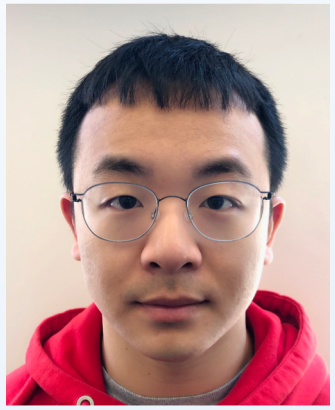
BTAS 2019

Face Anti-Spoofing: Past, Present and the Future

MICHIGAN STATE UNIVERSITY

Computer Vision Lab

Host



Yaojie Liu

Dr. Xiaoming Liu

Acknowledgement

This research 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.

Acknowledgement

Thank Joel Stehouwer, Amin Jourabloo, Yousef Atoum for the help on the presentation slides and contributions on this topic.

Outline

BTAS 2019

- Session I: **Introduction of face anti-spoofing and common approaches**
- Break: 15 mins
- Session II: **Deep learning approaches for face anti-spoofing**
- Break: 15 mins
- Session III: **Unknown attacks, additional sensors and practical tips**

What You Can Get from This Tutorial?

BTAS 2019

- Comprehensive review of the development of face anti-spoofing
- Latest research progresses and achievements
- First-hand system building tips

BTAS 2019

Session I: Introduction of Face Anti-spoofing and Common Approaches

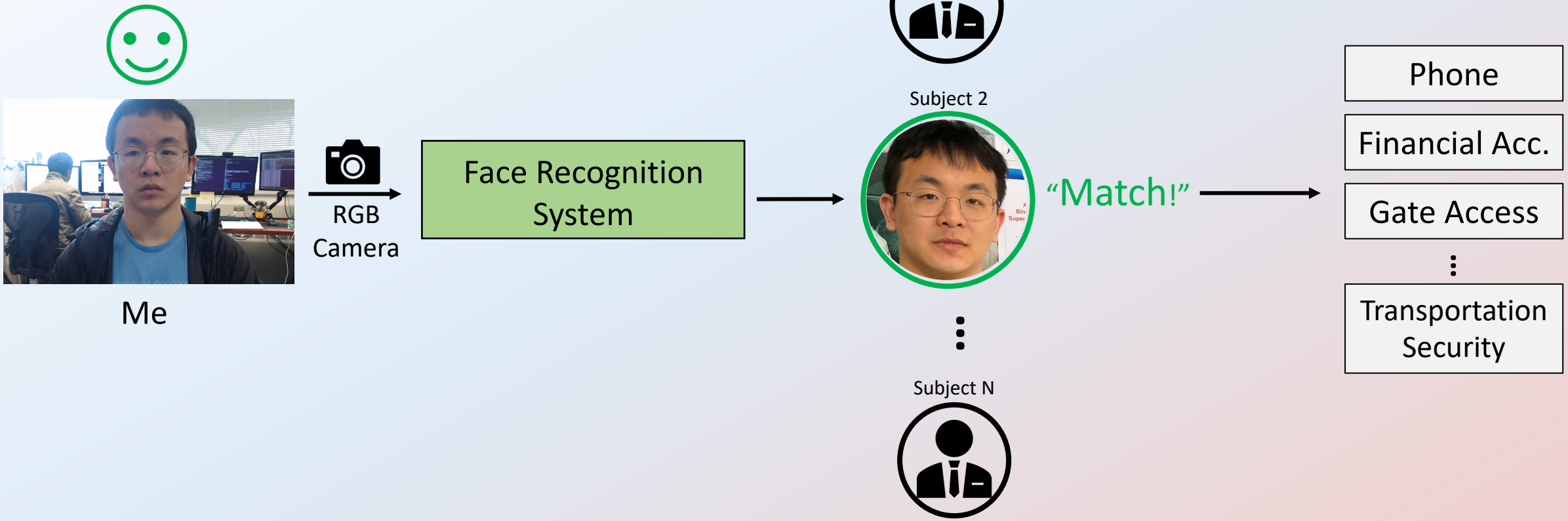
Host: Yaojie Liu

Outline

BTAS 2019

- Problem Definition and Motivation
- Common Spoof Attacks and Current Databases
- Conventional Approaches
  - Interaction Based Methods
  - Texture Analysis Methods
  - Temporal Analysis Methods

What is Face Anti-spoofing ?



What is Face Anti-spoofing ?

BTAS 2019

Attacker

Face Recognition System

Subject 1

Subject 2

Subject N

"Match!"

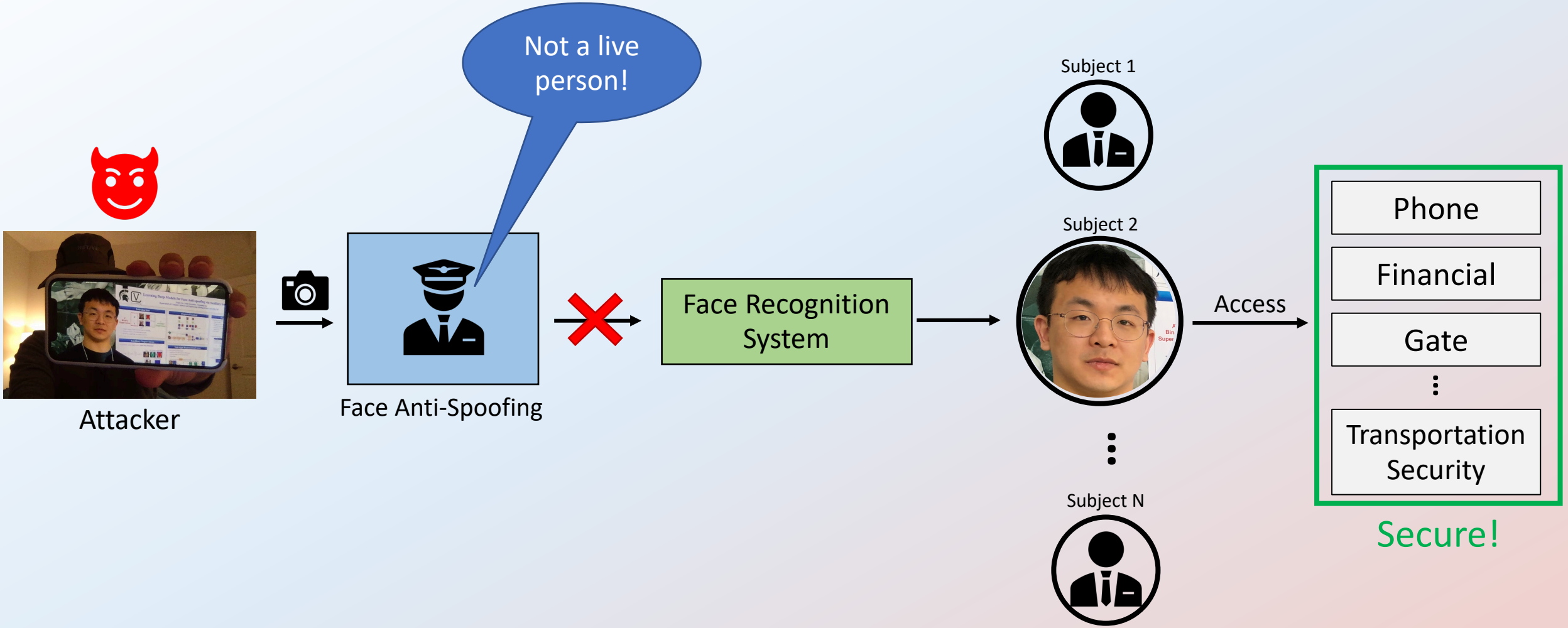
Access?

- Phone
- Financial
- Gate
- Transportation Security

Insecure!

What is Face Anti-spoofing ?

BTAS 2019



Challenges

[1] Z. Boulkenafet et. al. Face antispoofing using speeded-up robust features and fisher vector encoding. Signal Processing Letters, 2016
[2] Y. Liu et. al. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. CVPR 2018
[3] Z. Boulkenafet et. al. OULU-NPU: A mobile face presentation attack database with real-world variations. FG 2017
[4] Y. Liu et. al. Deep tree learning for zero-shot face anti-spoofing. CVPR 2019

Common Spoof Attacks

BTAS 2019

- Impersonation: the use of spoof to be recognized as someone else
- Obfuscation: the use of spoof to remove the attacker's own identity

Common Spoof Attacks

BTAS 2019

- Print
- Replay
- 3D Mask
- Makeup
- Partial Attack

Current Databases

BTAS 2019

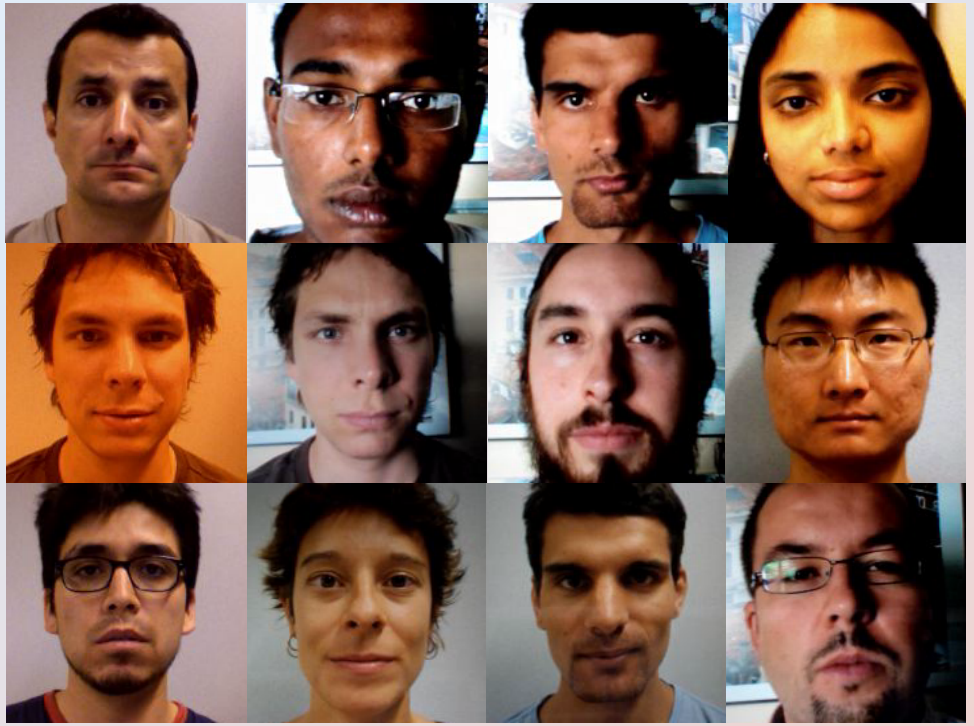
Database	Sensors	Print/Replay	Mask	Makeup	# Spoof Type	# Subjects	# Videos	Year
Replay-Attack	RGB	X			3	50	1200	2012
CASIA-FASD	RGB	X			3	50	600	2012
3DMAD	RGB, Depth		X		1	17	510	2014
MSU-MFSD	RGB	X			3	55	280	2015
MSU-USSA	RGB	X			8	1000	9,000 images	2016
HKBU MAR	RGB		X		2	35	1008	2016
MiW	RGB			X	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

Replay Attack Database

BTAS 2019

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

- Photo/video attacks
- Controlled/adverse sessions



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

CASIA-FASD Database

BTAS 2019

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

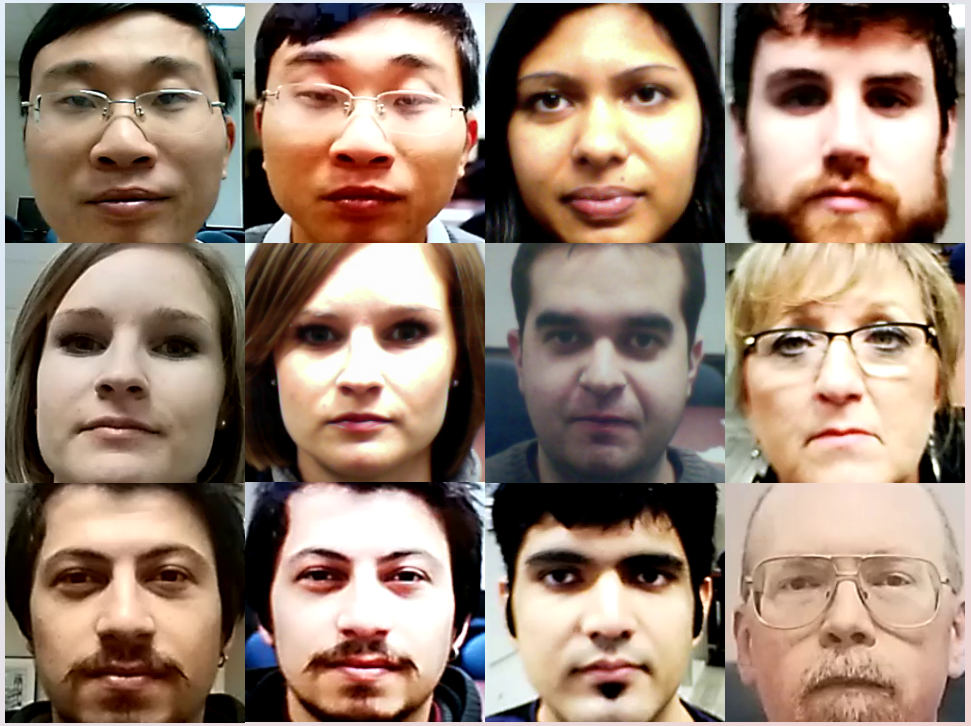
Zhang et. al., A Face Antispoofing Database with Diverse Attacks, ICB, 2012

MSU-MFSD Database

BTAS 2019

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 (720x480)
- Mostly used with CASIA and Replay



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

MSU-USSA Database

BTAS 2019

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

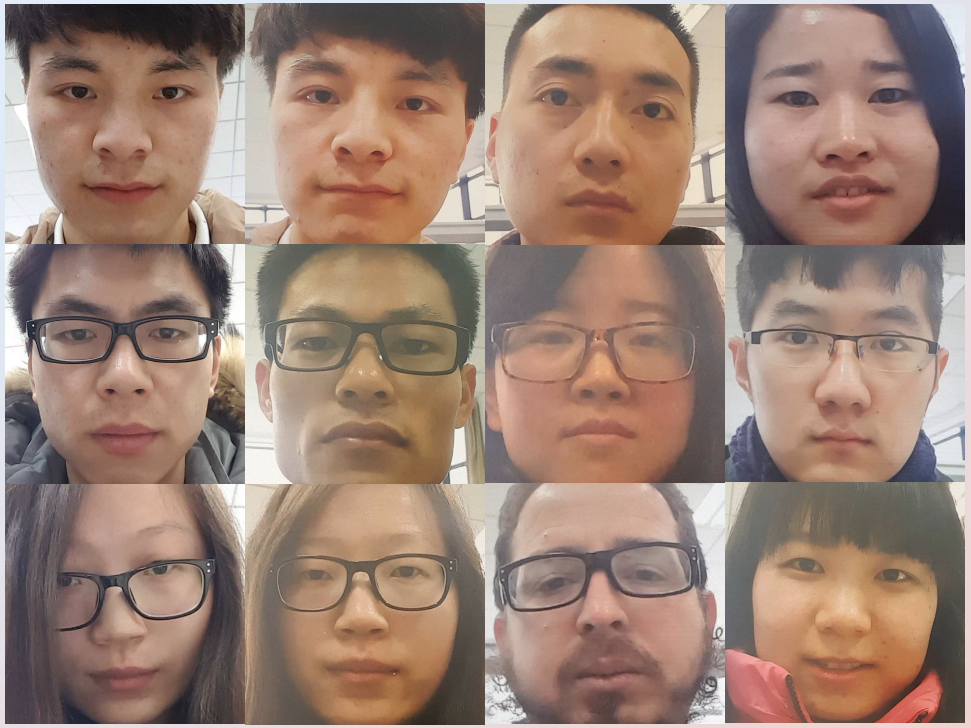
Patel et. al., Secure Face Unlock: Spoof Detection on Smartphones, TIFS 2016

OULU-NPU Database

BTAS 2019

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



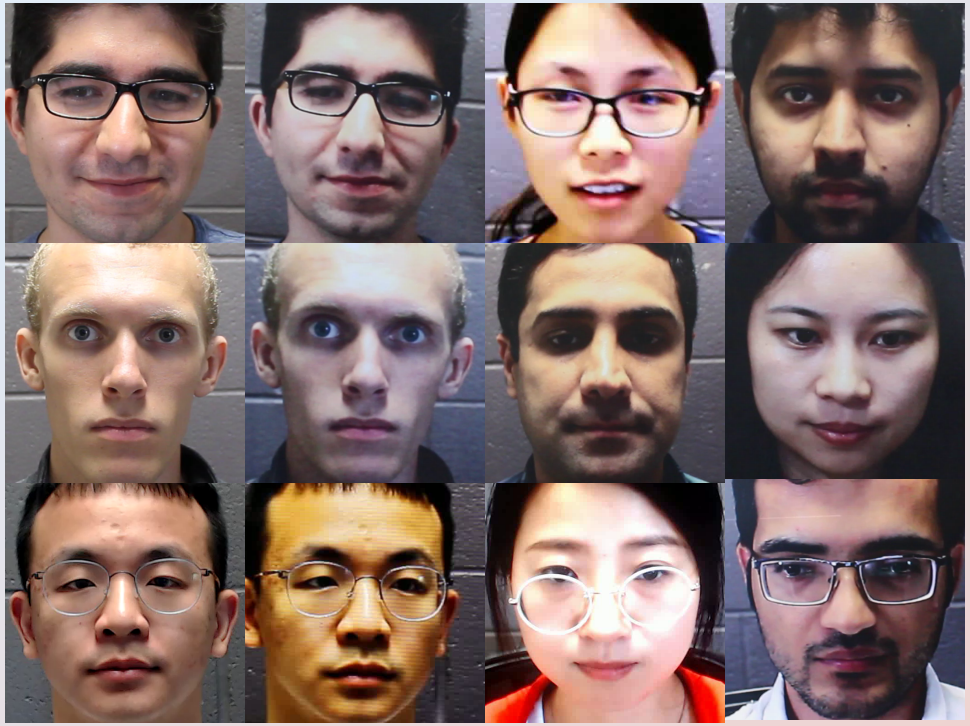
Boulkenafet et. al., OULU-NPU: A Mobile Face Presentation Attack Database with Real-World Variations, FG, 2017

SiW Database

BTAS 2019

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



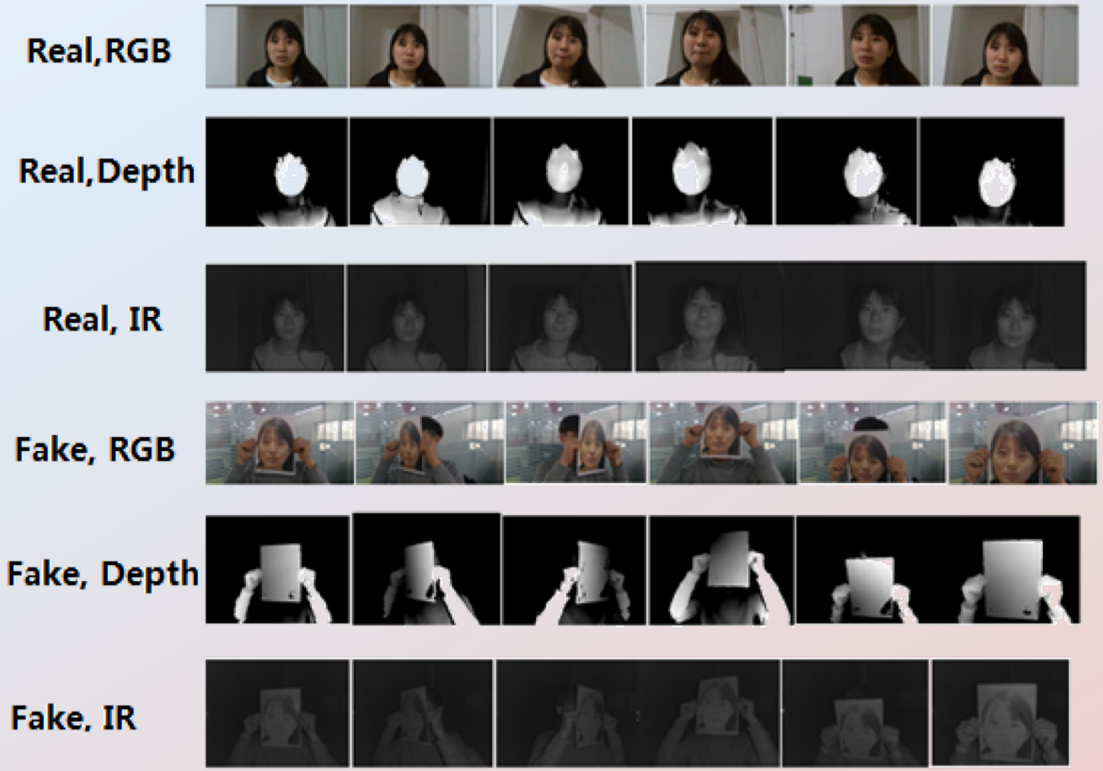
Liu et. al., Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision, CVPR, 2018

CASIA-SURF Database

BTAS 2019

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

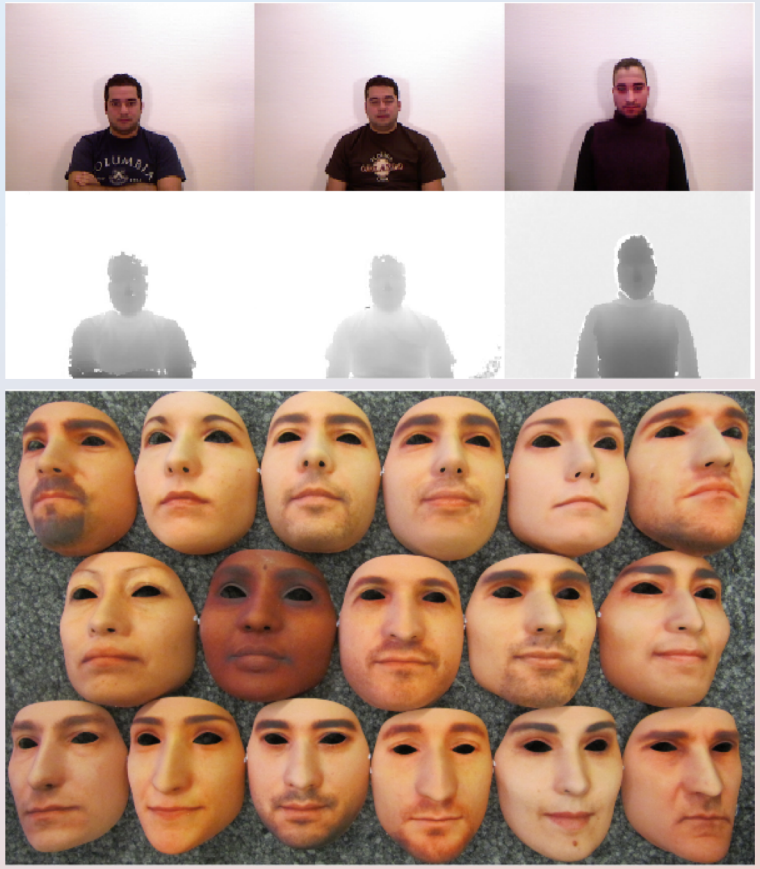


Zhang et. al., CASIA-SURF: A Large-scale Multi-modal Benchmark for Face Anti-spoofing, CVPR 20019

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

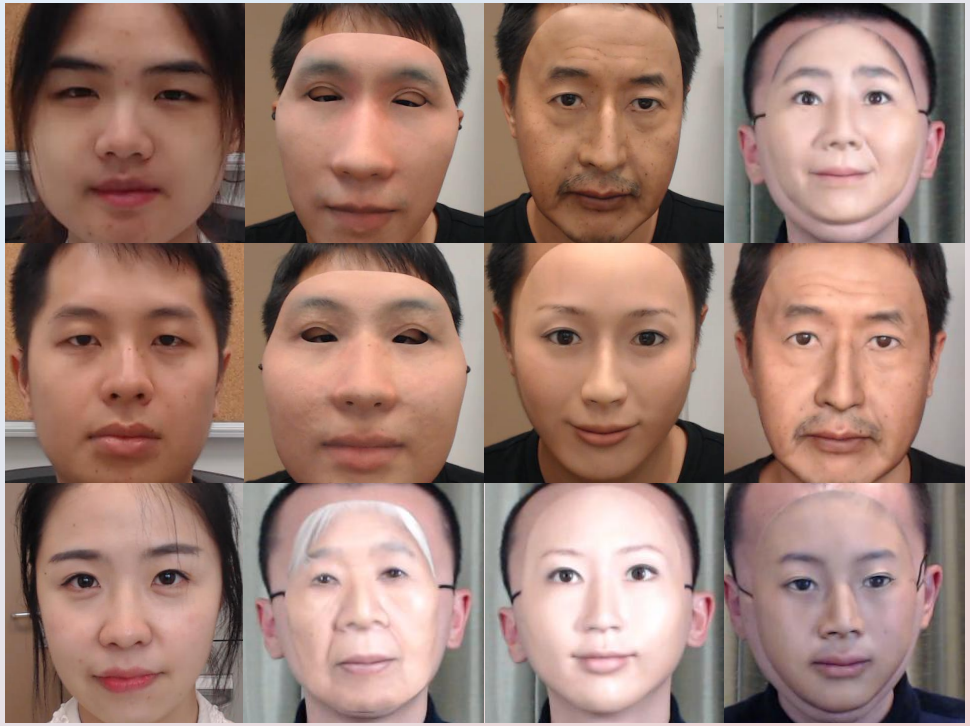


Erdogmus et. al., Spoofing in 2D Face Recognition with 3D Masks and Anti-spoofing with Kinect, BTAS 2013

HKBU MAR Database

BTAS 2019

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



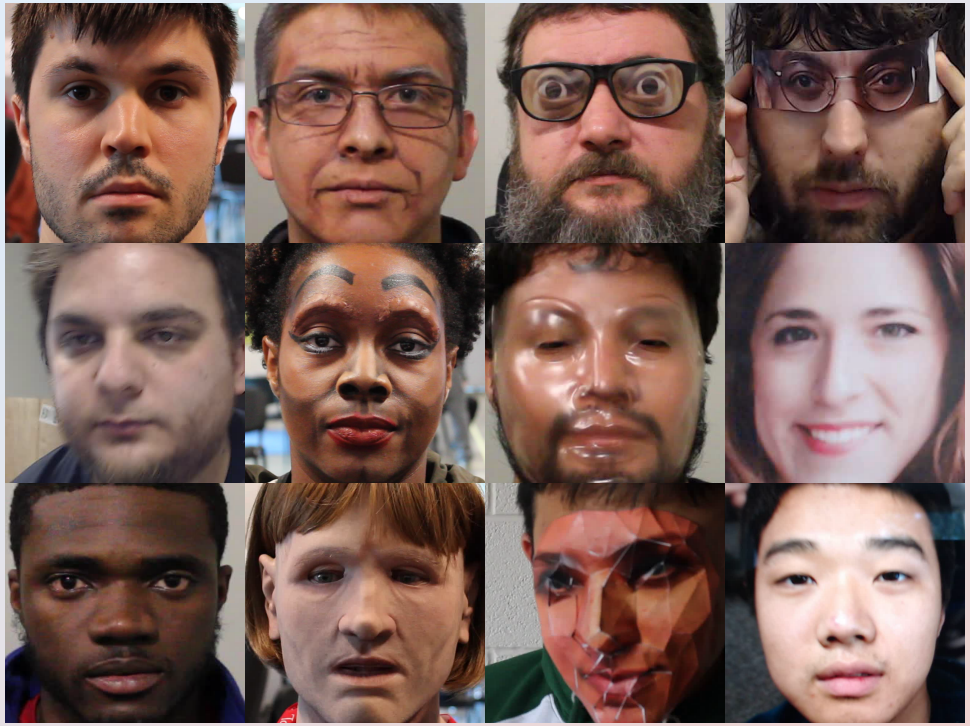
Liu et. al., rPPG Correspondence Feature for 3D Mask Face Presentation Attack Detection, ECCV 2018
Liu et. al., 3D Mask Face Anti-spoofing with Remote Photoplethysmography, ECCV 2016
Liu et. al., A 3D Mask Face Anti-spoofing Database with RealWorld Variations, CVPRW 2016

SiW-M Database

BTAS 2019

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

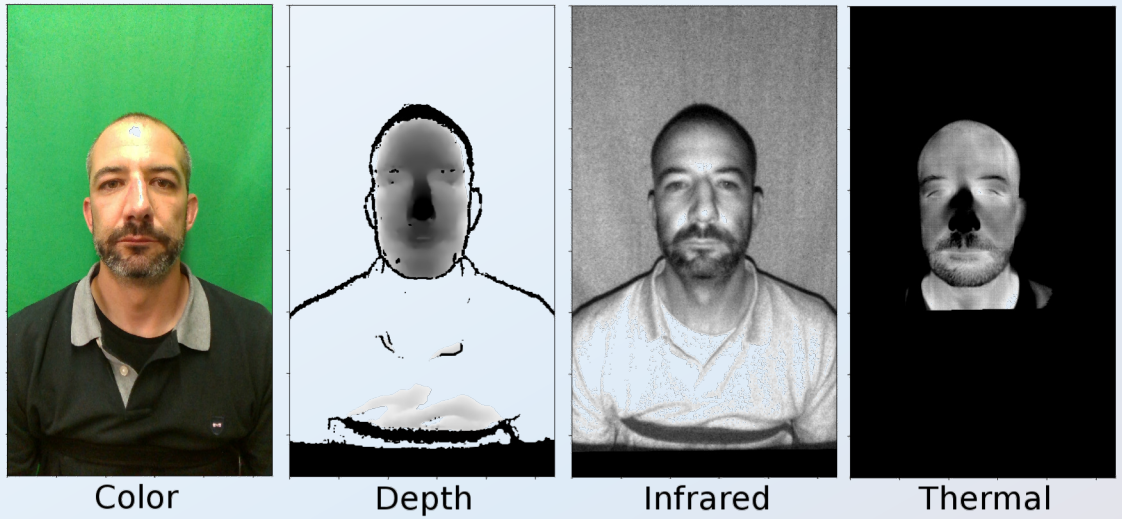


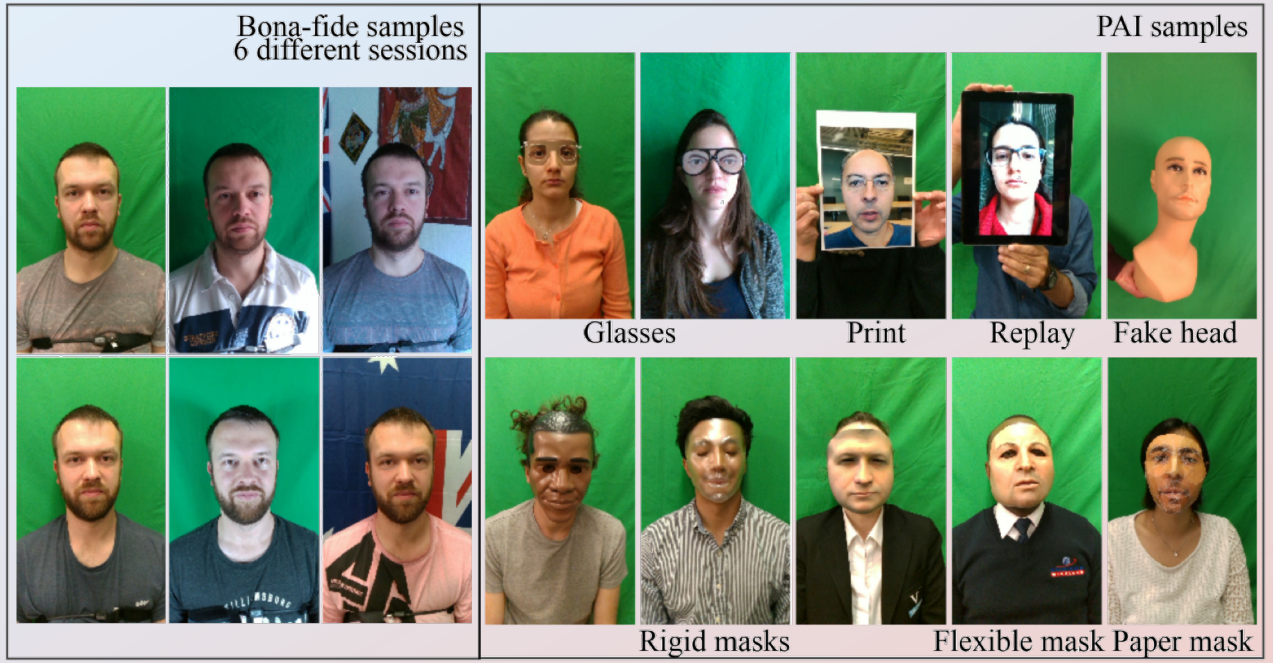
Liu et. al., Deep Tree Learning for Zero-shot Face Anti-Spoofing, CVPR 2019

WMCA Database

BTAS 2019

Database	Sensors	Print/Replay	Mask	Makeup	# Spoof Type	# Subjects	# Videos	Year
WMCA	RGB, NIR, Depth	X	X		7	72	1679	2019





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

Conventional Approaches

BTAS 2019

- Interaction Based Methods
- Texture Analysis Methods
- Temporal Analysis Methods

Conventional Approaches

BTAS 2019

- **Interaction Based Methods**
- Texture Analysis Methods
- Temporal Analysis Methods

Interaction Based Methods

BTAS 2019

- An interaction based method relies on discriminating between live and spoof via specified motion/behavioral cues that are native to live samples or require specific, voluntary user interaction.

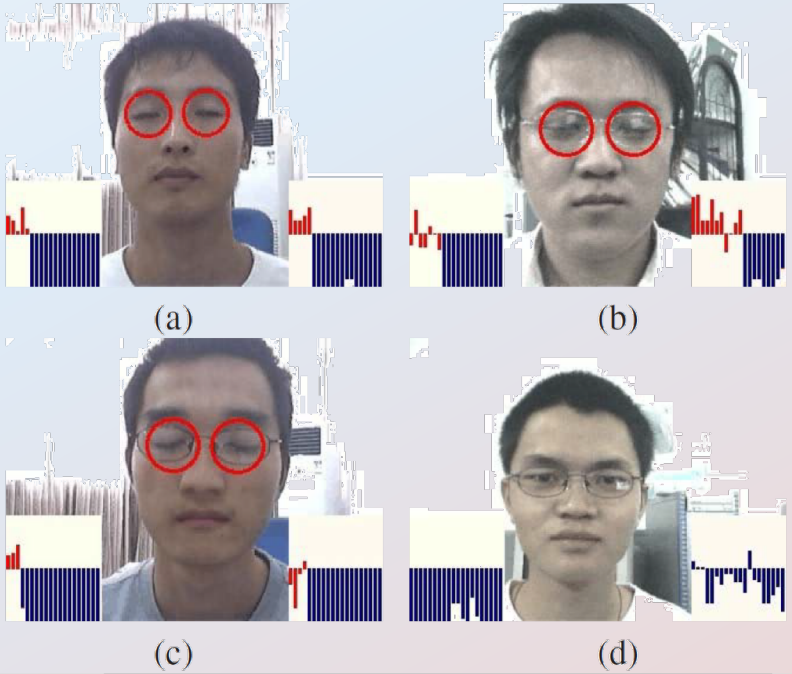
- Representative Works
  - Eyeblink-Based Anti-Spoofing[1,2]
  - Lip Motion Analysis[3]
  - Audio verification[4,5]

[1] G. Pan et. al., Eyeblink-Based Anti-Spoofing in Face Recognition from a Generic Web-Camera. ICCV, 2007
[2] L. Sun et. al., Blinking-based live face detection using conditional random fields. Advances in Biometrics, 2007.
[3] K. Kollreider et. al., Realtime face detection and motion analysis with application in "liveness" assessment. TIFS, 2007.
[4] G. Chetty. Biometric liveness checking using multimodal fuzzy fusion. In Fuzzy Systems (FUZZ), 2010
[5] G. Chetty and M. Wagner. Audio-visual multimodal fusion for biometric person authentication and liveness verification, 2006.

Eyeblink-Based Face Anti-Spoofing

BTAS 2019

- Proposal: The detection of eyeblinks is beneficial for discriminating between live samples and static photo attacks.
  - Live samples will exhibit eyeblinks
  - Photo attacks will be static and not exhibit eyeblinks

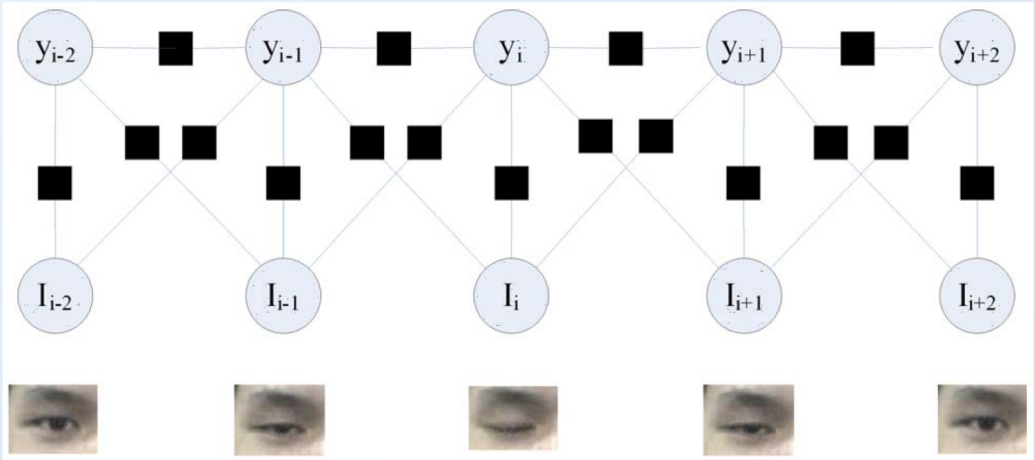


G. Pan et. al., Eyeblink-Based Anti-Spoofing in Face Recognition from a Generic Web-Camera. ICCV, 2007

Eyeblink-Based Face Anti-Spoofing

BTAS 2019

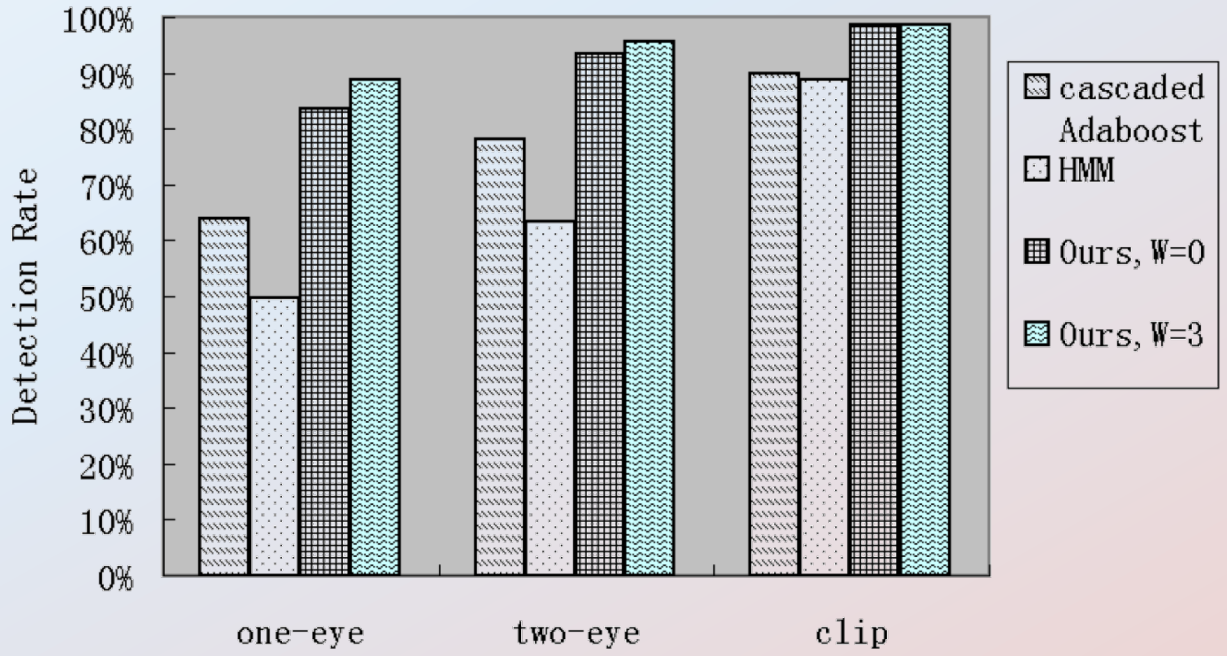
- Method: Conditional Random Field on eye portion



G. Pan et. al., Eyeblink-Based Anti-Spoofing in Face Recognition from a Generic Web-Camera. ICCV, 2007

Eyeblink-Based Face Anti-Spoofing

- One-eye: eye-blinking detection rate of the single eye
- Two-eye: eye-blinking detection rate of the two eyes
- Clip: The true detection rate of liveness



G. Pan et. al., Eyeblink-Based Anti-Spoofing in Face Recognition from a Generic Web-Camera. ICCV, 2007

Eyeblink-Based Face Anti-Spoofing

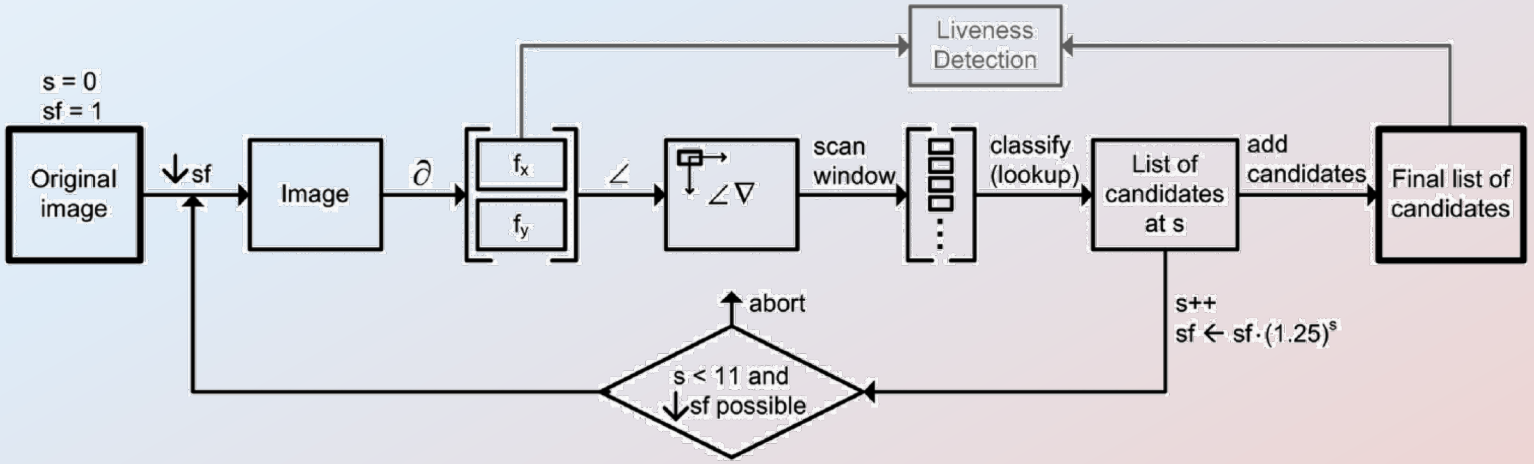
BTAS 2019

- Shortcomings
  - What happens if a live sample does not blink during the timeframe?
  - How to detect replay attacks?
  - How to detect cut-out eye photo attacks?

G. Pan et. al., Eyeblink-Based Anti-Spoofing in Face Recognition from a Generic Web-Camera. ICCV, 2007

Lip Motion Analysis

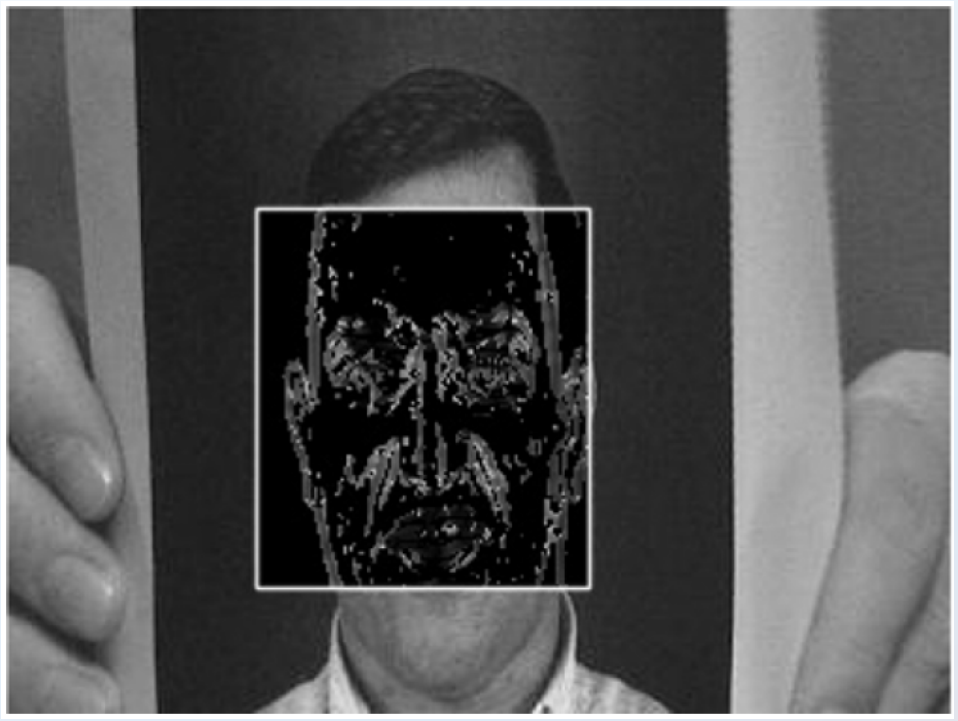
- The extraction of motion patterns when a user is moving his/her mouth is beneficial for discriminating between live samples and bent or rigid photo attacks.
  - A live sample will exhibit natural and non-uniform facial movement
  - A photo attack will exhibit non-natural (bent) or uniform (rigid) facial movement



K. Kollreider et. al., Realtime face detection and motion analysis with application in “liveness” assessment. TIFS, 2007.

Motion Examples

BTAS 2019



Bent Photo Attack

Live Access

K. Kollreider et. al., Realtime face detection and motion analysis with application in “liveness” assessment. TIFS, 2007.

Results

BTAS 2019

Yale Face Dataset

Method	Detection Rate	False Positives
Nguyen	86.6%	0
Proposed	100.0%	0

CMU-MIT Frontal Face Dataset

Method	Detection Rate	False Positive Rate
Rowley	89.2%	$1.27*10^{-6}$
Viola & Jones	92.9%	$1.27*10^{-6}$
Proposed	94.2%	$1.27*10^{-6}$
Proposed	93.0%	$1.00*10^{-6}$

K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun. Realtime Face Detection and Motion Analysis with Application in Liveness Assessment. In TIFS, 2007.

Lip Motion Analysis

BTAS 2019

- Shortcomings
  - How well does this method perform on bent photo attacks?
  - How to detect altered facial motion in replay attacks?
  - How to detect a flexible mask attack?
  - Does the camera have to be stationary?

K. Kollreider et. al., Realtime face detection and motion analysis with application in “liveness” assessment. TIFS, 2007.

Interaction Based Methods

BTAS 2019

- Pros
  - Simple implementations that model live samples
  - Effective solutions for their respective attack types
  - Handcrafted features are designed for efficient discriminability

- Cons
  - Require interactions from the user
  - Unable to evaluate individual images
  - Unable to generalize to new attack types

Texture Analysis Methods

BTAS 2019

- A texture analysis method relies on detecting additional high frequency information from print/replay attacks that does not exist in live samples.

- Pipeline
  - Handcrafted feature + Conventional Classifiers (SVM, LDA, and etc)

Z. Boulkenafet, J. Komulainen, and A. Hadid. Face Anti-Spoofing Based on Color Texture Analysis. In ICIP, 2015
Z. Boulkenafet, J. Komulainen, and A. Hadid. Face Anti-Spoofing Using Speeded Up Robust Features and Fisher Vector Encoding. IEEE Signal Processing Letters, 2017.
J. Maatta, A. Hadid, and M. Pietikainen. Face Spoofing Detection from Single Images using Micro-Texture Analysis. In IEEE IJCB, 2011.

Texture Based Methods

BTAS 2019

- Features
  - Difference of Gaussian (DoG)
  - LBP
  - LBP-TOP
  - Color LBP
  - IQA/IQM
  - SIFT/SURF

Face Anti-Spoofing Based on Color Texture Analysis. In ICIP, 2015
Face Anti-Spoofing Using Speeded Up Robust Features and Fisher Vector Encoding. IEEE Signal Processing Letters, 2017.
Face Spoofing Detection from Single Images using Micro-Texture Analysis. In IEEE IJCB, 2011.

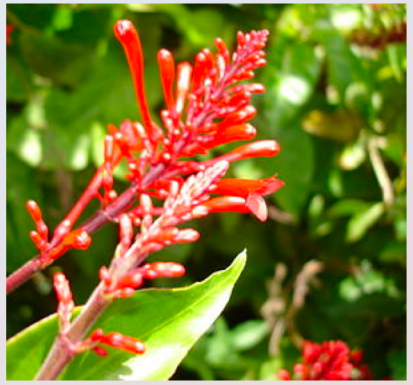
Difference of Gaussian (DoG)

BTAS 2019

- The subtraction of one blurred version of an original image from another, less blurred version of the original

$$\Gamma_{\sigma_1,\sigma_2}(x) = I * \frac{1}{\sigma_1\sqrt{2\pi}} e^{-(x^2)/(2\sigma_1^2)} - I * \frac{1}{\sigma_2\sqrt{2\pi}} e^{-(x^2)/(2\sigma_2^2)}.$$

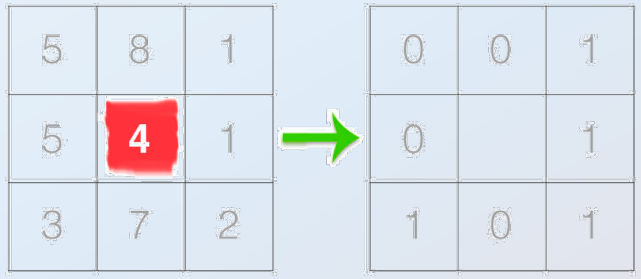
- Extraction of high-frequency details

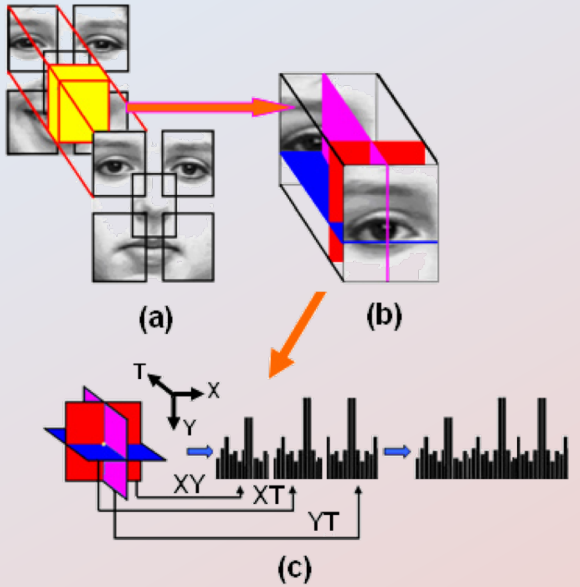


Local Binary Patterns (LBP)

- Divide image into cells (e.g. 16x16 pixels)
- For each cell, compare the pixel to its 8 neighbors.
- center pixel > the neighbor → "0“

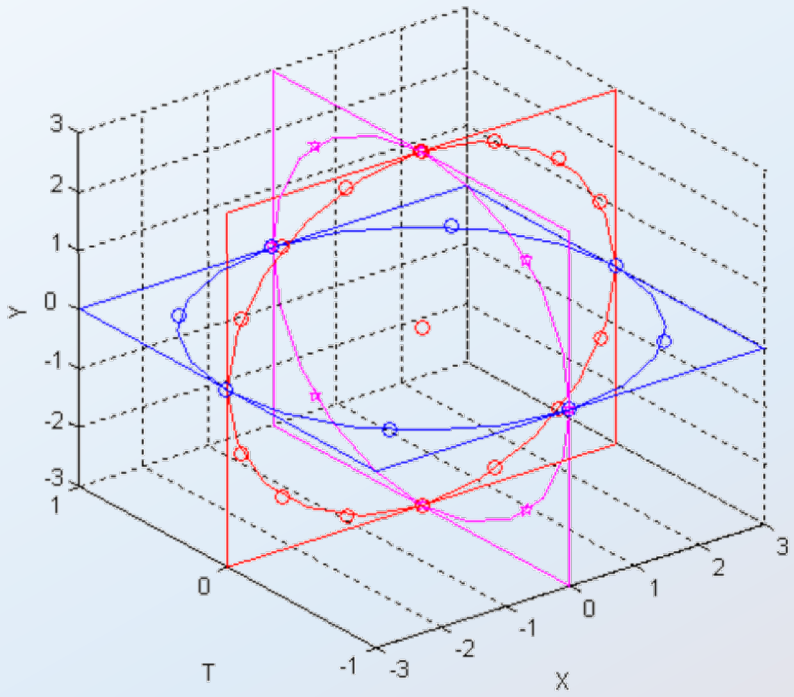
  center pixel <= the neighbor → “1".
- Compute the histogram of the frequency of 0/1
- Normalize and vectorize the histogram.

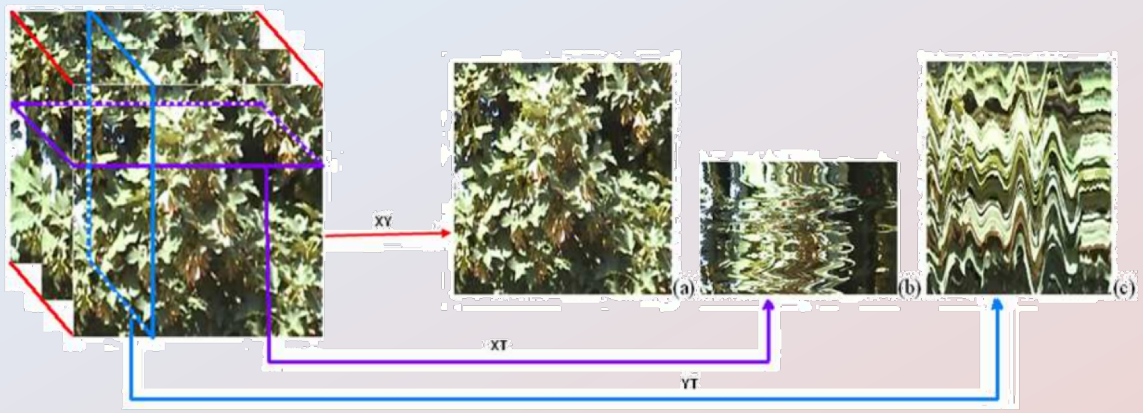




LBP-TOP

- local binary patterns from three orthogonal planes
  - X-Y, X-T, Y-T

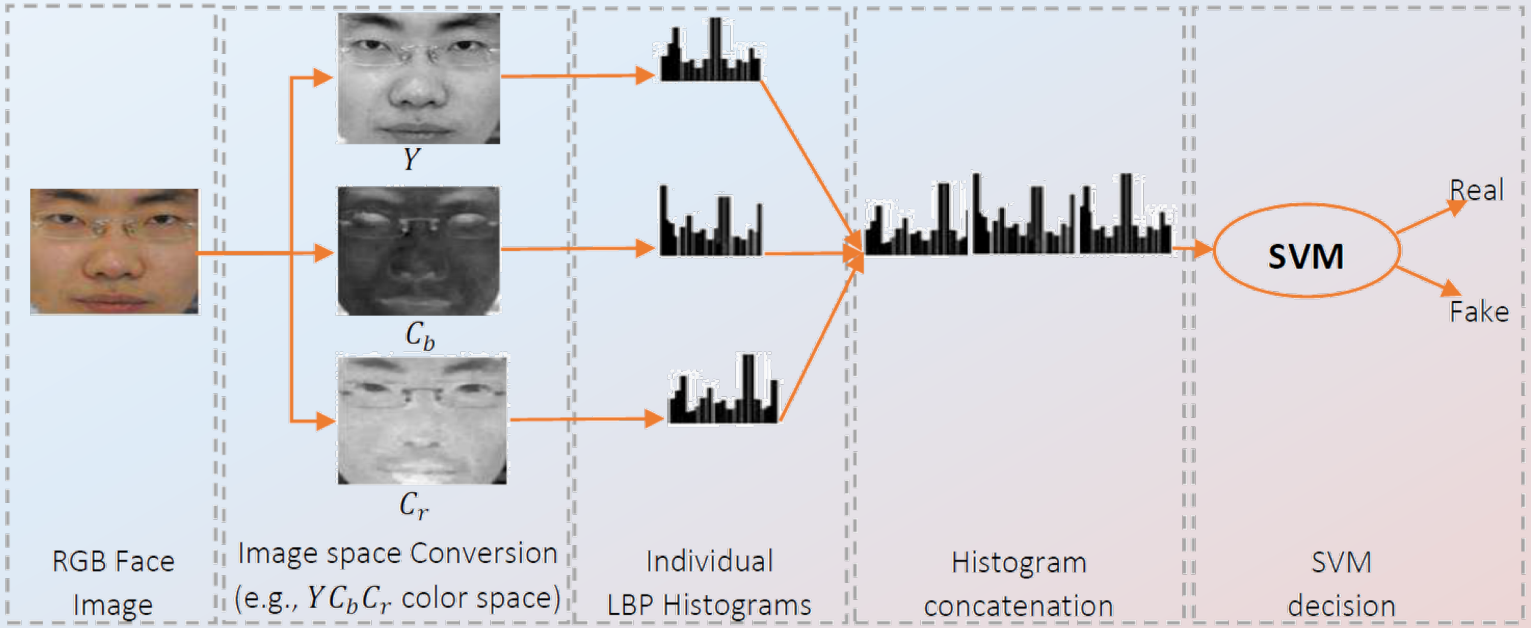




Tiago de Freitas Pereira et. al., LBP TOP based countermeasure against face spoofing attacks, ACCV workshop, 2012

Color LBP

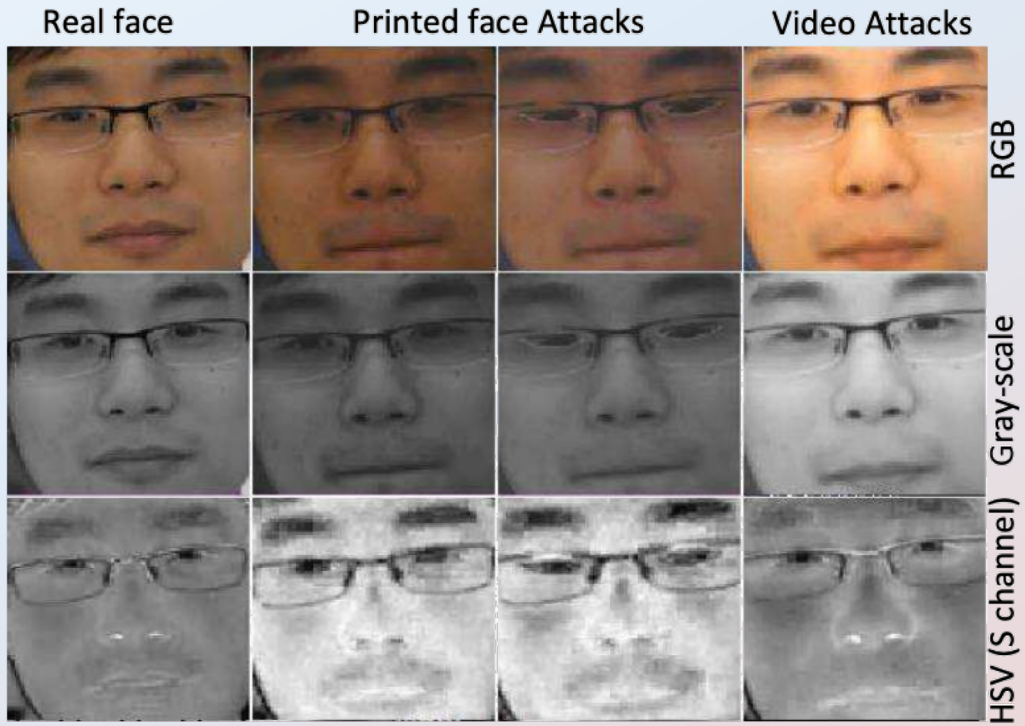
- Extract the LBP feature for each color channel
- Consider different color spaces



Z. Boulkenafet, J. Komulainen, and A. Hadid. Face Anti-Spoofing Based on Color Texture Analysis. In ICIP, 2015

Different Color Spaces

- RGB are highly correlated
- Isolating luminance from chrominance can lead to better LBP features



Different Color Spaces

BTAS 2019

- RGB are highly correlated
- Isolating luminance from chrominance can lead to better LBP features
- Ablation study on Replay database:

Method	EER	HTER
Gray-scale-LBP	15.3	15.6
RGB-LBP	5.0	6.6
HSV-LBP	6.4	7.0
YCbCr-LBP	0.7	3.3
YCbCr+HSV-LBP	**0.4**	**2.9**

Testing Results on Replay-Attack and CASIA-FASD

BTAS 2019

Method	Replay Attack		CASIA-FASD
	EER %	HTER %	EER %
IQA based	-	-	32.4
CCD	-	-	11.8
DOG	-	-	17.0
Motion+LBP	4.5	5.1	-
Motion	11.6	11.7	26.6
LBP	13.9	13.8	18.2
LBP-TOP	7.8	7.6	10.6
Color LBP	*0.4*	*2.9*	***6.2***

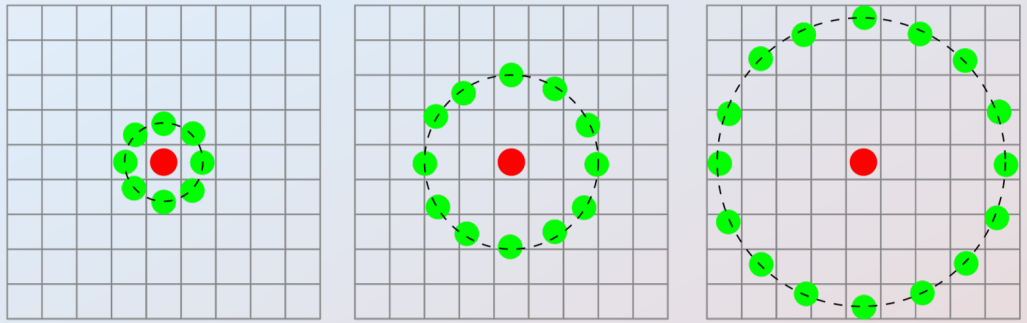
Z. Boulkenafet, J. Komulainen, and A. Hadid. Face Anti-Spoofing Based on Color Texture Analysis. In ICIP, 2015

Micro-Texture Analysis

BTAS 2019

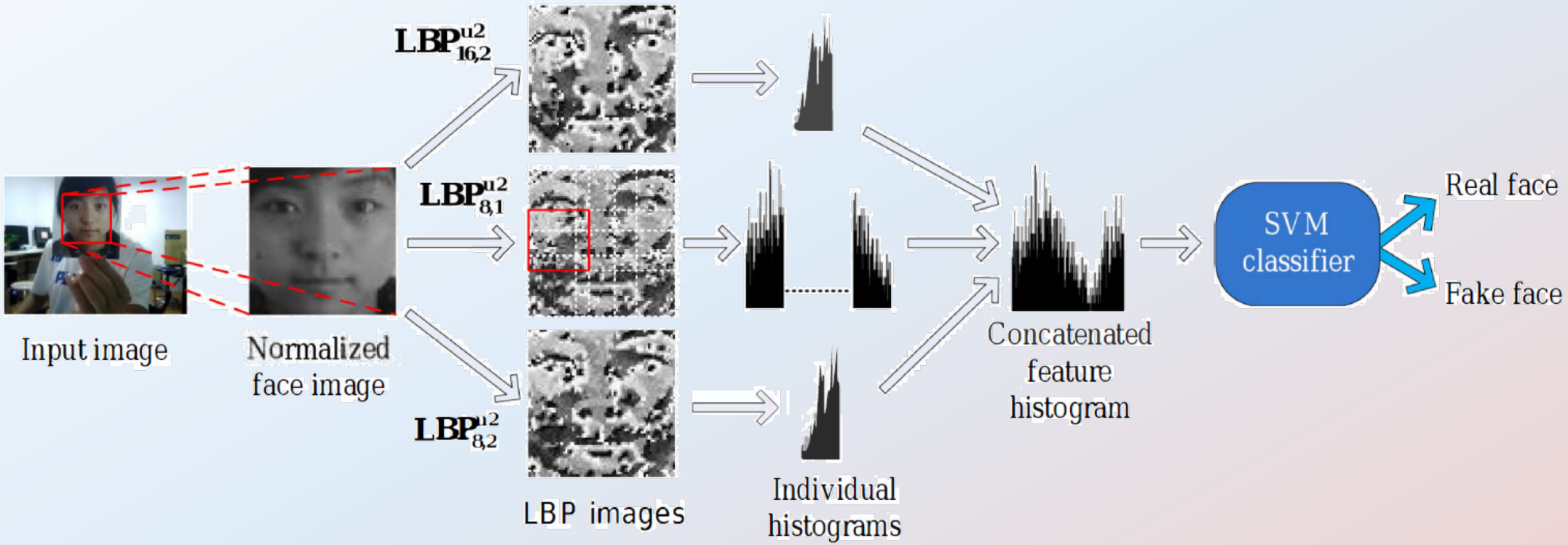
- Proposal: The multi-scale LBP feature is beneficial for discriminating between the luminance channel of live samples and photo attacks.
  - A live face will exhibit natural texture and reflectance
  - A photo attack will exhibit color gamut warping, artifacts, and unnatural reflectance

- Multi-scale LBP can detect anomalies in small patches or in larger patches.



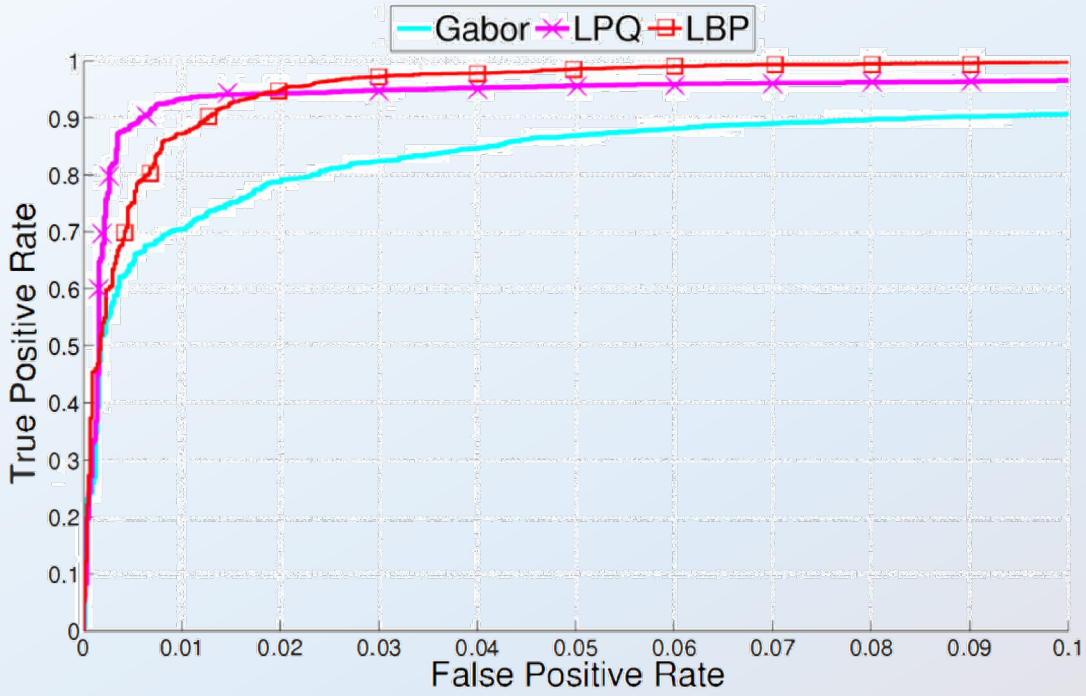
J. Maatta, A. Hadid, and M. Pietikainen. Face Spoofing Detection from Single Images using Micro-Texture Analysis. In IEEE IJCB, 2011.

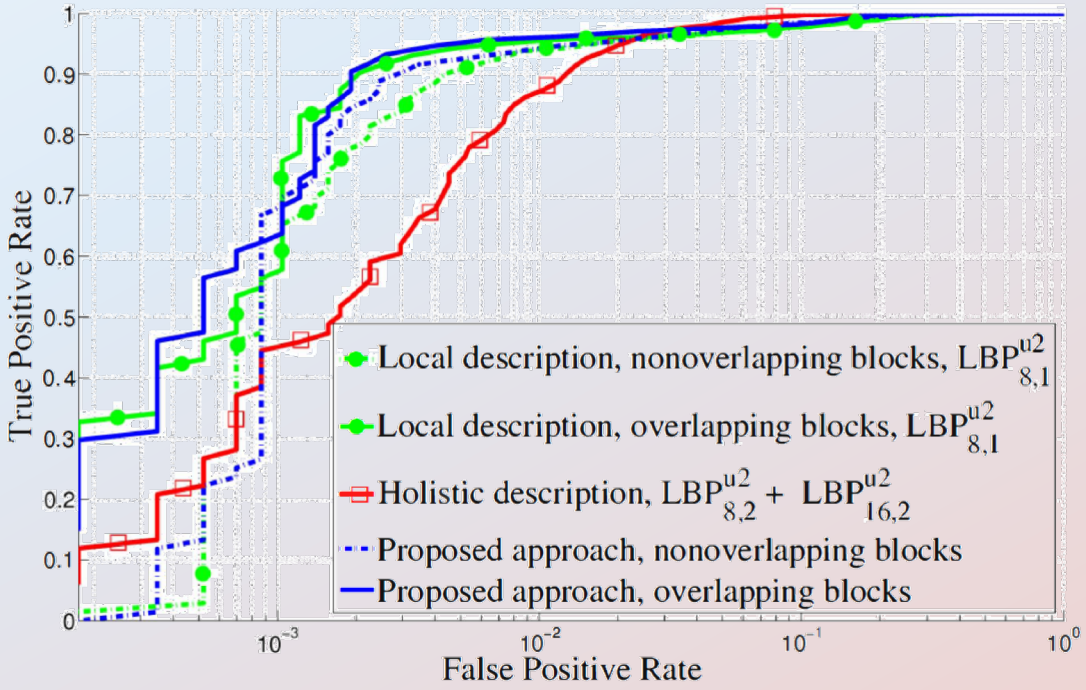
Micro-Texture Analysis



J. Maatta, A. Hadid, and M. Pietikainen. Face Spoofing Detection from Single Images using Micro-Texture Analysis. In IEEE IJCB, 2011.

Micro-Texture Analysis

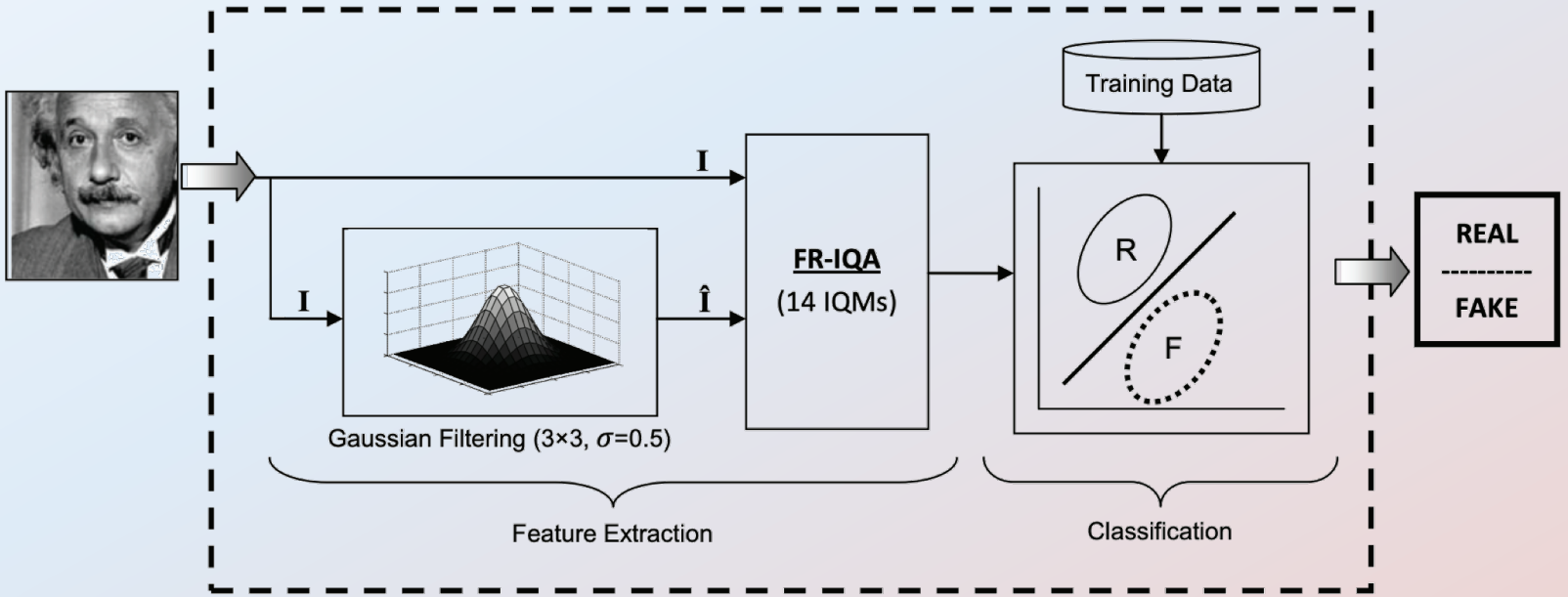




J. Maatta, A. Hadid, and M. Pietikainen. Face Spoofing Detection from Single Images using Micro-Texture Analysis. In IEEE IJCB, 2011.

IQA/IQM

- Image quality assessment/ Image quality measurement: assume the loss of quality produced by Gaussian filtering differs between real and fake biometric samples.



Javier Galbally and Sebastien Marcel. Face Anti-Spoofing Based on General Image Quality Assessment. *ICPR, 2014.*

IQA/IQM

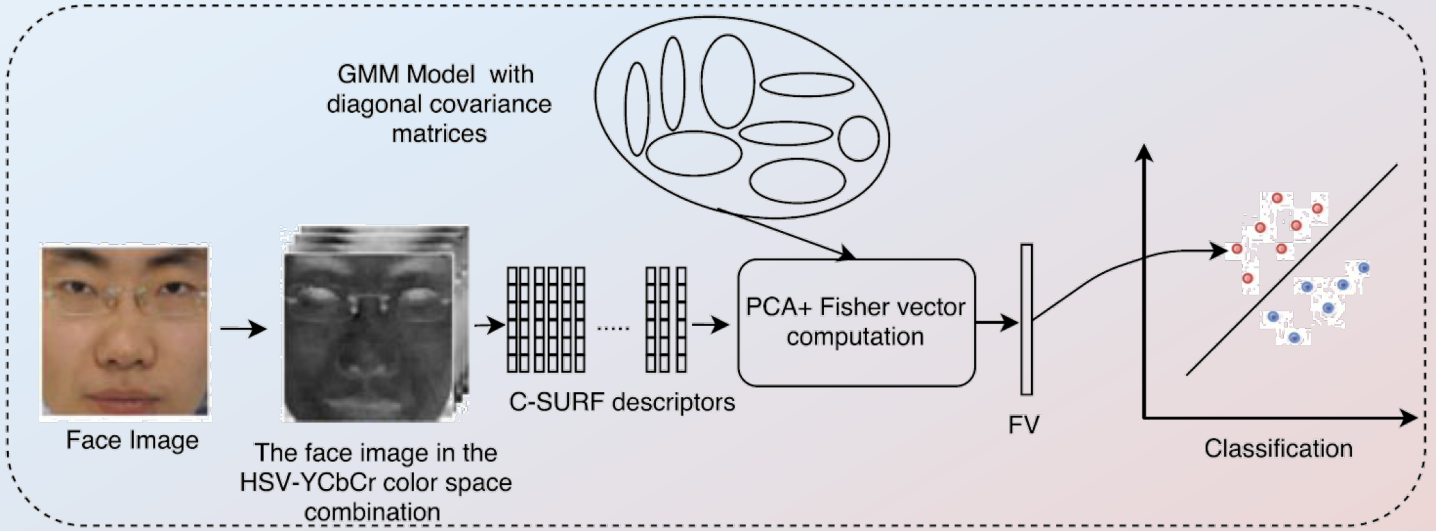
- Image quality assessment/ Image quality measurement

#	Acronym	Name	Ref.	Description
1	MSE	Mean Squared Error	[17]	$MSE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j})^2$
2	PSNR	Peak Signal to Noise Ratio	[18]	$PSNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\max(\mathbf{I}^2)}{MSE(\mathbf{I},\hat{\mathbf{I}})})$
3	SNR	Signal to Noise Ratio	[19]	$SNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{N\cdot M\cdot MSE(\mathbf{I},\hat{\mathbf{I}})})$
4	SC	Structural Content	[20]	$SC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\hat{\mathbf{I}}_{i,j})^2}$
5	MD	Maximum Difference	[20]	$MD(\mathbf{I},\hat{\mathbf{I}}) = \max\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert$
6	AD	Average Difference	[20]	$AD(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j})$
7	NAE	Normalized Absolute Error	[20]	$NAE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{i,j}\rvert}$
8	RAMD	R-Averaged MD	[17]	$RAMD(\mathbf{I},\hat{\mathbf{I}},R) = \frac{1}{R}\sum_{r=1}^{R}\max_r\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert$
9	LMSE	Laplacian MSE	[20]	$LMSE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}(h(\mathbf{I}_{i,j})-h(\hat{\mathbf{I}}_{i,j}))^2}{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}h(\mathbf{I}_{i,j})^2}$
10	NXC	Normalized Cross-Correlation	[20]	$NXC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}\cdot\hat{\mathbf{I}}_{i,j})}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}$
11	MAS	Mean Angle Similarity	[17]	$MAS(\mathbf{I},\hat{\mathbf{I}}) = 1-\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\frac{2}{\pi}\cos^{-1}\frac{\langle\mathbf{I}_{i,j},\hat{\mathbf{I}}_{i,j}\rangle}{\lvert\lvert\mathbf{I}_{i,j}\rvert\rvert\lvert\lvert\hat{\mathbf{I}}_{i,j}\rvert\rvert})$
12	MAMS	Mean Angle Magnitude Similarity	[17]	$MAMS(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(1-[1-\alpha_{i,j}][1-\frac{\lvert\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert\rvert}{255}])$
13	TED	Total Edge Difference	[21]	$TED(\mathbf{I}_\mathbf{E},\hat{\mathbf{I}}_\mathbf{E}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{\mathbf{E}i,j}-\hat{\mathbf{I}}_{\mathbf{E}i,j}\rvert$
14	TCD	Total Corner Difference	[21]	$TCD(N_{cr},\hat{N}_{cr}) = \frac{\lvert N_{cr}-\hat{N}_{cr}\rvert}{\max(N_{cr},\hat{N}_{cr})}$

Javier Galbally and Sebastien Marcel. Face Anti-Spoofing Based on General Image Quality Assessment. *ICPR, 2014.*

SIFT/SURF

- Proposal: Fisher vectors acting on Speeded Up Robust Features are an efficient method of extracting dense features to discriminate between live and spoof samples.
  - SURF will detect and utilize regions of interest to focus attention on discriminative local patches.



Z. Boulkenafet, J. Komulainen, and A. Hadid. Face Anti-Spoofing Using Speeded Up Robust Features and Fisher Vector Encoding. IEEE Signal Processing Letters, 2017.

SURF and Fisher Vectors

BTAS 2019

Method	Replay-Attack	CASIA-FASD
	Test	Test
LBP	45.9	57.6
LBP-TOP	49.7	60.6
Motion Mag	50.1	47.0
Color Texture$_1$	37.9	25.4
Color Texture$_2$	30.3	37.7
SURF	***26.9***	***23.2***

Method	Replay Attack		CASIA-FASD
	EER %	HTER %	EER %
CCD	-	-	11.8
DOG	-	-	17.0
Motion+LBP	4.5	5.1	-
LBP	13.9	13.8	18.2
LBP-TOP	7.8	7.6	10.6
Motion Mag	0.2	**0.0**	14.4
Color Texture$_1$	0.4	2.9	6.2
Color Texture$_2$	**0.0**	3.5	3.2
SURF	*0.1*	*2.2*	***2.8***

Z. Boulkenafet, J. Komulainen, and A. Hadid. Face Anti-Spoofing Using Speeded Up Robust Features and Fisher Vector Encoding. IEEE Signal Processing Letters, 2017.

Temporal Analysis Methods

BTAS 2019

- A temporal analysis method analyses the **involuntary** or **natural** movement or other phenomena of the face to discriminate between live and spoof samples.

- Representative Works
  - Optical Flow Fields (OFF)
  - Remote Photoplethysmography (rPPG)

W. Bao, H. Li, N. Li, and W. Jiang. A Liveness Detection Method for Face Recognition based on Optical Flow Field. In IEEE IASP, 2009
S. Liu, P. C. Yuen, S. Zhang, and G. Zhao. 3D Mask Face Anti-Spoofing with Remote Photoplethysmography. In ECCV 2016.
J. Hernandez-Ortega, J Fierrez, A. Morales, and P. Tome. Time Analysis of Pulse-Based Face Anti-Spoofing in Visible and NIR. In CVPR 2018.

Temporal Analysis Methods

BTAS 2019

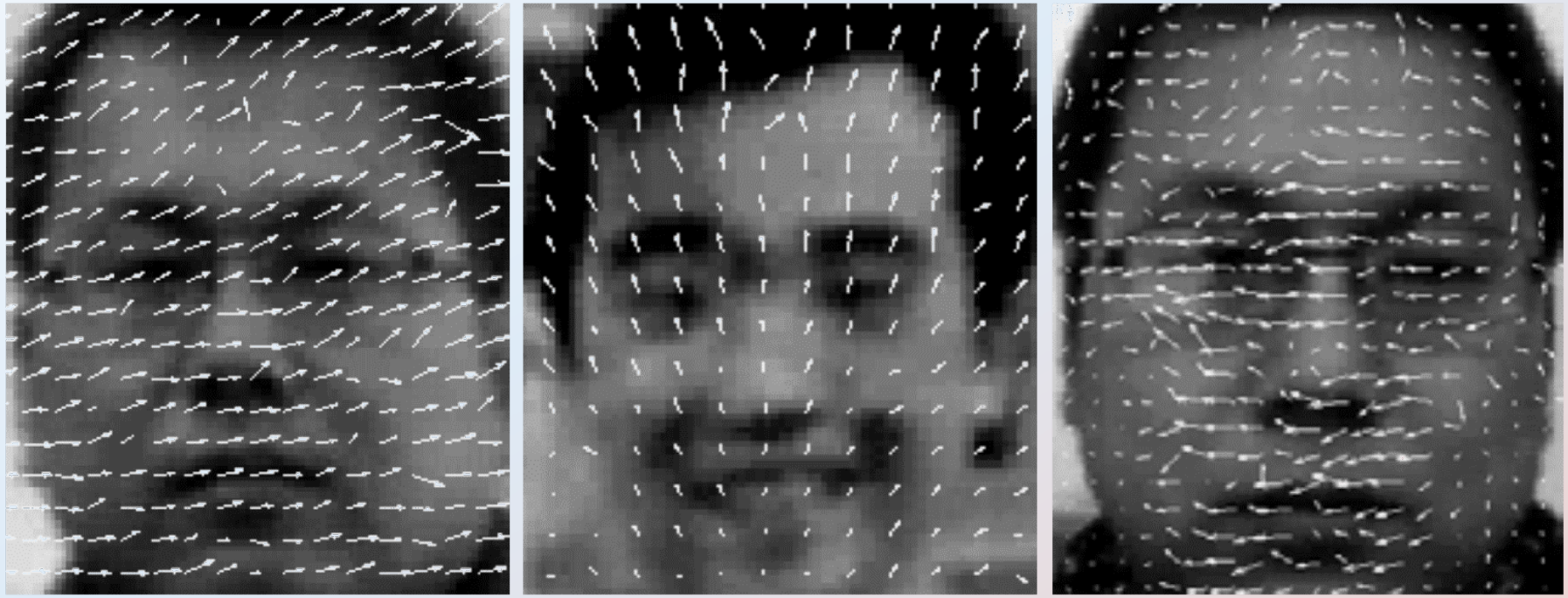
- A temporal analysis method analyses the **involuntary** or **natural** movement or other phenomena of the face to discriminate between live and spoof samples.

- Representative Works
  - **Optical Flow Fields (OFF)**
  - Remote Photoplethysmography (rPPG)

W. Bao, H. Li, N. Li, and W. Jiang. A Liveness Detection Method for Face Recognition based on Optical Flow Field. In IEEE IASP, 2009
S. Liu, P. C. Yuen, S. Zhang, and G. Zhao. 3D Mask Face Anti-Spoofing with Remote Photoplethysmography. In ECCV 2016.
J. Hernandez-Ortega, J Fierrez, A. Morales, and P. Tome. Time Analysis of Pulse-Based Face Anti-Spoofing in Visible and NIR. In CVPR 2018.

Optical Field Flow

- A temporal analysis method analyses the **involuntary** or **natural** movement or other phenomena of the face to discriminate between live and spoof samples.

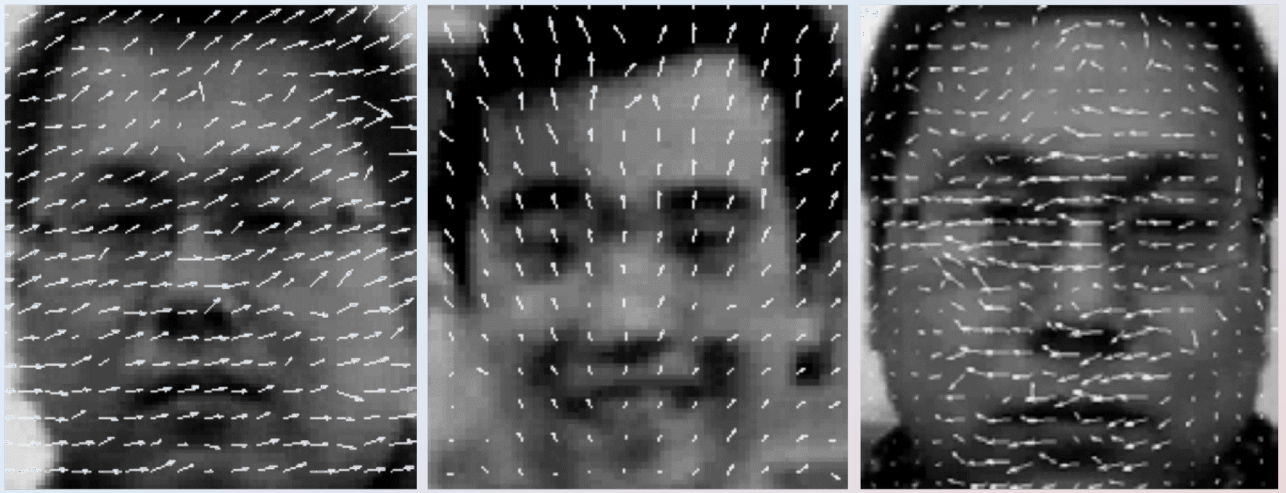


W. Bao, H. Li, N. Li, and W. Jiang. A Liveness Detection Method for Face Recognition based on Optical Flow Field. In IEEE IASP, 2009

Optical Field Flow

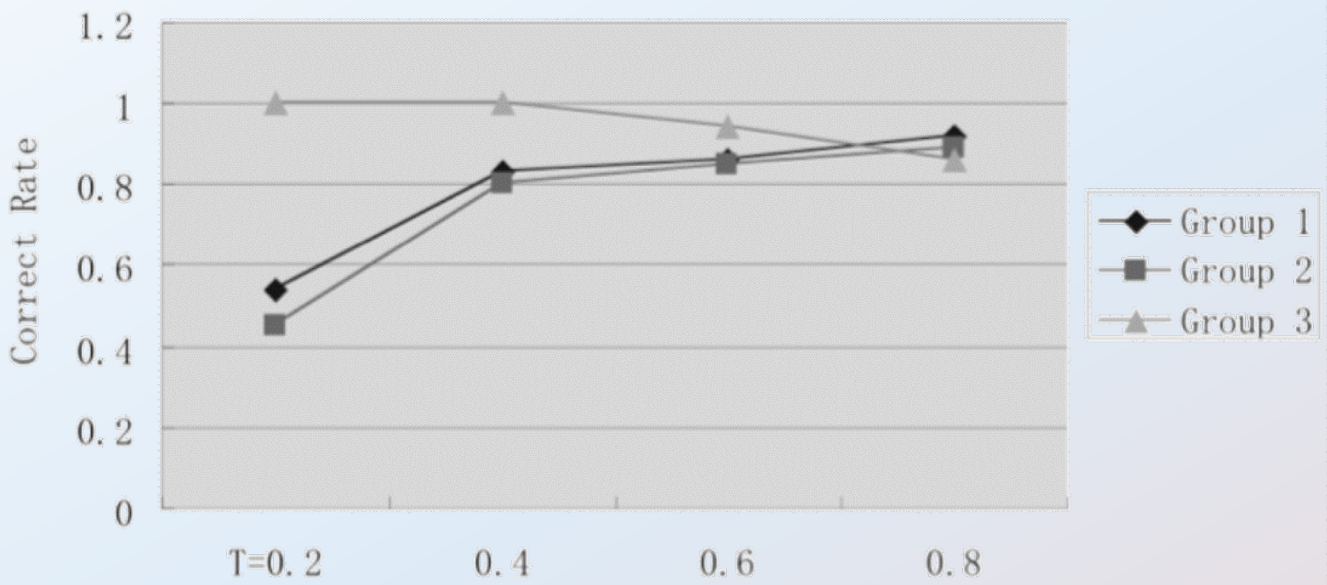
BTAS 2019

- Proposal: Optical flow fields are beneficial for discriminating between 3D live samples and 2D photo attacks.
  - The optical flow for real faces is non-uniform
  - The optical flow for rigid photo attacks is uniform
  - The optical flow for bent photos is non-uniform, but structured



W. Bao, H. Li, N. Li, and W. Jiang. A Liveness Detection Method for Face Recognition based on Optical Flow Field. In IEEE IASP, 2009

Optical Field Flow



Group	Time Frame Length			
	0.2	0.4	0.6	0.8
1	0.54	0.83	0.86	0.92
2	0.45	0.80	0.85	0.89
3	1.00	1.00	0.94	0.86

W. Bao, H. Li, N. Li, and W. Jiang. A Liveness Detection Method for Face Recognition based on Optical Flow Field. In IEEE IASP, 2009

Optical Field Flow

BTAS 2019

- Shortcomings
  - What is the minimum length of time required for strong classification?
  - How does the system behave if only part of the face is covered?

W. Bao, H. Li, N. Li, and W. Jiang. A Liveness Detection Method for Face Recognition based on Optical Flow Field. In IEEE IASP, 2009

Color Texture Analysis

BTAS 2019

Method	Replay Attack		CASIA-FASD	
	Dev	Test	Train	Test
Motion	50.2	50.2	47.7	48.2
LBP	44.9	47.0	57.3	57.9
LBP-TOP	48.9	50.6	60.0	61.3
Motion Mag	50.0	50.2	43.8	50.3
Color LBP -SVM-RBF	*22.5*	*20.6*	*47.5*	*43.9*
Color LBP -SVM-Linear	*17.7*	*16.7*	*38.6*	*37.6*

Method	Replay Attack		CASIA-FASD
	EER %	HTER %	EER %
IQA based	-	-	32.4
CCD	-	-	11.8
DOG	-	-	17.0
Motion+LBP	4.5	5.1	-
Motion	11.6	11.7	26.6
LBP	13.9	13.8	18.2
LBP-TOP	7.8	7.6	10.6
Motion Mag	0.2	0.0	14.4
Color LBP	*0.4*	*2.9*	***6.2***

Z. Boulkenafet, J. Komulainen, and A. Hadid. Face Anti-Spoofing Based on Color Texture Analysis. In ICIP, 2015

Temporal Analysis Methods

BTAS 2019

- A temporal analysis method analyses the **involuntary** or **natural** movement or other phenomena of the face to discriminate between live and spoof samples.

- Representative Works
  - Optical Flow Fields (OFF)
  - **Remote Photoplethysmography (rPPG)**

W. Bao, H. Li, N. Li, and W. Jiang. A Liveness Detection Method for Face Recognition based on Optical Flow Field. In IEEE IASP, 2009
S. Liu, P. C. Yuen, S. Zhang, and G. Zhao. 3D Mask Face Anti-Spoofing with Remote Photoplethysmography. In ECCV 2016.
J. Hernandez-Ortega, J Fierrez, A. Morales, and P. Tome. Time Analysis of Pulse-Based Face Anti-Spoofing in Visible and NIR. In CVPR 2018.

Remote Photoplethysmography (rPPG)

BTAS 2019

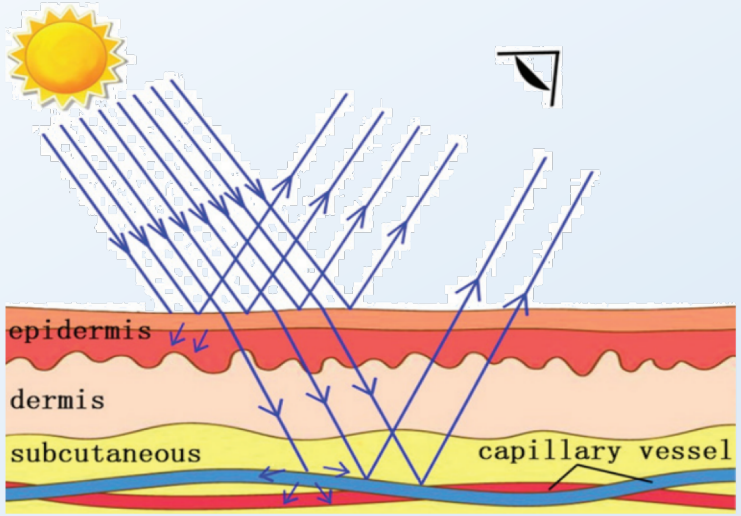
- Proposal: rPPG can be used to discriminate between live samples and 3D masks because a 3D mask will hide the rPPG signal from the live skin underneath.
  - The rPPG can be reliably predicted for a live sample
  - The rPPG cannot be predicted for a 3D mask sample

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

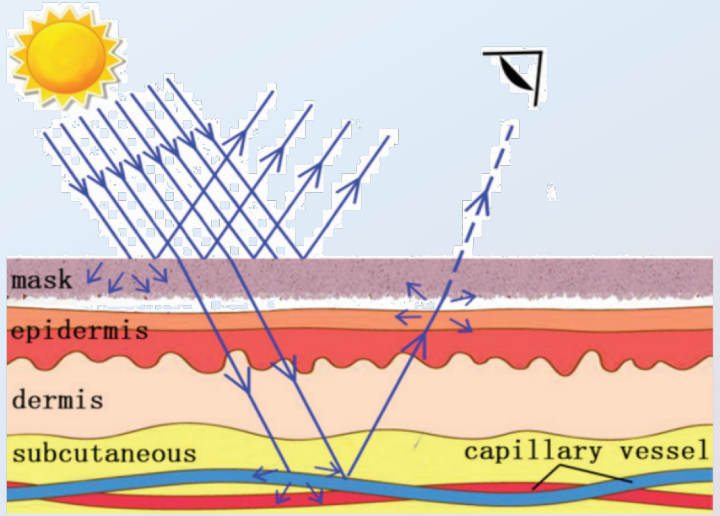
What is rPPG?

BTAS 2019

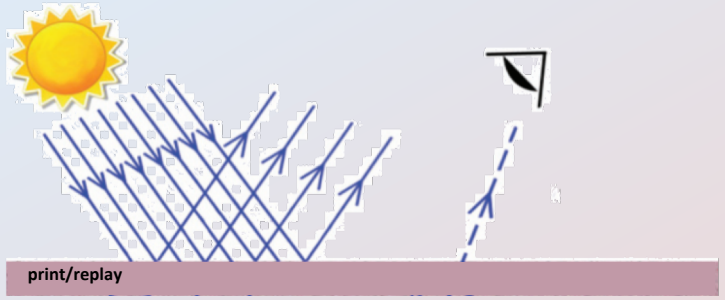
- Remote photoplethysmography: heart beat measurement from human skin using a non-contact camera



Live Face



3D Mask Spoof Face



Print/Replay Spoof Face

What is rPPG?

BTAS 2019

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

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

What is rPPG?

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

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

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

- Use signal-to-noise ratio (SNR) analysis

Haan et. al., Robust pulse-rate from chrominance-based rPPG, IEEE Transactions on biomedical engineering

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

Time Analysis of Pulse-Based Face Anti-Spoofing in Visible and NIR. CVPR 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

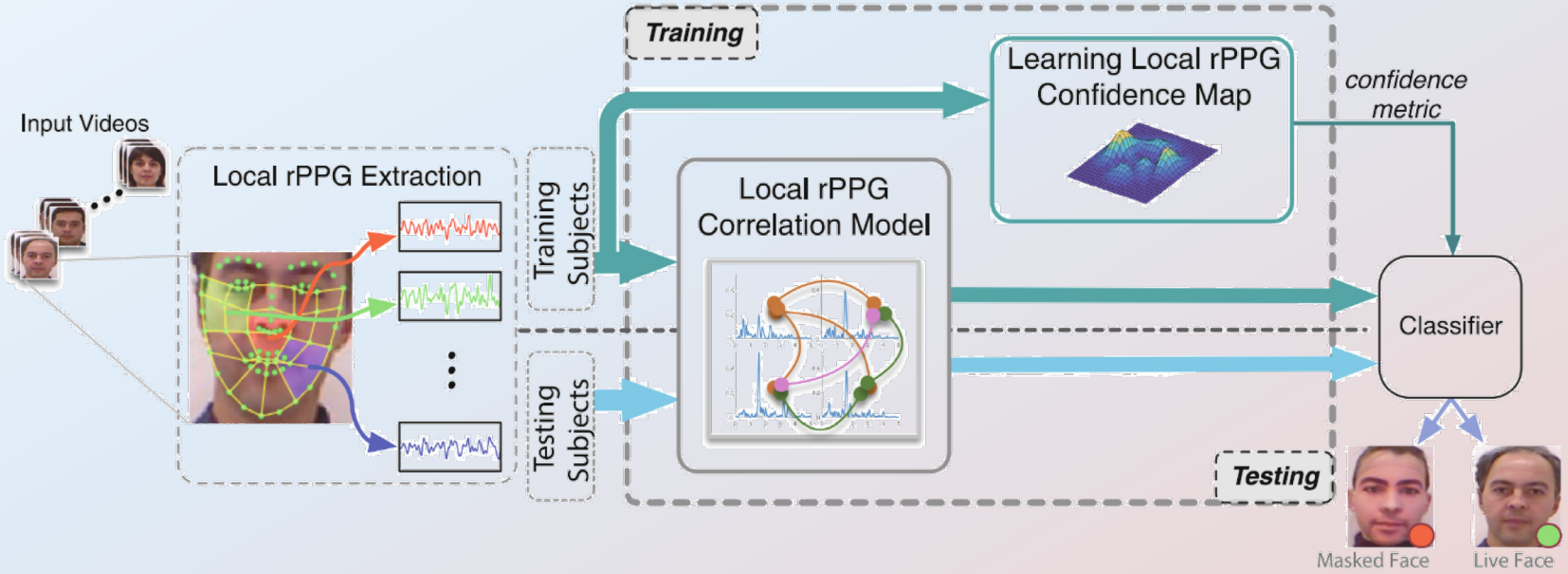
Time Analysis of Pulse-Based Face Anti-Spoofing in Visible and NIR. CVPR 2018.

Learning deep models for face anti-spoofing: binary or auxiliary supervision. CVPR 2018. (Talk in session 2)

3D Mask Face Anti-spoofing with Remote Photoplethysmography

BTAS 2019

- Handle 3D mask attack
- On live face, light go through skin and rPPG can be detected by camera
- On 3D mask, most lights are blocked by the mask, rPPG can be very weak

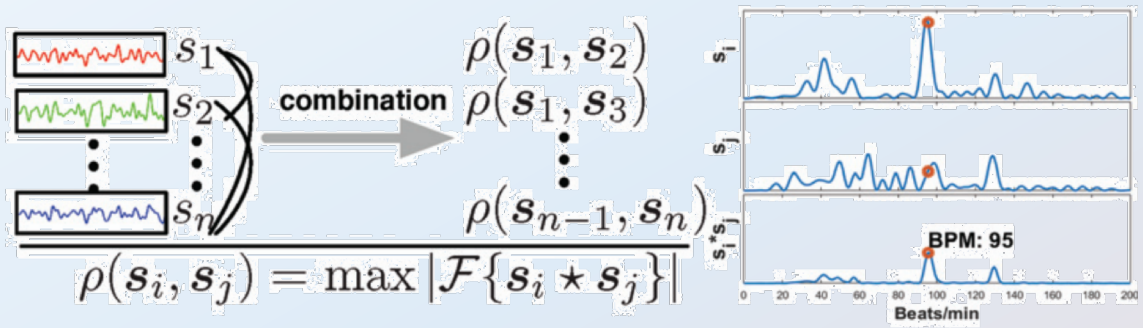


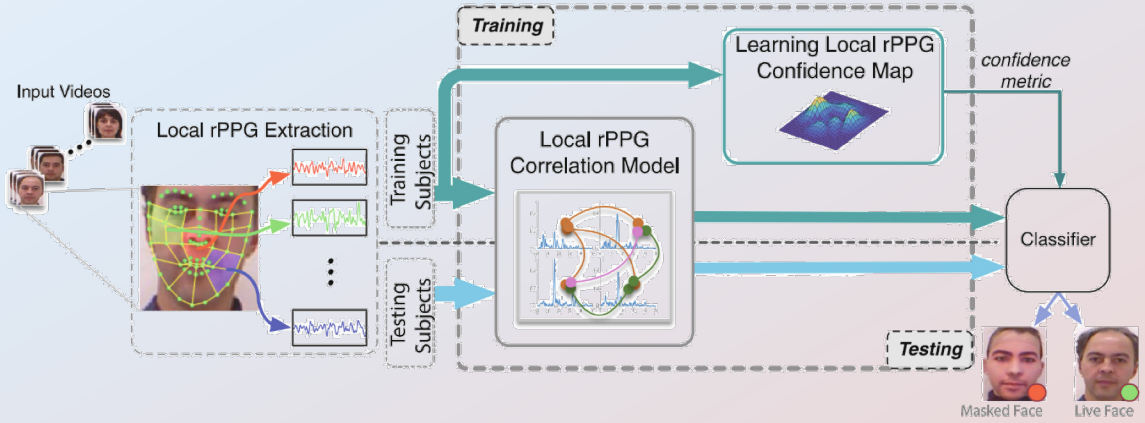
S. Liu, P. C. Yuen, S. Zhang, and G. Zhao. 3D Mask Face Anti-Spoofing with Remote Photoplethysmography. In ECCV 2016.

3D Mask Face Anti-spoofing with Remote Photoplethysmography

BTAS 2019

- Local rPPG correlation model



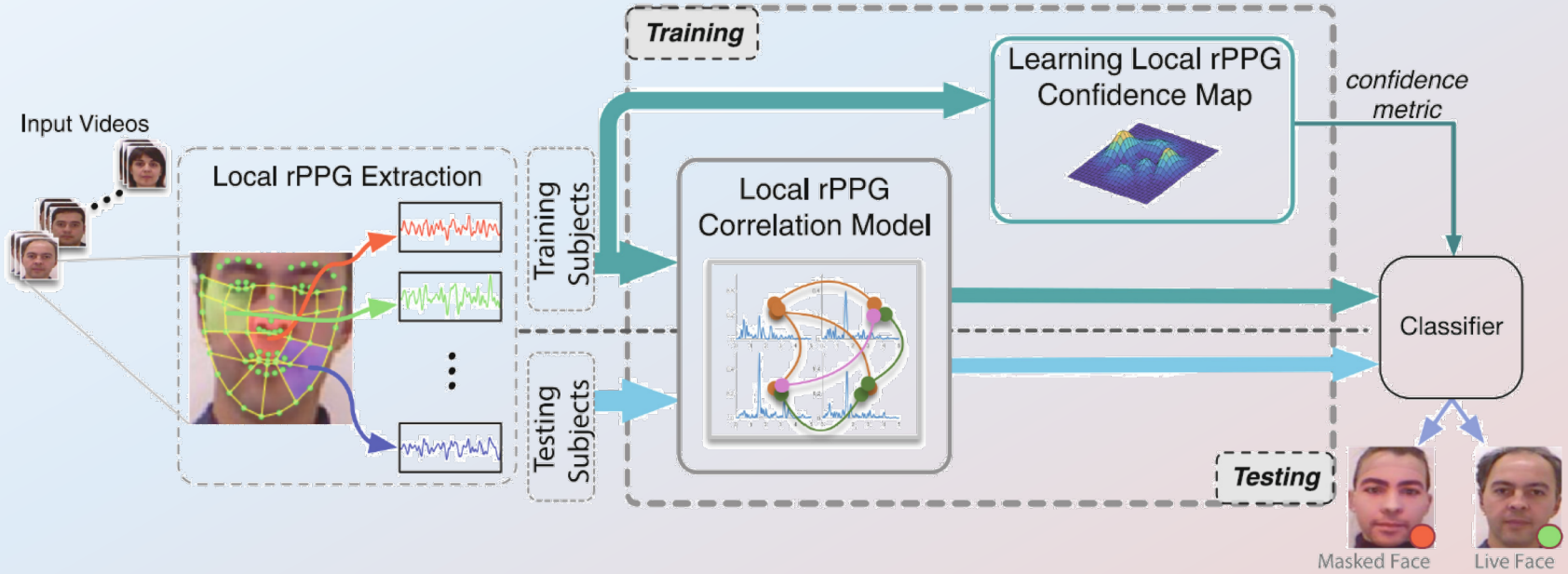


S. Liu, P. C. Yuen, S. Zhang, and G. Zhao. 3D Mask Face Anti-Spoofing with Remote Photoplethysmography. In ECCV 2016.

3D Mask Face Anti-spoofing with Remote Photoplethysmography

BTAS 2019

- local rPPG confidence map
  - reflects the reliability of local face regions



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

Remote Photoplethysmography (rPPG)

BTAS 2019

Method	Combined Dataset			Supplementary Dataset		
	HTER %	EER %	AUC %	HTER %	EER %	AUC %
Micro-Texture	13.8 ± 19.4	13.6	92.8	23.0 ± 21.2	22.6	86.8
Proposed	***9.7 ± 12.6***	***9.9***	***95.5***	***14.7 ± 10.9***	***16.2***	***91.7***

Method	3DMAD -> Sup			Sup -> 3DMAD		
	HTER %	EER %	AUC %	HTER %	EER %	AUC %
Micro-Texture	46.5 ± 5.1	49.2	51.0	64.2 ± 16.7	51.6	47.3
Proposed	***11.9*** ± 2.7	***12.3***	***94.9***	***17.4*** ± **2.4**	***17.7***	***91.2***

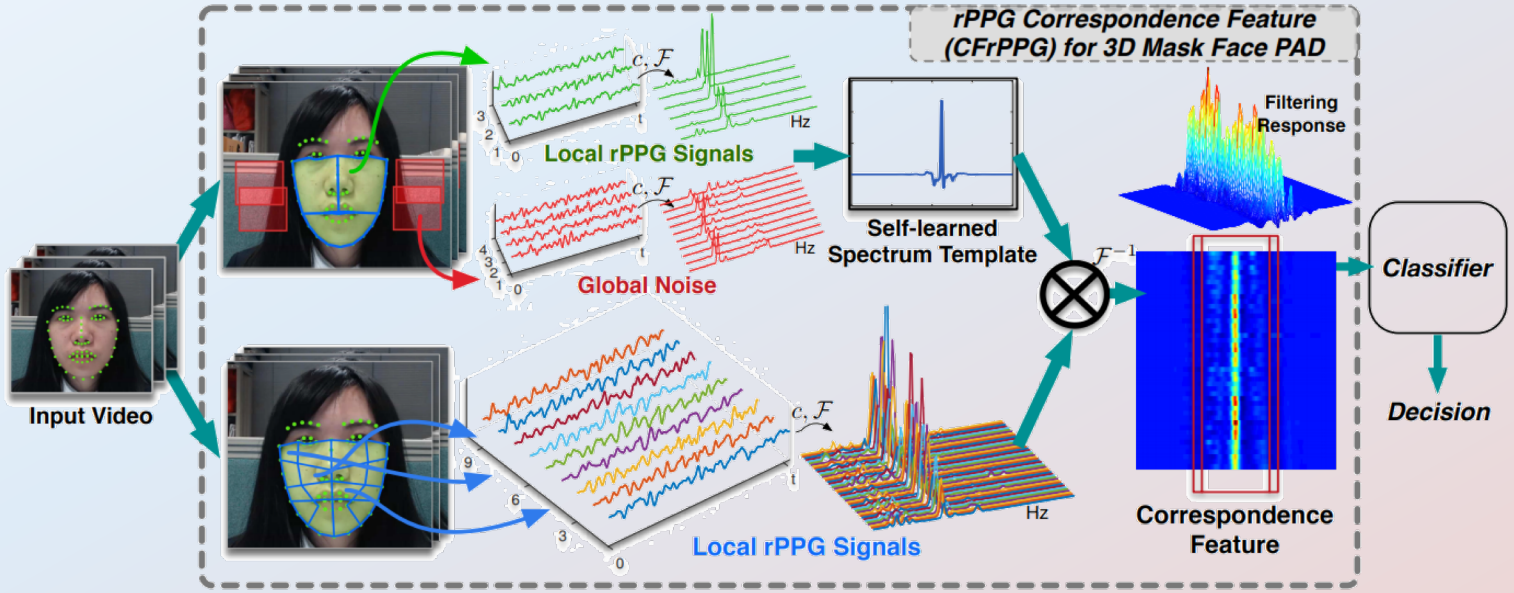
Inter and Intra-Dataset testing using the 3DMAD and Supplimentary datasets. The 3DMAD includes only hard masks, the supplementary includes hard masks and silicone masks.

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

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

BTAS 2019

- Leverage the background noise
- On live face, light go through skin and rPPG can be detected by camera
- On 3D mask, most lights are blocked by the mask, rPPG can be very weak



S. Liu, et. al., Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection. ECCV 2018.

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

BTAS 2019

- Perform well on cross-database testing

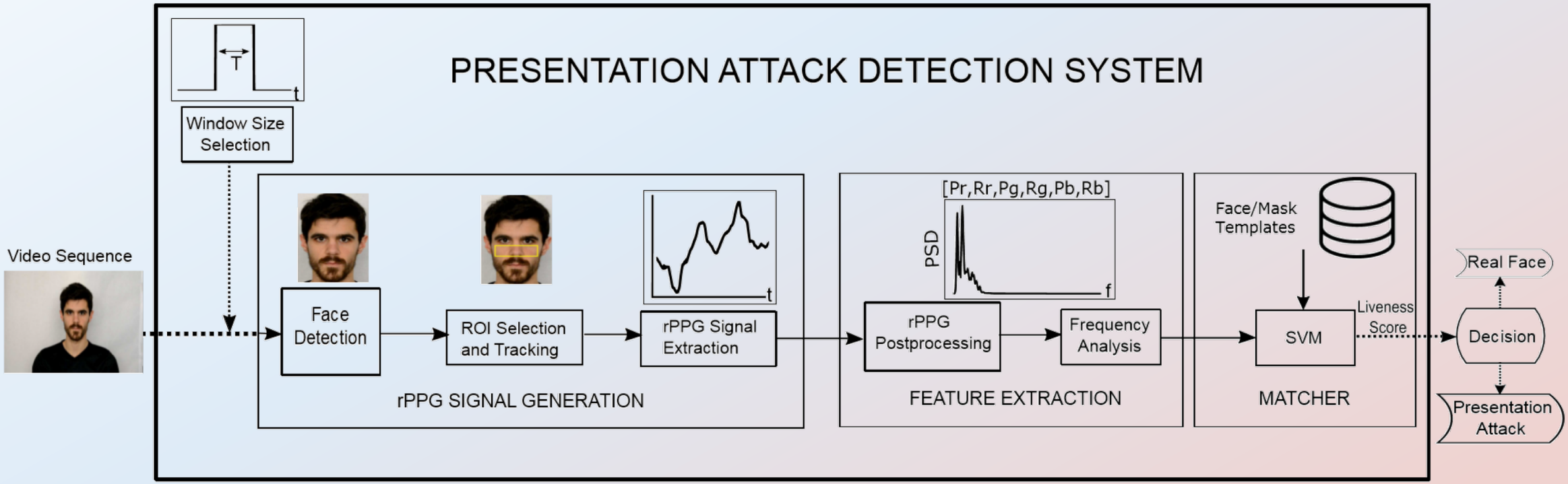
	3DMAD→HKBUMARsV2					HKBUMARsV2→3DMAD				
	HTER(%)	EER(%)	AUC(%)	FFR@ FLR=0.1	FFR@ FLR=0.01	HTER(%)	EER(%)	AUC(%)	FFR@ FLR=0.1	FFR@ FLR=0.01
MS-LBP [18]	53.0 ± 3.6	39.8	60.4	97.8	100.0	32.8 ± 11.5	32.5	75.3	58.5	87.8
CTA [41]	40.1 ± 7.8	40.2	62.1	87.1	98.3	47.7 ± 5.4	42.5	60.5	81.2	96.5
CNN	50.0 ± 0.0	47.8	54.6	82.6	97.9	50.0 ± 0.0	44.3	58.6	87.3	99.3
GrPPG [20]	24.3 ± 7.1	18.5	86.7	37.8	78.5	15.7 ± 6.8	15.4	87.2	20.6	94.5
LrPPG [19]	16.8 ± 5.0	10.9	95.6	12.4	61.7	17.4 ± 4.4	14.0	92.3	17.4	48.7
CFrPPG	**2.51 ± 0.1**	**5.08**	**99.0**	**2.19**	**19.6**	**2.55 ± 0.1**	**5.88**	**98.0**	**4.66**	**12.4**

S. Liu, et. al., Remote Photoplethysmography Correspondence Feature for 3D Mask Face Presentation Attack Detection. ECCV 2018.

rPPG Using Near Infra-Red (NIR) Data

BTAS 2019

- Proposal: NIR data more natively supports the prediction of rPPG, and is therefore more useful for rPPG-based anti-spoofing.



J. Hernandez-Ortega, J Fierrez, A. Morales, and P. Tome. *Time Analysis of Pulse-Based Face Anti-Spoofing in Visible and NIR. In CVPR 2018.*

rPPG Using Near Infra-Red (NIR) Data

BTAS 2019

Data	Video Length (s)	1	2	5	10	20	30	40	50	60
RGB	Mean EER (%)	46.9	45.7	42.1	40.1	40.0	40.0	36.6	30.0	25.0
	Std EER (%)	3.9	5.1	9.5	9.6	14.0	21.1	20.5	25.8	26.3
NIR	Mean EER (%)	42.4	41.7	38.4	30.9	30.0	16.6	5.0	0.0	0.0
	Std EER (%)	5.9	6.4	10.8	13.5	18.8	17.5	15.8	0.0	0.0

Subject based leave one out evaluation using RGB (3D-MAD, 17 subjects) data or NIR (self-collected, 10 subjects) data.

J. Hernandez-Ortega, J Fierrez, A. Morales, and P. Tome. *Time Analysis of Pulse-Based Face Anti-Spoofing in Visible and NIR. In CVPR 2018.*

Remote Photoplethysmography (rPPG)

BTAS 2019

- Shortcomings
  - How to construct rPPG groundtruth data?
  - How does the solution behave if the face is only half-covered?
  - How to improve performance on short videos?
  - How will rPPG behave for non-mask spoof types?

S. Liu, P. C. Yuen, S. Zhang, and G. Zhao. 3D Mask Face Anti-Spoofing with Remote Photoplethysmography. In ECCV 2016.
J. Hernandez-Ortega, J Fierrez, A. Morales, and P. Tome. *Time Analysis of Pulse-Based Face Anti-Spoofing in Visible and NIR. In CVPR 2018.*

Temporal Analysis Methods

BTAS 2019

- Pros
  - Models natural phenomena that are native to live samples
- Cons
  - Unable to evaluate individual images
  - Are these practical in real-time, commercial, scenarios?

W. Bao, H. Li, N. Li, and W. Jiang. A Liveness Detection Method for Face Recognition based on Optical Flow Field. In IEEE IASP, 2009
S. Liu, P. C. Yuen, S. Zhang, and G. Zhao. 3D Mask Face Anti-Spoofing with Remote Photoplethysmography. In ECCV 2016.

Summary

BTAS 2019

Factor	Interaction	Texture	Temporal
Evaluation on Individual Images		X	
Does not Require User Cooperation		X	X
Practical for Commercial Product	X	X	
Generalizable to Unknown Spoof Types	?	?	?

Summary

BTAS 2019

- Problem Definition and Motivation
- Common Spoof Attacks and Current Databases
- Conventional Approaches (before 2017)
  - Interaction Based Methods
  - Texture Analysis Methods
  - Temporal Analysis Methods

Summary

BTAS 2019

- Interaction Based Methods
  - Pro: Intuitive
  - Con: Easy to break
- Texture Analysis Methods
  - Pro: More robust than interaction based methods
  - Con: handcrafted features have limited performance
- Temporal Analysis Methods
  - Pro: Another degree of information
  - Con: Real-time?

Recent progress

BTAS 2019

- Deep Learning Based Methods
  - More data
  - More general
- Unknown Situations/Attacks

BTAS 2019

End of Session I

Q&A

MICHIGAN STATE UNIVERSITY

Computer Vision Lab

BTAS 2019

End of Session I

15 Minutes Break.

MICHIGAN STATE UNIVERSITY

Computer Vision Lab