




Biometric Encryption in "3D Face"


Michiel van der Veen
 "3D Face" end-user meeting
 March 22, Darmstadt, Germany



PHILIPS

Content

- Motivation
- Biometric encryption in "3D Face"
- Outlook




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

2

PHILIPS


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
-



MINORITY REPORT
EVERYBODY KNOWS YOUR MIND
JUNE 21

What about your (biometric) Identity?



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


3

PHILIPS


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 trust
 - 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



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

4

PHILIPS

www.ipc.on.ca

The image shows a screenshot of the Information and Privacy Commissioner of Ontario website (www.ipc.on.ca) on the left. On the right is a presentation slide titled "Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy". The slide features a red and black abstract pattern and lists the names of Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, and Alex Stojanov, Ph.D., Biometric Scientist, dated March 2007.

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

The slide includes three images illustrating biometric modalities: a 3D face scan, a fingerprint, and an iris scan.

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

PHILIPS

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

The diagram shows a 3D face scan being processed by "Feature Extraction". The resulting information is then spread to various applications, represented by icons for a credit card, a mobile phone, and a document. A list of template types is provided:

- JPEG
- Proprietary Templates
- Standardized Templates

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

PHILIPS

Biometric encryption enables secure storage and allows for diversification

The diagram illustrates the biometric encryption process. It starts with a 3D face scan, followed by "Feature Extraction", then "Biometric Encryption". The output is a secure binary hash template, which is then diversified into multiple versions. A list of template characteristics is provided:


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

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

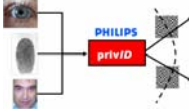
PHILIPS

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 - privID technology



–

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

PHILIPS

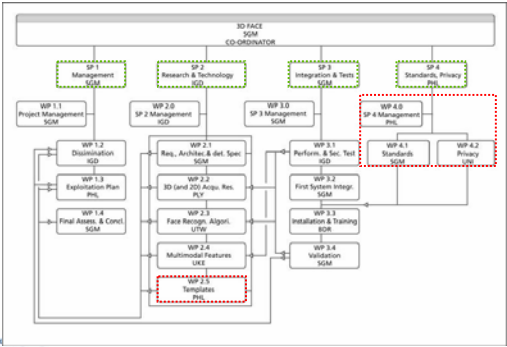
Content

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

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

PHILIPS

Template Protection in “3D Face”

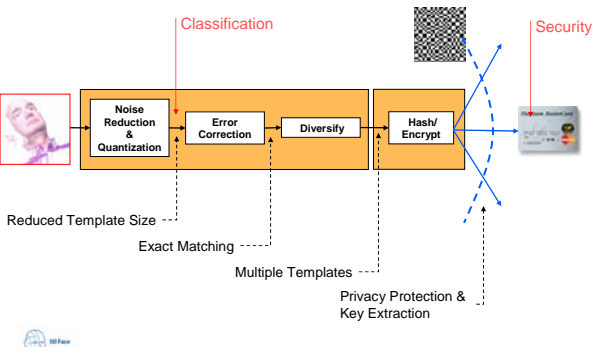


3D Face end-user meeting (March 22, 2007, Darmstadt) 11

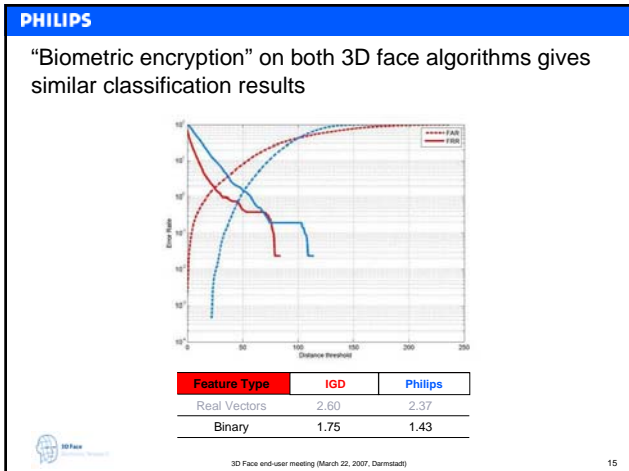
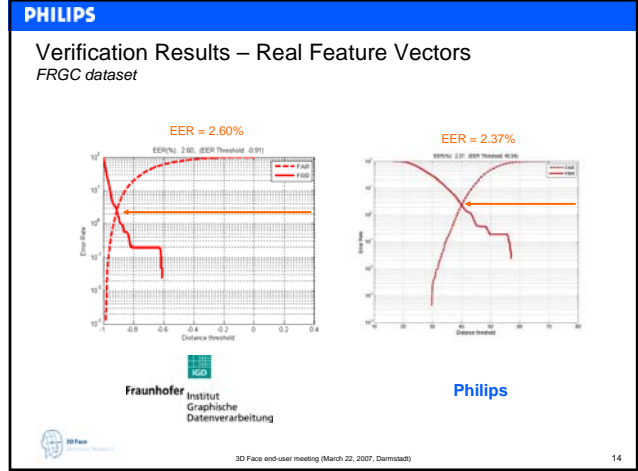
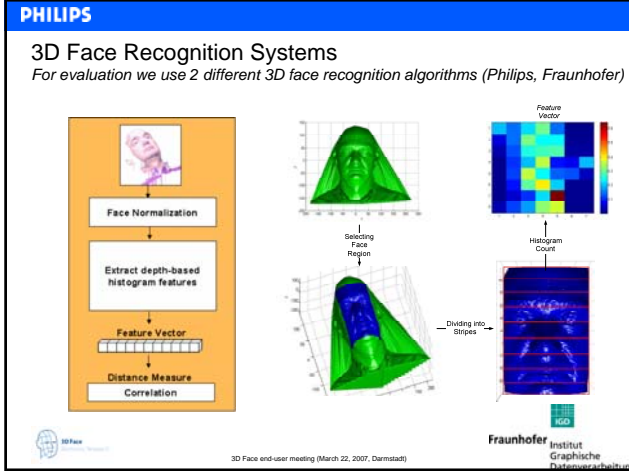
PHILIPS

Basic System – Architecture Overview

Binarization plays an important role and determines the recognition performance



3D Face end-user meeting (March 22, 2007, Darmstadt) 12



- PHILIPS**
- ### Content
- Motivation
 - Biometric encryption in “3D Face”
 - Outlook
- 3D Face end-user meeting (March 22, 2007, Darmstadt)

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)

