Biometric standardization and Presentation Attack Detection

Christoph Busch

Norwegian Biometrics Laboratory - Gjøvik
http://www.christoph-busch.de

The 1st Danish Biometrics Workshop

Copenhagen - November 26th, 2015
Norwegian Biometrics Laboratory (NBL)

- **Faculty-Members:**
  - Christoph Busch
  - Patrick Bours
  - Bian Yang
  - Faouzi Alaya Cheikh
  - Sule Yildirim
  - Erik Hjelmås
  - Raghu Ramachandra
  - Katrin Franke (adjunct member)
  - Ivar Farup (adjunct member)
  - Mohammad Derawi

- **PhD-Students:**
  - Ctirad Sousedik
  - Edlira Martiri
  - Guoqiang Li
  - Kiran Raja
  - Martin Olsen
  - Martin Stokkenes
  - Nabeel Al-Bahbooh
  - Soumik Mondal
  - Marta Gomez (guest from UAM)

- **Key-factors:**
  - Since 2008, 6 EU FP7 projects,
    2 Norwegian funded project
  - 1 US-government funded project,
    2 research projects with the German BSI,
    4 industrial projects,
  - cooperated with > 30 research partners
  - approx 110 peer-reviewed publications
Standardization Meetings
Biometric Applications
Biometrics and Access Control

Automated Border Control in Europe

- Automated but supervised border control since 08‘2009
- Self-Service to increase throughput

US VISIT

- Visitors with a criminal record are rejected
Smartphone Based Access Control

It won‘t take long

- that NFC enabled Smartphones will interact with most doors
Mobile Biometrics
Smartphone Access Control

Foreground authentication (user interaction)

- Deliberate decision to capture (willful act)
- Camera-Sensor
  - Fingerprint recognition
    - Apples iPhone 5S / Samsung Galaxy 5
    - Fingerphoto analysis
  - Face recognition
  - Iris recognition
- Touchpad: allows signature recognition

Background authentication (observation of the user)

- Microphone
  - Speaker recognition
- Accelerometer
  - Gait recognition
  - concurrent - unobtrusive
Biometric Gait Recognition

Data capture process
- periodical pattern in the recorded signal

Best result
- now at 6.1% Equal-Error-Rate (EER)
## Biometric Gait Recognition

- All benchmarked publications

<table>
<thead>
<tr>
<th>Publication</th>
<th>Sensor</th>
<th>Sensor-position</th>
<th>Number Subjects</th>
<th>Best Result [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ailisto [4], 2005</td>
<td>dedicated</td>
<td>back</td>
<td>36</td>
<td>6.4 (EER)</td>
</tr>
<tr>
<td>Rong [123], 2007</td>
<td>dedicated</td>
<td>back</td>
<td>21</td>
<td>5.6 (EER)</td>
</tr>
<tr>
<td>Pan [61], 2009</td>
<td>Wiimote</td>
<td>hip</td>
<td>30</td>
<td>70.1 (GMR)</td>
</tr>
<tr>
<td>Sprager [130], 2009</td>
<td>smartphone</td>
<td>hip</td>
<td>6</td>
<td>92.9 (CCR)</td>
</tr>
<tr>
<td>Gafurov [46], 2010</td>
<td>dedicated</td>
<td>ankle</td>
<td>10</td>
<td>59.0 (GMR)</td>
</tr>
<tr>
<td>Nickel (CASED)</td>
<td>smartphone</td>
<td>hip</td>
<td>48</td>
<td>6.1 (EER)</td>
</tr>
</tbody>
</table>

Smartphone Access Control

Capture process

• Camera operating in **macro** modus

Finger recognition study - 2012/2013

- Result: biometric performance at 1.2% EER

Biometric Eye Recognition

Images captured with either front or back camera

- Challenges
  - face and eye localization

Standards?

Operators may think:

„There are no standards on biometrics“
Biometric Standardisation

International Organization for Standardisation (ISO)

Joint Technical Committee One (JTC1)

International Electrotechnical Commission (IEC)

International Civil Aviation Organization (ICAO)

TC 68
Banking, Securities
Financial services

SC 17
Cards & Personal Identification

SC 27
IT Security Techniques

SC 37
Biometrics

SC37 to TC68

SC 37 Formal Liaisons

Christoph Busch
Biometric standardization and PAD
Copenhagen 2016-11-26
ISO/IEC SC37 Biometrics

Established by JTC 1 in June 2002 to ensure

- a high-priority, focused and comprehensive approach worldwide for the rapid development of formal generic biometric standards

Scope of SC37

- “Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects”

- http://www.jtc1.org

Next meeting: January, 2016

http://www.biometrics-center.ch/jtc1-sc37-martigny2015
Biometric Standardisation

Onion Layers

- **Layer 1: BDIR**
  - Digital representations of biometric characteristics

- **Layer 2: LDS**
  - CBEFF Meta-data

- **Layer 3+4:**
  - System properties
    - Security
    - Performance

- **Layer 5: BioAPI, BIP**
  - System Integration
The 19794-Family: Biometric data interchange formats

All parts binary encoding
Generation 2 of ISO/IEC 19794

G1

19794-1:2006

-2: 2005
-3: 2006
-4: 2005
-5: 2005
-6: 2005
-7: 2007
-8: 2006
-9: 2007
-10: 2007

All parts
binary encoding

G2

19794-1:2011

19794-1 AMD2 XML Framework

19794-1 AMD1 Conformance testing methodology

-2: 2011
-4: 2011
-5: 2011
-6: 2011
-7: 2011
-8: 2011
-9: 2011
-11: 2013
-13: 2013
-14: 2013

the semantic is equivalent for binary encoded and XML encoded records
For SmartCards: Finger minutiae data

ISO/IEC 19794-2:2011

- Ridges and valleys, core and delta
- Ridge bifurcation and ridge endings
  - finger minutiae
- Encoded information
  - Minutia point *(coordinates x,y)*
  - Minutia direction *(angle θ)*
- How many finger minutiae, and how many ridges between each pair of them?
- A very mature technology

Source: ISO/IEC 19794-4
Biometric Quality Standards

- ISO/IEC 29794-1 Biometric Sample Quality - Part 1: Framework
  - Data Structure of the Quality Block

<table>
<thead>
<tr>
<th>Quality Block</th>
<th>Data Structure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality Score</td>
<td>1 byte</td>
<td>[0,100] 255</td>
</tr>
<tr>
<td>Quality Algorithm Vendor ID</td>
<td>2 bytes</td>
<td>[1,65535]</td>
</tr>
<tr>
<td>Quality Algorithm ID</td>
<td>2 bytes</td>
<td>[1,65535]</td>
</tr>
</tbody>
</table>

- Quality metrics shall predict recognition accuracy!
  - “The correlation between predicted utility and observed utility of each sample is indicative of the effectiveness of the quality algorithm"
Quality Measures vs. Recognition Accuracy

- ISO/IEC 29794-1 Biometric Sample Quality - Part 1: Framework
  - Quality metrics shall predict recognition accuracy (utility)
NFIQ2.0 Features

Investigated Features (Local Metrics and Global Metrics)

- NFIQ 1.0 features (from 2004)
- NFIQ 2.0 will be the bases for revision of ISO/IEC 29794-4:2009
- Open source
Biometric Performance Testing Standard

ISO/IEC 19795-x, Information technology - Biometric performance testing and reporting

- Part 1: Principles & Framework
  - Guidance applicable to the broad range of tests
- Part 2: Testing Methodologies for Technology and Scenario Evaluation
  - Multiple visits, habituation, enrolment
- Part 3: Modality-Specific Testing
  - Modality (& application) specific methodologies
- Part 4: Interoperability Performance Testing
  - Performance on other vendors data
- Part 5: Framework for biometric device performance evaluation for access control
- Part 6: Testing Methodologies for Operational Evaluation
- Part 7: Testing of ISO/IEC 7816-based Verification Algorithms
Performance Metrics

Categorization in ISO/IEC 19795-1

• Technology testing
  ‣ Algorithmic level verification error
    - False-Match-Rate (FMR) - algorithm accepts „zero-effort“ impostor
    - False-Non-Match-Rate (FNMR) - algorithm rejects true identity

• Scenario testing and operational testing
  ‣ System level verification error
    - False-Accept-Rate (FAR)
    - False-Reject-Rate (FRR)
  ‣ System level error requires observation of:
    - Sample generation: Failure-to-Capture (FTC)
    - Enrolment: Failure-to-Enrol (FTE) - no reference for this subject
    - Verification: Failure-to-Acquire (FTA) - no probe feature vector
Graphical Presentation

DET curve (detection error trade-off curve)
- modified ROC curve which plots error rates on both axes (false positives on the x-axis and false negatives on the y-axis)
Security?

Operators will think:

„The biometric sensors must be robust against fake attacks“
Security?

- Presentation Attacks
Gummy Finger Production in 2000!

Attack without support of an enrolled individual

- Recording of an analog fingerprint from flat surface material
  - z.B. glass, CD-cover, etc.
    with iron powder and tape

- Scanning and post processing:
  - Correction of scanning errors
  - Closing of ridge lines (as needed)
  - Image inversion

- Print on transparent slide

- Photochemical production of a circuit board mold
Gummy Finger Production in 2000!

Reported in a publication by the German Federal Police

Presentation Attack Detection


- **presentation attack**
  presentation to the biometric capture subsystem with the goal of *interfering* with the operation of the biometric system

- **presentation attack detection (PAD)**
  automated *determination of a presentation attack*

Definitions in ISO/IEC 2382-37: Vocabulary
http://www.christoph-busch.de/standards.html

- **impostor**
  subversive biometric capture subject who attempts to being matched to someone else's biometric reference

- **identity concealer**
  subversive biometric capture subject who attempts to avoid being matched to their own biometric reference
### ISO/IEC 30107-1
Examples of Artificial and Human Attack Presentation

<table>
<thead>
<tr>
<th>Artificial</th>
<th>Complete</th>
<th>gummy finger, video of face</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Partial</td>
<td>glue on finger, sunglasses, artificial/patterned contact lens, non-permanent make up</td>
</tr>
<tr>
<td>Human</td>
<td>Lifeless</td>
<td>cadaver part, severed finger/hand</td>
</tr>
<tr>
<td></td>
<td>Altered</td>
<td>mutilation, surgical switching of fingerprints between hands and/or toes</td>
</tr>
<tr>
<td></td>
<td>Non-Conformant</td>
<td>facial expression/extreme, tip or side of finger</td>
</tr>
<tr>
<td></td>
<td>Coerced¹</td>
<td>unconscious, under duress</td>
</tr>
<tr>
<td></td>
<td>Conformant</td>
<td>zero effort impostor attempt</td>
</tr>
</tbody>
</table>

Source: ISO/IEC 30107-1
Presentation Attack Detection

ISO/IEC IS 30107-1 Standard

- soon available in the ISO-Portal

ISO/IEC IS 30107-1
Information Technology -- Biometric presentation attack detection -- Part 1: Framework
Definition of harmonized metrics in ISO/IEC 30107-3

- **Attack presentation classification error rate (APCER)**
  proportion of *attack presentations* incorrectly classified as *normal presentations* at the component level in a specific scenario

- **Normal presentation classification error rate (NPCER)**
  proportion of *normal presentations* incorrectly classified as *attack presentations* at the component level in a specific scenario
Smartphone Access Control

Finger recognition study - 2012/2013

- Observation
  - significant strong light reflection near the fingertip
  - from the cameras LED

- Reflection depends on
  - Shape of the finger
  - Consistency of the finger
  - Angle of the finger to the camera

- Attack detection, as light reflection differs from artefacts to genuine fingers

Finger recognition study - 2012/2013

• Results: Presentation Attack Detection (PAD)

• Conclusion: better Presentation Attack Detection than capacitive sensors
Eye recognition study - 2015

- Presentation Attack Detection (PAD) videos on iPhone 5 S and Nokia 1020

- Method based on Eulerian Video Magnification (EVM)
  - Normalized Cumulative Phase Information
Smartphone Access Control - with PAD

Method based on Eulerian Video Magnification (EVM)

Eye recognition study - 2015

• Method based on Eulerian Video Magnification (EVM)
  ‣ Normalized Cumulative Phase Information

• Zero Error Rates:
  ‣ APCER = 0 %
  ‣ NPCER = 0 %

Privacy Protection ?

Operators will think:

„Biometric systems must be compliant to data privacy and data protection principles“
Biometric Template Protection

We do NOT store fingerprint, iris or face images

- we transform templates to pseudonymous identifiers (PI)
- we reach
  - Secrecy: biometric references (PI) can be compared without decryption.
  - Diversifiability / Unlinkability: Unique pseudonymous identifier can be created for each application to prevent database cross-comparison
  - Renewability: we can revoke and renew template data.
  - Non-invertibility: Original biometric sample cannot be reconstructed


Biometric Template Protection

Protection at the **same accuracy level** is possible

- Bloom filter-based **pseudonymous identifiers**
- Successfully applied to iris, face, fingerprint and fingervein

- Example: Iris Segmentation

- Normalized Iris Texture

- Iris Feature Vector

- Binarised Iris Feature Vector

Protection at the same accuracy level is possible

- Bloom filter-based *pseudonymous identifiers*

Biometric Template Protection

Sub-Block $i$

Bloom Filter $i$

**Secrecy**

**Non-invertibility**

**Diversification**

**Noise robustness**

Biometric Template Protection enables revocability in biometric systems!
Data Protection Requirements

Technical framework on how to implement requirements for data privacy and data protection

• exists ISO/IEC 24745: Biometric Information Protection, (2011)
Your Operator Reality Check

Operators should ask the vendors

• Is there a vendor lock-in due to proprietary sensors?

  *I want the biometric capture device to be operated via BioAPI interface according ISO/IEC 19784!*

• Can comparison algorithms be replaced?

  *I want the biometric reference data to be stored in standardised interchange format according ISO/IEC 19794!*

• Is the accuracy of the algorithm good?

  *I want to see the technology performance test report according ISO/IEC 19795!*

• Is there data protection of stored biometric reference data?

  *I want the design of the systems to be compliant to ISO/IEC 24745*
Conclusion

Biometrics is possible with today's smartphones

- a multi-biometric authentication scheme with scaling factors is a good choice with respect to security threats

Biometric standards are available

Biometric system should be

- based on international ISO/IEC standards
- privacy friendly and not store plain biometric data on central servers
Further information on Biometric Standardization

- on ISO/IEC SC37
  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770&published=on
- on SC37 working group 3
  http://www.christoph-busch.de/standards-sc37wg3.html
- Next meeting: January, 2016
  http://www.biometrics-center.ch/jtc1-sc37-martigny2015
Contact

Contact:

Christoph Busch, Dr.-Ing.
Professor

P.O. Box 191, N-2802 Gjøvik, Norway
Phone: +47 61 13 51 94
Fax: +47 61 13 52 40
E-mail: christoph.busch@hig.no
www.hig.no | www.nislab.no