A Smartphone User Verification Method Based on Finger-Writing of a Simple Symbol

Atsushi Takahashi[1], Yohei Masegi[1], and Isao Nakanishi[1][0000−0001−9533−9987]

Tottori University, Tottori 680-8552, Japan
nakanishi@tottori-u.ac.jp

Abstract. Writer verification based on finger-writing of a simple symbol on a touch screen is proposed herein. The users write a simple and well-known symbol, for example, a circle, triangle, or square. In addition, the users write the symbol using their finger instead of a pen on a tablet. This allows more convenience with the use of the proposed method. However, it was observed that the original approach and obtained verification performance were not reliable. In this work, we create a new database using thirty participants. By examining individual features extracted from the database, the risk of misjudgment is found. In order to solve this problem, a coordinate transformation method is introduced. Moreover, normalization is examined for fusing individual features by comparing three normalization methods. The proposed method with appropriate coordinate transformation and normalization achieves an equal error rate of 10.6% even when all participants write only a simple circle.

Keywords: Writer verification · Simple symbol · Finger writing · Coordinate transformation · Normalization.

1 Introduction

With the progress of recent technologies, cellular phones have been replaced by smartphones. We can interact with anyone using smartphones, anytime, anywhere. Smartphones have become indispensable in our daily lives. On the other hand, the risk of leakage of personal information is increasing.

For person authentication, passwords, PIN codes, or patterns [1–3] have been used in smartphones. However, these require users to remember them. Therefore, there is a risk of forgetting them or mistaking them when entering them into an authentication system. These are inconvenience for users. Also, there is a risk of their being known by others. This makes it possible to spoof an authentication system.

Biometrics authentication has attracted attention since users never forget biometric data and never mistake to present them to an authentication system. As such modalities of biometrics, face-images, iris-images, and fingerprints are generally used and categorized as static biometrics, of which information can be extracted stable, and it results in higher authentication performance. However, these modalities always appear on the body surface. Therefore, it is easy to steal

their data (images) by others using a digital camera and to perform a spoofing attack using a counterfeit produced by the stolen data.

On the other hand, there are dynamic biometrics such as signatures, voiceprints, and gaits (walking motions). In particular, we focus on the signature, which verifies users by the writing of users' signatures [4–6] and has been used for authentication in personal digital assistant (PDA) systems [7–11], which equips a stylus pen and a tablet display. However, using the dedicated pen when signing is inconvenient for users. In recent years, it becomes general to write (touch) directly by a finger on a touchscreen instead of using the stylus pen [12–23]. However, to write a signature with a finger on a small touchscreen of a smartphone is very inconvenient for users. In addition, writing a signature requires users to spend a long time and it is also inconvenient for users. As a result, the signature is no longer used as an authentication method in smartphones.

Writer verification is to verify whether genuine users or not by the act of writing [24]. We have proposed a novel user (writer) verification method, where users write a symbol that is simple, well-known, and never forgotten and mistaken, for example, a circle, a cross, a triangle, or a square [25]. To write a simple symbol makes usability the highest. On the other hand, the descriptive content of the proposed method is well known to everyone and simple, so that to adopt some verification method based on pattern matching makes it very easy to imitate what users write. The security level may become low. However, if verification using extracted "habits" as individual features from written data and/or writing process is applied to the proposed method, a certain level of security is guaranteed. In other words, individual features independent of descriptive contents should be extracted in the proposed method. However, this original approach and obtained verification performance were not reliable since there were only 19 participants and extraction of individual features and fusion of these features were not fully discussed.

2 User verification based on finger-writing of a simple symbol

In this study, we assume user verification, where an applicant who wants to use a smartphone specifies one of the enrolled users. He/she writes a simple symbol, writing data are verified and judged whether he/she is genuine compared with the template relevant to the specified user. The verification is achieved based on Euclidian distance matching. The obtained distance is compared with a threshold that is determined in advance of verification; then, if the distance is smaller than the threshold, the applicant is regarded as a genuine user. If the distance is larger than the threshold, the applicant is regarded as ingenuine/imposter user. The threshold is empirically determined.

2.1 Finger-Writing Database

First, we constructed a new database using 30 participants to obtain more reliable results for performance evaluation. Simple symbols were a circle, triangle,

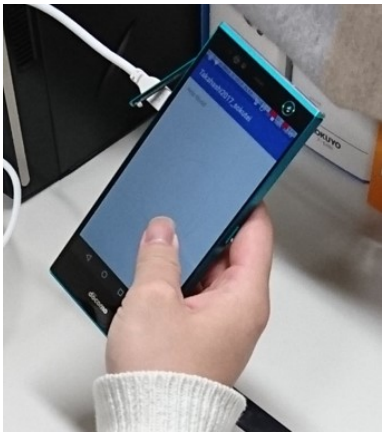

Fig. 1. A style for finger-writing.

and square. The smartphone used in this work was Arrows NX F-04G produced by Fujitsu Limited, Japan. Its specifications are summarized in Table 1. As the

Table 1. Specifications of the used smartphone.

OS	Android 5.0
CPU	MSM8994 2.0GHz
RAM	3 GB
ROM	32 GB
Display	5.2-inch IPS (1440 × 2560)
Size	146 × 70 × 8.8 mm
Weight	155 g

developing environment, Android Studio was used.

All participants were sitting a chair and wrote a symbol freely: some participants held a smartphone in their dominant hand and wrote a symbol with a thumb of the same hand, and some participants held the smartphone in their nondominant hand and wrote a symbol with an index finger of their dominant hand. A style for finger-writing a simple symbol is presented in Fig. 1. All participants wrote each symbol twenty times. As a result, there are 1800 data (30 participants ×3 symbols×20 times) in a database.

2.2 Individual Features

We selected 40 individual features which are considered being independent of descriptive contents as follows, **SP**: coordinate values at the starting point, **EP**:

coordinate values at the ending point, **MinX**: the minimum value in x coordinate, **MinY**: the minimum value in y coordinate, **MaxX**: the maximum value in x coordinate, **MaxY**: the maximum value in y coordinate, **MinP**: coordinate values (x and y) in the minimum pressure, **MaxP**: coordinate values in the maximum pressure, **MinT**: coordinate values in the minimum touching-area, **MaxT**: coordinate values in the maximum touching-area, **MinS**: coordinate values in the minimum speed, **MaxS**: coordinate values in the maximum speed, **MinA**: coordinate values in the minimum acceleration, **MaxA**: coordinate values in the maximum acceleration. **DX**: distance between the maximum and the minimum x, **DY**: distance between the maximum and the minimum y, **MC**: the means of coordinate values, **DSE**: distance between the starting and the end points, **WA**: writing area, **WT**: writing time, **MP**: the mean of pressure, **Pmin**: the minimum of pressure, **Pmax**: the maximum of pressure, **MT**: the mean of touching-area, **Tmin**: the minimum of touching-area, **Tmax**: the maximum of touching-area, **MS**: the mean of speed, **Smin**: the minimum of speed, **Smax**: the maximum of speed, **MA**: the mean of acceleration, **Amin**: the minimum of acceleration, **Amax**: the maximum of acceleration, **PS**: pressure at the starting point, **TS**: touching-area at the starting point, **SS**: speed at the starting point, **AS**: acceleration at the starting point, **PE**: pressure at the end point, **TE**: touching-area at the end point, **SE**: speed at the end point, and **AE**: acceleration at the end point. When using the coordinate values x and y, each individual feature has two dimensions (elements).

2.3 Coordinate Transformation and Normalization

Through the analysis of the features obtained from the database, we found a risk of mis-verification. For example, as illustrated in Fig. 2 (a), an extreme example could be assumed, where two symbols written by different participants A and B coincidentally have the maximum finger-pressure at the same point. In this case, these two participants cannot be discriminated using only the maximum finger-pressure point.

This mis-verification is caused by different writing areas. Thus, by adjusting the different areas, as illustrated in Fig. 2 (b), this problem could be addressed.

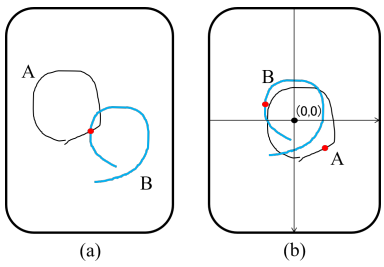

Fig. 2. Two circle symbols written by two participants.

This adjustment is achieved by extracting the centroids of the two symbols and then matching their coordinates. This process is called coordinate transformation 1 (CT1) hereafter. In addition to such an origin relocation, it is possible to transform the cartesian coordinates to polar equivalents. In the polar coordinates, each sampled point is expressed by a vector, that is, length and angle, and not the x and y coordinate values. This is called coordinate transformation 2 (CT2).

We had confirmed which coordinate transformation including not using transformation was suitable for each feature in advance. As a result, the CT2 was found to be effective for most of the features. However, the most suitable representation of coordinate values depended on the features. Therefore, suitable coordinate representation for each feature should be selected in verification.

In order to achieve higher verification performance, it is better to use individual features in combination than to use them alone. However, when fusing individual features, the normalization of their values is needed since their range of fluctuation is different from each other. Without the normalization, the influence of features with a small fluctuation range on verification could be ignored by that of features with a large fluctuation range. Thus, we had examined well-known three normalization methods, the min-max method, the MAD method, and the Z-score method [26] in advance and confirmed that the min-max and Z-score methods were superior to the MAD method.

2.4 Verification Performance When Fusing Features

Finally, we evaluated the verification performance when fusing the obtained features. However, there are 40 features, so that the number of their combinations results in a large set. Thus, we investigated in the following 10 cases, **All**: all features (number of features was 40), **Off**: off-line features (11), **On**: on-line features (29), **Start**: features of coordinate data, pressure, touching-area, speed, acceleration at the starting point during the writing, **End**: features of coordinate data, pressure, touching-area, speed, acceleration at the endpoint during the writing, **Area**: the mean, minimum, and maximum values and the minimum and maximum coordinate data for touching-area features, **Pres.**: the mean, minimum, and maximum values and the minimum and maximum coordinate data for pressure features, **Speed**: the mean, minimum, and maximum values and the minimum and maximum coordinate data for speed features, **Accel.**: the mean, minimum, and maximum values and the minimum and maximum coordinate data for acceleration features, and **Good**: features that achieved good performance, i.e., those whose EERs are less than the mean value of EERs for all features; therefore, the number of features depends on the symbols and normalization methods[1].

[1] For instance, 25 features, SP(CT2), EP(CT2), MinX(CT1), MinY(CT0), MaxX(CT0), MaxY(CT2), MinS(CT2), MinP(CT2), MaxP(CT2), MinT(CT2), MaxT(CT2), MinA(CT2), DX, DY, MC, WA, WT, Pmax, MT, Tmax, MS, MA, PE, SE, and AE when using the min-max method and writing ◯, where CT0 indicates the case using the original coordinate.

The number of data for making a template was 10; therefore, 10 data from 20 data of each participant were used for making a template and the remained 10 data were used in verification. Assuming the spoofing, other participants' 29×10 data were used as forged symbols for each participant.

A false rejection rate (FRR) corresponds to the ratio of the number of symbols that are written by genuine participants but mistakenly decided as being not genuine to the number of symbols that are written by genuine participants. A false acceptance rate (FAR) is the ratio of the number of symbols that are written by other participants but mistakenly decided as being genuine to the number of symbols that are written by other participants. Error rate curves, namely the FAR and the FRR, were plotted by changing the threshold, which is a security level. In general, these FAR and FRR curves have a trade-off characteristic, and when these curves have a crossing point, it corresponds to the equal error rate (EER). The verification performance was evaluated using the EER, and smaller EER implies better performance.

The number of cross-validations was set as 10. In each cross-validation, 10 data for generating a template from 20 data are changed, and EERs obtained from the 10 cross-validations were averaged.

The results for the three symbols are shown in Table 2. The cases where the EERs were the smallest in three normalization method are colored in red. The columns with EER difference from the smallest one of over than 1% are colored in blue and the columns with EER difference of less than 1% are not colored. The best verification performance of EER = 10.6% was obtained when fusing "Good" features using the min-max method with the circle symbol.

Table 2. EERs (%) when fusing features in three symbols.

(a) Circle

Features	Min-max	Z-score
ALL	11.0	11.9
Off	14.2	13.9
On	13.0	12.7
Start	20.0	18.1
End	15.7	14.2
Pres.	18.0	17.9
Area	17.2	17.7
Speed	16.7	16.3
Accel.	18.5	18.4
Good	10.6	11.0

(b) Triangle

Features	Min-max	Z-score
ALL	14.9	16.8
Off	17.5	16.3
On	16.7	18.1
Start	22.1	18.5
End	19.0	16.1
Pres.	18.9	18.2
Area	18.8	19.0
Speed	23.6	22.6
Accel.	26.1	25.2
Good	12.3	12.4

(c) Square

Features	Min-max	Z-score
ALL	12.8	14.7
Off	16.7	17.3
On	15.0	16.0
Start	20.0	17.6
End	16.4	14.4
Pres.	15.4	15.7
Area	17.2	17.9
Speed	21.5	22.2
Accel.	25.1	25.1
Good	11.4	11.5

3 Conclusions

To develop the writer verification system based on the finger-writing of a simple symbol on a touchscreen, we created a finger-writing database using 30 partic-

ipants and examined the effectiveness of coordinate transformation for extracting individual features and normalization for fusing the features. As a result, the best performance of EER = 10.6% was obtained using suitable coordinate transformation and normalization, even when all the 30 participants only wrote a simple circle symbol on a touchscreen. This shows the feasibility of the proposed method.

In this work, we used a simple verification method of Euclidian distance matching. For further works, we are planning to introduce a learning-based verification method such as support vector machines. Furthermore, the information of finger-orientation on a touchscreen which was used in Ref. [14] may be applicable as an individual feature in the proposed method. We are now trying to extract such a finger-orientation feature from a smartphone. Another challenge is to further increase the number of participants for improving the reliability of the results obtained in this paper.

References

1. R. Schlöglhofer and J. Sametinger, "Secure and Usable Authentication on Mobile Devices," Proc. of the 10th International Conference on Advances in Mobile Computing & Multimedia, 2012.
2. M. Rogowski, K. Saeed, M. Rybnik, M. Tabedzki, and M. Adamski, "User Authentication for Mobile Devices," Proc. of 12th International Conference on Information Systems and Industrial Management, pp.47-58, 2013.
3. U. Shafique, H. U. Khan, S. Waqar, A. Sher, A. Zeb, U. Shafi, and R. Ullah, "Modern Authentication Techniques in Smart Phones: Security and Usability Perspective," International Journal of Advanced Computer Science and Applications, vol. 8, no. 1, pp. 331-340, 2017.
4. A. K. Jain, F. D. Griess, and S. D. Connell, "On-Line Signature Verification," Pattern Recognition, vol. 35, no. 12, pp. 2963-2972, 2002.
5. G. Dimauro, S. Impedovo, M. G. Lucchese, R. Modugno, and G. Pirlo, "Recent Advancements in Automatic Signature Verification," Proc. of the 9th International Workshop on Frontiers in Handwriting Recognition, pp. 179-184, 2004.
6. J. Fierrez, and J. Ortega-Garcia, "On-Line Signature Verification," in A. K. Jain, P. Flynn, and A. A. Ross (eds.) Handbook of Biometrics, Springer, New York, 2007.
7. S. Sayeed, A. Samraj, R. Besar, and J. Hossen, "Online Hand Signature Verification: A Review," Journal of Applied Sciences, vol. 10, no.15, pp. 1632-1643, 2010.
8. I. M. El-Henawy, M. Z. Rashad, O. Nomir, and K. Ahmed, "Online Signature Verification: State of the art," International Journal of Computers & Technology, vol. 4, no. 2, pp. 664-678, 2013.
9. M. Diaz, M. A. Ferrer, D. Impedovo, M. I. Malik, G. Pirlo, and R. Plamondon, "A Perspective Analysis of Handwritten Signature Technology," ACM Computing Surveys, vol. 51, no. 6, pp. 117:1-39, 2019.
10. R. Ricci, G. Chollet, M. V. Crispino, S. Jassim, J. Koreman, A. Morris, M. Olivar-Dimas, S. Garcća-Salicetti, and P. Soria-Rodríguez, "The "SECUREPHONE" A Mobile Phone with Biometric Authentication and e-Signature Support for Dealing Secure Transactions on the Fly," Proc. of the International Conference on Security and Cryptography, pp. 9-16, 2006.

11. M. Martinez-Diaz, J. Fierrez, R. P. Krish, and J. Galbally, "Mobile Signature Verification: Feature Robustness and Performance Comparison," IET Biometrics, vol. 3, no. 4, pp. 267-277, 2014.
12. N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon, "Biometric-rich gestures: A novel approach to authentication on multi-touch devices," Proc. of the 30th ACM Conference on Human Factors in Computing Systems, pp. 977-986, 2012.
13. A. D. Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and I know it's you! Implicit Authentication based on Touch Screen Patterns," Proc. of 2012 Conference on Human Factors in Computing Systems, pp. 987-996, 2012.
14. M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication," IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 136-148, 2013.
15. N. Sae-Bae and N. Memon, "Online Signature Verification on Mobile Devices," IEEE Transactions on Information Forensics and Security, vol. 9, no. 6, pp. 933-947, 2014.
16. M. Martinez-Diaz, J. Fierrez, and J. Galbally, "Graphical Password-Based User Authentication with Free-Form Doodles," IEEE Transactions on Human-Machine Systems, vol. 46, no. 4, 2016.
17. M. Antal and L. Zsolt, "Biometric Authentication Based on Touchscreen Swipe Patterns," Proc. of 9th International Conference Interdisciplinarity in Engineering, pp. 8-9, 2015.
18. V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous User Authentication on Mobile Devices: Recent Progress and Remaining Challenges," IEEE Signal Processing Magazine, vol. 33, no. 4, pp.49-61, 2016.
19. R. Kumar, V. V. Phoha, and A. Serwadda, "Continuous Authentication of Smartphone Users by Fusing Typing, Swiping, and Phone Movement Patterns," Proc. of 8th IEEE International Conference on Biometrics: Theory, Applications, and Systems, 2016.
20. T. Nguyen, N. Sae-Bae, and N. Memon, "DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices," Computers & Security, vol. 66, pp. 115-128, 2017.
21. S. Al-Showarah, "The Effectiveness of Dynamic Features of Finger Based Gestures on Smartphones' Touchscreens for User Identification," International Journal of Interactive Mobile Technologies, vol. 11, no. 1, pp.133-142, 2017.
22. Y. Ku, L. H. Park, S. Shin,and T. Kwon, "It As Shown: Behavioral Pattern Lock for Mobile User Authentication," IEEE Access. vol. 7, pp. 69363-69378, 2019.
23. R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "BioTouchPass2: Touchscreen Password Biometrics Using Time-Aligned Recurrent Neural Networks," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2616-2628, 2020.
24. M. Sreeraj and S. M. Idicula, "A Survey on Writer Identification Schemes," International Journal of Computer Applications, vol. 26, no. 2, pp. 23-33, 2011.
25. A. Takahashi and I. Nakanishi, "Authentication Based on Finger-Writing of a Simple Symbol on a Smartphone," Proc. of International Symposium on Intelligent Signal Processing and Communication Systems, pp. 411-414, Nov. 2018.
26. A. A Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics, Springer, 2006.