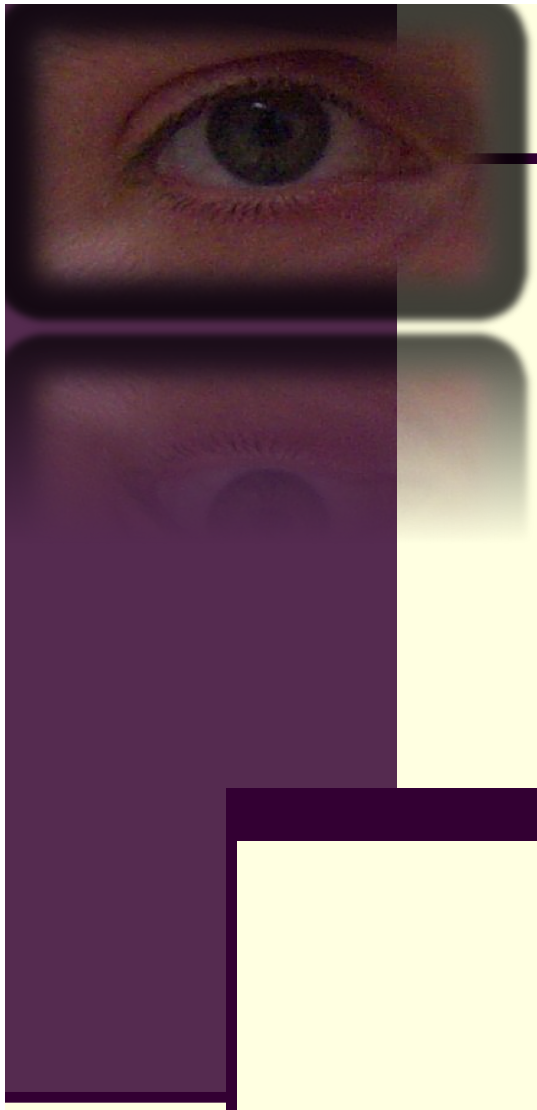


Recent Progress in Biometrics

Arun Ross

Associate Professor

Michigan State University

rossarun@cse.msu.edu

http://www.cse.msu.edu/~rossarun

A Question of Identity

- Who is this person?

About 704 results (0.61 seconds)

Image size:
464 × 594

Find other sizes of this image:
All sizes - Small - Medium

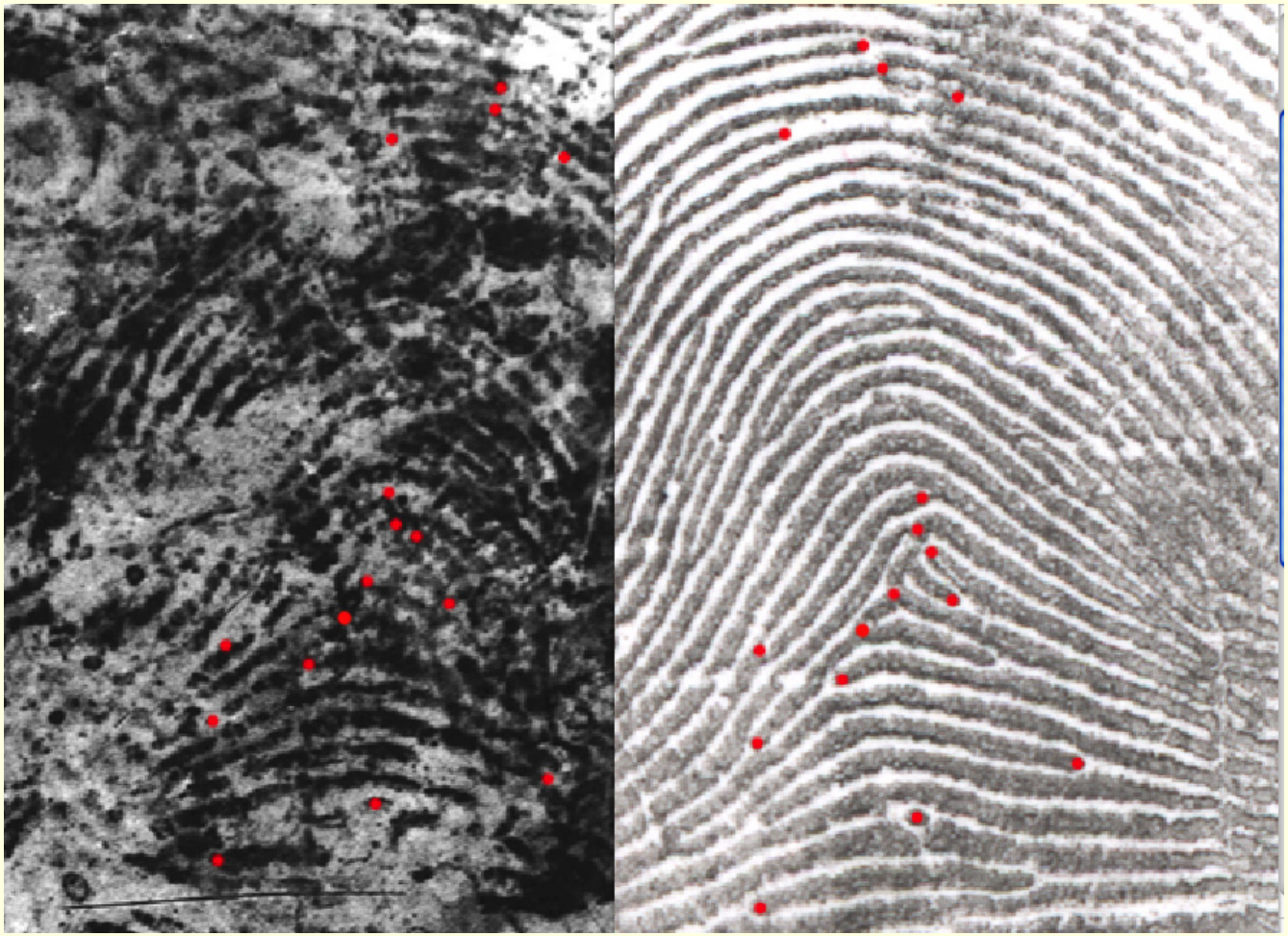
Best guess for this image: ***harrison ford young***

Visually similar images

Report images

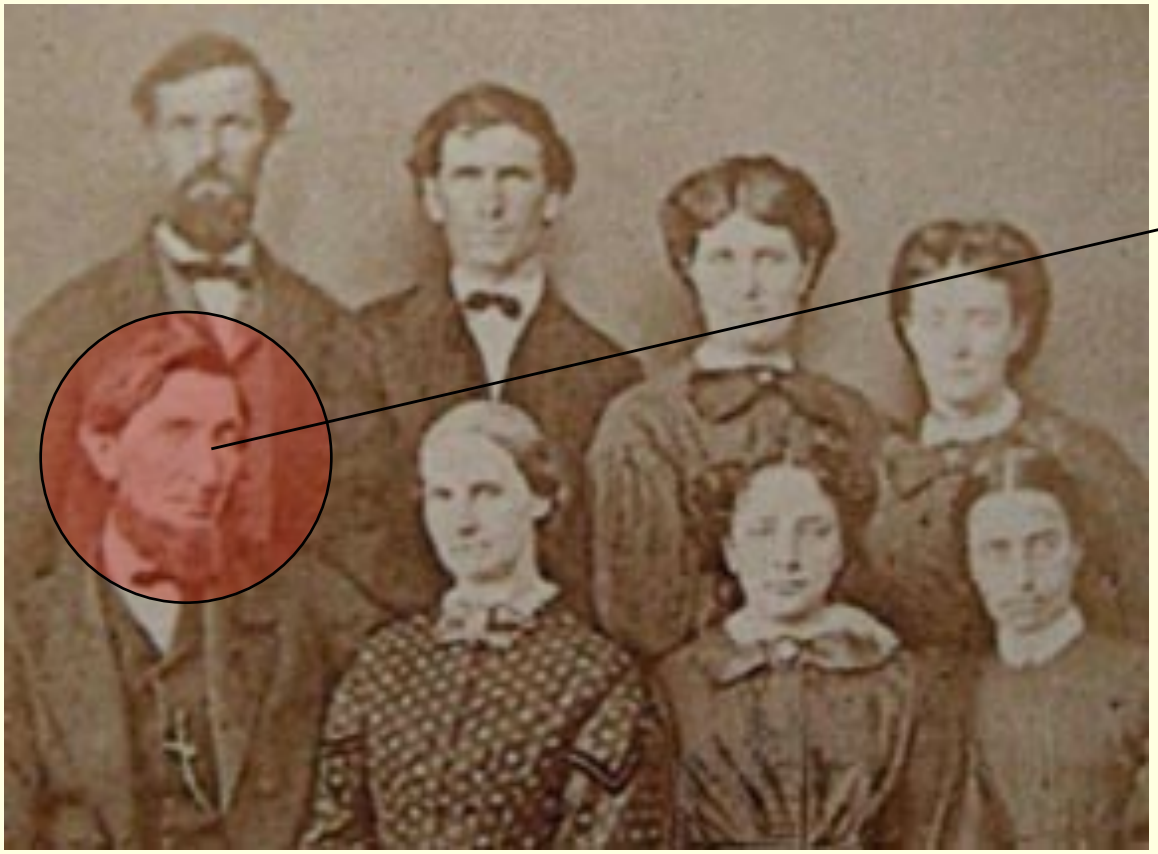
A Question of Identity

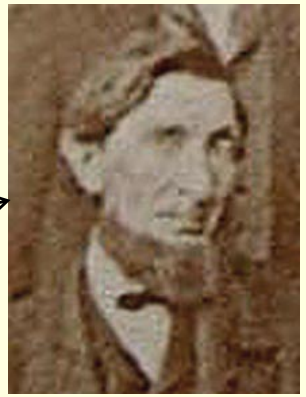
- Are these two prints from the same finger?

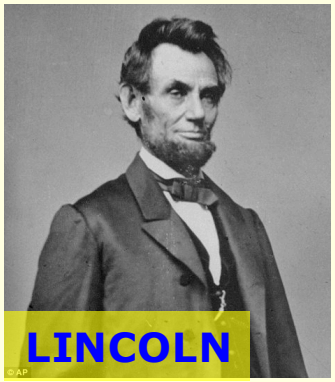


A Question of Identity

- Is this really a photograph of Abraham Lincoln?







?

A Question of Identity

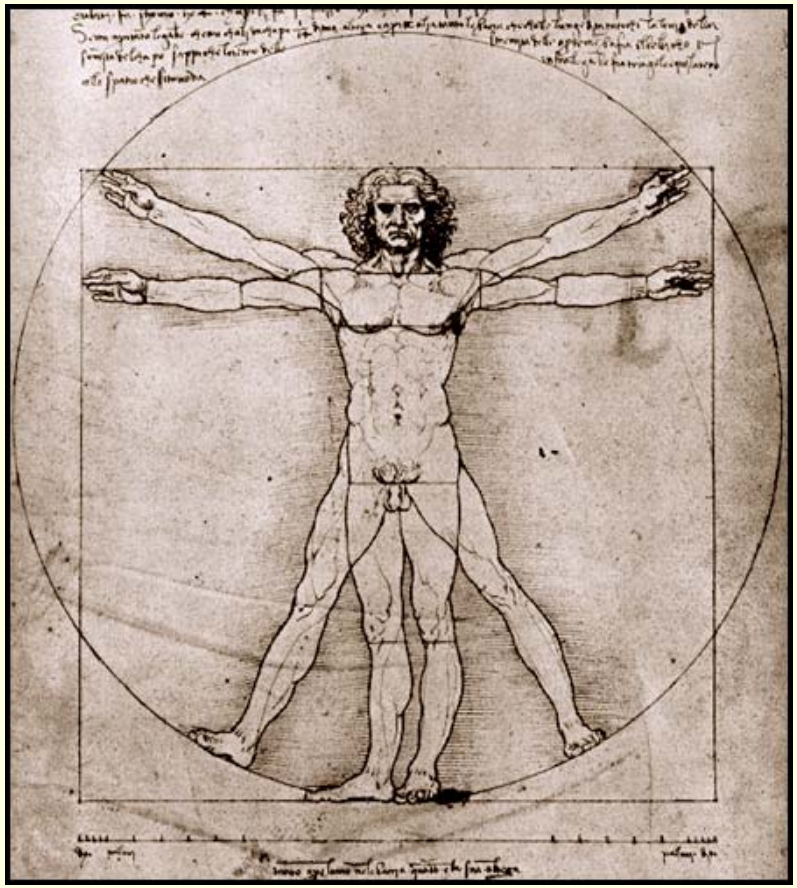
- Find all video frames in which Odette appears

A Question of Identity

- Is he the owner of this smart phone?

Biometric Recognition

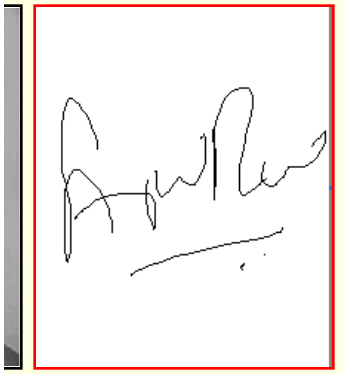
- Automated recognition of individuals based on their biological and behavioral characteristics
- Biological and behavioral characteristic of an individual from which distinguishing, repeatable biometric features can be extracted

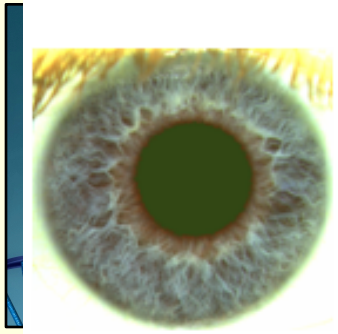


Biometric Traits

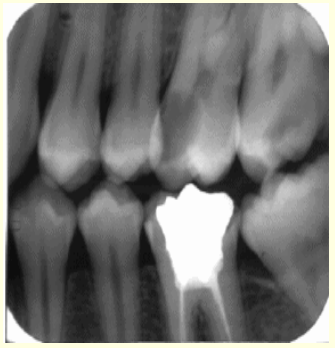


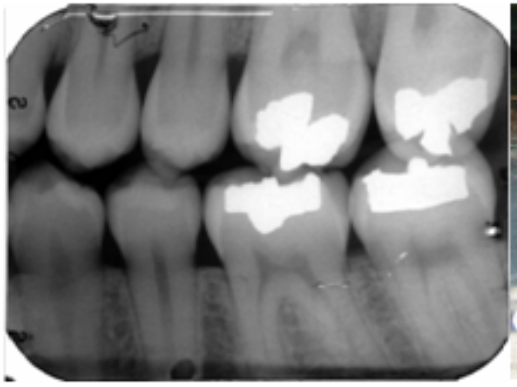


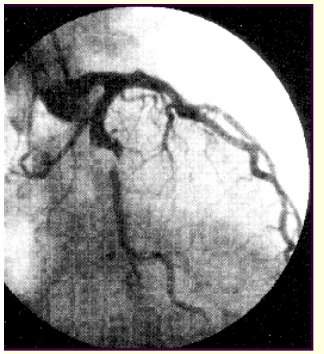






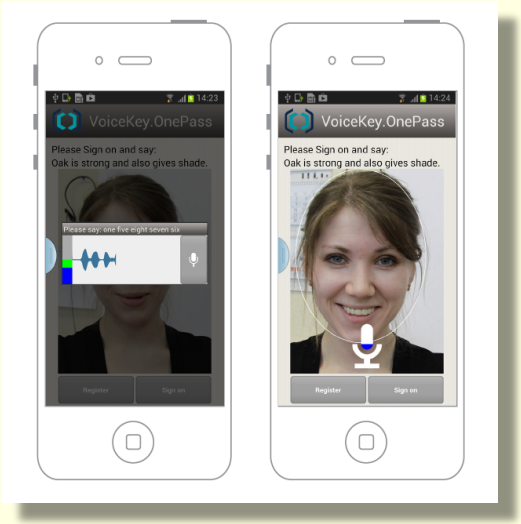




Biometric Applications

Iris: Frankfurt Airport

Fingerprint: US OBIM



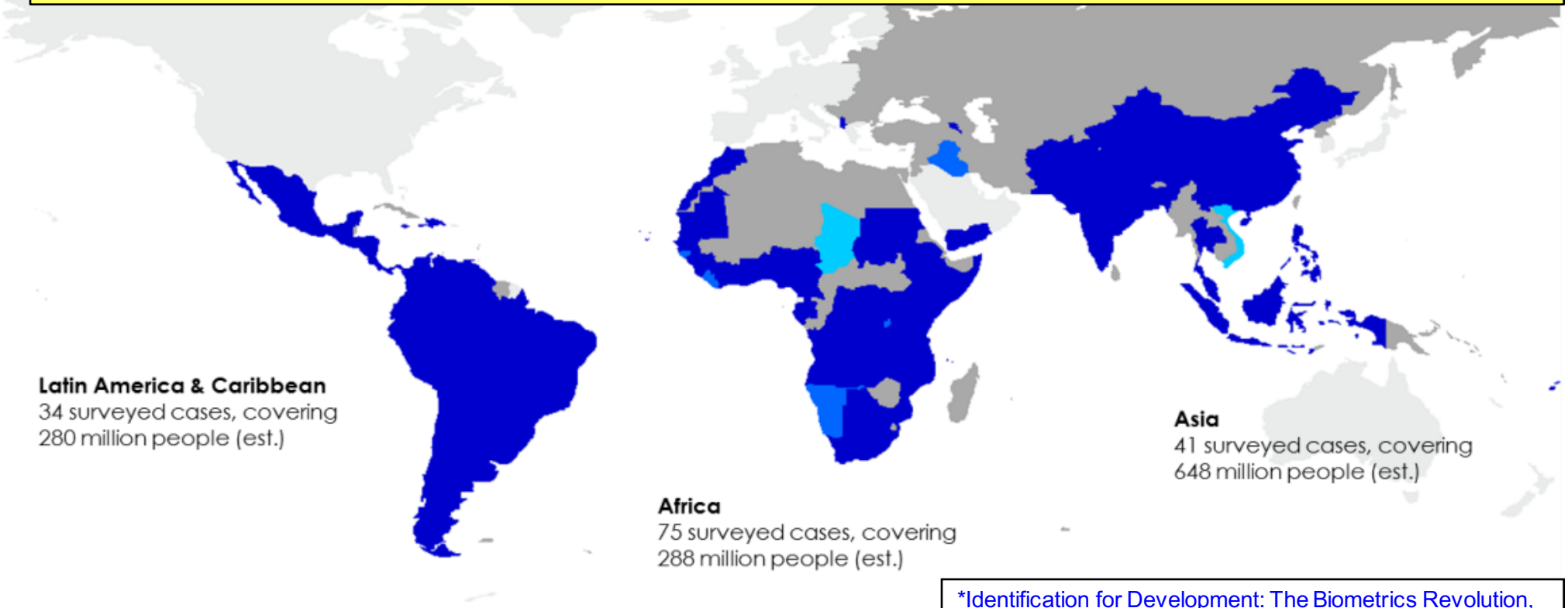
Face + Voice: Voice Key.OnePass

Fingerprint: Privaris Key Fob

Finger Vein: Japan ATMs

The Biometrics Revolution

Over 1 billion people have been covered by biometric identification programs in the Low Middle Income Countries



*Identification for Development: The Biometrics Revolution, A. Gelb and J. Clark, Center for Global Development, NW, Washington DC, Working Paper 315, Jan. 2013, http://www.cgdev.org/sites/default/files/1426862_file_Biometric_ID_for_Development.pdf

Identity vs Recognition

- We do not necessarily want to elicit identity
- We want to recognize a person

INPUT

Based on a single fingerprint image, we cannot say this belongs to *Jane Doe*

REFERENCE

We need a reference fingerprint image that is known to belong to *Jane Doe* in order to make this assessment

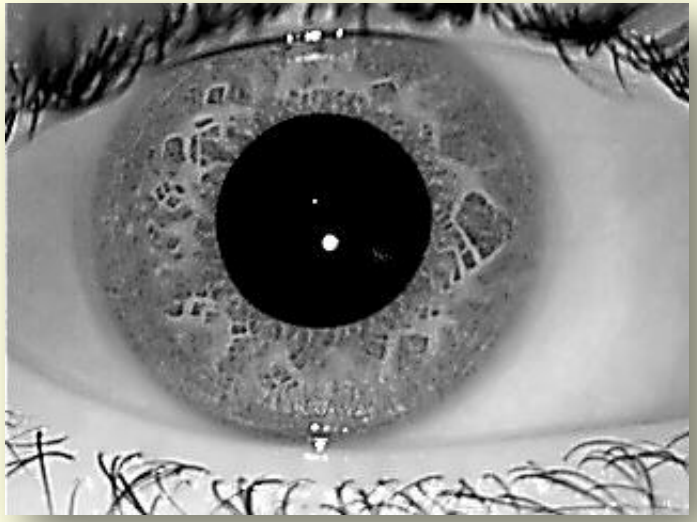
Information from a Single Image

- Gender
- Age
- Ethnicity
- Medical ailment
- Familial relation
- Name/PIN

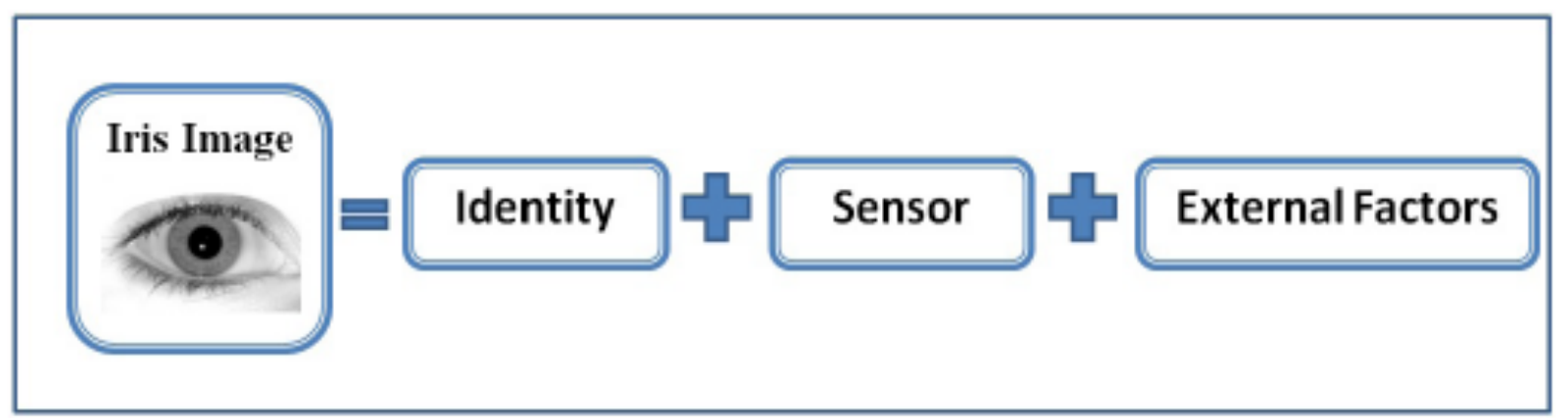
Dantcheva, Elia, Ross, "What Else Does Your Biometrics Data Reveal? A Survey on Soft Biometrics," TIFS 2016

What else is revealed in an iris image?

- Biographical:
  - Age, Gender, Race
- Anatomical:
  - Distribution of crypts, Wolfflin nodules, pigmentation spots
- Environmental:
  - Sensor, Illumination wavelength, Indoor/Outdoor
- Pathological:
  - Stromal Atrophy
- Other:
  - Pupil dilation level, Contact Lens



Determining Sensors from Images

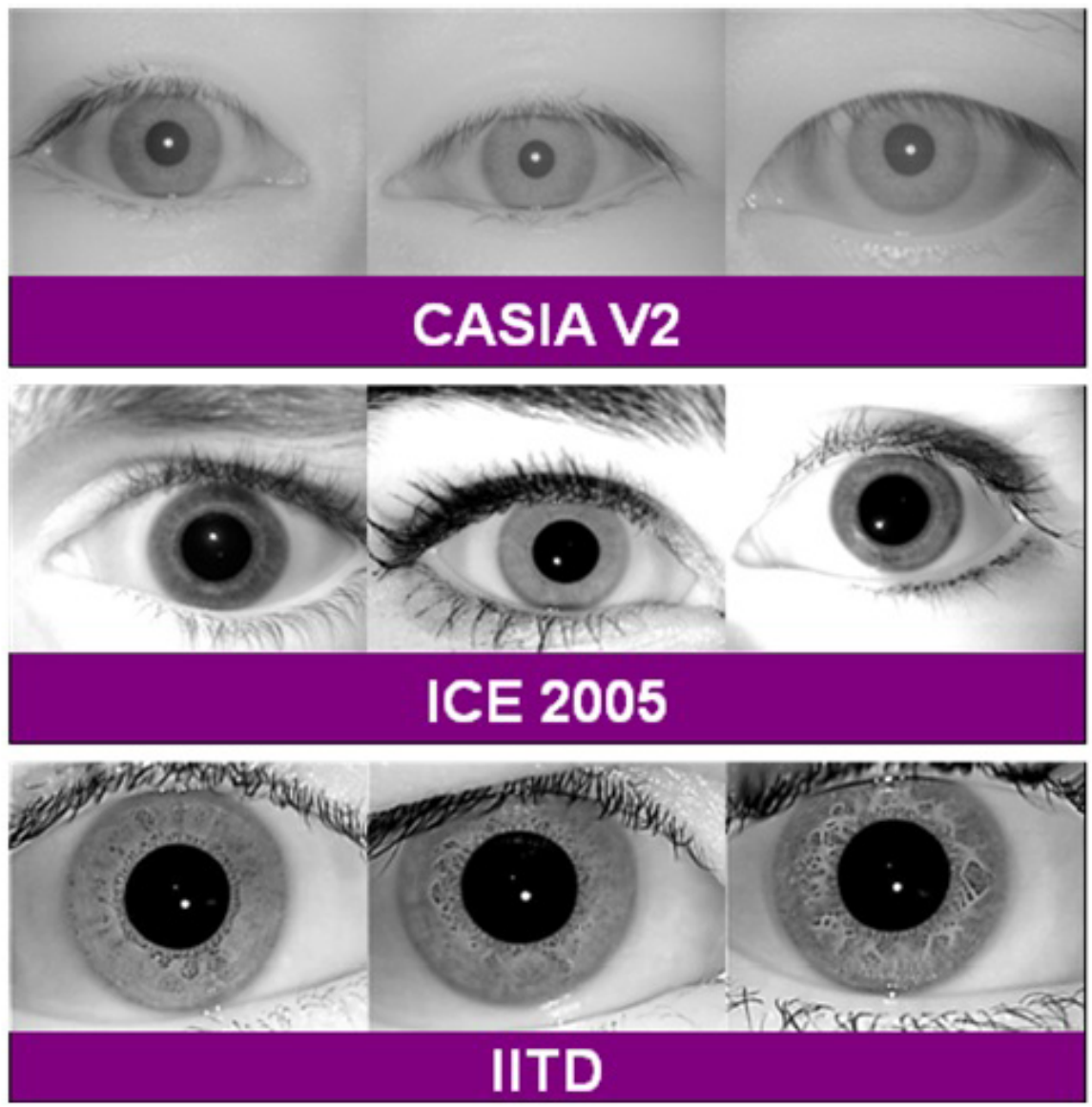


Kalka, Bartlow, Cukic, Ross, "A Preliminary Study on Identifying Sensors from Iris Images," CVPRW 2015

Actual \ Classified	ICE-LG	WVU-OKI	WVU-EverFocus	CASIAv3-OKI	CASIAv3$_p$	CASIAv2-OKI	CASIAv2$_p$
ICE-LG	1680	0	0	0	0	0	0
WVU-OKI	0	1680	0	0	0	0	0
WVU-EverFocus	9	0	1661	0	0	10	0
CASIAv3-OKI	0	0	0	1665	0	15	0
CASIAv3$_p$	103	155	47	210	1009	82	74
CASIAv2-OKI	0	0	0	0	0	1680	0
CASIAv2$_p$	0	0	0	0	0	0	1680

- **Classification accuracy is ~90%**

Determining Data Source



Which Dataset is this Image From?

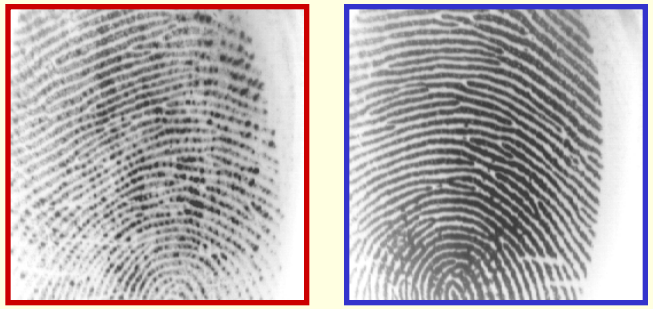
- **Classification accuracy ranged from 70% to 82%**

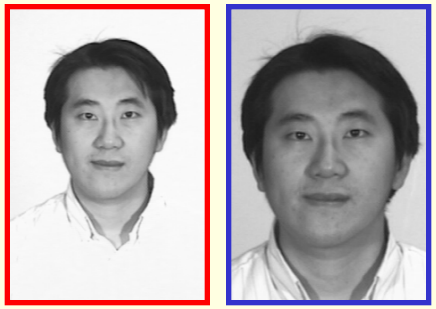
El Naggar, Ross, "Which Dataset is this Iris Image From?" WIFS 2015

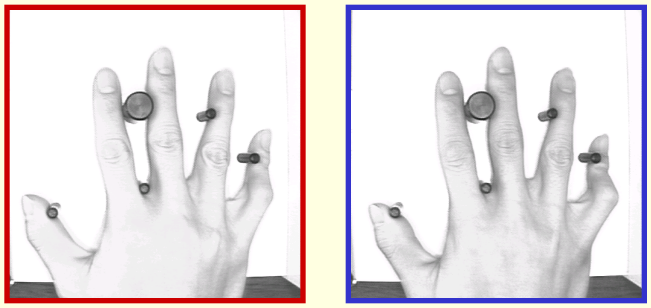
Dataset	MBGC	CASIA V3	UPOL	UBIRIS	WVU	IITD	ICE	CASIA V2
MBGC	174	0	0	7	2	1	4	4
CASIA V3	0	185	0	0	1	0	1	5
UPOL	3	1	164	18	1	0	3	2
UBIRIS	5	0	19	162	2	0	4	0
WVU	4	5	5	2	156	5	6	9
IITD	0	0	0	0	0	192	0	0
ICE	26	0	25	13	15	7	105	1
CASIA V2	23	5	0	7	34	2	1	120

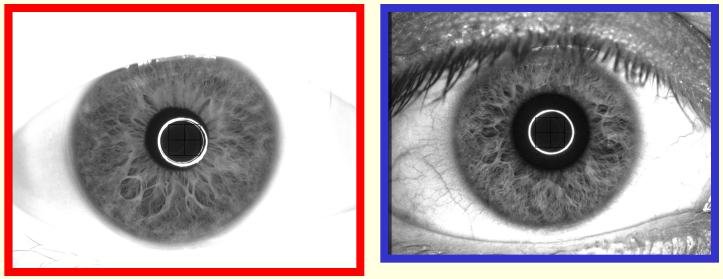
Biometric Matching

- Compute the similarity between two instances of biometric data



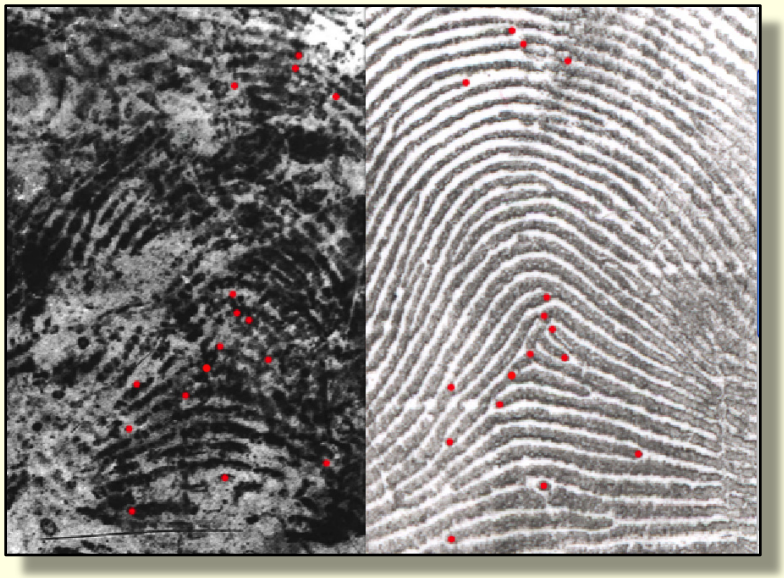


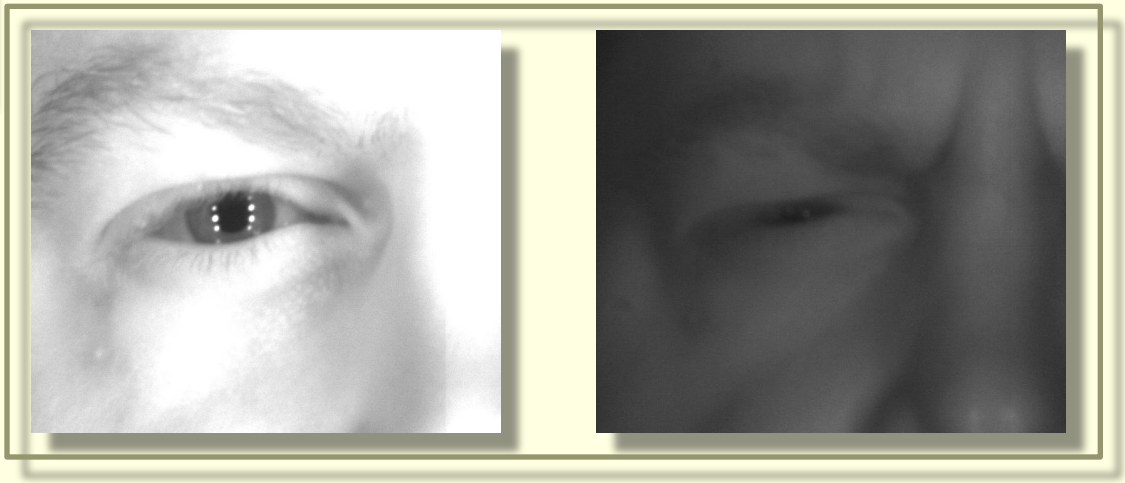




Real-world Matching

- Compute the similarity between two instances of biometric data corrupted by noise

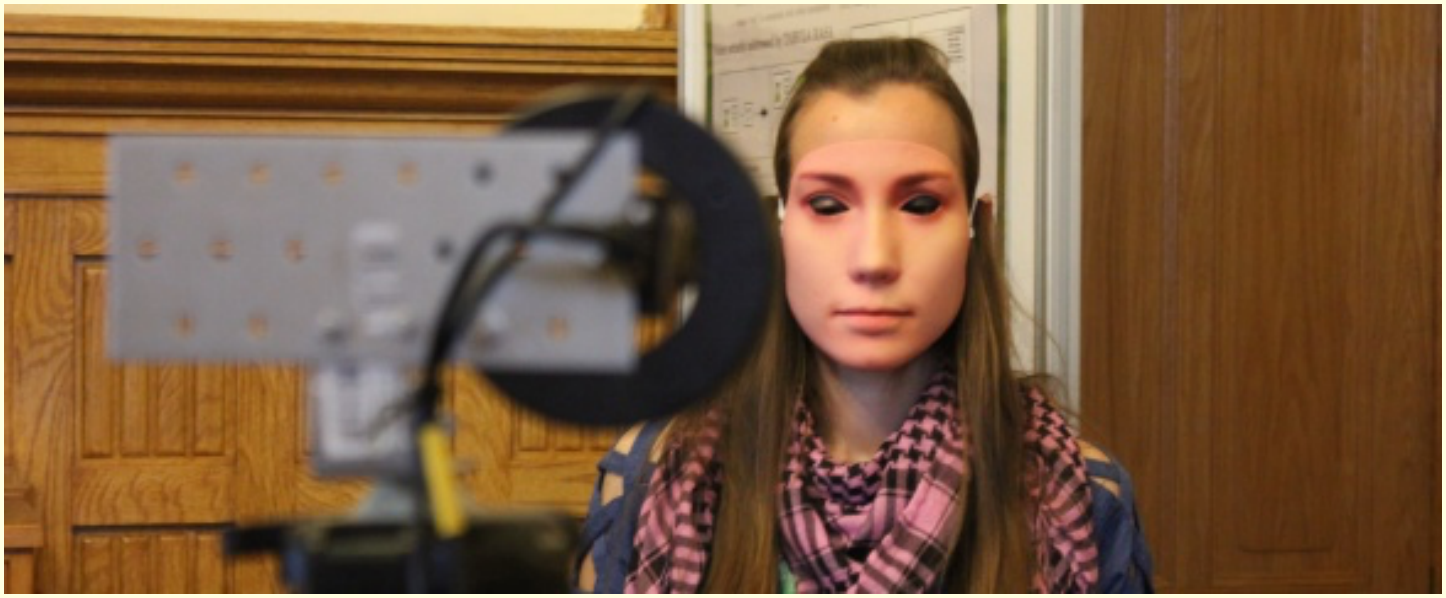




Beyond Pattern Recognition

- Ensuring that the input data is real and from a live person
- Protecting the biometric templates in the database
- Ensuring the privacy of an individual

Detecting Fake Faces and Fingers



Images from https://www.idiap.ch/dataset/3dmad

Current Research

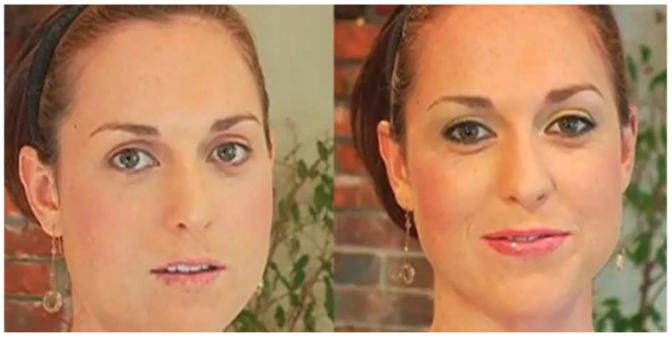
- MultiBiometrics:
  - Scores + Quality + Liveness Value
  - Biometrics + Biography
- Fingerprints:
  - Spoof Detection
  - TouchDNA
- Ocular Biometrics:
  - Image Forensics
  - Pupil Dilation
  - Mobile Phones/Periocular Biometrics
  - Soft Biometrics
- Face:
  - Hetergeneous Face Recognition
  - Privacy

Heterogeneous Face Recognition

Photo vs Sketch

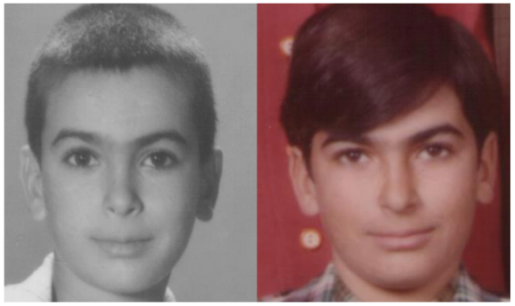
Fundamental Differences in Image Formation Characteristics

Before vs After Makeup



RGB vs NIR vs THM

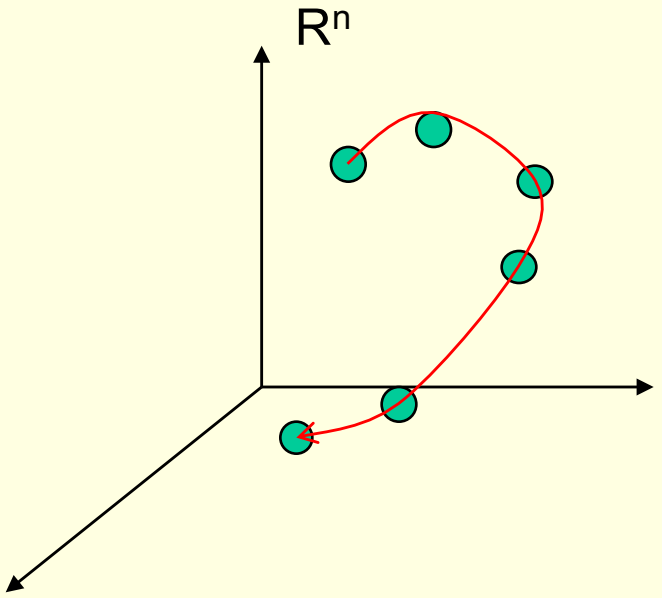
Young vs Old



2D vs 3D

“Simple” intra-user variations

- FNMR: False Non-Match Rate

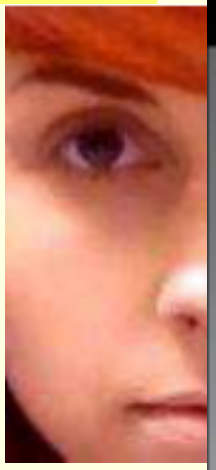


Changes Due to Illumination

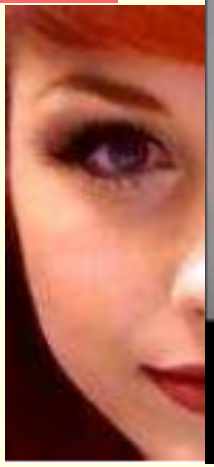
nachoguzman.net

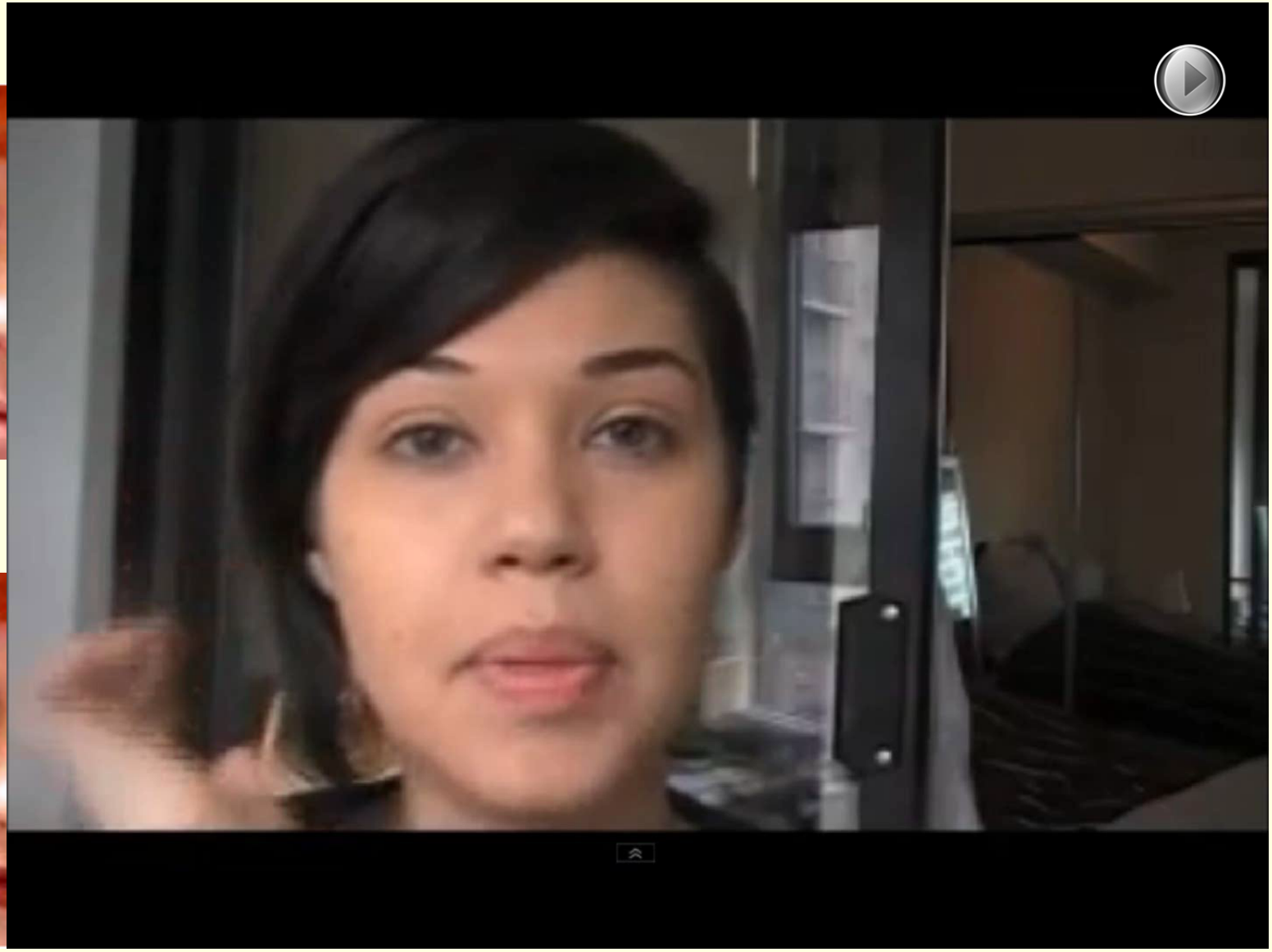
Before and After Makeup

BEFORE



AFTER





Dantcheva, Chen Ross, "Can Facial Cosmetics Affect the Matching Accuracy of Face Recognition Systems?," BTAS 2012

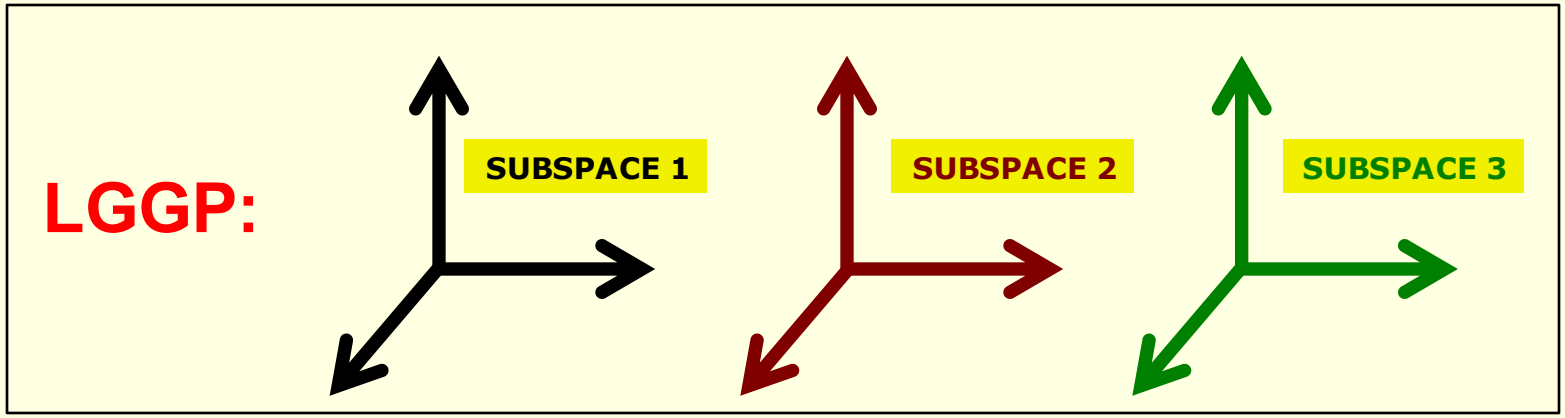
Patch-based Semi-Random Subspaces

- Encode the image using LGGP/HGORM/DS-LBP
- For each encoding scheme: generate multiple common subspaces
- Each subspace: generated from a semi-random set of patches extracted from encoded images

Chen, Dantcheva, Ross, "An Ensemble of Patch-based Subspaces for Makeup-Robust Face Recognition", Information Fusion, 2016

Matching: SRC and CRC Classifiers

- Two types of classifiers are used: Sparse Representation Classifier (SRC) and Collaborative Representation Classifier (CRC)
- Coefficient vectors of SRC and CRC are fused



$$\text{SRC:}\quad \varrho_1 + \varrho_2 + \varrho_3$$

$$\text{CRC:}\quad \pi_1 + \pi_2 + \pi_3$$

$$\psi_{LGGP}$$

Chen, Dantcheva, Ross, "An Ensemble of Patch-based Subspaces for Makeup-Robust Face Recognition", Information Fusion, 2016

Results of Proposed Method

- Method outperformed a number of academic face recognition algorithms and two COTS face matchers on the YouTube Makeup (YMU) dataset
- Its performance was comparable with a third COTS face matcher
- When fused with COTS, performance of the proposed method further improved

Chen, Dantcheva, Ross, "An Ensemble of Patch-based Subspaces for Makeup-Robust Face Recognition", Information Fusion Journal, 2016

Thermal versus Visible

VISIBLE

THERMAL

Cascaded Subspace Learning

- Filter images using CSDN/GIST/SQI
- Encode each patch using PSIFT/PHOG descriptor
- Select random set of patches from filtered images
  - Apply whitening transform to resulting feature vectors
  - Perform Hidden Factor Analysis (HFA)
  - Generate a common subspace based on the identity factor of HFA
- Multiple subspaces generated

Chen and Ross, "Matching Thermal to Visible Face Images Using Hidden Factor Analysis in a Cascaded Subspace Learning Framework," Pattern Recognition Letters, 2016

Hidden Factor Analysis (HFA)

- Face feature vector, t, is written as:

$$t = \beta + Ux + Vy + \epsilon$$

mean vector

subspace of cross-identity variation

latent identity factor

subspace of cross-spectral variation

latent spectrum factor

- The following parameters have to be estimated:

$$\Theta = \{\beta, U, V, \sigma^2\}$$

*** Gong et al, "Hidden Factor Analysis for Age Invariant Face Recognition." ICCV 2013**

EM Algorithm: Parameter Estimation

- Likelihood function is written as:

$$L_c = \sum_{i,k} \log p_\Theta(\boldsymbol{t}_i^k, \boldsymbol{x}_i, \boldsymbol{y}_k)$$

identity **spectrum**

- The following function is maximized:

$$\sum_{i,k} \int p_{\Theta_0}(\boldsymbol{x}_i, \boldsymbol{y}_k | T) \log p_\Theta(\boldsymbol{t}_i^k, \boldsymbol{x}_i, \boldsymbol{y}_k) d\boldsymbol{x}_i \boldsymbol{y}_k$$

*** Gong et al, "Hidden Factor Analysis for Age Invariant Face Recognition." ICCV 2013**

Extracting Identity Factor

- The identity factor can be computed as:

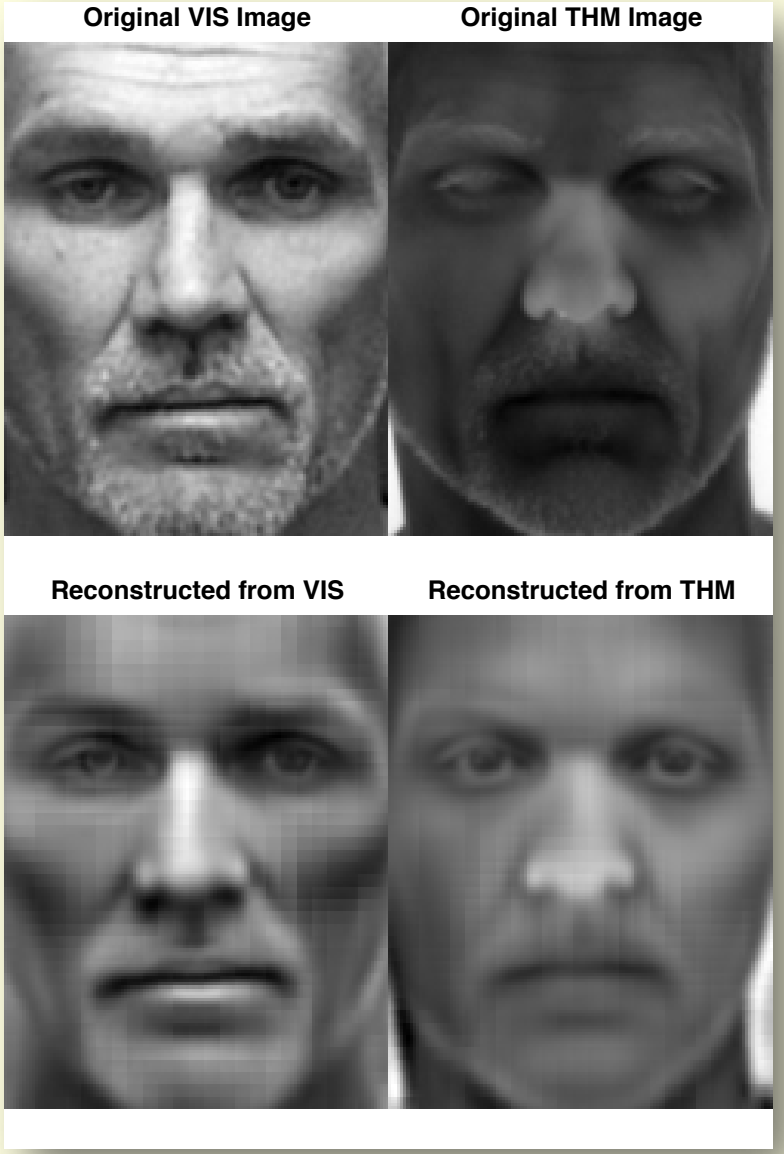
$$\boldsymbol{x} = \boldsymbol{U}\boldsymbol{U}^T\boldsymbol{\Sigma}^{-1}(\boldsymbol{t} - \boldsymbol{\beta})$$

where,

$$\boldsymbol{\Sigma} = \sigma^2\boldsymbol{I} + \boldsymbol{U}\boldsymbol{U}^T + \boldsymbol{V}\boldsymbol{V}^T$$

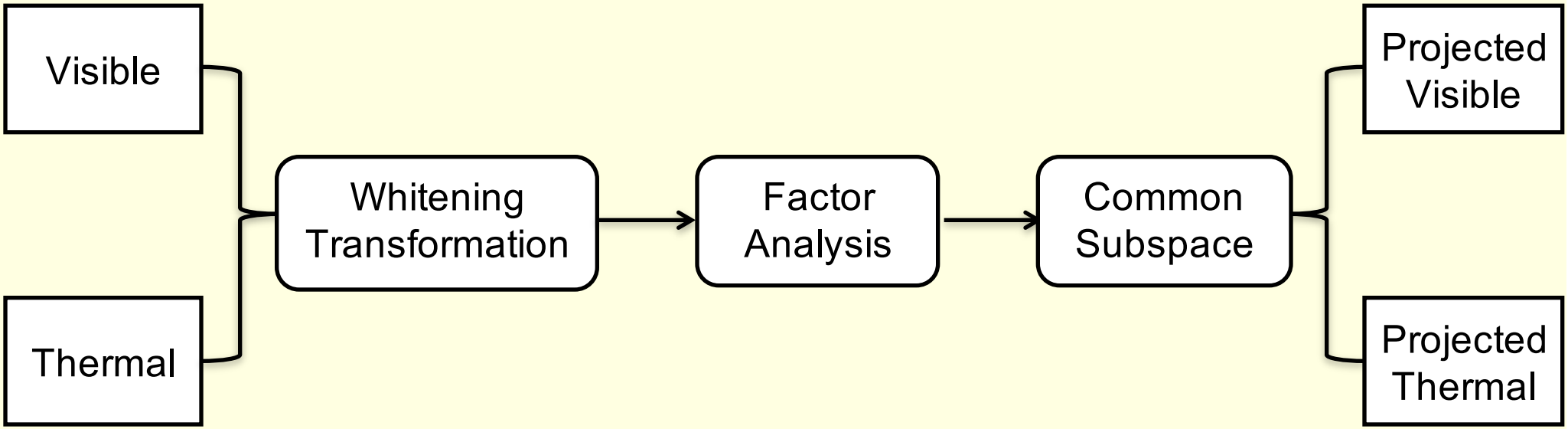
*** Gong et al, "Hidden Factor Analysis for Age Invariant Face Recognition." ICCV 2013**

The Identity Factor (on original image)



Chen and Ross, "Matching Thermal to Visible Face Images Using Hidden Factor Analysis in a Cascaded Subspace Learning Framework," Pattern Recognition Letters, 2016

Schematic of Proposed Method



- There are multiple common subspaces (different sets of random patches)
- In each subspace, Euclidean Distance matching scheme is used
- PSIFT and PHOG methods are combined using score-level fusion

Chen and Ross, "Matching Thermal to Visible Face Images Using Hidden Factor Analysis in a Cascaded Subspace Learning Framework," Pattern Recognition Letters, 2016

Results of Proposed Method

- Method outperformed all state-of-the-art matchers on the PCSO dataset (1003 subjects) both in terms of rank-1 accuracy and true accept rate at 1% false accept rate

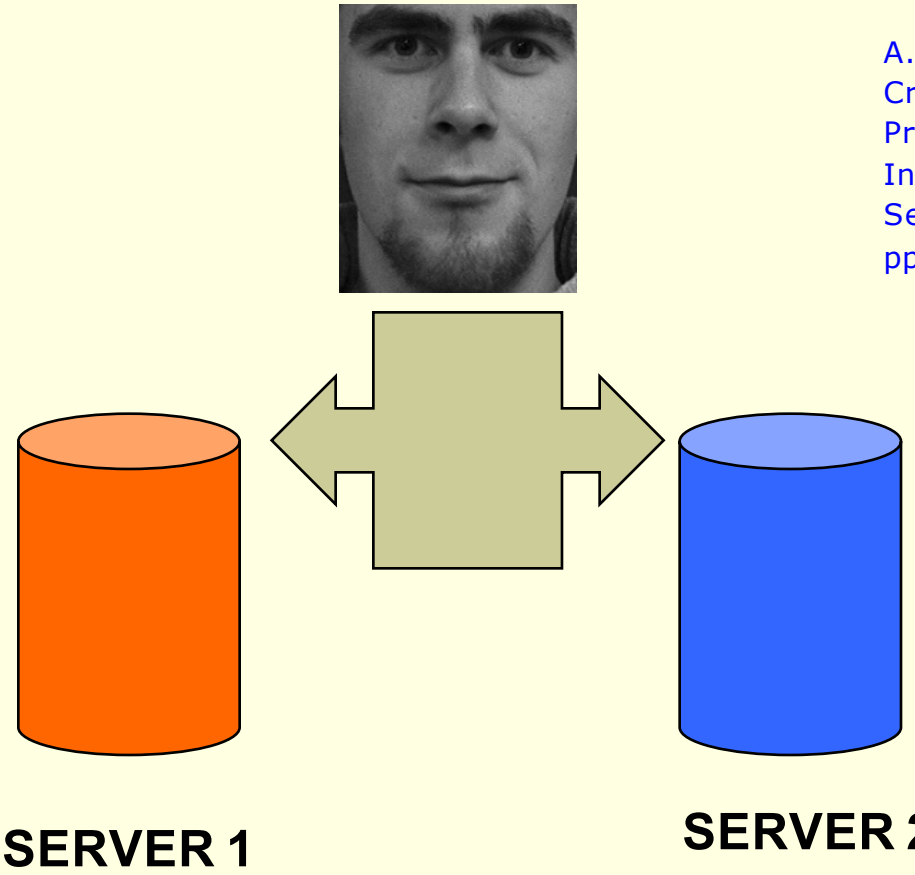
Chen and Ross, "Matching Thermal to Visible Face Images Using Hidden Factor Analysis in a Cascaded Subspace Learning Framework," Pattern Recognition Letters, 2016

Biometric Privacy

- Biometric data of an individual is sometimes stored in a central database
- Raises issues related to security and privacy of biometric data
  - Unlike compromised passwords, it is difficult to re-issue biometric data
  - Cross-database matching may be done to track individuals
  - Biometric data mining may be performed to glean information about identity

Proposed Strategy

- The input image is decomposed and stored in two separate servers: either server will be unable to deduce original identity



A. Ross and A. Othman, "Visual Cryptography for Biometric Privacy," IEEE Transactions on Information Forensics and Security (TIFS), Vol. 6, Issue 1, pp. 70 - 81, March 2011.

Visual Cryptography*

- Given an original binary image *T*, it is encrypted in *n* images, such that:

$$T = S_{h_1} \oplus S_{h_2} \oplus S_{h_3} \oplus \ldots \oplus S_{h_k}$$

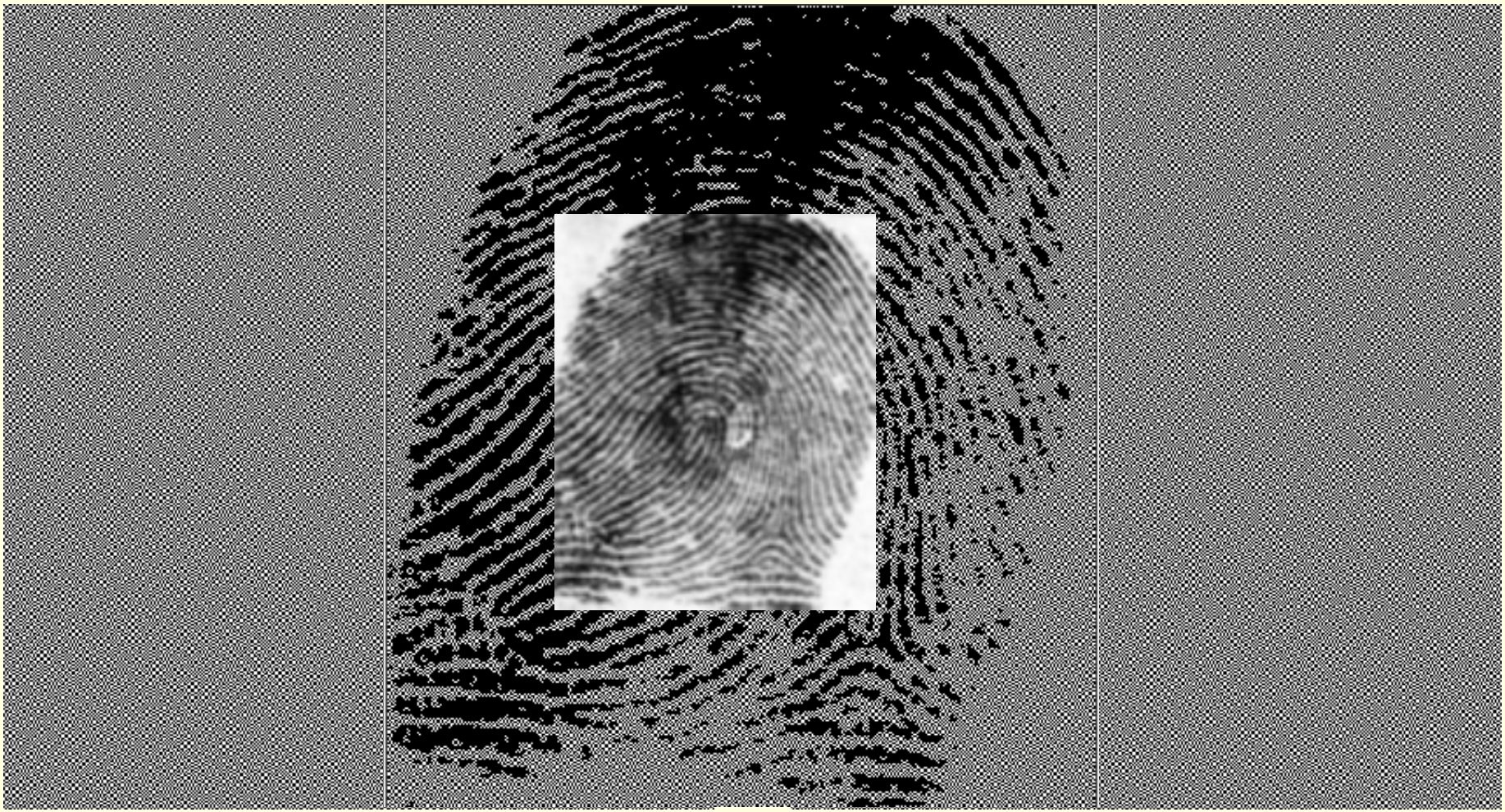
where $\oplus$ is a Boolean operation , S_{hi} is an image which appears as noise, $k \leq n$, and *n* is the number of noisy images

- This is referred to as *k-out-of-n* VCS

*** M. Naor and A. Shamir, "Visual cryptography," in EUROCRYPT, pp. 1–12, 1994**

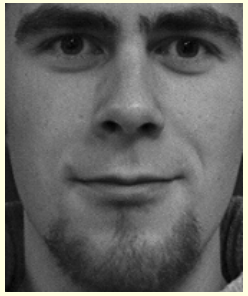
Sharing a secret image: Binary

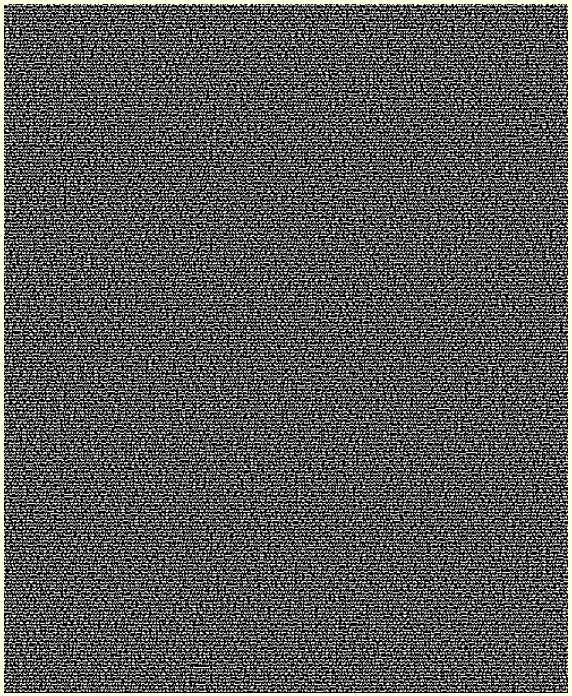
- Decomposing a fingerprint into two random images

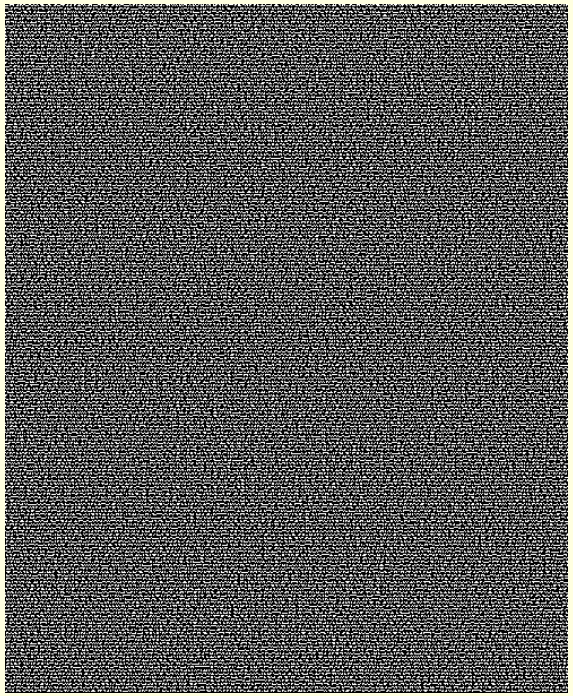


Sharing a secret image: Binary

- Decomposing a face into two random images







Gray-level Extended Visual Cryptography Scheme (GEVCS)

- VCS allows us to encode a secret image into n sheet images
- These sheets appear as a random set of pixels
- The sheets could be reformulated as natural images – known as host images

M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," Journal of WSCG 10(2), pp. 303–310, 2002.

Visual Cryptography: An Example

PRIVATE IMAGE

HOSTS (PUBLIC IMAGES)

PRIVATE IMAGE
AFTER DECRYPTION

HOSTS AFTER ENCRYPTION

Ross and Othman, "Visual Cryptography for Biometrics Privacy", TIFS 2011

Visual Cryptography

Actual Face

=

HOST IMAGE 1

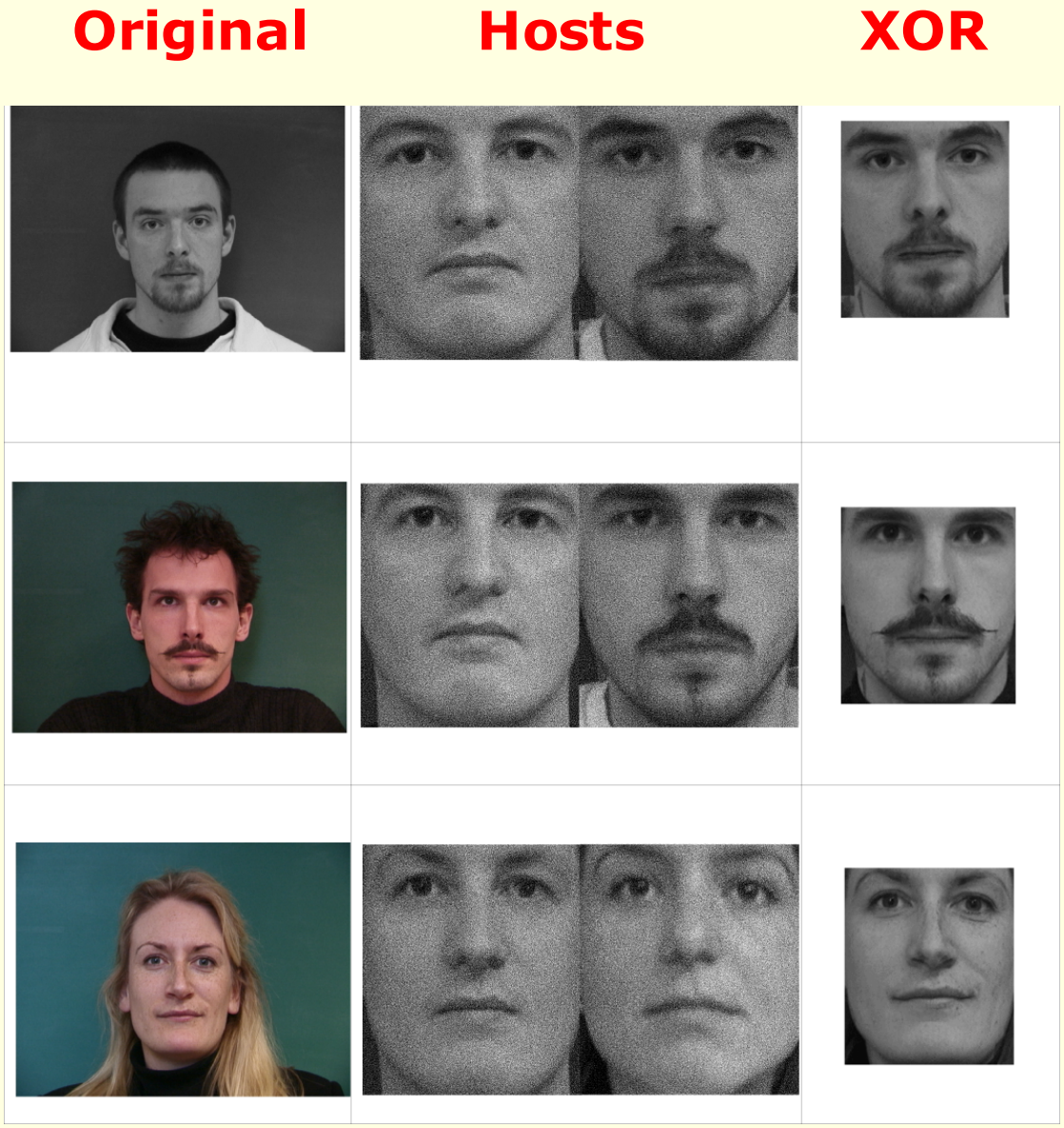
+

HOST IMAGE 2

Ross and Othman, "Visual Cryptography for Biometrics Privacy", TIFS 2011

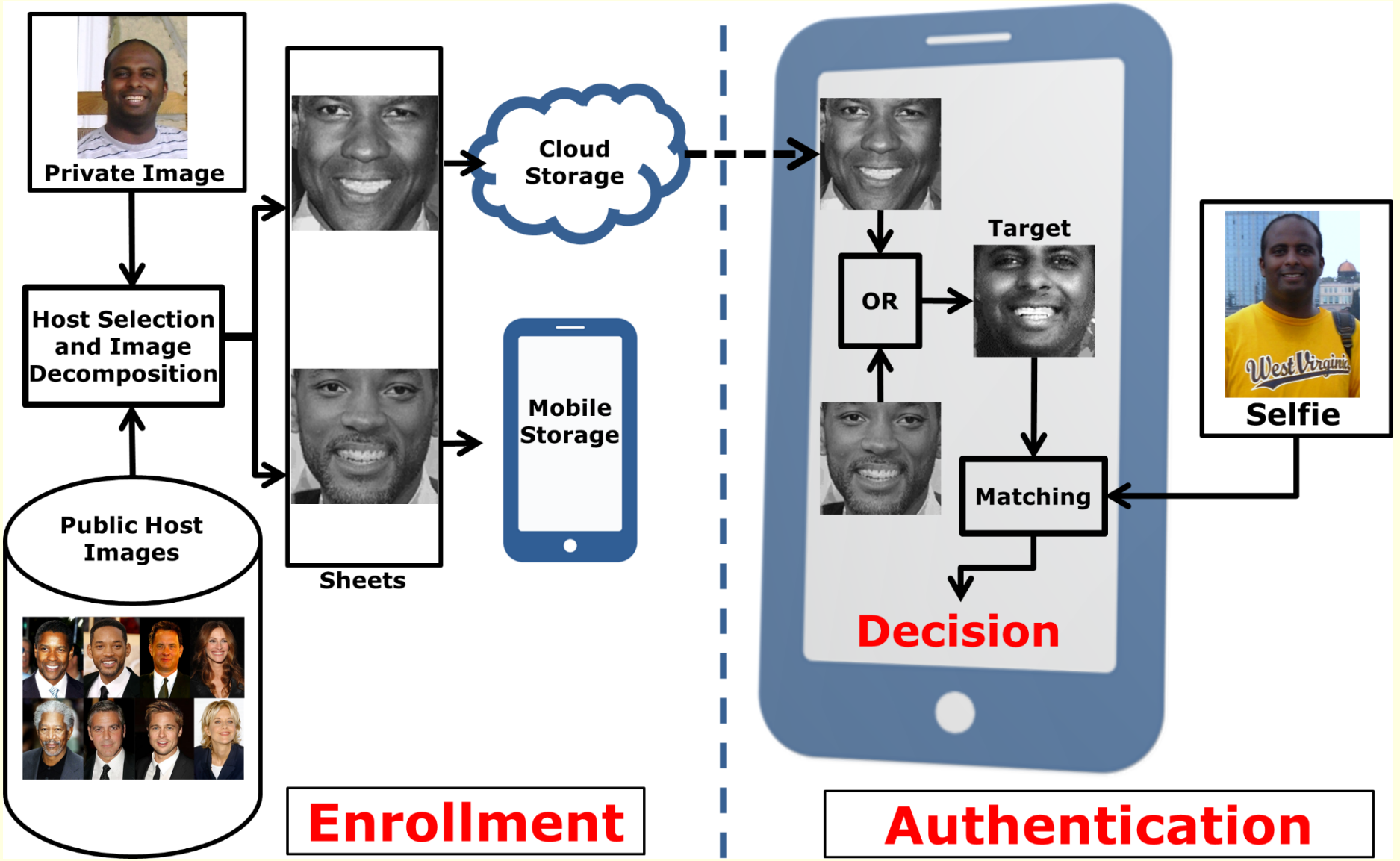
Automated Host Image Selection

- The original image is encrypted into two dynamically selected host images



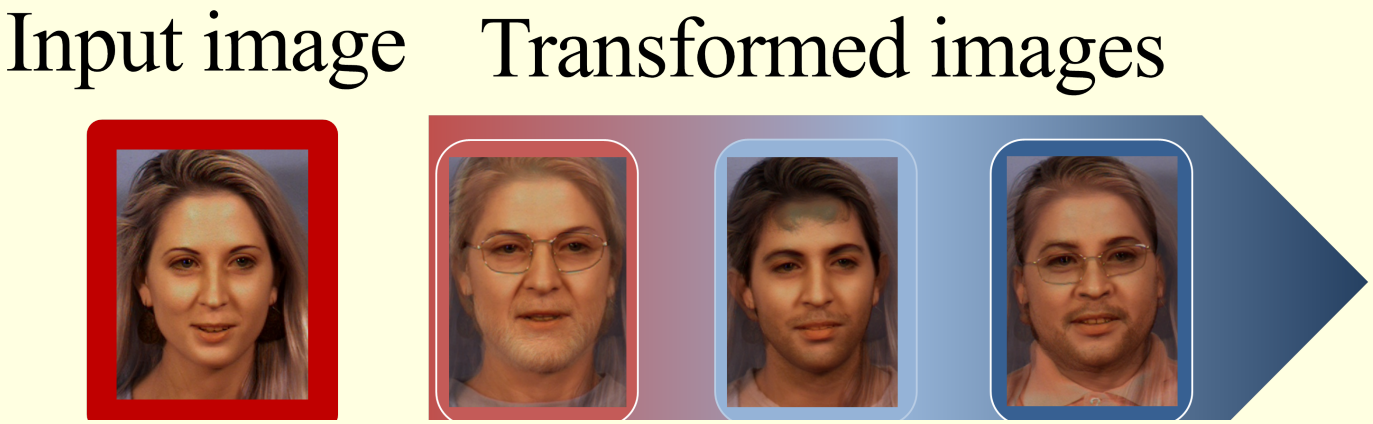
Ross and Othman, "Visual Cryptography for Biometrics Privacy", TIFS 2011

Application



Soft Biometric Privacy

- Gender attribute of an input face image is progressively suppressed
- With respect to a face matcher the identity is preserved



Identity	Alice	Alice	Alice	Alice
Gender	Female (confident)	Female (less confident)	Male (less confident)	Male (confident)

Othman and Ross, "Privacy of Facial Soft Biometrics: Suppressing Gender But Retaining Identity", ECCV Workshop, 2014

Gender Perturbation

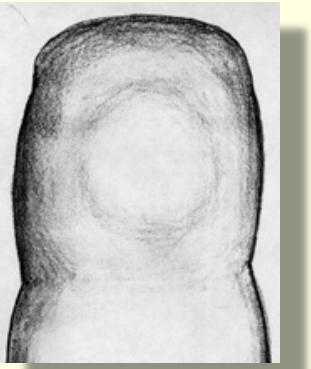
ORIGINAL IMAGES

MODIFIED IMAGES

Othman and Ross, "Privacy of Facial Soft Biometrics: Suppressing Gender But Retaining Identity", ECCV Workshop, 2014

Biometric Science Questions

- How can the biometric trait of an individual be effectively modeled using biologically tenable models?
- How can the uniqueness of a biometric trait, as it pertains to an individual, be deduced based on such models?
- What is the impact of age and disease on the stability and permanence of biometric characteristics?



Engineering Questions

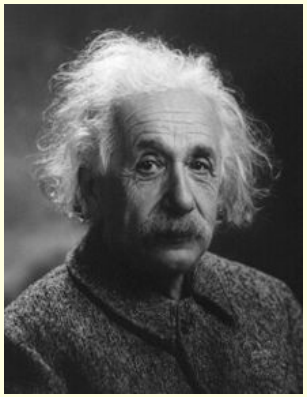
- What types of signal enhancement and matching models are necessary to conduct biometric recognition using severely degraded biometric data?
- How can biometric templates be stored and transmitted securely in order to accord privacy to users of the system?
- What types of statistical and mathematical models are essential to predict matching performance of large-scale biometric systems?
- How can large biometric databases be efficiently searched in order to rapidly locate an identity of interest?

Philosophical Musings

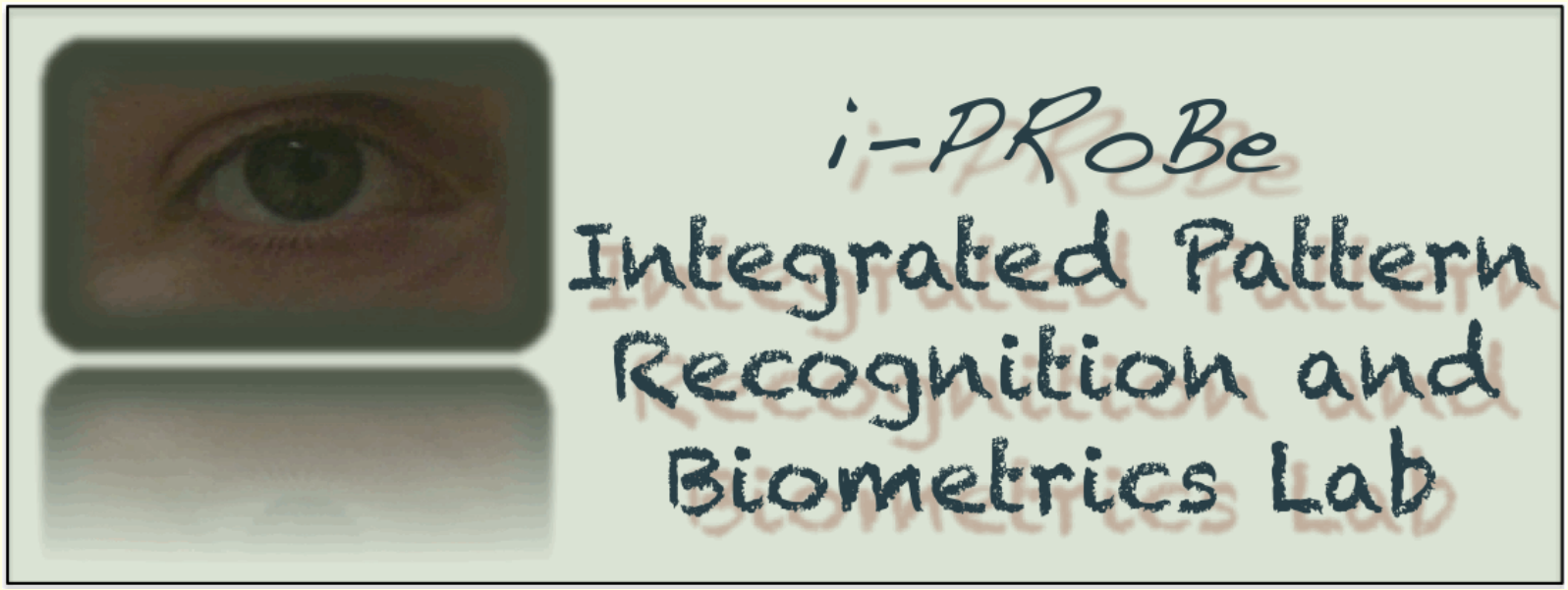
- What constitutes the identity of an individual?
- What are the societal implications of machines identifying humans?
- What are the moral and ethical implications of a biometric system misidentifying an individual in high-risk environments such as a combat zone?

Problem Solving

- We can't solve problems by using the same kind of thinking we used when we created them



The i-PRoBe Lab



http://www.cse.msu.edu/~rossarun/i-probe/

- Currently: 6 PhD students + 3 MS Students + 4 UG Students
- Collaboration with several biometric research groups


National Science Foundation
WHERE DISCOVERIES BEGIN


IARPA
BE THE FUTURE


NIST
National Institute of Standards and Technology
U.S. Department of Commerce


FEDERAL BUREAU OF INVESTIGATION
FBI
BIOMETRIC
Center of Excellence
Leading the World of Biometrics


ONR
OFFICE OF NAVAL RESEARCH


NIJ
NATIONAL INSTITUTE of JUSTICE


WV HIGHER EDUCATION POLICY COMMISSION

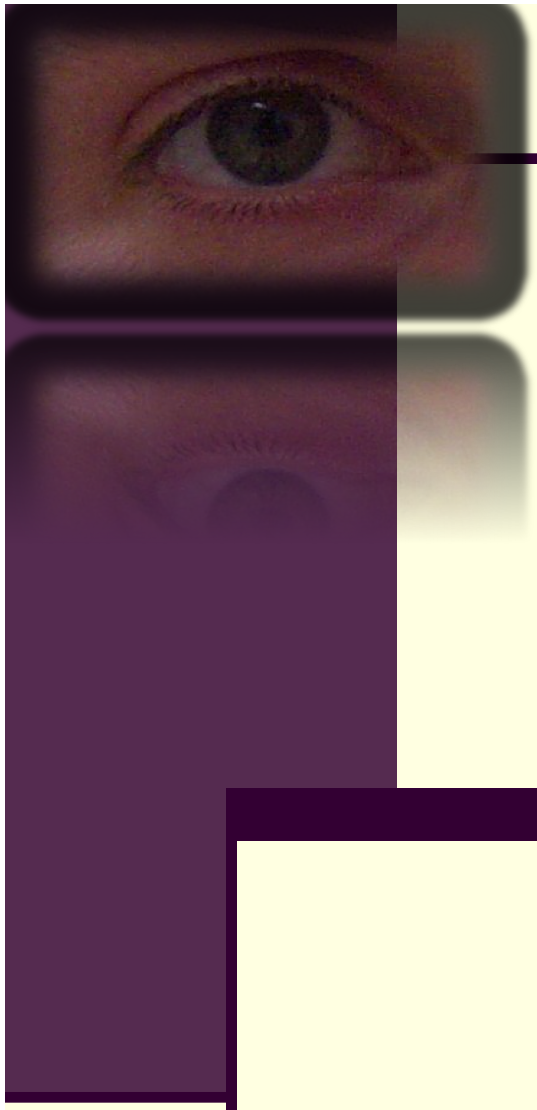

CITeR
CENTER FOR IDENTIFICATION TECHNOLOGY RESEARCH


BIMA
BIOMETRICS IDENTITY MANAGEMENT AGENCY


U.S. DEPARTMENT OF HOMELAND SECURITY


noblis
For the best of reasons


DRAPER
LABORATORY



Recent Progress in Biometrics

Arun Ross

Associate Professor

Michigan State University

rossarun@cse.msu.edu

http://www.cse.msu.edu/~rossarun