Biometric Jammer: Method to Prevent Unauthorized Capturing of Fingerprint in Consideration of User-friendliness

Translated version of presentation slides in Computer Security Symposium 2016 (http://www.iwsec.org/css/2016/)

January 16, 2017

Tateo OGANE and Isao ECHIZEN

National Institute of Informatics
Contents

1. Background and purpose of study
2. Principle of fingerprint authentication
3. Proposed method
4. Evaluation
1. Background and purpose of study
Background

Spread of fingerprint sensors

- Government and law enforcement
- Entry and exit control

Penetration of smartphones with fingerprint sensors[1]

---

PC

Smartphone

Downsizing of fingerprint authentication devices

Rapid increase of smartphones with fingerprint sensors

[1] Fingerprint sensor penetration in smartphone market to rise above 50% in 2017
http://www.digitimes.com/pda/a20160818PD208.html
Background

Threat of fingerprint stealing from shot images

Demonstration of fingerprint hacking by German hacker starbug (Jan Krissler) (Dec 2014)[2]
- Restored image from a picture of 3 meters away with commercial digital camera and several photos obtained in public
- Detected fingerprint from the image using commercial software VeriFinger
- Separately demonstrated to authenticate with iPhone 6 fingerprint sensor using rubber-like fake finger[3]
- Not demonstrated fingerprint authentication from restored image itself yet

Background

Fake fingers: known vulnerability of fingerprint sensors

Attacks can make fingerprint copies (fake fingers) which can be falsely recognized by fingerprint sensors by mold fingerprints precisely using various materials[4][5]. They can impersonate or log in illegally using fake fingers made from residual fingerprints.

Background

Traditional fingerprint hacking

- Residual fingerprints

Fake fingers

Fingerprint hacking with shooting

- Photographs

Restoration

Fake fingers

- Attacker does not need to obtain fingerprints physically
- No technical countermeasures to prevent from unintentionally capturing of fingerprints
Conventional measures: wearing gloves

Regular gloves

Touchscreen gloves

Touchscreen sticker on gloves

Even simple gloves can prevent secret shooting
No response with fingerprint sensors

Wearer can manipulate touchscreen with gloves on
Authentication with fingerprint sensors is not supported

Special pattern can be authenticated with Apple TouchID fingerprint sensors
Not a wearer’s own fingerprint

There is no definitive product with which fingerprint authentication is performed well
Purpose and means

Purpose: prevent illegal acquirement of fingerprint by shooting while ensuring user’s convenience
  • authenticate with contact-based fingerprint sensors
  • not authenticate from shot images
  • User-centric control: no need for enforcement in sensors and authentication systems

Means: proposition of attachable jamming patterns

Fingerprint sensors | Authenticable
Digital cameras | Not authenticable
2. Principle of fingerprint authentication
Principle of fingerprint sensors[6][7]

- Maps distribution of electrostatic capacitance between skin and electrode into voltages
- Electrostatic capacitance is affected by the distance from contact plane to skin surface

- Detects light reflection by the optical prism with image sensor
- Lights are scattered at the boundary of the prism on ridges
- Lights are totally reflected at the boundary of the prism on valleys

Feature point detection[8][9]

Fingerprint image  Restoring fingerprint  Detecting feature points

Example of feature point mapping[10]:

\[ p = \{x, y, t\} \]

\((x, y: \text{position}, t: \text{orientation})\)


Fingerprint matching

- Identify a person by comparing feature points between registered image and input image
- Faster and less data as it is a pattern matching problem between point clouds
- More secure as it does not need to store fingerprint images

http://www.nature.com/nature/journal/v449/n7158/box/449038a_BX1.html
Obtaining fingerprints from shot images

A lot of noise since the image is the sampled result of diffuse lights

Contrasts between ridges and valleys are differ by location

Unevenness of skin colors resulted by perspiration and blood vessels

Impossible to recognize fingerprints from shot images directly
Adaptive binarization

- A kind of special filtering
- Calculate binarization threshold $d(x, y)$ to an average of pixel brightness $I(x, y)$ in the local domain $D$

$$d(x, y) = \frac{1}{N} \sum_{x, y \subset D} I(x, y)$$

- Take the value near the ridge interval as a kernel size $k$ and the filter emphasizes fingerprint patterns eliminating the noises.
3. Proposed method
Proposed method

**Pattern layer**
- Light scattering properties in visible wavelength
- No need to cover all fingerprint
  → Capable of modifying disturbing effect and visual design
Material candidates: Zinc oxide or Titanium dioxide

**Base layer**
- Light transmission property in visible wavelength
- Cohesive to all ridges on contact and makes no bubbles
  → Capable of authentication by contact-based fingerprint sensors
Material candidates: Rubbers, silicones or food additives
Transparency against capacitive fingerprint sensors

- Details of scanned image are affected by the distance between contact place and skin surface.
- If base and pattern layer are thin enough, the electrostatic capacitance of both layers does not prevent the sensor from detecting fingerprint image (less than about 0.05 millimeters).

Influence of film thickness:
- Thinner
- Details are gradually lost
- Thicker
Transparency against optical fingerprint sensors

- Details of scanned image are affected by the existence of air bubbles between contact place and skin surface
- If base and pattern layer are thin enough, they do not affect condition of total reflection since the materials of them have some transmittance

Influence of film thickness

Air bubbles increase according to the paint thickness

Acquired image

Outline
Consideration of disturbing effect

When adaptive binarization is applied to the image on which jamming pattern is overlapped, the pattern plays a role of noise which is classified as below:
- Occurrence of fake feature points. Edges of the pattern are falsely recognized as ridges.
- Vanishing of original feature points. Ambiguous judgement of ridge ending and bifurcation excludes true positives.
- Type change of feature points. Judgement threshold changes by the existence of the pattern.
Noise invalidation attack by repainting the jamming pattern

Original image → Extracted pattern → Composited image

Interpolate pixels on the jamming pattern by sampling surrounding pixels

Noise decreases
Designing resistant patterns against noise invalidation attack

Recognize fingerprint images on which dots of the variable size are overlapped

Color types
(a) Light gray
(b) Average color of the finger
(c) Average color of surrounding pixels of the dot
(b)(c) are supposed as repainted images of noise invalidation attack

LPI: lines per inch
Matching result of pattern design

(a) Light gray

(b) Average color of the finger

- Higher cover rate is more effective
- Lower pattern resolution is more effective for same cover rate

(c) Average color of surrounding pixels of the dot

Required high cover rate and low pattern resolution (large pattern size)
4. Evaluation
Making prototype for evaluation

Appearance

Diagram

Base

Pattern

Skin

40% cover rate

Procedure

1. Paint base material (acrylic emulsion) over the fingerprint

2. Soak a cosmetic puff with pattern material (acrylic paint)

3. Transcribe pattern material into the finger tip using a stencil for nail art
Matching against shot images

Registration

Input types
- Not attached
- Attached
- Attached and pattern repainted

Input

Matching

After adaptive binarization

Can fingers attached BiometricJammer disturb fingerprint authentication from shot images?
Matching against fingerprint sensors

Registration

Input

Input types

Attached

Matching (3 x 3 = 9 times)

Can fingers attached BiometricJammer pass fingerprint authentication with contact-based fingerprint sensors?
### Environment for evaluation

<table>
<thead>
<tr>
<th>Attachment</th>
<th>Digital camera</th>
<th>Fingerprint sensors</th>
</tr>
</thead>
</table>
| - Base material: acrylic emulsion  
- Pattern material: acrylic paint including zinc oxide  
- Cover rate: 40% | - Body: Canon EOS 70D  
- Resolution: about 20 megapixels  
- ISO sensitivity: auto  
- Exposure: auto  
- Focusing: 1-point AF  
- Lens: Canon EF-S 18-135mm F3.5-5.6 IS STM | DigitalPersona EikonTouch 710  
(capacitive sensing)  
DigitalPersona U.are.U 4500  
(optical sensing) |

<table>
<thead>
<tr>
<th>Shooting environment</th>
<th>Fingerprint matching program</th>
</tr>
</thead>
</table>
| - Tester: 4 graduate students  
- Distance: 1 to 5 meters at 0.5m intervals  
- Lighting condition: outdoors, cloudy or sunny  
- Subject illuminance: 7800 to 31600 lx | Neurotechnology VeriFinger[11]  
(commercial software) |

http://www.neurotechnology.com/verifinger.html
Matching result against shot images

Number of persons matched per shooting distance

Using a capacitive sensor

- Succeeded to authenticate fingers from shot images at the distance of 3 meters or less using commercial digital camera
- Succeeded to disturb fingerprint authentication of fingers attached BiometricJammer at any distance, even the jamming patterns are repainted
Matching result against shot images

Average match score per shooting distance

Using a capacitive sensor

- Match score: A score according to similarity of arrangement of feature points
- In case of VeriFinger, two fingerprints are regarded as matched when the score is 48 or above at the 0.01 percent FAR (False Acceptance Rate)
- If the program failed to detect any feature point, match score is considered to be zero
Matching result against fingerprint sensors

Using a capacitive sensor

<table>
<thead>
<tr>
<th>Tester</th>
<th>Number of success</th>
<th>Minimum score</th>
<th>Maximum score</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>9</td>
<td>262</td>
<td>441</td>
</tr>
<tr>
<td>B</td>
<td>8</td>
<td>44</td>
<td>211</td>
</tr>
<tr>
<td>C</td>
<td>9</td>
<td>163</td>
<td>276</td>
</tr>
<tr>
<td>D</td>
<td>9</td>
<td>59</td>
<td>158</td>
</tr>
</tbody>
</table>

Using an optical sensor

<table>
<thead>
<tr>
<th>Tester</th>
<th>Number of success</th>
<th>Minimum score</th>
<th>Maximum score</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>9</td>
<td>196</td>
<td>333</td>
</tr>
<tr>
<td>B</td>
<td>3</td>
<td>19</td>
<td>80</td>
</tr>
<tr>
<td>C</td>
<td>9</td>
<td>263</td>
<td>370</td>
</tr>
<tr>
<td>D</td>
<td>9</td>
<td>179</td>
<td>375</td>
</tr>
</tbody>
</table>

Red letter: matched (score of 48 or above)

Failure case: unstable finger position (pressure and direction) at the registration

Succeeded to pass fingerprint authentication of fingers attached BiometricJammer