Biometric Encryption in “3D Face”

Michiel van der Veen

‘3D Face’ end-user meeting
March 22, Darmstadt, Germany

Content

• Motivation
• Biometric encryption in “3D Face”
• Outlook

Biometric systems are being rolled-out in many applications

• Large-scale criminal and civil AFIS
• Registered traveler programs
• Border crossing (3D Face)
• Attendance recording
• Access control
• Payment systems
• Ticketing
• ...

What about your (biometric) Identity?

Verifying identity becomes an integral part of many processes

In 2002, in US there were 3.3 Million cases of Identity Theft

• Current models for information sharing are largely based on thrust
  – Trading of information could be lucrative
  – Internet and networked systems
  – More people have access to personal data – remote access

• Threats
  – Identity theft
  – Harassment
  – Errors in databases
  – ...

Identity Management & Privacy Enhancing Tools
Biometric Encryption Aims

- Aims
  - Protect the biometric data and associated privacy
  - Introduce the revocability – the citizens right to revoke
  - Multi-identity for different applications
  - Greater public confidence and compliance with privacy laws
  - Suitable for large-scale ‘anonymous’ databases

- Modalities
  - Fingerprint
  - Face / 3D Face
  - Iris

Biometric identity information is spread around the applications leading to privacy threats

- Feature Extraction
  - JPEG
  - Proprietary Templates
  - Standardized Templates

Biometric encryption enables secure storage and allows for diversification

- Feature Extraction
- Biometric Encryption
- Diversity

- Small and secure binary hash templates
- Renewable and revocable templates
Existing work on Biometric Encryption

- In the academic world, biometric attention starts to receive full attention (fuzzy cryptography, fuzzy vault, fuzzy commitment)
  - Sometimes very complicated
  - Not all methods are practical (yet)
- Industry is working towards practical systems
  - IBM - cancelable biometrics
  - Philips - privID technology

Content

- Motivation

Biometric encryption in "3D Face"

- Outlook

Template Protection in "3D Face"

Basic System – Architecture Overview

Binarization plays an important role and determines the recognition performance
3D Face Recognition Systems

For evaluation we use 2 different 3D face recognition algorithms (Philips, Fraunhofer).

Verification Results – Real Feature Vectors

FRGC dataset

EER = 2.60%
EER = 2.37%

“Biometric encryption” on both 3D face algorithms gives similar classification results

<table>
<thead>
<tr>
<th>Feature Type</th>
<th>IGD</th>
<th>Philips</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raw vectors</td>
<td>1.35</td>
<td>1.35</td>
</tr>
<tr>
<td>Binary</td>
<td>1.75</td>
<td>1.43</td>
</tr>
</tbody>
</table>

Content

• Motivation

• Biometric encryption in “3D Face”

• Outlook
Take away

- Biometric encryption works!
  - In 3D Face, we show that classification performance of protected biometrics is comparable

- Biometric encryption is required to tackle privacy issues in biometric systems. Wide scale role out requires:
  - Technological developments (classification, fusion, security) for various modalities (face, fingerprint, iris, etc)
  - Integration in Identity Management systems
  - Standardization (e.g. ISO 24745)