Image Forensic: Face Spoofing

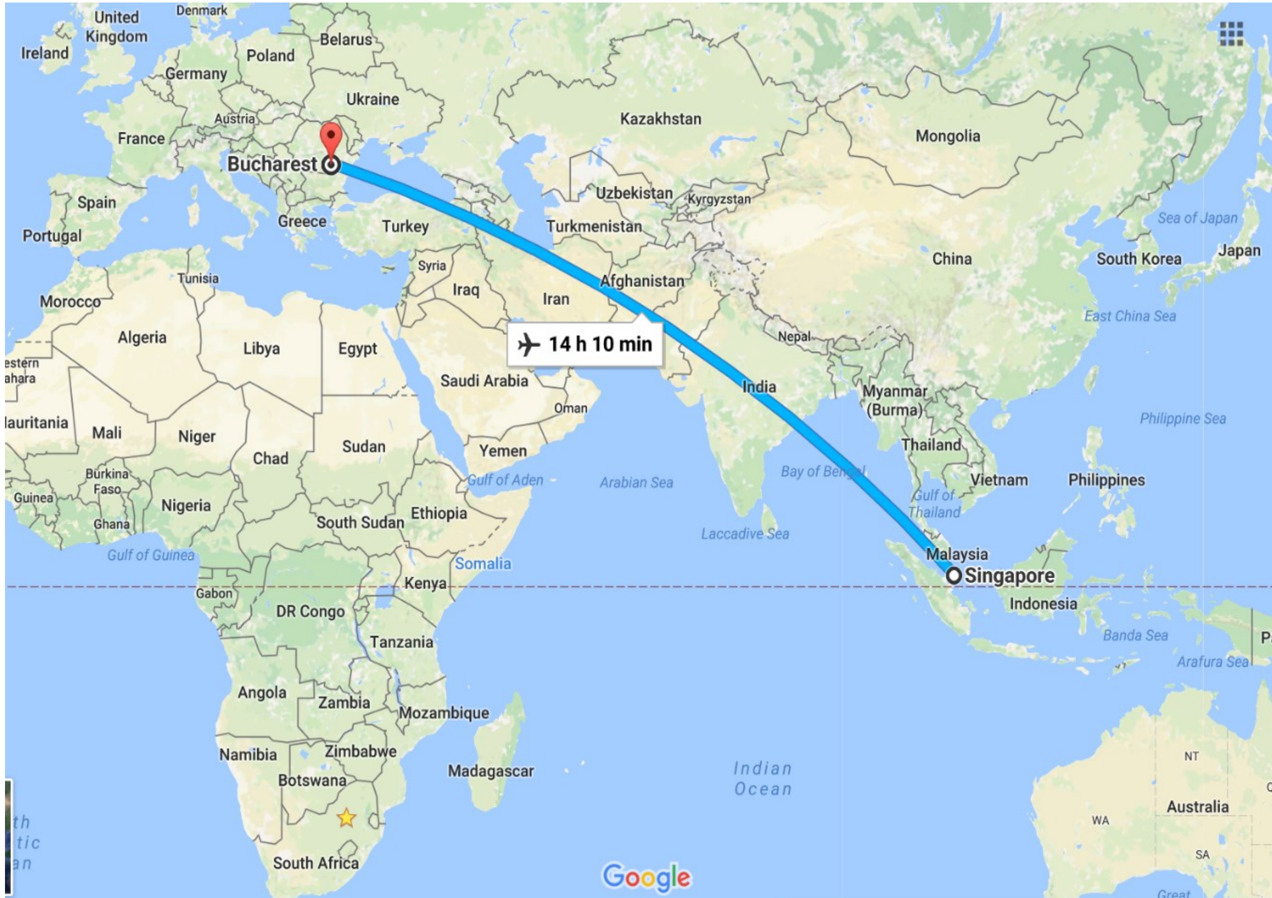
Alex Kot
ROSE Lab, CoE
Nanyang Technological University
Singapore

Acknowledgement: Li HaoLiang, Wang Shiqi, Cao Hong

NANYANG TECHNOLOGICAL UNIVERSITY

ROSE
Rapid-Rich Object Search Lab

Where is Singapore



NANYANG TECHNOLOGICAL UNIVERSITY

Yunnan Garden Campus



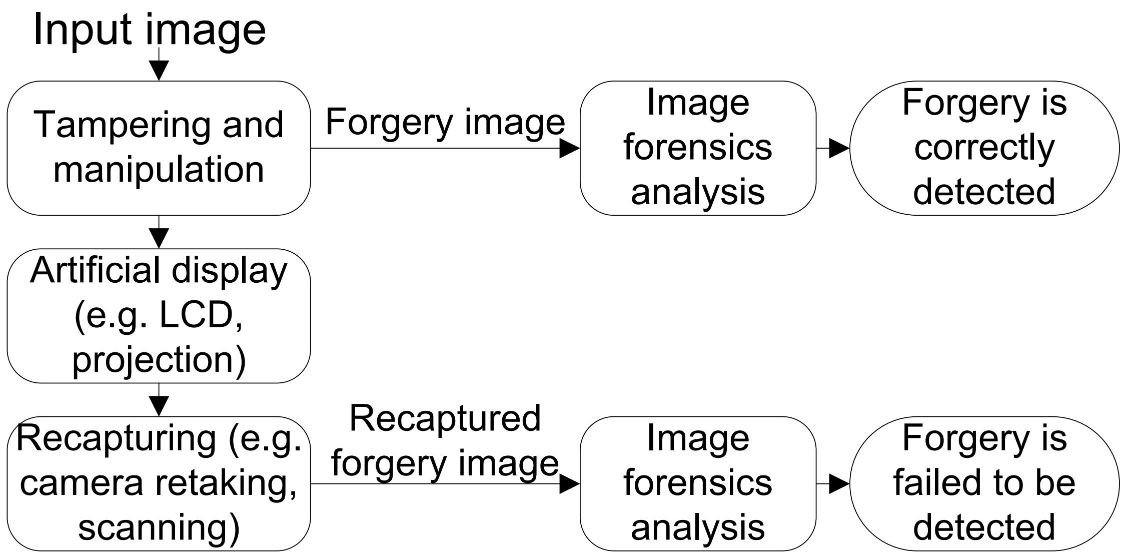






Are these photos captured directly from natural scenes?

Image Forensic: Image Recapturing Threat



- Artificial display media:
  - LCD and LED display, high-quality printing, photos, videos, projection…
- We study prevention of image recapturing threat using the common and ubiquitous LCD as the display media

Finely Recaptured Image Dataset

Examples of our finely recaptured images:

Canon DSC + Acer LCD

Olym. Mju DSC + NEC LCD

Olym. E500 DSLR+ Philips LCD

Our Recaptured Image Dataset:

- 9 camera-LCD combinations with 3 cameras and 3 LCDs
- A total of 2700 images

	Philips 190B6CG (19 Inch)	NEC AccuSync LCD 72VXM (17 Inch)	Acer AL712 (17 inch)
Canon Powershot A620	300	300	300
Olympus Mju 300	300	300	300
Olympus E500 DSLR	300	300	300

Human Identification of Carefully Recaptured Images

Survey steps:

- Introduction and training
- Inspection and decisions

Training photos:

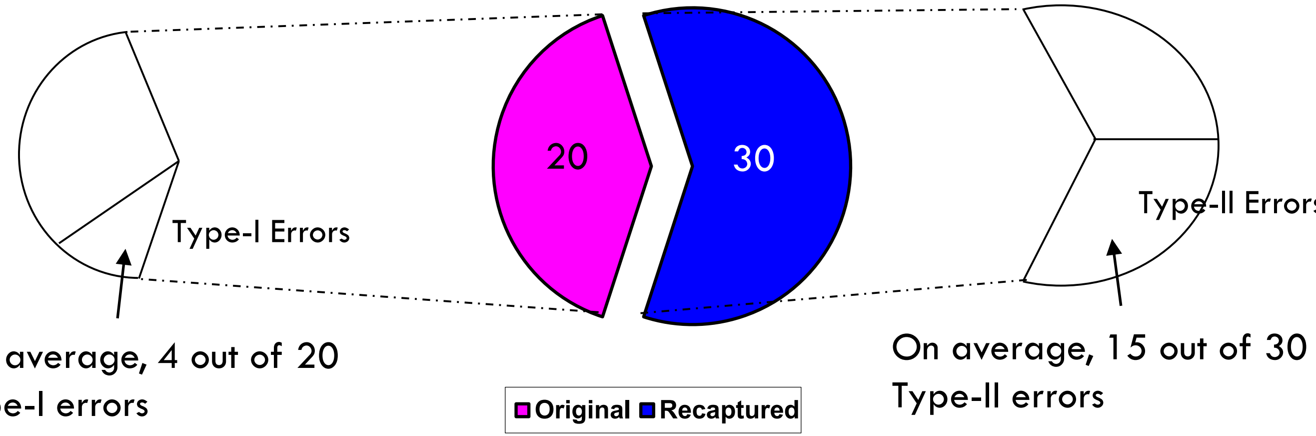
original retaken

50 Test photos (Mixture of natural and recaptured photos):

…

No Constraints on time, browsing tool and visual inspection methods

Human Classification Result



On average, 4 out of 20
Type-I errors

Ave Type-1 Err Rate: 20%
Std dev: 12.8%

On average, 15 out of 30
Type-II errors

Ave. Type-II Err Rate: 51%

Std dev: 18.3%

- 30 survey participants (mainly university staffs and students)
- Findings:
  - Human beings are poor in this classification, especially in identification of the recaptured images
- The finely recaptured photos post a threat to fool both human eyes and image forensic systems

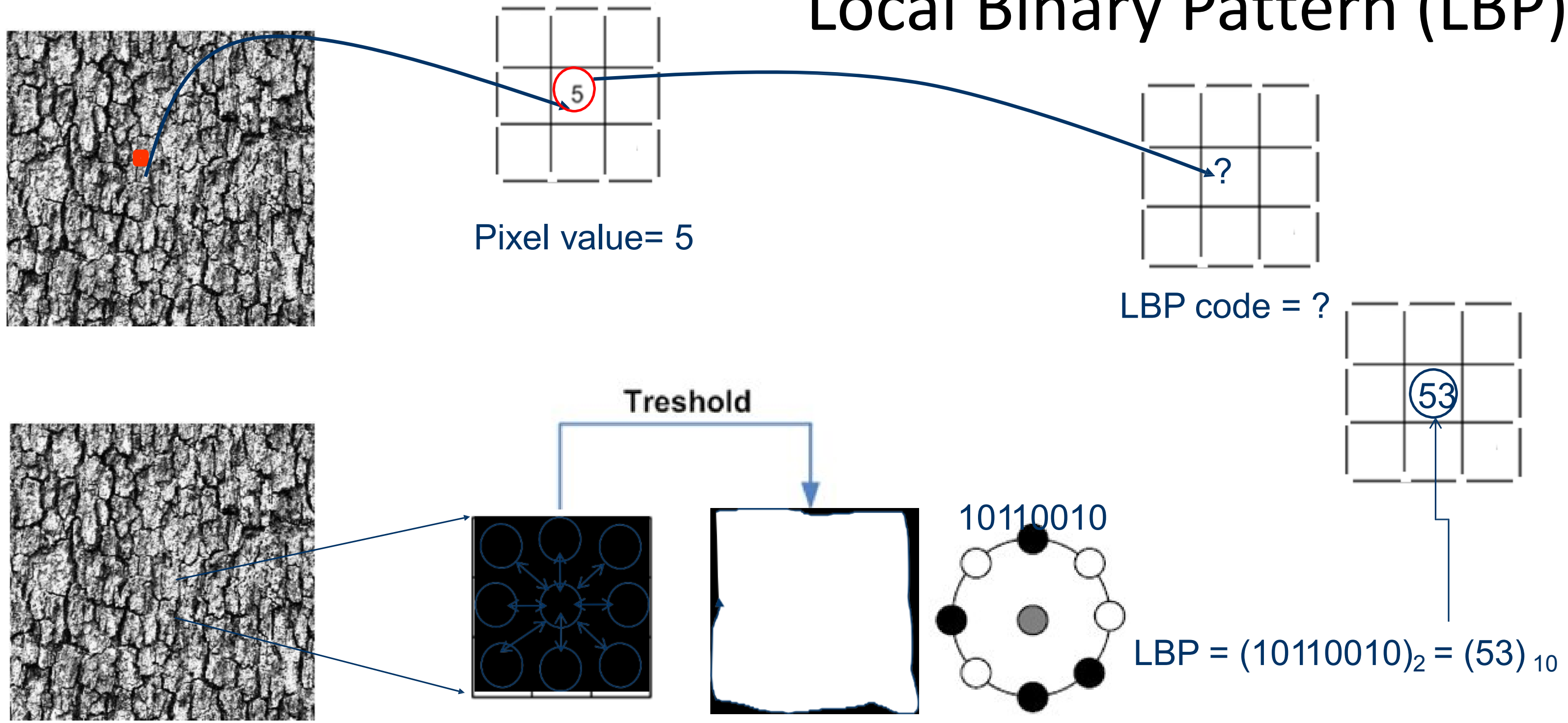
Artifacts of a Casually Recaptured Image on a LCD Screen

- Visible artifacts:
  - Textures
  - Loss of fine details
  - Color degradation
- Casually recapture often lead poor perceptional quality of the recaptured images

Original Image

A Recaptured Image

Local Binary Pattern (LBP)

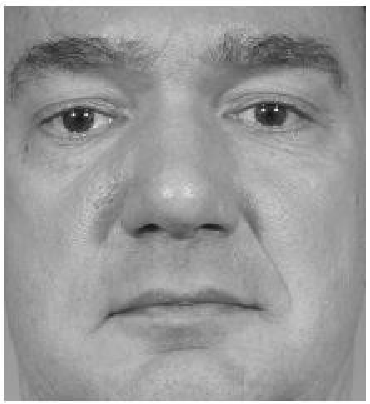


The value of the LBP code of a pixel (x_c, y_c) is given by:

$$LBP_{P,R} = \sum_{p=0}^{P-1} s(g_p - g_c)2^p \qquad s(x) = \begin{cases} 1, & if\ x \geq 0; \\ 0, & otherwise. \end{cases}$$

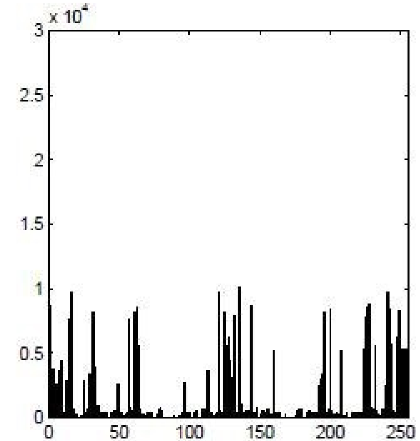
Courtesy from Abdenour Hadid

Example of an input image, the corresponding LBP image and histogram



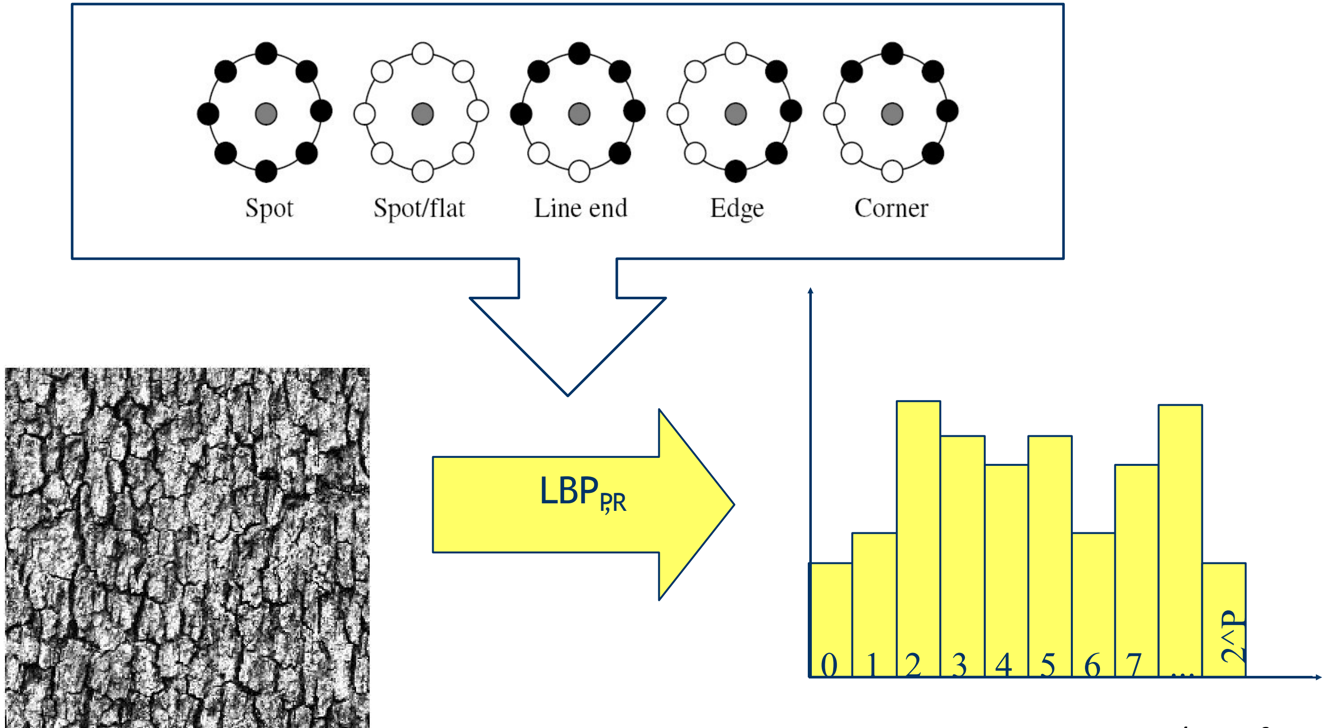
Input image

LBP image



LBP histogram

Courtesy from Abdenour Hadid



$LBP_{P,R}$ (P:#of pts, R:radius)

✓Invariance to any monotonic gray level change
✓ High discriminative power
✓ Computational simplicity

Proposed Features for Computer Identification of Recaptured Photos -[Cao&Kot IEEE ICASSP2010]

- Local Binary Patterns (LBP) [1]
  - To measure the texture patterns
  - 80 features
- Multi-Scale Wavelet Statistics (MSWS)
  - To measure the loss of fine details characteristics
  - 54 features
- Color Features (CF) [2, 3]
  - To measure the color anomalies
  - 21 features

1. Ojala *et al*. PAMI, 2002
2. Memon *et al*. ICIP 2004
3. Ma *et al*. ICME, 2006

Computer Classification Results

Image Datasets:

•2100 **recaptured** images and 2000 natural images (1024×1024) from 12 cameras

•80% for training and 20% for testing;

•Five random apportions of training and test images

•Probabilistic Support Vector Machine (PSVM) Classifier

Features	Dimension	EER (%)	EER Threshold
LBP	80	0.9	0.55
MSWS	54	1.1	0.35
CF	21	17.4	0.47
LBP+MSWS	134	0.7	0.43
LBP+MSWS+CF	**155**	**0.5**	**0.50**
Wavelet Stats	216	3.4	0.43

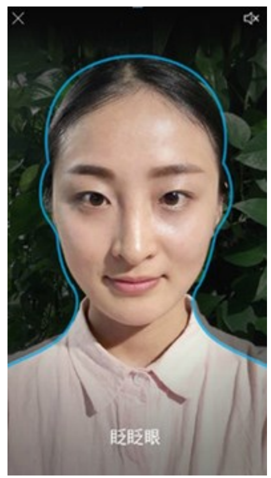
1. S. Lyu and H. Farid, "How Realistic is Photorealistic?," *IEEE Trans. on Signal Processing*, vol. 53, pp. 845-850, Feb 2005.
2. T.-T. Ng, S.-F. Chang, J. Hsu, L. Xie, and M.-P. Tsui, “Physics-Motivated Features for Distinguishing Photographic Images and Computer Graphics,” in Proc. ACM Int. Conf. on Multimedia, pp. 239-248, 2005

Image Forensic: Recapturing → Face spoofing

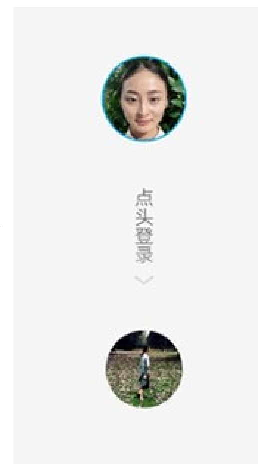
Biometric verification is becoming more and more popular. However, it is vulnerable being attacked.

Attacking

User Authorization
Alipay: Smile to Pay



Face Verification



User Authentication

- Printed Photo Attack
- Replay Video Attack
- Mask Attack

https://intl.alipay.com/

Face Spoofing Detection

- Distortion based approaches
  - Gabally *et al*., Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition. IEEE-TIP 2014
  - Wen *et al*. Face Spoof Detection With Image Distortion Analysis, IEEE-TIFS 2015
- Temporal information based approaches
  - Pinto *et al*., Using Visual Rhythms for Detecting Video-Based Facial Spoof Attacks. IEEE-TIFS 2015
  - Pinto *et al*., Face Spoofing Detection Through Visual Codebooks of Spectral Temporal Cubes. IEEE-TIP 2015
- Deep learning approaches
  - Menotti *et al*. Deep Representations for Iris, Face, and Fingerprint Spoofing Detection, IEEE-TIFS 2015
  - Yang *et al*. Learn Convolutional Neural Network for Face Anti-Spoofing, arXiv, 2014
- Domain adaptation based approaches
  - Yang *et al*. Person-Specific Face Antispoofing With Subject Domain Adaptation, IEEE-TIFS 2015
- Texture based approaches
  - Patel *et al*. Secure Face Unlock: Spoof Detection on Smartphones, IEEE-TIFS 2016
  - Boulkenafet *et al*. Face Spoofing Detection Using Colour Texture Analysis, IEEE-TIFS 2016
  - Boulkenafet *et al*. Face Anti-spoofing using Speed-Up Robust Features and Fisher Vector Encoding, IEEE-SPL 2017

Evaluation Datasets

Summary of 2D face spoofing datasets

Dataset	Year of Release	# Subj	#Samples (Live, Spoof)	Attack Type
IDIAP Replay-attack [EPFL]	2012	50	(200,1000)	Paper recapture attack Video recapture attack Image recapture attack
CASIA [CAS]	2012	50	(200, 450)	Paper recapture attack Video recapture attack Cut photo mask attack
MFSD [MSU]	2014	55	(110, 330)	Paper recapture attack Video recapture attack
USSA [MSU]	2016 (internet photos)	1140	(1140, 9120)	Paper recapture attack Image recapture attack
UVAD [CAMPINES]	2015 (not mobile camera)	404	(808, 16268)	Video recapture attack
ROSE-Youtu {NTU/Tencent]	2017 (real scenarios)	25	(570, 3430)	Paper recapture attack Video recapture attack Cut photo mask attack

Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition

[Galbally, Marcel and Fierrez, TIP, 2014]

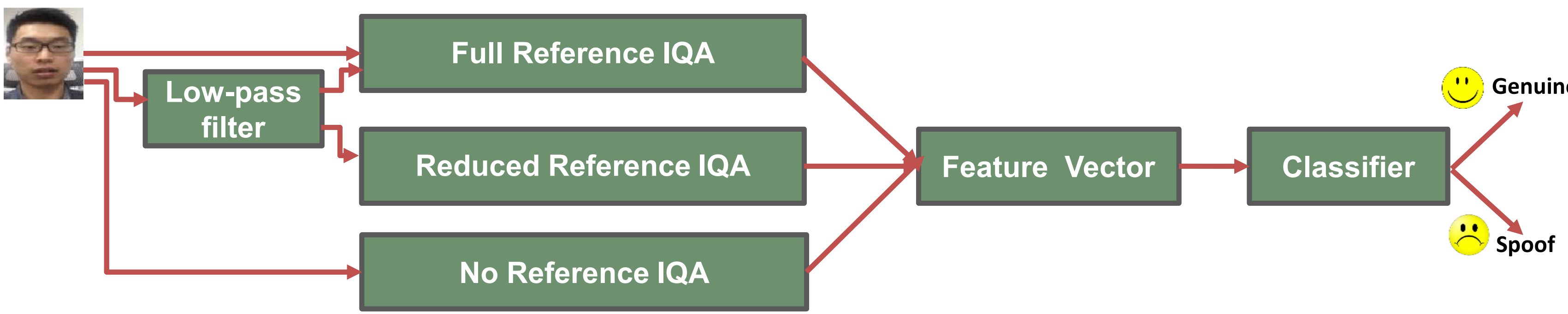
- Features
  - 25 image quality assessment scores
    - 20 full reference algorithms:
      - MSE, PSNR, SSIM, NAE, VIF….
      - Gaussian smoothing is employed to generate image pairs
    - 1 reduced reference algorithms
      - RRED
      - Gaussian smoothing is employed to generate image pairs
    - 4 no reference algorithms
      - JQI & HLFI (without training)
      - BIQI & NIQE (Training based approaches)
- Classifier
  - Linear discriminant analysis (LDA)
- Limitation
  - Acquisition environments are different
  - IQA is designed based on perceptual cues of human visual system

MSE: mean square error
PSNR: peak-signal-to-noise-ratio
SSIM: structural similarity
NAE: normalized absolute error
VIF: visual information fidelity
RRED: reduce reference entropic difference
JQI: jpeg image quality index
HLFI: high low frequency index
BIQI: blind image quality index
NIQE: natural image quality evaluator

Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition

[Galbally, Marcel and Fierrez, TIP, 2014]

- Image quality scores are employed as features
- Directly connects image quality assessment (IQA) and spoofing detection
- The proposed scheme is effective for iris, fingerprint and face spoofing
- 15.2% HTER for the Replay-attack database



Framework of the anti-spoofing scheme with image quality assessment

Face Spoof Detection with Image Distortion Analysis

[Wen, Han and Jain, TIFS, 2015]

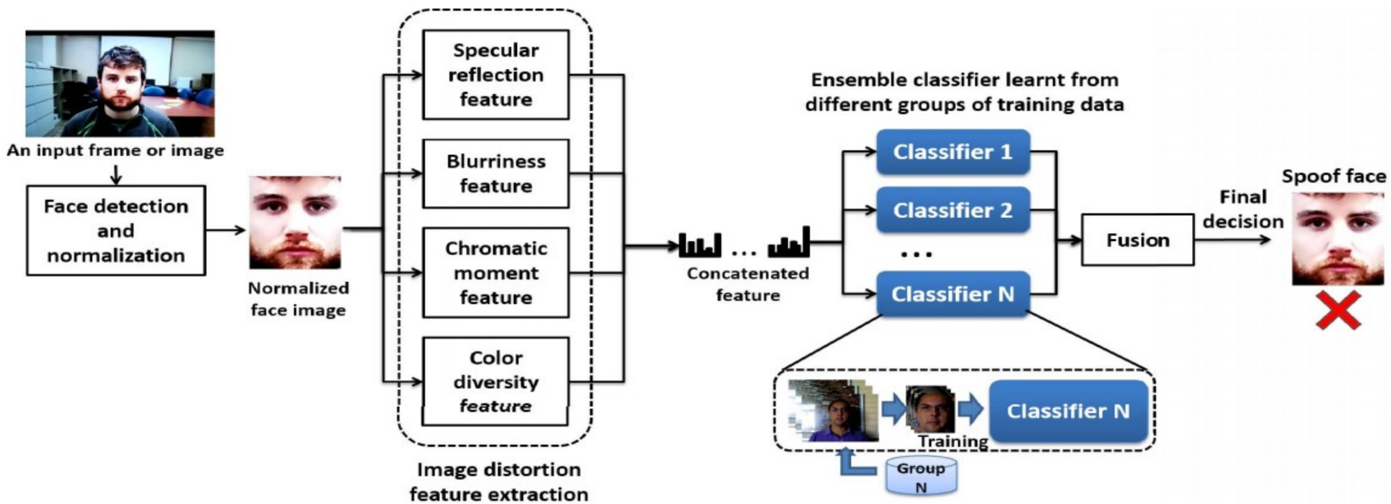
- Features
  - Specular Reflection
    - Specular pixel percentage
    - Mean and variance of specular pixels
  - Blurriness
    - Difference between original input and blurred version
    - Average edge depth
  - Chromatic Moment
    - HSV mean, deviation and skewness
    - Percentage of pixels in the minimal and maximal histogram bins
  - Color Diversity
    - The histogram bin counts of the top 100 most frequently appearing colors
    - The number of distinct colors appearing in the normalized face image

- Classifier
  - Ensemble Classifier
    - Divide the training set according to the attack type
    - Min rule for score fusion

Face Spoof Detection with Image Distortion Analysis

[Wen, Han and Jain, TIFS, 2015]

- Distortion based approach for face spoofing
- Four distortion relevant features are adopted
- Ensemble classifier is used for spoofing detection
- Achieves the performance (HTER = 7.4%) on Idiap replay-attack database



Face spoof detection algorithm based on image distortion analysis (source: Ref [4])

NANYANG TECHNOLOGICAL UNIVERSITY

ROSE Rapid-Rich Object Search Lab 博云搜索实验室

Secure Face Unlock: Spoof Detection on Smartphones

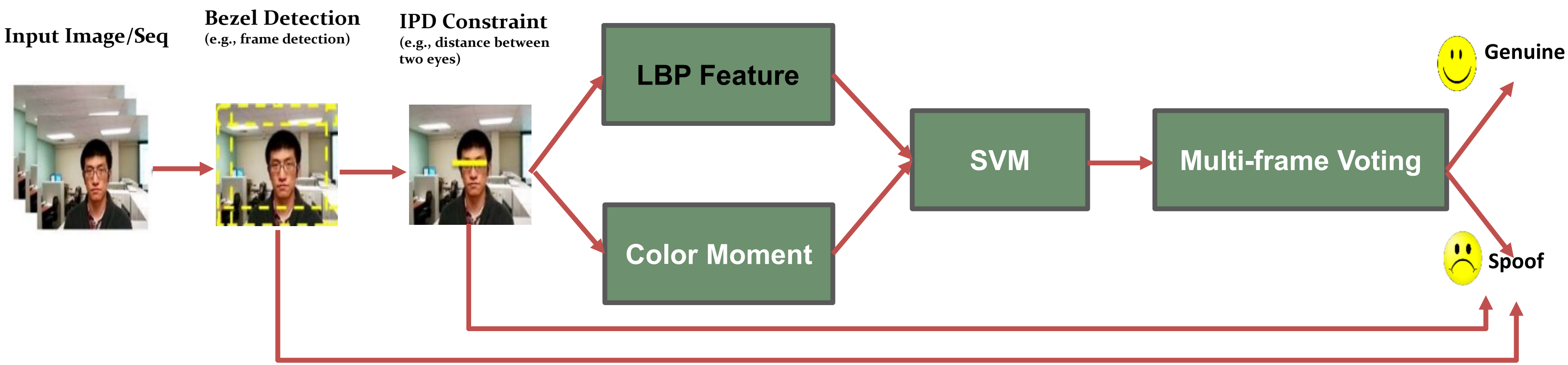
[Patel, Han and Jain, TIFS 2016]

- Rejection
  - Inter Pupilliary Distance (IPD) Constraint
    - IPD represents the distance between the center of the right eye to the center of the left eye
    - Faces that are either small or large are rejected
  - Bezel detection
    - Detect fairly constant colors along the top, bottom, right and left edges
- Complementary Features
  - Face texture analysis
    - **LBP** feature
  - Different color distribution of spoof and genuine faces
    - Color moment
- Classifier
  - SVM
- Voting
  - Two or more frames in a 3-frame sequence is live (majority voting)

Secure Face Unlock: Spoof Detection on Smartphones

[Patel, Han and Jain, TIFS 2016]

- A new database for smartphone spoof attack database (>1000 subjects)
- A novel spoofing pipeline with rejection, complementary feature representation and multi -frame voting
- Under the smartphone protocol for face unlock, the proposed approach achieves 0% HTER on Idiap Replay-Attack, 1.67% EER on CASIA FASD, and 2.67% EER on MSU-MFSD databases



Framework of the face anti-spoofing scheme with rejection, complementary feature representation and multi-frame voting

Using Visual Rhythms for Detecting Video-Based Facial Spoof Attacks

[Pinto, Schwartz, Pedrini and Rocha, TIFS, 2015]

- Features
  - Noise signature extraction
    - Subtracting original image with the blurred version
  - Fourier Spectrum
    - Calculating the Fourier Spectrum of the noise signature video
  - Visual Rhythms
    - Rotate the video and view the temporal-spatial information
  - Feature extraction
    - Gray-Level Co-occurrence Matrices (GLCM)
    - **LBP**, HOG
- Classifier
  - SVM

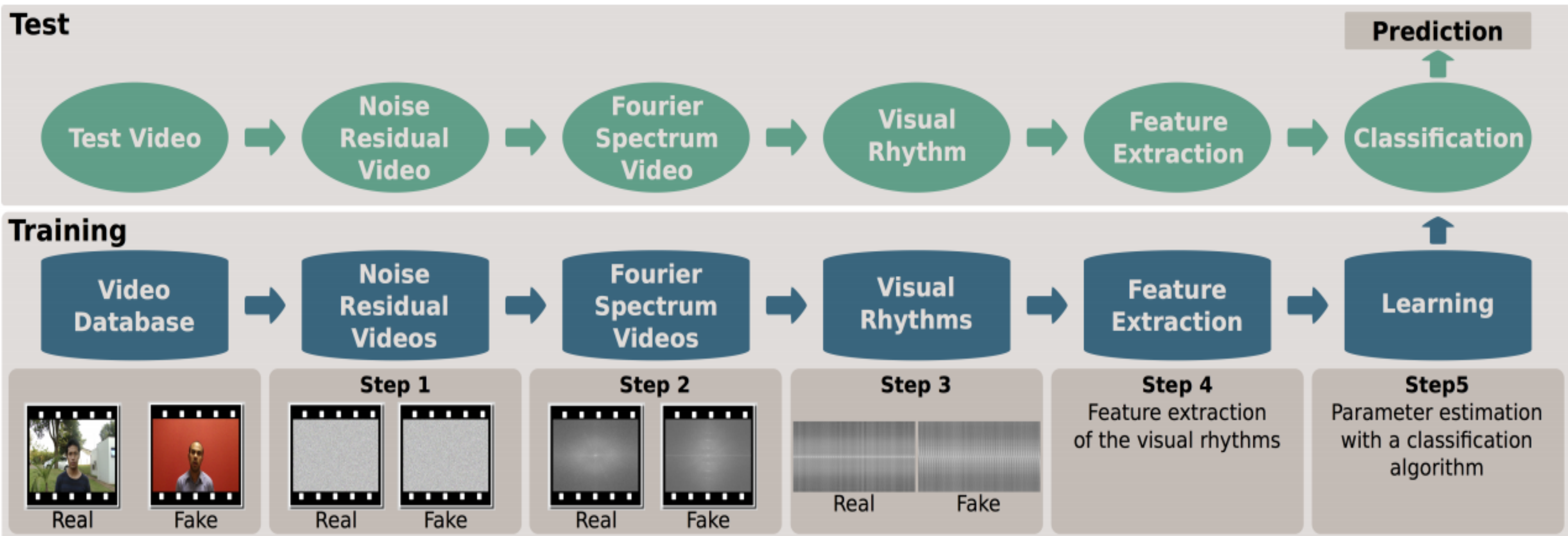
V_{RN}=V-h(V)
(h is the Gaussian filter)

$|F(u,v)| = \sqrt{R(u,v)^2 + I(u,v)^2}$
$V_{FS} = \log(1 + |F(u,v)|)$
(R and I are real and imaginary parts of the Fourier transform)

Using Visual Rhythms for Detecting Video-Based Facial Spoof Attacks

[Pinto, Schwartz, Pedrini and Rocha, TIFS, 2015]

- Propose a video based face spoofing detection scheme by utilizing the temporal info
- Employ Fourier analysis of noise signature to extract features based on visual rhythms
- The classification accuracy 14.27% (HTER) is achieved for Replay-Attack Database



Framework of the anti-spoofing scheme with Fourier spectrum of noise residual signal (source: Ref [6]).

Face Spoofing Detection Through Visual Codebooks of Spectral Temporal Cubes

[Pinto, Pedrini, Schwartz and Rocha, TIP, 2015]

- Features
  - Noise signature extraction
    - Subtracting original image with the blurred version
  - Fourier Spectrum
    - Calculating the Fourier magnitude and phase spectrum of the noise signature video
  - Time-Spectral descriptor
    - Intra: energy and entropy
    - Inter: correlation and mutual information
  - Mid level description
    - Bag of words
      - Selection of the visual words: random selection and clustering based selection
      - Visual words coding: hard-assignment and soft-assignment
- Classifier
  - SVM

V_{RN}=V-h(V)
(h is the Gaussian filter)

$|F(u,v)| = \sqrt{R(u,v)^2 + I(u,v)^2}$

$V_{FS} = \log(1 + |F(u,v)|)$

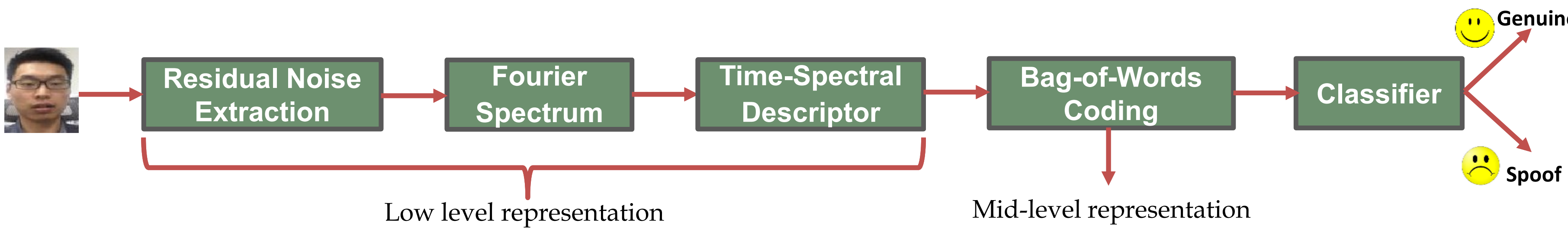
$V_{PS} = \arctan(\frac{I(u,v)}{R(u,v)})$

(R and I are real and imaginary parts of the Fourier transform)

Face Spoofing Detection Through Visual Codebooks of Spectral Temporal Cubes

[Pinto, Pedrini, Schwartz and Rocha, TIP, 2015]

- Combine low level and mid level features for face spoofing detection
- Temporal and spectral information are gathered
- An HTER of 2.75% and EER of 14.0% for Replay-attack and CASIA datasets



Framework of the visual codebook based face spoofing detection scheme.

The low-level representation of the videos is computed based on spectrum analysis of the noise signature

The mid-level representation of the videos is computed based on building the time-spectral visual words

Learn Convolutional Neural Network for Face Anti-Spoofing [Yang, Lei and Li, arXiv 2014]

- Pioneer method for deep learning based face spoofing
- Propose a CNN based face anti-spoofing pipeline

- CNN Architecture
  - AlexNet

- Training
  - Spatial data augmentation
    - Background regions are also contained
  - Temporal data augmentation
    - Multiple frames are fed into the network

- Classifier
  - Apply SVM on the last fully-connected layer

Achieved less than 5% HTER for CASIA & Replay-Attack datasets

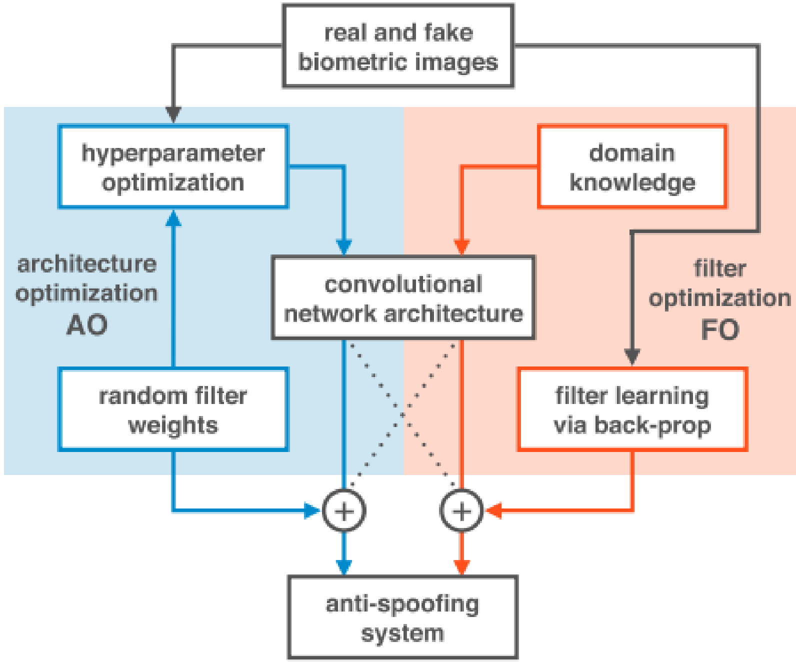
Deep Representations for Iris, Face, and Fingerprint Spoofing Detection

[Menotti, Chiachia, Pinto, Schwartz, Pedrini, Falcao and Rocha TIFS-2015]

- Propose a spoof-net for iris, face and finger print spoofing
- Propose the architecture optimization and filter optimization schemes
- 0.75% HTER for Replay-attack database

AO: determine the network structure based on existing structure and domain knowledge (spoofnet)

FO: determine the filter parameters based on backward propagation



Deep learning based scheme for spoofing detection (source: Ref [8])

Person-Specific Face Antispoofing With Subject Domain Adaptation [Yang, Lei, Yi and Li, TIFS 2015]

- Subject domain adaptation

  Given two subjects *a* and *b*
  - Establishing the relationship between two subject domains
  - Synthesize the fake features for target domain with the relationship
  - For each subject, train a classifier
- Features
  - MS-LBP (Multiscale-LBP)
  - HOG (Histogram of Gradient)
- Face spoofing
  - Face recognition to detect the face and classifier
  - Spoofing detection with the classifier of the subject
- Classifier
  - SVM (linear)
- Limitations
  - Assumptions in person specific transformation
  - Requires identical acquisition environment for source and target domains

$G_b = H_{ab} G_a + T_{ab}$ $F_b = H_{ab} F_a + T_{ab}$

H: Transformation matrix

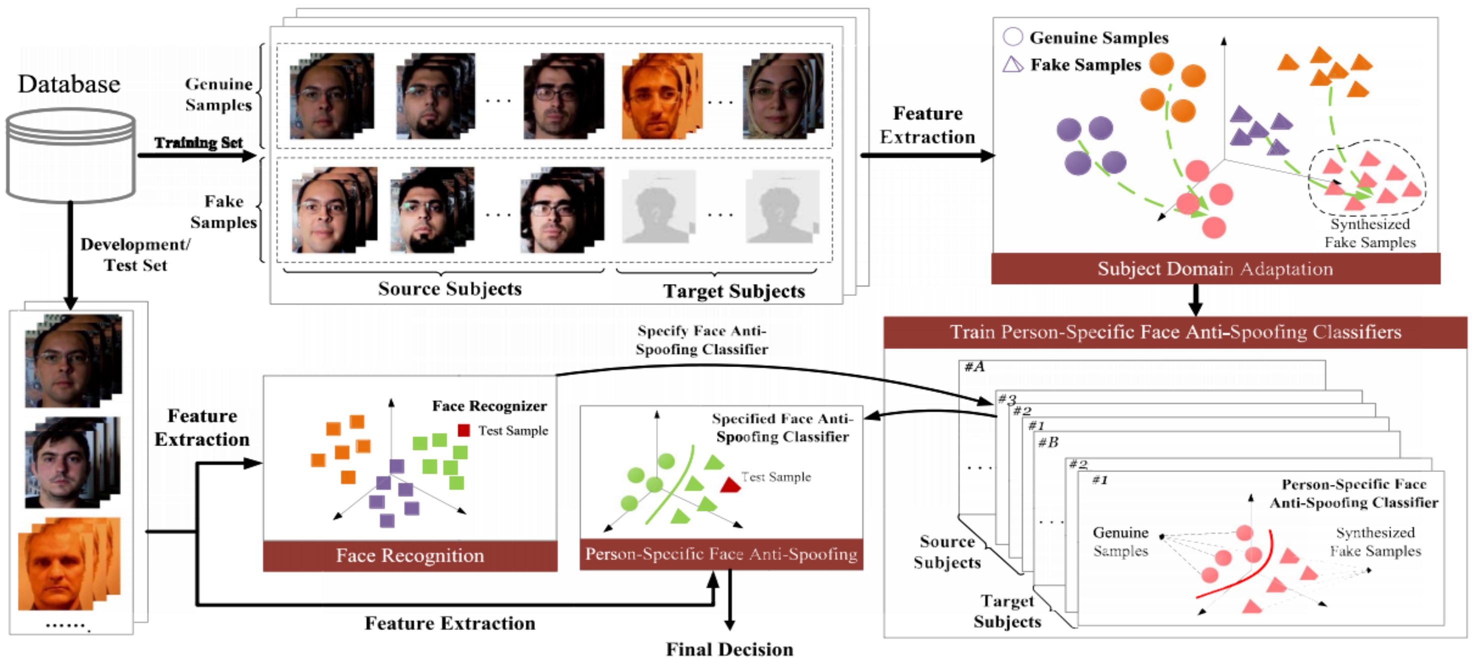
T: Bias matrix

G: Genuine features

F: Fake features

Person-Specific Face Antispoofing With Subject Domain Adaptation [Yang, Lei, Yi and Li, TIFS, 2015]

- Motivation
  - The genuine samples of one subject overlap the fake samples of another subject
  - The relationship between two genuine is similar to that between two fake samples

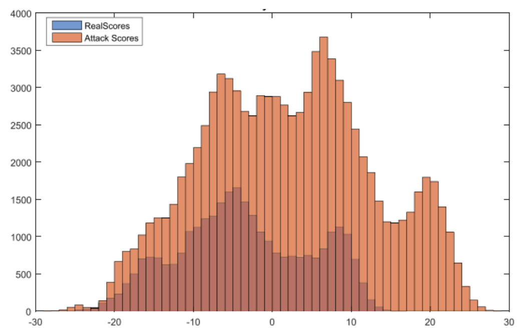


Person-Specific Face Anti-spoofing framework (source: [9])

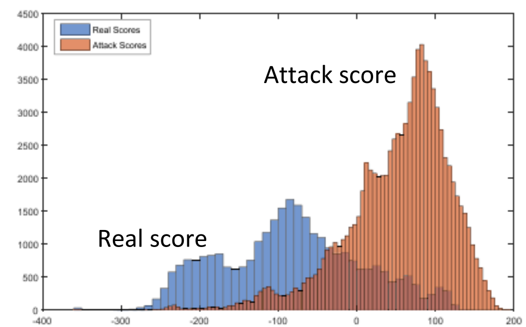
Face Spoofing Detection Using Colour Texture Analysis

[Boulkenafet, Komulainen and Hadid, TIFS 2016]

- Consider colour space info being affected in face spoofing detection
- Five features: **LBP**, COALBP, LPQ, BSIF, SID
- Significant performance improvement for intra-database (EER: from 0 to 3.5 % for Replay-Attack, CASIA, MSU databases)



Gray Scale



Cb Channel

$d(H_X, H_G, H_F) =$
$d_{\chi 2}(H_X, H_G) - d_{\chi 2}(H_X, H_F)$

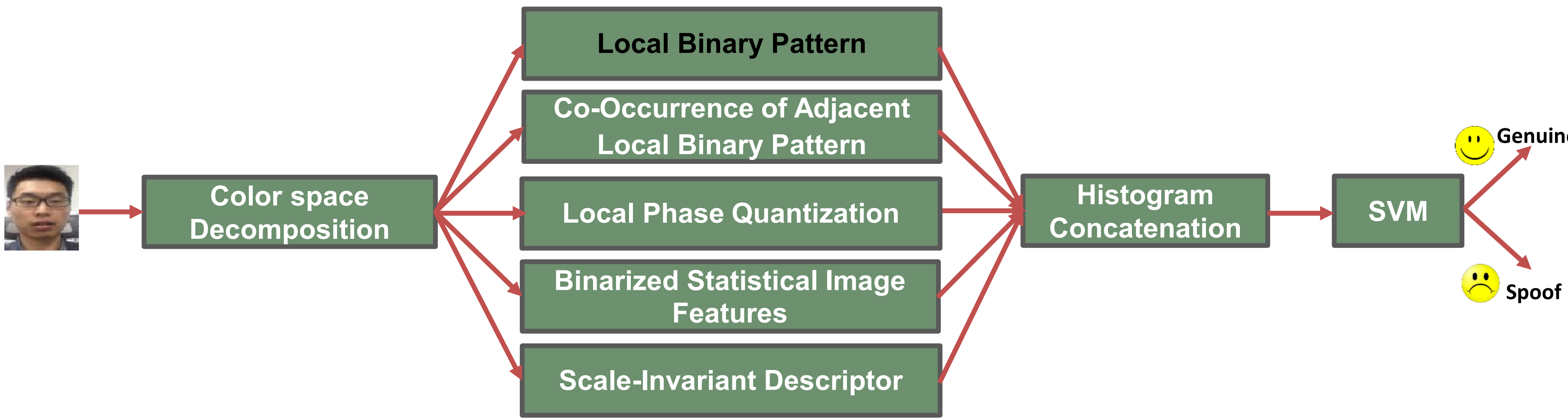
H_X, H_G, H_F: Histograms of test, genuine and fake samples

$d_{\chi 2}$: Chi – square distance

The distribution of the real and attack scores on the Replay-Attack Database (source: Ref [1]).
Left: gray scale (overlapped); Right: color channel (better separated)

Face Spoofing Detection Using Colour Texture Analysis

[Boulkenafet, Komulainen and Hadid, TIFS 2016]



Framework of the face anti-spoofing scheme with five colour texture features (LBP, COALBP, LPQ, BSIF, SID)

Color spaces: YCbCr (Y: Luma, Cb: blue-difference, Cr: red-difference)
HSV (hue-saturation-value)
RGB (red, green, blue)
Combination of YCbCr and HSV can achieve the best performance

Face Anti-spoofing Using Speed-Up Robust Features and Fisher Vector Encoding

[Boulkenafet, Komulainen and Hadid, SPL 2017]

- Features
  - SURF descriptor
    - Based on the sum of Haar wavelet around point of interest
    - Provides robust description of the texture with fast computation speed

$$V_j = [\sum d_x, \sum d_y, \sum |d_x|, \sum |d_y|]$$

$$\text{SURF} = [V_1, \dots, V_{16}]$$

d_x, d_y: Haar wavelet responses

  - Fisher Vector
    - The local SURF features are aggregated to Fisher Vector
    - Provides summary of the image based on the GMM

$$\phi_k^1 = \frac{1}{T\sqrt{w_k}} \sum_{t=1}^{T} \alpha_t(k) \left(\frac{x_t - \mu_k}{\sigma_k}\right)$$

$$\phi_k^2 = \frac{1}{T\sqrt{2w_k}} \sum_{t=1}^{T} \alpha_t(k) [\frac{(x_t - \mu_k)^2}{\sigma_k^2} \text{ -1}]$$

Input:

$\omega_k, \mu_k, \sigma_k$: GMM mode parameters

x_k: SURF feature

$\alpha_t(k)$: Soft assignment weight in GMM

T: The number of features

Output:

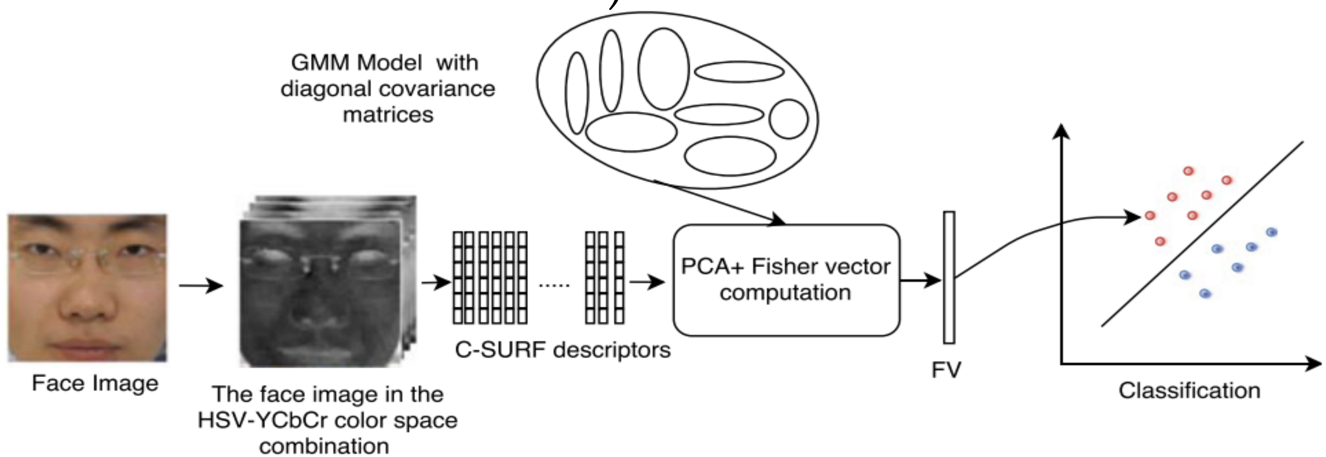
The Fisher Vector ϕ_k^1 and ϕ_k^2

- Classifier
  - Softmax classifier with cross entropy loss

Face Anti-spoofing Using Speed-Up Robust Features and Fisher Vector Encoding

[Boulkenafet, Komulainen and Hadid, SPL 2017]

- A texture based approach with SURF and FV for spoofing detection
- Strong generation ability to unseen attacks
- **Cross-database performance improvement** (19.1% to 31.8% HTER for cross-database evaluation)

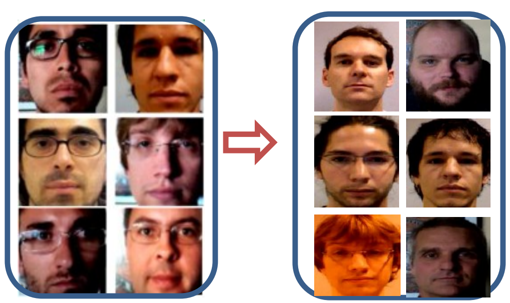


Framework of the face anti-spoofing scheme with SURF and FV (source: Ref [2])
HSV-YCbCr color space achieves the best performance

Unsupervised domain adaptation for face anti-spoofing

Current Research Status and Motivation

- Both hand-crafted features (e.g. Color Texture) and CNN based methods can achieve very good performance when training data and testing are coming from the same ‘domain’.
- When the training data and testing are captured from different domains, the detection ability suffers from a large performance drop.
- It is impossible to capture training data under all conditions.



Intra-database

Unknown-database

Problem Definition

- How can we train a more robust classifier based on training data with labeled information and testing data without label information?
  - e. g. Training samples are captured by several types of camera model, but testing samples are captured by the models which are not the same as the training ones.

Mobile phones for training

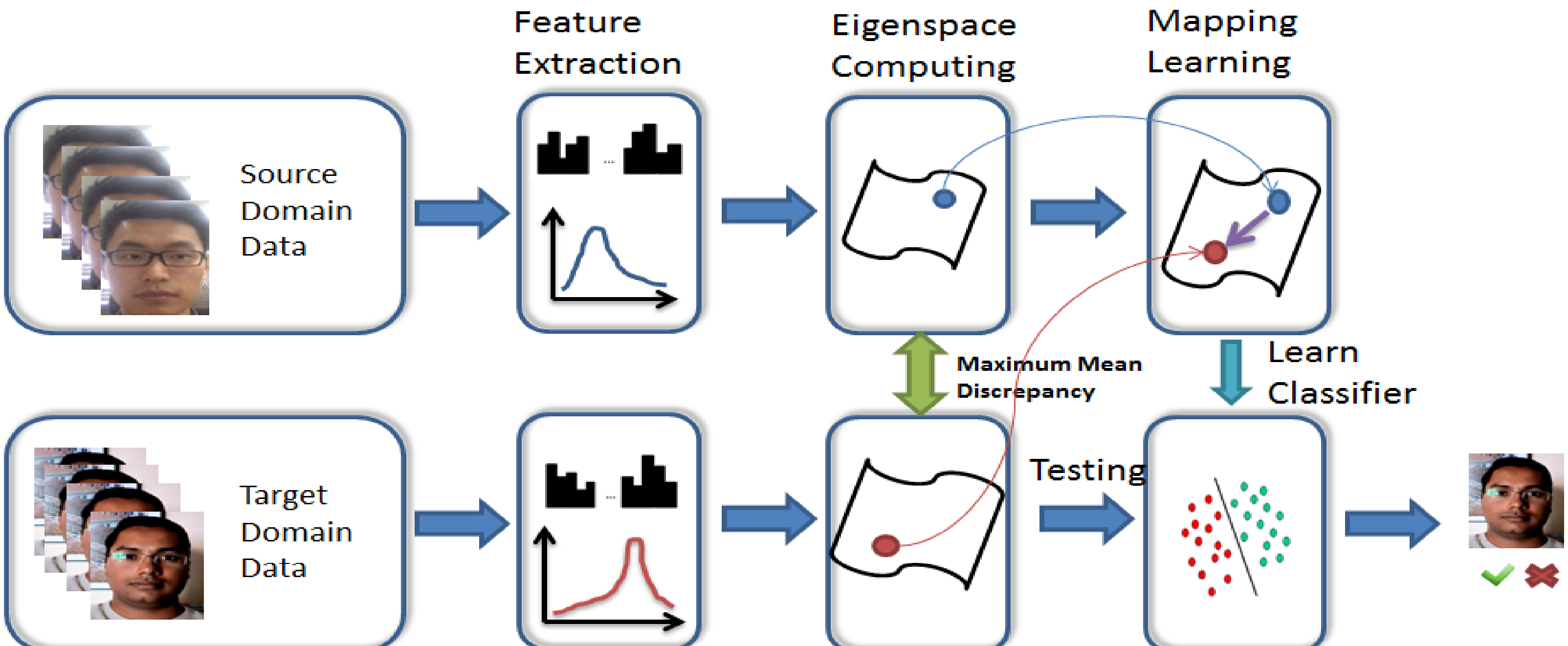
Mobile phones for testing

Motivation

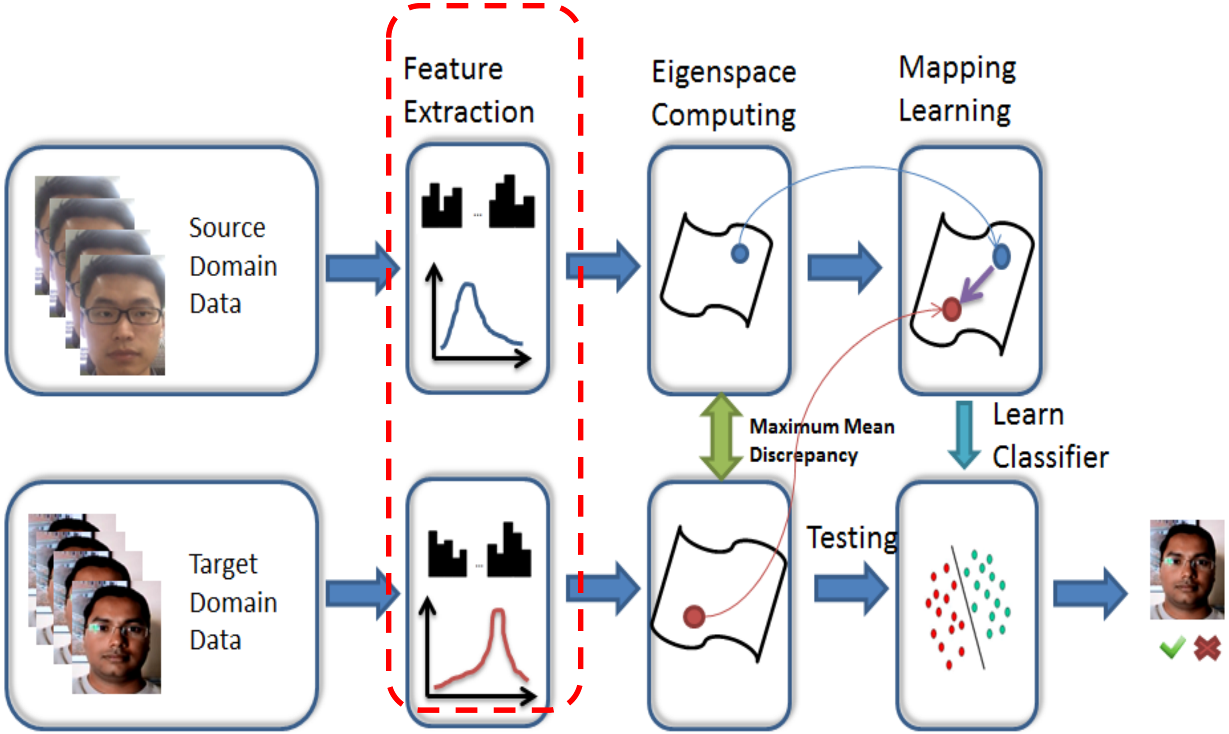
- Training data and Testing data have different distributions. A classifier trained on training data can not be generalized to testing data.
- By mapping the training data to a new space, we expect that the distribution of training and testing data are more similar.
- What are we going to do
  - How to model the distribution based on a specific problem (face anti-spoofing)?
  - How to reduce the distribution dissimilarity thus a more robust classifier can be trained?

Approach: unsupervised domain adaptation framework

The generalization and adaptation ability of state-of-the-art features are analyzed.

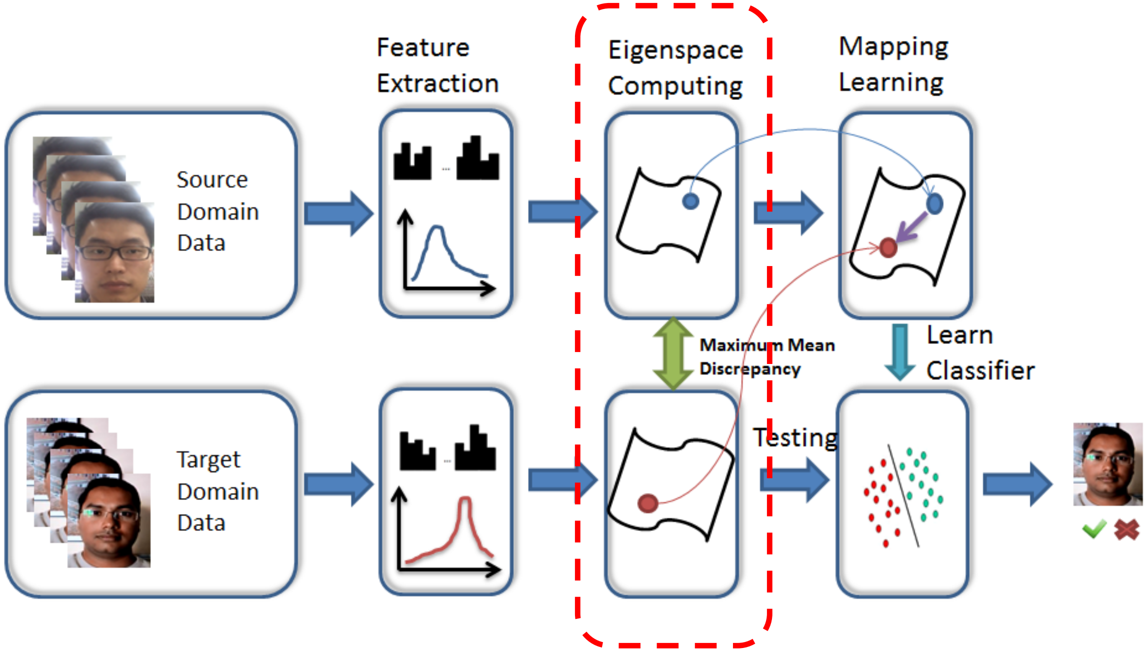


Framework



- Feature Extraction
  - Multiscale Wavelet
  - CoALBP(HSV, YCbCr)
  - LPQ (HSV, YCbCr)

Framework



- Eigenspace Computing: Noise factors can be modeled in low-dimension linear subspace
  - Facial Appearance
  - Illumination

$$\phi : \hat{\mathbf{X}}_s \Rightarrow \mathbf{U}_s, \quad \mathbf{X}_t \Rightarrow \mathbf{U}_t$$

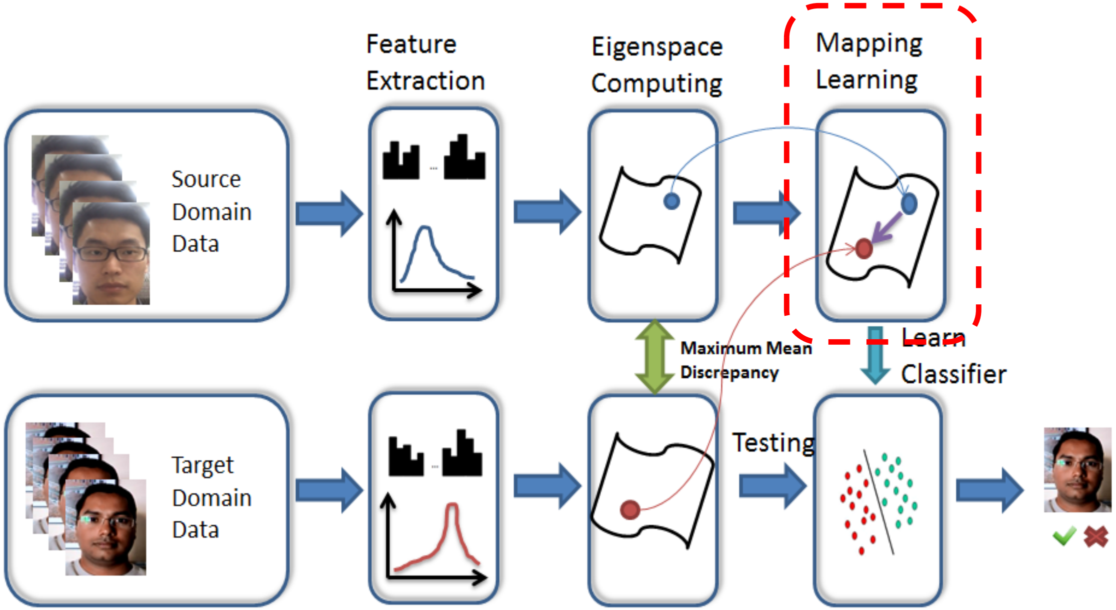
$$\mathbf{U}_s = \arg\max_{\|\mathbf{U}\|=1} \{\mathbf{U}^T \hat{\mathbf{X}}_s^T \hat{\mathbf{X}}_s \mathbf{U}\}$$

$$\mathbf{U}_t = \arg\max_{\|\mathbf{U}\|=1} \{\mathbf{U}^T \mathbf{X}_t^T \mathbf{X}_t \mathbf{U}\}$$

- Maximum Mean Discrepancy Measurement:

$$D(\hat{\mathbf{X}}_s, \mathbf{X}_t) = \|\mathbf{U}_s - \mathbf{U}_t\|_F^2$$

Framework

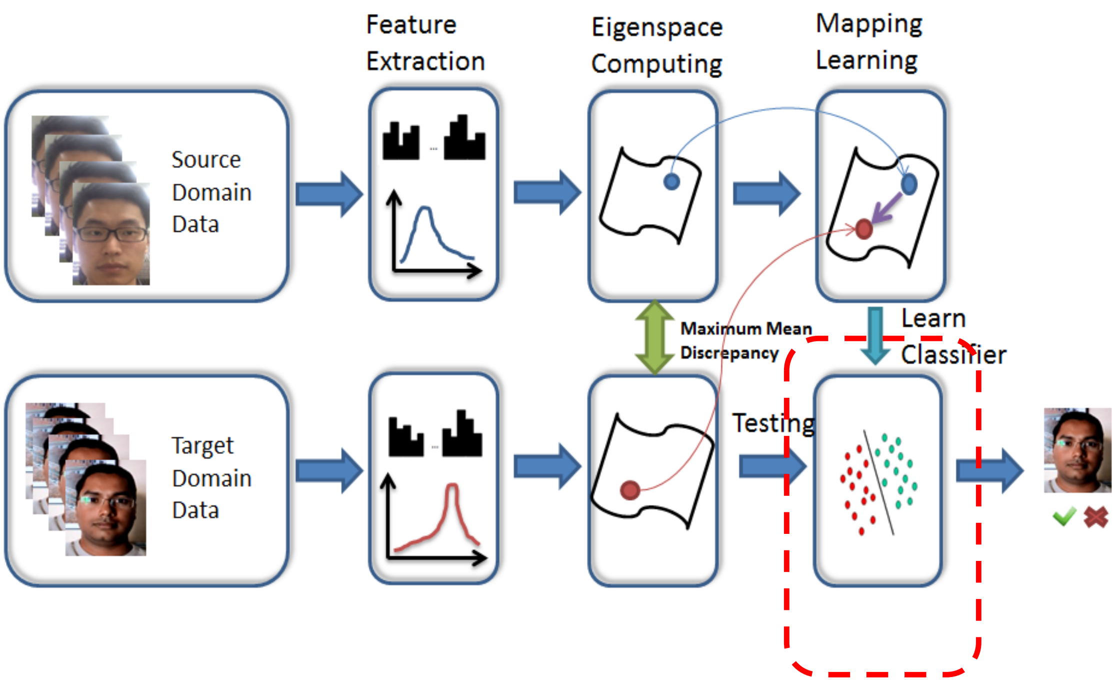


Mapping (Subspace Alignment):

$$\mathbf{M}^* = \mathrm{argmin}_{\mathbf{M}} \|\mathbf{U}_s\mathbf{M} - \mathbf{U}_t\|_F^2$$

$$\mathbf{M} = \mathbf{U}_s^T \mathbf{U}_t$$

Framework



Classifier: Support Vector Machine

Training Kernel:

$$\mathbf{K}_{ss} = \hat{\mathbf{X}}_s \mathbf{U}_s \mathbf{U}_s^T \mathbf{U}_t \mathbf{U}_t^T \mathbf{U}_s \mathbf{U}_s^T \hat{\mathbf{X}}_s^T$$

Testing Kernel:

$$\mathbf{K}_{st} = \hat{\mathbf{X}}_s \mathbf{U}_s \mathbf{U}_s^T \mathbf{U}_t \mathbf{U}_t^T \mathbf{X}_t^T$$

Experiment Setting

- Features:
  - Multiscale Wavelet (mean and deviation of Wavelet Subbands in different scale) [1]
  - Co-occurace of Adjacent Local Binary Pattern (CoALBP) in HSV and YCbCr space [2]
  - Local Phase Quantization (LPQ) in HSV and YCbCr space [3]
- Database:
  - Idiap REPLAY-ATTACK (I) [4]
  - CASIA Face AntiSpoofing (C) [5]
  - MSU Mobile Face Spoofing (M) [6]
- Evaluation: Half Total Error Rate (HTER)

Results(submitted & under revision)

- C: CASIA database, I: Idiap REPLAY-ATTACK database, M: MSU mobile face spoofing database
- A → B: Training on 'A' and evaluating on 'B'

Method		C → I	C → M	I → C	I → M	M → C	M → I
Wavelet	W/O DA	49.9%	49.2%	47.7%	48.6%	49.1%	50.0%
	DA	33.1%	19.1%	32.1%	31.3%	41.2%	35.1%
CoALBP (HSV)	W/O DA	50.3%	24.9%	50.0%	50.0%	50.0%	50.0%
	DA	33.4%	20.9%	33.2%	29.0%	34.2%	30.6%
CoALBP (YCbCr)	W/O DA	50.0%	15.1%	50.1%	50.0%	44.8%	50.0%
	DA	35.1%	**14.9%**	34.5%	29.0%	34.2%	36.9%
LPQ (HSV)	W/O DA	45.5%	54.9%	43.7%	53.5%	58.7%	59.1%
	DA	33.4%	21.2%	39.0%	24.9%	39.8%	33.2%
LPQ (YCbCr)	W/O DA	43.9%	44.3%	49.9%	46.2%	46.8%	50.0%
	DA	40.7%	16.3%	33.1%	27.8%	33.3%	31.8%

Thank You

References

[1] Zinelabidine Boulkenafet, Jukka Komulainen, Abdenour Hadid, Face Spoofing Detection Using Colour Texture Analysis. IEEE Trans. Information Forensics and Security 11(8): 1818-1830 (2016)

[2] Zinelabidine Boulkenafet, Jukka Komulainen, Abdenour Hadid, Face Antispoofing Using Speeded-Up Robust Features and Fisher Vector Encoding. IEEE Signal Process. Lett. 24(2): 141-145 (2017)

[3] Keyurkumar Patel, Hu Han, Anil K. Jain, Secure Face Unlock: Spoof Detection on Smartphones. IEEE Trans. Information Forensics and Security, 11(10), 2268-2283 (2016)

[4] Di Wen, Hu Han, Anil K. Jain, Face Spoof Detection With Image Distortion Analysis. IEEE Trans. Information Forensics and Security 10(4): 746-761 (2015)

[5] Javier Galbally, Sébastien Marcel, Julian Fiérrez, Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition. IEEE Trans. Image Processing 23(2): 710-724 (2014)

[6] Allan da Silva Pinto, William Robson Schwartz, Hélio Pedrini, Anderson de Rezende Rocha, Using Visual Rhythms for Detecting Video-Based Facial Spoof Attacks. IEEE Trans. Information Forensics and Security 10(5): 1025-1038 (2015)

References

[7] Allan da Silva Pinto, Hélio Pedrini, William Robson Schwartz, Anderson Rocha, Face Spoofing Detection Through Visual Codebooks of Spectral Temporal Cubes. IEEE Trans. Image Processing 24(12): 4726-4740 (2015)

[8] David Menotti, Giovani Chiachia, Allan da Silva Pinto, William Robson Schwartz, Hélio Pedrini, Alexandre Xavier Falcão, Anderson Rocha, Deep Representations for Iris, Face, and Fingerprint Spoofing Detection. IEEE Trans. Information Forensics and Security 10(4): 864-879 (2015)

[9] Jianwei Yang, Zhen Lei, Dong Yi, Stan Z. Li, Person-Specific Face Antispoofing With Subject Domain Adaptation. IEEE Trans. Information Forensics and Security 10(4): 797-809 (2015)

[10] Jianwei Yang, Zhen Lei, Stan Z. Li, Learn Convolutional Neural Network for Face Anti-Spoofing. CoRR abs/1408.5601 (2014)

[11] Ivana Chingovska, André Anjos, Sébastien Marcel: On the effectiveness of local binary patterns in face anti-spoofing. BIOSIG 2012: 1-7

[12] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in International Conference on Biometrics (ICB). IEEE, 2012, pp. 26–31.

Reference

[1] H. Cao and A. C. Kot, “Identification of recaptured photographs on LCD screens,” in IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP). IEEE, 2010, pp. 1790–1793.

[2] R. Nosaka, Y. Ohkawa, and K. Fukui, “Feature extraction based on co-occurrence of adjacent local binary patterns,” in Pacific-Rim Symposium on Image and Video Technology. Springer, 2011, pp. 82–91.

[3] V. Ojansivu and J. Heikkil¨a, “Blur insensitive texture classification using local phase quantization,” in International conference on Image and Signal Processing. Springer, 2008, pp. 236–243.

[4] I. Chingovska, A. Anjos, and S. Marcel, “On the effectiveness of local binary patterns in face anti-spoofing,” in International Conference of the Biometrics Special Interest Group (BIOSIG). IEEE, 2012, pp. 1–7.

[5] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, “A face antispoofing database with diverse attacks,” in International Conference on Biometrics (ICB). IEEE, 2012, pp. 26–31.

[6] D. Wen, H. Han, and A. K. Jain, “Face spoof detection with image distortion analysis,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 746–761, Apr 2015.

Validation Protocols

- Criterions
  - Receiver operating characteristic (ROC)
  - Half total error rate (HTER)
  - Equal error rate (EER)
  - Computational complexity (frame rate)

- Testing Protocols
  - Intra database
  - Cross(Inter) database

Backup Slide

- When a threshold is given, Half Total Error Rate is computed as the average of FAR and FRR.
- For face anti-spoofing problem, after training a classifier on training set, we first compute the threshold which minimize Equal Error Rate (EER) on development set

$$\tau^*_{\mathrm{EER}_\omega} = \arg\min_{\tau} |\mathrm{FAR}_\omega(\tau, \mathscr{D}_{\mathrm{dev}}) - \mathrm{FRR}(\tau, \mathscr{D}_{\mathrm{dev}})|$$

- Then, we can use the threshold to compute the HTER on Testing set

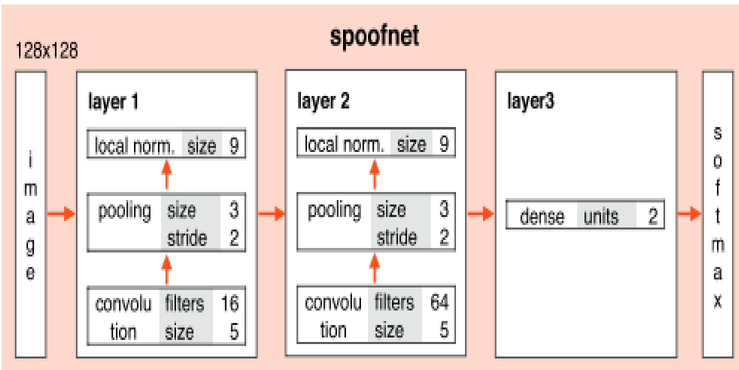
$$\mathrm{HTER}(\tau, \mathscr{D}_{\mathrm{test}}) = \frac{\mathrm{FPR}(\tau, \mathscr{D}_{\mathrm{test}}) + \mathrm{FNR}(\tau, \mathscr{D}_{\mathrm{test}})}{2} \quad [\%]$$

- Marcel, Sébastien, Mark S. Nixon, and Stan Z. Li. *Handbook of Biometric Anti-Spoofing*. Vol. 1. New York: Springer, 2014.

Deep Representations for Iris, Face, and Fingerprint Spoofing Detection

[Menotti, Chiachia, Pinto, Schwartz, Pedrini, Falcao and Rocha TIFS-2015]

Architecture of CNN (source: [8])

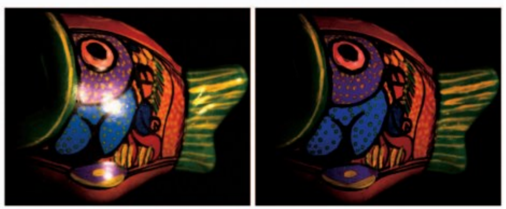


- Architecture optimization
  - Incorporate the domain knowledge and CF10-11 neural network structure
  - Two convolutional layers and one fully connected layer
- Filter optimization
  - Back propagation
  - Data augmentation is performed for training
- Limitation
  - Deep learning may easily cause overfitting

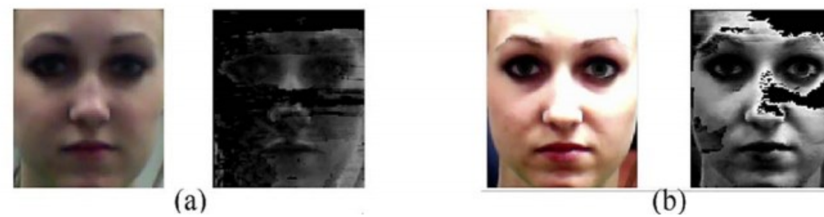
Pooling: aggregating activations from the filter in a given region.
Local normalization: normalize the output feature based on the local feature energy

Specular Reflection (Backup Slides for TIFS2015)

- Specular Reflection
  - The immediately reflected light rays are called specular or interface reflections, while those that have penetrated and then reflected back into the air are called diffuse or body reflections. [Tan and Ikeuchi, 2005, TPAMI]



Left: Textured input image,
Right: Specular-free image
(source: [Tan and Ikeuchi, 2005])



Left: genuine face and specular reflection component
Right: fake face and specular reflection component
(source: Ref [4])

[Tan and Ikeuchi, 2005, TPAMI] Separating Reflection Components of Textured Surfaces Using a Single Image