A Micro Biometric Authentication Mechanism Considering Minute Patterns of the Human Body

A proposal and the first attempt

Masahiro Fujita*, Yuto Mano†, Takuya Kaneko†, Kenta Takahashi‡, and Masakatsu Nishigaki*
* Graduate School of Science and Technology, Shizuoka University, Hamamatsu Japan
nisigaki@inf.shizuoka.ac.jp
† Graduate School of Informatics, Shizuoka University Hamamatsu Japan
‡RD Group, Security Research Dept., Hitachi, Ltd. Totsuka Japan

***Abstract*—We propose a new biometric authentication mechanism called "micro biometric authentication". This mechanism uses minute patterns of human body parts as biometric information. Minimization of the biometric information used for the authentication enables the mechanism to satisfy the following three requirements needed for biometric authentication systems: (i) higher tolerance against a masquerade attack, (ii) consideration of the issue of traceability, and (iii) higher authentication accuracy. As a first attempt, we developed a micro biometric authentication system that uses minute patterns of human skin texture. Experimental results showed that the system can achieve an EER of about 0.5% and that the mechanism satisfies all three requirements.**

Keywords— Biometric authentication; Privacy preservation; Re-registration; Minute patterns; Skin texture

I. INTRODUCTION

Biometric authentication is attractive because there is no need to remember secret information and no possibility of secret information being stolen or lost. Recently, the Fast Identify Online Alliance (FIDO) [1] developed an online authentication platform using biometrics, and Hitachi Ltd. promotes the widespread use of biometrics as a Public Biometrics Infrastructure (PBI), where biometric information can be used like the cryptographic key in the conventional Public Key Infrastructure (PKI) [2]. These movements have prompted companies and organizations to place considerable focus on biometric authentication. When we disseminate the progress of biometric authentication, however, there is one big problem in that biometric information is basically unchangeable. This leads to two issues: vulnerability to a masquerade attack and potential breach of privacy.

A masquerade attack is when an attacker steals and forges the biometric information of a legitimate user. The attacker can then log into the legitimate user's account by using the forged information. In fact, attackers have already been successful with this type of attack (e.g., [3][4]). Today, telephotographic lenses allow attackers to steal iris information from afar and remain undetected. Attackers can set up phishing Web sites to steal vein information. Masquerade attacks are a critical concern for biometric authentication since the biometric information is essentially vulnerable for life once it leaks out. We need a biometric authentication mechanism that has a higher tolerance against forgery (requirement 1).

The privacy issue is caused by the fact that biometric authentication is traceable. Suppose that, for example, a user uses the same biometric information on several Web accounts. If an attacker obtains this biometric information, he/she will quickly learn that these accounts are used by the same person. We need a biometric authentication mechanism that is capable of hindering traceability (requirement 2).

One technique used to tackle the above issues is biometric template protection, such as cancelable biometrics [8]. In this scheme, a user registers $F_R(X)$ as his/her template instead of X, where F is a transform function, X is the user's biometric information, and R is the user's random number. By using this scheme, the user can generate his/her new template by changing R. However, even if we use this scheme, X (biometric information) remains unchangeable. This unfortunately means that this scheme is not an effective countermeasure against masquerade attacks and the traceability concern.

Another technique is one-time biometric authentication, such as text independent speaker authentication or text prompt speaker authentication. However, the accuracy of these types of behavioral biometric authentication tends to be lower than that of physiological biometric authentication [5]. We need a biometric authentication mechanism that can achieve a higher authentication accuracy (requirement 3).

In this work, we try to achieve a biometric authentication mechanism that satisfies requirements 1–3. Our approach is to minimize the physiological biometric information used for authentication. We call our proposal "micro biometric authentication". A tiny section of the body is expected to be more difficult to forge (requirement 1). A user can use different minute parts one after another whenever the user wants to re-register the biometric information (requirement 2). Micro biometric authentication is based on physiological biometrics, so a reasonable level of authentication accuracy is expected (requirement 3). As the first attempt of micro biometric authentication, in this paper we apply a minute pattern of human skin texture to biometric authentication.

2157-0426/16 $31.00 © 2016 IEEE
DOI 10.1109/NBiS.2016.13

In Section II of this paper, we describe related works. Section III introduces our proposal and we implement a prototype system in Section IV. In Section V, we perform experiments, and Section VI discusses whether our proposal satisfies requirements 1–3. We conclude in Section VII with a brief summary and mention of future work.

II. Related Works

To the best of our knowledge, there is no research that has applied minute patterns of users' body parts to biometric authentication. For this reason, we introduce a few works related to "micro technology" and "one-time authentication".

A. Micro Printing

In general, the smaller something is, the more difficult it is for attackers to forge it. Micro printing is a forging prevention technology that takes advantage of using small things. The most common example we can give here is the technique used in printing money [6]: paper bills use micro characters, so it is not possible for printers with low resolution to perfectly copy them. This technology is an effective countermeasure against forging.

B. Artifact Metrics

Artifact metrics is an information security technology that uses the intrinsic characteristic of a physical object for authentication and clone resistance [7]. In general, we can manufacture the same objects by using the same manufacturing technology. However, in the microscopic world, each object has its own intrinsic characteristic pattern. For instance, each paper has its own intrinsic fiber pattern. By using the intrinsic pattern as a feature, we can identify individual objects. This pattern is subtle and random, making it very difficult to forge. One of the leading edge artifact metrics technologies is nano-artifact metrics [7], which is based on silicon nanostructures formed by an array of resist pillars that randomly collapse when exposed to electron-beam lithography.

C. Cancelable Biometrics

In cancelable biometrics [8], a user registers $F_R(X)$ as his/her template instead of X, where F is a transform function, X is the user's biometric information, and R is the user's random number. The procedures are as follows.

Registration phase:

1. The system reads a user's biometric information X.
2. The system generates a random number R for the user.
3. The system transforms X into $T=F_R(X)$.
4. T is registered as the user's template on the system.
5. R is stored in the user's smart card or on a trusted third party server.

Authentication phase:

1. The system reads the biometric authentication X' of a user who tries to log into the system as a legitimate user.
2. The system obtains the random number R of the user.
3. The system obtains the template T of the user.
4. The system transforms X' into $T'=F_R(X')$.
5. If T' is nearly equal to T, the system identifies the user as the legitimate user.

If the template is compromised or a user wants to change his/her template, the user can generate a new template by changing R.

D. Disposable authentication tokens put into user's body

Although they have not yet been put into practical use, an "authentication pill" and an "electric tattoo for authentication" have been proposed [9]. The strategy here is to put disposable authentication tokens into users' bodies so as not to get lost or stolen. The authenticity of tokens is checked with Radio Frequency Identification (RFID) technology.

This idea is very interesting, but it comes with a few problems. The authentication provided by these tokens is what-you-have authentication, which allows attackers to forge the tokens. For example, the electric tattoo used by legitimate users may be reused by attackers. Another problem is that, in the case of the authentication pill, users may have psychological resistance to swallowing the pill.

III. Micro Biometric Authentication

A. Concept

As discussed in Section I, we need a biometric authentication mechanism that satisfies requirements 1–3. From the viewpoint of authentication accuracy, the most plausible option is to use physiological biometric information. However, physiological biometric information is both traceable and forgeable. Our approach is to apply minute patterns of user's body parts into physiological biometric authentication. The mechanism, called "micro biometric authentication", satisfies requirements 1–3 as follows.

Requirement 1: In general, the smaller the patterns we use, the more difficult it becomes for attackers to manufacture a clone of the pattern. Moreover, it is much easier to take an image of a micro pattern with a microscopic lens. This means that micro biometric authentication can provide a higher tolerance against masquerade attack.

Requirement 2: A minute pattern is a tiny piece of biometric information, and thus we can extract a number of minute patterns from a user's body. Each minute pattern has a different feature. This means that a user can register/re-register new biometric information on the authentication system at any time. Whenever a user changes the registered biometric information, traceability is lost. Micro biometric authentication is thus capable of hindering traceability.

Requirement 3: The minute patterns of user's body parts used for authentication are physiological biometric information. In general, the accuracy of physiological biometric authentication is stable compared to that of behavioral biometric authentication. Therefore, micro biometric authentication can satisfy the requirement for higher authentication accuracy.

B. Applying Minute Pattern of Human Skin to Authentication

In this work, as a first attempt at micro biometric authentication, we apply a minute pattern of human skin texture to biometric authentication. We are able to observe the roughness of the skin surface clearly in the microscopic world.

This roughness mainly consists of sulcus cutis, crista cutis, and area cutanea. There are also various sweat glands and pores on human skin. Human skin texture is the pattern composed of these constituents. The size of this pattern is on the micrometer order, which presumably makes it difficult to manufacture a precise clone of the pattern.

C. Procedure of Micro Biometric Authenticadtion using Human Skin Texture

The micro biometric authentication works as follows (also, see Fig. 1). Here, we describe the following procedures as 1:1 authentication. Micro biometric authentication can also be applied to 1:N authentication.

Registration Phase:

1. A user registers his/her user ID into a system.
2. The system requests the user to draw a fiducial mark anywhere on the skin surface.
3. The user draws the mark anywhere on his/her skin surface.
4. The system reads the user's minute biometric information X using a microscope with the mark as a guide.
5. The system stores X as the user's template T in a database.

Authentication Phase:

1. A user inputs his/her user ID into the system.
2. The system reads the user's minute biometric information X' using a microscope with his/her fiducial mark as a guide.
3. The system retrieves the user's template T (=X) from the database.
4. If X' is nearly equal to T, the user is identified as a legitimate user.

IV. Implementation of Prototype System

We implement a prototype system of the micro biometric authentication. In this section, we describe the specifics of the implementation.

A. How to Find Registered Region on Human Skin Surface

The micro biometric authentication system needs a fiducial mark on the user's skin surface to identify the same region as the user's template. By changing the position of the mark, it is possible to re-register the biometric information of the user. By removing the mark, it becomes considerably difficult even for a legitimate user to find the position. Thus, users can control the lifetime of the registered skin texture by managing the fiducial mark. In addition, as described in Section VI.D, the fiducial mark can also be used to provide advanced biometric authentication mechanisms. However, as this is a prototype system, in this paper we chose a relatively simple method to prepare the mark—specifically, we draw the mark by solvent ink on the surface of the user's skin.

B. How to Obtain Micro Patterns

There are various ways of obtaining micro patterns of human skin texture. The three main ones shown in literature [10] involve using a confocal microscope, a 3D scanner, and a simple microscope. In this work, we chose to use a simple microscope because of costs and availability. We use the A2001 Dino-Lite Basic microscope manufactured by Thanko Inc. Table 1 shows the specifications of the microscope. In our prototype system, a 200x magnified image of a roughly 2.0×1.5 mm region of skin with a resolution of 640×480 pixel is captured with the microscope. The 256×256 pixel (about 1.0×1.0 mm) image around the central area of the 640×480 pixel image is then used as a template. (We found that there were several users who obtained out of focus images in 200x times magnification in our experiment (Section V). We therefore had them apply 205x magnification.)

Table 1 Specification of AM2001 Dino-Lite.

Model	AM2001 Dino-Lite Basic
Product Resolution	640×480 pixels (VGA)
Magnification Rate	10x-230x
Sensor	0.3 Mpixels, 1/4 inch CMOS

C. Image Alignment

The system can take an image of almost the same region as its template by using the mark. However, depending on the photographing environment, distortion and/or position deviation may occur. To cope with this issue, it is necessary to align the user's template image T (=X) and authentication image X' (also, see Fig. 2). We have to develop a system that makes it possible to align them automatically. However, as this is a prototype system, in this paper we align them manually. To be more specific, we use the vertices of each square of a template image (256×256 pixel) as guide points for the alignment. In the authentication phase, from a 640×480 pixel image taken by microscope, we look for the points that are similar to the guide points in the corresponding template image. The tetragonal region is then transformed into a 256×256 square image by using projective transformation. This image is then used as the authentication image.

D. Feature Extraction

We use skin roughness as the feature for authentication. To obtain a stable feature, each image is transformed by the following process implemented by a C++ program including Open CV Ver.2.4.9 [11].

1. Grayscale conversion: This is used to cope with illumination changes.
2. Histogram equalization: This is used to make the roughness pattern clear.
3. Low pass filter: This is used to ignore high frequency noises. In the prototype system, a 256×256 pixel image f(x,y) is discrete Fourier transformed to yield F(u,v) at the interval of $-128 \le u,v \le 127$ and then inverse discrete Fourier transformed with the coefficients of F(u,v) for $-128 \le u,v \le -63$ and $64 \le u,v \le 127$ set to zero to obtain the filtered image of f(x,y).
4. Adaptive threshold: This is used to extract the roughness pattern. We use a OpenCV library cvAdaptiveThreshold() whose parameters are set as follows: inAdaptiveMethod = ADAPTIVE_THRESH_MEAN_C; inThresholdType = THRESH_BINARY; inBlockSize = 25.

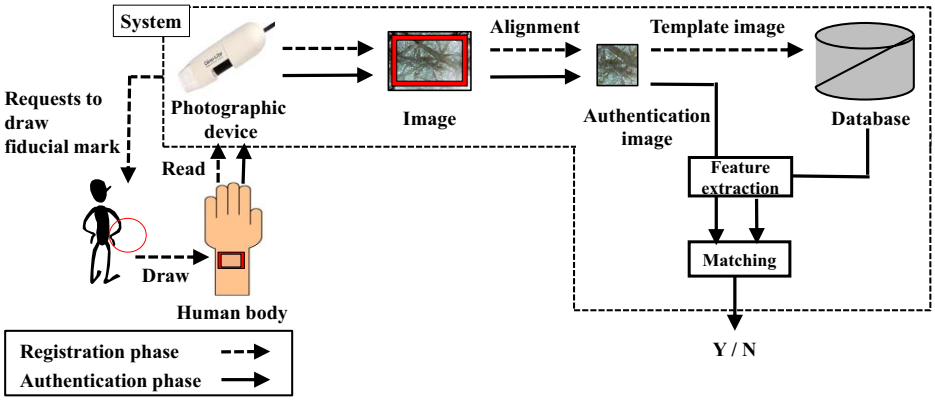


Fig. 1 System overview.

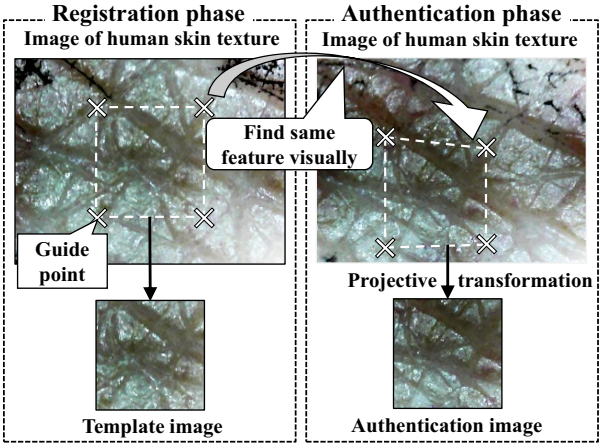


Fig. 2 Alignment overview.

Figure 3 shows an example of the skin texture image process. Figure 3(a) is the original image for a user captured on the first day, which is used as a template. By applying grayscale conversion and histogram equalization, we obtain the image in Fig. 3(d). After applying a low pass filter and adaptive threshold, we obtain the image in Fig. 3(g). Figure 3(b), (e), (h) and Fig. 3 (c), (f), (i) are the equivalent images to Fig. 3 (a), (d), (g) for the same user but captured on the second and third days, respectively.

E. Matching

In the prototype system, we calculate the matching score between a template image and an authentication image by normalizing cross-correlation. This calculation process is implemented by a C++ program including Open CV Ver.2.4.9. The matching score is calculated by using an OpenCV library cvMatchTemplate(). We use CV_TM_CCOEFF_NORMED as the matching algorithm. The matching score reaches 1.0 when the similarity is high.

V. User Experiment

We conducted a basic experiment in which we collected minute patterns of users' skin texture over three days. These patterns were then used to evaluate our proposal from the viewpoints of false acceptance rate (FAR) and false rejection rate (FRR).

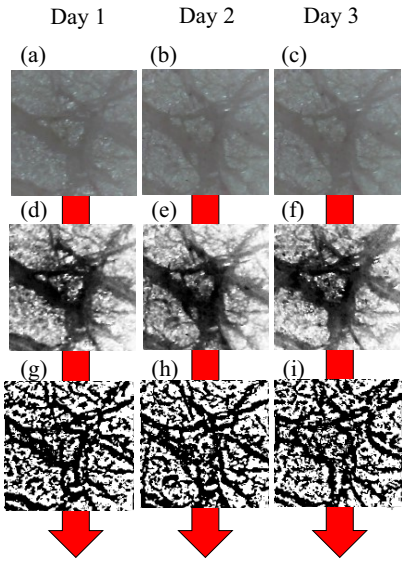


Fig. 3 Feature extraction.

A. Collecting Sample Images

We recruited ten participants (male: nine, female: one, age: 21–26), all of whom are students at Shizuoka University. Users drew fiducial marks by solvent ink in five places anywhere on the skin surface of their forearm. Microscope images were then collected on three consecutive days. We took two images of each mark once a day, which means we obtained 30 sample images (5 places × 2 images × 3 days) per participant.

Unfortunately, some of the marks disappeared over the course of daily life, and we were not able to take the images related with the disappeared marks. As Table 2 shows, 18 marks disappeared on the third day. We therefore collected 100 sample images (50 places × 2 images) on the first day, 100 sample images (50 places × 2 images) on the second day, and 64 sample images (32 places × 2 images) on the third day. The total number of sample images is 264.

B. Evaluation

We evaluated the false accept rate (FAR), false reject rate (FRR), and equal error rate (EER) of our system by using leave-one-out cross validation. For FAR, we calculated the matching

Table 2 Number of disappeared marks.

Subject	Day 1	Day 2	Day 3
1	0	0	0
2	0	0	5
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	5
8	0	0	0
9	0	0	3
10	0	0	5

scores between different places. The experimental setup of 10 participants × 5 places is intended to provide an evaluation equivalent to one with 50 individual users. This evaluation is thus a "between-user" evaluation. For FRR, we calculated the matching scores between the same places. This evaluation is also a "within-user" evaluation. Figure 4 plots the FAR and FRR calculated with different thresholds ranging from –1 to 1. Assuming that both the distribution of the matching scores between the same places and the distribution of the scores between different places follow normal distribution, we obtained EER=0.5% from Fig. 4.

VI. Discussion

A. Requirement 1

Our prototype system uses only similarity between an authentication image and template image for authentication. If an attacker obtains a template image, he/she must print the image using a printer and then try to carry out a masquerade attack (logging into the system by using printed data). This is probably the most general and effective attack against our prototype system, so we focus on this attack.

The size of skin used by our system is about 2.0 × 1.5 mm. Figure 5(a) shows an example image taken by a microscope and enlarged 200 times. We printed this image in the size of about 2.0 × 1.5 mm on a paper using some consumer-level printers. After that, we took images of the printed images with the microscope again. Figure 5(b), (c), and (d) shows these micrographic images for Brother MFC-8520DN, FUJI Xerox DocuPrint C525 A, and Canon PIXUSMP610, respectively. As the figures show, the printed images are very different from that image in Fig. 5(a), i.e., attackers cannot carry out a masquerade attack against our system by using consumer-level printers.

Of course, attackers may have access to super-resolution printers of the type used by professionals. In this case, the possibility of being successful in a masquerade attack is higher, but it also means that the costs of the attack are relatively high. Furthermore, we can apply some countermeasures in the system itself to reduce this possibility. A typical technology for this is liveness detection, such as checking sweat from sweat glands.

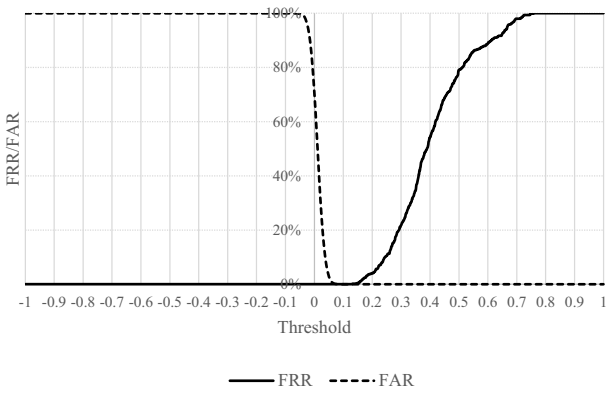
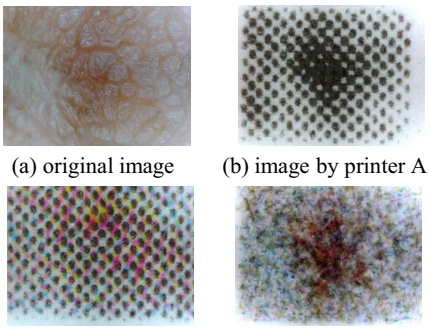


Fig. 4 FAR and FRR.



(a) original image (b) image by printer A

(c) image by printer B (d) image by printer C

Fig. 5 Forged images by consumer-level printers.

From the above, we can confirm that micro biometric authentication satisfies the requirement for higher tolerance against masquerade attacks.

B. Requirement 2

As discussed in Section V.B, EER was evaluated under the assumption that five different places on the same participant are considered to be five different users. If minute skin images captured from different places on the same participant are similar to each other, the FAR would become higher in this experimental setting. However, the results of the experiment in Section V.B showed that our prototype system achieved a remarkably lower FAR (EER is the point where FAR and FRR are equal; EER=0.5% means FAR=FRR=EER=0.5%). Judging from that, we can safely say that even in the same person, minute skin patterns captured from different places are distinct from each other. Therefore, whenever a user changes his/her registered template (minute pattern of skin texture), traceability is lost.

It is said that the total surface area of human skin reaches about 1.6 m^2 [12]. Our prototype system uses a 1.0×1.0 mm sample as each template. We can estimate that every user has about 2.6×10^6 minute patterns on his/her body. Therefore, even after taking into account the fact that we cannot use the skin patterns that are hidden beneath clothing, it is still plausible that every user will be able to use at least a few thousand patterns to a few tens of thousands of patterns on his/her skin. This number

is large enough for users to continue re-registering their new templates (minute pattern of skin texture).

From the above, we can confirm that micro biometric authentication satisfies the requirement of hindering traceability.

C. Requirement 3

As discussed in Section V.B, our authentication system achieved EER=0.5% for at least three days. To the best of our knowledge, there is no behavioral biometric authentication system that has a lower accuracy than EER=0.5 %. From the above, we can confirm that micro biometric authentication satisfies the requirement of higher authentication accuracy.

D. Using a Seal

The prototype system uses solvent ink for making the fiducial mark. We can also use a seal, which is slightly more expensive but has many advantages. One of the biggest advantages is that we can embed additional information on the seal that can be read under a microscope at the same time the skin image is captured. For instance, by printing a user ID on the seal, a user does not need to input his/her ID when logging into a 1:1 authentication system. Also, we can print a random number on the seal that can be used for template protection in cancelable biometric authentication systems. It should be noted here that even if the attacker can steal the seal of a legitimate user, it is still impossible to impersonate the legitimate user without genuine biometric information.

E. Brute Force Attack

As discussed in Section VI.B, a user will have about 2.6×10^6 minute patterns on his/her own skin. This means that attackers can use all their minute patterns for a brute force attack before they attempt to collect someone else's biometric information. This is a concern for our system.

A countermeasure against this type of attack is to apply the idea of artifact metrics to a fiducial mark. This can be achieved by using a seal as the fiducial mark and printing a different random number on each seal. In the registration phase, a seal is given to a user and then the random number on the seal is registered with the user's minute skin pattern in the authentication system. In the authentication phase, the random number on the seal is read by the microscope at the same time the skin image is captured. A user can be authenticated when both the minute skin pattern and the random number are confirmed. Attackers need to obtain both the biometric information and the seal to be successful in their brute force attack, meaning that it is almost impossible to succeed with this attack.

VII. Conclusion

In this paper, we proposed micro biometric authentication, which uses minute patterns of physiological biometric information. Minimization of the biometric information used for authentication helps instill the authentication mechanism with (i) higher tolerance against a masquerade attack, (ii) consideration of the issue of traceability, and (iii) higher authentication accuracy. As a first attempt, we applied minute patterns of human skin texture into the mechanism and conducted a basic experiment to check the feasibility of the mechanism. Results showed that the system achieved an EER of about 0.5%.

In future, we intend to implement an automatic alignment procedure for users' template/authentication images and to conduct a more comprehensive experiment with a number of participants over a long period of time. We will also investigate other modalities used for micro biometric authentication.

Acknowledgements

The authors acknowledge the valuable advice and suggestions given by Dr. Akira Otsuka and Dr. Tetsushi Ohki of the National Institute of Advanced Industrial Science and Technology, Japan and Prof. Hiromasa Nakatani and Prof. Hitoshi Saji of Shizuoka University, Japan. The authors are also grateful to Hiroaki Muramatsu of Shizuoka University, Japan for his support.

References

[1] *FIDO Aliance* [Online]. Available: https://fidoalliance.org/

[2] Y. Kaga *et al.*, "Biometric Authentication Platform for a Safe, Secure, and Convenient Society—Public Biometrics Infrastructure", Hitachi Review, vol. 64, no. 8, pp. 472–479, 2015.

[3] T. Putte and J. Keuning, "Biometrical fingerprint recognition: Don't get your fingers burned" in *Proc. IFIP TC8 / WG8.8 Fourth Working Conf. on Smart Card Research and Advanced Applications*, Bristol, pp. 289-303, 2000.

[4] K. Zoe (2014, December 29). *Politician's fingerprint 'cloned from photos' by hacker* [Online]. Available: http://www.bbc.com/news/technology-30623611

[5] Biometrics Security Consortium, *Biometric security technology handbook*, Ohmsha, Japan, 2006. (in Japanese)

[6] Bank of Japan (2004, August 23). Security Features of the New Bank of Japan Notes [Online]. Available: https://www.boj.or.jp/en/note_tfjgs/note/security/bnnew3.htm/

[7] T. Matsumoto *et al.*, "Nano-artifact metrics based on random collapse of resist", Sci. Rep., vol. 4, Aug. 2014.

[8] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics", *J. on Inf. Security*, pp. 1–25, 2011.

[9] V. Woollaston (2013, May 31). *The hi-tech tattoo that could replace ALL your passwords: Motorola reveals plans for ink and even pills to identify us* [Online]. Available: http://www.dailymail.co.uk/sciencetech/article-2333203/Moto-X-Motorola-reveals-plans-ink-pills-replace-ALL-passwords.html

[10] N. Arakawa *et al.*, "Development of Quantitative Analysis for the Micro-Relief of the Skin Surface Using a Video Microscope and Its Application to Examination of Skin Surface Texture", *J. of Cosmetic Chemists of Japan*, vol. 41, no. 3, pp. 173–180, 2007. (in Japanese)

[11] *Open CV* [Online], Available: http://opencv.org/

[12] A. E. Bender and D. A. Bender, "Body Surface Area," in *A Dictionary Food and Nutrition*, Oxford, England: Oxford University Press, 1995.