Security enhancement for touch panel based user authentication on smartphones

Daiki Izumoto and Yasushi Yamazaki
The University of Kitakyushu, Fukuoka, Japan
E-mail: a9mca002@eng.kitakyu-u.ac.jp, y-yamazaki@kitakyu-u.ac.jp Tel/Fax: +81-93-695-3259

***Abstract*—With the rapid spread of smartphones, user authentication for privacy protection is becoming increasingly important. Pattern lock is one of the most typical user authentication methods using a touch panel on smartphones. However, despite its high usability, it is vulnerable to shoulder surfing and smudge attacks. Therefore, to improve security of touch panel based user authentication on smartphones while maintaining usability, we propose a method that combines the function of pattern lock and handwritten biometrics and demonstrate its effectiveness through simulation experiments.**

I. Introduction

With the rapid spread of smartphones, user authentication for privacy protection is becoming increasingly important. Conventional and typical smartphone user authentication methods are personal identification number (PIN), password, and pattern lock, which are widely used because they are easy for users to perform. However, these user authentication methods present a risk that others may learn a PIN, password, or pattern from peeping (shoulder surfing) or a residual fingerprint on a touch panel (smudge attacks). Therefore, resistance to shoulder surfing and smudge attacks must be improved while maintaining usability.

In addition, biometric authentication using biometric information that can be obtained from sensors mounted on smartphones is attracting attention as a user authentication method that balances usability and security on smartphones [1]. Biometric authentication has no risk of being forgotten or lost and is highly resistant to impersonation. Currently, biometric authentication that has been put to practical use in smartphones is mainly fingerprint, face, and iris authentication. However, these user authentication methods have the disadvantage that the smartphone cost increases because a special sensor must be mounted on the smartphone to obtain biometric information or perform highly secure authentication. Therefore, in this paper, we focus on biometric information by using handwriting information that can be obtained from the standard touch panel on a smartphone.

Examples of research on biometrics using handwriting information that can be obtained from touch panels include a method using Japanese Kanji signatures [2] and a method using initials [3]. However, in the former case, such signatures are not always suitable to write on a small smartphone screen, and in the latter case, the user needs to be familiar with the method to stably acquire biometric information, which is not convenient. Therefore, it is considered desirable to obtain handwriting information from simple actions familiar to the user. Pattern lock is a simple graphic writing authentication method. Therefore, we thought that we could improve its resistance to impersonation while maintaining its usability by simultaneously obtaining handwriting information reflecting personal characteristics at the time of writing the pattern of the pattern lock and combining it with graphic information of the pattern.

On the basis of the above idea, this paper proposes a method to combine the function of pattern lock and biometric authentication using handwriting information to improve security while maintaining the usability of the pattern lock. We also report the results of evaluating the effectiveness of the proposed method by simulation experiments.

The remainder of this paper is organized as follows. In Section II, biometric information-based user authentication system using touch panel is described. Next, experimental results are presented in Section III. Finally, conclusions are stated in Section IV.

II. Biometric information-based user authentication system using touch panel

A. Related Research

In this paper, we extract features that are effective for identifying a user from handwriting information that can be obtained when writing a pattern of the pattern lock. Angulo and Wästlund [4] proposed a method to improve security by combining the function of biometrics with pattern lock. They used two features: the time at which a finger touches around each of the nine dots on the touch panel and the time at which a finger moves from one dot to the next. In their experiments, they used the above two features and achieved up to 10.4% EER (Equal Error Rate). They used only these two features, but the features that can be obtained directly from smartphones include not only coordinates and time but also pressure and contact area. In addition, Lee et al. [5] proposed the writing speed-related features that are calculated by coordinates and time. We thought that using these features may possibly improve authentication accuracy. Therefore, in this paper, in addition to the features used in the related research, features such as writing speed, pressure, and contact area are obtained at the same time, and using these features for authentication is expected to further improve authentication accuracy.

B. Selecting Features

As a preliminary experiment, the features used for authentication were determined by examining the effectiveness for individual identification against features such as writing time and pressure that can be obtained from around a dot and between dots of the pattern lock.

First, we define the features that can be obtained directly from the touch panel of a smartphone as the first features and the features that can be calculated from the first features as the secondary features. The first features are listed in Table I.

TABLE I
FIRST FEATURES THAT CAN BE OBTAINED FROM A SMARTPHONE

Name	Description
Position on touch panel	X-coordinate Y-coordinate
Time stamp	Acquisition time of time series data
Contact state	Contact state of writing surface and finger Contact:1, No contact:0
Contact area	Contact area of the finger touching the writing surface
Pressure	Finger pressure touching writing surface

Next, we calculate the secondary features from the first features of Table I. We calculate the secondary features such as writing time, speed, and average pressure from the first features obtained around each dot and between dots on the pattern lock.

Here, we define the around-dot area as the area of 40 $\times$ 40 pixels whose center corresponds to each dot and define the between-dot area as the area between one around-dot area and the adjacent around-dot area in the writing order (see Figure 1). Some features obtained in the preliminary experiment were referred to the features proposed by Lee et al. [5]. Table II lists the secondary features extracted in the preliminary experiment.

Moreover, we define the dot that is passed over when writing a pattern as the passing point and define the pair of one around-dot area and the adjacent between-dot area as the section. Among the features shown in Table II, Nos. 1 to 15 are obtained from each around-dot area, and Nos. 16 to 31 are obtained from each between-dot area. As the number of passing points increases in writing a pattern, the number of features also increases. For example, when there are nine passing points, the number of features used is $31 \times 8 + 1 = 249$.

Next, normalization is performed to make the range of data constant for each calculated secondary feature. Assuming that the i-th feature is x_i, the maximum value of the i-th feature is x_{max}, the minimum value of the i-th feature is x_{min}, and the normalized i-th feature is f_i, the normalization is defined as equation (1).

$$f_i = \frac{x_i - x_{min}}{x_{max} - x_{min}} \tag{1}$$

In the preliminary experiment, we use the secondary features that are normalized on the basis of (1) and investigate the features that are effective for individual identification.

- Preliminary experiment conditions

Table III lists the conditions of the preliminary experiment, and Figure 2 lists the pattern used.

TABLE II
SECONDARY FEATURES EXTRACTED IN PRELIMINARY EXPERIMENT

No.	section	Features name
1	around dot	Writing time around dot
2		Writing time around dot / Total writing time
3		Average writing speed around dot
4		Max writing speed around dot
5		Min writing speed around dot
6*		Average writing speed around dot / Max writing speed around dot
7*		Min writing speed around dot / Average writing speed around dot
8*		Time of max writing speed around dot / Writing time around dot
9*		Time of min writing speed around dot / Writing time around dot
10		Average pressure around dot
11		Max pressure around dot
12		Min pressure around dot
13		Average contact area around dot
14		Max contact area around dot
15		Min contact area around dot
16	between dot	Writing time between dots
17		Writing time between dots / Total writing time
18		Average writing speed between dots
19		Max writing speed between dots
20		Min writing speed between dots
21*		Average writing speed between dots / Max writing speed between dots
22*		Min writing speed between dot / Average writing speed between dots
23*		Max writing speed between dot / Average writing speed between dots
24*		Min writing speed between dot / Average writing speed between dots
25		Average pressure between dots
26		Max pressure between dots
27		Min pressure between dots
28		Average contact area between dots
29		Max contact area between dots
30		Min contact area between dots
31		Angle from start point between dots
32	Total	Total writing time

* Referred to [5]

TABLE III
PRELIMINARY EXPERIMENT CONDITIONS

Device used	Arrows MO3
Written information	Patterns
Number of subjects	5
Total number of training patterns	50 (5 subjects $\times$ 10 times)
Total number of test patterns	25 (5 subjects $\times$ 5 times)
Total number of simple forged patterns	50 (5 subjects $\times$ 10 times)

- Results of preliminary experiment

We defined the variance of the feature obtained from each user's training patterns as the intra-class variance and the variance between the features obtained from each user's training patterns and the features obtained from target user's simple forged patterns as the inter-class variance. In the preliminary experiment, we used the F ratio calculated from the ratio of the inter-class variance to the intra-class variance as a criterion of features effective for individual identification. Features with higher F ratio reflect more individuality.

The F ratio was calculated for each feature obtained when writing the pattern in Figure 2. Figure 3 shows the results of averaging the F ratio obtained from each around-dot and each between-dot area for the same type of features. The feature number in Figure 3 corresponds to the number in Table II. On the other hand, Figure 4 shows the results of averaging the F ratio obtained from each around-dot and between-dot area for every section. The number at the end of each section in Figure

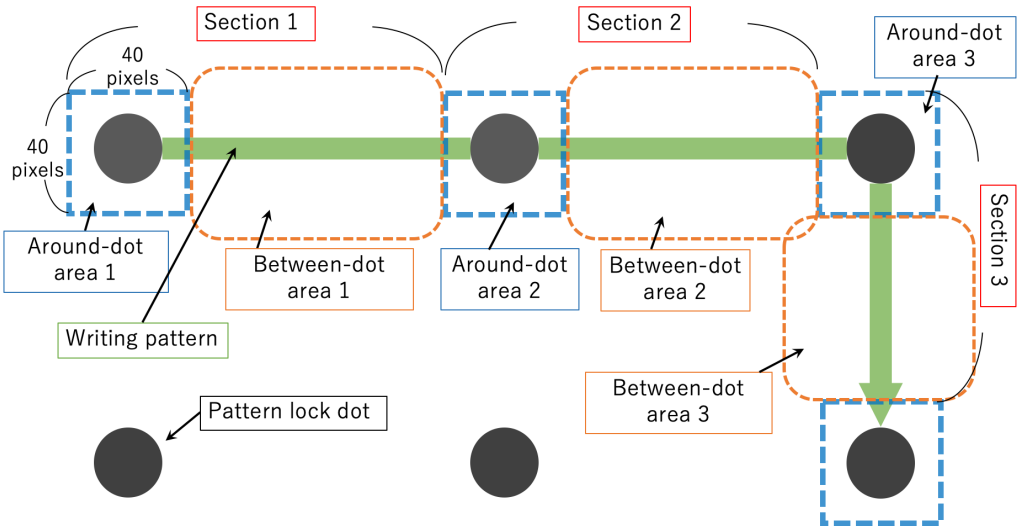

Fig. 1. Definition of around-dot area and between-dot area

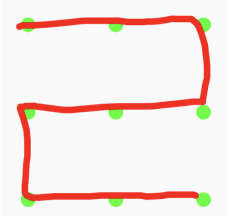

Fig. 2. Pattern used in preliminary experiment

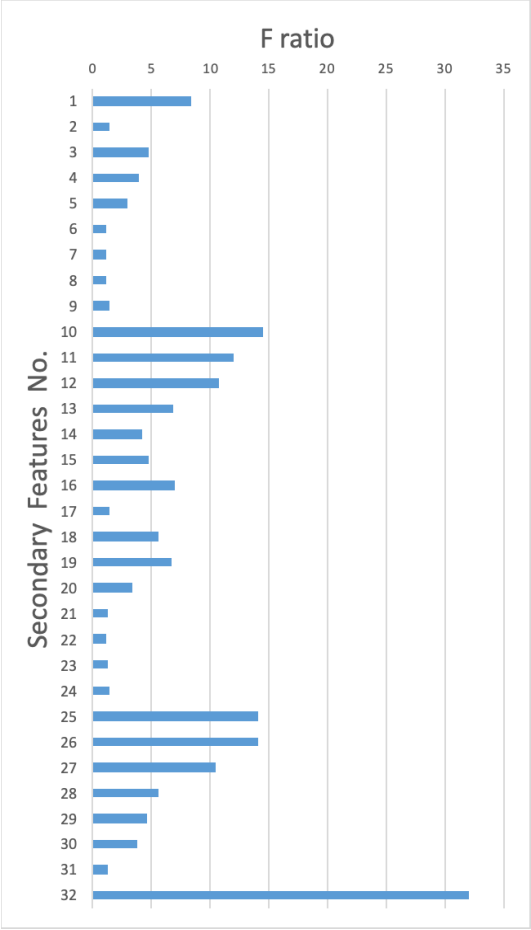

Fig. 3. Average value of F ratio for each feature

4 indicates the order of the sections passed when writing the pattern.

Focusing on the features related to the writing time (Nos. 1, 2, 16, 17, and 32) in Figure 3, the F ratio for the total writing time (No. 32) is large, but the F ratios for the writing time of around-dot and between-dot areas (Nos. 1, 2, 16, and 17) are relatively small. Based on these results, there is a high possibility that features cannot be stably extracted in local areas such as around-dot or between-dot areas.

On the other hand, in Nakamura and Toyoda [6], a Katakana character is divided into three parts (beginning, middle, and end), and features are extracted for each part. Evaluation results revealed that the middle and end parts had larger F ratios than the beginning part. From Figure 4, the results of the preliminary experiment also show that the F ratio is small in the beginning part (around and between dots 1,2,3) of the pattern and the features with a large F ratio appear in the middle part (around and between dots 4,5,6) and the end part (around and between dots 7,8,9) as in the case of Nakamura and Toyoda [6].

From the above discussion, instead of dividing the pattern into around-dot or between-dot areas, we decided to divide the pattern into beginning, middle, and end parts and broaden the area for obtaining the features for each area, which is expected to enable more stable feature extraction. Therefore,

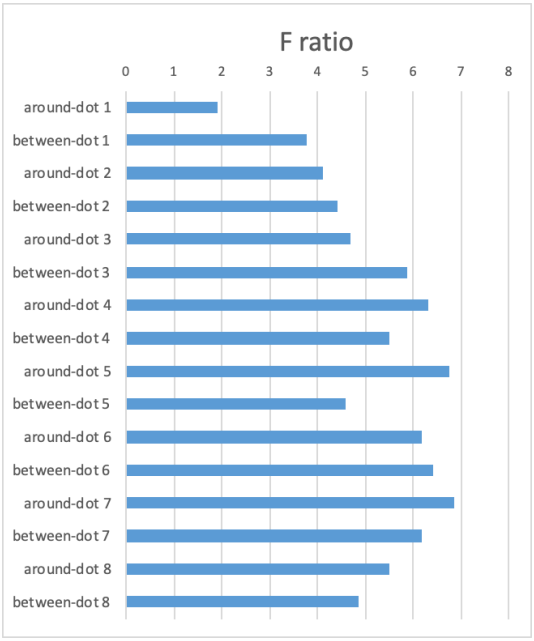

Fig. 4. Average value of F ratio for each section

in this paper, with reference to Nakamura and Toyoda [6], the pattern is divided into three parts, and for each part, features such as writing speed, pressure, and contact area are extracted. Table IV lists the secondary features used for evaluation. Here, the section changes the part divided in accordance with the number of passing points at the time of pattern writing.

The number of passing points is p, the division points of the beginning and middle parts are the p_{bm}-th passing point, and the dividing points of the middle and end parts are the p_{me}-th passing point. Then, p_{bm} and p_{me} are defined by equations (2) and (3), respectively. Here, $\lceil p/3 \rceil$ represents the smallest integer $p/3$ or more. Figure 5 shows an example of division when the number of passing points of the pattern is eight.

$$p_{bm} = \lceil p/3 \rceil \quad (2)$$

$$p_{me} = p - (p_{bm} - 1) \quad (3)$$

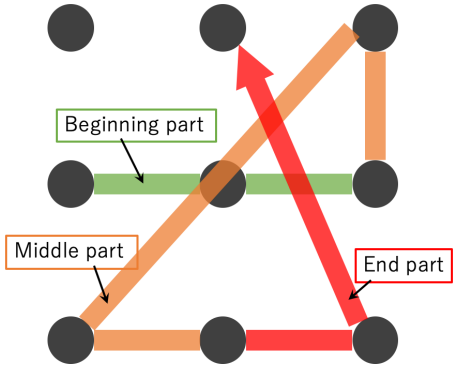

Fig. 5. Example of pattern division (in the case of eight passing points)

TABLE IV
SECONDARY FEATURES USED FOR AUTHENTICATION

No.	part	Features name
1	beginning part	Writing time beginning part
2		Writing time beginning part / Total writing time
3		Average writing speed beginning part
4		Max writing speed beginning part
5		Min writing speed beginning part
6		Average writing speed beginning part / Max writing speed beginning part
7		Min writing speed beginning part / Average writing speed beginning part
8		Time of max writing speed beginning part / Writing time beginning part
9		Time of min writing speed beginning part / Writing time beginning part
10		Average pressure beginning part
11		Max pressure beginning part
12		Min pressure beginning part
13		Average contact area beginning part
14		Max contact area beginning part
15		Mix contact area beginning part
16		Angle from start point beginning part
17	middle part	Writing time middle part
18		Writing time middle part / Total writing time
19		Average writing speed middle part
20		Max writing speed middle part
21		Min writing speed middle part
22		Average writing speed middle part / Max writing speed middle part
23		Min writing speed middle part / Average writing speed middle part
24		Time of max writing speed middle part / Writing time middle part
25		Time of min writing speed middle part / Writing time middle part
26		Average pressure middle part
27		Max pressure middle part
28		Min pressure middle part
29		Average contact area middle part
30		Max contact area middle part
31		Min contact area middle part
32		Angle from start point middle part
33	end part	Writing time end part
34		Writing time end part / Total writing time
35		Average writing speed end part
36		Max writing speed end part
37		Min writing speed end part
38		Average writing speed end part / Max writing speed end part
39		Min writing speed end part / Average writing speed end part
40		Time of max writing speed end part/ Writing time end part
41		Time of min writing speed end part/ Writing time end part
42		Average pressure end part
43		Max pressure end part
44		Min pressure end part
45		Average contact area end part
46		Max contact area end part
47		Min contact area end part
48		Angle from start point end part
49	Total	Total writing time

C. User authentication algorithm

Figure 6 shows the process of authentication in the proposed method.

By using the features shown in Table IV, matching is performed by using three types of algorithms: Manhattan distance, support vector machine (SVM), and random forest. We define the pattern written by the authenticating user as a genuine pattern. In the case of Manhattan distance, we divide the genuine pattern into training and test patterns. The distance between the features obtained from the training pattern and the features obtained from the test pattern or the simple forged pattern is calculated. If the distance is smaller than the preset threshold, the user is authenticated to be genuine; otherwise, the user is not.

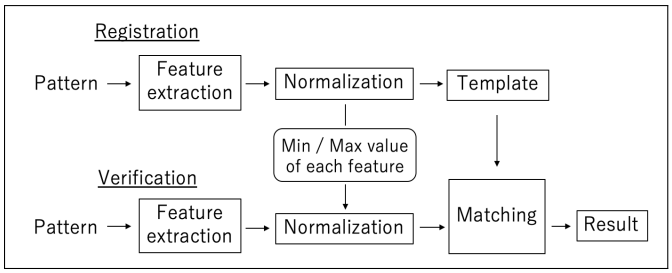

Fig. 6. User authentication algorithm

In the case of SVM and random forest, the genuine pattern and the simple forged pattern are divided into a training pattern and a test pattern, and features obtained from the training pattern are used as training data. The training data is used to train each algorithm, and the test pattern of the user is identified by a two-class classification of a person and others by the algorithm after training (see Figure 7).

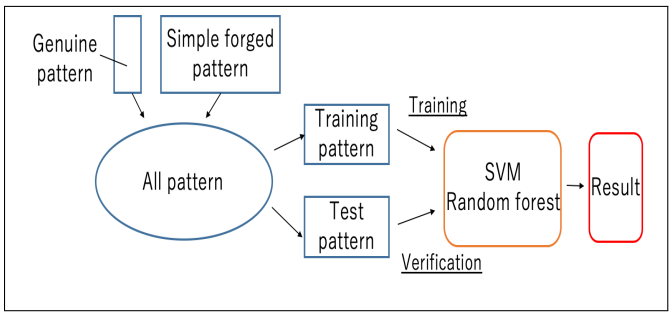

Fig. 7. Process of authentication of SVM and Random forest

III. SIMULATION EXPERIMENTS

Two experiments were conducted to evaluate the reliability of the proposed method. First, we compared the authentication accuracies of the proposed method and the related method [4]. Next, we evaluated the change in the authentication accuracy when one or two parts from which the features are extracted were selected from among the beginning, middle, and end parts. Three patterns were used in the experiment, and each pattern had a different number of passing points at the time of writing and a different angle at the time of bending. Figures 8 to 10 list the patterns used in the experiments, and Table V lists the parameters of the experiments.

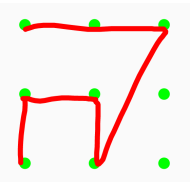

Fig. 8. Pattern A

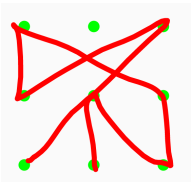

Fig. 9. Pattern B

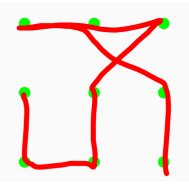

Fig. 10. Pattern C

TABLE V
EXPERIMENTAL CONDITIONS

Device used	Arrows MO3
Written information	Pattern (A,B,C)
Number of subjects	10
Total number of patterns	200 (10 subjects × 20 times)
Obtained information	Position on touch panel (X,Y) Time stamp Contact state (1 or 0) Contact area Pressure

A. Comparison with related method

First, we evaluated and compared the authentication accuracy when using the features in the related method [4] and in the proposed method. In the experiment, patterns other than that of the person in the comparison are treated as simple forged data. The methods were compared using Manhattan distance, SVM, and random forest, and the EER was calculated as the authentication accuracy. Table VI lists the EER when using the features in the related method [4] and proposed method.

TABLE VI
EER COMPARISON BETWEEN RELATED AND PROPOSED METHODS

pattern		method	Manhattan	SVM	Random forest
EER (%)	A	Related research [4]	19.4	11.0	9.0
		Proposed	10.6	4.3	6.1
	B	Related research [4]	16.3	8.6	6.7
		Proposed	6.7	1.9	3.7
	C	Related research [4]	10.8	4.4	3.8
		Proposed	5.4	1.2	3.1

From Table VI, the proposed method has lower EER and higher authentication accuracy than the related method [4] for all algorithms. In addition, since each pattern has a different EER, the authentication accuracy may possibly change depending on the shape of the pattern. Since the number of passing points increases and the value of EER decreases in the order of A, B, and C, increasing the number of passing points in the pattern may possibly have improved the authentication accuracy.

B. Authentication accuracy for each part

Next, the authentication accuracy for the beginning, middle, and end parts of each pattern and the recognition accuracy when two of the parts were selected were determined and evaluated. Table VII lists the EER for each part of each pattern in the case of using Manhattan distance.

TABLE VII
EER FOR EACH PART

part		beginning	middle	end	beginning & middle	beginning & end	middle & end	all parts
EER (%)	A	23.7	17.3	11.7	14.4	10.5	11.1	10.6
	B	18.9	11.4	9.7	10.3	8.0	6.4	6.7
	C	15.2	11.4	10.7	7.57	6.19	5.9	5.4

From Table VII, the end part has the lowest EER in any pattern and high authentication accuracy. In addition, when

two parts are combined, the combined middle and end parts have the lowest EER except for pattern A and high authentication accuracy. In all patterns, the combined middle and end parts have an EER close to the EER of all parts. In addition, the combined beginning and end parts in pattern A and the combined middle and end parts in pattern B can obtain EERs lower than the EER of all parts. Therefore, it is considered that the authentication accuracy may be improved by obtaining the features only from the part where the individual features tend to appear, rather than obtaining the features from the whole pattern.

Moreover, the authentication accuracy for each part of each pattern was also evaluated in the case of using SVM, with the consideration that the EER was the lowest in the proposed method when using SVM in the previous experiment as shown in Table VI. The evaluation results revealed that pattern A had the lowest EER in the end part, but patterns B and C had the lowest EERs in the middle part. As shown in Table VIII, the middle part of pattern A has the same number of passing points as the beginning and end parts, but the middle parts of patterns B and C have more passing points than the beginning and end parts. Therefore, it is considered that the authentication accuracy for each part was affected by the number of passing points in the case of using SVM.

TABLE VIII
NUMBER OF PASSING POINTS IN EACH PART

part		beginning	middle	end
Number of passing points	A	2	2	2
	B	2	3	2
	C	2	4	2

IV. CONCLUSIONS

In this paper, we proposed a method to combine the function of pattern lock and biometric authentication using handwritten information to improve the security while maintaining the usability of pattern lock. The effectiveness of the proposed method was evaluated by reliability evaluation experiments. From results of the experiment, the proposed method achieved higher authentication accuracy than the related method [4], demonstrating its effectiveness. Future work includes evaluating tolerance to trained forged patterns and investigating the relationship between pattern shape and authentication accuracy.

ACKNOWLEDGMENTS

Part of this work was supported by JSPS KAKENHI Grant Number JP16K00190.

REFERENCES

[1] P.A.Tresadern, C.McCool, N.Poh, P.Matejka, A.Hadid, C.Levy, T.F.Cootes, and S.Marcel, "Mobile Biometrics : Combined Face and Voice Verification for a Mobile Platform," *IEEE Pervasive Computing*, 12, 1, pp.79-87, 2013.

[2] T.Sowa, S.Sunada, Y.Yamazaki, and T.Miyazaki, "Biometric Bit String Generation from Handwritten Signature on Smart Device," in *Proc. of fourth Int'l Workshop on Information and Communication Security (WICS '16)*, pp.662-665, 2016.

[3] R.Yamagami and Y.Yamazaki, "Biometric Bit String Generation from Handwritten Initials on Smart Phones," in *Proc. of fifth Int'l Workshop on Information and Communication Security (WICS '17)*, pp.516-521, 2017.

[4] J.Angulo and E.Wästlund, "Exploring Touch-Screen Biometrics for User Identification on Smart Phones," *IFIP Advances in Information and Communication Technology*, 375, pp.130-143, 2012.

[5] L.L.Lee, T.Berger, and E.Aviczer, "Reliable On-Line Human Signature Verification System," *IEEE Trans. PAMI*, 18, 6, pp.643-647, 1996.

[6] Y.Nakamura and J.Toyoda, "An Extraction of Individual Handwriting Characteristics Based on Calligraphic Skills (in Japanese)," *IEICE Trans.*, J77-D-II, 3, pp.510-518, 1994.