



Biometrics and cryptography - *On biometric keys, their information content and proper use*

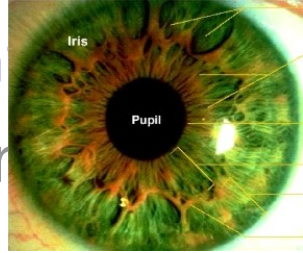
Rainer Plaga (BSI)

**Conference on Biometric Feature
Identification and Analysis, Göttingen,
7.9.2007**



Agenda

- ❑ Requirements protection of biometric information
- ❑ A chance: Protecting templates by applying error correcting and cryptographic methods
- ❑ A security challenge and requirements to meet it
 - ❑ Biometric keys with sufficient length for secure applications: future possibilities
- ❑ Achievable length of biometric keys
 - ❑ Theoretical estimation method
 - ❑ Estimates based on the results of “BioP2” field test
- ❑ Suitable use case for biometric keys - Summary



Security Requirements - Biometrics

- ❑ Biometrics = **Authentication** method - who is **authorised**? Other methods: e.g. smart card, password query
- ❑ template is the authentication information = e.g. finger print, equivalent to pass word:



= Fgj%67\$

Threat to biometric security

- ❑ **Threat:** Spying out the **templates** in the authentication-data storage file
- ❑ **Result:**
 - ❑ Attacker assumes false Identity
 - ❑ **Integrity of system is broken**
 - ❑ can happen also with password, **BUT** biometric features cannot be changed





Agenda

- Requirements protection of biometric information
- A chance: Protecting templates by applying error correcting and cryptographic methods
- **A security challenge and requirements to meet it**
 - Biometric keys with sufficient length for secure applications: future possibilities
- Achievable length of biometric keys
 - Theoretical estimation method
 - Estimates based on the results of “BioP2” field test
- Suitable use case for biometric keys - Summary





Protecting templates by applying error-correcting and cryptographic methods



- ❑ **Security mechanism:** Do not store: “**Template**” but: “**HASH(Template)**”. - For passwords **industry standard** (e.g. in Linux oder WindowsXP).
- ❑ This protects template because:
HASH(Template) \Rightarrow Template ist **computationally difficult** problem. Example: *Juels/Watteberg (1999)* see above, other implementations have been described
- ❑ For biometric this technique is not standard **up to now** because:
 - ❑ A. biometric templates are **noisy**.
 - ❑ B. biometric templates contain **to little information** to withstand “brute-force” attacks

Problem A. - „biometric noise“

- The transmission of biometric information must employ a „noisy channel“, three basic types:
 - 1. sensor noise
 - 2. environment noise
 - 3. Feature noise
 - 4. Algorithmic noise



3. Aenderung der Merkmale



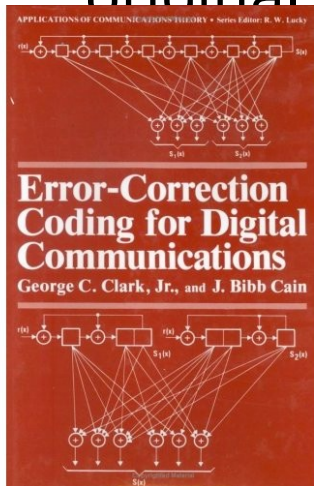
2. Aenderung Umgebungsbedingungen



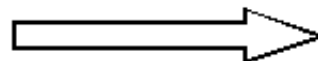
1. Sensorrauschen

Solution to „biometric noise“ problem 1

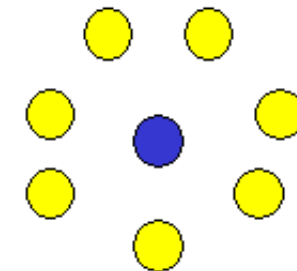
- ..is „error correction“
- The protected template is stored with additional „helper information“ that allows to remove the noise
- „Price“ paid: protected template shorter than original template „information loss“



Input



The channel



Possible output,
if up to one
error occurs.



Solution to „biometric noise“ problem 2



- ❑ Template is converted to a **„bit identical, unique data set that can be derived repeatedly from a user biometric (Hao et al., 2006)“**
- ❑ Call this data set: **„biometric key“**
- ❑ Biometric key can be hashed to cryptographically protect its biometric information



Solution to „biometric noise“ problem 3 - example values for Iris (Daugman 2003)



- ❑ Template with redundancy & noise, length **m** (2048) bits
- ❑ Compressed template with e (79.6) bits of noise: length **n** (249) bits.
- ❑ Compressed error corrected template a.k.a as „biometric key“ **k** (24.6) bits



Agenda

- Requirements protection of biometric informatic
- A chance: Protecting templates by applying error correcting and cryptographic methods
- **A security challenge and requirements to meet it**
 - Biometric keys with sufficient length for secure applications: future possibilities
- Achievable length of biometric keys
 - Theoretical estimation method
 - Estimates based on the results of “BioP2” field test
- Suitable use case for biometric keys - Summary



Brute force attacks on cryptographically protected templates 1

- „Dictionary attack“ -
E.g. „Sfinge“
tools (Capelli
et al.,
University of
Bologna)
allows
creation
„dictionary“ of
protected
fingerprint
templates



Biometric System Laboratory - SFinGe



Examples of fingerprints generated by Sfinge v2.5





Brute force attacks 2

- ❑ Online „crack services“ break (i.e. invert) hashes with a length of up to 40 bits at modest cost





Brute force attacks 3

- Consequence of possibility for „Dictionary attack“ - both for password and biometric template: entropy of password or „noise free (i.e. error corrected)“ template should be at least about **ca. 50 bits**



Agenda

- Requirements protection of biometric information
- A chance: Protecting templates by applying error-correcting and cryptographic methods
- **A security challenge and requirements to meet it**
 - Biometric keys with sufficient length for secure applications: future possibilities
- **Achievable length of biometric keys**
 - Theoretical estimation method
 - Estimates based on the results of “BioP2” field test
- Suitable use case for biometric keys - Summary

Biometrics idealized as a noisy, memoryless Shannon channel

- ❑ Information source: biometric feature of human
- ❑ Information sink: template in data base
- ❑ Assume:
 - ❑ *1. Template is free of correlations*
 - ❑ *2. No “algorithmic noise”*
 - ❑ *3. Number of noise bit “e” is constant*
 - ❑ *4. Extracted biometric information varies randomly from person to person (system is “ergodic”)*

Relation between FAR and biometric key length 1

- Hamming bound
- Number of possible keys $|C|$:

$$|C| \leq \frac{2^n}{\sum_{i=0}^e \binom{n}{i}}$$

Relation between FAR and biometric key length 2

- Hamming bound
- Number of possible keys $|C|$

$$\text{FAR} = P_{\text{id}} = \frac{\text{number of falsely matching templates}}{\text{number of all templates}}$$

$$\text{FAR} = \frac{\sum_{i=0}^e \binom{n}{i}}{2^n}$$

Relation between FAR and biometric key length 3

- length of biometric key:

$$k = \log_2(|C|)$$

$$k \leq -\log_2(\text{FAR})$$



Estimate of biometric key length from BioP2 FARs

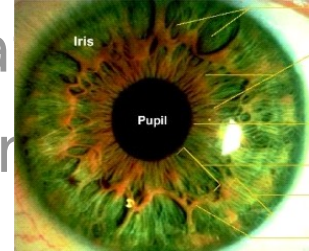


- From FAR results of „BioP2 project“ (biometric system test at Frankfurt International Airport): Finger and Iris : FRR=2%, FAR= 10^{-5} corresponding to $k \sim 17$ bits
- A protected template created from data of a **SINGLE** finger or iris feature taken within BioP2 cannot be longer than about **17 bits**



Agenda

- Requirements protection of biometric information
- A chance: Protecting templates by applying error correcting and cryptographic methods
- **A security challenge and requirements to meet it**
 - Biometric keys with sufficient length for secure applications: future possibilities
- Achievable length of biometric keys
 - Theoretical estimation method
 - Estimates based on the results of “BioP2” field test
- **Suitable use case for biometric keys - Summary**





Conclusion 1 - secure protection of biometric templates



- For a secure protection scheme at least one of the following three conditions must be met:
 - 1. *The technical performance of biometric systems is substantially improved*
 - 2. *More than one biometric feature (multi modal or multi instance) is used, e.g. more than one finger*
 - 3. *A novel feature with high information content is used for biometrics, e.g. DNA*



Conclusion 2 - secure protection of biometric templates



- 1. *Biometric features cannot be kept confidential*
- 2. *Biometric keys are best used to cryptographically protect stored biometric information against misuse*



Kontakt



Bundesamt für Sicherheit in der
Informationstechnik (BSI)
Dr. Rainer Plaga,
rainer.plaga@bsi.bund.de

www.bsi.bund.de
www.bsi-fuer-buerger.de