INVITED PAPER *Special Section on Enriched Multimedia — Potential and Possibility of Multimedia Contents for the Future —*

BiometricJammer: Method to Prevent Acquisition of Biometric Information by Surreptitious Photography on Fingerprints

Isao ECHIZEN[†a)], ***Fellow and*** **Tateo OGANE**[†], ***Nonmember***

SUMMARY Advances in fingerprint authentication technology have led to it being used in a growing range of personal devices such as PCs and smartphones. However, they have also made it possible to capture fingerprints remotely with a digital camera, putting the target person at risk of illegal log-ins and identity theft. This article shows how fingerprint captured in this manner can be authenticated and how people can protect their fingerprints against surreptitious photography. First we show that photographed fingerprints have enough information to spoof fingerprint authentication systems by demonstrating with "fake fingers" made from such photographs. Then we present a method that defeats the use of surreptitious photography without preventing the use of legitimate fingerprint authentication devices. Finally, we demonstrate that an implementation of the proposed method called "BiometricJammer," a wearable device put on a fingertip, can effectively prevent the illegal acquisition of fingerprints by surreptitious photography while still enabling contact-based fingerprint sensors to respond normally.

key words: *biometrics, fingerprint authentication, anti-spoofing, fake fingers, surreptitious photography*

1. Introduction

Biometric authentication is becoming increasingly common and is now installed as a standard feature on many personal devices such as PCs and smartphones. The spread of fingerprint authentication has been particularly remarkable—the proportion of smartphones that feature fingerprint sensors is expected to reach 67% during 2018 [1]. In addition, the resolution of image sensors has increased to the point where they can capture biometric information. It is now feared that fingerprint information which is conventionally obtained by contact-based fingerprint sensors could be obtained remotely by taking a surreptitious photograph. In 2014, a German hacker showed that he had successfully obtained a politician's fingerprint by taking photographs from a distance with an off-the-shelf digital camera [2]. The same hacker also demonstrated that a "fake finger" created using such a photograph can be used to unlock a smartphone [3]. In short, we now face another threat: the use of a photograph of someone's fingerprints for illegal logins and identity theft.

Although wearing gloves is an effective way to prevent fingerprints from being photographed, doing so is inconvenient for users who need to operate legitimate fingerprint authentication devices. We have thus developed a method for preventing surreptitious photography of fingerprints that prevents the improper acquisition of fingerprint information without seriously inconveniencing the user. We implemented this method in a prototype device called "BiometricJammer" and used it to demonstrate that our proposed method performs effectively.

Section 2 describes related work, Sect. 3 describes how the fingerprint authentication systems can be spoofed using fingerprints replicated from photographs, and Sect. 4 discuss methods for preventing fingerprint information from being obtained from photographs. Finally, in Sect. 5, we describe the implementation of our prototype and evaluation.

2. Related Works

An open issue in the field of automated biometric is "liveness security"—that is, is the biometric property being used to access the system from a real living person? In the case of fingerprints, although attacks using dead or altered fingers has been reported [4], [5], most vulnerability studies have focused on spoofing using fake fingers, i.e., two- or three-dimensional replicas of residual fingerprints. In the early 2000s, Putte and Keuning [6] and Matsumoto et al. [7] reported that a number of commercial fingerprint sensors could be spoofed with a three-dimensional mold made of cheap materials such as silicone rubber or gelatin. More recently Cao and Jain [8] succeeded in unlocking modern smartphones by using printed fingerprints created using an off-the-shelf inkjet printer and special conductive ink. Nowadays there are many tutorials on the web on how to make such replicas using common materials.

Traditional countermeasures against fingerprint spoofing use "liveness detection," which detects specific biological properties in addition to fingerprint images. These methods are either hardware- or software-based.

Hardware-based methods detect biomedical properties that are difficult to reproduce using materials commonly used for creating fake fingerprints. For example, Reddy et al. [9] proposed a method based on pulse oximetry which detects peripheral oxygen saturation (SpO_2) using probes of different wavelength. Baldisserra et al. [10] uses a chemical sensor that detects a skin odor different from those of fake finger materials. The method of Martinsen et al. [11] measures bioelectrical impedance using an array of electrodes, that of Rowe et al. [12] uses multispectral imaging under different illuminations, orientations and polarization conditions, and that of Cheng and Larin [13] uses optical coher-

Manuscript received June 1, 2017.
Manuscript revised August 25, 2017.
Manuscript publicized October 16, 2017.

[†] The authors are with National Institute of Informatics, Tokyo, 101–8430 Japan.
a) E-mail: iechizen@nii.ac.jp

DOI: 10.1587/transinf.2017MUI0001

ence tomography which can obtain in-depth imaging of human tissue including epidermis and dermis. One drawback of these methods is that an extra device is required, and such a device is difficult to attach to existing systems.

Software-based methods detect evidence of liveness using captured fingerprint images themselves. These methods require more than one image or an image of higher resolution to verify a fingerprint. For example, Derakhshani et al. [14] proposed a method that used the difference between perspiration patterns obtained from a pair of fingerprint images captured at an interval. The method of Chen et al. [15] measures skin elasticity when a finger is pressed on a sensor surface, that of Marcialis et al. [16] analyzes distribution of pores, and that of Moon et al. [17] distinguishes textures between a live finger and a fake fingerprints using wavelet analysis.

Multi-modal biometric systems had been considered more secure than systems using a single biometric property. However, Rodrigues et al. [18] showed that such systems are even less secure if one of the biometric traits can be spoofed. Subsequently, Johnson et al. [19], Akhtar et al. [20], Marasco et al. [21] proposed fusion methods more robust against spoofing attempts.

Outside the fingerprint community, several recent study have focused on privacy protection. Harvey [22] created fashion camouflage art that prevents detection by computer vision, Feng and Prabhakaran [23] created an automated application program that facilitates the camouflage design, and Yamada et al. [24] suggested simple eyewear that prevents automatic face detection without inhibiting face-to-face communication. We aim to apply similar ideas to fingerprint security and privacy by developing a method that prevents fingerprints from being stolen without harming the effectiveness of relevant security systems.

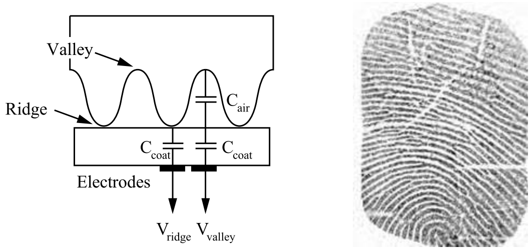
3. Principles of Fingerprint Authentication

3.1 Obtaining Fingerprint Data

In this section we explain the principles of fingerprint sensors that are currently in widespread use.

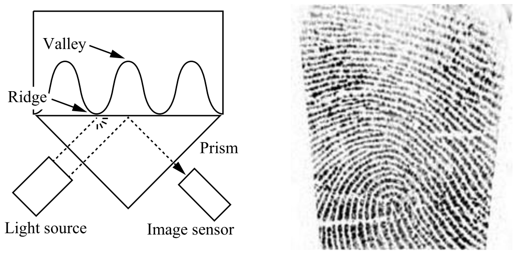
Figure 1 illustrates the principle of capacitive fingerprint sensor [25]–[27]. It has a two-dimensional array of electrodes embedded in a chip. When a finger is placed on the chip, a small electrical charge is created between the surface of the finger and each electrode. Since the amount of the charge vary according to the distance between the skin and the corresponding electrode, ridges and valleys in the fingerprint result in different capacitances. The sensor maps each voltage applied to a micro-capacitor to the intensity of a pixel.

The sensor is coated with dielectric material such as passivation oxide or polymer compound to protect the silicon chip against physical impacts and chemical substances. Since sensing accuracy decreases with an increase in the coating thickness, the coating is typically less than 20 μm thick [28], [29].



(a) Schematic diagram (b) Captured image

Fig. 1 Principle of capacitive fingerprint sensor.



(a) Schematic diagram (b) Captured image

Fig. 2 Principle of optical fingerprint sensor.

Figure 2 illustrates the principle of optical fingerprint sensor [30], [31]. A prism is used to measure the differences in reflection conditions. The light entering the prism is reflected at the valleys of the fingerprint due to making use of frustrated total internal reflection (FTIR). In contrast, the light is randomly scattered at the ridges since the refraction index changes due to the contact of the finger skin. The sensor maps the reflected light to the pixel intensities.

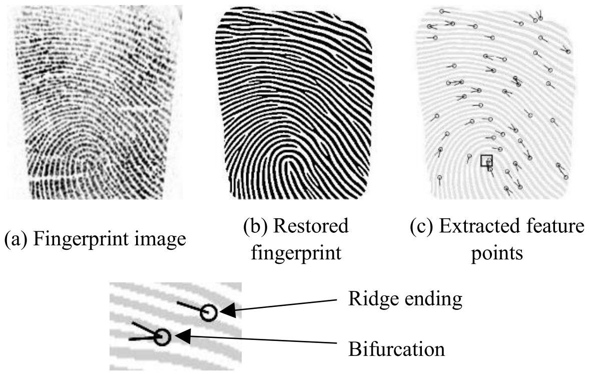
An FTIR-based sensor introduces trapezoidal distortion in captured image since the optical path length varies with the contact point [32]. The sensor is sensitive to the presence of air bubbles, even only a few μm of air bubbles can make the pixels brighter [33].

3.2 Extracting and Matching Feature Points

Minutiae matching is most commonly used to recognize fingerprints from obtained fingerprint images [34]. This method involves detecting and matching of feature points (minutiae) instead of focusing ridges and valleys directly. Ridge endings and bifurcations are used in particular among a number of feature types.

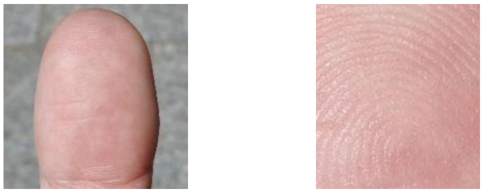
Figure 3 shows a fingerprint image for each step of minutiae detection. A captured image consists of two-dimensional array of intensities while a minutiae detector considers a fingerprint to be a bunch of connected lines in which ridge endings and bifurcations are to be detected. Several technologies have made fingerprint detection more effective, including image binarization [35], [36], image enhancement [37], [38], crease removal [39], [40].

The extracted feature points are represented as a set of triplets p = {x, y, t}, where x and y represent the feature coordinates, and t represents the feature orientation. These



(a) Fingerprint image (b) Restored fingerprint (c) Extracted feature points

Fig. 3 Minutiae detection.



(a) Whole fingerprint (b) Close-up

Fig. 4 Example of fingerprint photographs.

feature points are saved in a list which is called a fingerprint template. A fingerprint matcher compares the feature point list obtained from the input image with the one obtained from an image registered in advance to identify a fingerprint. Fingerprint matching can thus be regarded as a pattern matching problem between sets of points.

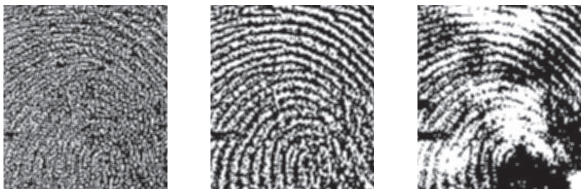
3.3 Obtaining Fingerprints from Fingerprint Photographs

Figure 4 (a) shows an example of a fingerprint image taken with a digital camera, and Fig. 4 (b) shows a close-up of the same image. Digital cameras differ from contact-based fingerprint sensors in that they sample the shades produced by the ridges and valleys of the fingerprint instead of the physical structure of the fingerprint. As a result, these images tend to be noisy and lacking in contrast. However, this problem can be overcome by using noise removal techniques such as spatial filtering.

One type of spatial filtering is called adaptive binarization [41], [42]. For a pixel at (x, y), the threshold value $d(x,y)$ is expressed as the average intensity over a local region D of pixel intensities $I(x,y)$:

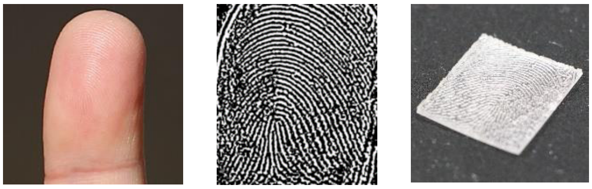
$$d(x,y) = \frac{1}{\mathrm{N}} \sum_{x,y \subset \mathrm{D}} I(x,y) \tag{1}$$

In the context of digital image processing, D is assumed to be a square region of convolution kernel. Let k the kernel size that is the length of one side of D. Figure 5 shows the results of performing adaptive binarization on an image shown in Fig. 4 (b) in various kernel sizes. The actual spacing between ridges is ~10 pixels in this example, thus the results show that the fingerprint can be effectively restored when k is close to the spacing.



(a) k=3 (b) k=11 (c) k=99

Fig. 5 Results of adaptive binarization.



(a) Photograph (b) Binarized image (c) Fake finger

Fig. 6 Fingerprint replication.

3.4 Replicating Fingerprints from Fingerprint Photographs

We demonstrated how attackers can replicate fingerprints from photographs taken from a distance by actually making fake fingers using off-the-shelf stamp-making machine. Figure 6 shows images at each step of fingerprint replication. We took several images using two digital single-lens reflex (DSLR) cameras and a smartphone at various distances and cut out fingertip areas of the images. Next we scaled the images to the resolution of fingerprint sensors (~500 pixels per inch) and adaptively binarized them with kernel size k = 11 pixels. Then we printed the scaled images on a transparent plastic sheet and used the stamp-making machine as a stamp template. The machine irradiated ultraviolet light through the transparent regions of the template, solidifying the photosensitive emulsion coated on a rubber sheet of stamp material. Finally, we washed out the emulsion that had not been irradiated. The resulting sheet had ridges and valleys similar to the binarized image.

We verified that the fake fingers described above can spoof fingerprint authentication system. We acquired images of real fingerprints and the fake fingers using a fingerprint sensor. Then we matched both images using commercial fingerprint matching program Neurotechnology VeriFinger [43]. It calculates matched scores based on the similarity between feature points extracted from both images. The score is close to zero for different fingerprints and reaches hundreds for the same fingerprints (upper limit is not regulated). The minimum score at which a matching is considered as a true match is called matching threshold. It is linked to the false acceptance rate (FAR) as shown in the following formula:

$$\text{Threshold} = -12 \log_{10} \text{FAR} \tag{2}$$

Table 1 Matching scores of replicated fingerprints.

Camera (distance in m)	Binarized image	Fake finger captured with a capacitive sensor	Fake finger captured with an optical sensor
DSLR camera (5.4)	97	96	51
DSLR camera (1.6)	179	163	109
Smartphone (0.3)	94	116	78

For example, a matched score of 48 or more is regarded as true match for the FAR of 0.01%, 96 or more is as well for the FAR of 0.000001%.

Table 1 shows the results. According to the definition above, all samples in the table could deceive fingerprint authentication system for the FAR of 0.01%. In addition, if the binarized image could spoof a fingerprint recognition system, the replicated fingerprint could also spoof the system since the ridge endings and bifurcations were preserved although the image quality may have been degraded through the physical process of replication.

In our test, the scores for the capacitive sensor were close to those for the source image and much better than those for the optical sensor. However, it does not mean that capacitive sensors are easier to deceive since the quality of captured image depends on the material and the method of replication.

4. Proposed Method

4.1 Research Policies and Approach

We decided the method to be devised for the problem of surreptitious photography of fingerprints must meet three requirements.

- The method must enable the user's fingerprints to be authenticated using contact-based fingerprint sensors.
- The method must make it impossible to authenticate a fingerprint derived from a photograph.
- The method must be user-centric, i.e., no need for enforcement in sensors or by authentication systems

Our approach to achieving these requirements is to use a "wearable jamming pattern" that users can put on and take off in accordance with the situation.

4.2 Overview of Proposed Method

As shown in Fig. 7, the wearable jamming pattern consists of a base layer that is transparent to visible light and a pattern layer that scatters light in the visible region. The base layer sticks securely to the user's fingertip so that the pattern layer is superimposed over the fingerprint and interferes with fingerprint recognition. The material used for each layer must be safe to the human body. Candidate materials are silicone and medical wound dressings for the base layer and zinc oxide and titanium dioxide for the pattern layer.

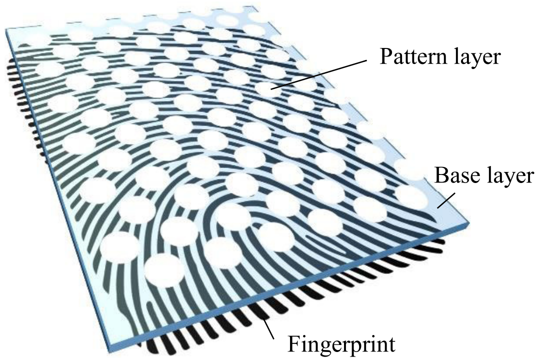
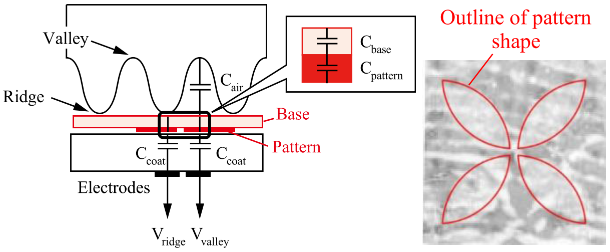


Fig. 7 Overview of proposed method.



(a) Schematic diagram (b) Captured image

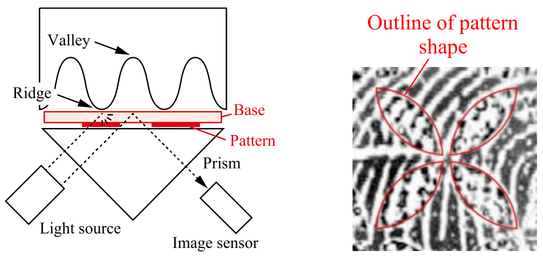
Fig. 8 Effect of jamming pattern on capacitive fingerprint sensor.

Coverage rate and line density have a significant influence on the jamming effect. As we describe in Sect. 4.5, patterns with a coverage rate of 40% or more and a line density of 10 LPI or less are suggested in case of uniform dot patterns. Shape is less important and arbitrary shapes with above conditions are expected to have similar effects.

4.3 Transparent to Fingerprint Sensors

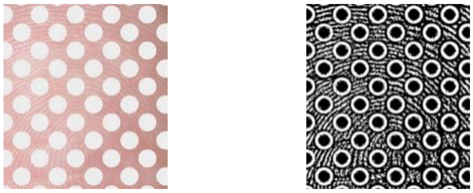
A user wearing the proposed jamming pattern should still achieve authentication using contact-based fingerprint sensors. Figure 8 shows the effect of the jamming pattern on capacitive fingerprint sensor. If the base layer and pattern layer are both made of dielectric material, their effect can be regarded as an increase in the thickness of the coating material on the contact plane. The quality of the captured image is affected by the distance between the finger and an electrode. Compared with Fig. 1 (b), the contrast and sharpness are lower in Fig. 8 (b). However, a minutiae detector can extract feature points from the image since ridges and valleys can still be distinguished. We confirmed that both layers of less than 50 μm thick did not prevent minutiae detection.

Figure 9 shows the effect of the jamming pattern on optical fingerprint sensor. As described above, ridges and valleys are distinguished by the total internal reflection condition on the prism surface. When a finger with the jamming pattern contacts the prism, the sensor light reflects or scatters at the boundary of the base material and the air since the reflectance of the material is closer to that of the glass than to that of the air.



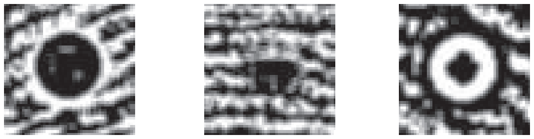
(a) Schematic diagram (b) Captured image

Fig. 9 Effect of jamming pattern on optical fingerprint sensor.



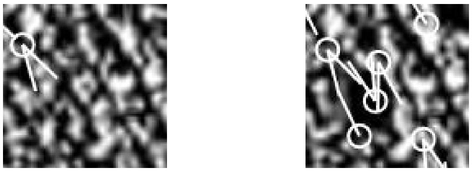
(a) Photograph (b) Binarized image

Fig. 10 Example of jamming pattern.



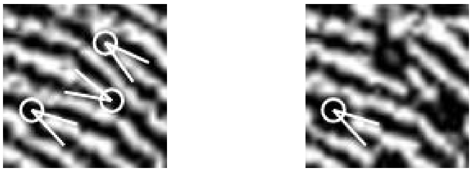
(a) Dot is darker than skin (b) Roughly equal brightness (c) Dot is brighter than skin

Fig. 11 Example effect of jamming pattern.



(a) Without jamming pattern (b) With jamming pattern

Fig. 12 Generation of spurious feature points.



(a) Without jamming pattern (b) With jamming pattern

Fig. 13 Loss of original feature points.

Despite this light-scattering property of the pattern layer, light is not blocked by the pattern shapes since the layer is thin enough for the sensor light. There are broken ridges, especially within the pattern shape, since air bubbles were mixed when we painted the pattern material. We can overcome this problem by using production methods that suppress the formation of bubbles.

Minutiae detector is able to repair defects in obtained images, e.g. broken ridges in Fig. 9 (b). In contrast, feature points are still preserved despite of the repair. As described in Sect. 5.4, we observed no decline in success rate for the scanned images with jamming pattern.

4.4 Effects of Jamming Pattern

The proposed method causes fingerprint recognition from photographs to fail by adding jamming pattern. As discussed above, for a fingerprint from a photograph to be recognized, the fingerprint has to be emphasized by performing spatial filtering with a suitable kernel size. When this is done, the jamming pattern superimposed on the fingerprint is also emphasized, and this disrupts the fingerprint recognition process. Figure 10 shows an example of jamming pattern with a uniform dot shape, and Figure 11 shows an example of the jamming effects caused by this pattern. The dots produce the smallest amount of the effects when there are of the same level of brightness as the skin. The greater the difference in brightness between the dots and the skin, the greater the effects.

The jamming pattern causes the following types of interference.

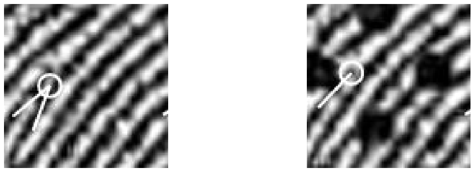
- Generation of spurious feature points: the minutiae detector detects ridges in an input image comprising a set of pixels and uses them to reconstruct a set of lines. During this process, partial defects and extra branches not present in the original ridges are removed, but the superimposed dots result in the jamming factors being incorrectly recognized as ridges, which results in the creation of false endings and bifurcations (Fig. 12).

- Loss of original feature points: the superimposition of dots close to a feature points leads to ambiguity in the judgment of endings and bifurcations although judgement was previously performed correctly, so these feature points are excluded from the detection results. Moreover, when the connection relationships between ridges become overly complicated, the resulting structure may be regarded as unreliable, and the detected set of feature points may be discarded in its entirety (Fig. 13).

- Misclassification of feature points: due to the high sensitivity noise in the input image, the classification of feature points into endings and bifurcations tends to vary somewhat. When dots are superimposed on the input image, the threshold value for this classification varies and can result in the feature points being classified into different types (Fig. 14).

4.5 Investigation of Pattern Types

As mentioned above, effects of the jamming pattern are



(a) Without jamming pattern (b) With jamming pattern

Fig. 14 Misclassification of feature points.

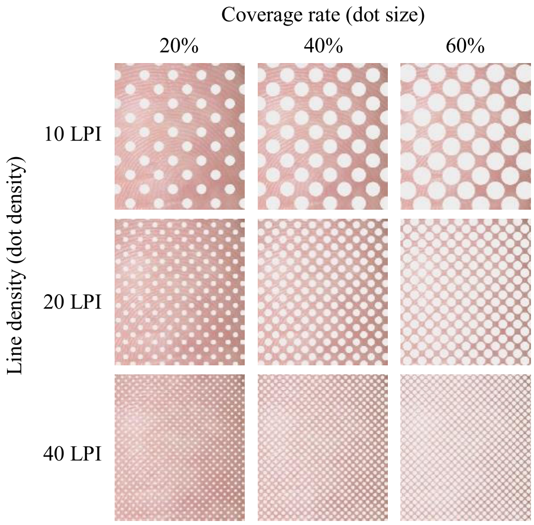
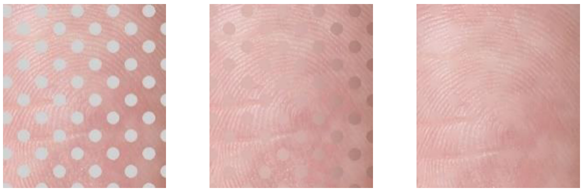


Fig. 15 Sample patterns.

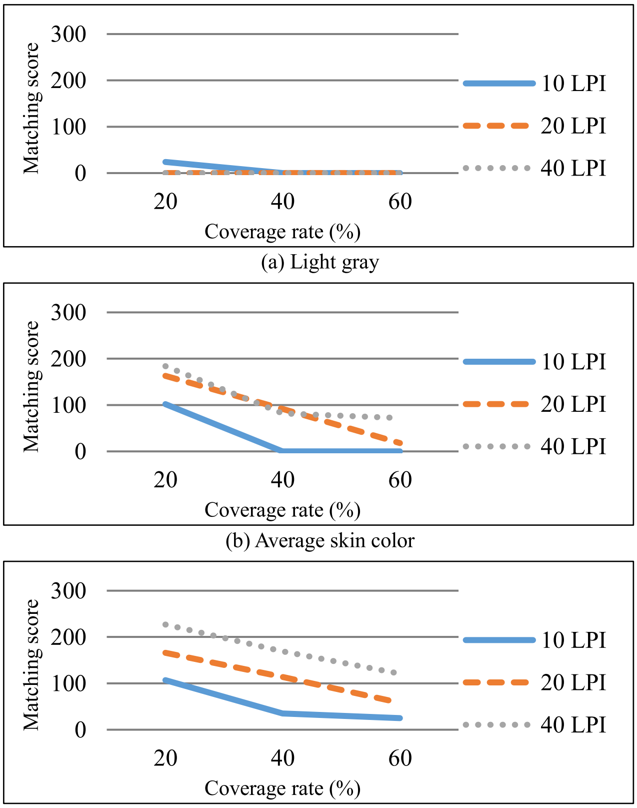


(a) Light gray (b) Average skin color (c) Skin color around each dot

Fig. 16 Fill methods.

weakest when the pattern has roughly the same brightness as the skin. Attackers might attempt to exploit this characteristic by filling in the pattern regions with skin color to cancel out the effects. To examine the extent to which patterns can withstand this type of attack, we performed a fingerprint recognition simulation using sample patterns of varying size. We prepared samples with coverage rates of 20%, 40%, and 60% and with line densities of 10 LPI, 20 LPI, and 40 LPI for each coverage rate (Fig. 15). Using each of the nine sample patterns produced in this way, we processed the same fingerprint image by applying three different fill methods in which the dot pattern was filled in with (a) light gray, (b) the average skin color, and (c) the skin color around the periphery of each dot, and we used these as input images for fingerprint recognition (Fig. 16).

Figure 17 shows the matching results. We used VeriFinger to match images and regarded score of 48 or above as a successful match for FAR of 0.01%. Cases in which a feature point could not be detected were given a matching score of zero. With a light gray fill color, none of the patterns were matched (i.e., the interference was successful). However, with the other two fill methods, the matching scores were much higher. For the same line density, the matching score decreased as the coverage rate increased, and for the same coverage rate, the matching scores decreased with the line density. These results show that a pattern with a coverage rate of 40% or more and a line density of 10 LPI or less is resilient against pattern canceling attacks based on color filling.



(a) Light gray

(b) Average skin color

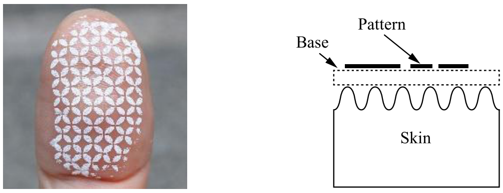
(c) Skin color around the periphery of each dot

Fig. 17 Sample pattern matching results.

5. Evaluation

5.1 Evaluation Prototype

Taking into account the results of our investigation described above, we implemented the proposed method in a product called “BiometricJammer” that can be applied to the user’s fingertips. We painted acrylic resin for the base layer using a paintbrush and transcribed acrylic paint for the pattern layer using a nail art template which has geometric pattern instead of uniform dot pattern described so far. Resulting pattern had 40% coverage rate and 13 LPI line density. The appearance and structure of this device are shown in Fig. 18.

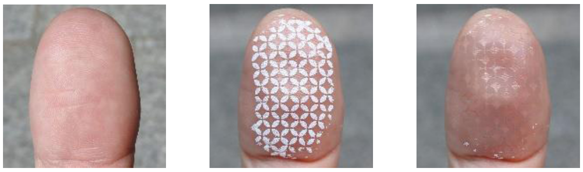


(a) Appearance (b) Structure

Fig. 18 Prototype device used for evaluation.

Table 2 Evaluation environment.

Implementation	BiometricJammer (acrylic resin for base and acrylic paint for patterns, coverage rate 40%)
Fingerprint sensors	(a) DigitalPersona EikonTouch 710 (capacitive sensing, scan size 13×18 mm, resolution 508 ppi) (b) DigitalPersona U.are.U 4500 (optical sensing, scan size 15×18 mm, resolution 512 ppi)
Digital camera	Canon EOS 70D (20.2 megapixel, automatic ISO speed, automatic exposure, 1-point autofocus)
Lens	Canon EF-S 18–135 mm F3.5–5.6 IS STM (focal length fixed at 135 mm)
Shooting distance	1–5 m (in 0.5-m increments)
Lighting conditions	Outdoors, cloudy/sunny (subject illumination: 7,800–31,600 lux)



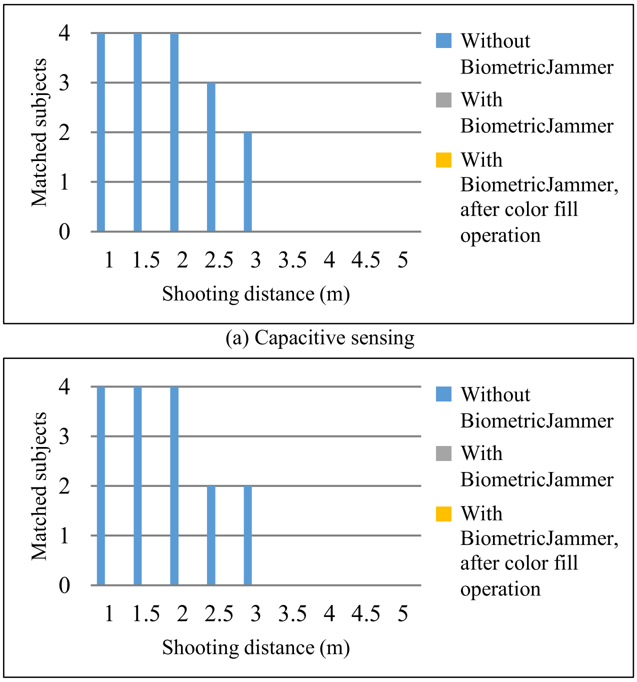
(a) Without BiometricJammer (b) With BiometricJammer (c) With BiometricJammer, after color fill operation

Fig. 19 Input images.

5.2 Matching from Photographs

We used our BiometricJammer prototype device and four subjects to evaluate the effectiveness of our proposed method. The evaluation environment is summarized in Table 2. The evaluation procedure was as follows.

- Step 1: use a fingerprint sensor to scan and record the test subject's fingerprint (thumb on right hand) before attaching the prototype.
- Step 2: take a picture of the same finger with a digital camera; match this photograph against the image recorded in step 1 (Fig. 19 (a)).
- Step 3: attach the prototype to the same finger and take a photograph of it; match this photograph against the image recorded in step 1 (Fig. 19 (b)).
- Step 4: fill in the pattern parts of the photographic image obtained in step 3 using the average color of the surrounding pixels; match the resulting image against the image recorded in step 2 (Fig. 19 (c)).



(a) Capacitive sensing

(b) Optical sensing

Fig. 20 Matched subjects using VeriFinger.

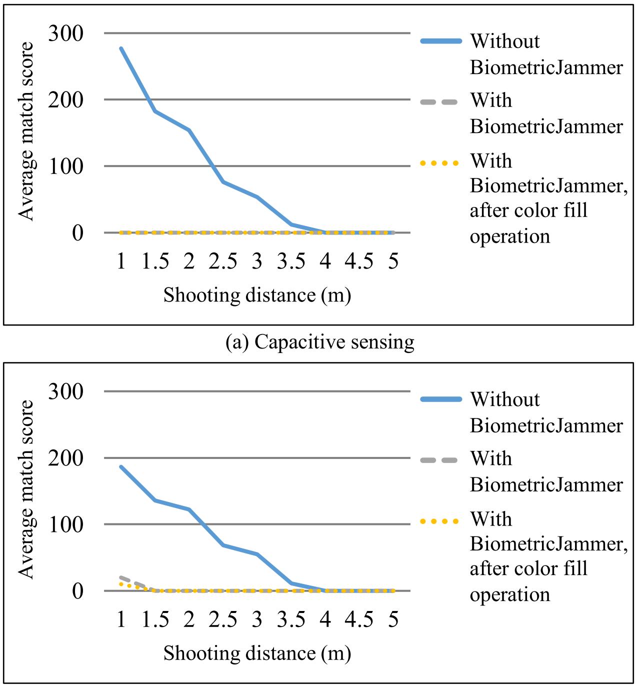
The photographs used in steps 2, 3, and 4 were scaled to the same size as the recorded image in step 1 (~500 ppi) by using image processing software. They were then adaptively binarized with a kernel size k = 11 pixels. We used two fingerprint matching software packages to perform matching: Neurotechnology VeriFinger and NIST Biometric Image Software (NBIS) [44].

5.3 Matching Results from Photographs

Figures 20 and 21 show the matching results from photographs using VeriFinger. The former shows how the number of matches varied with the shooting distance and the latter shows the average match scores of the subjects. Figures 20 (a) and 21 (a) are results using a capacitive sensor and Figs. 20 (b) and 21 (b) are results using an optical sensor. We again regarded the score of 48 or above as a successful match for the FAR of 0.01%. We also regarded the score to zero if no feature point was detected due to the low image quality.

In case of "without BiometricJammer", all the test subjects were matched when the shooting was from a distance of 2 m or less, and some of them could be matched at a distance of up to 3 m. This indicates that attackers can take fingerprint images with sufficient quality to spoof fingerprint authentication without being noticed by the target. However, fingerprint cannot be obtained from all photographs in which fingers appear since most photographs does not focus on the fingertips, and the fingerprints may even be blurred due movement by the target.

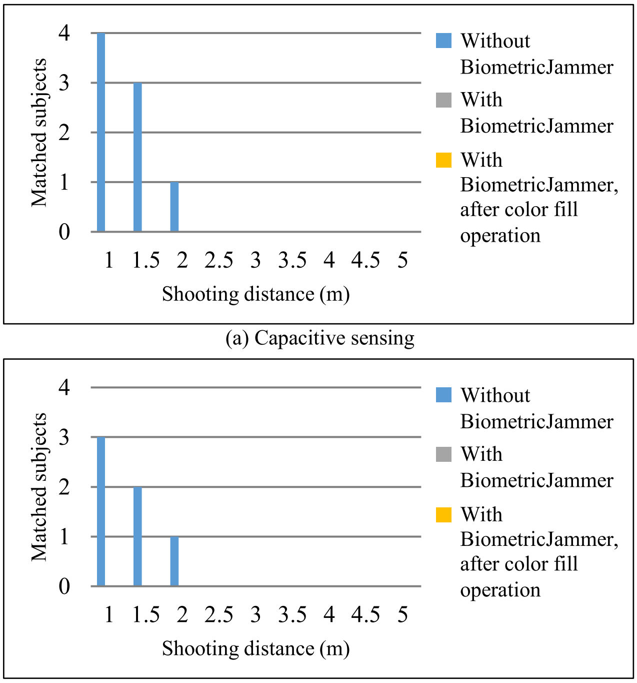
In contrast, in cases of "with BiometricJammer" and



(a) Capacitive sensing

(b) Optical sensing

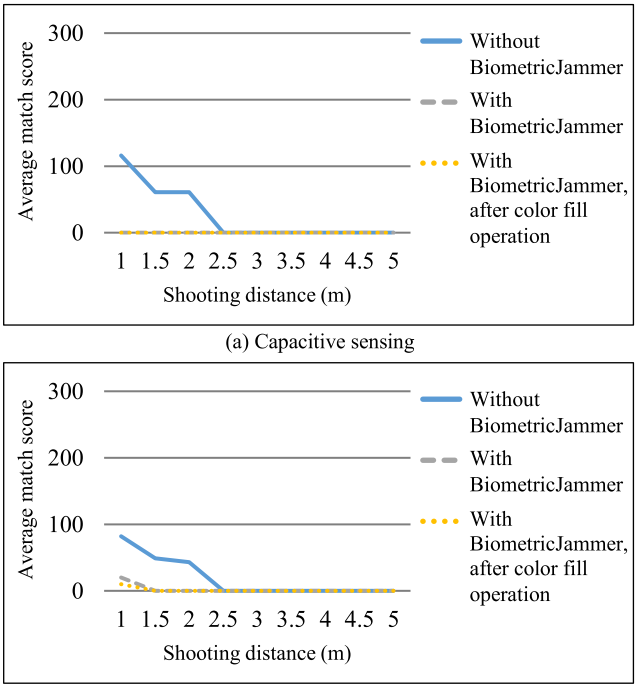
Fig. 21 Average match scores using VeriFinger.



(a) Capacitive sensing

(b) Optical sensing

Fig. 22 Matched subjects using NBIS.



(a) Capacitive sensing

(b) Optical sensing

Fig. 23 Average matching scores using NBIS.

“with BiometricJammer, after color fill operation”, number of matched subjects was zero at any distance since match scores were either zero or less than 48. These results are consistent with those in Sect. 4.5 in which a pattern with a coverage of 40% or more and a line density of 10 LPI or less can effectively prevent fingerprint recognition and even defeat color filling methods.

About the difference between the sensing methods used for fingerprint registration, although the optical sensor had lower scores for the registered fingerprints, the matching results were comparable to those for the capacitive sensor. We think that is because feature points were well extracted at registration though image quality may have differed between the methods.

Figures 22 and 23 show the matching results from photographs using NIST Biometric Image Software (NBIS). The former shows how the number of matches varied with the shooting distance and the latter shows the average matching scores of the subjects. Figures 22 (a) and 23 (a) are results using a capacitive sensor and Figs. 22 (b) and 23 (b) are results using an optical sensor. We used the MINDTCT feature detector to detect minutiae from image, and the BOZORTH3 fingerprint matcher to match the minutiae between the registered and input images. Both are included in the NBIS toolkit. Though the false acceptance rate was not clear, we followed the general guideline; i.e., a match score more than 40 was regarded as a successful match [45]. We also regarded the score to zero if no feature point was detected due to the low image quality.

The results are similar to those for VeriFinger. In case of “without BiometricJammer”, subjects were matched at 2 m or less. In cases of “with BiometricJammer” and “with BiometricJammer, after color fill operation”, number of matched subjects was zero at any distance. In former case, matched subjects were less than for VeriFinger since matching accuracy was more sensitive to image ro-

Table 3 Matching results with fingerprint sensors for VeriFinger.

(a) Capacitive sensing

Test subject	Successful matches	Min. score	Max. score
A	9	262	441
B	8	44	211
C	9	163	276
D	9	59	158

(b) Optical sensing

Test subject	Successful matches	Min. score	Max. score
A	9	196	333
B	3	19	80
C	9	263	370
D	9	179	375

Table 4 Matching results with fingerprint sensors for NBIS.

(a) Capacitive sensing

Test subject	Successful matches	Min. score	Max. score
A	9	52	111
B	2	14	42
C	7	38	80
D	0	0	30

(b) Optical sensing

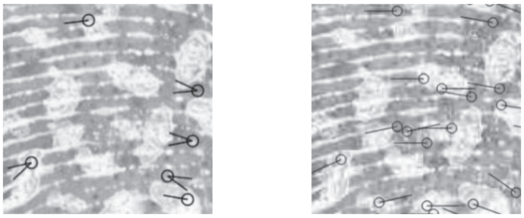
Test subject	Successful matches	Min. score	Max. score
A	8	39	76
B	0	9	23
C	9	41	94
D	2	22	48

tation and scaling. Better matching could be obtained by more precisely aligning the input images with the registered ones. About the difference between the sensing methods used for fingerprint registration, optical sensing resulted in less matched subjects and lower match scores than capacitive sensing, similar to the trend in the case of VeriFinger.

5.4 Matching with Fingerprint Sensor

Next, we investigated whether legitimate fingerprint authentication with a fingerprint sensor could be achieved when wearing the prototype BiometricJammer. For each type of fingerprint sensor, we obtained three registration images and three authentication images, and performed matching a total of nine times, recording the total number of successes and the maximum and minimum matching scores. We again used VeriFinger and NBIS for the matching.

Table 3 shows the results for VeriFinger. Three of the four test subjects achieved successful matching in every trial. The large variation in matching scores was due to the lack of consistency in the placement of the subjects' fingers on the fingerprint sensor since each sensor had no means to guide finger placement. The number of successes was particularly low for subject B since the captured regions of the registered images were biased to the left while those of the input images were biased to the right. As a result, there was little common area between the images. The results shows that there is no decline in success rate when the jamming pattern is attached if the matching program is accurate enough.



(a) VeriFinger (b) NBIS

Fig. 24 Difference in detected minutiae for subject D (capacitive sensing).

Table 4 shows the results for NBIS. Subjects A and C again scored well while subjects B and D had worse scores than for VeriFinger. As mentioned above, image rotation affected the accuracy of the matching program. The most remarkable finding was that none of the images matched for subject D for capacitive sensing while all of them matched under the same condition for VeriFinger.

Figure 24 shows the difference in detected minutiae for subject D between programs. VeriFinger well repaired the ridge gaps caused by the printed pattern of BiometricJammer, whereas NBIS detected many spurious feature points. This is attributed to the paint being too thick due to the lack of adjustment function for the pattern material.

6. Conclusion

Advances in biometric technology have made our everyday lives more secure and more convenient through the use of biological information for personal identification and authentication. However, the risks associated with the theft and exploitation of this biological information are also increasing. We focused on the problem of fingerprint theft by means of surreptitious photography and developed a method called BiometricJammer that prevents the illegal acquisition of fingerprints without inconveniencing the user. Evaluation testing using a prototype implementation demonstrated that it is possible to extract fingerprints from photographs and that the proposed technique provides an effective countermeasure to this problem.

We think proposed method is not a goal. As we derived an effective pattern experimentally, it remains a task for the future work to explain theoretically how the jamming pattern lowers match score effectively.

Other forms of biological information besides fingerprints that could be used for personal identification and authentication include the patterns of the iris and of the veins in the fingers or palms. We plan to continue researching methods aimed at preventing the illegal acquisition of each type of information.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Numbers JP16H06302, JP15H01686, and JP16K12431.

References

[1] Credit Suisse, “Global smartphone fingerprint penetration to reach 67% by 2018E,” China Smartphones Sector, p.32, https://doc.research-and-analytics.csfb.com/docView?sourceid=em&document_id=x675378&serialid=Y1p6aGBM4ca8YeQ5seIP CDUoDvUzjVc5p4c4dlQKcwU%3d (referenced 2017-04-19).

[2] Chaos Computer Club, “Fingerprint biometrics hacked again,” https://www.ccc.de/en/updates/2014/ursel (referenced 2017-04-19).

[3] Chaos Computer Club, “Chaos Computer Club breaks Apple TouchID,” https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid (referenced 2017-04-19).

[4] P. Sengottuvelan and A. Wahi, “Analysis of Living and Dead Finger Impression Identification for Biometric Applications,” Proc. International Conference on Computational Intelligence and Multimedia Applications, pp.466–470, 2007.

[5] S. Yoon, J. Feng, and A.K. Jain, “Altered Fingerprints: Analysis and Detection,” IEEE Trans. Pattern Anal. Mach. Intell., vol.34, no.3, pp.451–464, 2012.

[6] T. van der Putte and J. Keuning, “Biometrical Fingerprint Recognition: Don’t Get Your Fingers Burned,” Proc. Working Conf. on Smart Card Research and Advanced Applications (4th), Proc. IFIP TC8/WG8.8, pp.289–303, 2000.

[7] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, and R.L. van Renesse, “Impact of Artificial “Gummy” Fingers on Fingerprint Systems,” Proc. SPIE, vol.4677, pp.275–289, 2002.

[8] K. Cao and A.K. Jain, “Hacking Mobile Phones Using 2D Printed Fingerprints,” MSU Technical Report, MSU-CSE-16-2, 2016.

[9] P.V. Reddy, A. Kumar, S.M.K. Rahman, and T.S. Mundra, “A New Antispoofing Approach for Biometric Devices,” IEEE Trans. Biomed. Circuits Syst., vol.2, no.4, pp.328–337, 2008.

[10] D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, “Fake Fingerprint Detection by Odor Analysis,” Proc. International Conference on Biometrics, LNCS 3832, pp.265–272, 2006.

[11] Ø.G. Martinsen, S. Clausen, J.B. Nysæther and S. Grimnes, “Utilizing Characteristic Electrical Properties of the Epidermal Skin Layers to Detect Fake Fingers in Biometric Fingerprint Systems – A Pilot Study,” IEEE Trans. Biomed. Eng., vol.54, no.5, pp.891–894, 2007.

[12] R.K. Rowe, K.A. Nixon, and P.W. Butler, “Multispectral Fingerprint Image Acquisition,” Advances in Biometrics, pp.3–23, 2008.

[13] Y. Cheng and K.V. Larin, “In Vivo Two- and Three-Dimensional Imaging of Artificial and Real Fingerprints With Optical Coherence Tomography,” IEEE Photon. Technol. Lett., vol.19, no.20, pp.1634–1636, 2007.

[14] R. Derakhshani, S.A.C. Schuckers, L.A. Hornak, and L. O’Gorman, “Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners,” Pattern. Recogn., vol.36, no.2, pp.383–396, 2003.

[15] Y. Chen, S. Dass, and A.K. Jain, “Fingerprint Deformation for Spoof Detection,” Proc. Biometrics Symposium, 2005.

[16] G.L. Marcials, F. Roli, and A. Tidu, “Analysis of Fingerprint Pores for Vitality Detection,” Proc. International Conference on Pattern Recognition, pp.1289–1292, 2010.

[17] Y.S. Moon, J.S. Chen, K.C. Chan, K. So, and K.C. Woo, “Wavelet based fingerprint liveness detection,” Electron. Lett., vol.41, no.20, pp.1112–1113, 2005.

[18] R.N. Rodrigues, L.L. Ling, and V. Govindaraju, “Robustness of multimodal biometric fusion methods against spoof attacks,” Journal of Visual Languages & Computing, vol.20, no.3, pp.169–179, 2009.

[19] P.A. Johnson, B. Tan, and S. Schuckers, “Multimodal Fusion Vulnerability to Non-Zero Effort (Spoof) Imposters,” International Workshop on Information Forensics and Security, pp.1–5, 2010.

[20] Z. Akhtar, G. Fumera, G.L. Marcialis, and F. Roli, “Robustness Analysis of Likelihood Ratio Score Fusion Rule for Multimodal Biometric Systems under Spoof Attacks,” Proc. IEEE International Carnahan Conference on Security Technology, pp.1–8, 2011.

[21] E. Marasco, Y. Ding, and A. Ross, “Combining Match Scores with Liveness Values in a Fingerprint Verification System,” Proc. International Conference on Biometrics: Theory Applications and Systems, pp.418–425, 2012.

[22] A. Harvey, “CV Dazzle: Camouflage from Computer Vision,” http://cvdazzle.com (referenced 2017-5-22).

[23] R. Feng and B. Prabhakaran, “Facilitating Fashion Camouflage Art,” Proc. 21st ACM international conference on Multimedia, pp.793–802, 2013.

[24] T. Yamada, S. Gohshi, and I. Echizen, “Privacy Visor: Method for Preventing Face Image Detection by Using Differences in Human and Device Sensitivity,” Proc. 14th IFIP International Conference on Communications and Multimedia Security, vol.8099, pp.152–161, 2013.

[25] C. Tsikos, “Capacitive Fingerprint Sensor,” US Patent 4353056, 1982.

[26] A.G. Knapp, “Fingerprint Sensing Device and Recognition System Having Predetermined Electrode Activation,” US Patent 5325442, 1994.

[27] M. Tartagni and R. Guerrieri, “A Fingerprint Sensor Based on the Feedback Capacitive Sensing Scheme,” IEEE J. Solid-State Circuits, vol.33, no.1, pp.133–142, 1998.

[28] M. Tartagni, B. Gupta, and A. Kramer, “Capacitive Distance Sensor,” US Patent 6114862, 2000.

[29] F.P. Lane, G. Gozzini, and H.M. Siegel, “Capacitive Fingerprint Sensor With Protective Coating Containing a Conducive Suspension,” US Patent 6693441, 2004.

[30] H.J. Caulfield and D.R. Perkins, “Fingerprint Identification Apparatus,” US Patent 3716301, 1973.

[31] L. Coetzee and E.C. Botha, “Fingerprint Recognition in Low Quality Images,” Pattern Recognition, vol.26, pp.1441–1460, 1993.

[32] S.M. Rao, “Method for producing correct fingerprints,” Appl. Opt., vol.47, no.1, pp.25–29, 2008.

[33] K. Sumi, “Fingerprint Authentication System, The Journal of the Institute of Image Information and Television Engineers, vol.58, no.6, pp.759–762, 2004. (in Japanese)

[34] A. Jain, L. Hong, and R. Bolle, “On-line Fingerprint Verification,” IEEE Trans. Pattern Anal. Machine Intell., vol.19, no.4, pp.302–313, 1997.

[35] N.K. Ratha, S. Chen, and A.K. Jain, “Adaptive Flow Orientation-based Feature Extraction in Fingerprint Images,” Pattern Recognition, vol.28, no.11, pp.1657–1672, 1995.

[36] D. Maio and D. Maltoni, “Direct Gray-scale Minutiae Detection in Fingerprints,” IEEE Trans. Pattern Anal. Machine Intell., vol.19, no.1, pp.27–40, 1997.

[37] L. O’Gorman and J.V. Nickerson, “An Approach to Fingerprint Filter Design,” Pattern Recognition, vol.22, no.1, pp.29–38, 1989.

[38] L. Hong, Y. Wan, and A. Jain, “Fingerprint Image Enhancement: Algorithm and Performance Evaluation,” IEEE Trans. Pattern Anal. Machine Intell., vol.20, no.8, pp.777–789, 1998.

[39] D.S.G. Vernon, “Automatic detection of secondary creases in fingerprints,” Opt. Eng., vol.32, no.10, pp.2616–2623, 1993.

[40] C. Wu, J. Zhou, Z.-Q. Bian, and G. Rong, “Robust Crease Detection in Fingerprint Images,” Proc. Conf. Computer Vision and Pattern Recognition, vol.II, pp.505–510, 2003.

[41] J. Sauvola and M. Pietikäinen, “Adaptive document image binarization,” Pattern Recognition, vol.33, no.2, pp.225–236, 2000.

[42] P.D. Wellner, “Adaptive Thresholding for the DigitalDesk,” EuroPARC Report EPC-93-110, 1993.

[43] Neurotechnology, “VeriFinger SDK,” http://www.neurotechnology.com/verifinger.html. (referenced 2017-04-20).

[44] National Institute of Standards and Technology, “NIST Biometric Image Software (NBIS),” https://www.nist.gov/services-resources/software/nist-biometric-image-software-nbis (referenced 2017-04-27).

[45] National Institute of Standards and Technology, “User’s Guide to Export Controlled Distribution of NIST Biometric Image Software

(NBIS-EC),” http://www.nist.gov/customcf/get_pdf.cfm?pub_id=51096, (referenced 2017-04-20).

Isao Echizen received B.S., M.S., and D.E. degrees from the Tokyo Institute of Technology, Japan, in 1995, 1997, and 2003, respectively. He joined Hitachi, Ltd. in 1997, and until 2007 was a research engineer in the company’s systems development laboratory. He is currently a professor and a director of the Information and Society Research Division, the National Institute of Informatics (NII), an advisor to the director general of the NII, and a professor in the Department of Informatics, the School of Multidisciplinary Sciences, The Graduate University For Advanced Studies (SOKENDAI). He is also a visiting professor at the Tsuda University and was a visiting professor at the University of Freiburg in 2010 and at the University of Halle-Wittenberg in 2011. He has been engaged in research on information security and content security and privacy. He received the Best Paper Award from the IPSJ in 2005 and 2014, the Fujio Frontier Award and the Image Electronics Technology Award in 2010, the One of the Best Papers Award from the Information Security and Privacy Conference and the IPSJ Nagao Special Researcher Award in 2011, the Docomo Mobile Science Award in 2014, and the Information Security Cultural Award in 2016. He is a member of the Information Forensics and Security Technical Committee and the IEEE Signal Processing Society.

Tateo Ogane joined the National Institute of Informatics in 2011 and is currently a senior technical specialist at NII. He has been engaged in the development, implementation, and evaluation of technologies to prevent unauthorized copying of cinema screens and displays, ones for preventing face recognition from camera images (implemented as a “PrivacyVisor”), and ones for preventing fingerprint extraction from camera images (implemented as a “BiometricJammer”). His current research interest is the development of image/video processing software.