Micro Disposable Biometric Authentication : An Application Using Fingernail Minute Textures for Nonsensitive Services

Micro Disposable Biometric Authentication

- An Application Using Fingernail Minute Textures for Nonsensitive Services -

Genki Sugimoto, Masahiro Fujita, Yuto Mano, Tetsushi Ohki and Masakatsu Nishigaki
Shizuoka University, Japan
3-5-1 Johoku, Naka, Hamamatsu, Shizuoka, 432-8011 Japan
+81-53-478-1467
nisigaki@inf.shizuoka.ac.jp

Abstract

Recently, biometric authentication has been applied to not only sensitive services such as in emigration/ immigration inspection systems and ATMs but also nonsensitive services such as entry/exit management systems of theme parks or coin lockers. However, biometric authentication requirements for sensitive and nonsensitive services differ; each service requires suitable biometric authentications. In this paper, disposable micro biometric authentication using minute fingernail texture for nonsensitive biometric authentication is proposed.

CCS Concepts

• Security and privacy → Security services → Authentication → Biometrics • Information systems → Information systems applications

Keywords

Biometrics; Privacy preservation; Disposability; Minute pattern; Nail texture

1. Introduction

Biometric authentication is a verification process based on physiological biometric information or behavioral biometric information. In comparison to authentication using password or token, biometric authentication is convenient because it does not require remembering security-related information and there is no possibility of information being lost or stolen. In recent years, in addition to sensitive services such as immigration/emigration inspection and ATMs [1], biometrics are becoming increasingly used for nonsensitive services such as access management systems for amusement parks and coin lockers [2]. Sensitive services and nonsensitive services require different biometrics requirements. In this work, we focus on the use of biometric information for authentication in nonsensitive services.

A service that requires confirmation of the identity of the user is defined as "sensitive service." Typically, this is a relatively expensive service or a service used to some extent for a long time. For many sensitive services, authentication will be implemented by using real names of users. It is important that countermeasures must be adopted against masquerade attacks carried out by counterfeiting biometric information. A masquerade attack is caused by an attacker who steals and forges the biometric information of a legitimate user. In fact, cases have been reported in which an attacker copied a face photograph or used an artificial finger from the biometric information stolen and succeeded in spoofing [3][4]. In recent years, stealing high-resolution images of iris and fingerprints from a long distance is not difficult because of the high performance of cameras. Besides, because it is required for a sensitive service to be able to confirm identity over a relatively long period, countermeasures against changes with time of biometric information (e.g., adoption of biometric information with little change over time) are also required.

Meanwhile, a service that is sufficient to confirm the attribution of the user (e.g., whether or not he/she has already paid the fee) is defined as "nonsensitive service." Typically, this is a relatively inexpensive service or a temporarily used service. Even in the case of cheap services and/or short-term services, reasonable measures against masquerade attacks should be taken, considering the cost–security balance. Indeed, in such services as coin lockers, security is essential since personal possessions or valuable items are kept. Thus, nonsensitive services require tolerance against forgeries similar to that required by sensitive services (requirement 1: unforgeability).

An attribute authentication system does not always require to register user's real name. Therefore, in the case of a nonsensitive service, users can confirm their identity anonymously or by using a pseudonym. However, in biometric information is traceable. Suppose that, for example, a user uses the same biometric information on several anonymous accounts. If an attacker gets the biometric information, he/she can understand these accounts are used by the same person. Biometric information cannot be reset by changing or replacing like passwords and tokens. Therefore, even if it is a nonsensitive anonymous service, we should strictly protect the privacy concerning user tracking (requirement 2: untraceability).

Biometric authentication has become widespread, and presenting biometric information is required for various services. The more the exposure opportunities of biometric information are, the greater the risk of leakage. Especially for low-priced services, since great amounts of funds are not allocated for security measures, it is inevitable that biometric authentication used in nonsensitive services will increase the risk of leakage of biometric information compared to the risk in the case of sensitive services. For this reason, nonsensitive services require a disposal mechanism for biometric information (requirement 3: disposability). From this view point, adopting biometric information with a large change with time (biometric information of the past and current are different with each other) may be effective.

As described above, sensitive services and nonsensitive services have different biometric requirements. For this reason, both

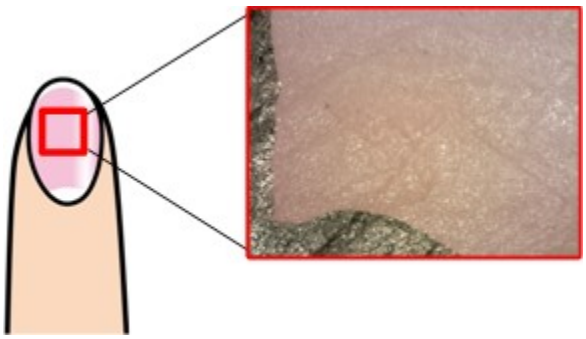


Figure 1: Texture pattern on the fingernail plate (the black area is a part of mark)

biometric authentication used for sensitive services and that for unsensitive services should be properly discussed individually. However, only the studies about the biometric authentication for sensitive services have been extensively reported so far.

In this paper, micro biometric authentication using minute patterns on fingernail surface is proposed as a nonsensitive biometric authentication method satisfying requirements 1 to 3. Section 2 introduces related studies. Section 3 explains our proposed method. In Section 4, a basic experiment to demonstrate the possibility of the proposed method is presented and evaluated. Some discussions are presented in Section 5, and this paper is summarized in Section 6.

2. Related Research

A method to tackle requirement 2 is biometric template protection, such as cancelable biometrics [7] . In this method, a user registers $F_R(X)$ as his/her template instead of X, where F is a transform function; X is a user's biometric information; R is a user's random number, so that the user can generate his/her new template by changing R. However, even if we use this method, X (biometric information) is still unchangeable. This means that the biometric template protection is not a measure to protect physical biometric information, but a measure to protect only the template.

For the protection of physical biometric information, the transient biometric authentication and the micro biometric authentication have been studied so far. However, to the best of our knowledge, there is no research that applies minute patterns of nail surface into biometric authentication. For this reason, we introduce some works related with "nail" or "minute patterns".

Garg et al. proposed an authentication method that uses vertical longitudinal striations on the entire nail surface as a feature and showed its usefulness [5]. However, since vertical longitudinal striations are indicated as invariant features like fingerprints, they do not satisfy requirement 2 or requirement 3. Furthermore, because it seems that resistance to spoofing by imitation is also low, vertical longitudinal striations do not fulfill requirement 1.

Barros Barbosa et al. proposed biometric authentication using the nail surface [6]. Although their transient authentication method satisfies requirement 3 by using a nail growth, forging or counterfeiting is not very difficult because the nail image photographed with a normal camera can be used for authentication. In addition, when multiple accounts are registered using the same nail at around the same time, there is a possibility of merging of accounts by using registration information. As a result, requirement 1 and requirement 2 are not satisfied.

As a method satisfying requirements 1 and 2, we proposed a method called “micro biometric authentication” [8]. This method uses the static feature of a minute pattern of skin textures.

In general, the smaller patterns we use, the more difficult it becomes for attackers to manufacture a clone of a pattern. Nevertheless, taking an image of a minute pattern with a microscopic lens is considerably easy. This "asymmetry of the cost of photographing and counterfeiting" motivated us to register biometric information of a certain microscopic site as a template and realize biometric authentication that requires a large cost for forgery even if the information of the site is stolen.

By using a minute biological part, the updatable number of body parts is increased because a number of minute patterns are extracted from a user’s body. The user changes the body part updated to another biological part on the user's own intention when the necessity arises, in the same sense as changing the password or replacing the token. Every time the user updates the biological part, the biometric information registered for authentication is changed, and the traceability is divided. However, this method cannot satisfy requirement 3 since skin texture patterns are not an aging biometric information over a relatively long period of time.

As far as the authors know, biometrics that satisfy requirements 1 to 3 do not exist. In Section 3 and later, “disposable micro biometrics,” a method that satisfies all requirements, is proposed.

3. Disposable Micro Biometrics

3.1 Micro Biometrics Using Fingernail Textures

To realize micro biometric authentication that satisfies requirement 3, we use a body part that grows/changes over time. In this study, we focus on micro biometric authentication using a minute region of the nail as one form of realization.

The nail is a part of the skin and is composed of a toe, a nail bed, a nail plate, a nail matrix, a free edge, and the like [9]. When the surface of the nail is greatly enlarged by a microscope, the pattern on the surface of the nail can be seen (Figure 1). By using this minute concavo–convex pattern as authentication information, it is expected that micro biometric authentication using nail texture images can be realized. The speed at which the nail grows (the length of the newly made nail) is said to be 0.1 [mm/day] [10]. As the nail of a user grows and the part earlier used for authentication reaches the free edge, the user will cut the nail. When the nail is cut, the previous biometric information is discarded.

As described in Section 2, micro biometric authentication satisfies requirements 1 and 2. As described above, biometric authentication using biometric parts that change over time satisfies requirements 3. By combining both, a "disposable micro biometric authentication" method that satisfies requirements 1 to 3 is realized.

3.2 Procedure

The procedure of this authentication system is shown below (see also Figure 2). Although the procedure of 1: 1 authentication is shown here, it can also be applied to 1: N authentication.

Registration Phase:

1. The user registers his/her ID in the system.

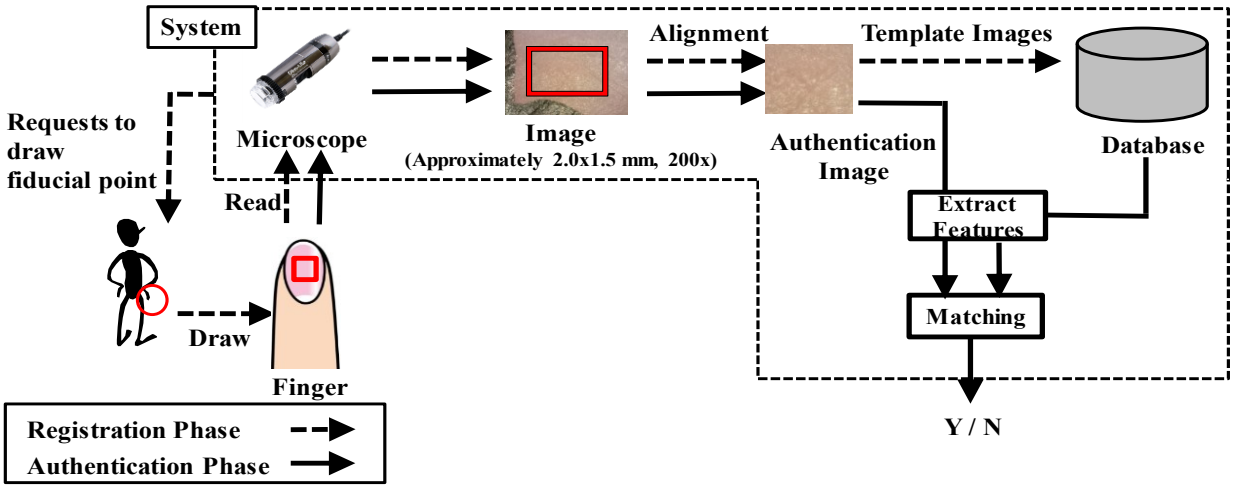


Figure 2: System overview

2. The system asks the user to print a mark on the nail surface.
3. The user prints a mark on the nail surface.
4. The system follows the mark and reads the user's minute biometric information X with a microscope.
5. The system saves X as a user's template in the database.

Authentication Phase:

1. The user presents his/her ID to the system.
2. The system follows the mark and reads the user's minute biometric information X' with a microscope.
3. The system refers to the user's template T (= X) from the database.
4. When X' is sufficiently close to T, the user is judged to be an authorized user.

3.3 System

The system constructed is described in detail. This system is based on the micro biometric authentication system implemented in literature [8] and a program module that extracts features from nail images is added. When comparing the templates of nail images and authentication images, the similarity of patterns on nail surfaces was calculated by template matching. However, as the reflection of the nail surface changes due to illumination fluctuation every time the image is taken, the similarity decreases even for the image of the legitimate user. To cope with this, we apply local binary pattern transformation.

3.3.1 Registered Region

In micro biometrics authentication, it is necessary for users to print a mark on the surface of the nail to help the authentication system discover the registered micro site from the entire nail. As the nail grows and the marked area reaches the free edge, the user can physically discard the registered biometric information by cutting the nail. If the user wants to change the biometric information used for authentication immediately, the user can print new mark on the nail surface and re-register the region. Every time the position of this mark is changed, the user can change the biometric information used for authentication. In this paper, we adopted a method of directly printing a mark on the surface of the nail using water-based ink and applying a top coat (transparent manicure) from above to protect the mark.

3.3.2 Image Alignment

When photographing nails, a microscope was used in this paper. The microscope used is AM7915-Dino Lite Edge S (manufactured by Sanko Co., Ltd.). This system used a nail image magnified 200 times (2592 × 1944 pixels, approximately 2.0 × 1.5 mm) taken with the microscope. In the registration phase, a central 800 × 800 pixel area of the 2592 × 1944 pixel image is cut out and used as a template image. In the authentication phase, the system searches for the area (800 × 800 pixels) most similar to the template from 2592 × 1944 pixel images and extracts the area.

3.3.3 Feature Extraction

In this study, we used the concave–convex pattern of the surface of the nail as a feature. To obtain stable features, the template image and the authentication image are converted to local binary patterns (LBP) after conversion to grayscale. LBP, proposed by Ojala in 1994, is known for robustness to changes in the gray values of an image [11]. We use scikit-image Ver.0.14dev [12] to implement LBP conversion.

3.3.4 Matching

Matching is performed by comparing histograms of the template image and the authentication image after LBP conversion (Figure 3). For comparison of histograms, a method using the chi-squared value of the histogram value is adopted. The matching score d (H_1, H_2), where H_1 is the histogram of the template image and H_2 is the histogram of the authentication image, is calculated by the following equation.

$$d(H_1, H_2) = \sum_I \frac{(H_1(I) - H_2(I))^2}{H_1(I) + H_2(I)}$$

4. Evaluation

4.1 Dataset

To confirm the efficiency of the proposed method, a basic authentication experiment using minute nail images was carried out for three days. Five students of the university cooperated as the subjects. Three nails of the index finger, the middle finger, and the ring finger of the right hand per person were used, and two arbitrary minute regions, one in the center of the upper half area (toe side) and another in the center of the lower half area (root side), of each nail were

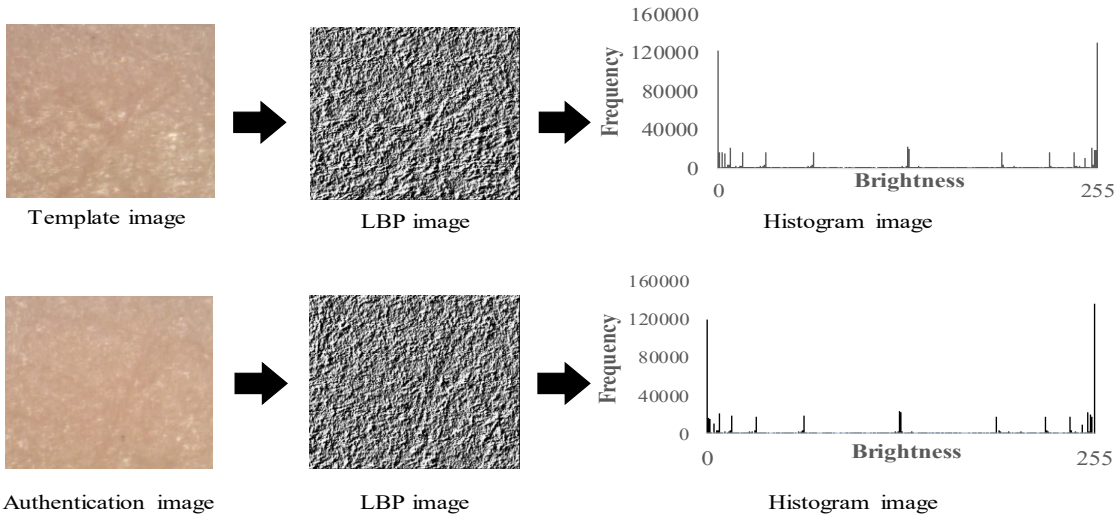


Figure 3: Feature extraction and matching

photographed with a microscope.

Those images (six regions in total) taken in the morning on the first day were used as template images. Authentication images of each regions were taken once a day. Authentication images of the first day were taken in the afternoon, and authentication images of the second and third days were taken at arbitrary times of day.

At the time of photographing the template, a mark was printed with water-based ink on each six regions of the nail to be photographed, and a topcoat was applied from above. It is noted that these marks were not printed on the exact positions of each minute regions. In the authentication phase of this experiment, a registration area was found based on the mark printed on the nail and the experimenter (authors) photographed the regions so that the appearance matched as much as possible with the template image.

4.2 Procedure

We evaluated the proposed method based on the samples of the minute nail images obtained as described in Section 4.1. Hereinafter, we refer to the minute region in the root side of the index finger as 1, the toe side as 2, and the middle finger and ring finger as 4 to 6 in the same way. The template image of region j ($1 <= j <= 6$) of subject i ($1 <= I <= 5$) is denoted as $t_{i,j}$, and the authentication image of region q ($1 <= q <= 6$) of subject p ($1 <= p <= 5$) on day r ($1 <= r <= 3$) is expressed as $a_{p,q,r}$.

4.3 Authentication accuracy

Whether authentication using minute regions of nails is possible or not was evaluated. The matching score of the legitimate subjects on the first day was calculated by comparing $t_{i,j}$ with $a_{p,q,r}$ ($i = p, j = q, r = 1$), and the matching score of other subjects/regions is calculate by comparing $t_{i,j}$ with $a_{p,q,r}$ ($i \neq p , j \neq q, r = 1$). On the second and third days, the matching scores are calculated in the same way with $r = 2$ or $r = 3$. Figure 4 shows the FRR and the FAR when changing the authentication threshold (θ). When calculating the equal error rate (EER) on the first day, it was EER ≈ 0.07 with $\theta \approx 0.01$. On the second day, EER ≈ 0.09 with $\theta \approx 0.01$, and on the third day EER ≈ 0.1 with $\theta \approx 0.01$. Although EERs were slightly high, this system can sufficiently identify the minute regions of the fingernail.

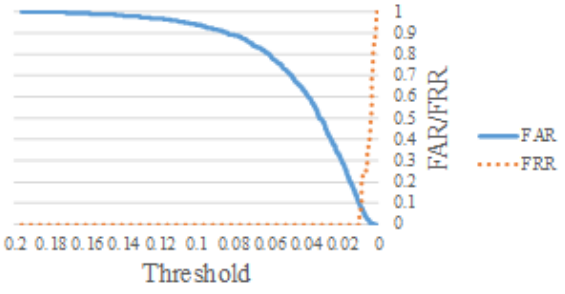
4.4 Disposability of biometric information

Whether the minute pattern on the nail surface is disposable or not was evaluated. If another region of the same nail is identified as another person's, it can be said that even when users use the same nail, every time users re-register a different region on the nail, the association of biometric information of the past and current can be divided. The matching score of the legitimate regions was calculated by comparing $t_{i,j}$ with $a_{p,q,r}$ ($i = p, j = q, 1 <= r <= 3$), and the matching score of other regions of the same nail was calculated by comparing $t_{i,j}$ with $a_{p,q,r}$ ($i = p, j = q - 1$ (for $j = 2, 4, 6$) or $j = q + 1$ (for $j = 1, 3, 5$), $1 <= r <= 3$). Figure 5 shows the FRR and the FAR when changing the authentication threshold. When the EER was calculated at this time, it was EER ≈ 0.09 with $\theta \approx 0.1$. Because this is almost the same EER (and θ) as compared with the other person's regions evaluated in Section 4.3, it is possible to regard the different regions of the same nail as the regions of another person.

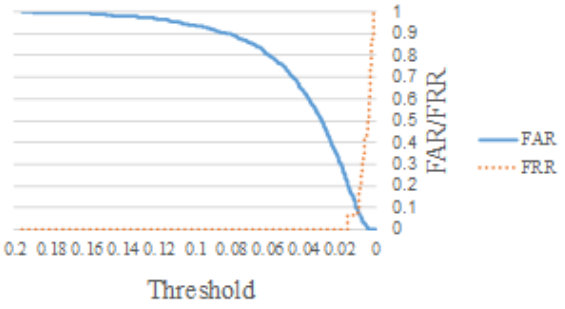
5. Discussion

5.1 Requirement 1

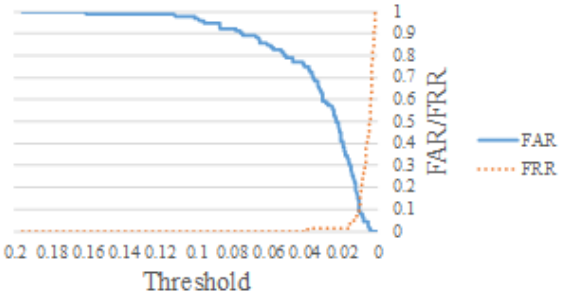
In this system, a nail image in the range of approximately 0.7 × 0.7 mm magnified at about 200 times by a microscope



day1



day2



day3

Figure 4: FAR and FRR for 3 days

is used as a template. As long as any authentication image is fed to the system by using the legitimate microscope, attackers must generate micro-level counterfeits to successfully carry out a masquerade attack, and hence counterfeiting costs are relatively high. Therefore, this system satisfies requirement 1 (tolerance against a forgery).

5.2 Requirement 2

By using the finer region of fingernail, the number of updatable times of the region (the number of times until the unused region is exhausted when using the minute regions one by one) increases. When the necessity arises in the same sense as changing the password or replacing the token, the user changes the fingernail region used up to then to another

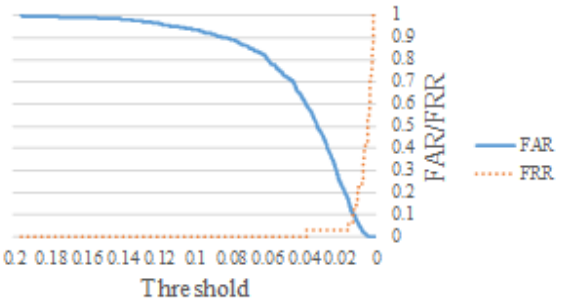


Figure 5: FAR and FRR on the same nail

fingernail region of the user's choice. Every time the user updates the fingernail region, the biometric information used for authentication is changed, and thus the traceability between registered biometric information is lost. Therefore, this system satisfies requirement 2 (hindering traceability).

5.3 Requirement 3

It is obvious that when the nail grows and the part earlier used for authentication reaches the free edge, the registered biometric information can be discarded by cutting the nail. In addition, as shown in Section 4.4, for even the same nail of the same user, the minute pattern on fingernails is different for each region. In other words, it can be considered that the registered biometric information can be discarded by changing the nail regions even before the nail grows. Therefore, we can say that the minute pattern on the nail surface is a disposable biometric information. Thus, this system satisfies requirement 3 (disposability).

5.4 Limitation

As mentioned in Section 1, nonsensitive services are inexpensive and/or temporarily used services. In the case of inexpensive services, convenience may be given priority to security because the costs for countermeasures should be commensurate with the value of services. From this viewpoint, the proposed biometric authentication that requires the use of microscopes with 200× magnification may not be suitable for inexpensive services. If even using an inexpensive low-magnification microscope can improve the security to a certain extent, using a micro body part for authentication could be effective. In the case of services temporarily used, such as coin lockers that can keep customer's valuable goods, it is likely that a high degree of security is required. In such cases, the proposed method is considered to be suitable.

6. Conclusion

In this paper, we proposed biometric authentication using minute regions of the fingernail as a disposable biometric authentication method suitable for nonsensitive services and evaluated it through a basic experiment. Experimental

results showed that the effectiveness of the proposed system from the viewpoints of the accuracy and disposability. Since it was a basic experiment with a small number of samples this time, it could not be evaluated statistically. Hence, in addition to improvement of accuracy, reevaluation by increasing the number of samples is a future work to be addressed urgently.

References

[1] Japanese bank using fingerprint authentication at its ATMs. 2015. Available: http://www.biometricupdate.com/201512/japanese-bank-using-fingerprint-authentication-at-its-atms.

[2] Privacy Information Center. 2018. Available: https://www.universalorlando.com/web/en/us/privacy-info-center/index.html#subnav-e.

[3] T. Putte and J. Keuning. 2000. 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*, 4(1):289-303. DOI= https://doi.org/10.1007/978-0-387-35528-3_17.

[4] K. Zoe. Politician's fingerprint 'cloned from photos' by hacker. 2014. Available: http://www.bbc.com/news/technology-30623611.

[5] Shruti Garg, Amioy Kumar, and M. Hanmandlu. 2014. Finger Nail Plate: A New Biometric Identifier. *International Journal of Computer Information Systems and Industrial Management Applications*, 6(1):126-138. DOI= https://doi.org/10.1016/j.eswa.2013.07.057.

[6] Igor Barros Barbosa, Theoharis, and Ali E. Abdallah. 2016. On the use of fingernail images as transient biometric identifiers. *Machine Vision and Applications*, 27(1):65-76. DOI= https://doi.org/10.1007/s00138-015-0721-y.

[7] C. Rathgeb and A. Uhl. 2011. A survey on biometric cryptosystems and cancelable biometrics. *J. on Inf. Security*, pp. 1-25. DOI= https://doi.org/10.1186/1687-417X-2011-3.

[8] Masahiro Fujita, Yuto Mano, Takuya Kaneko, Kenta Takahashi, and Masakatsu Nishigaki. A Micro Biometric Authentication Mechanism Considering Minute Patterns of the Human Body. *19th International Conference on Network-Based Information Systems*, 159-164, 2016.

[9] David de Berker. 2013. Nail anatomy. *Clinics in Dermatology*, 31(5):509-515. DOI= https://doi.org/10.1016/j.clindermatol.2013.06.006.

[10] S Yaemsiri, N Hou, MM Slining, and K He. 2010. Growth rate of human fingernails and toenails in healthy American young adults. *JEADV*, 24(4):420-423. DOI= https://doi.org/10.1111/j.1468-3083.2009.03426.x.

[11] T.Ojala, M. Pietikainen, and D. Harwood. 1994. Performance evaluation of texture measures with classification based on Kullback discrimination of distributions. *Proceedings of 12th International Conference on Pattern Recognition*, Vol.1. DOI= https://doi.org/10.1109/ICPR.1994.576366.

[12] scikit-image. 2018. Available: http://scikit-image.org/.