Face Recognition System Security: Template Protection and Anti-spoofing

Pong C Yuen
Head and Professor
Department of Computer Science
Hong Kong Baptist University

IAPR/IEEE Winter School on Biometrics 9-13 Jan 2017

Collaborators…

- Anil Jain, Michigan State University

- YC Feng, Hong Kong Baptist University
- MH Lim, Hong Kong Baptist University
- GC Mai, Hong Kong Baptist University
- SQ Liu, Hong Kong Baptist University

- GY Zhou, University of Oulu
- XB Li, University of Oulu

Outline

1. Background and Motivations
2. Face Template Protection
3. Face Anti-spoofing
4. Conclusions

Background and Motivations

- Face Recognition
  - The most intrinsic biometric authentication, active research topic & widely used in industrial applications

Automated Passenger Clearance System (Immigration Dept.)

Unlock phone

face-recognition payment Alipay

Source: china.com and iomniscient.com

Background and Motivations

- Re-visit face recognition procedure

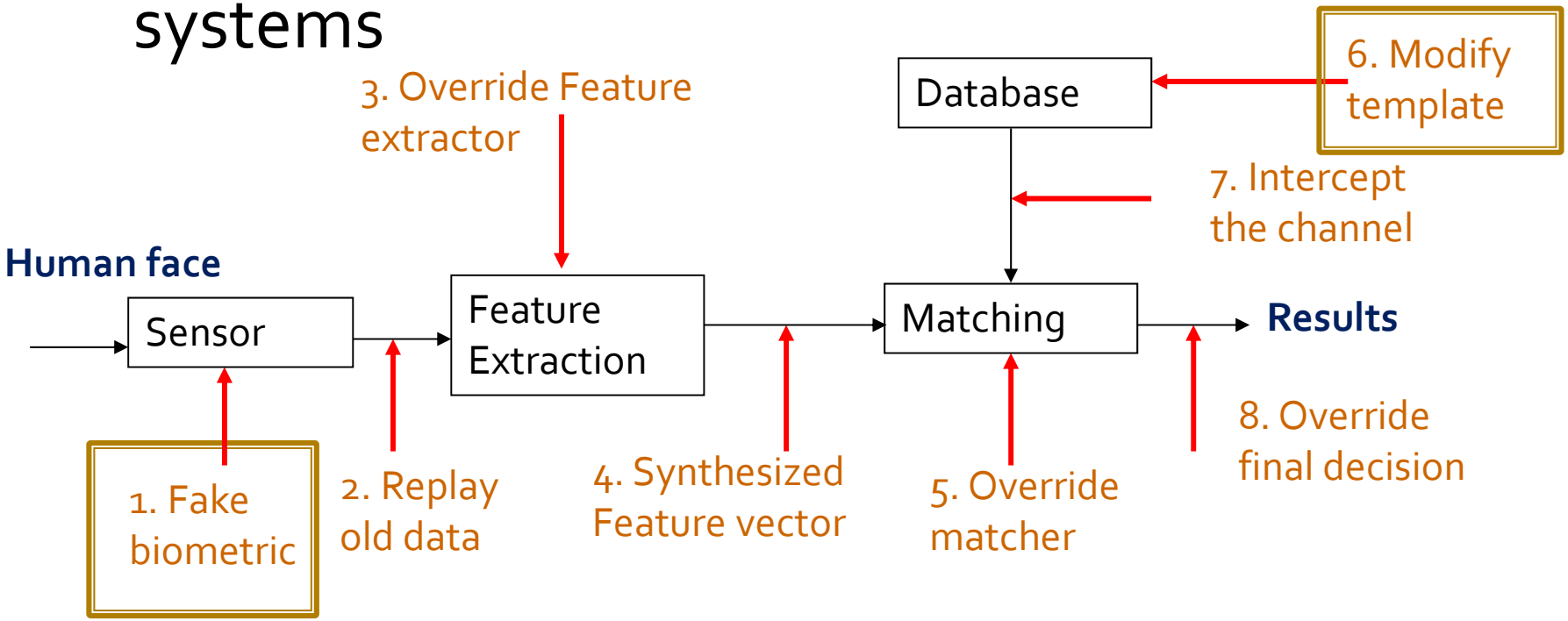
Courtesy of Ms. Xiaobai Li

Background and Motivations

What happens if
the face recognition system is NOT secure?

Background and Motivations

- Vulnerabilities: Ratha *et al*. [IBM Sys J 2001] pointed out eight possible attacks on biometric systems



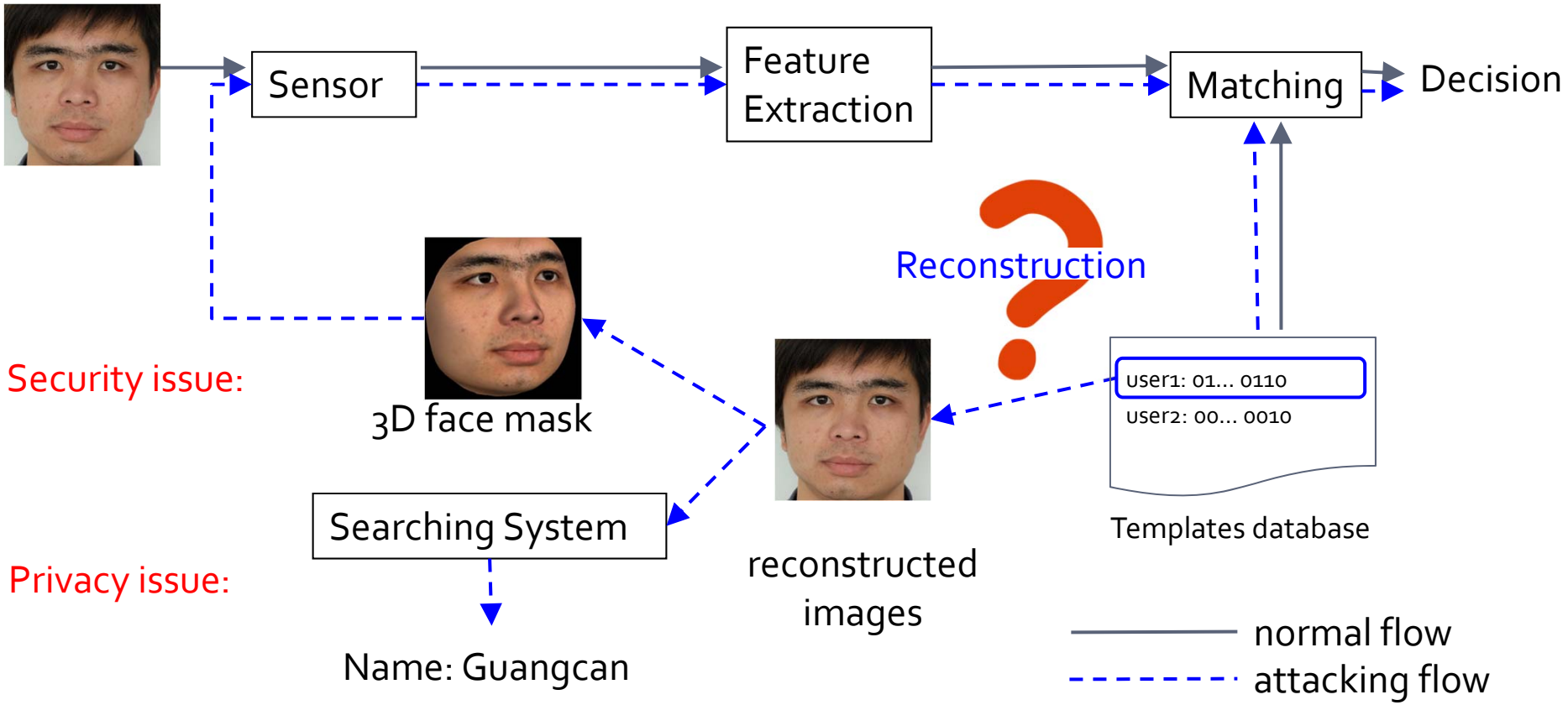
Part I:
Face Template Protection

Outline: Face Template Protection

1. Can we reconstruct a fake face from templates?
2. Review on existing techniques in protecting face templates
3. Our work
   a. Hybrid approach
   b. Binary Discriminative Analysis for binary template generation
   c. Binary template fusion for multi-biometric cryptosystems
   d. Entropy measurement for biometric verification systems

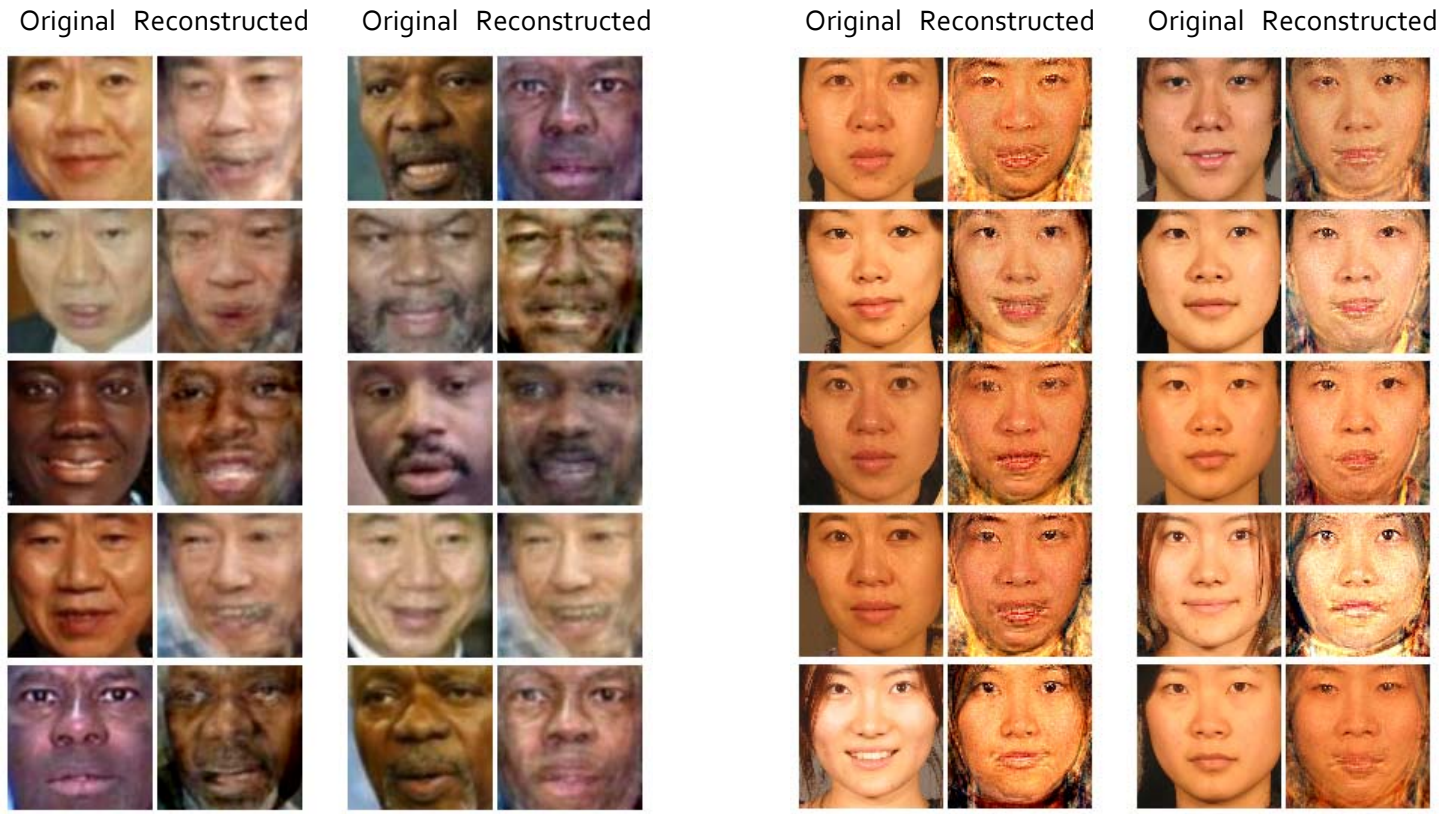
Can we reconstruct a fake face from templates?

Image Reconstruction Attack



Sample Reconstructed Faces using RBF Regression [1]

- Feature extractor [2], an implementation of FaceNet [3]

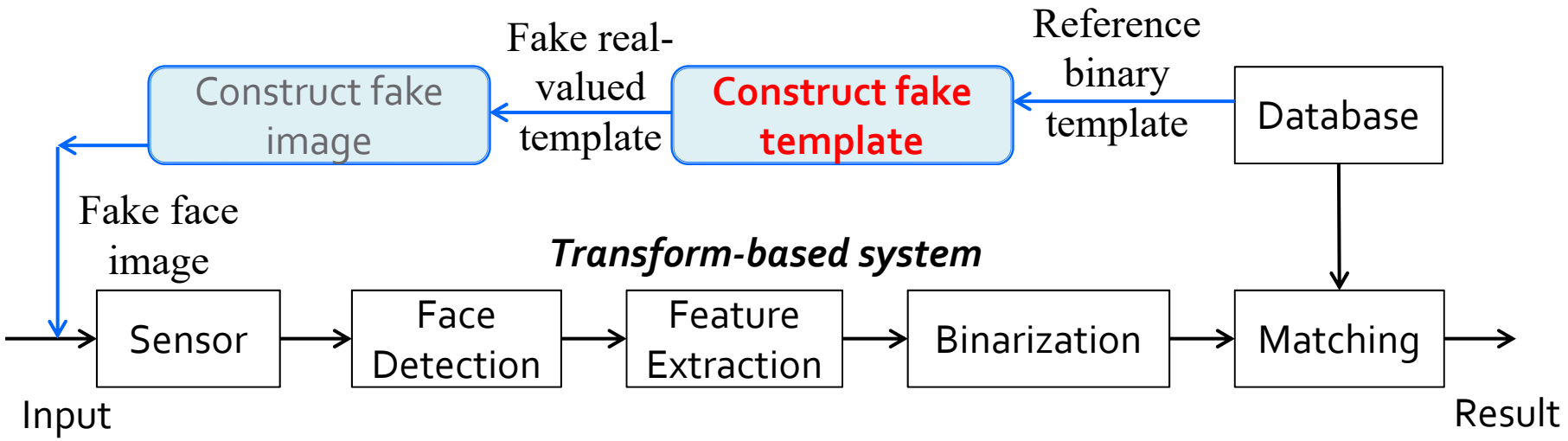


(a) LFW (b) FRGC V2.0

1. Mignon, Alexis, and Frédéric Jurie. "Reconstructing Faces from their Signatures using RBF Regression." BMVC2013
2. Brandon Amos et al, “OpenFace: Face Recognition with Deep Neural Networks”, [URL]
3. Schroff, Florian et al. "Facenet: A unified embedding for face recognition and clustering." CVPR2015

From Binary Template to Face Image

- Is binary template secure?



Reference: Y C Feng, M H Lim and P C Yuen, Masquerade attack on transform-based binary-template protection based on perceptron learning, *Pattern Recognition*, 2014.

Security and Privacy Issues

- If a face template stored in database is compromised, it may cause security and privacy problems.

Modification/ Replacing	• Modify/replace the templates to the ones preferred by attackers
Uniqueness	• Since biometric is "unique" feature for individual, it is hard to reset or re-issue
Information Leakage	• May cause fake face attacks
Cross-platform matching	• Templates stolen from one system may be used to attack another system

Criteria for Generating Protected Template

Security	Discriminability	Cancelability
• Computationally hard to reconstruct the original template from the protected template.	• The discriminative power of the protected template should be as good as that of the original face template so that system performance will not be affected.	• The protected template can be canceled and re-issued from original template if it is stolen or lost.

Basic Idea

- General approach: *Never* store the original raw biometric template
- Straightforward method: Protection with traditional encryption/hashing methods (e.g. DES, MD5)
  - Small change in input cause large change in output
  - Intra-class variations => not good for matching
  - NOT feasible
- The template protection schemes can be classified into two categories [Jain *et al. EURASIP JASP* 2008]
  - *Biometric Cryptosystem*
  - *Transformation-based*

Review on Existing Techniques for Face Template Protection

Existing Techniques

Biometric Cryptosystem

- Encrypt the original templates with a helper data
- Apply error-correcting coding methods to handle intra-class variance
- Require input in finite fields

Transform-based

- Transform the original templates into a new domain
- Apply one-way transforms
- Cancelable
- High trade-off between discriminability and security

Biometric Cryptosystems

Key-binding

- The cryptographic key is independent from biometric data.
- ***Advantage***: Tolerance of intra-class variations
- ***Disadvantage***: Require finite field input & NOT for cancelability purpose

Key generation

- The cryptographic key is directly generated from the biometric data.
- ***Advantage***: Direct key generation
- ***Disadvantage***: Hard to generate secure and variance-tolerant key

Transform-based Approach

Non-invertible transform

- The transform is non-invertible.
- ***Advantage***: High security
- ***Disadvantage:*** Trade-off between security & discriminability

Salting

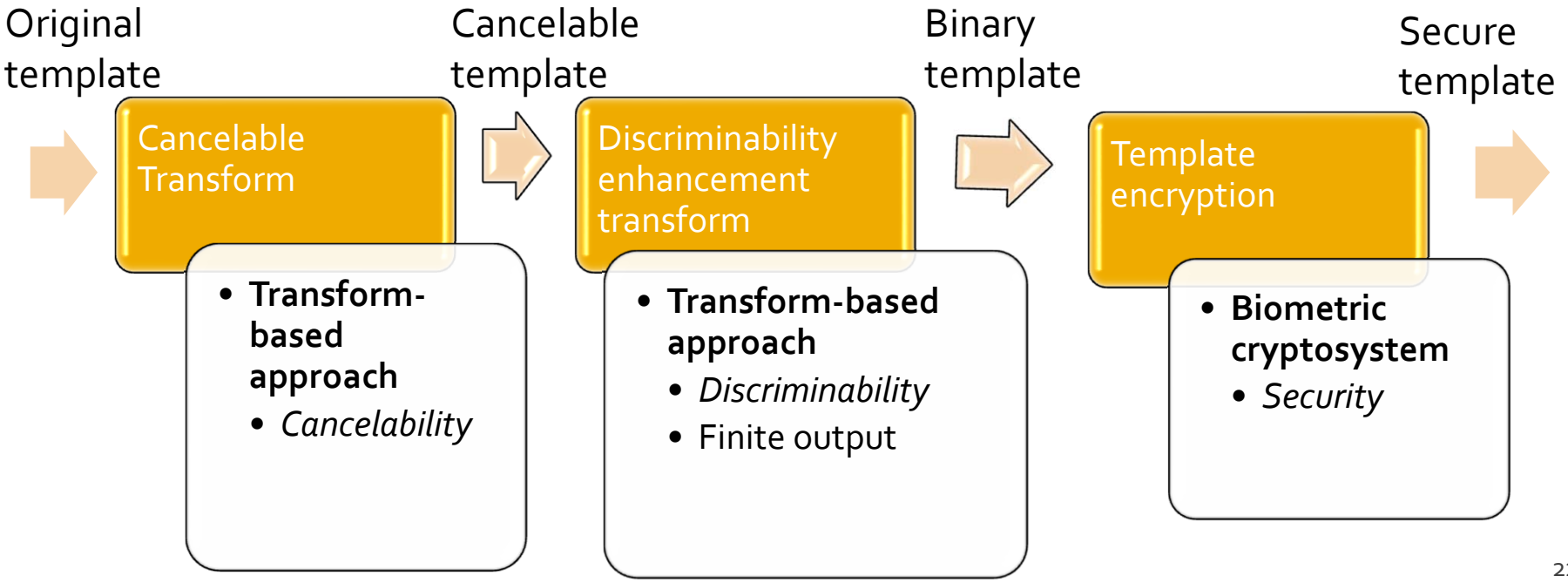
- A user-specific key is applied in transform to diverge the outputs, resulting in high performance
- ***Advantage***: Cancelable & High performance
- ***Disadvantage***: Unsecure user-specific key & invertible transform

Our Work

- Hybrid approach [TIFS 2010]
- Binary Discriminative Analaysis for binary template generation [TIFS 2012]
- Binary template fusion for multi-biometric cryptosystems [IVC 2017]
- Entropy measurement for binary template based system [IEEE TC 2016]

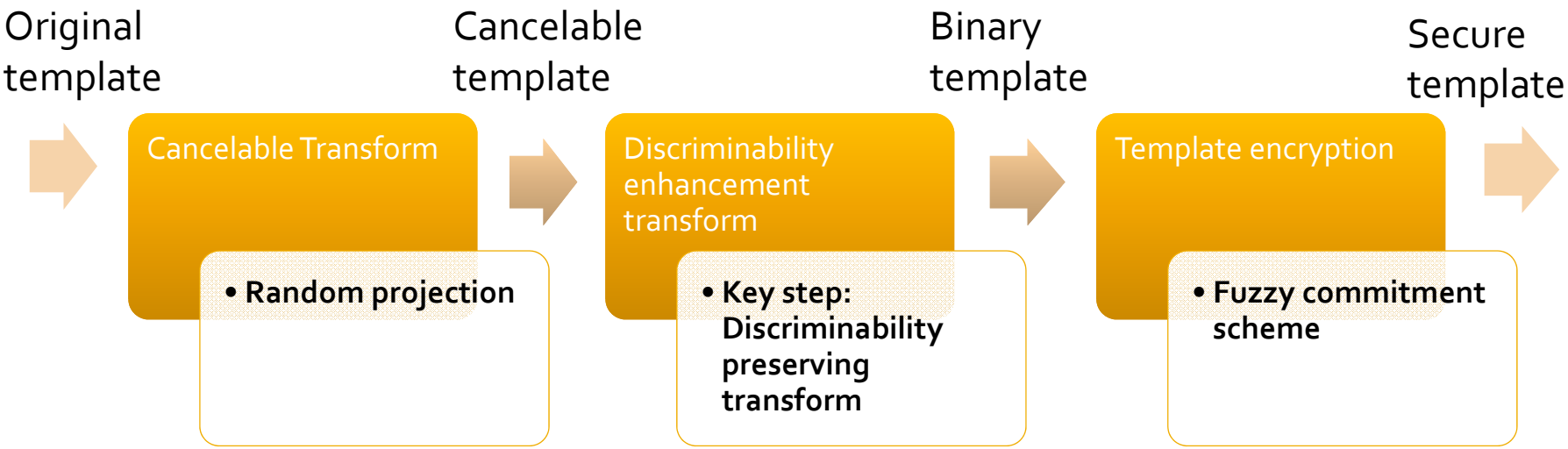
1. Proposed Hybrid Framework [TIFS 2010]

- One single approach cannot satisfy all security, discriminability and cancelability requirements
- A new hybrid approach: transformation-based biometric cryptosystem



3-step Algorithm

- The three-step hybrid algorithm



- The discriminability preserving transform should
  - convert the cancelable template into binary template
  - preserve the discriminability via transform.

Experimental Results

- Experiment settings:
  - Database:

c : No. of individuals.
m: No. of samples for each individual.
q : No. of training samples per individual

CMU PIE

FERET

FRGC

Database	c	m	q	Variations
CMU PIE	68	105	10	Illumination, pose, expression
FERET	250	4	2	Mild expression, illumination
FRGC	350	40	5	expression, illumination, mild pose

Experimental Results

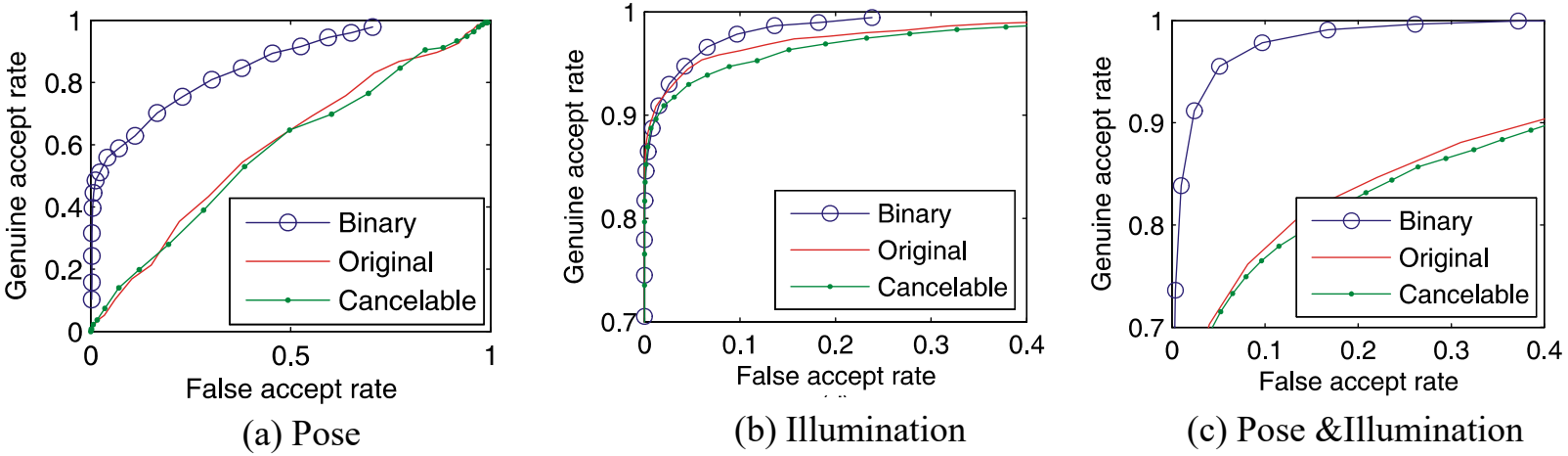
- Experiment settings
  - Fisherface [Belhumeur *et al.* PAMI 1997] applied for feature extraction
  - To evaluate
    - Template discriminability
    - Recognition accuracy
    - Cancelability

Template Discriminability

- Experimental settings
  - Choose three subsets from the CMU PIE database for experiments.
  - kr: length of the cancelable templates
  - kc: length of the binary templates

Database	c	m	q	kr	kc	Variations
CMU PIE-1	68	4	2	40	56	Pose
CMU PIE-2	250	21	4	40	84	Illumination
CMU PIE-3	350	105	10	40	210	Pose & illumination

Template Discriminability



- Observations
  - Cancelable templates slightly degrade some discriminability
  - Binary templates enhance discriminability.

=> The generated binary templates are discriminative

Recognition Accuracy

- Experimental settings
  - CMU PIE, FERET, FRGC databases used.

Database	c	m	q	kr	kc
CMU PIE	68	105	10	40	120, 150, 180, 210
FERET	250	4	2	150	120, 150, 180, 210
FRGC	350	40	5	250	150, 200, 250, 350

- Implement authentication with different kc. And comparing the performance with the
  - Original fisherface algorithm ("Original")
  - Random multispace quantization scheme ("RMQ-S") [Teoh *et al*. PAMI 2006]

Recognition Accuracy

- In the transformed-based scheme, keys can be issued in two ways.

- Experiments are done in two scenarios
  - Common key scenario
  - User-specified key scenario

Common-key Scenario

- Observation
  - The proposed hybrid algorithm outperforms the original fisherface and the RMQ algorithm

EER(%)	Fisherface	*kc*-1	*kc*-2	*kc*-3	*kc*-4	RMQ
CMU PIE	18.18	7.61	7.30	6.95	**6.81**	11.93
FERET	12.58	9.52	8.86	8.61	**8.55**	12.83
FRGC	31.75	17.93	17.40	16.70	**16.68**	21.87

User-specified Key Scenario

- Observation
  - The proposed hybrid algorithm outperforms the original fisherface and the RMQ algorithm

EER(%)	Fisherface	*kc*-1	*kc*-2	*kc*-3	*kc*-4	RMQ
CMU PIE	18.18	9.41	8.41	8.70	**8.26**	11.68
FERET	21.66	3.38	3.36	3.34	**3.62**	4.49
FRGC	31.75	9.03	9.18	9.08	**9.13**	11.03

2. Binary Template Generation [TIFS 2012]

- The discriminability of the binary templates is the key for hybrid approach
- Existing schemes lack of discriminability evaluations of the binary templates
- Traditional discriminability optimization methods are not effective
  - Employ differentiation
  - Differentiation is not feasible in Hamming space
- Propose a **binary discriminant analysis [1]** to optimize the discriminability of the binary templates

[1] Y C Feng and P C Yuen, "Binary Discriminant Analysis for Generating Binary Face Template," *IEEE Transactions on Information Forensics and Security, vol.* 7, no. 2, pp.613-624, 2012.

Rationale

- Use a series of linear discriminant functions (LDF) to form a binary template $\mathrm{b}=(b_1,b_2\ldots b_i\ldots b_k)$ from input sample x.

$$b_i(x) = \begin{cases} 0 & \text{if } w_i^T x + t_i > 0 \\ 1 & \text{else} \end{cases}$$

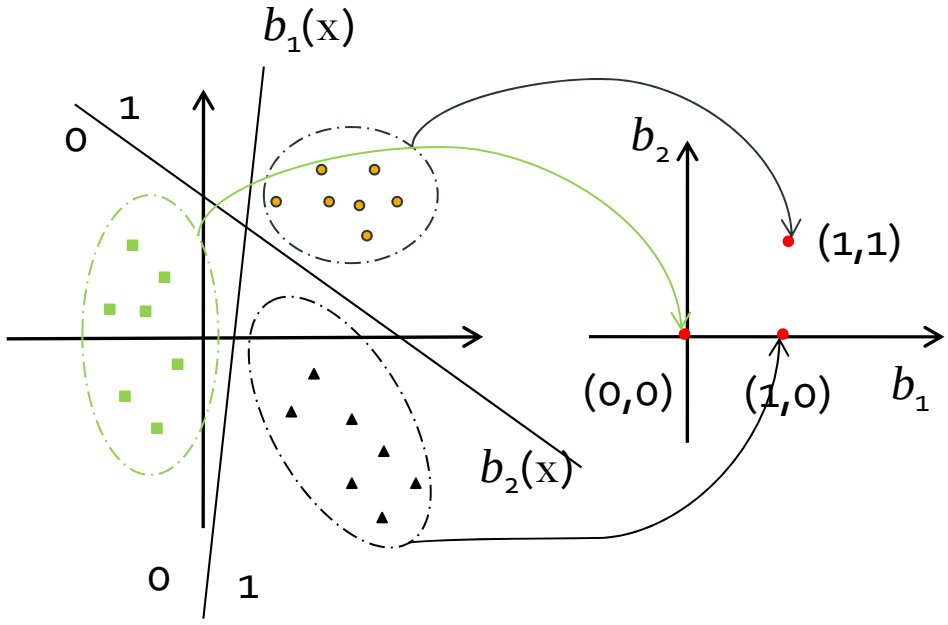
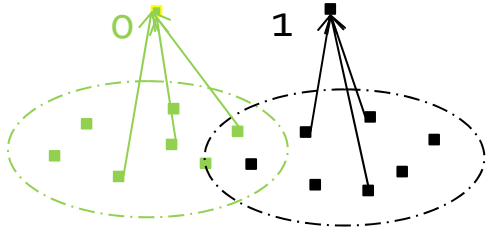


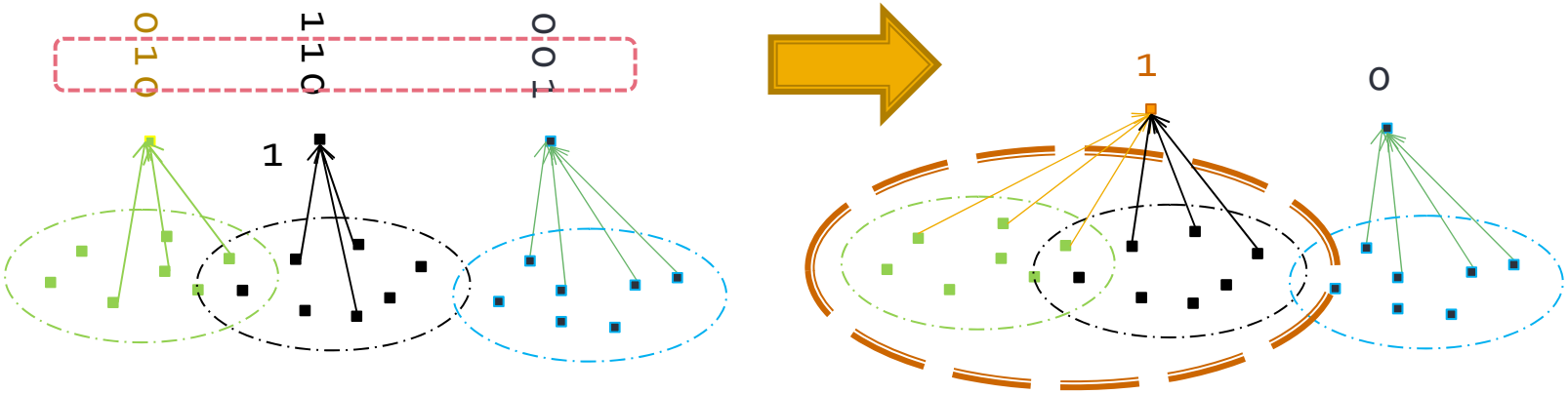
Illustration in 2-D space

Rationale

- Inspired by perceptron
  - Can find a LDF to classify two classes



  - Construct a continuous perceptron criteria function to find optimal (w , t)
    - Can be extended to multiple classes with labels of multiple bits, just like binarization



Experimental Results

- Experiment settings

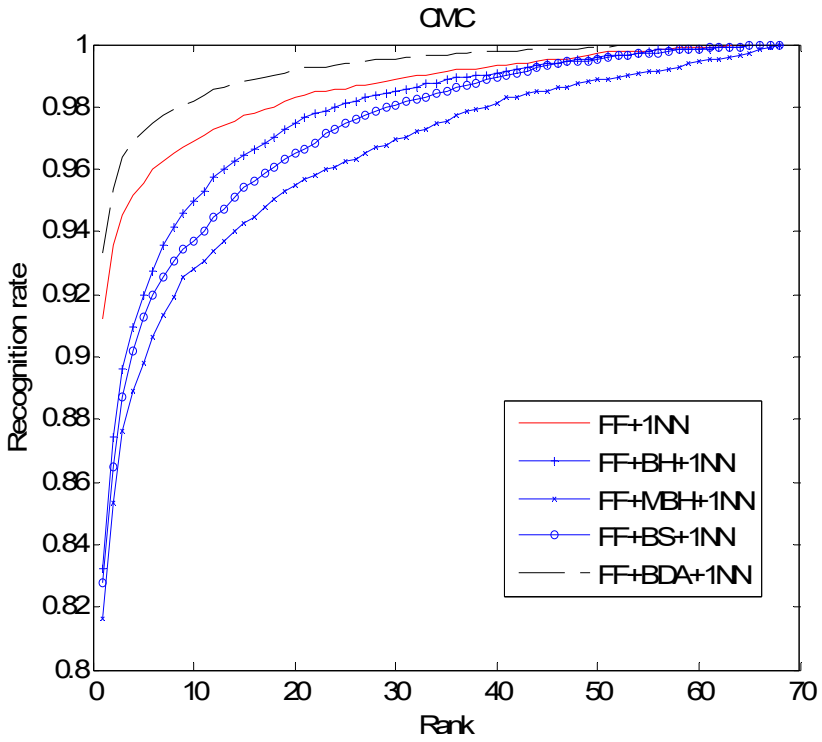
CMU PIE

FRGC

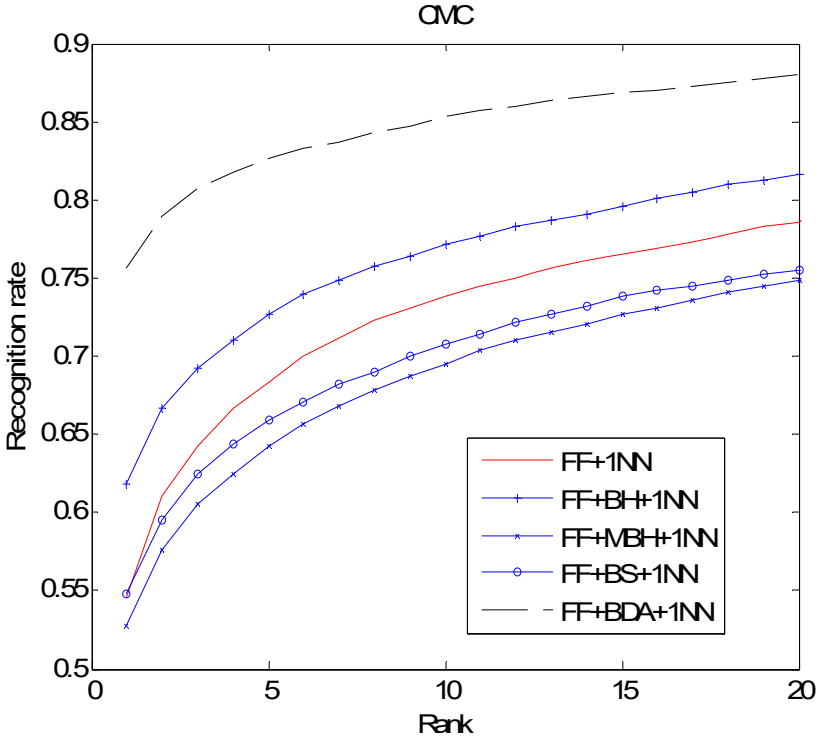
c : No. of individuals.
N_p: No. of samples for each individual.
N_t : No. of training samples per individual

Database	c	N_p	N_t	Variations
CMU PIE	68	105	10	Illumination, pose, expression
FRGC	350	40	5	expression, illumination, mild pose

Experimental Results

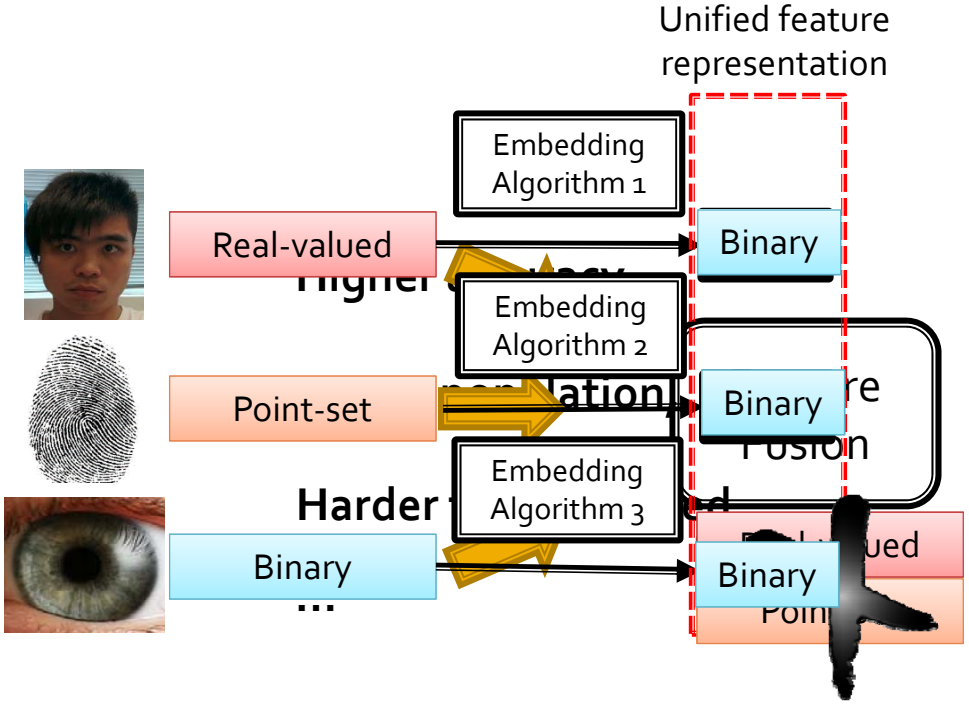


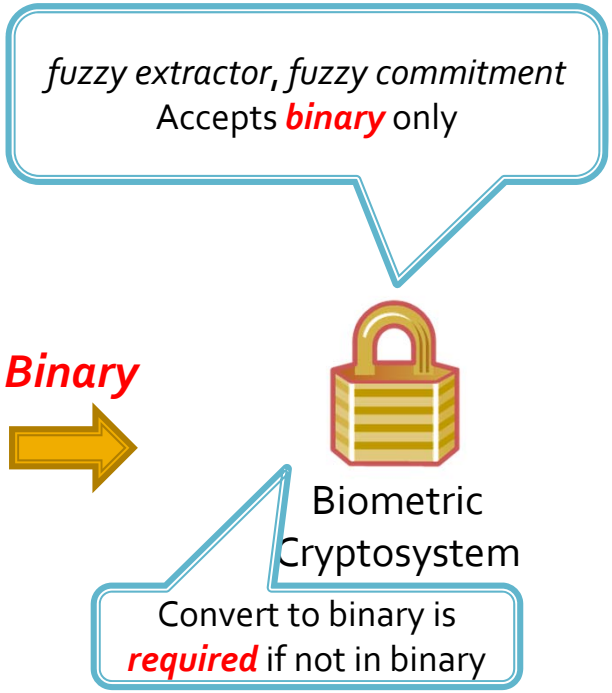
(a) CMU PIE



(b) FRGC

3. Binary Template Fusion for Multi-biometric Cryptosystem [IVC 2017]



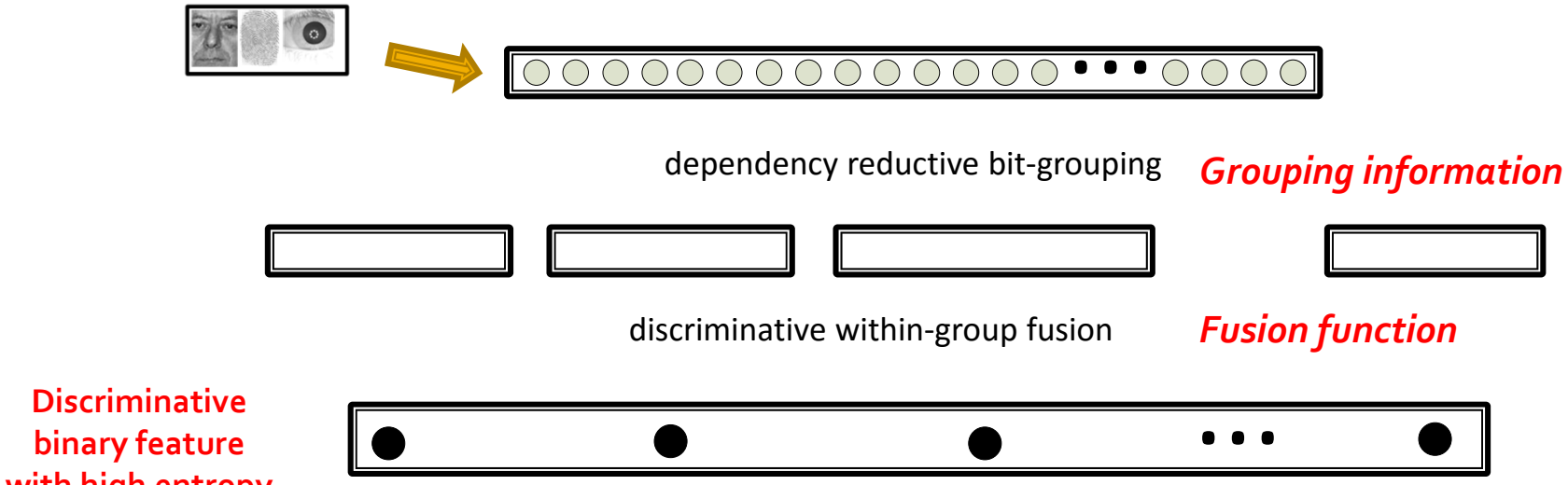


Criteria for Binary Template Fusion

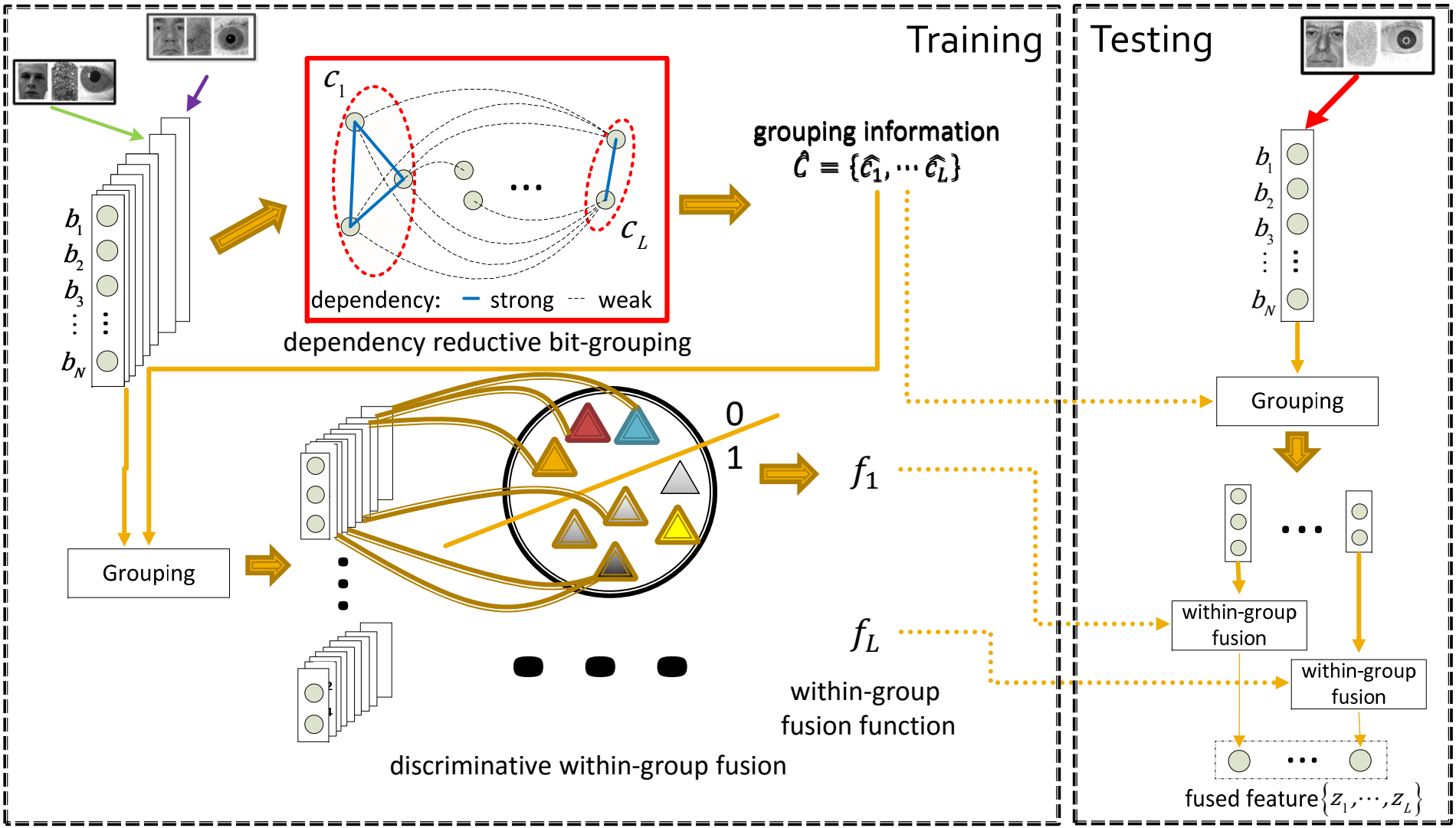
- Discriminability
  - Small intra-user variations ***of*** feature bits
  - Large inter-user variations ***of*** feature bits
- Security (high-entropy)
  - Low dependency ***among*** bits
  - High uniformity ***of*** feature bits
- Privacy
  - No information leakage from helper data

Proposed Binary Template Fusion

- Stage one: dependency-reductive bit grouping
  - Dependency among bits (**security**)
- Stage two: discriminative within-group fusion
  - Bit-uniformity (**security**), intra-user variations (**discriminability**), inter-user variations (**discriminability**)



Proposed Binary Template Fusion

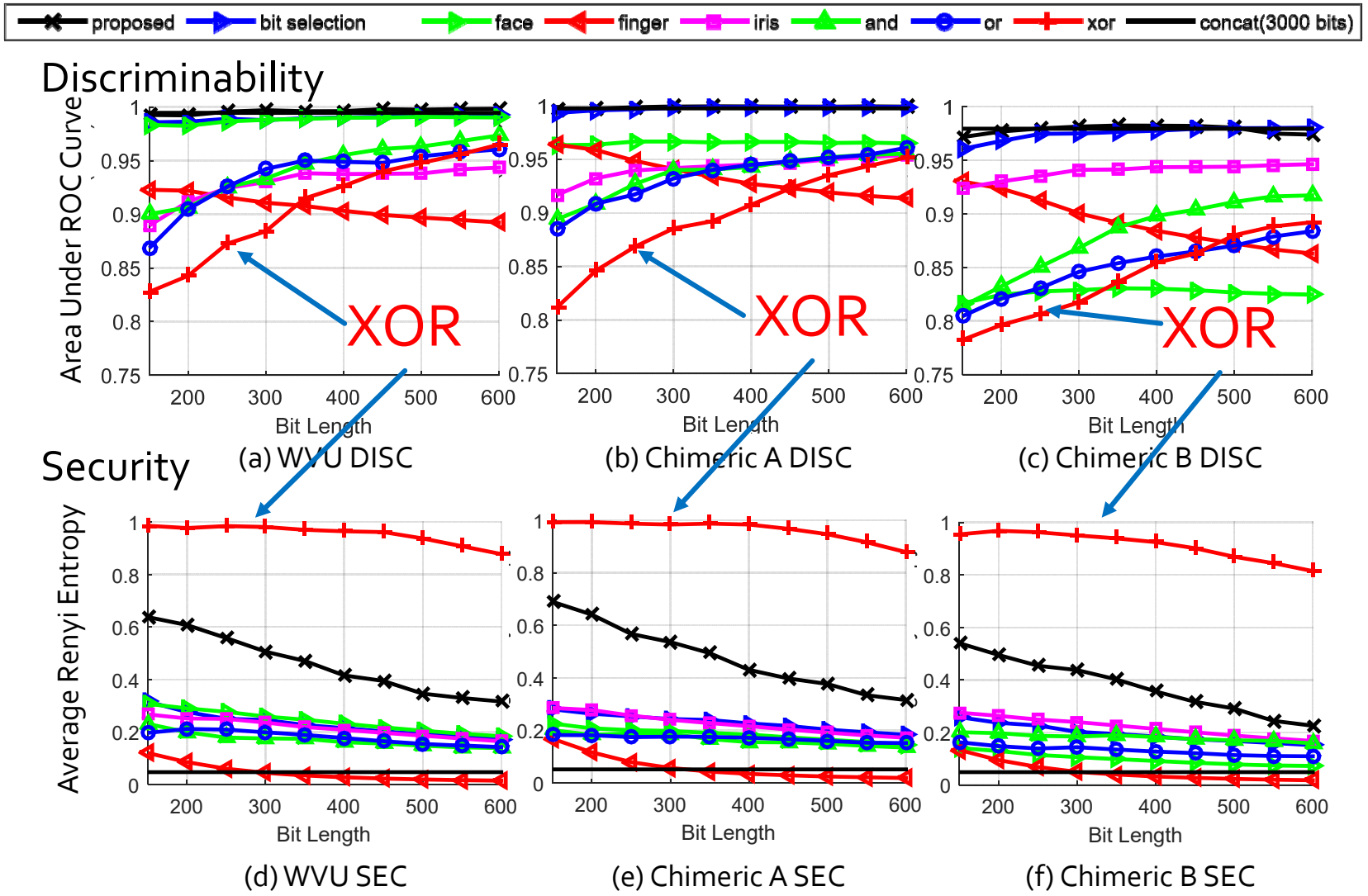


Experiments

- Evaluation
  - Discriminability (Area under ROC curve)
  - Security (average Renyi entropy, Hidano et al. BIOSIG2012)
- Experiments settings

Multimodal Database	WVU	Chimeric A (FVC2000DB2 + FERET + CASIA)	Chimeric B (FVC2002DB2 + FRGC + ICE2006)
Subjects	106	100	100
Training Sample	3	4	4
Testing Sample	2	4	4

Experimental Results



- Related work:

M H Lim, S Verma, G C Mai and P C Yuen, "Learning discriminability-preserving histogram representation from unordered features for multibiometric feature-fused template protection", *Pattern Recognition*, In press, 2016

4. Entropy Measurement for Biometric Verification Systems [IEEE T C 2016]

- Guessing and entropy
  - Entropy of n-bit
    - Sampling with replacement
      - n-bit entropy → 2^n guessing attempts for correct guess on average
    - Sampling w/o replacement
      - n-bit entropy → $\frac{2^n+1}{2}$ guessing attempts for correct guess on average
  - Expected #(guessing trials) $E[T]$

$$E[T] = \begin{cases} 2^{H(X)}, & \text{for sampling with replacement} \\ \dfrac{2^{H(X)}+1}{2}, & \text{for sampling w/o replacement} \end{cases}$$

where $H(X)$ denotes the entropy of variable $X = \{x_i\}$

M H Lim and P C Yuen, Entropy Measurement for Biometric Verification Systems, *IEEE Transactions on Cybernetics*, 2016

Entropy Measurement for Biometric Verification Systems

- Guessing entropy
  - Entropy $H(X)$ can then be expressed as

$$H(X) = \begin{cases} \log_2(E[T]), & \text{for sampling with replacement} \\ \log_2(2E[T]-1), & \text{for sampling w/o replacement} \end{cases}$$

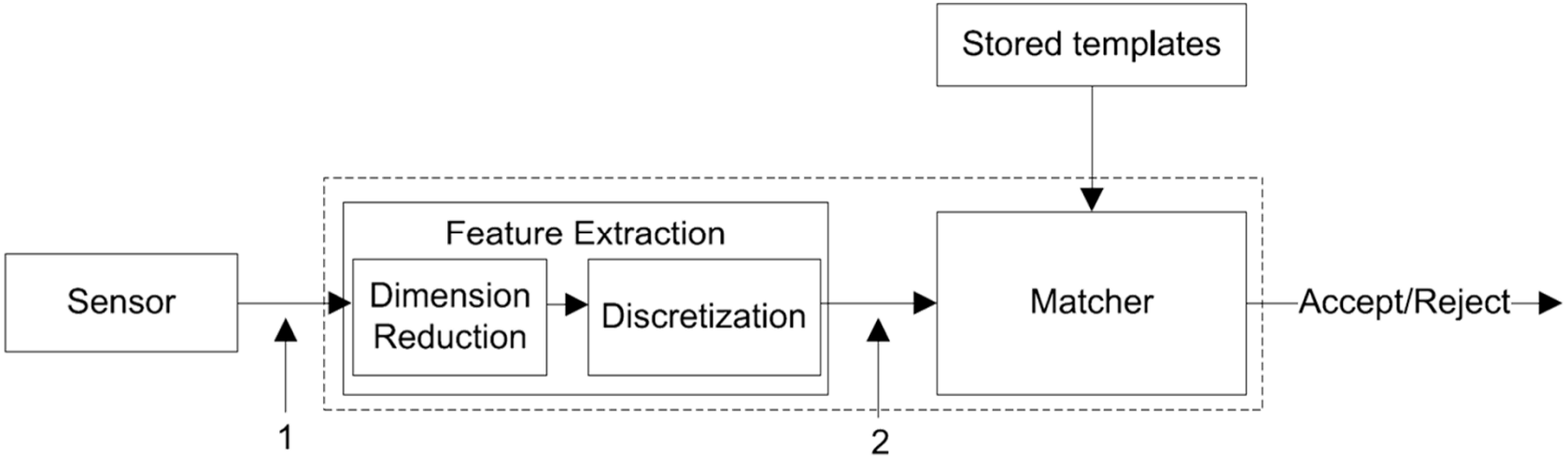
  - By definition, Expected #(guessing trials)$E[T]$

$$E[T] = \sum_{T=1}^{T_{\max}} T \cdot P(X_{\text{trial}} = T)$$

where $P(X_{\text{trial}} = T)$ denotes probability of taking T trials for the first adversarial success in guessing and $T_{\max}$ denotes the maximum number of trials that is dependent on the guessing strategy

Adversarial Sampling

- Sampling with replacement
  - Sensor-signal tapping attack (point 1)
- Sampling w/o replacement
  - Discretizer-signal tapping (point 2)

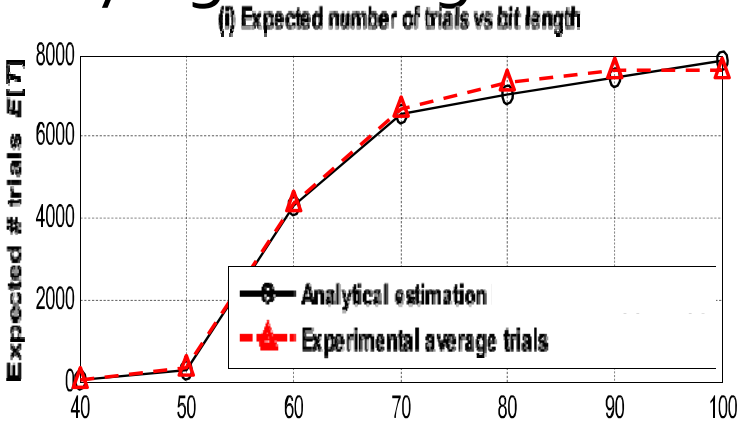


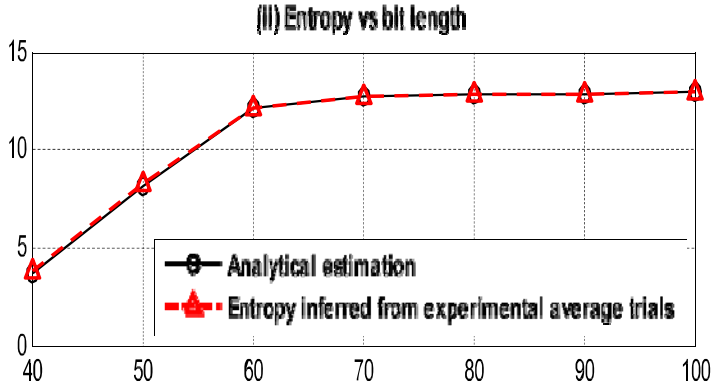
Experiments

- Analytic expressions validation
  - Sampling without replacement
    - *Synthetic Dataset*, imposter distributions that are modeled as normal distributions
  - Sampling w/o replacement
    - *Real Dataset*, a large subset of FERET face dataset
      - 3000 images, 250 subjects, 12 images per subject
    - Feature extractor: *ERE+RDBA+EP*
      - Eigenfeature regularization and extraction with reliability-dependent bit allocator with equal-probable (RDBA + EP) discretizer

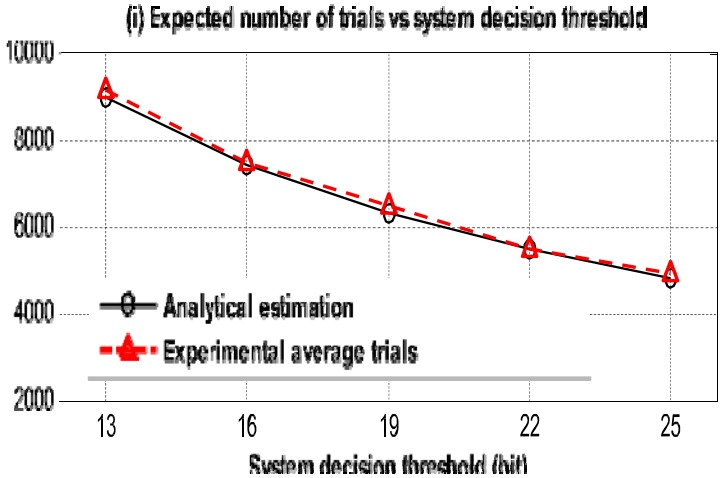
Sampling with Replacement

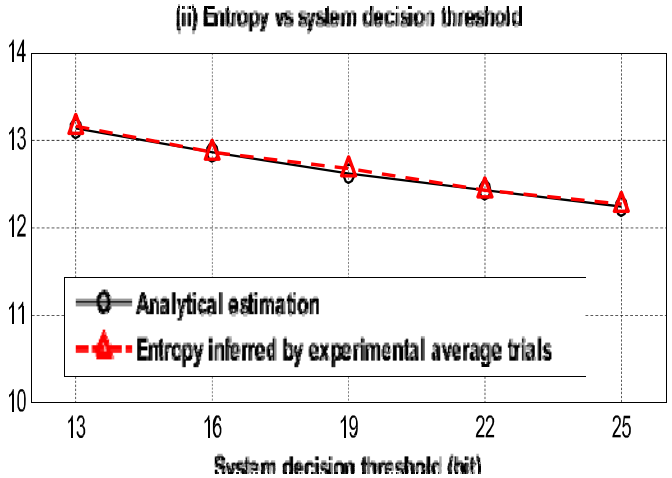
- Varying bit length





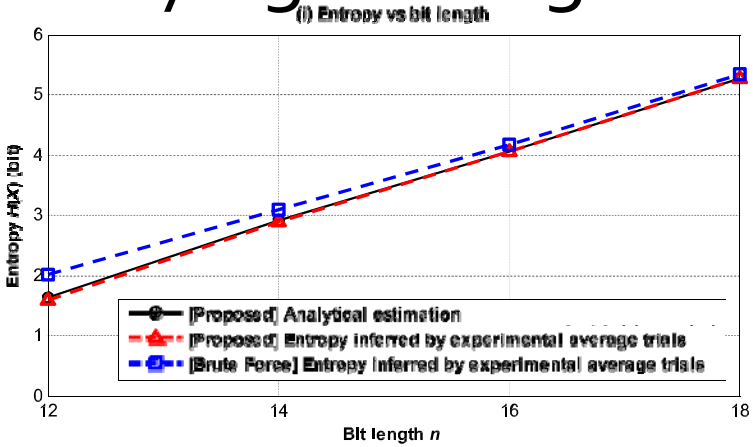
- Varying decision threshold

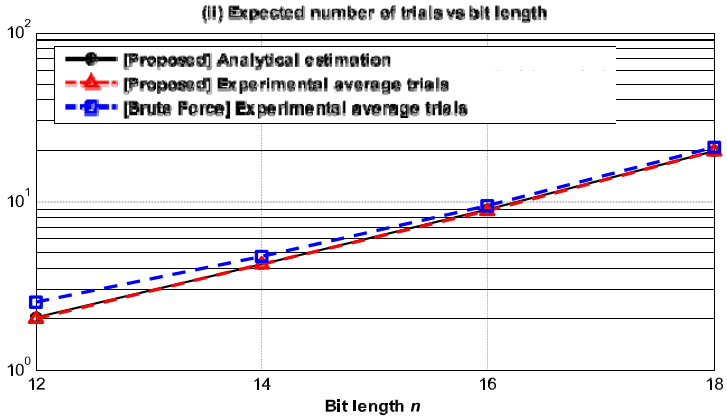




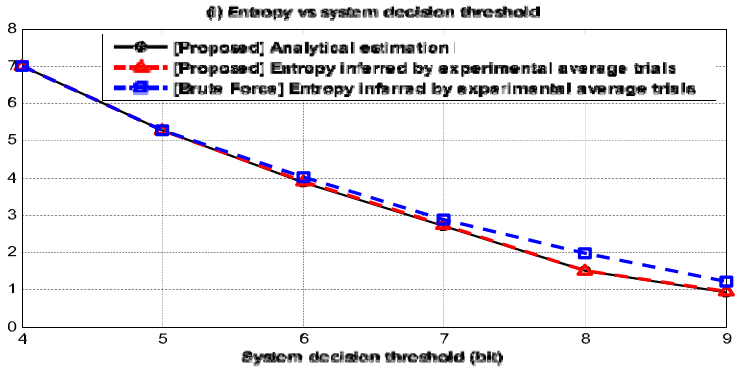
Sampling w/o Replacement

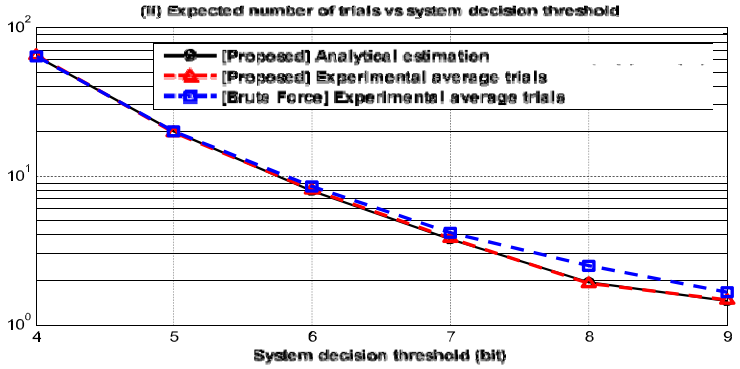
- Varying bit length n





- Varying system decision threshold





Section Conclusion

Section Conclusion

- Face images can be reconstructed from unprotected templates stored in face recognition system
  - Template protection is required
- Single template protection scheme (biometric cryptosystems and transformation-based) is not sufficient, but hybrid approach.
- Introduced some of our works. A lot of work in template protection needs to be done.

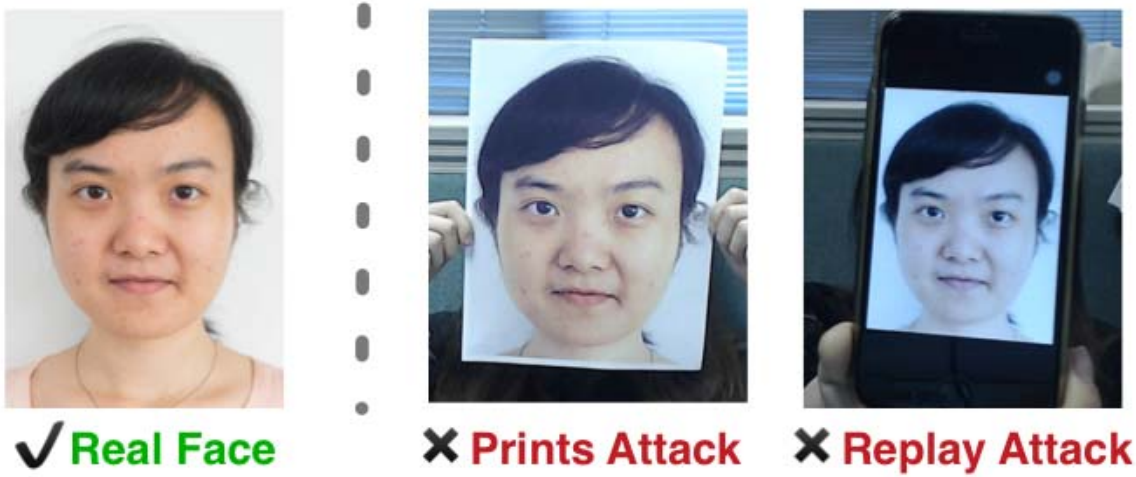
Part II:
Face Anti-Spoofing

Outline: Face Anti-spoofing

1. Background and Motivations
2. Related Work
3. Proposed Methods
4. Conclusions

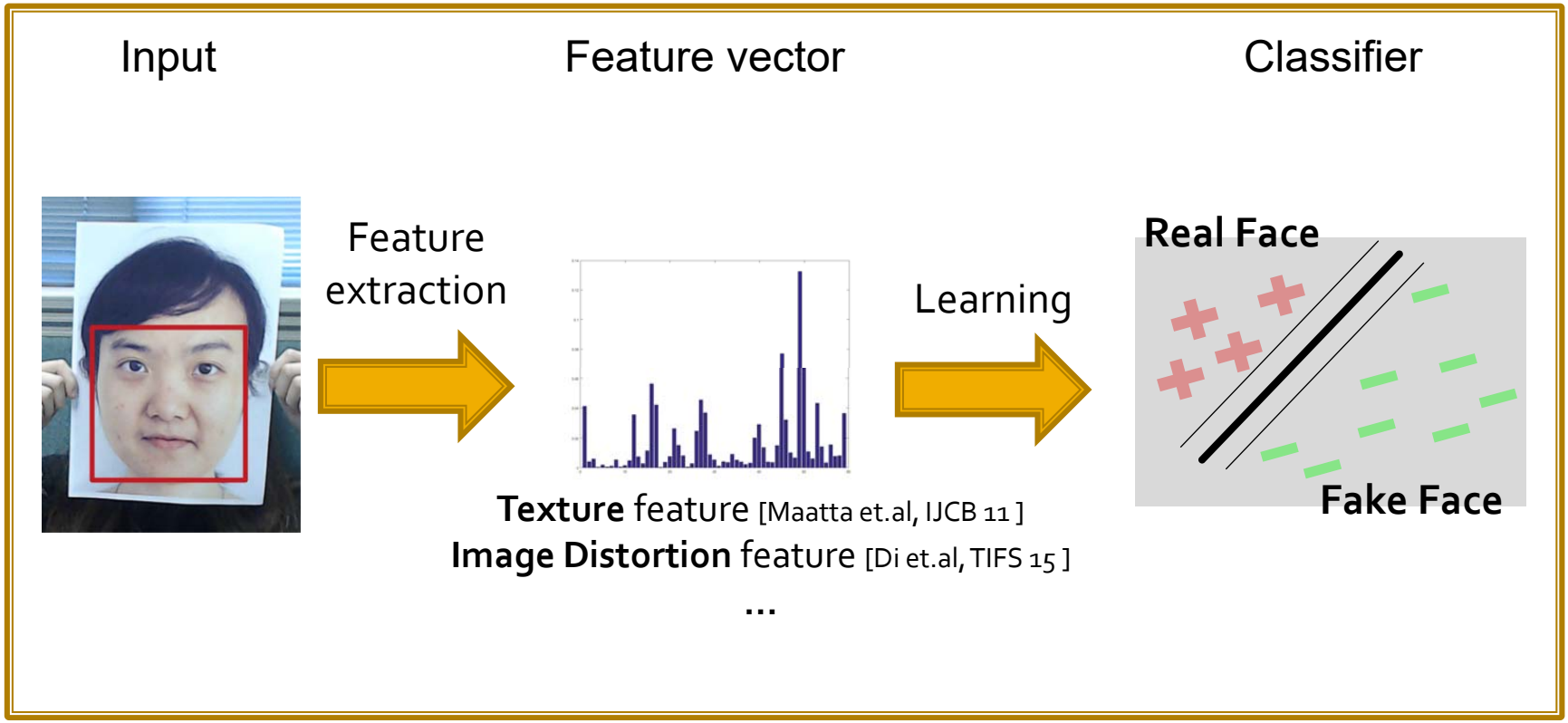
Background and Motivations

- Face Spoofing Attack
  - With rapid development of social network such as Facebook and Twitter, face information can be easily acquired (facebook, twitter) and abused



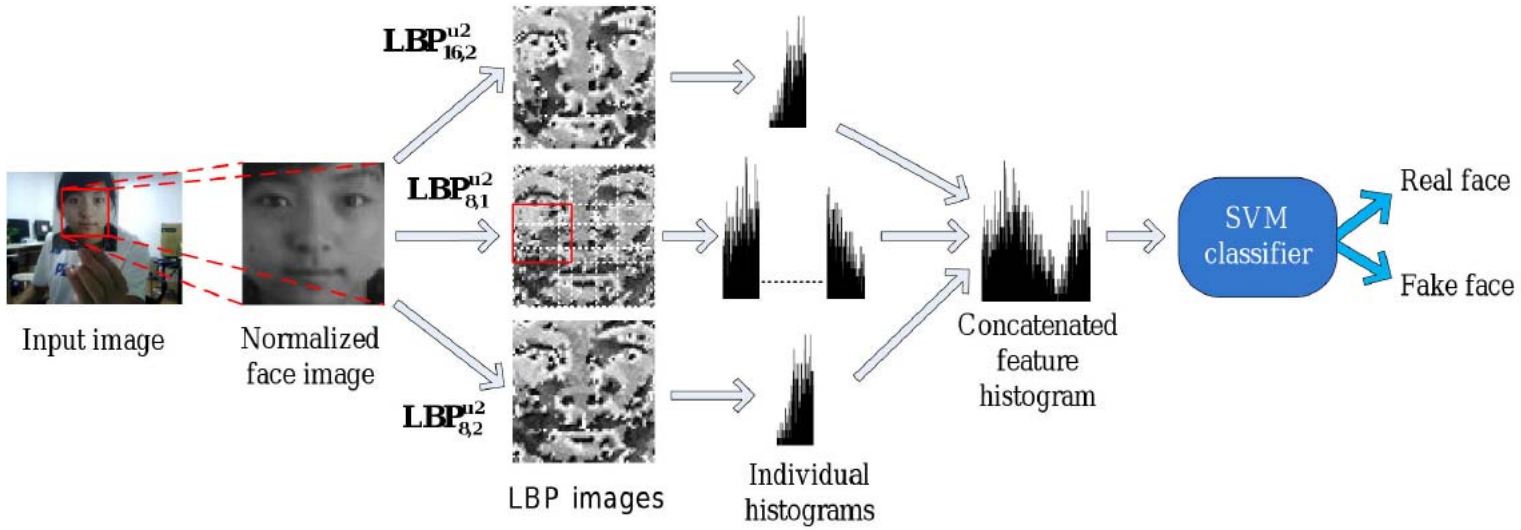
Background and Motivations

- Anti-spoofing approach: Appearance-based
  - Spoof media (print and screen) and genuine face has different appearance



Background and Motivations

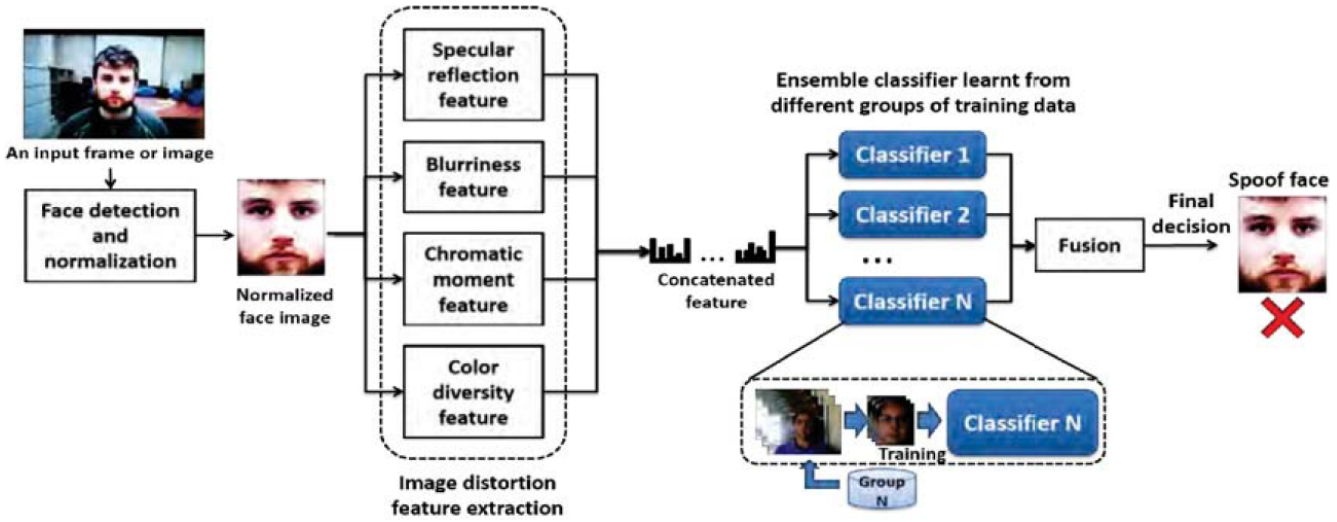
- Anti-spoofing approach: Appearance-based
  - Spoof media (Prints and screen) has different texture, comparing with genuine face



Source: Jukka Maatta, Abdenour Hadid, Matti Pietikainen, "Face Spoofing Detection From Single Images Using Micro-Texture Analysis", *IJCB* 2011

Background and Motivations

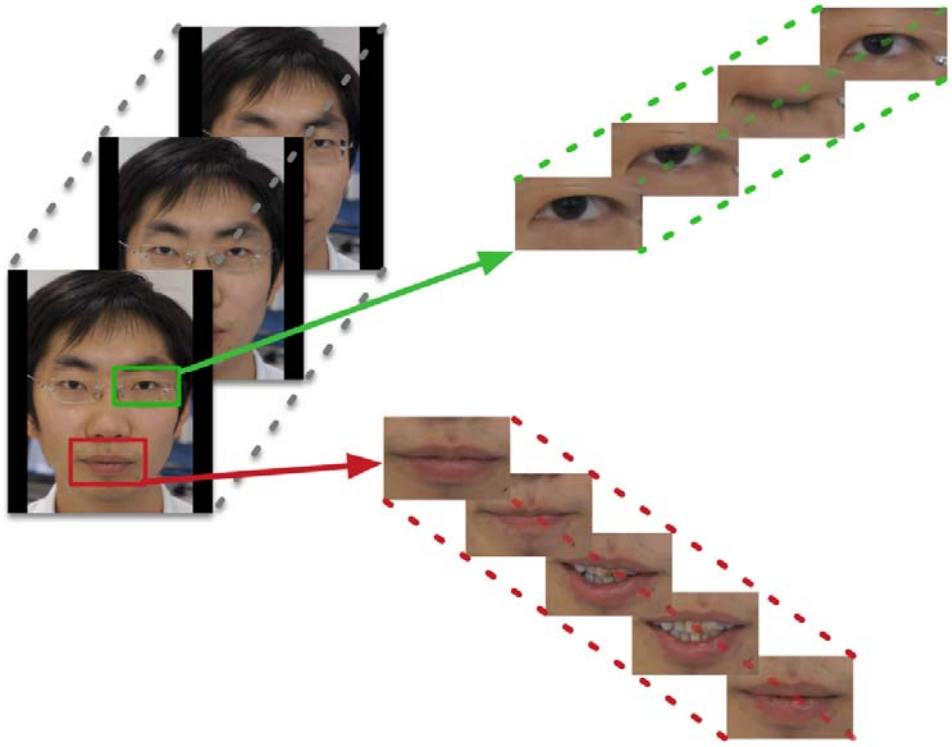
- Anti-spoofing approach: Appearance-based
  - Spoof media (Prints and screen) has specific quality defects



Source: Di Wen, Hu Han, Anil K. Jain, "Face Spoof Detection with Image Distortion Analysis", *TIFS* 2015

Background and Motivations

- Anti-spoofing approach: Motion-based
  - 2D spoofing medium cannot move, or has different motion pattern compare with real face



Background and Motivations

- Anti-spoofing approach: Motion-based
  - **Eyeblink-based** anti-spoofing in face recognition from a generic web-camera (G.Pan et al., ICCV'07)
  - Real-time face detection and **motion analysis** with application in liveness assessment. (K. Kollreider et al., TIFS'07)
  - A liveness detection method for face recognition based on **optical flow field** (W. Bao et al., IASP'09)
  - Face liveness detection using **dynamic texture** (Pereira et al., JIVP'14)
  - Detection of face spoofing using **visual dynamics** (S. Tirunagari et al., TIFS'15)

Background and Motivations

- Performance on traditional face spoofing attack

	Replay Attack		Print attack	
Pipelines	***Dev***	***Test***	***Dev***	***Test***
DMD+SVM (face region)	8.50	7.50	0.00	0.00
DMD+LBP+SVM (face region)	5.33	3.75	0.00	0.00
PCA+SVM (face region)	20.00	21.50	16.25	15.11
PCA+LBP (face region)	11.67	17.50	9.50	5.11
DMD+LBP+SVM (entire video)	0.50	0.00	0.00	0.00
PCA+LBP+SVM (entire video)	21.75	20.50	11.50	9.50

[S. Tirunagari et al., TIFS'15]

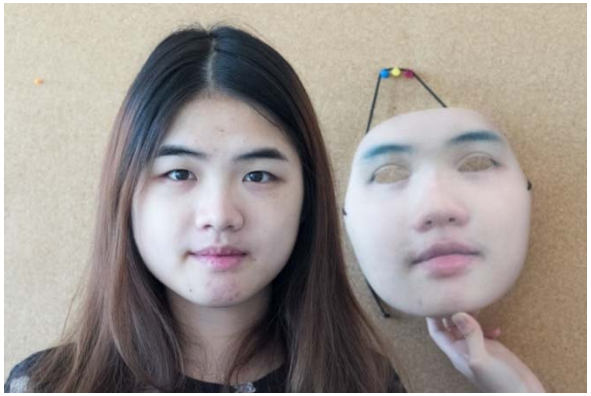
Promising results are achieved on tradition face spoofing attack

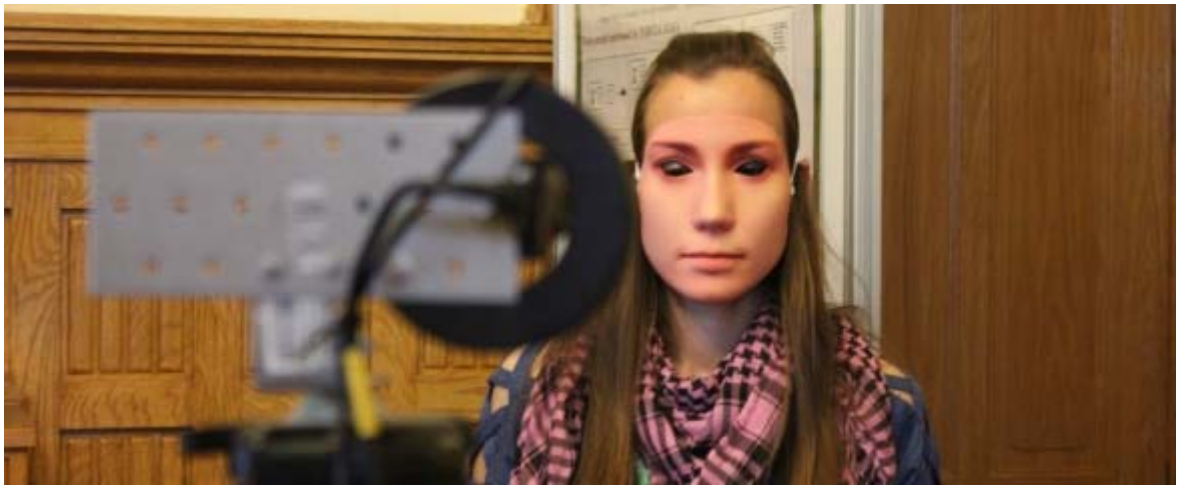
Background and Motivations

Problem solved?

Background and Motivations

- **New Challenge**: 3D Mask Attack
  - With development 3D reconstruction and 3D printing technology, 3D face model can easily be constructed and used to spoof the security system





Source: idiap.ch

Mask is made from ThatsMyFace.com

Background and Motivations

- **New Challenge**: Super-realistic 3D Mask
  - 3D mask can be so real that we can hardly differentiate them from appearance

(a) Life face

(b) Real-F hyper real mask

Source: real-f.jp

Background and Motivations

Hong Kong SAR | Hong Kong

Hong Kong airport security fooled by these hyper-real silicon masks

Masks like the one that transformed a Chinese kid into a U.S. grandpa are now available online

By Tea Li | 8 November, 2010

Suspicious old folks: the Elder Mask from SPFX Masks is so real.

Before...

That Chinese guy who disguised himself as an old white man to slip by Hong Kong airport security and board an Air Canada flight might have ordered his old man mask from SPFX Masks (http://www.spfxmasks.com) .

This is the stuff that entered popular imagination with the Mission Impossible television series (http://www.youtube.com/watch?v=b6qcIlhLE3c&NR=1) and is used by the CIA (http://abcnews.go.com/Health/Cosmetic/story?id=1354130) and as prosthetics for medical conditions (http://www.prosthesis.com/services.htm) .

Now we can order our own so-real-its-creepy mask online.

Silicon masks from SPFX adhere to facial features such that the mask is able to move with the musculature of the wearer, like a second skin. The mask is attached to a neck flap and some come with silicon gloves to disguise the hands and forearms as well.

is attached to a neck flap and some come with silicon gloves to disguise the hands and forearms as well.

Check out the video above of a demonstration of the Elder Mask (http://www.spfxmasks.com/maskelder.html) from SPFX, which resembles the one that Chinese stowaway was caught with in Canada. Priced at US$689, the mask is aimed at Halloween revelers and haunted house actors.

... and after.

But the passenger who breached Hong Kong airport security on October 29 used his mask to smuggle himself into Canada.

The Chinese man who appeared to be in his early 20s disguised himself as an elderly Caucasian man, obtained a boarding pass from a U.S. citizen while in transit in Hong Kong, and boarded the Air Canada flight using an Aeroplan card for identification.

Read more details about the case from the confidential alert obtained by CNN (http://articles.cnn.com/2010-11-04/world/canada.disguised.passenger_1_flight-crew-hong-kong-regional-communications-officer?_s=PM:WORLD) .

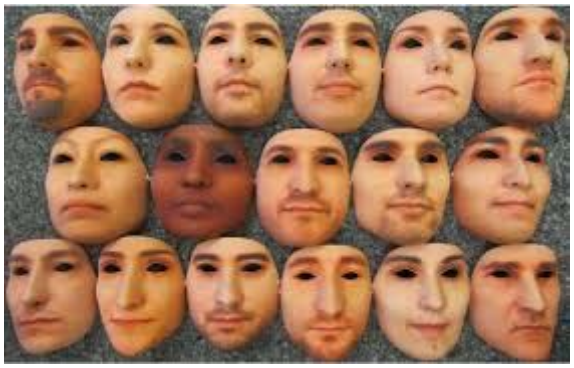
Source: http://travel.cnn.com/hong-kong/visit/hong-kong-airport-security-fooled-these-hyper-real-silicon-masks-743923/

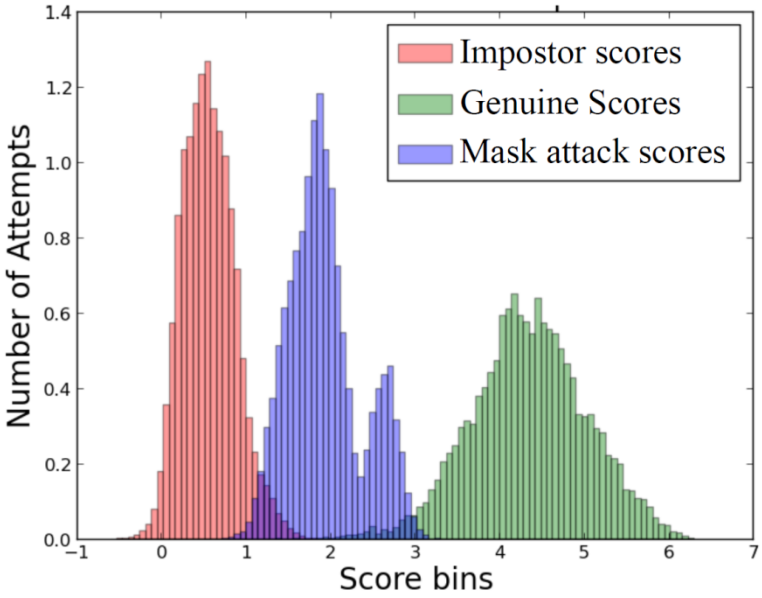
Related Work

- Existing works on 3D Mask Spoofing Attack
  - The 3DMAD dataset [Erdogmus et al., BTAS'13]
  - LBP-based solution [Erdogmus et al., TIFS'14]

Related Work

- The 3DMAD dataset
  - Score distributions of genuine, impostor, and mask attack scores of 3DMAD using ISV for 2D face verification

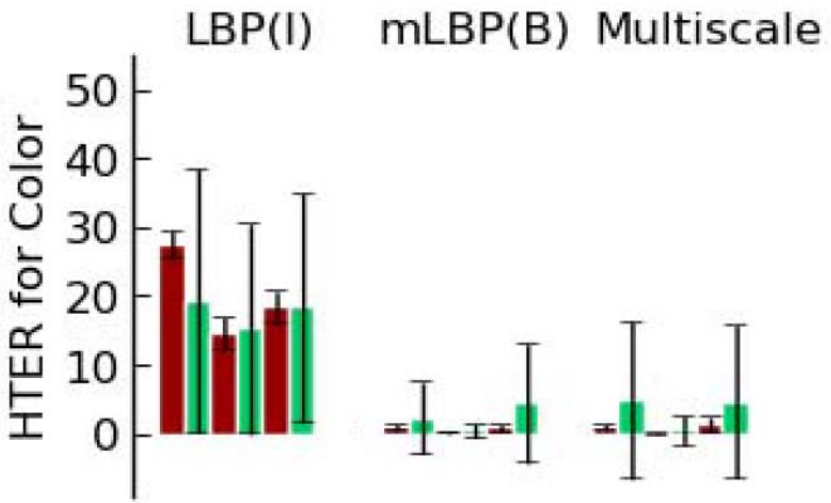


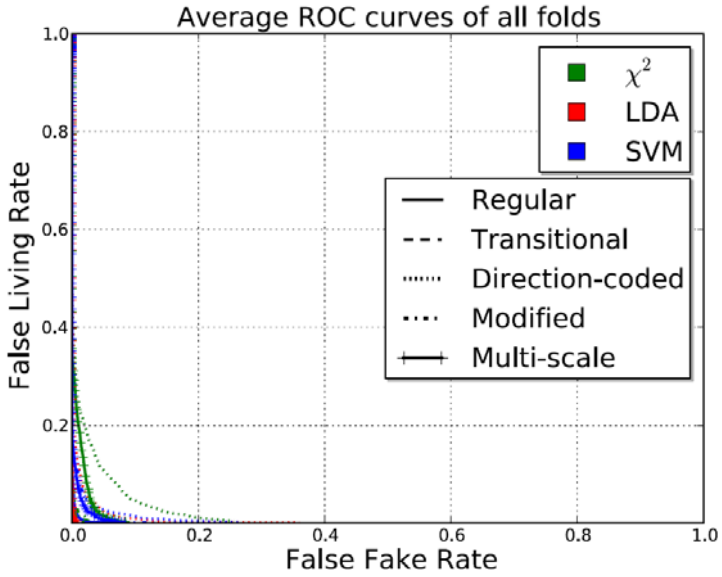


[Erdogmus et al., BTAS'13]

Related Work

- LBP-based solution
  - The multi-scale LBP features yield to very good results on 3DMAD [Erdogmus et al., TIFS'14]





[Erdogmus et al., TIFS'14]

Analysis of Existing Methods

- Pros and Cons

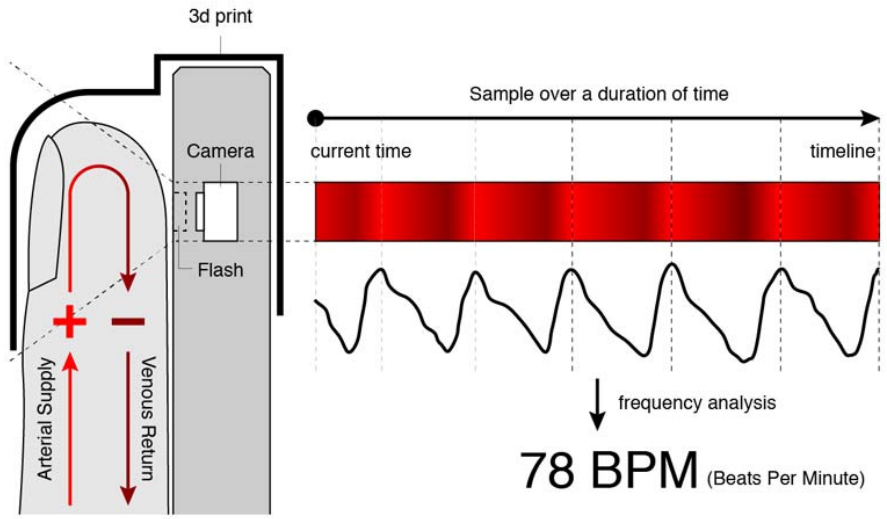
  + Achieve high performance in 3DMAD dataset

  - **Hyper real 3D mask may not have quality defects**
  - **LBP-based solution may not perform well under cross database scenario**

- What do we need?
  - A new discriminative liveness cue
  - More 3D mask datasets for comprehensive experiments

Our Proposed Approach

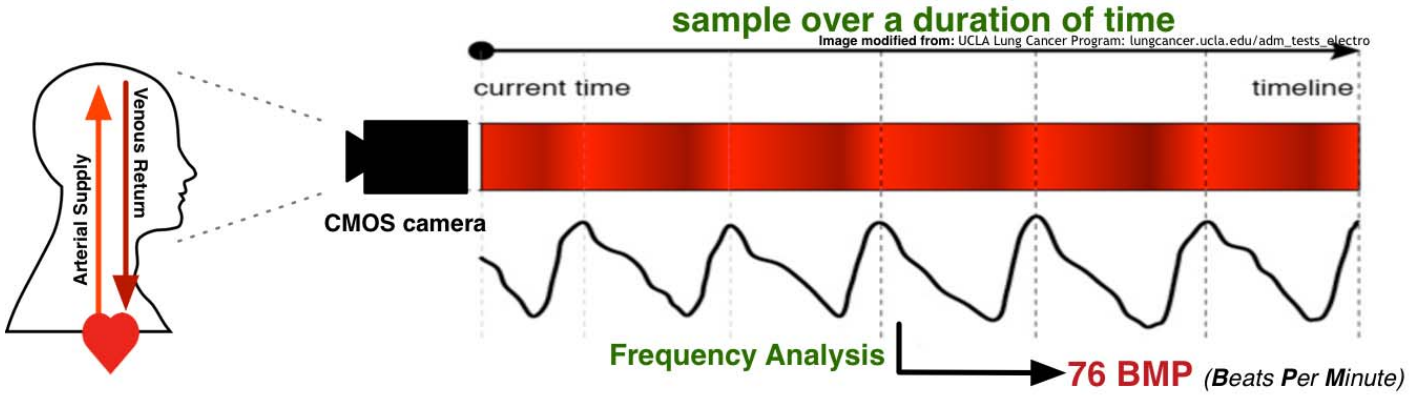
- PhotoPlethysmoGraphy (**PPG)**



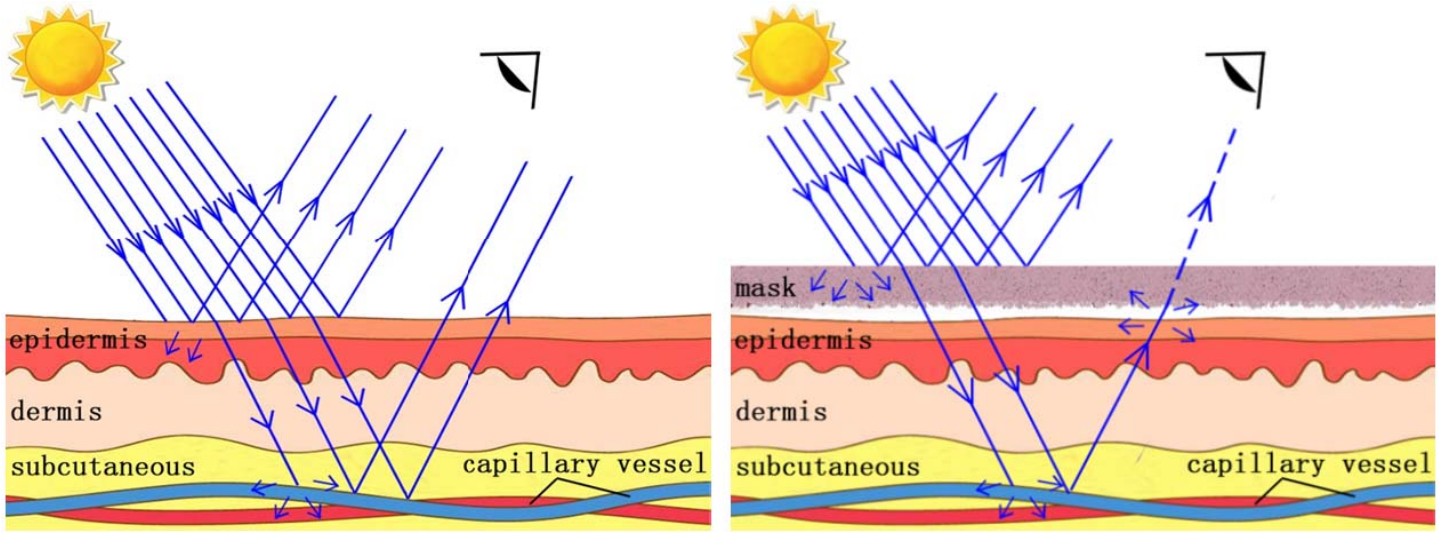
Pic. from UCLA Lung Cancer Program http://lungcancer.ucla.edu/adm_tests_electro.html

Our Proposed Approach

- remote PhotoPlethysmoGraphy (rPPG)



Principle of rPPG Based Face Anti-Spoofing



(a) (b)

(a) rPPG signal can be extracted from genuine face skin.

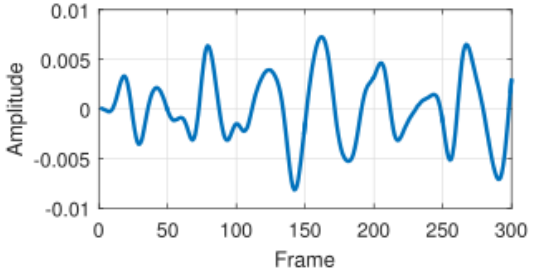
(b) rPPG signals will be **too weak** to be detected from a masked face.

- light source needs to penetrate the mask before interacting with the blood vessel.
- rPPG signal need to penetrate the mask before capturing by camera

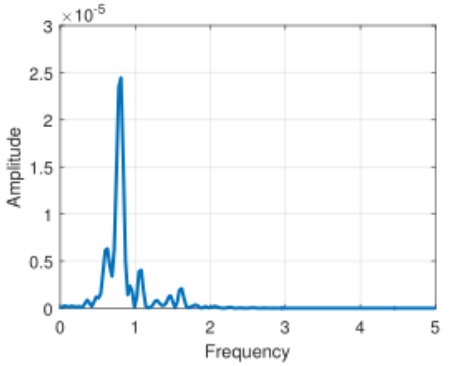
Principle of rPPG Based Face Anti-Spoofing

genuine face

(a)



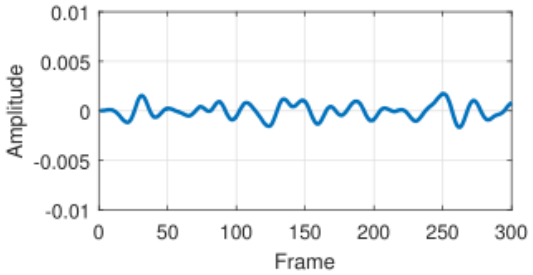
(b)



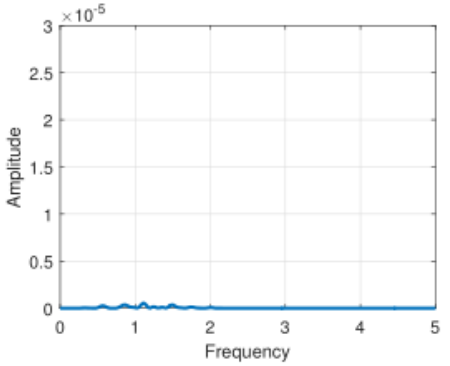
(c)

masked face

(d)

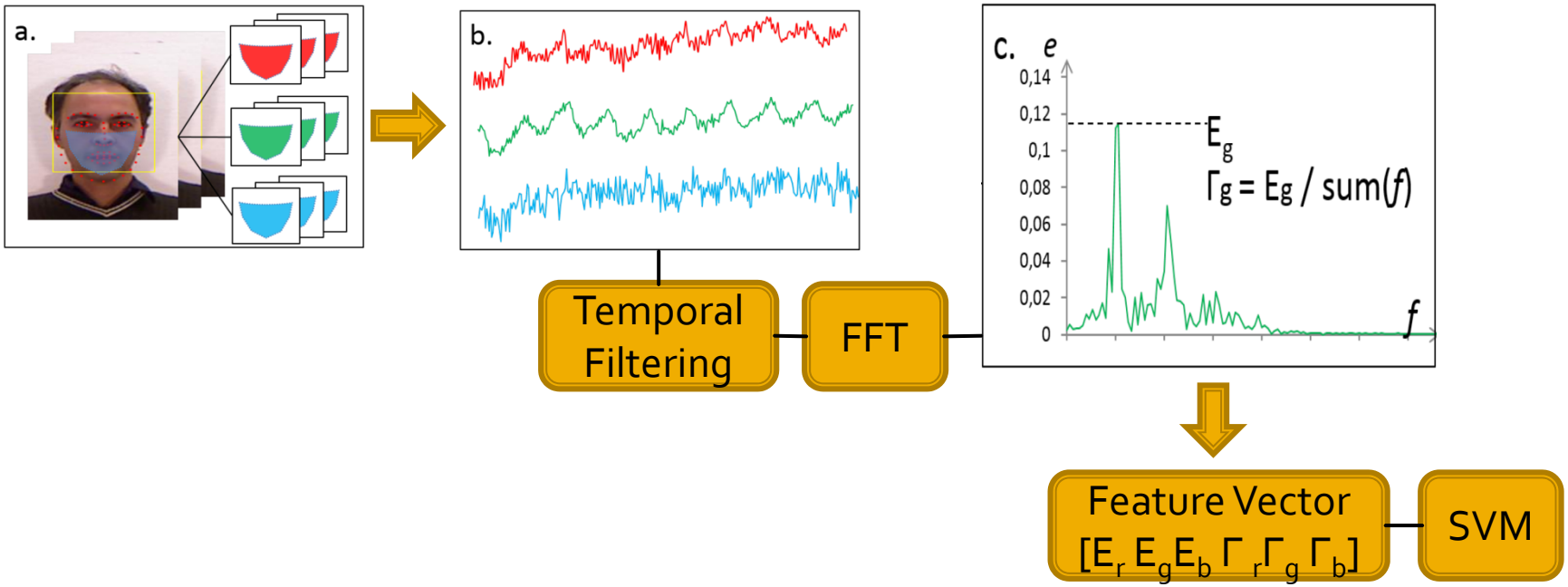


(e)



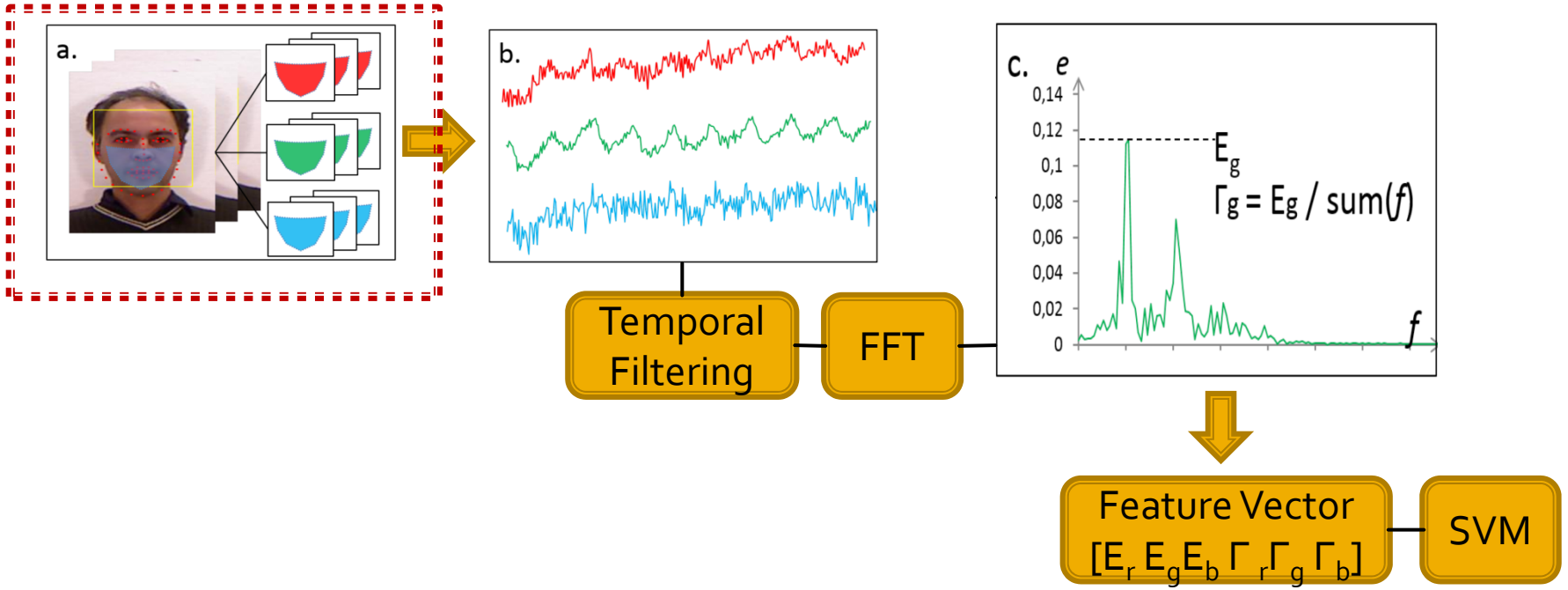
(f)

Global rPPG-based Face Anti-Spoofing [ICPR 2016]



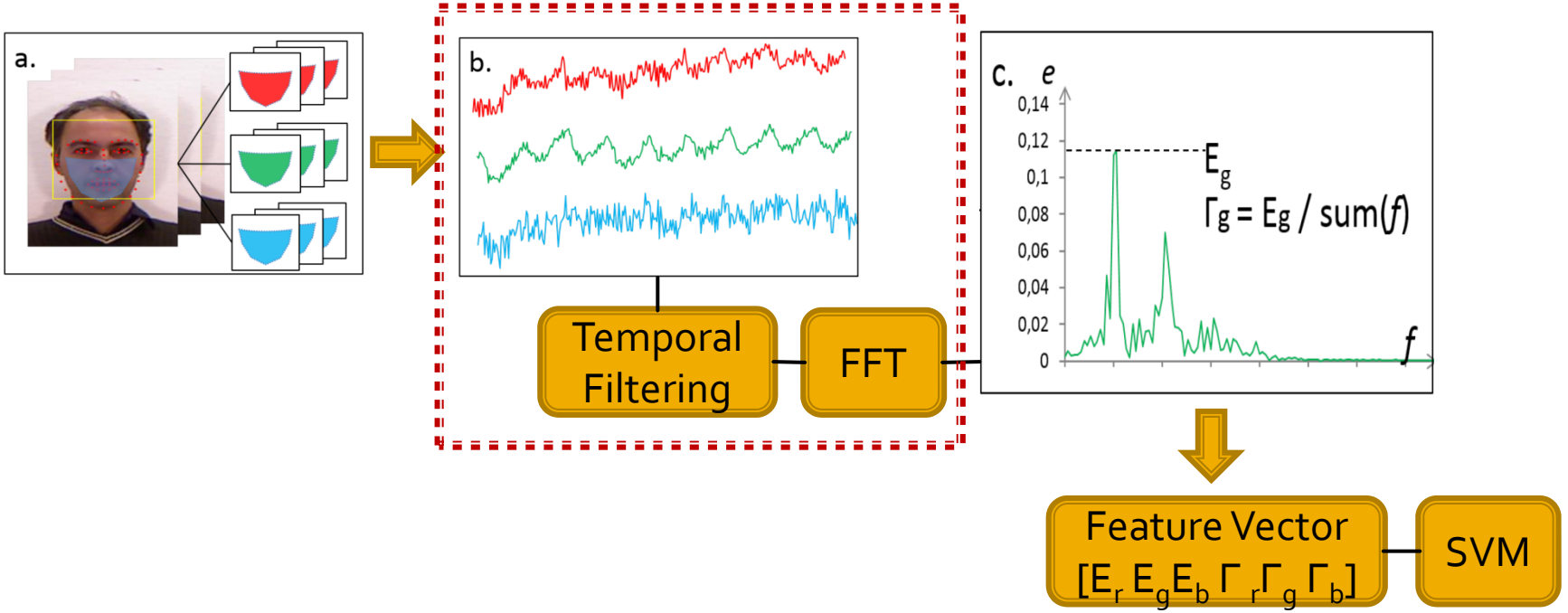
X Li, J Komulainen, G Zhao, P C Yuen and M Pietikainen "Generalized face anti-spoofing by detecting pulse from face videos", *ICPR* 2016

Global rPPG-based Face Anti-Spoofing



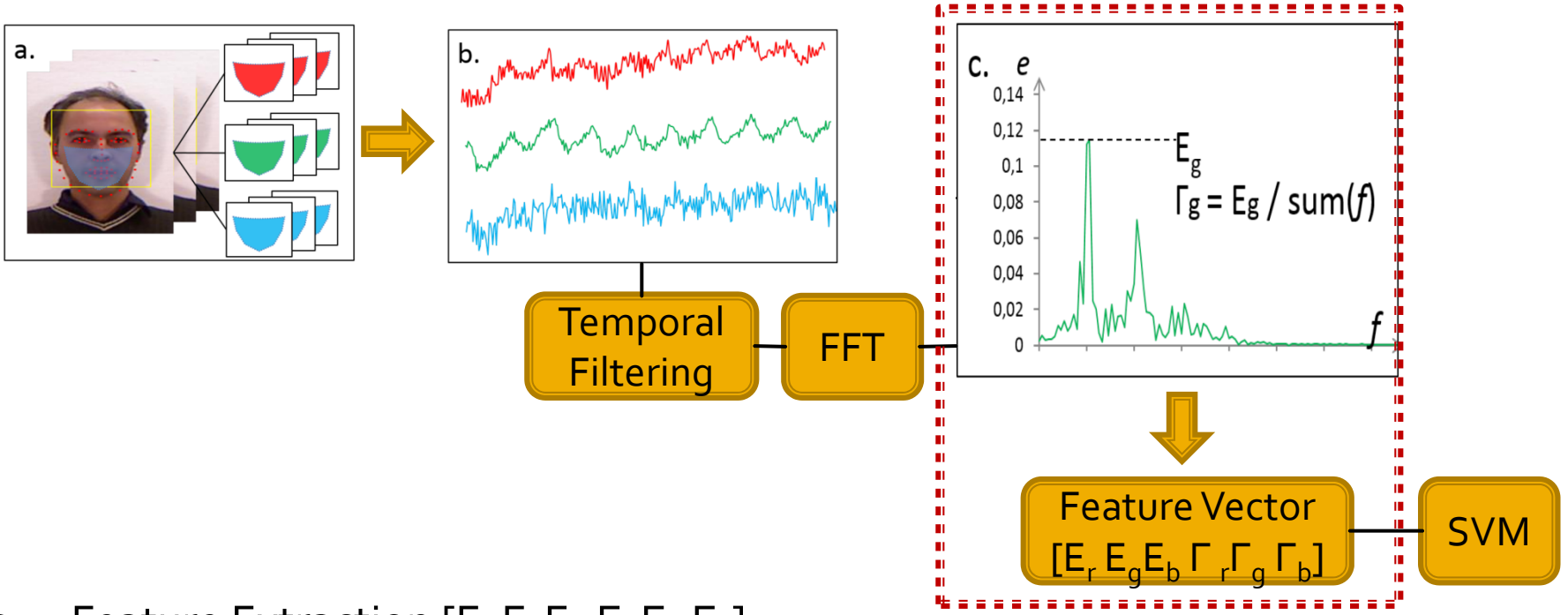
a. Face Detection and ROI tracking
   - Use Viola-Jones face detector on the first frame
   - Find 66 facial landmarks [CVPR'13 Asthana et.al] within the face bounding box. Use 9 of them to define the ROI
   - ROI is tracked through all frames using KLT

Global rPPG-based Face Anti-Spoofing



b. Three raw pulse signals r_{raw} g_{raw} and b_{raw} are computed one from each RGB channel, respectively.
   - FIR bandpass filter with a cutoff frequency range of [0.7; 4] Hz ([42; 240] beat-per-minute)
   - Use fast Fourier transform (FFT) to convert the pulse signals into frequency domain-> PSD curve: f

Global rPPG-based Face Anti-Spoofing



c. Feature Extraction $[E_r\ E_g E_b\ \Gamma_r \Gamma_g\ \Gamma_b]$

- $E = \max(e(f))$
- $\Gamma = \frac{E}{\sum_{\forall f \in [0.7,4]} e(f)}$

Experiments

- Data:
  - 3DMAD [TIFS'14 Erdogmus et.al]
    - 255 videos recorded from 17 subjects
    - Masks made from *ThatsMyFace.com*
  - 2 REAL-F Mask
    - 24 videos recorded from 2 subjects
    - Hyper real masks from *REAL-F*

Experiments

- Results on 3DMAD
  - LOOCV protocol [Erdogmus *et.al* TIFS'14]

	3DMAD-dev	3DMAD-test	
Method	EER(%)	HTER(%)	EER(%)
Pulse (ours)	**2.31**	**7.94**	**4.17**
LBP-blk	0	0	0
LBP-blk-color	0	0	0
LBP-ms	0	0	0
LBP-ms-color	0	0	0

Note:

LBP-blk: $LBP_{8,1}$ extracted from 33 blocks of a gray-scale face

LBP-blk-color: LBP-blk but extracted separately from each RGB color channel

LBP-ms: multi-scale LBP extracted from a whole gray-scale face image combining $LBP_{8,1}$, $LBP_{8,2}$, $LBP_{8,3}$, $LBP_{8,4}$, and $LBP_{16,2}$

LBP-ms-color: LBP-ms but extracted separately from each RGB color channel

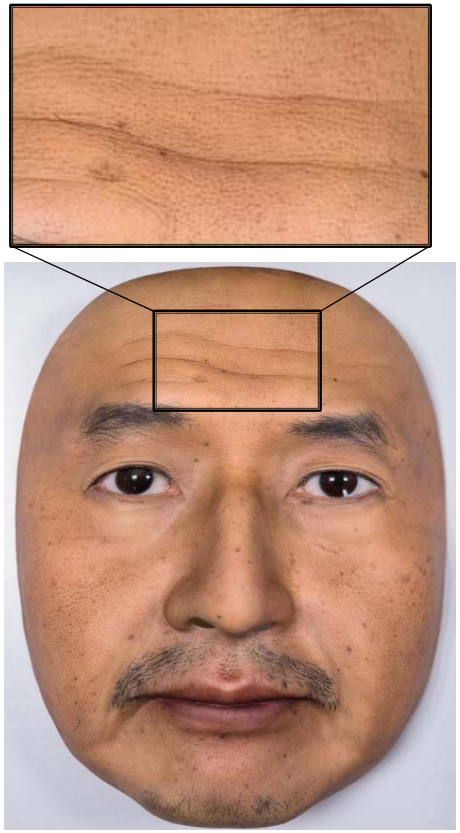
Experiments

- Results on REAL-F
  - Randomly select 8 subjects from 3DMAD for training and the other 8 subjects as the development set

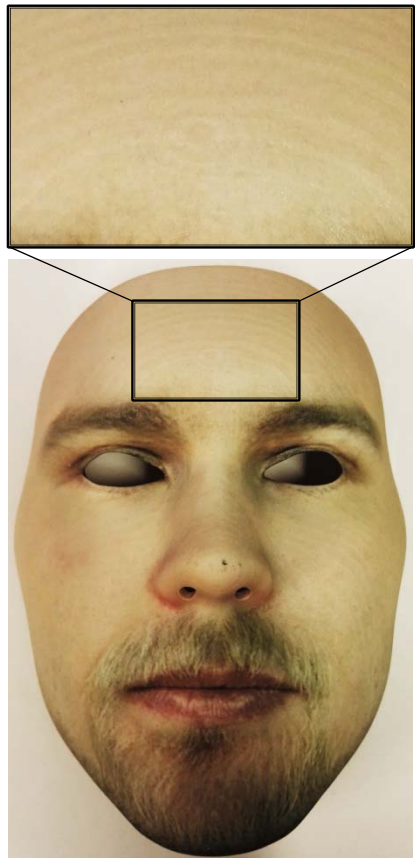
	REAL-F			
Method	HTER(%)	EER(%)	FPR (FNR=0.1	FPR (FNR=0.01)
Pulse (ours)	**4.29**	**1.58**	**0.25**	**3.83**
LBP-blk	26.3	25.08	37.92	48.25
LBP-blk-color	25.92	20.42	31.5	48.67
LBP-ms	39.87	46.5	59.83	73.17
LBP-ms-color	47.38	46.08	86.5	95.08

Analysis of Results

- Observations:
  - LBP-based texture method gives *zero error for 3DMAD* dataset but very *large error in REAL-F*
  - Global rPPG method (pulse) provides *very small errors in both 3DMAD and REAL-F datasets*



REAL-F



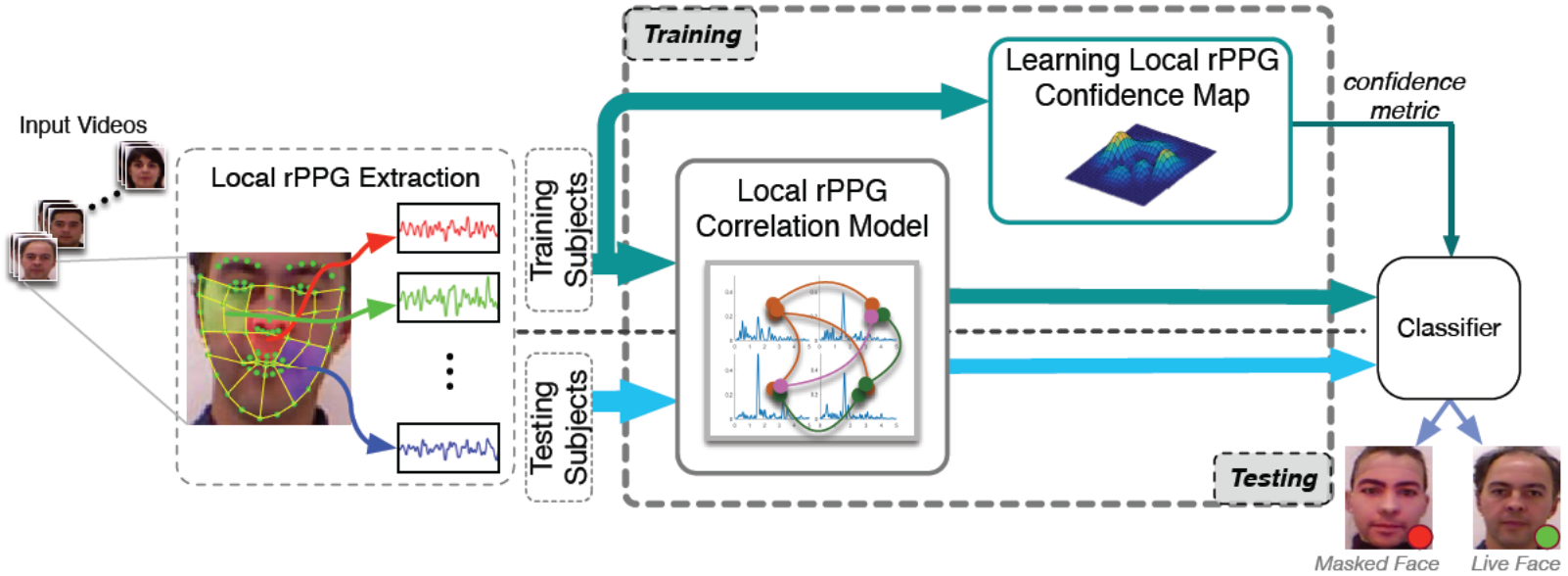
3DMAD

Limitations on Global rPPG method

- Global rPPG signal is sensitive to certain variations such as illuminations, head motion and video quality
- Global solution cannot provide structure information
- rPPG signal strength may vary along different subjects

How to increase the robustness of rPPG-based Face Anti-spoofing?

Proposed Local rPPG based Face Anti-Spoofing Method [ECCV 2016]

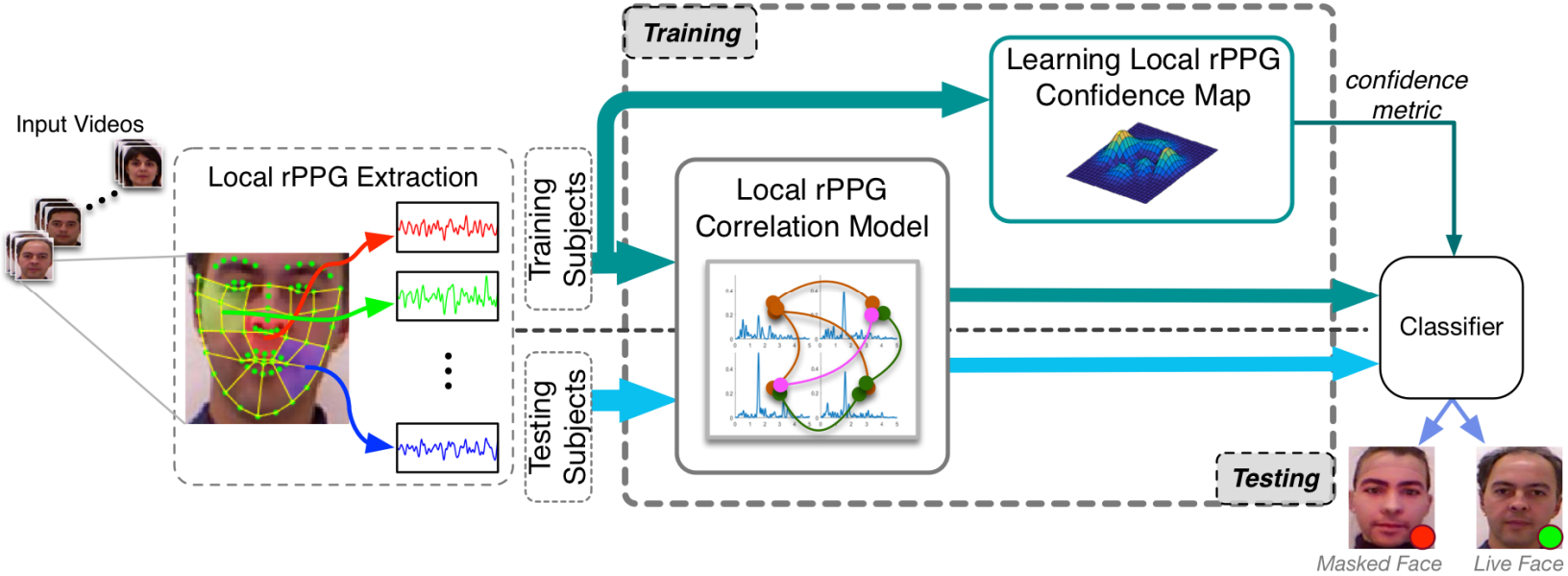


3D Mask Face Anti-spoofing with Remote Photoplethysmography

Siqi Liu, Pong C. Yuen, Shengping Zhang and Guoying Zhao

ECCV 2016

Local rPPG based Face Anti-Spoofing Method



(a) Local ROIs are pre-defined based on the facial landmarks. Local rPPG signals are extracted from these local face regions.

(b) Extract Local rPPG patterns through the proposed **local rPPG correlation model**.

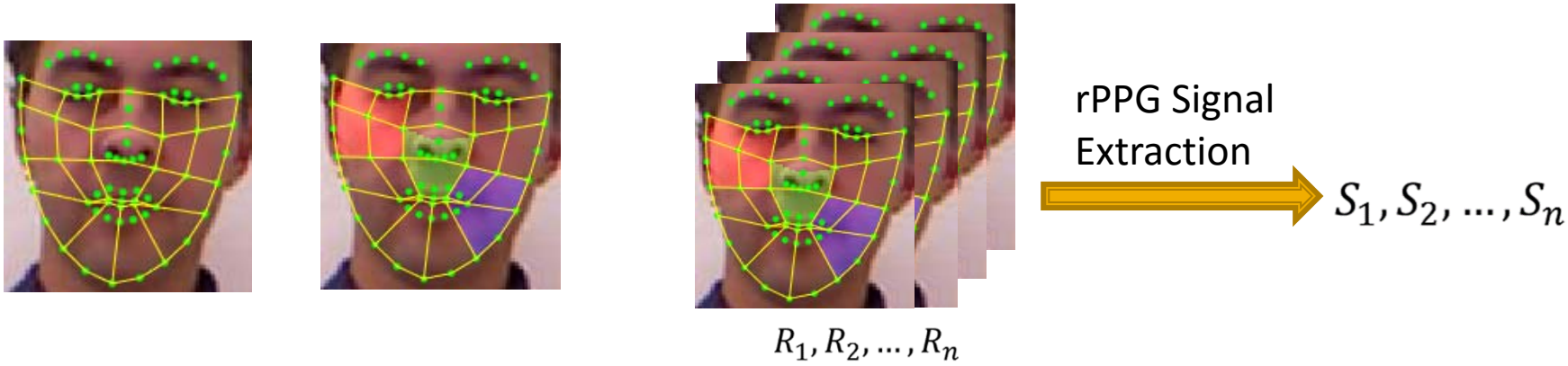
(c) Training stage: local rPPG confidence map is learned, and then transformed into distance metric for classification.

(d) Classifier: SVM

1. Local rPPG Signal Extraction

- (1) ROI detection and tracking
  - Landmark detection and tracking
  - Local ROIs are pre-defined based on the facial landmarks

- (2) rPPG Signal Extraction
  - We adopt (Haan et.al., TBE, 2013) method to extract rPPG signals.



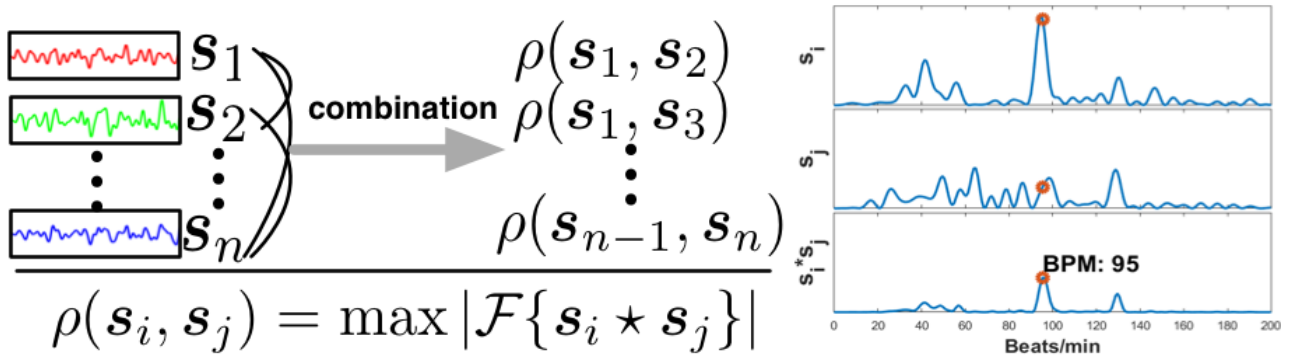
2. Local rPPG Correlation Model

- For genuine face, local rPPG signals should have high consistency
  - The heart rate signal is generated from the same source: **Heart Beat**
- For masked face, local rPPG signals should have a small frequency similarity and periodicity
  - For masked face, rPPG signal is blocked and only remain environmental noise.

We could minimize the effect of random noise and boost the vital rPPG through the cross-correlation of local rPPG.

2. Local rPPG Correlation Model

Similarity of all the possible combinations of local rPPG signals



Through the cross-correlation operation, we could filter out the shared heartbeat related frequency and reduce the effect of noise.

Meanwhile, signals from local masked face regions will suppress with each other with cross correlation, because they are random noise and do not share the same periodic frequency.

3. Learning Local rPPG Confidence Map

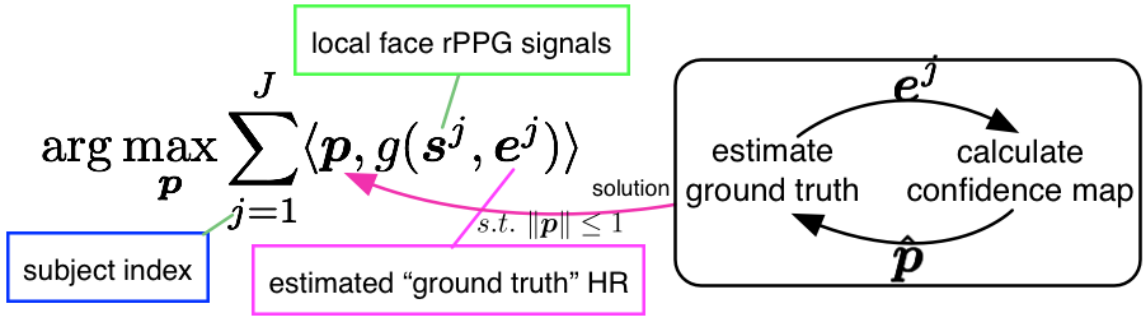
- Local rPPG correlation pattern may not be sufficient to handle noise in some cases
  - rPPG signals may be too weak in low quality video and concealed by noise
- rPPG signal strength varies along local face region with a stable spatial distribution

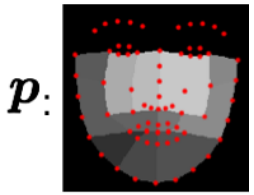
*We could learn a **local rPPG confidence map***

1. emphasizing the region with strong HR signal, and
2. weaken the unreliable region with pale HR signal.

3. Learning Local rPPG Confidence Map

- Given ***J*** training subjects, learn the local rPPG confidence map ***p*** which reflects the reliability of local face regions:





- Using local rPPG confidence map ***p*** to weight the distance metric in classifier

Experiments

- **Dataset**
- 3DMAD [TIFS'14 Erdogmus et.al]
  - 255 videos recorded from 17 subjects
  - Masks made from ThatsMyFace.com

- Supplementary (SUP) Dataset:
  - 2 Mask type: 8 subjects: ThatsMyFace (6), REAL-F (2)
  - Captured by WebCam Logitech C920 (1280*720 RGB)

Experiments

- Intra-database Experiment (***LOOCV***) [Erdogmus et al., TIFS'14]
  - Supplementary (SUP) Dataset
  - Combined (3DMAD+SUP) Dataset

- Cross-database Experiment
  - Train on 3DMAD, Test on SUP dataset
  - Train on SUP, Test on 3DMAD dataset

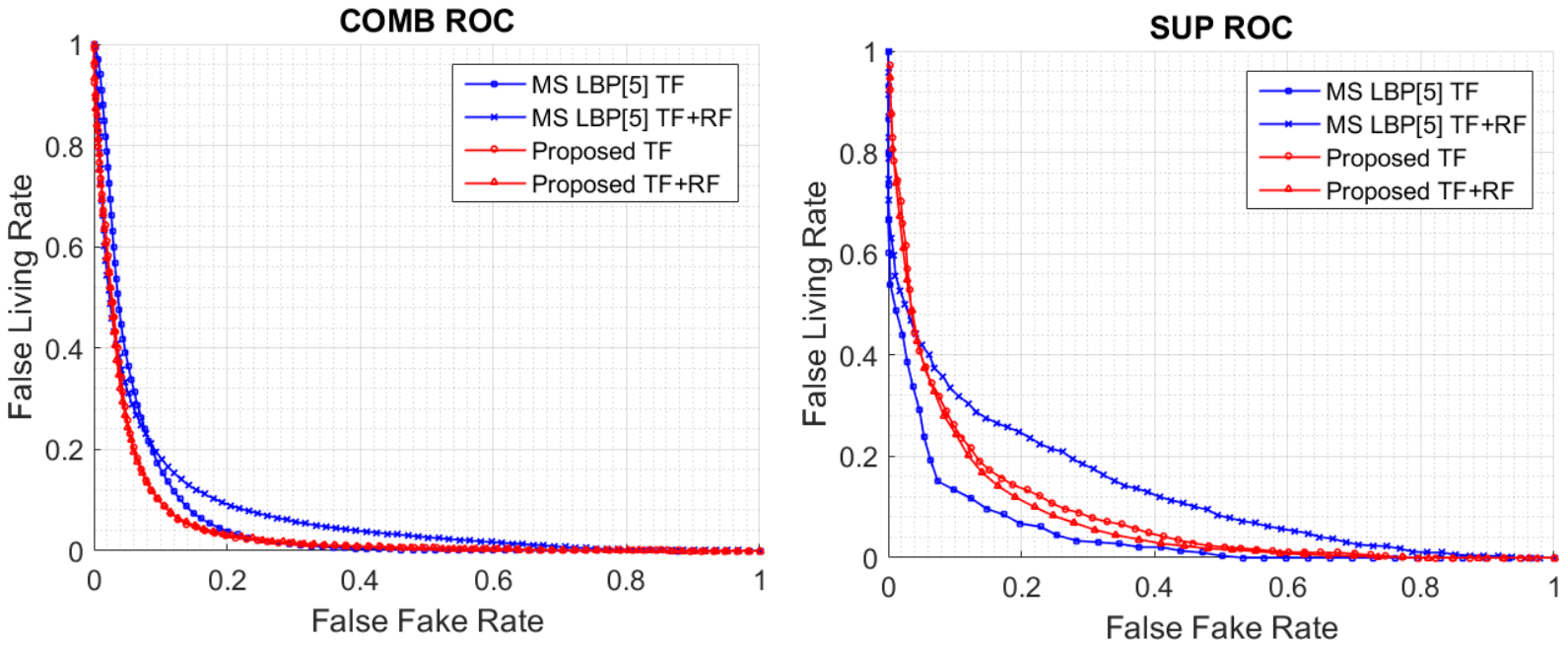
Experiment Results

- Intra-database experiments (***LOOCV***)

	COMB dataset			
	HTER_dev	HTER_test	EER	AUC
MS-LBP	13±6.3	13.8±19.4	13.6	92.8
Ours	**9.2±2.0**	**9.7±12.6**	**9.9**	**95.5**
	SUP dataset			
	HTER_dev	HTER_test	EER	AUC
MS-LBP	19.5±11.1	23.0±21.2	22.6	86.8
Ours	**13.5±4.7**	**14.7±10.9**	**16.2**	**91.7**

Experiment Results

- Intra-database experiments



•Appearance based method achieve good performance on ThatsMyFace mask. But performance drops on REAL-F mask

Experiment Results

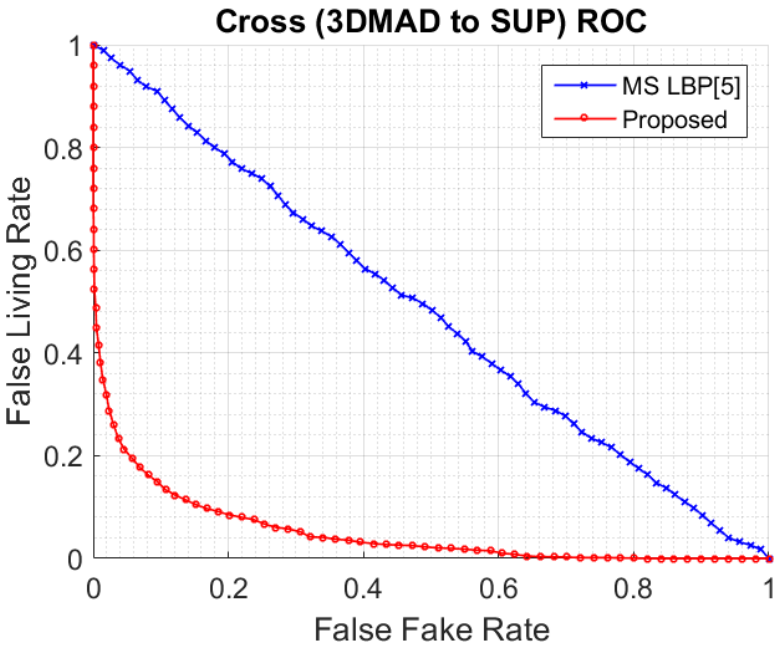
- Cross-database experiments

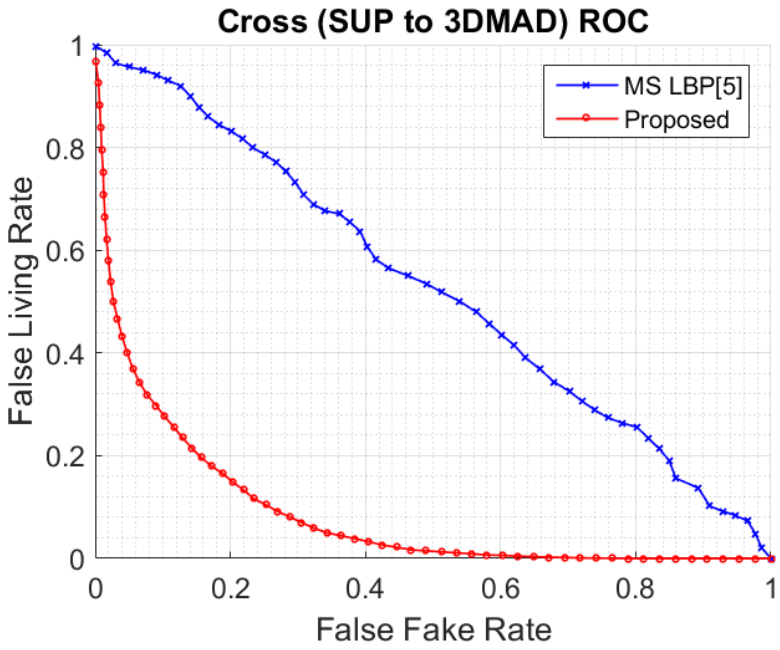
	3DMAD to SUP			SUP to 3DMAD		
	HTER	EER	AUC	HTER	EER	AUC
MS-LBP	46.5±5.1	49.2	51.1	64.2±16.7	51.6	47.3
Proposed	**11.9±2.7**	**12.3**	**94.9**	**17.4±2.4**	**17.7**	**91.2**

- Our proposed method is robust encountering the cross-database scenario
- The appearance based method exposes the aforementioned drawbacks in the cross-database scenario

Experiment Results

- Cross-database experiments

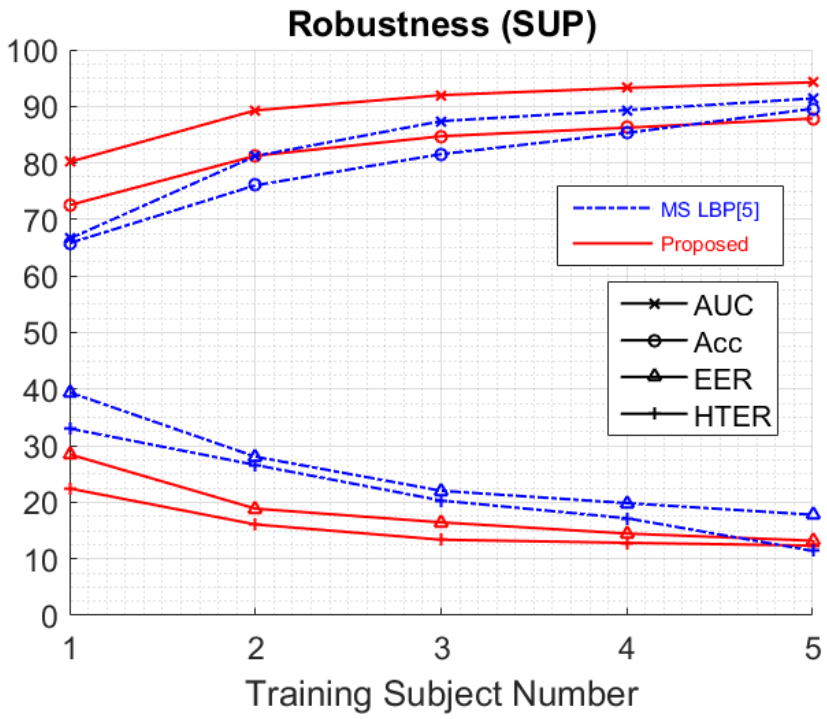


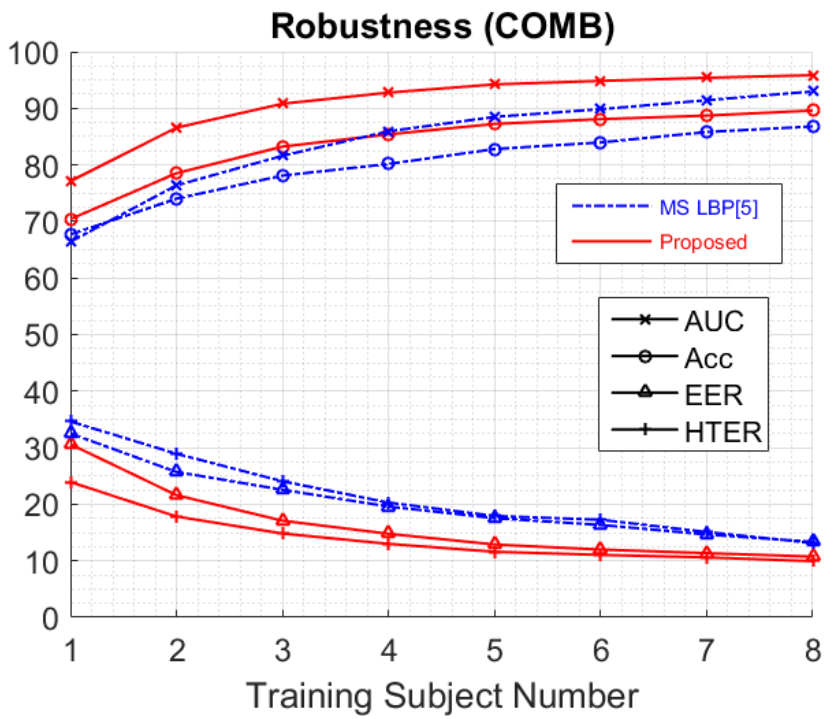


•Our proposed method is robust encountering the cross-database scenario
•Performance of appearance based method drops dramatically under cross-database scenario

Experiment Results

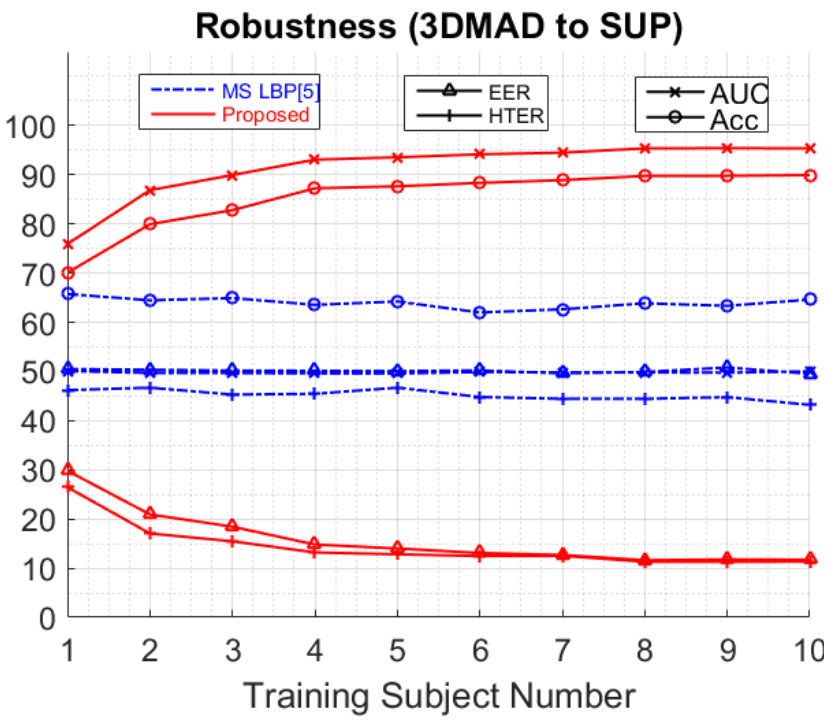
- Robustness experiments
  - Test with different number of training subjects
  - Intra-database:

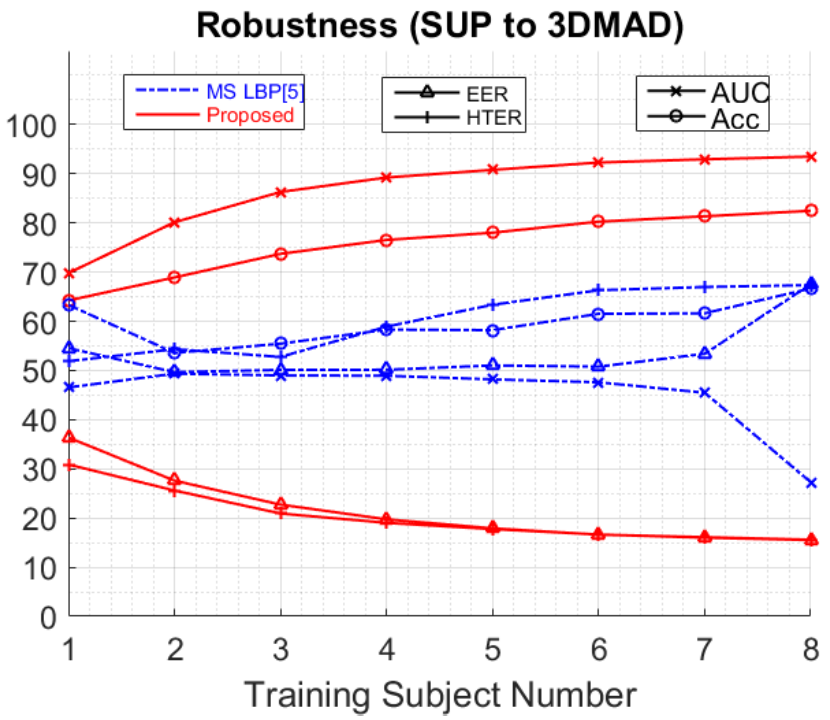




Experiment Results

- Robustness experiments
  - Cross-database:





Conclusion

- rPPG is a promising approach for face anti-spoofing against 3D mask
- We proposed a global and a local rPPG models for 3D mask face anti-spoofing and the results are encouraging.
- Still, a lot work needs to be done on improving the robustness on the variations, such as head motion, illuminations, video quality, pose and occlusion.

Conclusion

- Only one publicly available dataset: 3DMAD
- We created a new dataset: HKBU-MARs

  http://rds.comp.hkbu.edu.hk/mars

Thank you!

References (Face Template Protection)

- G. MAI, M H Lim and P C Yuen, Binary Feature Fusion for Discriminative and Secure Multi-biometric Cryptosystems, *Image and Vision Computing*, In press, 2016
- M H Lim and P C Yuen, Entropy Measurement for Biometric Verification Systems, *IEEE Transactions on Cybernetics*, 2016
- M H Lim, S Verma, G C Mai and P C Yuen, "Learning discriminability-preserving histogram representation from unordered features for multibiometric feature-fused template protection", *Pattern Recognition*, In press, 2016
- Y C Feng, M H Lim and P C Yuen, Masquerade attack on transform-based binary-template protection based on perceptron learning, *Pattern Recognition*, 2014
- YC Feng & PC Yuen, Binary discriminant analysis for generating binary face template, *IEEE Transactions on Information Forensics and Security*, 2012
- YC Feng, PC Yuen, AK Jain, A hybrid approach for generating secure and discriminating face template, *IEEE Transactions on Information Forensics and Security*, 2010

References (Face Anti-spoofing)

1. N. Erdogmus and S. Marcel, “Spoofing face recognition with 3d masks”, *TIFS*, 2014
2. J. Maatta, A. Hadid, and M. Pietikainen. “Face spoofing detection from single images using micro-texture analysis”, *IJCB*, 2011.
3. D. Wen, H. Han, and A. K. Jain, “Face spoof detection with image distortion analysis”, *TIFS*, 2015.
4. G. Pan, L. Sun, Z. Wu, and S. Lao. “Eyeblink-based antispoofing in face recognition from a generic webcamera”, *ICCV*, 2007.
5. T. de Freitas Pereira, J. Komulainen, A. Anjos, J. M. De Martino, A. Hadid, M. Pietikainen, and S. Marcel, “Face liveness detection using dynamic texture.”, *EURASIP JIVP*, 2014.
6. X. Li, J. Komulainen, G. Zhao, P. C. Yuen, and M. Pietikainen, “Generalized face anti-spoofing by detecting pulse from face videos”, *ICPR*, 2016.
7. S. Liu, P C. Yuen, S. Zhang, and G. Zhao, “3D Mask Face Anti-spoofing with Remote Photoplethysmography” , *ECCV*, 2016.
8. S. Liu, B. Yang, P C. Yuen, G. Zhao, “A 3D Mask Face Anti-spoofing Database with RealWorld Variations” , *CVPRW*, 2016.