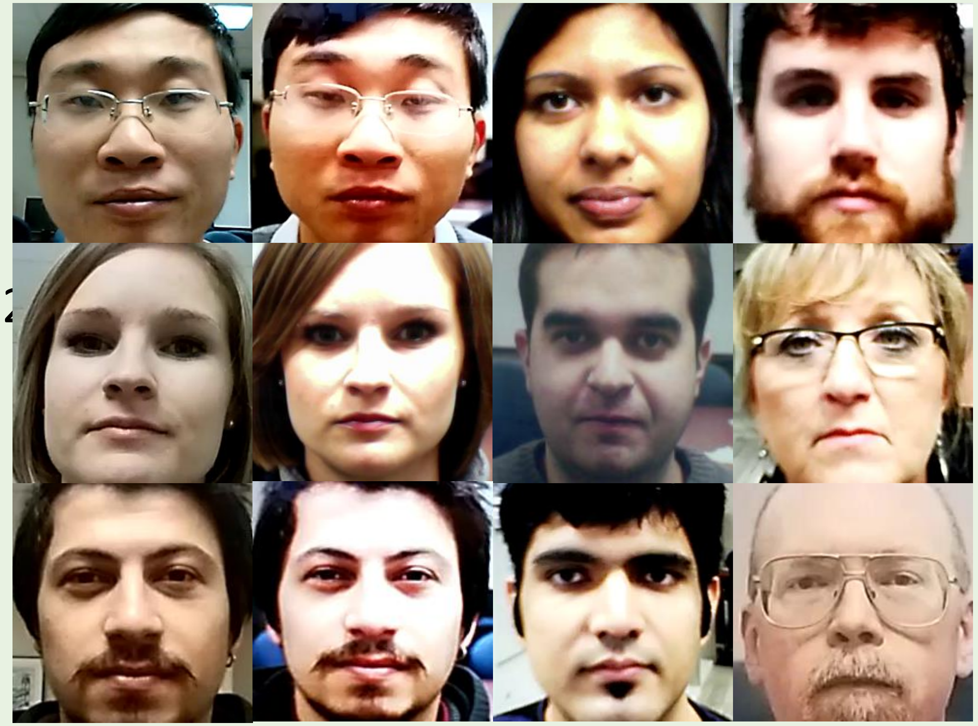


1. Zhang et. al., A Face Antispoofing Database with Diverse Attacks, ICB, 2012

MSU-MFSD Database

Database	Sensors	Print/Replay	Mask	Makeup	# Spoof Type	# Subjects	# Videos	Year
MSU-MFSD	RGB	X			3	55	280	2015

- Two capture devices
  - Build-camera in MacBook Air 13 (640*480)
  - Front camera in Google Nexus 5 Android phone (72
- Mostly used with CASIA and Replay



1. Wen et. al., Face Spoof Detection with Image Distortion Analysis, TIFS 2015

MSU-USSA Database

Database	Sensors	Print/Replay	Mask	Makeup	# Spoof Type	# Subjects	# Videos	Year
MSU-MFSD	RGB	X			3	55	280	2015

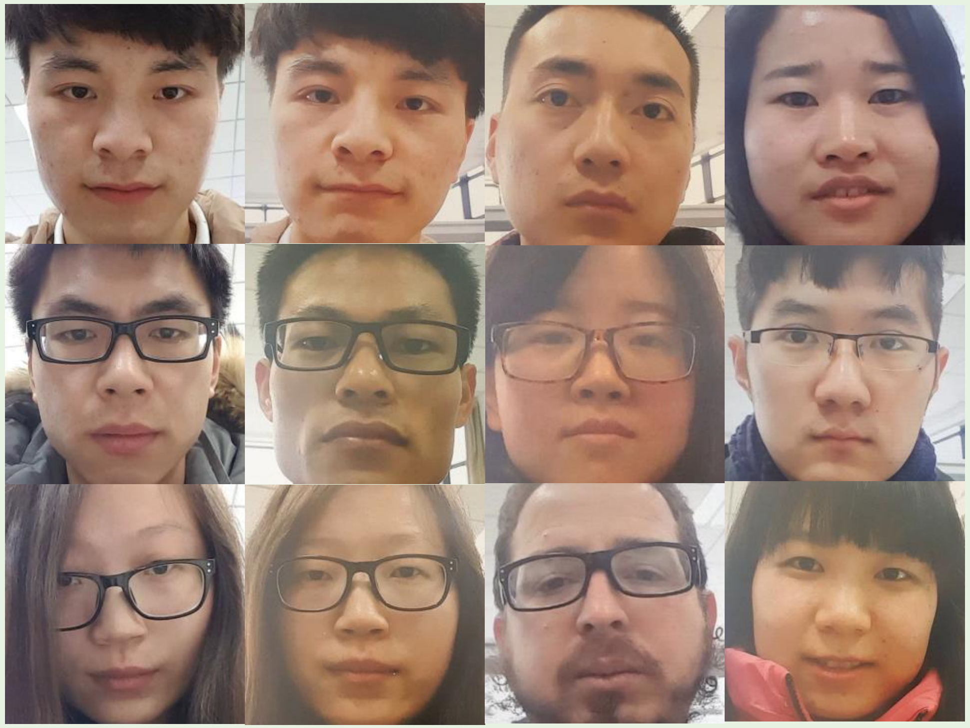
- Live images from Internet
- Higher resolution compared with MFSD
  - Front-facing camera in the Google Nexus 5 Android phone (1280 × 960).
  - Rear-facing camera in the Google Nexus 5 Android phone (3264 × 2448)
- Spoof from 8 devices

1. Patel et. al., Secure Face Unlock: Spoof Detection on Smartphones, TIFS 2016

OULU-NPU Database

Database	Sensors	Print/Replay	Mask	Makeup	# Spoof Type	# Subjects	# Videos	Year
OULU-NPU	RGB	X			4	55	4950	2017

- 6 camera, 1080P resolution
- Comprehensive evaluation protocols

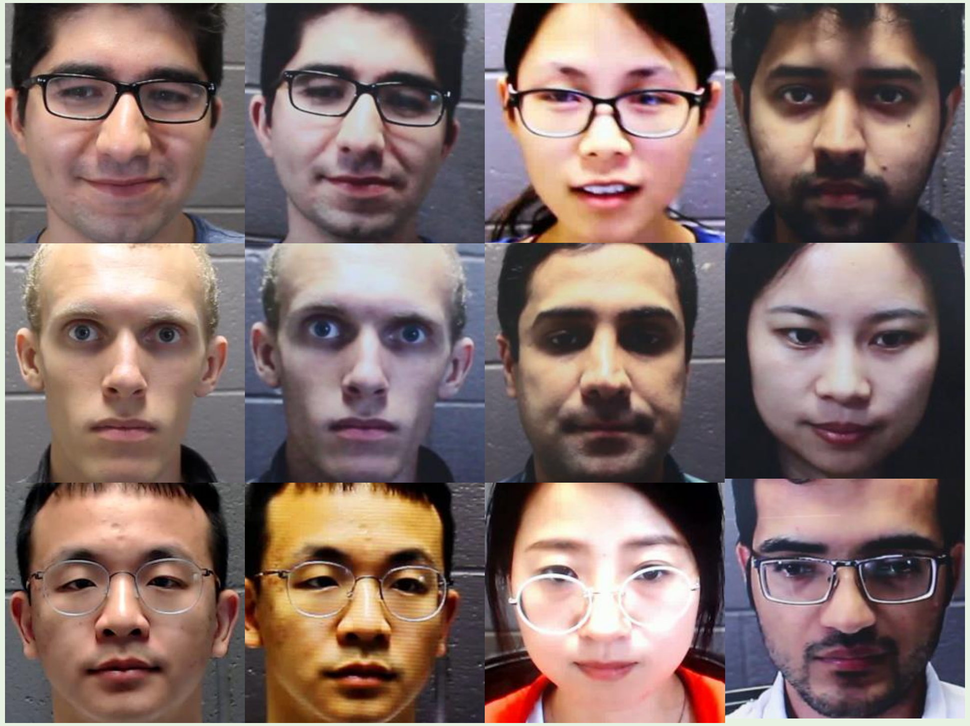


1. Boulkenafet et. al., OULU-NPU: A Mobile Face Presentation Attack Database with Real-World Variations, FG, 2017

SiW Database

Database	Sensors	Print/Replay	Mask	Makeup	# Spoof Type	# Subjects	# Videos	Year
SiW	RGB	X			6	165	4478	2018

- Pose, illumination, expression
- More subjects
- Comprehensive evaluation protocols



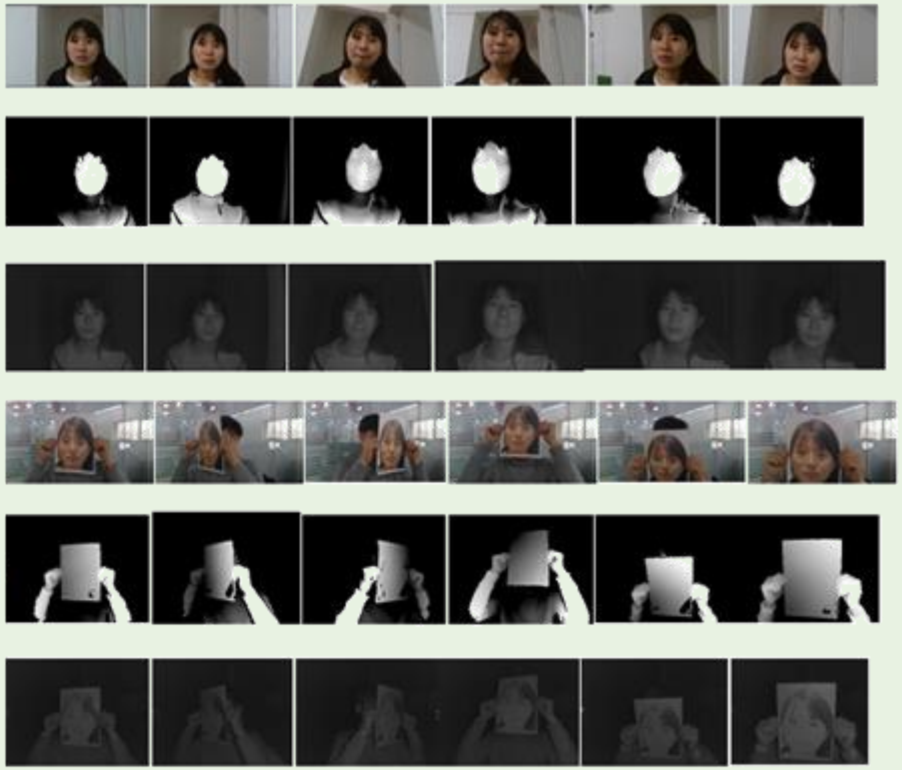
1. Liu et. al., Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision, CVPR, 2018

CASIA-SURF Database

Database	Sensors	Print/Replay	Mask	Makeup	# Spoof Type	# Subjects	# Videos	Year
CASIA-SURF	RGB, NIR, Depth	X				1000	21000	2019

- Multi modalities
- More subjects/videos

Real,RGB
Real,Depth
Real, IR
Fake, RGB
Fake, Depth
Fake, IR



1. Zhang et. al., CASIA-SURF: A Large-scale Multi-modal Benchmark for Face Anti-spoofing, CVPR 2019

3DMAD Database

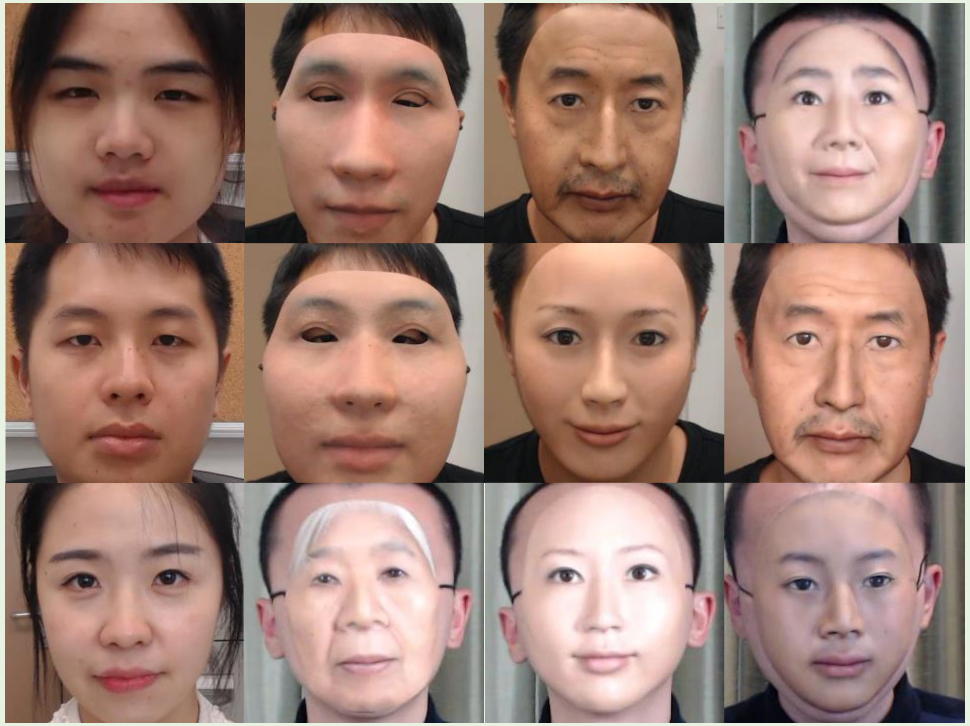
Database	Sensors	Print/Replay	Mask	Makeup	# Spoof Type	# Subjects	# Videos	Year
3DMAD	RGB, Depth		X		1	17	510	2014

- Multi modalities
- More subjects/videos

1. Erdogmus et. al., Spoofing in 2D Face Recognition with 3D Masks and Anti-spoofing with Kinect, BTAS 2013

HKBU MAR Database

Database	Sensors	Print/Replay	Mask	Makeup	# Spoof Type	# Subjects	# Videos	Year
HKBU MAR	RGB		X		2	35	1008	2016

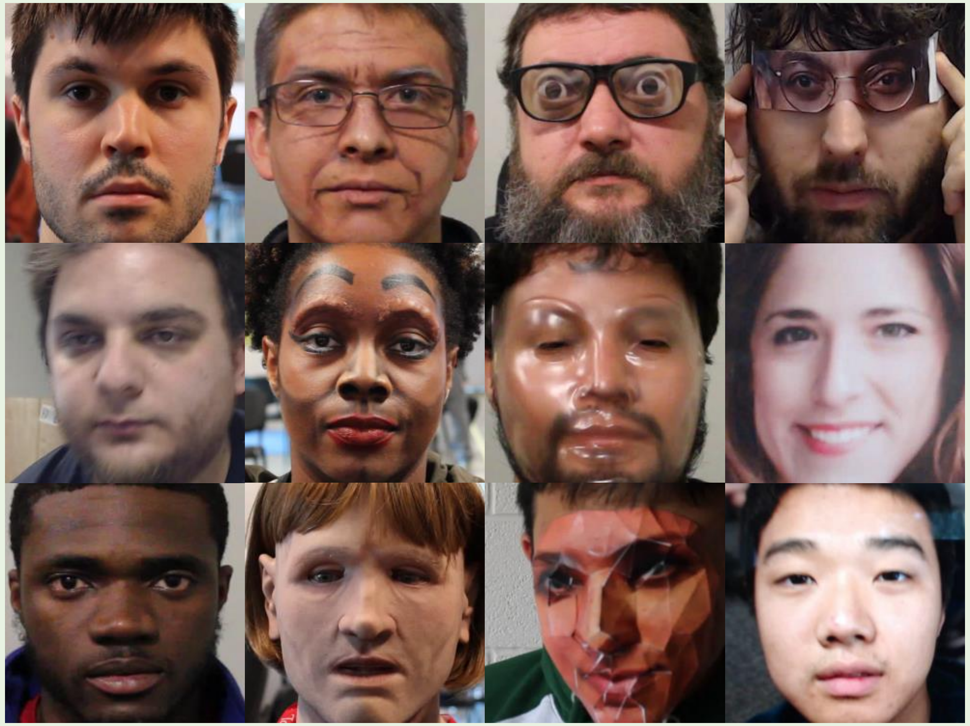


1. Liu et. al., rPPG Correspondence Feature for 3D Mask Face Presentation Attack Detection, ECCV 2018
2. Liu et. al., 3D Mask Face Anti-spoofing with Remote Photoplethysmography, ECCV 2016
3. Liu et. al., A 3D Mask Face Anti-spoofing Database with RealWorld Variations, CVPRW 2016

SiW-M Database

Database	Sensors	Print/Replay	Mask	Makeup	# Spoof Type	# Subjects	# Videos	Year
SiW-M	RGB	X	X	X	13	493	1630	2019

- More spoof types
- Leave-one-out testing protocols
- Include **hard** live and spoof samples



1. Liu et. al., Deep Tree Learning for Zero-shot Face Anti-Spoofing, CVPR 2019

CelebA-Spoof Database

Database	Sensors	Print/Replay	Mask	Makeup	# Spoof Type	# Subjects	# Videos	Year
CelebA-Spoof	RGB	X	X		4	10,177	625,537 (I)	2020

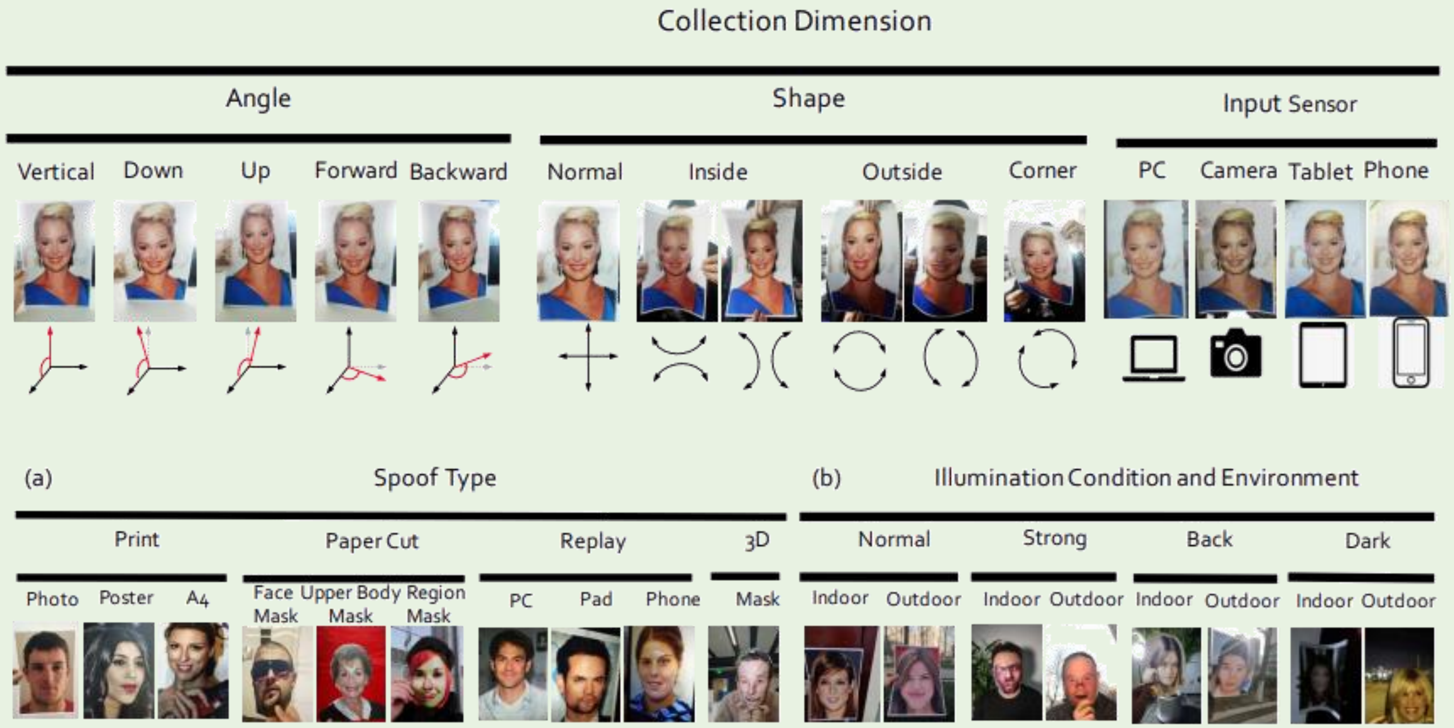
- Rich variations and annotations

1. Zhang et. al., CelebA-Spoof: Large-Scale Face Anti-Spoofing Dataset with Rich Annotations , ECCV 2020

CelebA-Spoof Database

Database	Sensors	Print/Replay	Mask	Makeup	# Spoof Type	# Subjects	# Videos	Year
CelebA-Spoof	RGB	X	X		4	10,177	625,537 (I)	2020

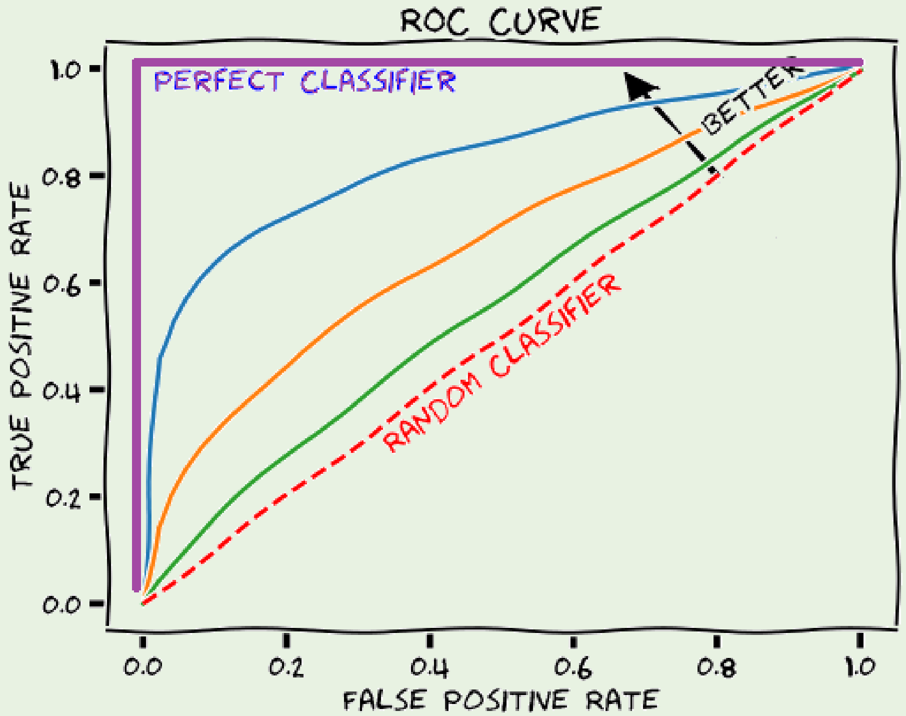
- Testing protocols less challenging
- Better to design new protocols or do cross-database testing



1. Zhang et. al., CelebA-Spoof: Large-Scale Face Anti-Spoofing Dataset with Rich Annotations , ECCV 2020

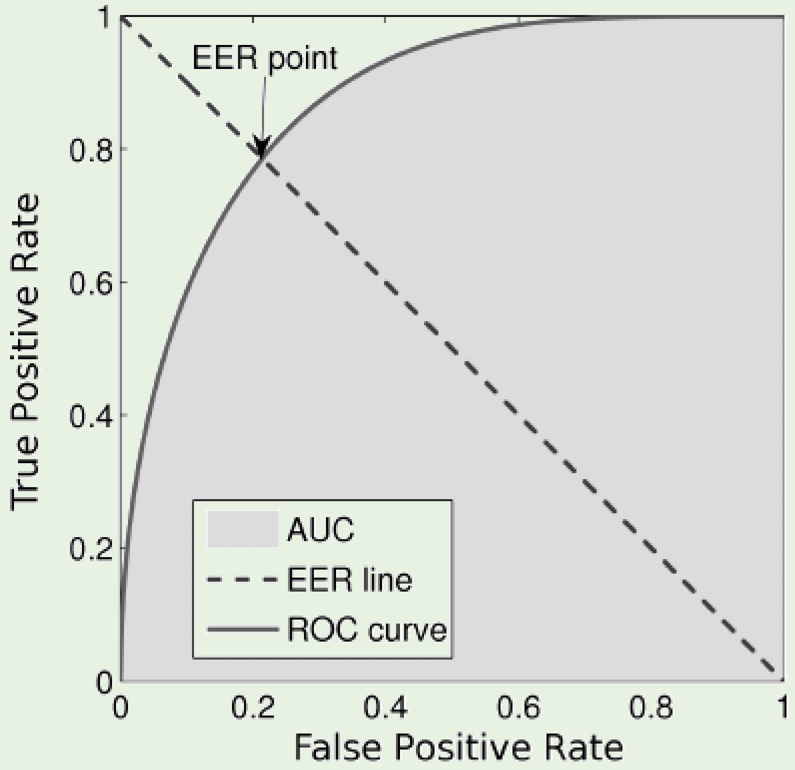
Evaluation metrics

- Area Under the Curve (AUC)
  - 0.5 → useless model
  - <0.7 → sub-optimal performance
  - 0.7 – 0.8 → good performance
  - > 0.8 → excellent performance
  - 1 → perfect
- EER
- APCER / BPCER / ACER
- TPR at FPR = x (e.g. x = 0.2%)



Evaluation metrics

- Area Under the Curve (AUC)
- EER
  - False pos rate = False neg rate
- APCER / BPCER / ACER
- TPR at FPR = x (e.g. x = 0.2%)



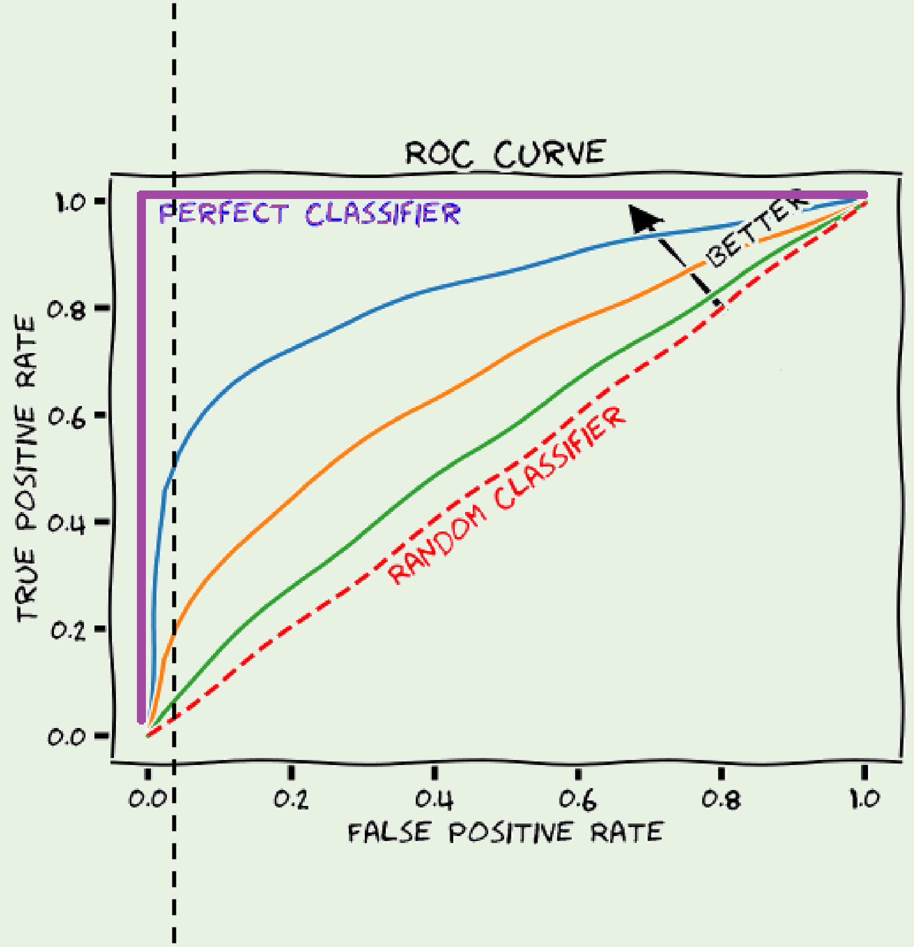
Evaluation metrics

- Area Under the Curve (AUC)
- EER
- APCER / BPCER / ACER
  - ISO standard
  - APCER: Attack Presentation Classification Error Rate
  - BPCER: Bona Fide Presentation Classification Error Rate
  - ACER: (APCER+BPCER)/2
- TPR at FPR = x (e.g. x = 0.2%)

Evaluation metrics

- Area Under the Curve (AUC)
- EER
- APCER / BPCER / ACER

- TPR at FPR = x (e.g. x = 0.2%)



Evaluation metrics

- We recommend:
  - EER
  - APCER / BPCER / ACER
  - TPR at FPR = x (e.g. x = 0.2%)

Summary

- Direct FAS
- Auxiliary FAS
- Temporal FAS
- Generative FAS
- Cross-domain FAS
- Unknow attack FAS

Problem 1: Training-Testing Difference

- Cross-domain and unknown attack performances are still poor
  - EER for intra-testing: ~ 0% – 5%
  - EER for inter-testing: ~ 15% - 50%
- How cross-domain testing contribute to real-world applications?

Problem 2: Explainablity

- Spatial explainablity
- Temporal explainablity
- Spoofing process explainablity
- Research on camera and imaging

Problem 3: New Attacks

- Can we transfer our knowledge of FAS to other attacks?
  - Face/Generic adversarial attacks
  - Face /Generic manipulation attacks
- Counter attacks to current methods
  - 3D mask attacks with flashing light → rPPG methods

End of Session II

7 Minutes Break

MICHIGAN STATE UNIVERSITY

Computer Vision Lab

IJCB 2020