A Generalized Framework for Privacy and Security Assessment of Biometric Template Protection

Xuebing Zhou

CASED - Center for Advanced Security Research Darmstadt
Hochschule Darmstadt

Gaithersburg, March 09, 2012
Content

- Biometric template protection
- How to assess biometric template protection
  the systematic evaluation framework
- Assessment of different systems
- Conclusions
- Future work
Privacy and security risks
- Identity theft
- Unchangeability
- Cross matching
- Harm of privacy
Privacy and security risks

- Identity theft
- Unchangeability
- Cross matching
- Harm of privacy
Biometric Template Protection
Biometric Template Protection
Biometric Template Protection
Biometric Template Protection

Properties of protected templates (PT)
Biometric Template Protection

- Properties of protected templates (PT)
  - Irreversibility
Properties of protected templates (PT)
- Irreversibility
- Robustness
Properties of protected templates (PT)
- Irreversibility
- Robustness
- Diversity
Properties of protected templates (PT)
- Irreversibility
- Robustness
- Diversity
- Unlinkability
State of the Art of Template Protection

- Transformation-based algorithms
  - Biometric salting
    - Biometric encryption [Soutar99, Savvides04, Takaragi07 etc.]
    - Biohashing [Teoh04, Teoh09, Ao09 etc.]
  -Cancelable biometrics [Ratha01, Zuo08, Bolle09 etc.]

- Biometric cryptosystems
  - Fuzzy extractor [Dodis03]
  - Fuzzy commitment scheme [Juels99]
  - Helper data scheme [Tuyls04]
  - Fuzzy vault scheme [Juels02]
  - Quantization index modulation [Linnartz03, Buhan08]
Biometric Template Protection

ISO Architecture*

- Pseudonymous Identifier Encoder ($PIE$): $[PI, AD] = PIE(M)$, $M$ is observed biometric data in enrolment
- Pseudonymous Identifier Recorder ($PIR$): $[PI'] = PIR(M', AD)$, $M'$ is probe biometric data
- Pseudonymous Identifier Comparator ($PIC$): $v = PIC(PI, PI')$, $v$ is comparison result
- Stored protected template $[PI, AD]$, where $PI$ is pseudonymous identifier and $AD$ is auxiliary data

* ISO/IEC 24745 (2011) Information technology - Security techniques - Biometric Information protection
How to Assess Template Protection

- Protection goals - Evaluation criteria
  - **Security of PI**: Hardness to find an $M^*$ (“pre-image” of $PI$), which can pass $PI$-verification process
  - **Privacy protection ability**:
    - Irreversibility: Hardness to find an $M^*$, which is very close to the original $M$
    - Privacy leakage: Information about $M$ contained in protected templates
  - **Unlinkability**:
    - Cross matching: Personal identifiable information contained in protected templates
    - Leakage amplification: Additional information about $M$ or pre-image of $PI$ gained when combining protected templates of the same subject
How to Assess Template Protection

- Threat models - description of an adversary
  - Naive Model: Adversary has no information about the system
  - Advanced Model: Adversary has full knowledge of the algorithm (Kerckhoffs’ principle) and properties of biometric data
  - Collision Model: Adversary owns a large amount of biometric data and can exploit inaccuracies of the biometric system

- Distribution of biometric features
  - Important a priori information for an adversary
  - Essential for security and privacy assessment
How to Assess Template Protection

Evaluation framework

Protection Goals
- Objectives of evaluation (evaluation criteria)

Threat Models
- Ability and knowledge of an adversary
- Accessible system parameters

Theoretical Evaluation
- Independent of an attack algorithm

Evaluation
- Experiment with test data
- Measuring theoretical metrics e.g. conditional entropy, mutual information

Evaluation
- Experiment with test data
- Measuring efficiency of an attack, e.g. success rate, recovery rate

Analysis

Complementary results

Analysis
How to Assess Template Protection

Definition of security:

Let \( A(AD, PI) = [M', PI'] \) be a reconstruction function, where \( PI' = PIR(M', AD) \). \( T_A \) is the computational time required in one reconstruction and \( n \) is the average number of reconstructions needed to get a \( [M', PI'] \) such that \( PIC(PI, PI') = 1 \) for a positive authentication result.

Then, a template protection algorithm is \((T, \epsilon)\)-secure, if for all \( A \)

\[
T_A \geq T \\
\log_2 n \geq \epsilon
\]
How to Assess Template Protection

- Definition of security:
  - Let \( A(AD, PI) = [M', PI'] \) be a reconstruction function, where \( PI' = PIR(M', AD) \). \( T_A \) is the computational time required in one reconstruction and \( n \) is the average number of reconstructions needed to get a \( [M', PI'] \) such that \( PIC(PI, PI') = 1 \) for a positive authentication result.
  - Then, a template protection algorithm is \((T, \varepsilon)\)-secure, if for all \( A \)
    \[
    T_A \geq T \\
    \log_2 n \geq \varepsilon
    \]
How to Assess Template Protection

Definition of security:
- Let $A(AD, PI) = [M', PI']$ be a reconstruction function, where $PI' = PIR(M', AD)$. $T_A$ is the computational time required in one reconstruction and $n$ is the average number of reconstructions needed to get a $[M', PI']$ such that $PIC(PI, PI') = 1$ for a positive authentication result.
- A template protection algorithm is ($T, \varepsilon$)-secure, if for all $A$
  \[
  T_A \geq T \\
  \log_2 n \geq \varepsilon
  \]

Definition of privacy:
- Let $A(AD, PI) = [M', PI']$ be a reconstruction function, where $PI' = PIR(M', AD)$. $T_A$ is the computational time required in one reconstruction; for a given threshold $t$, $n$ is the average number of reconstructions needed to get a $[M', PI']$ such that for a distance function $dist(M, M') < t$.
- A template protection algorithm is ($t, T, \varepsilon$)-preserving, if for all $A$
  \[
  T_A \geq T \\
  \log_2 n \geq \varepsilon
  \]
Assessment of Different Protected Systems

- The fuzzy commitment scheme for 3D face recognition
- The fuzzy commitment scheme for iris recognition
- The fuzzy vault algorithm for fingerprint recognition
## Assessment of Different Protected Systems

### Security assessment

<table>
<thead>
<tr>
<th>System</th>
<th>$L_S$</th>
<th>Naive Model</th>
<th>Advanced Model</th>
<th>Collision Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>3D Face Fuzzy Commitment</td>
<td>71 bit</td>
<td>70 $O(1)$</td>
<td>11.13 $O(1)$</td>
<td>$\varepsilon=-\log_2(FAR)$ FAR@FRR 6.48 1.12%@19.97%</td>
</tr>
<tr>
<td>Iris Fuzzy Commitment</td>
<td>72 bit</td>
<td>71 $O(1)$</td>
<td>14.25 $O(1)$</td>
<td>7.41 0.59%@22.74%</td>
</tr>
<tr>
<td>Fingerprint Fuzzy Vault*</td>
<td>128 bit</td>
<td>127 $O(1)$</td>
<td>34.54 $O(n \log^2(n))$</td>
<td>13.29 0.01%@9%</td>
</tr>
</tbody>
</table>

Assessment of Different Protected Systems

Privacy protection ability in the advanced model:

- High privacy leakage, which can cause cross matching and leakage amplification
- Irreversibility is measured with the privacy definition for $t=0$. It shows computational complexity to retrieve the original biometric features

<table>
<thead>
<tr>
<th>System</th>
<th>$L_s$</th>
<th>Privacy leakage</th>
<th>Irreversibility</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>$\epsilon$</td>
</tr>
<tr>
<td>3D Face Fuzzy Commitment</td>
<td>71 bit</td>
<td>77.5 bit</td>
<td>74.2 bit</td>
</tr>
<tr>
<td>Iris Fuzzy Commitment</td>
<td>72 bit</td>
<td>4311 bit</td>
<td>14.25 bit</td>
</tr>
<tr>
<td>Fingerprint Fuzzy Vault*</td>
<td>128 bit</td>
<td>892.59 bit</td>
<td>34.54 bit</td>
</tr>
</tbody>
</table>

Assessment of Different Protected Systems

- Unlinkability in the advanced model:
  - Cross matching is a serious problem
  - It should be avoided to use any personal identifiable information in the systems
  - Additionally, the privacy leakage is unavoidable in these system due to error tolerance, but it should be minimized

<table>
<thead>
<tr>
<th>System</th>
<th>Cross matching</th>
<th>Leakage Amplification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3D Face Fuzzy Commitment</td>
<td>🙁 EER=5%</td>
<td>😊 no feasible attack yet</td>
</tr>
<tr>
<td>Iris Fuzzy Commitment</td>
<td>🙁 EER=16.34%</td>
<td>😋</td>
</tr>
<tr>
<td>Fingerprint Fuzzy Vault*</td>
<td>no assessment in the paper</td>
<td>no assessment in the paper</td>
</tr>
</tbody>
</table>

Conclusions

- The framework is useful to detect vulnerabilities of the existing algorithms.
- The framework enables rigorous assessment, which is important and necessary for the development of template protection.
- All the protection goals need to be taken into account.
- Threat models are the important prerequisites. Security and privacy protection ability of a system can be overestimated, if unrealistic assumption is made.
- Unique and measurable metrics such as the metrics used in the security and privacy definitions, are necessary for ranking of different algorithms.
Future Work

- Universal and constructive criteria, which can guarantee security and privacy performance of template protection
- An extended evaluation including both security and recognition performance
- Benchmarking and certification for template protection
References


- Zhou, Xuebing; Kuijper, Arjan; Busch, Christoph: Cracking Iris Fuzzy Commitment In: IEEE the International Conference on Biometrics (ICB 12), 2012

- Zhou, Xuebing; Kuijper, Arjan; Veldhuis, Raymond; Busch, Christoph: Quantifying Privacy and Security of Biometric Fuzzy Commitment In: IEEE the International Joint Conference on Biometrics (IJCB 11), 2011