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?
Are these two prints from the same finger?
A Question of Identity

- Is this really a photograph of Abraham Lincoln?
Find all video frames in which Odette appears
A Question of Identity

- Is he the owner of this smart phone?
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

Fingerprint: Privaris Key Fob

Face + Voice: Voice Key.OnePass

Finger Vein: Japan ATMs
The Biometrics Revolution

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

Prevalence of developmental biometrics:
- National: at least 1 country-wide application (e.g., national ID, elections)
- Sub-national: at least 1 state or ministry-level application (e.g., civil service payroll, pensions)
- Project: at least 1 project-level application (e.g., health and demographic survey)

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

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

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

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


<table>
<thead>
<tr>
<th>Actual</th>
<th>Classified</th>
<th>ICE-LG</th>
<th>WVU-OKI</th>
<th>WVU-EverFocus</th>
<th>CASIAv3-OKI</th>
<th>CASIAv3p</th>
<th>CASIAv2-OKI</th>
<th>CASIAv2p</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICE-LG</td>
<td>1680</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WVU-OKI</td>
<td>0</td>
<td>1680</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WVU-EverFocus</td>
<td>9</td>
<td>0</td>
<td>1661</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>CASIAv3-OKI</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1665</td>
<td>0</td>
<td>15</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CASIAv3p</td>
<td>103</td>
<td>155</td>
<td>47</td>
<td>210</td>
<td>1009</td>
<td>82</td>
<td>74</td>
<td></td>
</tr>
<tr>
<td>CASIAv2-OKI</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1680</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>CASIAv2p</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1680</td>
<td></td>
</tr>
</tbody>
</table>

- **Classification accuracy is ~90%**
Determining Data Source

CASIA V2

ICE 2005

IITD
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

<table>
<thead>
<tr>
<th>Dataset</th>
<th>MBGC</th>
<th>CASIA V3</th>
<th>UPOL</th>
<th>UBIRIS</th>
<th>WVU</th>
<th>IITD</th>
<th>ICE</th>
<th>CASIA V2</th>
</tr>
</thead>
<tbody>
<tr>
<td>MBGC</td>
<td>174</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>CASIA V3</td>
<td>0</td>
<td>185</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>UPOL</td>
<td>3</td>
<td>1</td>
<td>164</td>
<td>18</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>UBIRIS</td>
<td>5</td>
<td>0</td>
<td>19</td>
<td>162</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>WVU</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>2</td>
<td>156</td>
<td>5</td>
<td>6</td>
<td>9</td>
</tr>
<tr>
<td>IITD</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>192</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ICE</td>
<td>26</td>
<td>0</td>
<td>25</td>
<td>13</td>
<td>15</td>
<td>7</td>
<td>105</td>
<td>1</td>
</tr>
<tr>
<td>CASIA V2</td>
<td>23</td>
<td>5</td>
<td>0</td>
<td>7</td>
<td>34</td>
<td>2</td>
<td>1</td>
<td>120</td>
</tr>
</tbody>
</table>
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**:
  • Heterogeneous Face Recognition
  • Privacy
Heterogeneous Face Recognition

- Photo vs Sketch
- Before vs After Makeup
- RGB vs NIR vs THM
- Young vs Old
- 2D vs 3D

Fundamental Differences in Image Formation Characteristics
“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

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

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.
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:

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

- 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:

\[ L_c = \sum_{i,k} \log p(\Theta) (t^k_i, x_i, y_k) \]

- The following function is maximized:

\[ \sum_{i,k} \int p(\Theta_0 (x_i, y_k | T) \log p(\Theta) (t^k_i, x_i, y_k) dx_i y_k \]

* Gong et al, “Hidden Factor Analysis for Age Invariant Face Recognition.” ICCV 2013
Extracting Identity Factor

- The identity factor can be computed as:

\[ x = UU^T \Sigma^{-1} (t - \beta) \]

where,

\[ \Sigma = \sigma^2 I + UU^T + VV^T \]

* Gong et al, “Hidden Factor Analysis for Age Invariant Face Recognition.” ICCV 2013
The Identity Factor (on original image)

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

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

Biometric data of an individual is sometimes stored in a central database. This 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

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, $S_{h_i}$ 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

Visual Cryptography: An Example

Visual Cryptography

Actual Face

HOST IMAGE 1

HOST IMAGE 2

Automated Host Image Selection

The original image is encrypted into two dynamically selected host images

<table>
<thead>
<tr>
<th>Original</th>
<th>Hosts</th>
<th>XOR</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.jpg" alt="Original Image" /></td>
<td><img src="image2.jpg" alt="Host Image 1" /></td>
<td><img src="image3.jpg" alt="XOR Image 1" /></td>
</tr>
<tr>
<td><img src="image4.jpg" alt="Original Image" /></td>
<td><img src="image5.jpg" alt="Host Image 2" /></td>
<td><img src="image6.jpg" alt="XOR Image 2" /></td>
</tr>
<tr>
<td><img src="image7.jpg" alt="Original Image" /></td>
<td><img src="image8.jpg" alt="Host Image 3" /></td>
<td><img src="image9.jpg" alt="XOR Image 3" /></td>
</tr>
</tbody>
</table>

Gender attribute of an input face image is progressively suppressed.

With respect to a face matcher the identity is preserved.

Gender Perturbation

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
Recent Progress in Biometrics

Arun Ross
Associate Professor
Michigan State University
rossarun@cse.msu.edu

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