PHILIPS

3D Face
Biometric Research

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

1

PHILIPS

www.ipc.on.ca

PHILIPS

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

PHILIPS

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

Feature Extraction

- JPEG
- Proprietary Templates
- Standardized Templates

PHILIPS

Biometric encryption enables secure storage and allows for diversification

Feature Extraction

Biometric Encryption

diversity

- Small and secure binary hash templates
- Renewable and revocable templates

2

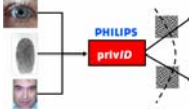**Slide 9 — Existing work on Biometric Encryption**

PHILIPS

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 - canceable biometrics

  - Philips - priv*ID* technology

  - ....

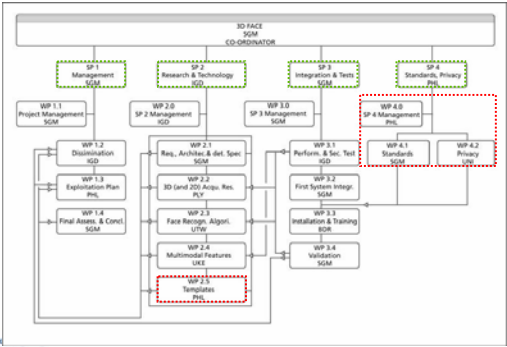3D Face end-user meeting (March 22, 2007, Darmstadt)   9

Slide 10 — Content

PHILIPS

Content

- Motivation

- Biometric encryption in "3D Face"

- Outlook

3D Face end-user meeting (March 22, 2007, Darmstadt)   10

Slide 11 — Template Protection in "3D Face"

PHILIPS

Template Protection in "3D Face"

3D Face end-user meeting (March 22, 2007, Darmstadt)   11

Slide 12 — Basic System – Architecture Overview

PHILIPS

Basic System – Architecture Overview

Binarization plays an important role and determines the recognition performance

Classification   Security

Noise Reduction & Quantization → Error Correction → Diversify → Hash/ Encrypt

Reduced Template Size
Exact Matching
Multiple Templates
Privacy Protection & Key Extraction
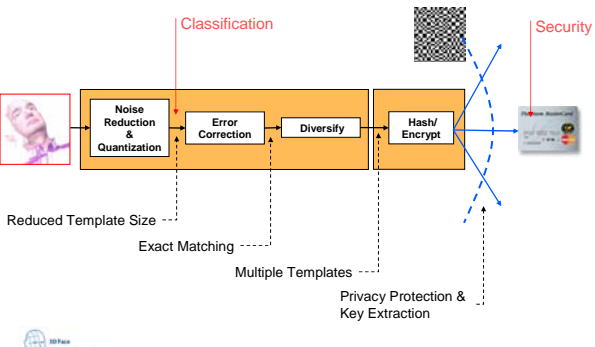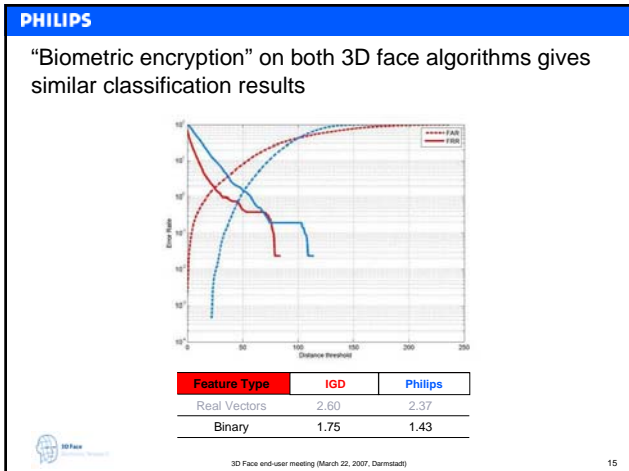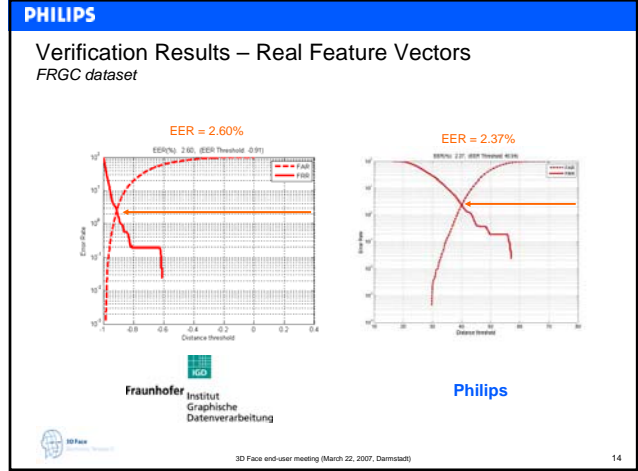
3D Face end-user meeting (March 22, 2007, Darmstadt)   12

3

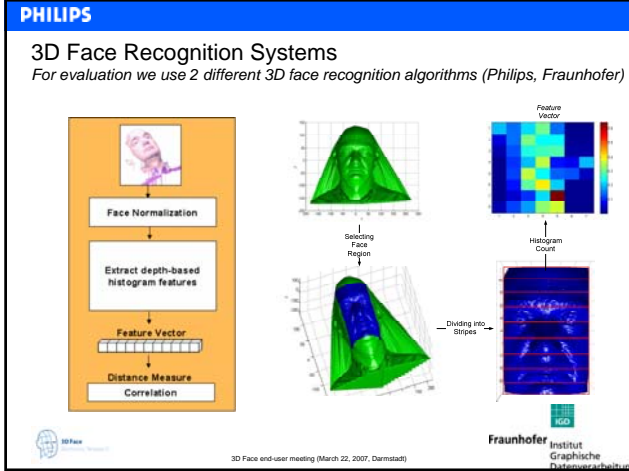### 3D Face Recognition Systems
For evaluation we use 2 different 3D face recognition algorithms (Philips, Fraunhofer)

Verification Results – Real Feature Vectors
FRGC dataset

EER = 2.60%

EER = 2.37%

Fraunhofer Institut Graphische Datenverarbeitung

Philips

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

Feature Type	IGD	Philips
Real Vectors	2.60	2.37
Binary	1.75	1.43

Content

- Motivation

- Biometric encryption in "3D Face"

- Outlook

PHILIPS

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)

3D Face
Biometric Research

5