The Authentication System Automatically Generating Feature Points  
- Effect of Dummy Feature Points

Hiroshi Dozono  
Saga University  
Faculty of Science and Engineering  
1-18-25 Saga, JAPAN 840-8502  
Email: hiro@dna.ec.saga-u.ac.jp

Tatsuya Chuto  
KYOCERA Document Solutions  
Department of Advanced Fusion  
1-18-25 Saga, JAPAN 840-8502  
Email: 17578001@edu.cc.saga-u.ac.jp

Kenta Uchikoshi  
Saga University  
Department of Advanced Fusion  
1-18-25 Saga, JAPAN 840-8502  
Email: nak@fukuoka-u.ac.jp

Masanori Nakakuni  
Fukuoka University  
Email: nak@fukuoka-u.ac.jp

Abstract—Recently, the devices which are equipped with touch panels, such as smartphone and tablet, become widespread. As the biometric authentication device, the fingerprint reader are equipped to the smartphone upper than middle range, however the almost of smartphone in low range and tablet devices do not equip the fingerprint reader. For such devices, PIN or the pattern of connecting points are used as authentication methods. In our group, the authentication method which can generate the feature points automatically from freehand pattern is researched. In this report, the authentication method which raises the strength as the knowledge authentication with adding dummy points to the generated pattern is introduced.

Keywords—Mobile system security, Biometric Authentication, Multi-modal Authentication

I. INTRODUCTION

Recently, due to the advance of communication and mobile technology, the information level in the society is highly developed and the computers and the networks become necessary for our life. However, the awareness for the security does not advance in spite of the importance of the security.

Especially the smartphones and tablet devices, in which many personal information is recorded, the risk of the leak is high because it is carried 24/7. It may be possible to be peeked the privacy such that the records of the Emails and SNS. For this problem, we are developing the biometric authentication system using the touch panel which is equipped to almost mobile devices. The distinguishing features of this system are 1) It is portable because it does not need the special input device or sensor except the touch panel. 2) It is the hybrid of both the knowledge based authentication, which uses the pattern of the connections between the feature points generated from hand written pattern, and the biometric authentication, which uses the writing speed between the feature points. This system is considered to perform much higher security level compared with the authentication method equipped to the conventional mobile devices using pattern or PIN.

In this paper, we propose the improvement of this system with adding the dummy points to raise the security level of knowledge based authentication, and the performance is examined by the experiments of authentication. This paper is organized as follows. In section 2, the overview of the authentication method using touch panel is mentioned. In section 3, the proposed authentication method which generates feature points automatically is mentioned in order of generation of feature points, biometric authentication based on feature points and addition of dummy feature points. In section 4, the experimental results of knowledge based authentication, biometric authentication and biometric authentication using dummy feature points are shown.

II. AUTHENTICATION METHODS USING TOUCH PANEL

As the popularization of the mobile devices such as smartphones and tablet devices, the devices which equipped with touch panel become widespread. And these devices grow in usage and popularity to the people who is not familiar to the conventional computers. In these situation, a simple authentication method which uses touch panel is desired. As the authentication method using touch panels, the signature written on the touch panel is often used. However, it is difficult to write identical signature on slippery touch panel especially for capacitive type panel which is recently equipped to almost all mobile devices. As the another method, the authentication method which uses the knowledge factors with selecting the symbols or positions in the image is often used. However this method has a weakness for stealthy glance. Android devices uses the lock screen which uses the knowledge factor with connecting the points displayed on the touch panel. However, the patterns which can be drawn are not flexible, and users tend to select simple patterns because the points are fixed. Thus, this method also has a weakness for stealthy glance. For avoiding stealthy glance, biometric authentication is effective. Biometric authentication is classified to 2 types; biometrics authentication using biological features and biometric authentications using behavioral features. As the biological features, the fingerprints, vein patterns and iris patterns are often used. They can achieve high accuracy, however special sensor devices, such as fingerprint reader, are required for implementation. As the behavioral features, keystroke timings[2]
and penmanship of handwritten patterns[3] or signature[4] are often used. They can be obtained from conventional input devices, however the accuracy of authentication is lower than that of biological features. At the same time, high accuracy is not always necessary for the devices which is used personally because authentication is used as the lock method just in case the device is stolen or possessed by malicious users. In this paper, the biometric authentication method which uses the biological features obtained from touch panel is proposed. We have proposed an authentication system using the behavior biometrics during drawing the symbol displayed in the touch panel[5]. This system uses pen speed and pen pressure at all sampling times as behavior biometrics, and marks 0.1 as Equal Error Rate(ERR). However, capacitive type panel, which is mostly used recently, can not detect pen pressure, and it requires much computational costs for matching all pen speed and pen pressure at all sampling time. For this problem, we propose an authentication system which generates feature points automatically.

In this paper, FAR(False Acceptance Rate) and FRR(False Rejection Rate) are used as the indexes of accuracy. FAR is the rate of accepting the another user falsely. FRR is the rate of rejecting registered user falsely. Both FAR and FRR should be small enough for secure authentication method.

III. THE BIOMETRIC AUTHENTICATION SYSTEM WHICH GENERATES THE FEATURE POINTS AUTOMATICALLY

It is considered to be difficult to use completely free drawing patterns on the touch panel for authentication, because the user can not redraw the same pattern without guidelines or user may not recall the pattern which was registered to the system. For this problem, the pattern used for the authentication is often limited to the easily recallable pattern such as the signature. However, it is difficult to write same signature for the people, who are not familiar to write signature, such as Japanese.

For this problem, we proposed the authentication system which generates the feature points automatically from the freely written pattern. During the authentication, the feature points are shown on the display as guideline, the user can redraw the pattern with connecting the points on the touch panel. The example of the feature points generated from handwritten pattern is shown in Fig.1. We have reported this system in [1] and [6]. In this paper, the improvements of the detection of feature points and accuracy of biometric authentication, and introduction of dummy feature points are presented.

A. Detection of the Feature Points

The system proposed in this research conducts the authentication with extracting the feature values based on the feature points detected from the handwritten pattern. The feature points should be connected in the registered order, the feature values should be matched with the registered values. The feature point does not denotes a exact point, and it rather denotes a area, which changes depending on the situation around the point.

1) Detection using curvature: The feature points are detected using curvature. The curvature is calculated using the coordinates of 3 consecutive points on the line. The curvature is calculated by the following equation when 3 points A,B and C are given as shown in Fig.2.

$$\text{curvature} = \left( \frac{1}{(1 + (d(t))^2)} \right)^{\frac{3}{2}} \ast (d(t + 1) - d(t))$$

If calculated curvature is more than the pre-setted threshold, point B is marked as a candidate of feature point. For each candidate, the curvature is calculated again with exchanging x-coordinate and y-coordinate, and if the curvature is more than the threshold again, point B is marked as feature point. The reason why the curvature is calculated twice is to avoid the miss detection of feature points because the curvature becomes large for nearly vertical line with small difference of x-coordinate. The threshold is set as 0.2 through some experiments.

2) Detection using distance: If the line gently curves in long interval, the feature point is not marked in long distance, and it affects the accuracy of biometric authentication and the recalling of the registered pattern for the user. For this problem, the rule to mark the feature points in the pre-setted
interval is added. For the irregular user who knows this system, it becomes difficult to guess the pattern because additional feature points are generated without the curve on the line.

3) Detection using inner product: Through some experiments, miss detection of the feature points for the sharp curving lines such as the edges on zigzag line. For this problem, the rule using inner product is added. In Fig.3, for the origin $O$, vector $\vec{a}$ and vector $\vec{b}$ are defined for the point A and point B. With moving point B on the line, if the angle between vector $\vec{a}$ and vector $\vec{b}$ becomes larger than the presetted threshold, the feature point is generated on the crossing point of the curved line and the parallel line of vector $\vec{b}$. The angle is calculated using inner product of vector $\vec{a}$ and $\vec{b}$. The threshold is set as 70 degree through experiments.

4) Integration of the feature points: If the feature points are generated too dense on the line, it becomes easy to guess the registered line for irregular user. For this problem, the overlapping feature points are integrated to the centroid of them as shown in Fig.4. Additionally, the starting point and terminal point are integrated for looping line as shown in Fig.5. passing the feature points are taken as the timings when the pen enters the circle area of feature points.

1) Optimization of the biometric authentication: The change of the feature values by time should be considered for the biometric authentication, especially for that using behavior biometrics. The feature values may change by environment, injury of the user and the experience of the user. Or, depending on the character of the user, some user may write the pattern exactly, others may write the pattern roughly.

For these problems, the feature values and the thresholds of authentication are adjusted in every successful authentication process. With this adjustment, the authentication system gets to fit the user with repeating authentication.

C. Dummy feature points

For using this authentication system, it is recommend to set the number of feature points from 5 to 8. However, the larger number of the feature points causes the degradation of FRR in some experiments because of worsening of repeatability. Inversely, the fewer number of the feature points leads to the accidental success of the authentication of irregular users, and it causes the raise of FAR.

For this problem, the system which allows the user to add the dummy feature points at arbitrary position on the screen. The dummy feature points can be registered after the registration of the hand written pattern. In the authentication process, the authentication becomes failure if the hand written pattern passes any dummy feature points. Fig.7 shows the registration of dummy feature points.

B. Biometric authentication using writing speed

As the feature of biometric authentication, writing speed is used. As the feature points are generated at suitable intervals, the writing speed can be substituted to the time intervals to pass through the feature points as shown in Fig.6. The moments of
IV. EXPERIMENTAL RESULTS

A. Experimental results of knowledge based authentication using connection patterns

At first, the experimental results of knowledge based authentication using connection patterns are shown. Fig. 8 shows the connection pattern with 5-8 feature points used in this experiments.

These patterns are generated by the proposed system in the registration process of hand written patterns by some users. As mentioned in the previous section, the feature points without the line is presented to the examinees. 10 examinees who did not know the pattern tried the authentication 3 times for each pattern, thus each pattern is tried 30 times. All examinees experienced this system before in the experiments of previous system. Table 1 shows the result. With 4 feature points, one examinee is authenticated once, however with more than 5 feature points no examinees can be authenticated because they can not guess the pattern. The number of examinees who can identify the starting point of the pattern is the largest for the 8 feature points because it tend to be guessed that the starting point is top when the pattern resembles the circle. Thus the user should register the pattern which does not start from top of the pattern on the screen.

B. Experimental results of biometric authentication using writing speed

1) Method of experiments: This experiment is conducted with 16 examinees including the regular user. The regular user registers the handwritten pattern, and repeats the authentication 20 times to adjust the parameters. And the other 15 examinees try the authentication 20 times for each patterns whose numbers of feature points are from 5 to 8 with changing the connecting patterns are known and unknown. The sketch of the experiments is shown in Fig.9.

These patterns are generated by the proposed system in the registration process of hand written patterns by some users. As mentioned in the previous section, the feature points without the line is presented to the examinees. 10 examinees who did not know the pattern tried the authentication 3 times for each pattern, thus each pattern is tried 30 times. All examinees experienced this system before in the experiments of previous system. Table 1 shows the result. With 4 feature points, one examinee is authenticated once, however with more than 5 feature points no examinees can be authenticated because they can not guess the pattern. The number of examinees who can identify the starting point of the pattern is the largest for the 8 feature points because it tend to be guessed that the starting point is top when the pattern resembles the circle. Thus the user should register the pattern which does not start from top of the pattern on the screen.

B. Experimental results of biometric authentication using writing speed

1) Method of experiments: This experiment is conducted with 16 examinees including the regular user. The regular user registers the handwritten pattern, and repeats the authentication 20 times to adjust the parameters. And the other 15 examinees try the authentication 20 times for each patterns whose numbers of feature points are from 5 to 8 with changing the connecting patterns are known and unknown. The sketch of the experiments is shown in Fig.9.

These patterns are generated by the proposed system in the registration process of hand written patterns by some users. As mentioned in the previous section, the feature points without the line is presented to the examinees. 10 examinees who did not know the pattern tried the authentication 3 times for each pattern, thus each pattern is tried 30 times. All examinees experienced this system before in the experiments of previous system. Table 1 shows the result. With 4 feature points, one examinee is authenticated once, however with more than 5 feature points no examinees can be authenticated because they can not guess the pattern. The number of examinees who can identify the starting point of the pattern is the largest for the 8 feature points because it tend to be guessed that the starting point is top when the pattern resembles the circle. Thus the user should register the pattern which does not start from top of the pattern on the screen.

B. Experimental results of biometric authentication using writing speed

1) Method of experiments: This experiment is conducted with 16 examinees including the regular user. The regular user registers the handwritten pattern, and repeats the authentication 20 times to adjust the parameters. And the other 15 examinees try the authentication 20 times for each patterns whose numbers of feature points are from 5 to 8 with changing the connecting patterns are known and unknown. The sketch of the experiments is shown in Fig.9.

These patterns are generated by the proposed system in the registration process of hand written patterns by some users. As mentioned in the previous section, the feature points without the line is presented to the examinees. 10 examinees who did not know the pattern tried the authentication 3 times for each pattern, thus each pattern is tried 30 times. All examinees experienced this system before in the experiments of previous system. Table 1 shows the result. With 4 feature points, one examinee is authenticated once, however with more than 5 feature points no examinees can be authenticated because they can not guess the pattern. The number of examinees who can identify the starting point of the pattern is the largest for the 8 feature points because it tend to be guessed that the starting point is top when the pattern resembles the circle. Thus the user should register the pattern which does not start from top of the pattern on the screen.

B. Experimental results of biometric authentication using writing speed

1) Method of experiments: This experiment is conducted with 16 examinees including the regular user. The regular user registers the handwritten pattern, and repeats the authentication 20 times to adjust the parameters. And the other 15 examinees try the authentication 20 times for each patterns whose numbers of feature points are from 5 to 8 with changing the connecting patterns are known and unknown. The sketch of the experiments is shown in Fig.9.

These patterns are generated by the proposed system in the registration process of hand written patterns by some users. As mentioned in the previous section, the feature points without the line is presented to the examinees. 10 examinees who did not know the pattern tried the authentication 3 times for each pattern, thus each pattern is tried 30 times. All examinees experienced this system before in the experiments of previous system. Table 1 shows the result. With 4 feature points, one examinee is authenticated once, however with more than 5 feature points no examinees can be authenticated because they can not guess the pattern. The number of examinees who can identify the starting point of the pattern is the largest for the 8 feature points because it tend to be guessed that the starting point is top when the pattern resembles the circle. Thus the user should register the pattern which does not start from top of the pattern on the screen.
C. Experiments with knowledge of connecting pattern

With knowledge of connecting patterns, the authentication becomes purely biometric authentication. The average of FRR and FAR with changing the number of feature points is shown in Fig.11. FAR is unacceptably high for less than 7 feature points. This system is not secure as biometric authentication if the connecting pattern is known by irregular users for less than 7 feature points. For the case of 8 feature points, FAR becomes less than 10%, however FRR becomes 30% for regular user.

D. Experimental results using dummy feature points

Next, the experiments using dummy feature points are conducted. In the experiments, one dummy feature point is added to the pattern with 4-6 feature points. The regular user and other 5 examinees try the authentication in 10 times for each number of feature points. At first, existence of the dummy feature point is not known to the examinees except the regular user, and same experiments are repeated with notifying existence of dummy feature points. The examinees are selected from the previous examinees who experienced this system without dummy feature points. The sketch of this experiment is shown in Fig.12. The experimental results are shown in table 2 and table 3. In the 1st trials, the examinees tend to pass all feature points because they does not know existence of dummy feature points, so they are not authenticated. In the 2nd trials, even if the examinees know existence of feature points, they can not be also authenticated. In Fig.13, Fig.14 and Fig.15, the causes of the failures are shown for the cases of 4 feature points, 5 feature points and 6 feature points respectively.

<table>
<thead>
<tr>
<th># of feature points</th>
<th>Regular user</th>
<th>Examinee A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

TABLE II. EXPERIMENTAL RESULTS USING DUMMY FEATURE POINTS (1ST TRIALS)

For the case of 5 or 6 feature points, the examinees pass dummy feature points for more than 90% of trials. From
this result, dummy feature points are effective to raise the security level. For case of 4 feature points, the biometric authentication using writing speed prevents the authentication, even if the examinees avoid the dummy feature points and pass the knowledge authentication using connecting pattern. On the other hand, the regular user may forget the position of dummy feature points, and may fail authentication with passing the dummy feature points.

V. Conclusion

In this paper, the authentication system which generates feature points automatically is introduced. The improvements of detection of feature points and dummy feature points are implemented to the system to raise the security level. As a result, if the connecting pattern is unknown, the security level is considered to be sufficiently high, however if the connecting pattern is known, the security level which provided by the biometrics using writing speed is not satisfying. However, it can avoid the authentication when the knowledge based authentication was broken by chance in the experiments. This may be improved with adding another biometric features obtained during writing pattern. The experience of the examinees who help this study may be bias to the experimental result.

As the feature work, the automatic generation or suggestion of the dummy feature points by system will strengthen the security level of knowledge based authentication. As mentioned before, biometric authentication using the writing pattern should be improved to be acceptable level without knowledge based authentication. Furthermore, the scale of the experiments was small. The experiments with more examinees and observation in long terms should be required.

REFERENCES