

PHILIPS

Privacy Protection in Biometrics

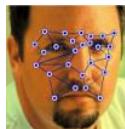
Bart van Rijnsoever
Philips Research

EU Hitachi Science and Technology Forum
May 20, 2006

PHILIPS

Biometrics

- Biometrics enhance the security of many services
- Biometrics add much convenience for the end-user when replacing passwords and PIN-codes



2

No part of the contents or materials available on this presentation may be reproduced, licensed, sold, published, transmitted, modified, adapted, publicly displayed, broadcast (including storage in any medium by electronic means whether or not transiently for any purpose save as permitted herein) without the prior written permission of the author

Biometric Applications

- Use of biometrics is increasing
 - Security (access control, transaction, tracing)
 - Personalization
- Security services
 - Automated Fingerprint Identification System
 - Visa Information System
- Biometric passports and identity cards
- Biometric access control systems
 - Building access
 - Computer or mobile phone log-on
 - Electronic banking
- Biometric ticketing
 - Boarding cards
 - Stadium tickets



Privacy and biometrics

- Identity theft
 - Adoption of someone else's identity
 - Abuse of biometric data for false identification or verification
 - Fingerprints can be copied and abused
 - Other biometrics are less vulnerable, e.g., iris scan
 - Centrally stored biometric data can be copied and abused
 - Protection of databases may fail

Privacy and biometrics

- Identity theft
- Cross-matching
 - Find a person's identity in a databases on the basis of biometric data
 - Trace a person's activities by matching biometrics data in different databases

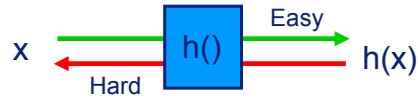
5

Privacy and biometrics

- Identity theft
- Cross-matching
- Extraction of medical data
 - Derive medical information from biometric data

6

Password protection using one-way hash function



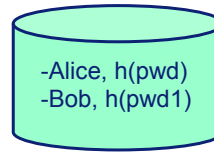
Trusted



1. Types pwd'
2. Computes $h(pwd')$

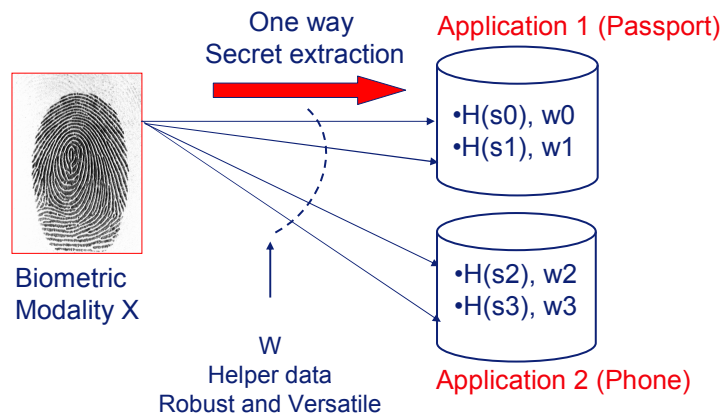
Untrusted

3. Alice, $h(pwd')$



4. Check:
 $h(pwd') == h(pwd)$

Biometric template protection

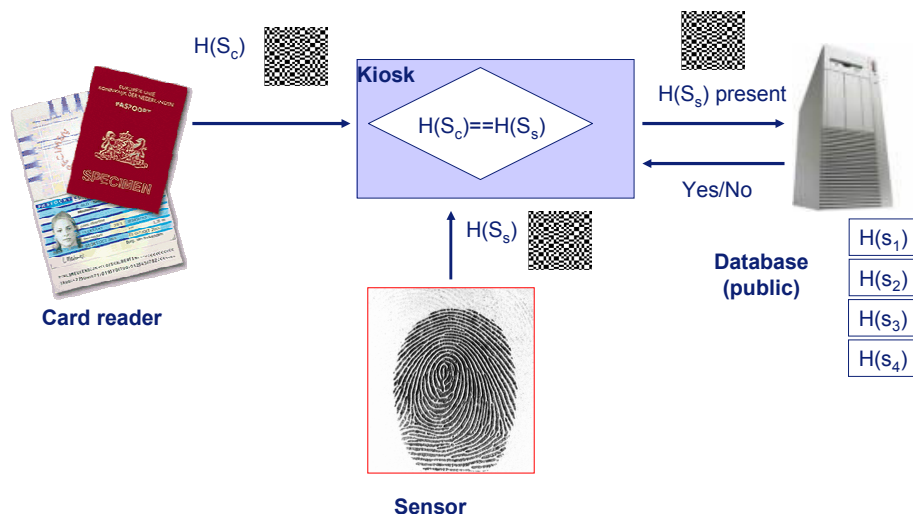


Biometric ePassport



- Look-alike-fraud
 - Use a passport of someone looking like yourself
- An electronically verify-able biometric modality prevents this fraud
 - Do person and passport match?
- Examples of Biometric data stored on the passport
 - Facial scan
 - Fingerprints
- Protection of biometric information
 - Unauthorized use of biometric data stored on passport
 - If biometric data is stored centrally, it might be used for unauthorized purposes

Biometric ePassport and template protection



Advantages biometric template protection

- Safe storage in centralized database
- Low-cost storage (small template size)
- Fast read-out and matching time

www.secure-identification.com

11

