Addressing Privacy issues in high security biometrics recognition applications

Dr. Nalini K Ratha*
Exploratory Computer Vision Group
IBM T. J. Watson Research Center
Hawthorne, NY 10532

*Joint work with members of biometrics research team
Privacy Issues

• Biometrics is secure but not secret

• It is the strongest form of personally identifying information

• You are giving away a part of yourself.

• Cross matching can be used to track individuals without consent (Allows institutions to share data. Allows attack at the weakest point)

• If a biometric is lost or stolen, it is compromised forever

• It cannot be revoked or replaced (while you can change your phone number or credit card number)

Is there a backwards compatible solution for privacy preserving authentication?
Hash Functions: Ideal for passwords and text

HIRE ALL LINUX PROGRAMMERS

FIRE ALL LINUX PROGRAMMERS

MD5

33B21856A91D2FBB
5BC4144C69B23F85

1 character difference

65 bits difference !!!!

43C08679B2FD54C6
5467DDCC9C00AD49

Can we simply hash a fingerprint?!
Hashing: Doesn’t work for biometrics

- 26 points match
- 15 points don’t match

MD5

F313C86188DDE96b
D48AD58CDECDB9E8

Don’t match at ALL!!

MD5

80BC979099C2FA64
3E4C5432A03E01B8

OK
Do templates hide the true identity already?

- It is often believed that the biometrics templates once extracted from the biometrics signal will not be helpful in generating the signal.
- Recent research has shown that from a fingerprint template, a possible fingerprint image can be generated that can fool a recognition system >80% of the time.
- Hence, the biometrics systems need to be careful in exposing the features in clear.
Related work

<table>
<thead>
<tr>
<th>Authors</th>
<th>Technique</th>
<th>Method</th>
<th>Registration Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Soutar et al. 98</td>
<td>Biometric Encryption</td>
<td>Random phase matrix (Fourier domain)</td>
<td>Requires absolute registration</td>
</tr>
<tr>
<td>Ratha et al. 08</td>
<td>Cancelable biometrics</td>
<td>Geometric distortion</td>
<td>Requires absolute registration</td>
</tr>
<tr>
<td>Uludag et al. 04</td>
<td>Fuzzy vault</td>
<td>Error tolerant set encoding</td>
<td>Requires absolute registration</td>
</tr>
<tr>
<td>Teoh et al. 04</td>
<td>Bio-hashing</td>
<td>Random projection (Global texture descriptor)</td>
<td>Quantization reduces individuality</td>
</tr>
<tr>
<td>Tulyakov et al. 05</td>
<td>Complex hashing</td>
<td>Geometric hash function</td>
<td>No registration required</td>
</tr>
</tbody>
</table>
Cancelable Biometrics

- Intentional **repeatable** distortion
  - Generates a similar signal each time for the same user

- Compromised scenario:
  - a new **distortion** creates a new biometrics

- Comparison scenario:
  - **different** distortions for different accounts

- **Backwards compatibility**
  - Representation is not changed.

© New Yorker Magazine (Charles Addams)
Challenges

Registration

Transformation

Same?

Intra-user variation
Feature Domain Transformation

Feature Extraction

Cartesian Transformation

Polar Transformation

Surface Folding Transformation
Invariant features

- Independent triangle features
  - The sides
- Dependent triangle feature
  - Height at largest side
- Fingerprint features
  - Minutiae angles with respect to triangle
Triangles can be enumerated

\( (s_1, s_2, s_3) \)

Quantize
Constrain side lengths

\( s_1, s_2, s_3 \) quantized using \( p \) bits

Impossible and possible triangles

\( (s'_1, s'_2, s'_3) \)
Enrolment

Minutia Triplets

Triangle Indexing

Triangle Hashing

Binarization

Mutation

Randomization

Encryption
Verification

Enrolled Token + Template
Steps in building a cancelable iris system

- Segmentation
- Feature extraction
- Cancelable techniques ♦
Method 1: GRAY COMBO

- template based row shift and combination
  - Step 1: for each row shift circularly:
    - Intensity +, -
    - One row can be used more than once
    - Easy methods: odd+even, fold like a mirror

- Step 2: combine two rows together to get a new one:
  - Combine rows 1, 3 to the new 1st row
  - Combine rows 2, 8 to the new 2nd row
  - Combine rows 4, 6 to the new 3rd row
  - Combine rows 5, 7 to the new 4th row
Method 2: BIN COMBO

- code based row shift and combination
  - Step 1: for each row shift circularly:

- Step 2: combine two rows together to get a new one:
  - Binary XOR, or NXOR
  - One row can be used more than once
  - Easy methods: odd+even, fold like a mirror

Combine rows 1, 3 to the new 1st row
Combine rows 2, 8 to the new 2nd row
Combine rows 4, 6 to the new 3rd row
Combine rows 5, 7 to the new 4th row
Method 2: example

Shift Strength: 0

Shift Strength: 10

Shift Strength: 40

Shift Strength: 240
Method 2: example (cont.)

- Odd XOR Even
- Odd XOR (NOT Even)
- Top XOR Bottom
- Random Combination
Method 3: GRAY SALT

- **template based salty noise**
  - Just plus a unique pattern --- random noise, random pattern or random synthetic iris texture
  - Generate new code according to the new texture
Example

\[ + \]

\[ \rightarrow \]

\[ + \]
Method 4: BIN SALT

- code based salty noise
  - Just plus a unique binary pattern --- random noise, random pattern or random synthetic iris code
Example

\[ \text{Image 1} + \text{Image 2} \rightarrow \text{Image 3} \]
Matcher

- Assume head tilt is not heavy
- Matching algorithm need to be modified:
Conclusions

- Large biometrics systems need to be aware of potential biometrics database losses and other attacks on biometrics authentication process.
- Secure matching (inside a secure coprocessor) of biometrics can enhance security.
- Many options are available in building privacy enhanced biometrics systems.
  - Cancelable biometrics can enhance privacy.
  - We demonstrated examples of cancelable fingerprint and iris systems.
  - Cancelable/revocable/anonymous has been used interchangeably.
  - Legal/policy issues not part of this talk.
- TURBINE, RISE, Ontario Privacy commissioner report – where are we in the US?
Observations

- Many high security applications use/will use biometrics-based identification and authentication
  - Watch lists
  - On-line citizen services
  - Credit card transaction authorizations
  - Background checks
  - Passport/drivers license issue
  - Secure installation access
  - Mobile payments
- Biometrics is expected to provide the non-repudiable verification for the identity
- Such systems need to be aware and enhance security and privacy risks with handling biometrics data
- The biometrics databases are often very huge
- Smaller enterprise (e.g., retail stores) will not invest in protecting the biometrics data
Large collection leads to privacy issues

... Two sides of the same coin