BiometricJammer: 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

http://politicsofcolor.com/wp-content/uploads/2015/04/dongjae-feat1.jpg

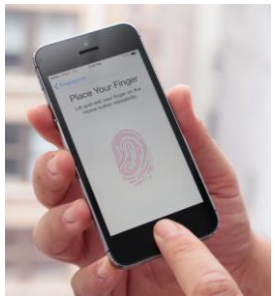
Entry and exit control

https://www.nisseicom.co.jp/column/column_security/07.images/column_image-02.jpg

PC

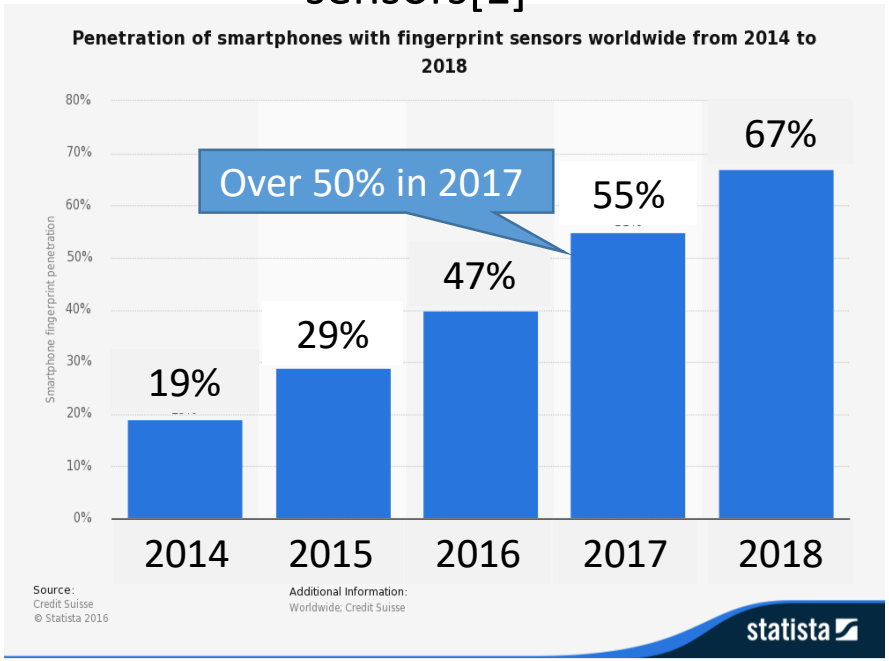
https://ja.wikipedia.org/wiki/%E7%94%9F%E4%BD%93%E8%AA%8D%E8%A8%BC#/media/File:Reading_Fingerprint.jpg

Smartphone



http://payprotec.com/wp-content/uploads/2014/06/Septimius_02_610x436.jpg

Penetration of smartphones with fingerprint sensors[1]



http://www.statista.com/statistics/522058/global-smartphone-fingerprint-penetration/

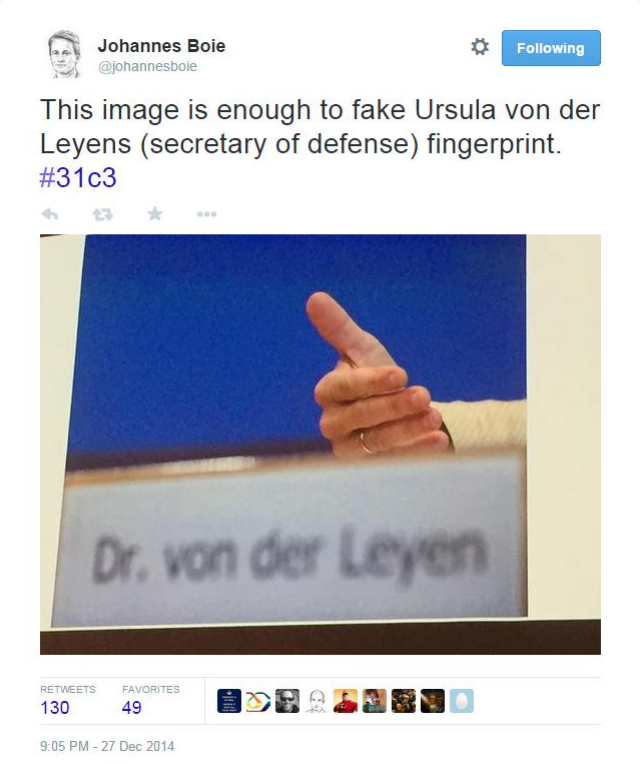
Downsizing of fingerprint authentication devices

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



https://www.shellandco.net/wp-content/uploads/2014/12/tweet_finger.png

https://www.youtube.com/watch?v=pIY6k4gvQsY

https://www.youtube.com/watch?v=pIY6k4gvQsY

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

[2] Fingerprint Biometrics hacked again
https://www.ccc.de/en/updates/2014/ursel

[3] Chaos Computer Club breaks Apple TouchID
http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

Background

Fake fingers: known vulnerability of fingerprint sensors

http://ichef-1.bbci.co.uk/news/660/media/images/74270000/png/_74270693_fake.png

http://regmedia.co.uk/2013/09/22/iphone5_touchid_crack.png?x=648&y=348&crop=1

https://i.ytimg.com/vi/KBMqoUYxUJs/sddefault.jpg

http://www.zdnet.com/article/apples-advanced-fingerprint-technology-is-hacked-should-you-worry/

Attackers 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

[4] Putte and Keuning. “Biometrical Fingerprint Recognition: Don’t Get Your Fingers Burned,” in Proc. Working Conf. on Smart Card Research and Advanced Applications (4th), Proc. IFIP TC8/WG8.8, pp. 289-303, 2000.
[5] Matsumoto et al.. “Impact of Artificial “Gummy” Fingers on Fingerprint Systems,” in Proc. Of SPIE, vol. 4677, pp. 275-289, 2002.

Background

Traditional fingerprint hacking

Residual fingerprints

https://en.wikipedia.org/wiki/Fingerprint#/media/File:Dacty_poederen.JPG

Fake fingers

http://www.zdnet.com/article/apples-advanced-fingerprint-technology-is-hacked-should-you-worry/

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

https://www.kaunet.com/images/goods/main/large/K2704302.jpg

Even simple gloves can prevent secret shooting

No response with fingerprint sensors

Touchscreen gloves

http://direct.sanwa.co.jp/images/goods/200-PEN001BK_MX.JPG

Wearer can manipulate touchscreen with gloves on

Authentication with fingerprint sensors is not supported

Touchscreen sticker on gloves

https://www.kickstarter.com/projects/nanotips/taps-touchscreen-sticker-w-touch-id-ships-before-x

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

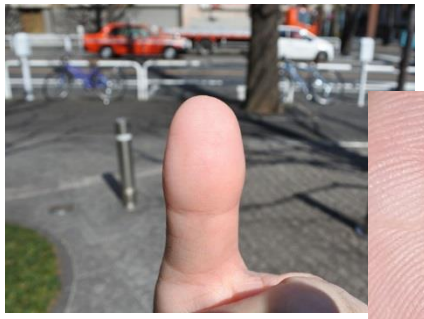
- authenticate with contact-based fingerprint sensors
- not authenticate from shot images
- User-centric control: no need for enforcement in sensors and authentication systems

Means: proposition of attachable jamming patterns

Fingerprint sensors

Authenticable

Digital cameras

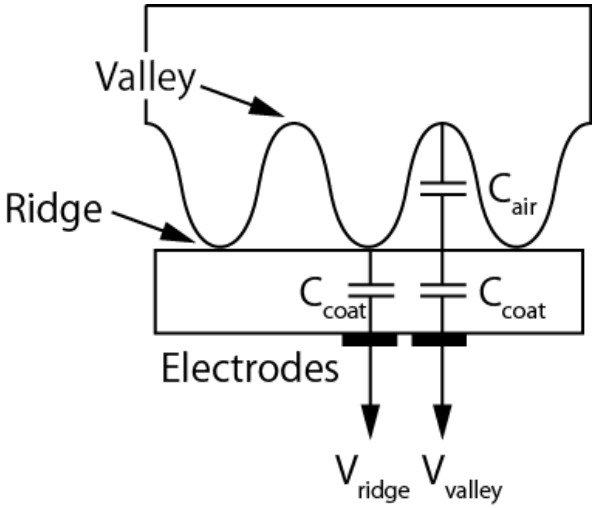


Not authenticable

2. Principle of fingerprint authentication

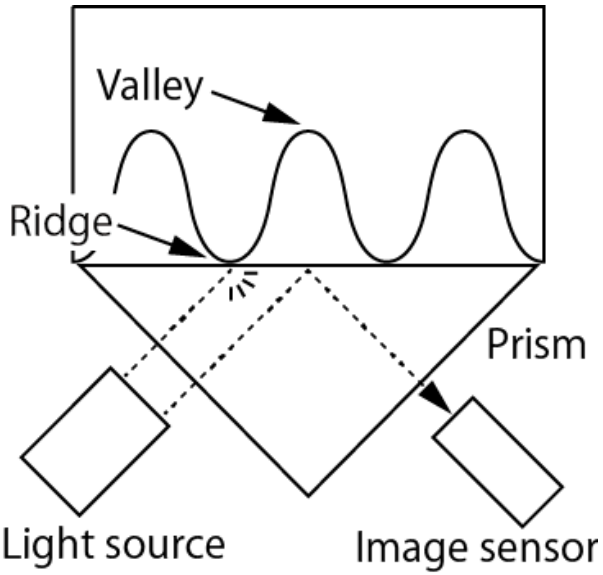
Principle of fingerprint sensors[6][7]

Capacitive sensor



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

Optical sensor



- 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

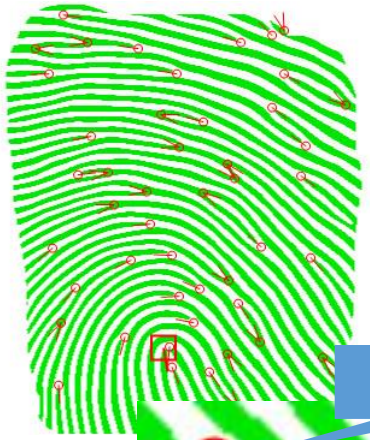
[6] Japan patent office, standard technology collection, “Input and recognition of biometric verification” (in Japanese), http://www.jpo.go.jp/shiryou/s_sonota/hyoujun_gijutsu/biometric/mokuji.htm
[7] Ichiro Fujieda, “Basics of image input and output devices” (in Japanese), Morikita Publishing, 2005

Feature point detection[8][9]

Fingerprint image

Restoring fingerprint

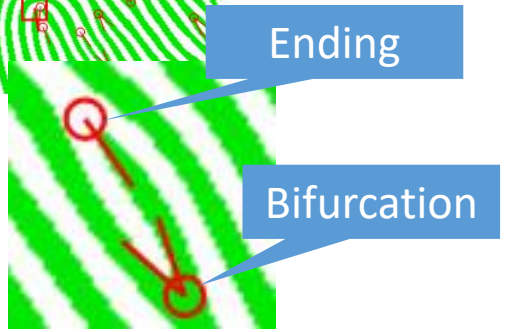
Detecting feature points



Example of feature point mapping[10]:

$p = \{x, y, t\}$

$(x, y$: position, t : orientation$)$



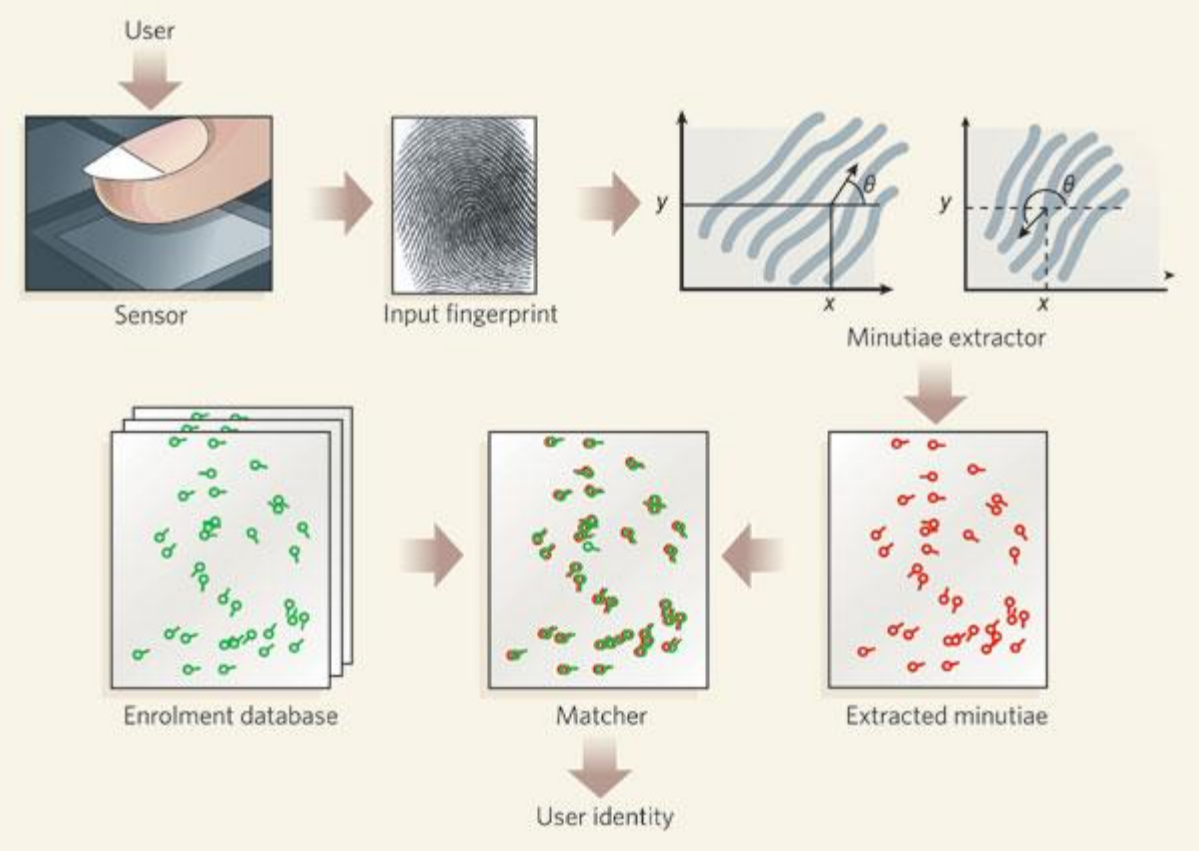
Feature points (minutiae)

[8] Jain et al.. "On-line Fingerprint Verification," IEEE Transactions on Pattern Analysis Machine Intelligence, vol.19, no.4, pp. 302-313, 1997.

[9] Hong et al.. "Fingerprint Image Enhancement: Algorithm and Performance Evaluation," IEEE Transactions on Pattern Analysis Machine Intelligence, vol.20, no. 8, pp. 777-789, 1998

[10] National Institute of Standards and Technology, "User's Guide to Expert Controlled Distribution of NIST Biometric Image Software (NBIS-EC)," http://www.nist.gov/customcf/get_pdf.cfm?pub_id=51096

Fingerprint matching

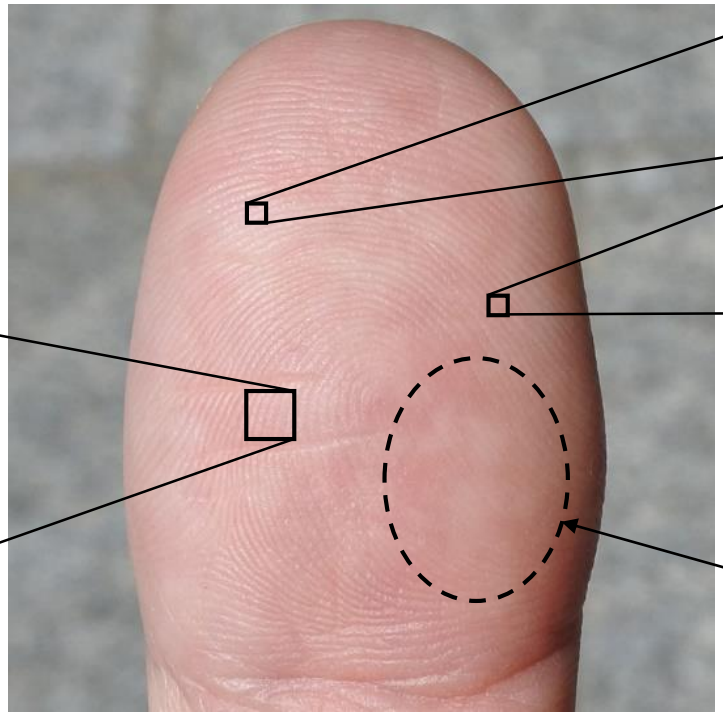


http://www.nature.com/nature/journal/v449/n7158/box/449038a_BX1.html

- 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

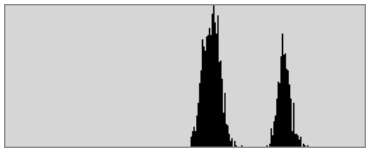
Obtaining fingerprints from shot images

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



Shot image

Histograms

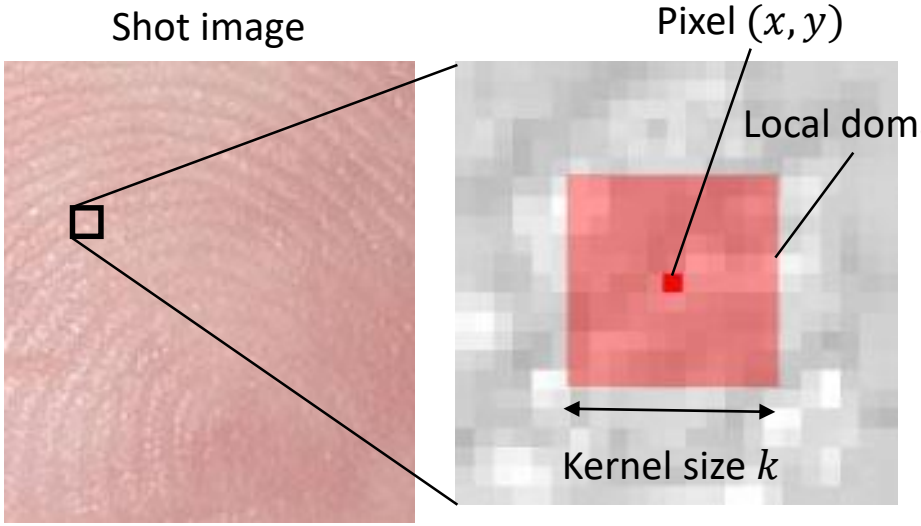


Contrasts between ridges and valleys are differ by location

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

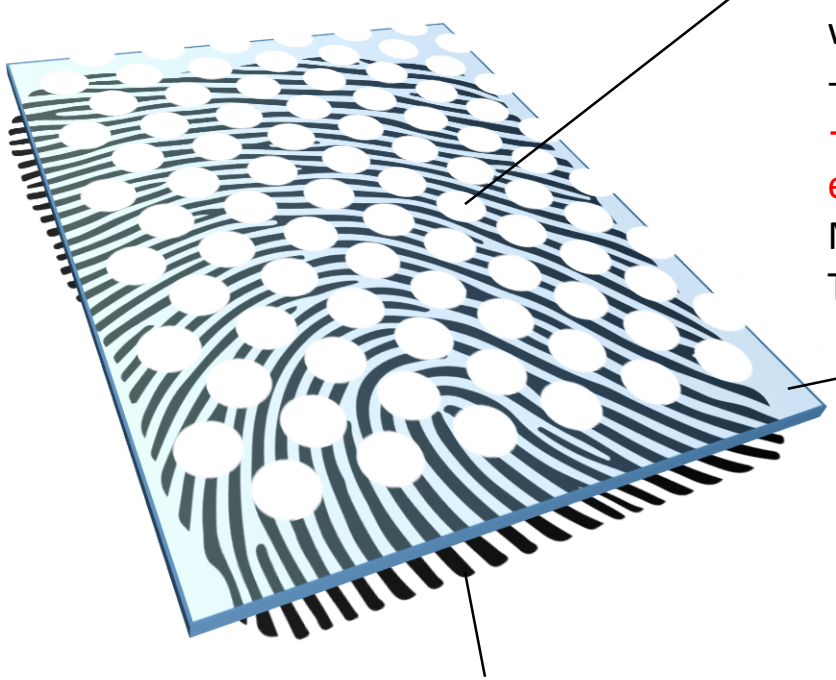
$$d(x, y) = \frac{1}{N} \sum_{x,y \subset D} I(x, y)$$

$k = 3$ $k = 11$ $k = 99$

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



Fingerprint

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

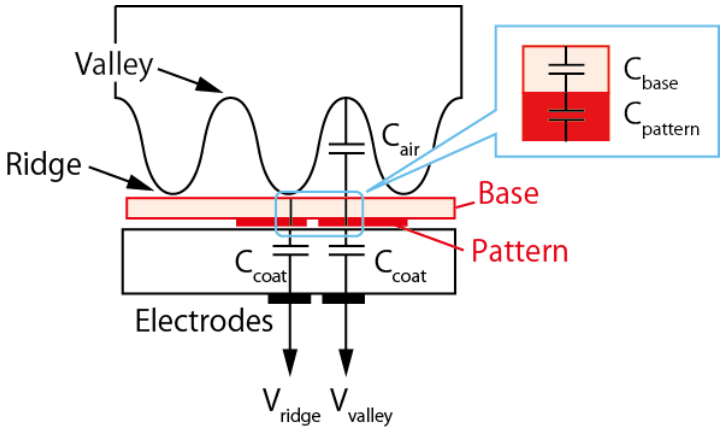
Base layer

- Light transmission property in visible wavelength
- Cohesive to all ridges on contact and makes no bubbles

→Capable of authentication by contact-based fingerprint sensors

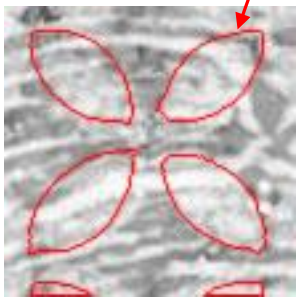
Material candidates: Rubbers, silicones or food additives

Transparency against capacitive fingerprint sensors



Acquired image

Outline

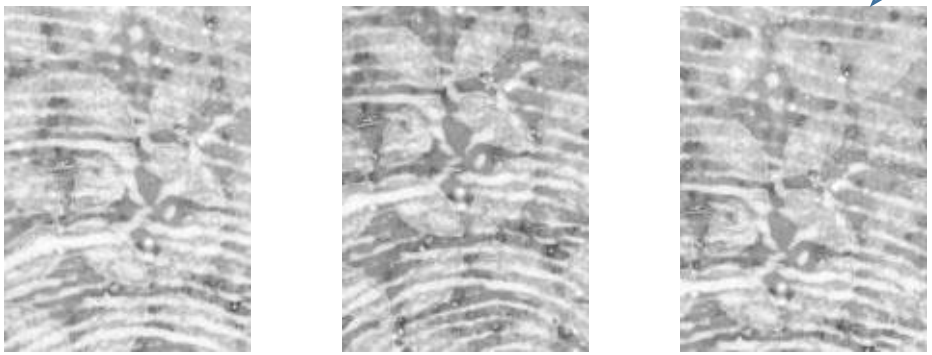


- Details of scanned image are affected by the distance between contact place and skin surface
- If base and pattern layer are thin enough, the electrostatic capacitance of both layers does not prevent the sensor from detecting fingerprint image (less than about 0.05 millimeters)

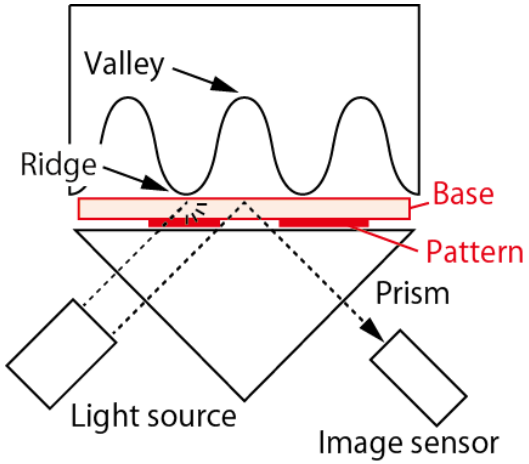
Influence of film thickness

Details are gradually lost

Thinner ⟷ Thicker



Transparency against optical fingerprint sensors



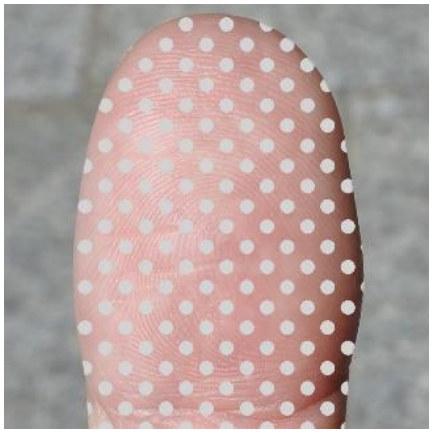
Acquired image

- 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

Thinner ⟷ Thicker

Consideration of disturbing effect



Sample pattern

Dot are darker than the skin

Both have the similar brightness

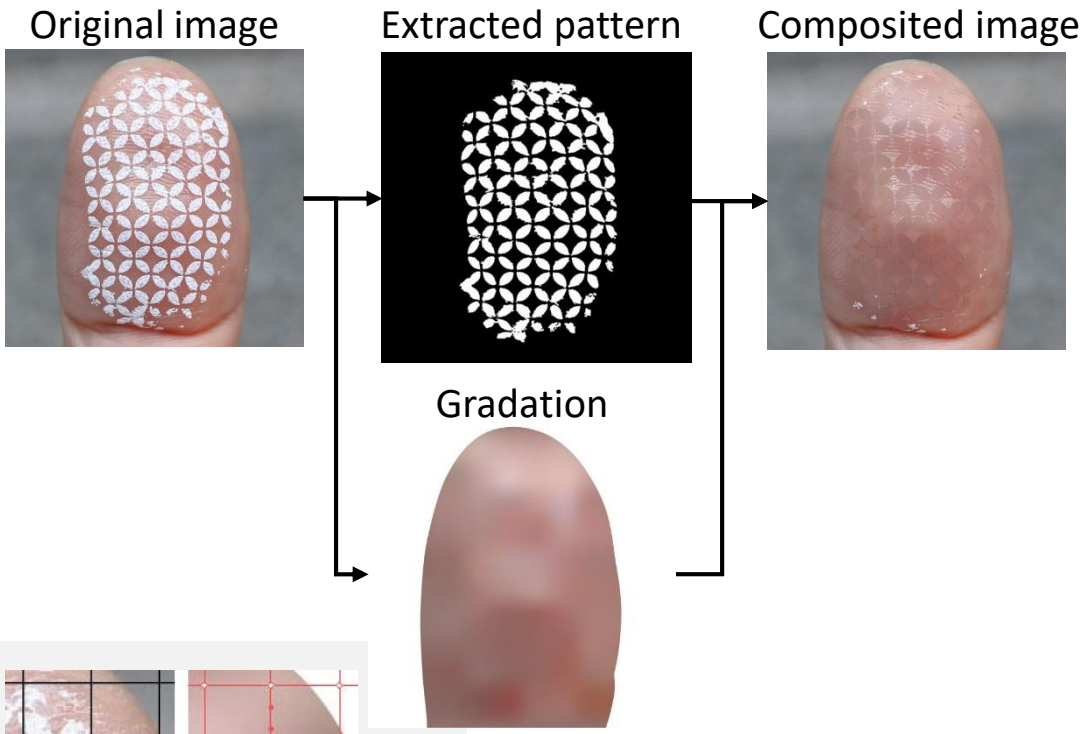
Dot are brighter than the skin

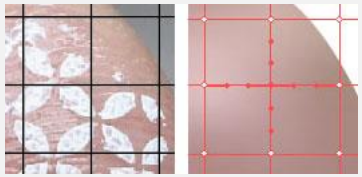
Less effective

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:

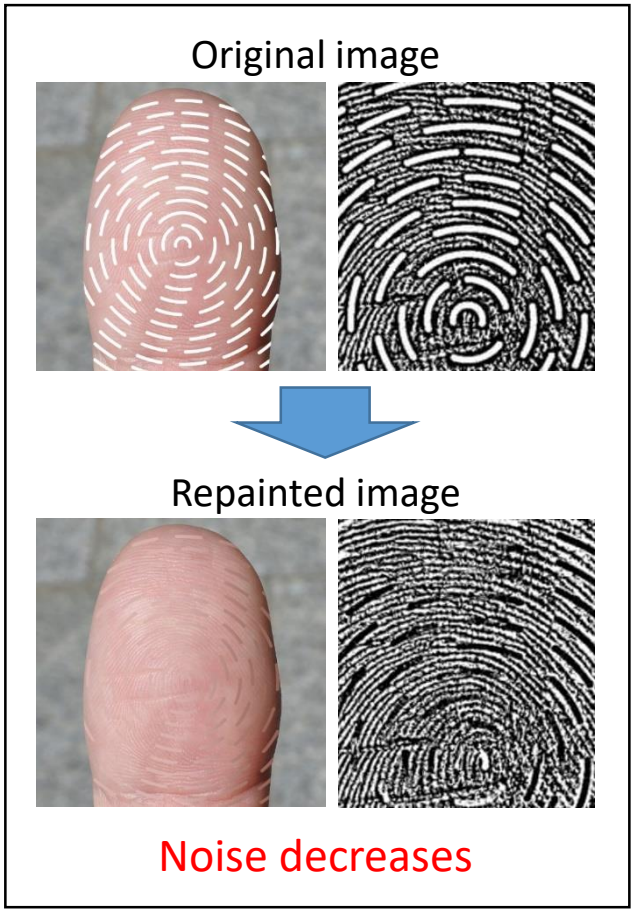
- Occurrence of fake feature points. Edges of the pattern are falsely recognized as ridges.
- Vanishing of original feature points. Ambiguous judgement of ridge ending and bifurcation excludes true positives.
- Type change of feature points. Judgement threshold changes by the existence of the pattern.

Noise invalidation attack by repainting the jamming pattern

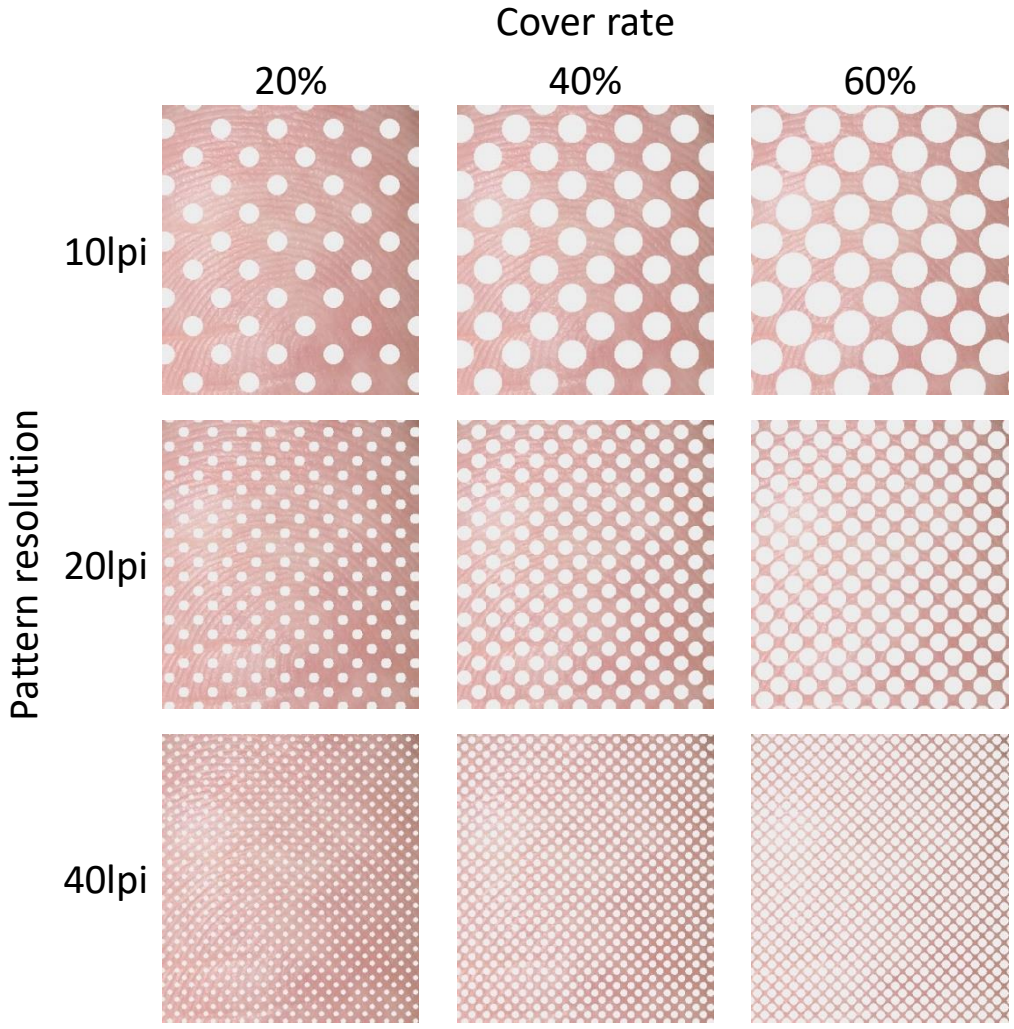




Interpolate pixels on the jamming pattern by sampling surrounding pixels



Designing resistant patterns against noise invalidation attack



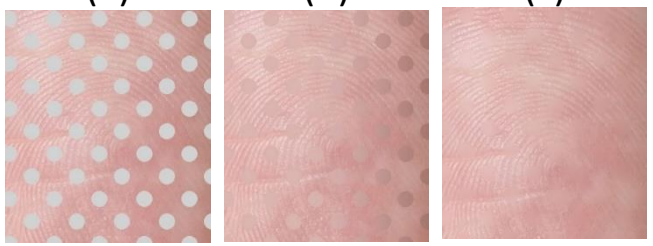
Recognize fingerprint images on which dots of the variable size are overlapped

Color types

(a) Light gray
(b) Average color of the finger
(c) Average color of surrounding pixels of the dot

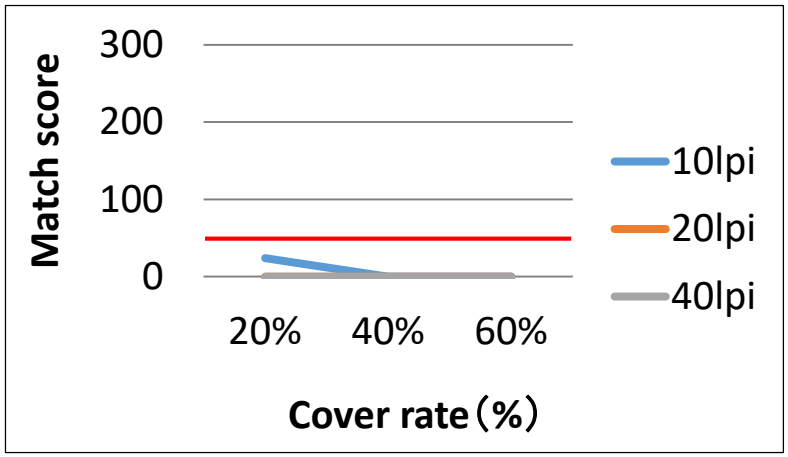
(b)(c) are supposed as repainted images of noise invalidation attack

(a) (b) (c)

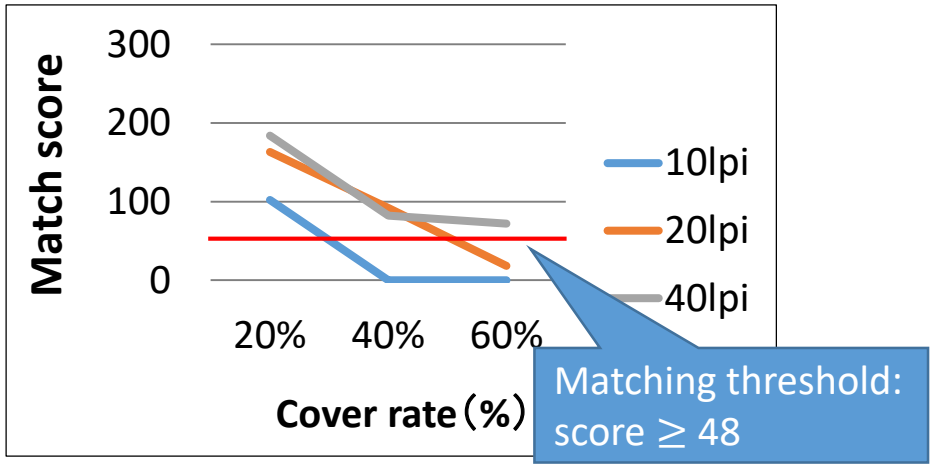


LPI: lines per inch

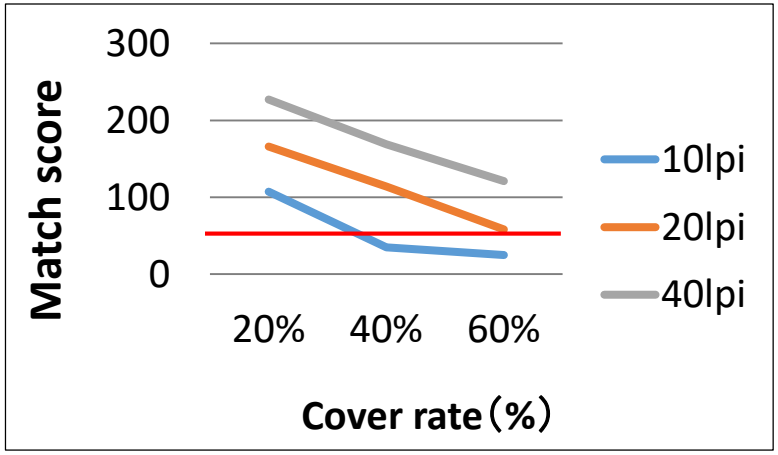
Matching result of pattern design



(a) Light gray



(b) Average color of the finger



(c) Average color of surrounding pixels of the dot

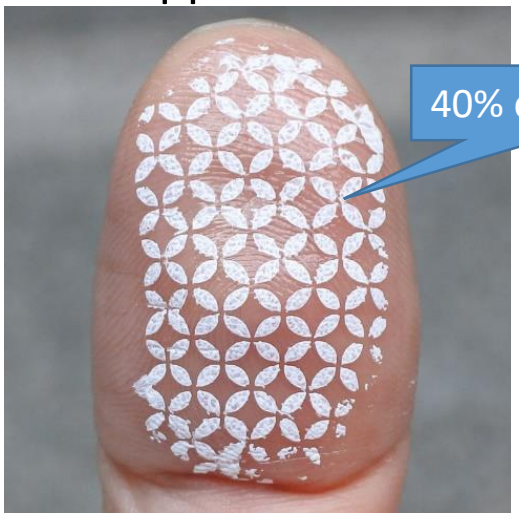
- Higher cover rate is more effective
- Lower pattern resolution is more effective for same cover rate

Required high cover rate and low pattern resolution (large pattern size)

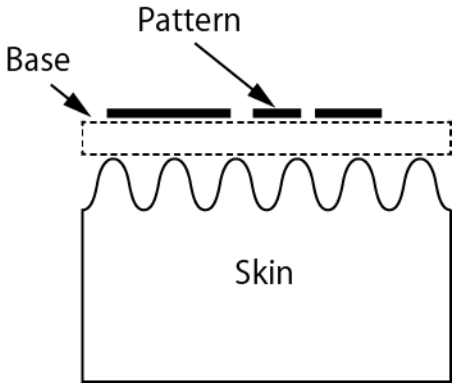
4. Evaluation

Making prototype for evaluation

Appearance



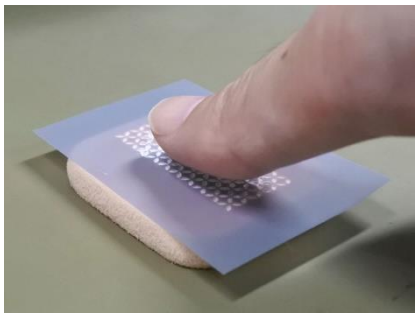
Diagram



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

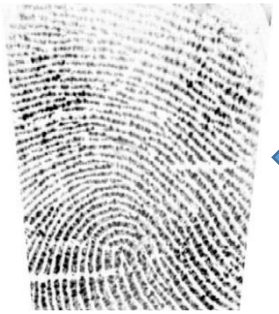
Input

Input types

Not attached

Attached

Attached and pattern repainted



Matching

After adaptive binarization

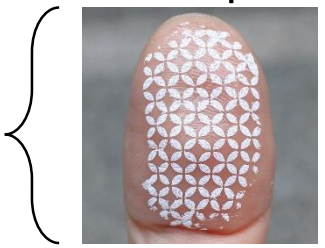
Can fingers attached BiometricJammer disturb fingerprint authentication from shot images?

Matching against fingerprint sensors

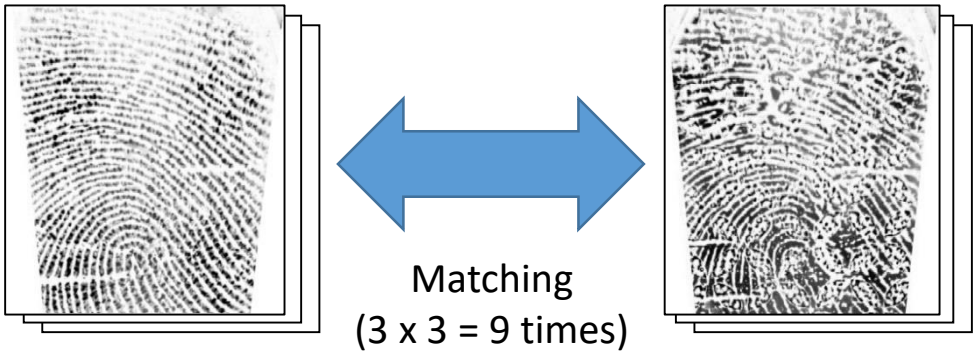
Registration

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

Attachment

- Base material: acrylic emulsion
- Pattern material: acrylic paint including zinc oxide
- Cover rate: 40%

Digital camera

- 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

Shooting environment

- 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

Fingerprint matching program

Neurotechnology VeriFinger[11] (commercial software)

Fingerprint sensors

DigitalPersona EikonTouch 710 (capacitive sensing)

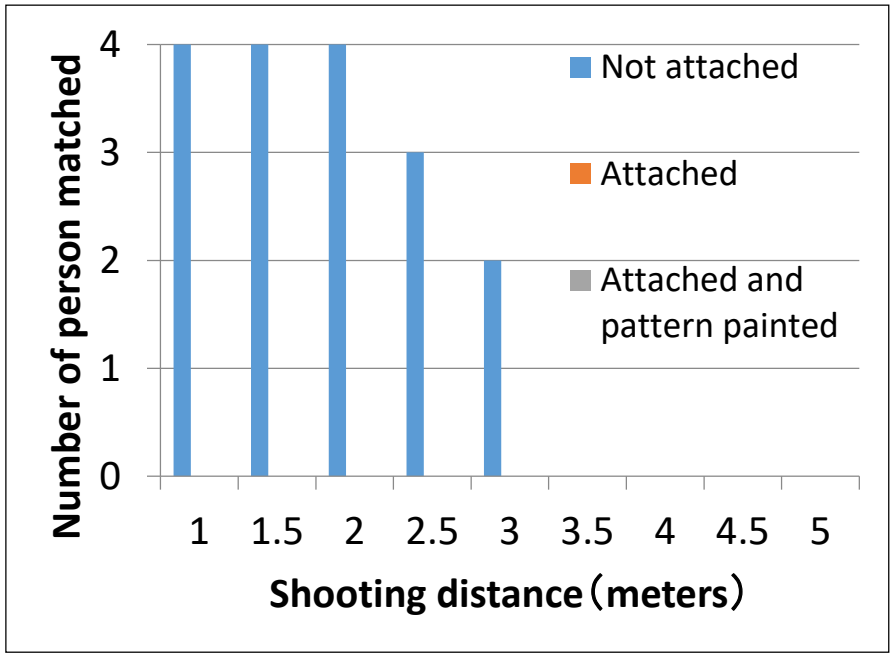
DigitalPersona U.are.U 4500 (optical sensing)

[11] Neurotechnology, VeriFinger SDK
http://www.neurotechnology.com/verifinger.html

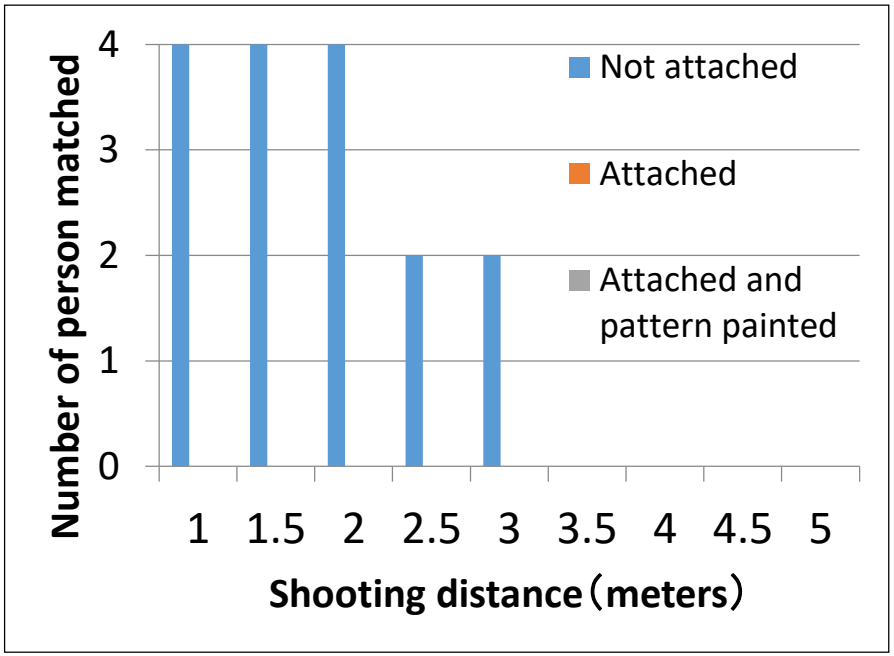
Matching result against shot images

Number of persons matched per shooting distance

Using a capacitive sensor



Using an optical sensor

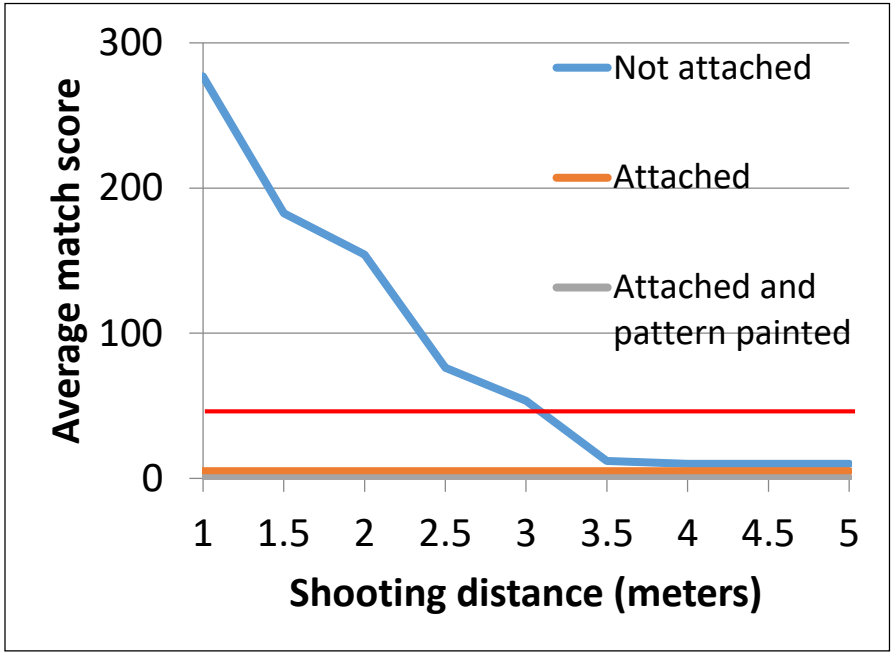


- Succeeded to authenticate fingers from shot images at the distance of 3 meters or less using commercial digital camera
- Succeeded to disturb fingerprint authentication of fingers attached BiometricJammer at any distance, even the jamming patterns are repainted

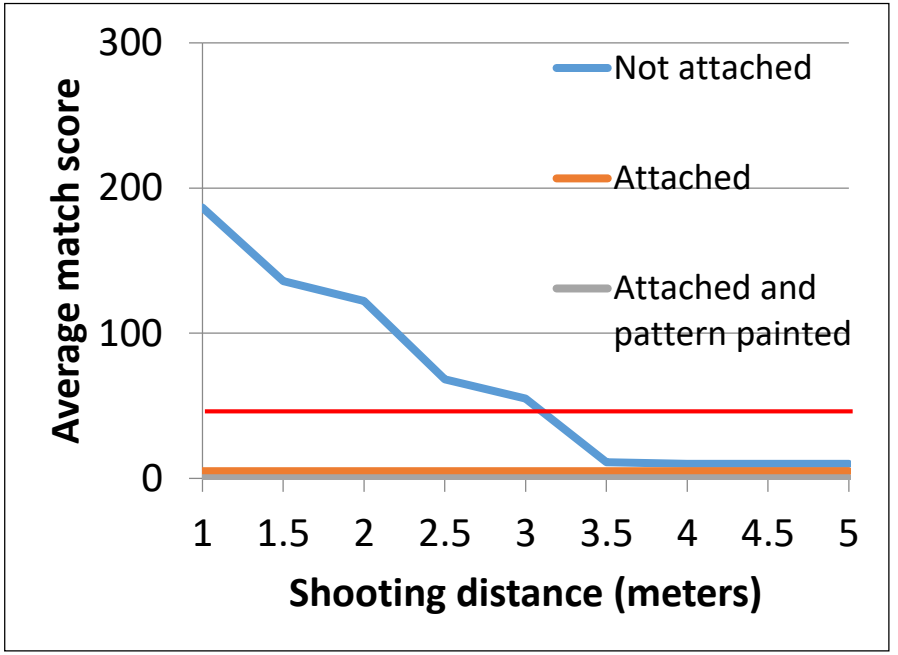
Matching result against shot images

Average match score per shooting distance

Using a capacitive sensor



Using an optical 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

Tester	Number of success	Minimum score	Maximum score
A	9	262	441
B	8	44	211
C	9	163	276
D	9	59	158

Using an optical sensor

Tester	Number of success	Minimum score	Maximum score
A	9	196	333
B	3	19	80
C	9	263	370
D	9	179	375

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