We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

4,800
Open access books available

122,000
International authors and editors

135M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS BOOK CITATION INDEX INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

7

Cancelable Biometric Identification by Combining Biological Data with Artifacts

Nobuyuki Nishiuchi and Hiroka Soya
Tokyo Metropolitan University
Japan

1. Introduction

In present day information-oriented society, the ability to accurately and rapidly identify an individual in various situations, such as identity verification at an ATM, login authentication, and permitting access to secured rooms, has taken on considerable importance. Personal identification systems that rely on knowledge, for example, a password and ID number, or possession, for example, an ID card or keys, are subject to loss, counterfeiting, and theft. In addition, such systems suffer from the inability to identify the genuine user if the information is borrowed on permission of the user. Due to these limitations, the development of an identification system based on biometrics has attracted a great deal of interest as it obviates the requirement for physical possession or memorization of a security code and has the potential to differentiate individuals with high accuracy (Ashbourn, 2000; Prabhakar et al., 2003; Jain et al., 2004a, 2004b). To date, fingerprints, veins, iris, retina patterns, facial and other features have been used for biometric identification. The ideal biological data for biometrics has the following five characteristics (Wayman, 2000):

i. Distinctive: the biological data differs from one person to another.
ii. Repeatable: the biological data remains constant over a long period.
iii. Accessible: it is easy to view the biological data.
iv. Acceptable: it is not objectionable to show the biological data.
v. Universal: all people possess the biological data.

From different viewpoints, the five characteristics are associated with the potential problems and limitations of biometric identification.

1.1 Problems of biometric identification

Current biometric identification systems have a number of problems that are related with the five characteristics of biological data described in the above section. The three main problems are as follows:

Problem 1: The biological data cannot be replaced.
For instance, if a user's fingers are lost, or if fingerprint information is stolen, the user cannot use a fingerprint identification system. This problem is related with characteristics (ii) and (v).

Problem 2: Users are specified only from the biological data.

As biological data is information linked directly with individuals, if biological data is leaked, the user can be specified using only the leaked biological data. This problem is related with characteristic (i).

Problem 3: The biological data can be collected without consent of the user.

In general, because biological features are exposed on the surface of the body, such as the face, fingerprints, and iris, it is difficult to keep these features concealed from others. This problem is related with characteristics (iii) and (iv).

Due to these problems, current biometric identification systems have a major vulnerability: spoofing. Yamada et al. (2000), Stén et al. (2003), Hirabayashi et al. (2004), and Matsumoto (2006) described this vulnerability of biometric identification and demonstrated that it is possible with existing technology to obtain fingerprint information from adhered surface residue and replicate the fingerprint on an artificial finger. The theft and counterfeit of exposed biological information can be accomplished by first capturing an individual's targeted information as a two-dimensional image, and then using the data to reproduce a counterfeit model.

As a result of this vulnerability to spoofing, and despite progress with various types of biometric systems, users are often hesitant to submit their unique biological data during the initial enrollment process (Gunn, 2010). It is easy to envision that users of restricted facilities, such as buildings, commercial establishments, accommodations, and amusement parks, may not willingly submit the necessary biological information for a biometric identification system.

To overcome these limitations, novel approaches for the development of practical biometric identification systems that do not retain or require potentially sensitive user information are needed.

1.2 Proposed method of cancelable biometric identification

In this chapter, we introduce a novel method of cancelable biometric identification that combines biological data with the use of artifacts and is resistant to spoofing. In this identification system, the user first attaches an artifact (a sticker with two dots) to the fingernail of the thumb or forefinger during the enrollment step, and subsequently presents the finger (biological data) with the attached artifact to the system for imaging. The position and direction of the artifact are uniquely detected based on the individual's biological data (outline of finger) using image processing. In the identification step, the user presents the finger with the attached artifact, and identification is accomplished by comparison of the probe and reference data. As the randomness of the position and direction of the artifact on the fingernail is quite high, the user can be uniquely identified. Notably, this system represents cancelable biometric identification, because once the artifact is removed from the fingernail, re-enrollment is required. From the viewpoint of ease of use, our proposed method is more acceptable than other identification methods using artifacts, such as RFID implants (Rotter et al., 2008).

This chapter is organized as follows. In Sections 2 and 3, the details of the proposed method of cancelable biometric identification are described. In Sections 4 and 5, the results of experiments and simulations using this method are presented and discussed. In Section 6, the features of the proposed method are summarized and applications of the method are proposed. Finally, conclusions and future directions are offered in Section 7.

2. Experimental setup

The artifact and hardware prototypes used in the experimental biometric identification system are shown in Figures 1 and 2. At the actual application stage, the artifact will be designed to have a less intrusive appearance and provide a higher level of security, and the imaging hardware will be smaller and more compact.

2.1 Artifact

We evaluated two artifact prototypes, having either a circular- or square-shaped design (Figure 1). For both types, a white base sticker was marked with one red and one blue dot. The circular artifact was 6 mm in diameter, and the square artifact was 5 × 1.5 mm in size. In the enrollment step, the user first attaches the artifact to the fingernail of the thumb or forefinger, and image processing is used to extract the dots on the artifact. As our initial evaluation did not detect any differences between the two types of artifacts during the data extraction, we selected the square type for use in further experiments because of its ease of fabrication. For practical use, the base sticker should be circular, transparent, and have dots printed with dye that can only be detected only under specific lighting, to maximize the difficulty of re-attaching the artifact at the same position and angle. To facilitate user acceptance of the system, ideally, the fingernail would not appear different from its usual appearance, and the attached artifact would not interfere with daily life. Moreover, it may also be possible to mark the fingernail directly with dye to serve as the artifact.

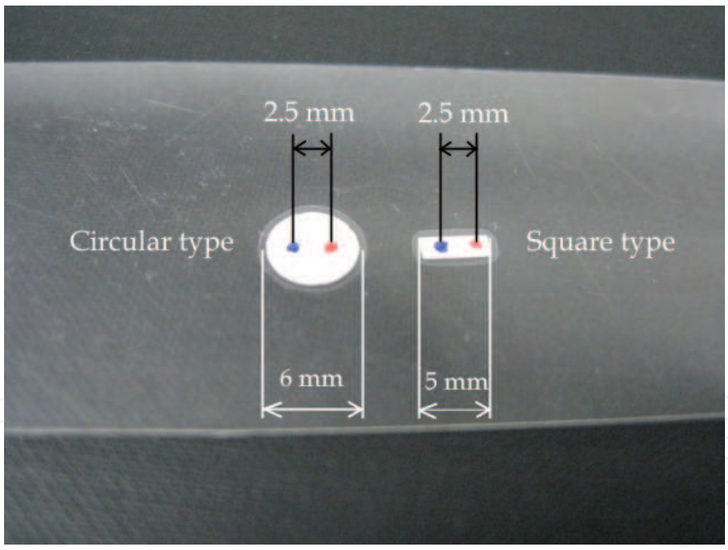


Fig. 1. Artifact used in the present system (left: circular type, right: square type)

2.2 Experimental device configuration

The device configuration of the experimental biometric identification system is illustrated in Figure 2. After placing the thumb or forefinger (in this experiment, the thumb was used) with the attached artifact on the stage, an image of the user's thumb was obtained with a single CCD camera (XC-505; Sony, Japan) under illumination by a LED light (NSF-150W; Shimatec, Japan). A black cloth was used as a backdrop to facilitate image processing. All images were analysed using Visual C++ 2008 software (Microsoft) and a 640 × 480 pixel

capture board (FDM-PCI4; Photron Ltd., Japan). A representative input image obtained using this system is shown in Figure 3.

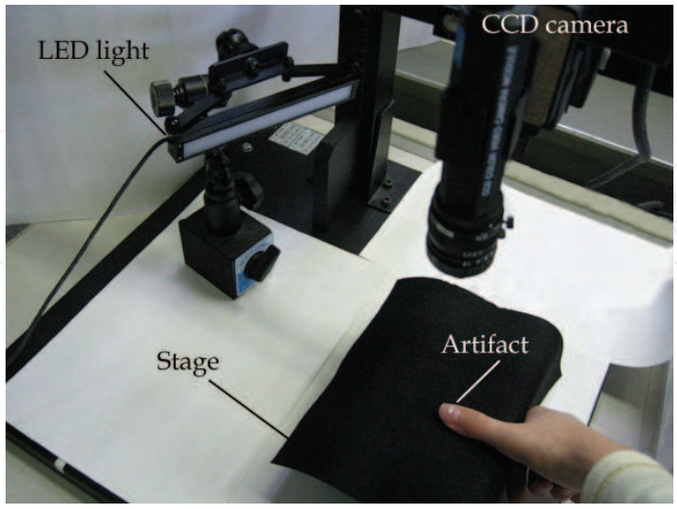


Fig. 2. Configuration of the experimental biometric identification system during image capture

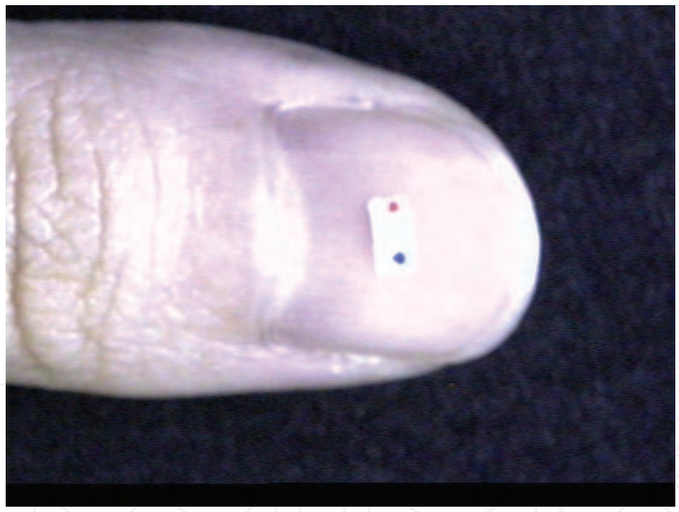


Fig. 3. A representative input image showing the artifact on a fingernail

3. Algorithm for cancelable biometric identification

The algorithm flow of the proposed cancelable biometric identification system is outlined in Figure 4. The enrollment step proceeds until feature extraction (edge pursuit and distance calculation) is performed, and the obtained reference data is then stored in the database. The algorithm flow of the identification step can be divided into four parts and begins with processing of the first input image for the artifact (binarization and center extraction; Figure 4). The second step involves image processing for the finger (binarization and edge extraction), while the third and fourth steps consist of feature extraction (edge pursuit and

distance calculation) and comparison, respectively. The details of the algorithm are described in the following subsections.

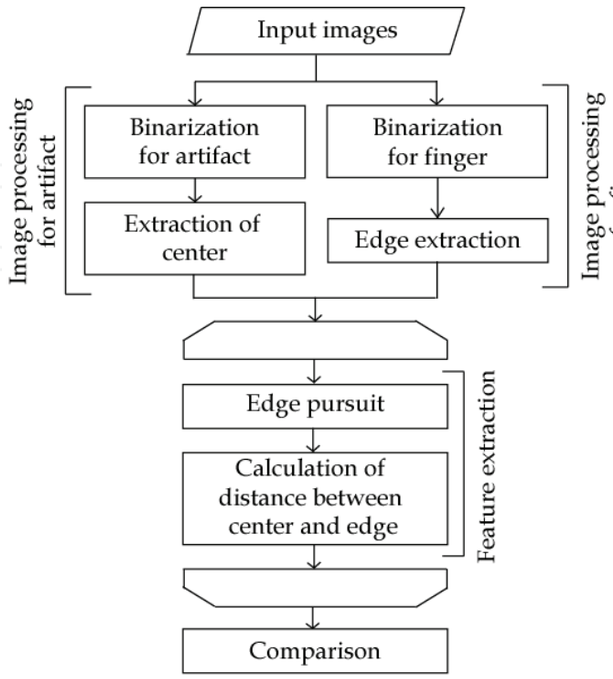
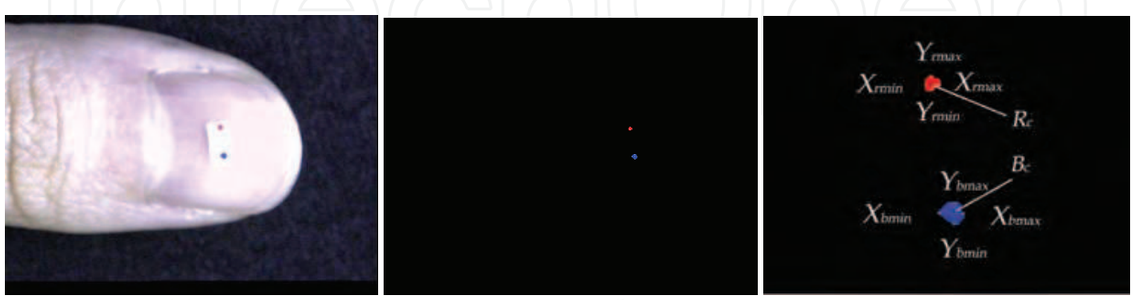


Fig. 4. Flow chart of the algorithm used for the identification step

3.1 Image processing for artifacts

In this step, the center of each dot on the artifact in the input image is determined. First, the input image is binarized by the color of each dot (blue and red), and the area of each dot is extracted (Figure 5(b)). To determine the center of the blue area, horizontal maximum X_{bmax} and minimum X_{bmin} and vertical maximum Y_{bmax} and minimum Y_{bmin} are searched by horizontal and vertical scanning, respectively. The intersection point of line segment $X_{bmax}X_{bmin}$ and $Y_{bmax}Y_{bmin}$ is determined to represent the center of blue point area (B_c). Using the identical process, the center of the red area (R_c) is also detected (Figure 5(c)).



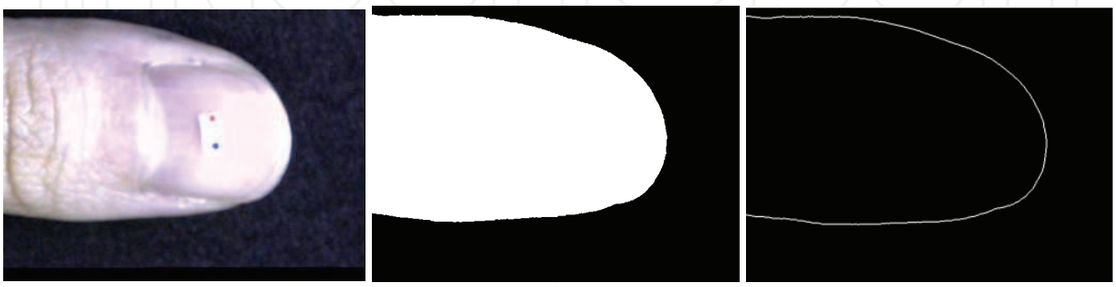
(a) (b) (c)

Fig. 5. Image processing for the artifact, showing a (a) representative input image, (b) extraction of the two colored dots, and (c) detection of the center of each dot area (zoomed image)

In this study, we used colored dots on the artifact and the above algorithm to detect the center of each colored dot. However, as only the position of two points (or a vector) is needed, it is possible to introduce variations to the shape and color of the artifact.

3.2 Image processing for fingers

In the next step of image processing, the finger outline is determined from the input image. The input image is first processed by binarization to separate the background and finger area into a binary image (Figure 6(b)). The finger outline is then obtained by edge extraction using a Laplacian filter (Figure 6(c)).

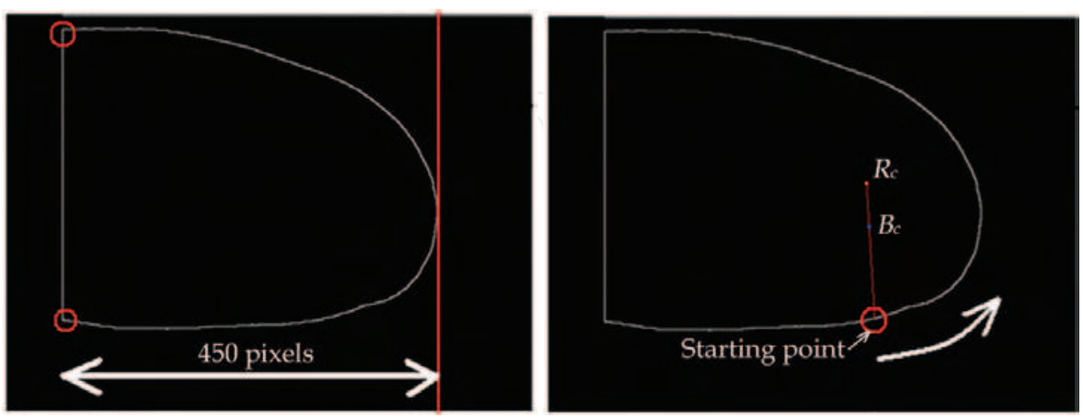


(a) (b) (c)

Fig. 6. Image processing for the finger, showing a (a) representative input image, (b) extraction of the finger area (binary image), and (c) extraction of the finger outline (edge image)

3.3 Feature extraction

As a preprocessing step for feature extraction to equalize the volume of finger outline data, the finger outline is excised at a set distance (450 pixels) from the edge of the fingertip (indicated by a vertical line in Figure 7(a)), and the edges opposite the fingertip (towards the first finger joint) are connected with a line (Figure 7(a)). The fingertip location is decided based on the horizontal maximum point of the finger outline by horizontal scanning.



(a) (b)

Fig. 7. Feature extraction. (a) Extracted outline of the finger and connection of the edges (red circles indicate the edges), (b) Detection of the starting point for pursuing the finger outline based on the points on the artifact

For the feature extraction processing, the finger outline pixels are pursued in an anti-clockwise direction from the starting point until returning to that point (Nishiuchi, 2010), and the distance between pixels on the finger outline and the middle of the two dots (between B_c and R_c) on the artifact is measured continuously. The starting point for pursuing the finger outline is detected based on the intersection between the finger outline and the extended line connecting points R_c and B_c on the artifact (Figure 7(b)).
A representative graph based on the feature extraction processing procedure is presented in Figure 8, where the horizontal and vertical axes represent the position of the pursued pixels and the measured distance, respectively. The data shown in Figure 8 is used for the reference and probe data during identification to determine whether a presented finger and artifact are genuine or an imposter. The red area in Figure 8 corresponds to the line connecting the two edges (red circles in Figure 7(a)) of the outline of the finger. The data within this area is not used during the comparison step.

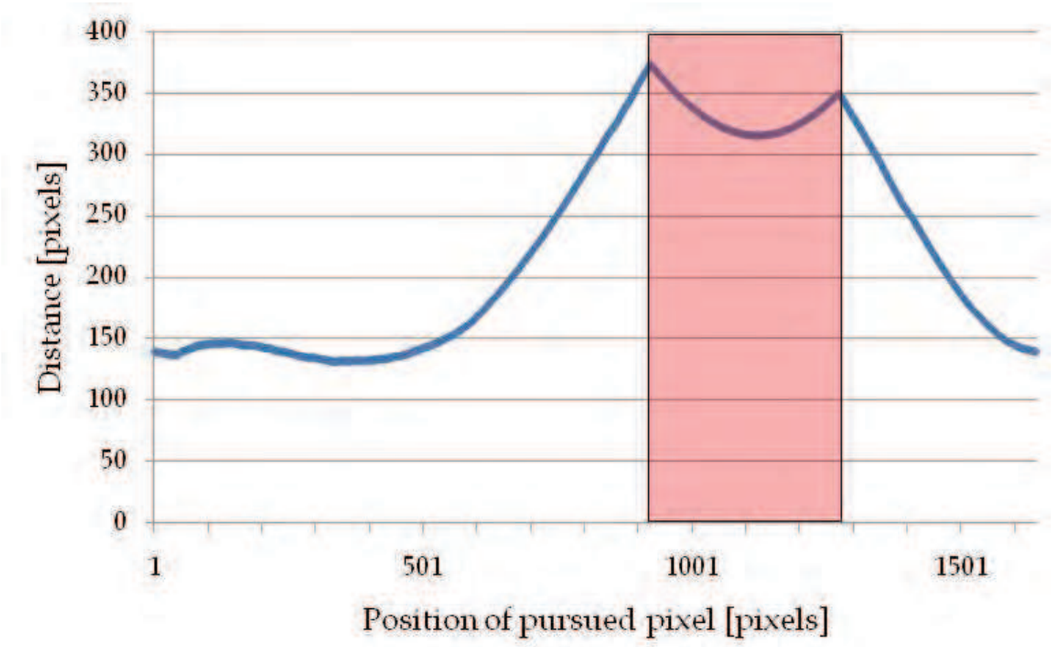


Fig. 8. Distance between the pixels on the outline of finger and the middle of the two dots on the artifact

3.4 Comparison

In the final comparison step, the correlation coefficient (R) is used for the comparison between the reference and probe data. Correlation coefficient R is calculated using Equation (1):

$$R = \frac{\sum_{i=1}^{n}(x_i - x_{aa})(y_i - y_{aa})}{\sqrt{\sum_{i=1}^{n}(x_i - x_{aa})^2}\sqrt{\sum_{i=1}^{n}(y_i - y_{aa})^2}} \quad (1)$$

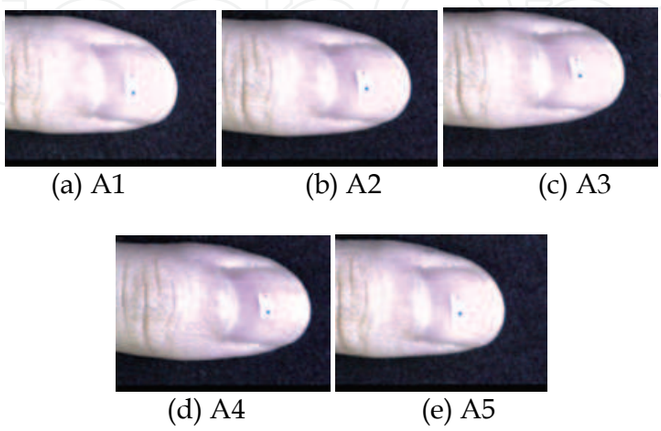
In Equation (1), x_i (i=1, 2, 3, …,n) represents reference data, y_i (i=1, 2, 3, …, n) represents probe data, and x_{aa} and y_{aa} represent the arithmetic average of x_i and y_i, respectively.

4. Experimental evaluation

To evaluate the proposed biometric identification method, the following three experiments were conducted.
EXP. 1 Genuine trial: validation of repeatability
EXP. 2 Imposter trial: validation of anti-spoofing
EXP. 3 Genuine trail- artifact is removed and re-attached: validation of anti-spoofing
The set of EXP. 1 and EXP. 2 was performed as a general evaluation of the proposed biometric identification method to allow comparison with previous biometric systems, and EXP. 3 was conducted as a validation of the anti-spoofing property of our system using a genuine user who had removed and re-attached the artifact. The details and outcomes of each experiment are described in the following subsections.

4.1 Genuine trial: validation of repeatability

To validate the repeatability of the proposed biometric identification method, five images of a finger with an attached artifact were each captured for five subjects (A-E) with the finger resting on the stage of the imaging system. A representative set of captured images for subject A is shown in Figure 9. The reference data (Data A1) was then compared with the probe data (Data A2 to Data A4) of the genuine subject.
The result of the comparison for subject A is shown in Figure 10, where the horizontal and vertical axes represent the position of the pursued pixels and the measured distance, respectively, and the five lines represent each feature extracted from the five images of the genuine finger with the attached artifact. On comparison of the plotted reference and probe data, it is clear that they are quite similar. This determination was confirmed by examining the correlation coefficients resulting from the comparison for all five subjects (Table 1). As the minimum values of the correlation coefficients are all 0.996 or greater, the repeatability for the identification was considered to be high. In addition, the repeatability could be increased by using a guide for fixing the finger in place during the capture of the input image (data not shown).



(a) A1 (b) A2 (c) A3

(d) A4 (e) A5

Fig. 9. Five images of the identical genuine finger of subject A with an attached artifact

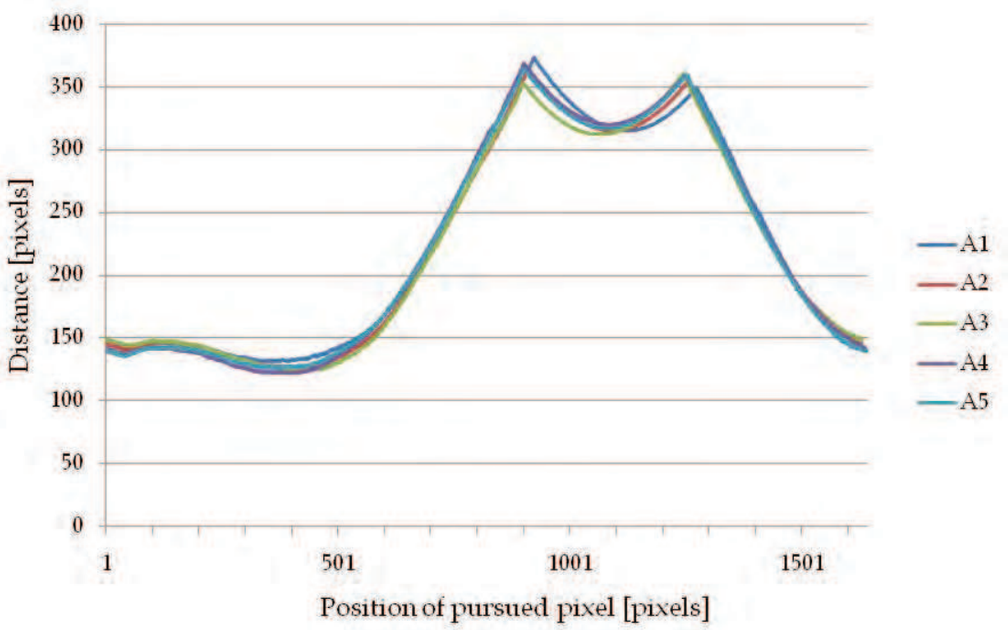


Fig. 10. Distance between the pursued pixels on the outline of finger and the artifact for the genuine trial of subject A

Subject	A	B	C	D	E
Average	0.9972	0.9976	0.9989	0.9993	0.9996
Maximum	0.9984	0.9986	0.9998	0.9996	0.9998
Minimum	0.9962	0.9964	0.9971	0.9991	0.9995

Table 1. Correlation coefficients for the comparison of the reference and probe data obtained during the genuine trial for subject A-E

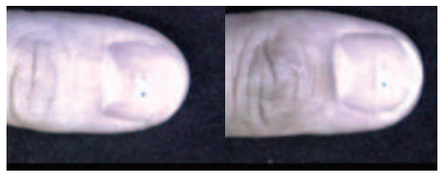
4.2 Imposter trail: validation of anti-spoofing

After validating the repeatability of the proposed method, its resistance to spoofing was next evaluated by capturing five images of fingers with an attached artifact from five subjects (A-E) (Figure 11). The reference data (Data A) was then compared with the probe data (Data B to E) of the four imposter subjects. As an added element to evaluate the spoofing resistance, the imposter subjects (B-E) attempted to mimic the position and angle of the artifact of the genuine user (A) by referring to an image of the genuine user's finger with the attached artifact.

The result of the comparison between the data of the imposters and genuine user is shown in Figure 12, where the horizontal and vertical axes represent the position of the pursued pixels and the measured distance, respectively, and the five lines represent the features of each subject (A-E). It can be seen that lines of subjects D and E are quite similar to subject A. Table 2 lists the correlation coefficients resulting from the comparison between genuine user A with each of the imposters. As can be seen in Table 2, the correlation coefficients of A-D

and A-E tended to be high. However, for the genuine trial, the correlation coefficient values were 0.996 or higher, whereas the imposter trial resulted in values ranging from 0.680 to 0.983. In addition, the distributions from the genuine and imposter trials did not interfere. When the threshold value for identification was set at 0.995, both the false rejection rate (FRR) and false acceptance rate (FAR) were 0%. Even though the imposter subjects attempted to mimic the artifact position of the genuine user, it was difficult to set the artifact at the identical position and angle as that of the genuine user, demonstrating the resistance of our proposed system to spoofing.

(a) A (b) B (c) C



(d) D (e) E

Fig. 11. Images of fingers with attached artifacts for five subjects (A, genuine user; B-E, imposter subjects)

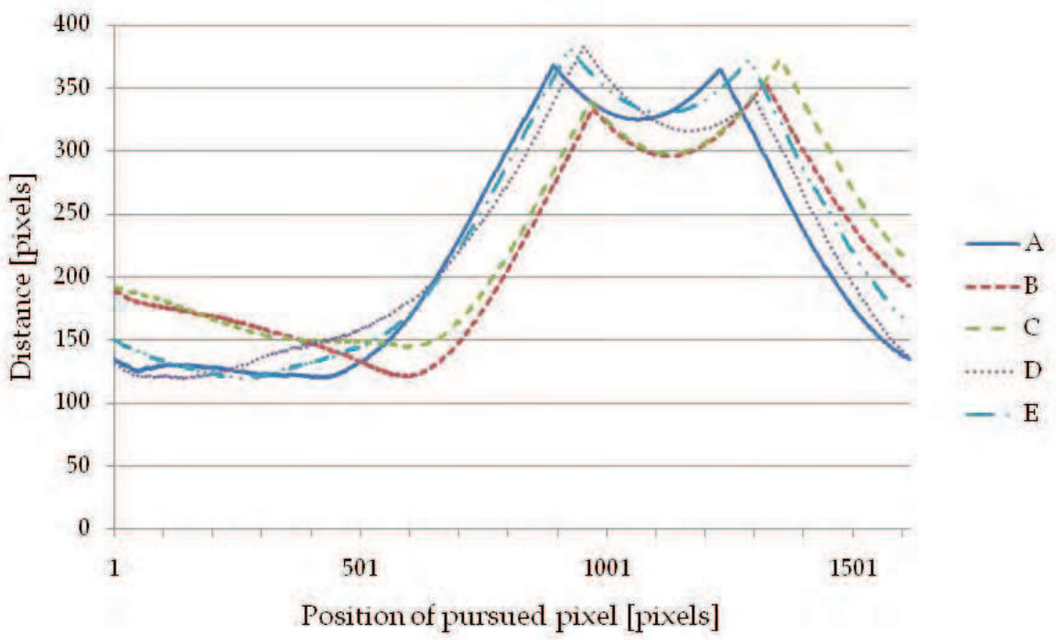


Fig. 12. Distance between the pixels on the outline of the finger and the artifact for the five subjects of the imposter trial

A-B	A-C	A-D	A-E
0.6844	0.7313	0.9705	0.9826

Table 2. Correlation coefficients for the comparison of the reference (A) and probe data (B-E) obtained for the imposter trial

4.3 Genuine trial: artifact is removed and re-attached

In this experiment, we validated the ability of the proposed biometric identification system to reject a genuine user who had removed and re-attached the artifact. Two captured images of the identical finger of subject A with an attached artifact that was removed once and attached again in a random position are shown in Figure 13. The reference data (Data A) was then compared the probe data (Data A′; re-attached artifact) of subject A.

(a) A (b) A′

Fig. 13. Images of a genuine finger with an attached artifact (left) that was removed once and re-attached in a random position (right)

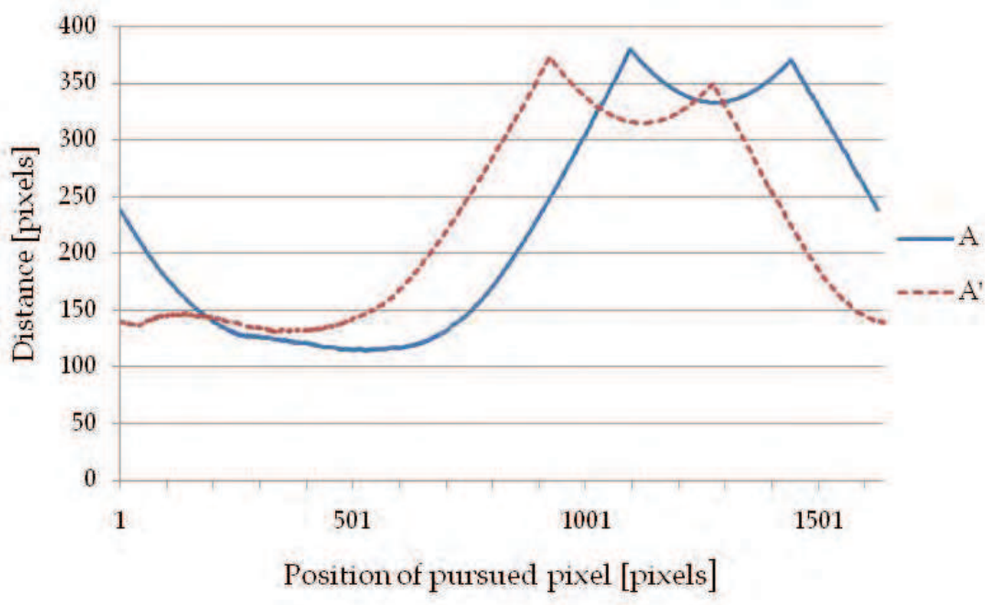


Fig. 14. Distance between the pixels on the finger outline and the reference artifact (A) and the artifact that was removed once and re-attached randomly (A′)

The result of the comparison between Data A and A′ is shown in Figure 14. From the plotted data, it is clear that the two lines are markedly different with respect to the shift on the horizontal axis, which was also reflected in the low correlation coefficient between Data A and A′ of 0.660. Thus, even if the genuine user attempts to access the system after removal of the artifact, re-enrollment is necessary. In Section 4.2, the finger shapes of a few imposters were quite similar to the genuine user. However, even when an imposter attempted to spoof using the genuine finger outline and an imitation finger, spoofing is prevented by the randomness of the position and angle of the artifact. In Section 5.1, we confirmed the security level of the proposed biometric identification method depending on the randomness of the position and angle of the artifact.

5. Validation of security level

To validate the security level of the proposed biometric identification method, the following two simulations were conducted.
SIM. 1: Security level depending on the position and angle of the artifact
SIM. 2: Security level depending on the amount of biological data
The level of security, as verified by each simulation, is an important factor for demonstrating the practical use of the proposed system. The details of each simulation are described in the following two subsections.

5.1 Security level depending on the artifact position and angle

In this simulation, we verified the allowable range of the position and angle of the artifact for identification when the artifact is removed and re-attached. Specifically, we attempted to determine the degree of change in the artifact position or angle that prevents the imposter from being verified by the system, as determined by the correlation coefficient. The position and angle of the artifact of Figure 5(a) were changed in the simulation program based on the following two conditions:
Condition 1: The artifact is moved in the direction of x (horizontal direction) and the direction of y (vertical direction) by one pixel (approximately 0.05 mm).
Condition 2: The artifact is rotated by one degree.
The results of the simulation under conditions 1 and 2 are shown in Figures 15 and 16, respectively. If the threshold value for identification is set at 0.995 based on the results presented in Section 4.2, and the artifact is moved 11 pixels (0.55 mm) or more in the x direction, or 10 pixels (0.50 mm) or more in the y direction, the correlation coefficient falls below the threshold level and the genuine user is not accepted into the system (Figure 15). If the acceptable range for placement of the artifact on the fingernail is assumed to be 5.0 × 5.0 mm, the randomness of the artifact position is calculated as follows:

$5.0 / 0.55 \times 5.0 / 0.50 = 90$ patterns

If the threshold value is set at 0.995 and the artifact is rotated 5.0 degrees or more, the genuine user is not accepted into the system (Figure 16). Under this condition, the randomness of the angle of the artifact is calculated as follows:

$360 / 5 = 72$ patterns

Considering the combination between the position and angle of the artifact, and assuming that the position and angle are independent parameters, the randomness of the method is calculated as follows:

90 × 72 = 6480 patterns

The relative scale of the range of positions (0.55 × 0.50 mm) and angles (5.0 degrees) with respect to the finger outline are shown in Figure 17. From these simulations, it was clearly demonstrated that the randomness of the artifact is quite high. Therefore, if someone attempted to mimic the position and angle of the genuine artifact, the inherent randomess of the proposed identification system would effectively prevent such spoofing attempts.

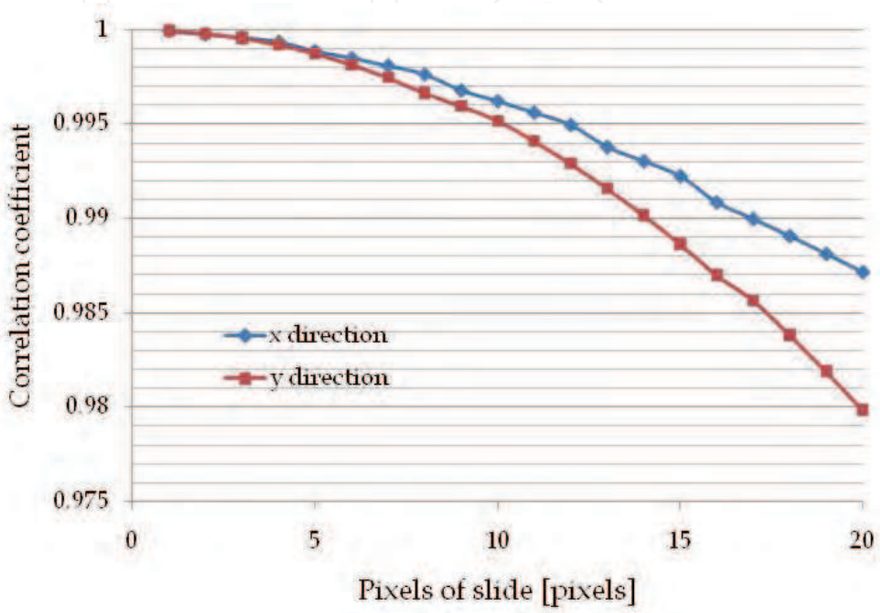


Fig. 15. Effect on the correlation coefficient by moving the artifact in the *x* (blue line) or *y* (red line) direction

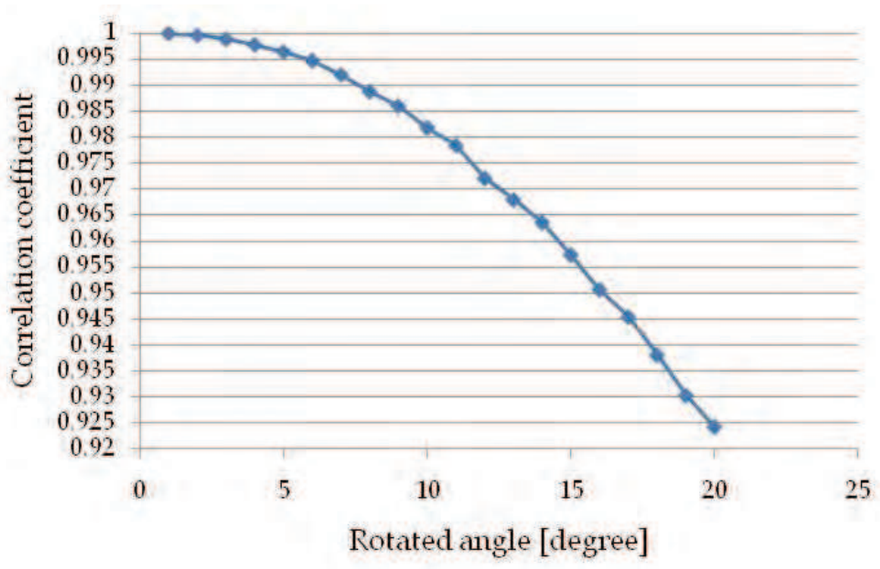
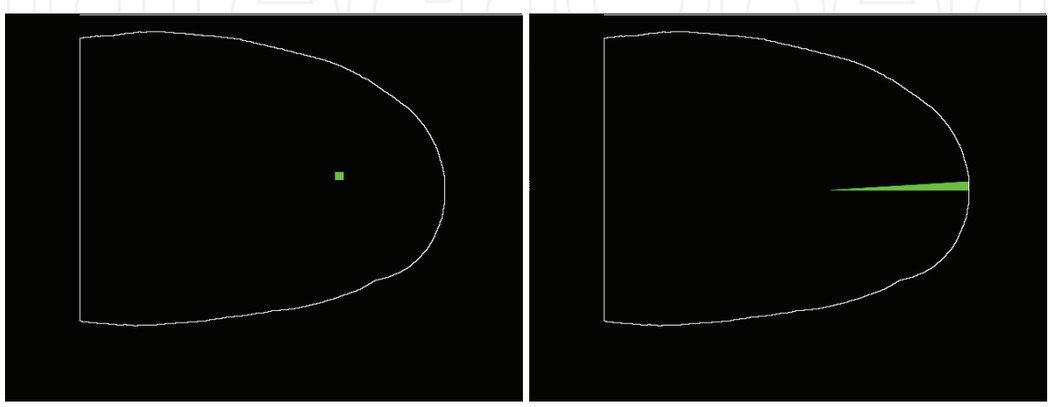


Fig. 16. Effect of rotating the artifact position on the correlation coefficient

Notably, this estimation is based on the placement range of 5.0 × 5.0 mm for the artifact; however, the acceptable range for placement of the artifact on the fingernail is thought to be even wider.

From the viewpoint of fingernail growth, which relates to Problem 1 described in the Introduction, the proposed method possesses the advantage of cancelable identification. It is estimated that the fingernails of adults grow approximately 0.1 mm per day. Thus, based on the simulation results and the constant growth rate of fingernails, a genuine user would need to re-enroll in the system within six days.



(a) (b)

Fig. 17. Relative scale of the allowed range for identification with respect to the finger outline; (a) positional range (0.55 × 0.50 mm) and (b) angular range (5.0 degrees)

5.2 Security level depending on the amount of biological data

In a second simulation, we verified the relationship between the amount of biological data (finger outline data) and the security level of the proposed biometric identification system. The amount of finger outline data corresponds to the number of pursuit pixels counted from the starting point during the image processing step. All finger outline data shown in Figure 8, with the exception of the red area, were used for the comparison in the experiments in Section 4. Although the uniqueness of the finger outline is relatively low, it represents biological data, similar to that provided by fingerprints, veins, or the iris. Therefore, depending on the situation, it is conceivable that users may hesitate to enroll finger outline data in the identification system, which relates to Problem 2 described in the Introduction. Thus, we have proposed identification using biological data that is not specific to the user, but is specific only with respect the artifact position. In the second simulation, the amount of required biological data was examined by decreasing the amount of finger outline data that allowed distinguishing between the genuine user and an imposter.

All data of subject A and the imposters (B-E) were used for the simulation. Figure 18 is a graphical result of the simulation, where the vertical axis represents the correlation coefficient and the horizontal axis represents the decrease ratio of finger outline data. When the decrease ratio in the horizontal axis in Figure 18 is replaced with the number of data (the distance in pixels between the artifact and finger outline), 100% corresponds to 1283 and 0.26% corresponds to 4. From the simulation results, even if the decrease ratio is decreased by as much as 0.56% (the number of data is 8), the genuine user can be distinguished from imposters. Based on this simulation experiment, it is clear that the collected biological data

cannot be used to identify the user, but can be used to specify the position of the artifact and identify the genuine user. Moreover, the meaningfulness of the collected data can be canceled by simply removing the artifact. Thus, for identification using the proposed method, the users are not required to enroll their highly unique biological data, which is unavoidable using current biometric systems.

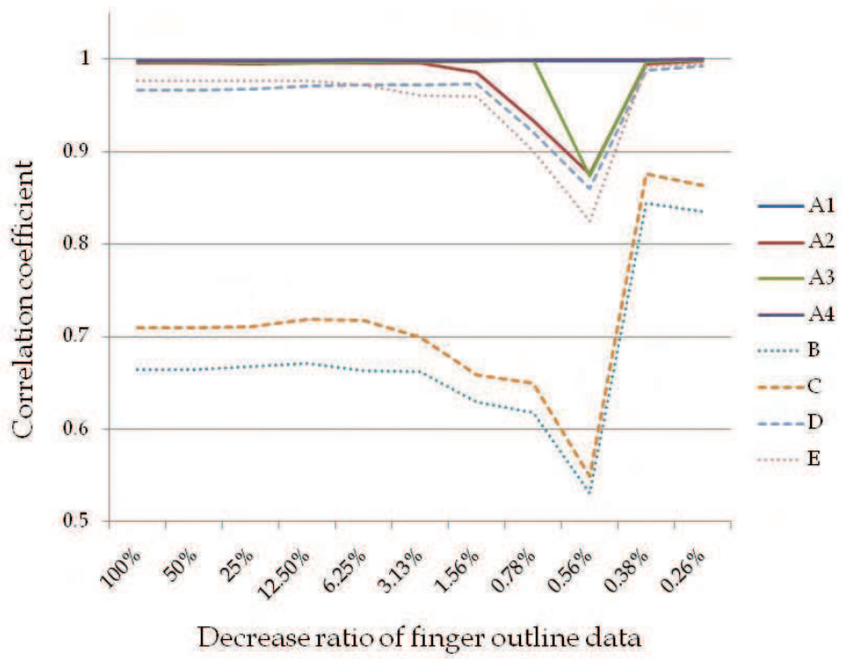


Fig. 18. Effects of decreasing the amount of finger outline data used in the identification on the correlation coefficient

6. Summary and proposed application system

6.1 Summary

The proposed cancelable biometric identification system has a number of advantages over current systems. The features of the proposed method are summarized as follows:

1. Cancelable biometric identification: Registered information can be canceled by simply removing the artifact. Even if the genuine user attempts to access the system, once the artifact is removed, re-enrollment is necessary (refer to Section 4.3). Moreover, due to the constant growth of fingernails, identification is not possible after a certain period of time (approximately one week).
2. Controllable security level: The security level of the system can be adjusted by controlling the amount of permissible biological and artifactual data.
   I. Artifacts:
      I-a. Using sufficient information to allow identification of the artifact (random pattern, code, or artifact-metrics proposed by Matumoto et al. (2000): the secondary biological data is artificially appended to the fingernail).
      I-b. Using only information that allows the position and direction of the artifact to be detected (a few dots).

II. Biological data:
   II-a. Using all information that allows identification of the user (all data shown in Figure 8, except the red area).
   II-b. Using only information that allows the position and direction of the artifact to be detected. In other words, the user cannot be identified only by biological data (refer to Section 5.2).

When (I-a) and (II-a) are combined, three identifications are performed. The first is the identification of the biological data, the second is identification of the artifact, and the third is the relation between the biological data and the artifact. Yamagishi et al. (2008) described this method using fingerprints and a random pattern as an artifact. When (I-b) and (II-b) are combined, only the third identification is conducted.

3. Non-necessity for the registration of unique biological information: Although the outline of the finger constitutes biological data, the information it provides in itself is not sufficient for individual identification. Moreover, when the amount of biological data collected for identification is decreased, it is impossible to identify an individual (refer to Section 5.2). Therefore, the enrollment of biological data that can uniquely identify the user is unnecessary in this proposed biometric verification system.
4. Strength against spoofing: If the biological data and artifact are stolen, spoofing can be prevented due to difficulty of reproducing the biological data in relation to the artifact that is required for identification (refer to Sections 4.1, 4.2, 4.3, and 5.1).

6.2 Proposed application of the system

The conditions for the application of the proposed method are as follows: (a) only a limited number of enrollments can be accommodated by the system, and (b) the use period is approximately five days. The flow of use of the proposed system at a hotel is illustrated in Figure 19. At the time of check-in, the user attaches the artifact to the fingernail and enrolls

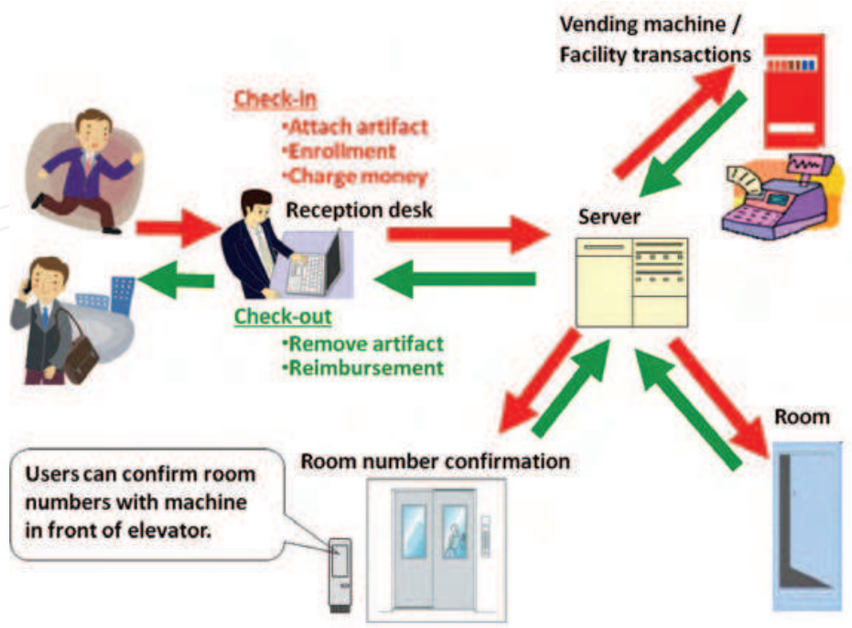


Fig. 19. Potential applications of the proposed system in a hotel setting

the artifact and biological data with the system. After the enrollment, the user can enter and exit his/her room without possession of a room key. Moreover, the possession of a wallet or purse becomes unnecessary while the user is within the hotel facilities, thus improving safety and convenience. For practical use, a transparent sticker containing the two dots marked with a dye that can only be detected using specific lighting (Takayanagi, 2009) would serve as the artifact (Figure 20).

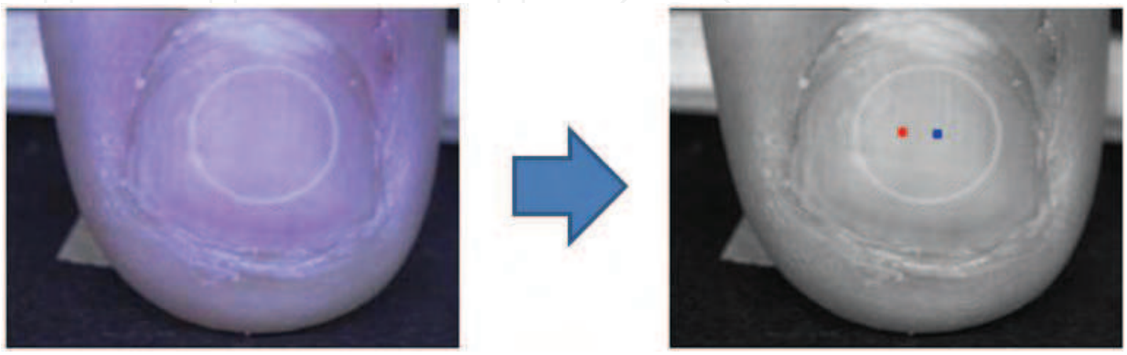


Fig. 20. Image of a fingernail with a transparent artifact (left: appearance under natural light, right: appearance under specific lighting)

Under these conditions, the proposed biometric identification system would also be suitable for use as a one-day pass for office and factory buildings, and amusement and medical facilities, among numerous other potential applications.

7. Conclusions

We have described a novel method of cancelable biometric identification that combines biological data with the use of an artifact. The algorithm of the identification step can be divided into four parts: processing of the input image for the artifact; image processing for the finger; feature extraction, which involved determining the distance between the artifact and finger outline; and comparison of the reference and probe data. Based on the results of the three evaluative experiments and two simulations described here, several strengths of the proposed method can be recognized. First, the proposed method is a type of cancelable biometric identification, as registered information can be canceled by simply removing the artifact. Second, the proposed method allows control of the security level by adjusting the amount of biological and artifactual data. Third, the registration of unique biological information is not necessary for the identification system. Finally, the proposed method is resistant to spoofing.

Despite these apparent strengths, a few limitations of the proposed method warrant mention. First, the application of the proposed method is limited by two conditions: (a) only a limited number of enrollments can be accommodated by the system, and (b) the use period is approximately five days. Although the potential field of applications is limited by these two conditions, the proposed method is characterized by user friendliness and relative simplicity that do not exist in current identification methods. Second, the usability of the identification system should be improved. Specifically, it is necessary to develop a material for use as the artifact that remains firmly in place and a mechanism that permits the user to easily detach the artifact on exiting the system.

8. Acknowledgments

The authors would like to thank Mr. Toshihito Sioya To and Mr. Ryota Tsurumiat at Toppan Technical Design Center Co., Ltd. for their constructive support. This study was partially supported by the Research Fund of A-STEP (FS) in the Heisei 22 fiscal year, and is the identification system presented in this chapter is patent pending (Japan Patent No. 2011-003885).

9. References

Ashbourn, J. (2000). Biometrics: Advanced Identity Verification, The Complete Guide, Springer-Verlag.

Gunn, L. (2010). VIEWPOINT: Would you use a biometric solution to authorise a transaction at an ATM?, European ATM Security Team (EAST), https://www.european-atm-security.eu/Welcome%20to%20EAST/&action=fullnews&id=62. Accessed in April 2011.

Hirabayashi, M., Tanabe, T., and Matsumoto, T. (2004). Can We Make Artificial Fingers That Fool Fingerprint Systems? (Part VI), Technical Report of Institute of Electronics, Information, and Communication Engineers, ISEC2003-139, pp. 151-154.

Jain, A. K.; Ross, A. and Prabhakar, S. (2004a).An Introduction to Biometric Recognition, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp. 4-20.

Jain, A. K., Pankanti, S., Prabhakar, S., Hong, L., Ross, A., and Wayman, J. L. (2004b). Biometrics: A Grand Challenge, Proceedings of International Conference on Pattern Recognition, pp. 935 – 942.

Matsumoto, H., Matsumoto, T. (2000). Artifact-metric Systems, Technical Report of the Institute of Electronics, Information and Communication Engineers, ISEC2000-59, pp. 7-14.

Matsumoto, T. (2006). Biometric Authentication Systems: Vulnerability of Biometric Authentication - On the Issue of Physiological Spoofing –, IPSJ (Information Processing Society of Japan) Magazine, Vol. 47, No. 6, pp. 589-594.

Nishiuchi, N., Komatsu, S., Yamanaka, K. (2010). Biometric verification using the motion of fingers: a combination of physical and behavioural biometrics, International Journal of Biometrics, Vol. 2, No. 3, pp. 222-235 .

Prabhakar, S., Pankanti, S., Jain, A. K. (2003). Biometric Recognition: Security & Privacy Concerns", IEEE Security and Privacy Magazine, Vol. 1, No. 2, pp. 33-42.

Rotter, P., Daskala, B., Compañó, R. (2008). RFID implants: opportunities and challenges for identifying people. IEEE Technology and Society Magazine, Vol. 27, Issue 2, pp. 24–32.

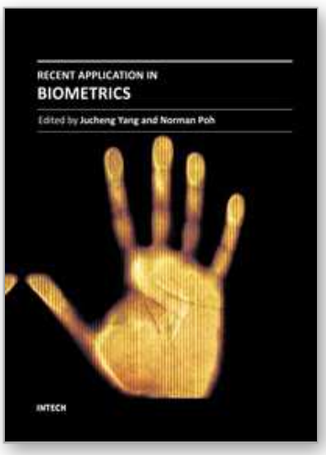
Stén, A., Kaseva, A., Virtanen, T. (2003). Fooling Fingerprint Scanners - Biometric Vulnerabilities of the Precise Biometrics 100 SC Scanner, Proceedings of 4th Australian Information Warfare and IT Security Conference 2003, pp. 333-340.

Takayanagi, Y., Kamijo, K., Katto, J. (2009). Invisible Barcode Extraction using Color Channel Estimation, Technical report of IEICE. Multimedia and virtual environment 109(149), pp. 31-36.

Wayman, J. (2000). National Biometric Test Center Collected Works 1997-2000, pp. 1–3.

Yamada, K., Matsumoto, H., and Matsumoto, T. (2000). Can We Make Artificial Fingers That Fool Fingerprint Systems?, Technical Report of Institute of Electronics, Information, and Communication Engineers, ISEC2000-45, pp. 159-166.

Yamagishi, M., Nishiuchi, N., Yamanaka, K. (2008). Hybrid Fingerprint Authentication Using Artifact-Metrics, International Journal of Biometrics, Vol. 1, No. 2, pp. 160-172.



Recent Application in Biometrics

Edited by Dr. Jucheng Yang

ISBN 978-953-307-488-7
Hard cover, 302 pages
Publisher InTech
Published online 27, July, 2011
Published in print edition July, 2011

In the recent years, a number of recognition and authentication systems based on biometric measurements have been proposed. Algorithms and sensors have been developed to acquire and process many different biometric traits. Moreover, the biometric technology is being used in novel ways, with potential commercial and practical implications to our daily activities. The key objective of the book is to provide a collection of comprehensive references on some recent theoretical development as well as novel applications in biometrics. The topics covered in this book reflect well both aspects of development. They include biometric sample quality, privacy preserving and cancellable biometrics, contactless biometrics, novel and unconventional biometrics, and the technical challenges in implementing the technology in portable devices. The book consists of 15 chapters. It is divided into four sections, namely, biometric applications on mobile platforms, cancelable biometrics, biometric encryption, and other applications. The book was reviewed by editors Dr. Jucheng Yang and Dr. Norman Poh. We deeply appreciate the efforts of our guest editors: Dr. Girija Chetty, Dr. Loris Nanni, Dr. Jianjiang Feng, Dr. Dongsun Park and Dr. Sook Yoon, as well as a number of anonymous reviewers.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen