Fake Fingers and Stolen Templates: Topics in Biometric Security

Dr. Stephanie Schuckers, Clarkson University
Director, Center for Identification Technology Research

Presented March 2014
Center for Identification Technology Research (CITeR)

A National Science Foundation (NSF) Industry/University Cooperative Research Center (IUCRC)

CONDUCTING RESEARCH IN SCIENCE AND TECHNOLOGY WHICH SUPPORTS

Identity in a Networked Global Society

SCOPE

Physiological, Behavioral, and Molecular Biometrics

Industry-driven research providing insight into the future of ID Technology
Current and Committed Affiliates—Fall 2013

- Aware
- Biometric Identity Management Agency
- Booz Allen Hamilton
- Borders, U of Arizona
- CUBRC
- DoD-National Center for Credibility Assessment
- Department of Defense—R&E Enterprise
- DoD-Defense Intelligence Agency
- Department of Homeland Security—S & T
- Department of Homeland Security—Office of Biometric Identity Management (OBIM)
- FBI: Federal Bureau of Investigation
- FLIR, Inc
- Honeywell
- Incadence Strategic Solutions
- Laurea Institute
- Lockheed Martin
- Microsoft
- Morphotrak
- NSA: National Security Agency (2 organizations)
- NexID Biometrics, LLC
- Northrop Grumman
- Qualcomm
- Raytheon
- Raytheon BBN Technologies
- Science Applications International Corporation (SAIC)
- SRC, Inc
- US Army ARDEC
How does an I/UCRC operate?

Affiliate Advisory Board (AAB)
- Composed of Government And Industry
- Votes to determine funded projects
- Pulls Next-Gen ID Technology
- Incorporates research results in strategy

CITeR Research Team
- Composed of Faculty, Researchers, Graduate students, Undergraduates
- Proposes projects to AAB
- Pushes Next-Gen ID Technology
- Executes research
Summary of Major Outcomes and Impact of CITeR

• **Books (e.g.)**
  - Li, Jain (Eds.), *Handbook of Face Recognition*, Springer Verlag, 2005.

• **Public datasets**, ([http://www.clarkson.edu/citer/research/collections](http://www.clarkson.edu/citer/research/collections))
  - e.g., Public releases of large multi-modal datasets;
  - Quality in Face and Iris Research Ensemble (Q-FIRE): face/iris video 8m

• **Software**: ([http://www.clarkson.edu/citer/research/tools.html](http://www.clarkson.edu/citer/research/tools.html))
  - MUBI multibiometrics fusion analysis and PRESS (statistical framework)

• **M1 standards support** in multibiometric fusion and liveness

• **Over 300 publications** to date

• **Over 100 Master’s/Ph.D.** students graduated to date

• **Technology transfer & Start-ups**: Fingerprint liveness algorithms (NexID Biometrics LLC), eye vein biometrics (EyeVerify), scars/marks/tattoos algorithms, altered finger detection
Identity Authentication

- What you have
e.g., ID cards, passports, keys

- What you know
e.g., password, PIN, user ID

- Who you are
e.g., biometrics: fingerprints, face, iris, voice, DNA

Two step—enrollment (reference) and verification (matching)
BYOD

• Rise in mobile payments
  - Purchasing and financial transactions
  - Near field communication using mobile devices for “credit card” payments at the point of service

• Increased need for security AT the device
  - “Bring your own device” (BYOD)
  - Multifactor authentication

• Personal authentication device

Techradar, 1/16/2013
Challenges in Biometrics

• **Privacy (acceptability)**
  Data protection
  Data sharing

• **Security (circumvention)**
  Biometrics are not secret
  Biometrics cannot be changed
Privacy

- Personal information
  Biographic information (name, age, DOB, address, gender)
  Issued identifiers (e.g., social security number)
  Physiologic (e.g. biometrics, medical)
- In US, legal concept of PII--“Personally Identifiable Information”
- Obligation to protect personal information
- Disclosure of how data used and giving individuals control
- Need technologies to support

Soutar, NSF workshop, 2010
1. Presentation attacks
2. Replay attacks
3. Overriding feature extraction
4. Tampering with feature sets
5. Corrupting the matcher
6. Tampering with stored templates
7. Attacking channel stored templates and matcher
8. Overriding final decision

Ratha et al, Enhancing security and privacy in biometrics-based authentication systems, 2001
Template Security

Cancelable Biometrics

Biometric Cryptosystems

An entity that binds the biometric template and secret key cryptographically


Desired Traits for Template Security

Irreversibility

Also, robustness, diversity, others

Unlinkability

C Rathgeb, C Busch Multi-Biometric Template Protection: Issues and Challenges, 2012
Presentation Attacks-Spoofing

- Famous “gummy finger” by Matsumoto in 2002
- Early liveness detection paper by Derakhshani, et al, in 2003
- In 2009, fingerprint spoof attack at Japanese border by a Korean woman reported
- In 2013, Brazilian doctors used a cooperative spoof with a time and attendance biometric system
- Number of successful spoofing events is unknown
Presentation Attacks

- Spoofing is a common term used most in the past decade.
- ISO Standards underway:
  - **Presentation Attack** Definition: Presentation of an artefact or human characteristic to the biometric capture subsystem in a fashion that could interfere with the intended policy of the biometric system*
  - Divided into Two (or more) categories
    - Human Based
    - Artificial Based
  - Why?
    - Posing as another individual
      - Positive ID applications
    - Hiding your identity
      - Negative ID applications
      - May form ‘new’ identity for positive ID

*from: ISO/IEC CD 30107-1, Information Technology — Biometrics -- Presentation Attack Detection
Categories of Human Presentations Attacks (Non-Artefact Methods)

- **Lifeless**
  - Cadaver

- **Altered**
  - Mutilation (e.g. scarring, amputation, acid)
  - Surgical modification (e.g. new fingerprint, nose job, face lift)

- **Non-Conformant**
  - Impersonation (e.g. voice mimicry, forged signature)
  - Presentation (e.g. hand shape control, facial expression/extreme, tip of side of finger)

- **Conformant**
  - Zero effort impostor attempt (normal presentation)

- **Coerced**
  - Unconscious or under duress

Artificial Presentation Attacks

• Procedure to create an artificial presentation attack characteristic:
  
  Source of biometric characteristic – Obtain information to describe characteristic
  
  Production of artefact – Process for creating artefact to present characteristic to sensor
Source of Biometric Characteristics (1)

- **Cooperative**
  Characteristic captured directly from individual with assistance (e.g. finger mold, hand mold, face mask)

- **Latent**
  Characteristic captured indirectly through latent sample (e.g. latent fingerprint, latent palmprint, hair, skin, body fluid)

- **Recording**
  Characteristic captured directly from individual onto media (e.g. photograph, video recording, audio recording)

Source of Biometric Characteristics (2)

• **Template Regeneration**
  Regenerate characteristic from template (e.g. fingerprint regeneration, face)

• **Synthetic**
  Synthetic characteristic, not mapped to real person (e.g. synthetic fingerprint, iris, face, voice, wolf synthesized sample)

• **Impersonation**
  Conversion of natural characteristic to another individual’s with artificial assistance (e.g. computer assisted voice)

Feng and Jain, Advances in Biometrics article, 2009.
Production of Artefact (1)

- Mold/cast
  Create 3D representation of characteristic (negative)
  Cast is reproduction created from mold (e.g. theatrical face mask, finger artefact of modeling clay, gelatin, silicone, latex, wood glue, glycerin, etc.)

- Mask – modify or conceal characteristics (partially or completely) with artefact
Production of Artefact (2)

- Direct rendering
  - Printing 2D (e.g. photo of iris or face, fingerprint printed on transparency/paper)
  - Printing 3D (e.g. contact lens printed with pattern, prosthetic hand printed with vein pattern)
  - Etching (e.g. fingerprint etched on metal)
  - Painting – patterns and colors painted on prosthesis

- Digital Media
  - Computer screen – laptop or tablet to present image or video
  - Audio – recording of voice

Seelen, “Countermeasures Against Iris Spoofing with Contact Lenses,” Iridian Technologies Inc.


Stolen Template to Fake Fingerprint—A Scenario

- Template is reduced set of stored “features” used for matching
- Stolen feature data must be “regenerated” to form biometric
  Shown possible for fingerprint and other biometrics

- Use process similar to latent fingerprints

Feng and Jain, Advances in Biometrics article, 2009.
Biometrics is part of security system. Layers of security are needed to minimize vulnerabilities.
Minimizing Spoofing Risk

• Application-specific risk assessment
  What is the role of biometrics in my application? (Is it needed?)
  Does it improve upon former methods of identity management?
  What is the impact of spoofing vulnerability?
  What is the public perception of spoofing vulnerability?

• Consider these questions for two applications
  - Electronic passport with a biometric
  - iPhone
Minimizing Spoofing Risk

• Ways to mitigate risk
  Multifactor
    Combinations of what you have, what you know and biometrics
  Multi-biometrics—require multiple biometrics
  Liveness detection or anti-spoofing

“It Is ‘Liveness’, Not Secrecy, That Counts.”
Presentation Attack Detection (PAD)

- Presentation Attack Detection (PAD) *
  Automated determination of a presentation attack

- Examples of PAD
  Liveness detection (failure)
  Artefact detection
  Altered biometric detection
  Others terms that have been used: anti-spoofing, biometric fraud, spoof detection, authenticity detection, etc.

*from: ISO/IEC CD 30107-1, Information Technology — Biometrics -- Presentation Attack Detection
Even “liveness detection” may not measure liveness!
Presentation attack detection (PAD) may be a better term.
Many methods which detect spoofing may not really measure “liveness”
Hardware-based Fingerprint Liveness Detection

- Hardware-based
  - Temperature
  - Pulse
  - Blood pressure
  - Odor
  - Electrocardiogram
  - Multispectral imaging, spectroscopy
  - Others

- Should be integrated carefully so spoof cannot be combined with any live finger to be accepted
  - e.g. translucent spoof fooling light-absorption-based pulse oximeter

Software-based Fingerprint Liveness Detection

- Examples proposed
  - Skin deformation
  - Elasticity
  - Pores
  - Perspiration pattern
  - Power spectrum
  - Noise residues in valleys
- Combining multiple features
- Must represent variability of live subjects (dry, moist, variable environments, ages, ethnicity)
- Reliance on the properties of spoof materials
- Must stay one step ahead of would-be attacker—software upgrade

Another Liveness Detection Method
(Needed equipment: clamp and microphone)
Benchmarking

• Liveness Detection Competitions
  Sense of the State of the Art in the Field
  Publically available databases to support R&D (even after competitions)
  Co-host: Fingerprint—Clarkson U & U of Cagliari;
  Iris—Clarkson U, Notre Dame University & Warsaw U of Technology

  • LivDet 2009
    – Fingerprint Algorithms

  • LivDet 2011
    – Fingerprint Algorithms
    – Fingerprint Systems

  • LivDet 2013
    – Fingerprint Algorithms
    – Fingerprint Systems
    – Iris Algorithms

http://www.clarkson.edu/citer/research/collections
Examples from LivDet 2013

- Crossmatch (Left to Right): Live, Body Double, Latex, Playdoh, Wood Glue

- Swipe (Left to Right): Live, Body Double, Latex, Playdoh, Wood Glue


http://prag.diee.unica.it/fldc/
Liveness Detection—LivDet 2013 Fingerprint

• Part 1. Algorithms
  Four datasets
  Eleven submissions

• Part 2. Systems
  – Two submissions

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Scanner</th>
<th>Model</th>
<th>Res (dpi)</th>
<th>Image size</th>
<th>Live samples</th>
<th>Fake samples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Biometrika</td>
<td>FX2000</td>
<td>569</td>
<td>312X372</td>
<td>2000</td>
<td>2000</td>
</tr>
<tr>
<td>2</td>
<td>Italdata</td>
<td>ET10</td>
<td>500</td>
<td>640X480</td>
<td>2000</td>
<td>2000</td>
</tr>
<tr>
<td>3</td>
<td>Crossmatch</td>
<td>L SCAN GUARDIAN</td>
<td>500</td>
<td>640X480</td>
<td>2500</td>
<td>2500</td>
</tr>
<tr>
<td>4</td>
<td>Swipe</td>
<td>96</td>
<td>variable</td>
<td></td>
<td>2500</td>
<td>2500</td>
</tr>
</tbody>
</table>


http://prag.diee.unica.it/fldc/
<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Biomet</th>
<th>Italdata</th>
<th>Crossm</th>
<th>Swipe</th>
<th>Avg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dermalog</td>
<td>98.3</td>
<td>99.2</td>
<td>44.53</td>
<td>96.47</td>
<td>84.63</td>
</tr>
<tr>
<td>Anon1</td>
<td>98</td>
<td>98.85</td>
<td>50.53</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATVS</td>
<td>94.95</td>
<td>50</td>
<td>45.2</td>
<td>53.55</td>
<td>60.93</td>
</tr>
<tr>
<td>Anon2</td>
<td>98.2</td>
<td>99.4</td>
<td>45.2</td>
<td>94.19</td>
<td>84.25</td>
</tr>
<tr>
<td>UniNap1</td>
<td>95.3</td>
<td>96.5</td>
<td>68.8</td>
<td>85.93</td>
<td>86.63</td>
</tr>
<tr>
<td>UniNap2</td>
<td>93.45</td>
<td>90.55</td>
<td>47.87</td>
<td>73.15</td>
<td>76.26</td>
</tr>
<tr>
<td>UniNap3</td>
<td>93.45</td>
<td>96.5</td>
<td>47.87</td>
<td>85.93</td>
<td>80.94</td>
</tr>
<tr>
<td>Anon3</td>
<td>94.3</td>
<td>97.2</td>
<td>46.89</td>
<td>94.75</td>
<td>83.29</td>
</tr>
<tr>
<td>HZ-JLW</td>
<td>67.05</td>
<td>86.85</td>
<td>44.44</td>
<td>84.81</td>
<td>70.79</td>
</tr>
<tr>
<td>Itautec</td>
<td>91</td>
<td>96.1</td>
<td>57.73</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAoS</td>
<td>95.4</td>
<td>54.1</td>
<td>52.62</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Part 2: Systems Results

- Anonymous 4 received the best results for both FerrLive and FerrFake.
- Anonymous 4 received only a 1.4% FerrLive and 0% FerrFake.
- Dermalog received an 11.8% FerrLive and a 1.4% FerrFake.

Error Rates for Submitted Systems

<table>
<thead>
<tr>
<th></th>
<th>FerrLive</th>
<th>FerrFake</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dermalog</td>
<td>11.8</td>
<td>0.6</td>
</tr>
<tr>
<td>Anonymous</td>
<td>1.4</td>
<td>0</td>
</tr>
</tbody>
</table>

Examples from Iris LivDet Database

Sample Images from Clarkson University Liveness Database: left (live), right (spoof)

Sample Images from Warsaw University of Technology Liveness Database: left (live), right (spoof)

Sample Images from Notre Dame University Liveness Database: left (live), right (spoof)

http://people.clarkson.edu/projects/biosal/iris/
Results-LivDet 2013 Iris

Rate of misclassified Live Iris Images (ferrlive) for submitted algorithms

Rate of misclassified Spoof Iris Images (ferrfake) for submitted algorithms

http://people.clarkson.edu/projects/biosal/iris/
Notional Tradeoffs in Multifactor Authentication

Can we achieve both security & convenience?

Caution: Actual tradeoffs will rely on specific application and chosen solutions.
Special Thanks

Current team
- Peter Johnson
- David Yambay
- Fang Hua
- Gerald Brennan
- Matt Sherry
- Megan Rolewiecz
- Laura Holsopple
- Shannon Ralston

Collaborators
- Arun Ross
- Bojan Cukic
- Joe Skufca
- Larry Hornak

(Some) former students
- Aditya Abhyankar
- Bozhao Tan
- Reza Derakhshani
Funding provided by:

- National Institute of Standards and Technology (NIST)
- National Science Foundation (NSF)
- Dept. of Homeland Security (DHS)
- Center for Identification Technology Research (CITeR)
CITeR Contact Info

- **Clarkson University:**
  Dr. Stephanie Schuckers, CITeR Director, 315.268.6536
  Laura Holsopple, Managing Director, {sschucke, lholsopp}@clarkson.edu

- **West Virginia University:**
  Dr. Bojan Cukic, Site Director, 304.293.9686
  bojan.cukic@mail.wvu.edu

- **University of Arizona:**
  Dr. Judee Burgoon, Site Director, 520.621.5818
  Dr. Jay Nunamaker, Co-Director, {jburgoon, jnunamaker}@cmi.arizona.edu

- **University at Buffalo:**
  Dr. Venu Govindaraju, Site Director, 716-645-1558
  venu@cubs.buffalo.edu

- **Michigan State University (planned):**
  Dr. Arun Ross, 517.353.9731
  rossarun@cse.msu.edu