Fingerprint Presentation Attack Detection with OCT

Ctirad Sousedik – ctirad.sousedik@hig.no

Ralph Breithaupt - ralph.breithaupt@bsi.bund.de

Christoph Busch – christoph.busch@hig.no
Fingerprint Presentation Attack Detection with OCT

Outline

- Motivation
- Advantages
- Method
- Results
- Conclusion
- Future plans
Motivation

- Fingerprint sensors are vulnerable to spoofing attacks
- Fingerprint spoofing is widely researched
- Fingerprint Presentation Attack Detection (PAD) methods proposed as a countermeasure
- State-of-the-art countermeasures are vulnerable to high-quality artefact fingerprints fabricated using novel approaches
Motivation

State-of-the-art in fingerprint Presentation Attack Detection (PAD)

- Countermeasures based on the original scan
  - Typically try to make use of a 2D representation of the fingerprint provided by 2D sensors
  - Results not satisfactory for high-quality artifact fingerprints
- Countermeasures based on extra sensors
  - Try to measure various properties of genuine fingerprints
  - Vulnerable to novel fake fingerprint fabrication methods that take the measured properties into account

Fingerprint Presentation Attack Detection with OCT
Motivation

State-of-the-art in fingerprint Presentation Attack Detection (PAD)

- Possible solution
  - Combining a large number of different information channels about the genuine properties
  - Additional sensors and complex analysis of the 2D scan
- Problems
  - Too much information to be considered – machine learning necessary
  - Hard to teach how to recognize novel, previously unexpected, fakes
Motivation

Rather a single scanning technology that:

- Can capture enough information for the biometric recognition purposes
- Can capture enough information for Presentation Attack Detection
- Provides for scans that can be understood, and the genuine data can be defined
Method

• Analysis of 3D volumetric data
• Scanning of the 3D internal structure of the fingertip
• Optical Coherence Tomography (OCT)
Advantages

- 3D scanning of the fingertip
- Greatly increases the difficulty of spoofing the sensor
- Actual scanning of the inner fingerprint
- Better functionality under difficult conditions – wet, greasy fingers
Challenges

- Large amount of volumetric data to be processed in a matter of seconds
- Applicability to even larger amounts of data for wider scanning areas and resolutions
- Non-compliant capture subject behavior
- Noise in the OCT data
Database

- 4 x 4 x 2.5 mm large scanning volume
- 200 x 200 x 512 voxels resolution
- 226 subjects, 3 fingers per subject, 11 scans per finger
- > 7400 scans of genuine fingerprints
- 30 classes of artefact fabrication approaches, 9 artefact fingerprints per class, 11 scans per artefact fingerprint
- > 2900 scans of artefact fingerprints
Thin-layered artefact

Thick-layered artefact

Database
Proposed approach

Inner fingerprint layer

Outer fingerprint layer
Fingerprint Presentation Attack Detection with OCT

Proposed approach

- Volume divided into $w_g \times h_g$ columns
- In each column, all the row data added together to form a single function
Proposed approach

- Detection of peak position $p$ and approximate peak energy $e$ for an otherwise constant function
Proposed approach

- Detection of peak position $p$
- and approximate peak energy $e$
  for a function with an otherwise constant slope

Fingerprint Presentation Attack Detection with OCT

Ctirad Sousedík, Ralph Breithaupt, Christoph Busch
Proposed approach

- Each column function analyzed using overlapping windows of length $W$

- Each window detects a peak using the previous method

- $P$ peaks with highest energy are selected as the layer responses
Proposed approach

Fast computation:

0.02 s

per scan of 20 MB on a single CPU thread
Results

Genuine finger scan

OCT scan

Layers detected
Results

Artefact finger scan

OCT scan

Layers detected
Results

ISO/IEC WD 30107 liveness detection metrics [3]

- **False Live Detection Rate (FLDR)**: proportion of non-live presentation characteristics incorrectly classified as being live.

- **False Non-Live Detection Rate (FNLDR)**: proportion of live presentation characteristics incorrectly classified as being non-live.

![Diagram showing OCT fingerprint scans, genuine scans, and fake scans with misclassification rates (FNLDR and FLDR).]
### Results

- Classification using the strength of the responses when detecting the scans

<table>
<thead>
<tr>
<th></th>
<th>FLDR</th>
<th>FNLDNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our method</td>
<td>11.32%</td>
<td>3.52%</td>
</tr>
<tr>
<td>Menrath and Breithaupt</td>
<td>25.37%</td>
<td>6.17%</td>
</tr>
</tbody>
</table>
Conclusion

- Fast and robust method for OCT scan layer detection
- Potential for further development
Future plans

• New data collection in scope of the project OCT II
• Greater scanning volume
• Higher resolution
• Lower noise levels
Future plans

- Sweat glands detection and analysis
- Inner fingerprint analysis and comparison to the outer fingerprint
- Outer fingerprint extraction to 2D format
Thank you

Ctirad Sousedik – ctirad.sousedik@hig.no
Ralph Breithaupt - ralph.breithaupt@bsi.bund.de
Christoph Busch – christoph.busch@hig.no


