A Method for Authentication using Behavior Biometrics on WEB

Hiroshi Dozono¹, Naoto Yamasaki¹, Masanori Nakakuni²

¹ Faculty of Science and Engineering, Saga University, 1-Honjyo Saga, 840-8502 JAPAN
² Information Technology Center, Fukuoka University, 8-19-1, Nanakuma, Jonan-ku, Fukuoka 814-0180 JAPAN

Abstract—Recently, many WEB services are supplied from network, and many cloud systems are operated on the WEB. For accessing these services, authentication should be required, and as the conventional authentication method password authentication with inputting password in the WEB form is mainly used. However password authentication involves some issues. For this problem, we propose a biometric authentication method which can be used on the WEB. In this paper, we propose an authentication framework using HTML5, and implemented the authentication method using the biometrics obtained from handwritten pattern using HTML5.

Keywords: Biometrics, Authentication, WEB application, Touch panel, HTML 5

1. Introduction

Recently, large amount of data is stored on the network system, and are accessible from WEB because of the growth of the cloud system. And many WEB applications are supplied from internet such as office applications. On the WEB, the password authentication method is mainly used because the conventional authentication system can only handle static data such as password. However, password authentication method involves some issues. For example, password can be stolen easily because the password is a mere string, and may be guessed from personal information like birth day or name of the family.

For this problem, we introduce the biometric authentication method which can be used on the WEB. The biometric authentication method can be classified in two types: Biometric authentication method using biological characteristics and Biometric authentication method using behavior characteristics. In this paper, we use biometric authentication method using behavior characteristics obtained from touch panel because it does not need additional hardware for obtaining biometric features. We proposed the biometric authentication method using touch panel in [1]. This method is implemented as the standalone application on iOS. In this paper, we implemented this system using HTML5, which can be executable on multi-platform system using WEB browser.

2. 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(Figure 1). 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.

3. Authentication System using HTML 5

HTML5 is the advanced version of Hyper Text Markup Language (HTML). HTML5 is the markup language, which consists of HTML, Javascript and CSS. HTML is used to define the contents of WEB pages, CSS is used to define the layouts of WEB pages. Javascripts realize the dynamic WEB pages which are required to implement the authentication system with behavior biometrics. Using these features, the control of animations, storage of data in local system, and socket communication via network can be implemented using HTML 5. Furthermore, a method, which is named Canvas, is provided for drawing shapes in real time, and we use this method for implementing authentication system.

3.1 Implementation of authentication system using HTML 5

In many WEB based system which requires authentication, password authentication is applied. The password is static information, thus it can be compared with registered password on server side which is implemented in server side scripts, such as PHP, Perl. However, it is difficult to implement the authentication method using dynamic data such as behavior biometrics because of the execution speed of server side script or the delay concerning the network. For this problem, the authentication method which uses client side scripts such as HTML5 or Java which can measure the dynamic data in real time is considered to be effective.

For implementing authentication system using HTML5, the security of the data used for authentication should be considered. The simplest implementation is shown in Fig.2. When the user requests the authentication, the WEB application including the authentication program is sent from the server to the user client, and executed on the client. Then, the measured biometrics and the registered biometrics stored in the local clients is compared, and if they are matched, the secret code which notifies the success of authentication is sent to the server, and finally the server starts service to the user. This method is simple, and the authentication data can be stored in the local clients. Considering the leakage of the authentication data from server, it is ideal to store authentication data in local clients. However, this method is critical because HTML 5 source program used for authentication can be easily obtained. If the source code is obtained, it is easy to make dummy program which mimics the successful authentication. If the HTML 5 source code can be encrypted, and can be executed directly in browser using encrypted code, this problem can be cleared, however the encryption of source code is not implemented to HTML 5 yet.

For this problem, the authentication method shown in Fig.3 is proposed. When the user requests the authentication,
to the server via encrypted channel, and it is compared with the registered data stored in the server. If they are matched, the server starts service. Using this method, the WEB application sent from the server just measures the behavior biometrics, and send the data to server, thus the attacker can not mimic the successful authentication without the successful biometric data even if he can get the source code of HTML 5 program. For this system, the special care will be required for registering the biometric data on server. Because the attacker may mimic the user in registering the data. For this problem, the user should be authenticated using another method when he register the data.

Fig.4 shows the another implementation. The difference from the system shown in Fig.3 is the place for storing registered data. The system in Fig.4 stores the registered data encrypted on the server in local clients, end it to the server, and the authentication is executed on the server. There are some discussions for which is better to store the data on the local clients and the server depending on the characteristics of systems. Our method can be implemented in both type. Of course, the registered data is needed to be encrypted on the server, and needed to be registered after authentication of the user using another method.

4. The System Which Generates Feature Points

In [1], we reported a system which generates feature points. As shown in Figure 5, this system generates feature points automatically from the freehand curving line. These points are displayed on the touch panel during authentication to increase reproducibility of the registered curving line. With displaying the points without curving line, the pattern of connecting the points is used as knowledge factor for authentication. The pen speeds between the points are used as behavior factor for biometric authentication. The feature points are generated on the points which have large feature value. We used 2 factors to detect feature points. The first factor is inner products between the scanned points, and the sharp change of the direction of the line is detected. The second factor is curvature of the line, and the loose change of the direction is detected. After detecting feature points, the dense feature points are integrated as shown in Fig.6 because too many feature points disturb the smooth drawing of the line.

The advantage of this method is small number of parameters compared with conventional method. The conventional method for matching handwritten patterns with registered data uses all scanned points. Thus, it needs complex computations, and needs the transmission of large data for authenticating on the server. Our method uses some parameters which represent the pen speed between feature points, thus the computation becomes simple, and needs to transmit small number of data.

5. Experimental Results

5.1 Experimental results using HTML 5

To examine the detection of feature points using HTML5, the experiments are conducted. In this experiments, the server-client model is not used. The experiments of detecting the feature points and authentications are conducted in the client using HTML 5.
As mentioned in the previous section, the strength of the security of the connecting pattern of feature points as knowledge factor and the security of the behavior biometrics of the pen speeds between the feature points are examined with the experiments of authentications. Both of them are obtained clients and authenticated using HTML 5.

As the integrated environment for developing HTML 5 program, we used ApranaStudio 3. And we specified Chome as default browser because the operation of HTML 5 is different for each browser.

In the experiments, one user, who is one of the authors, registered his handwritten pattern, and the registered user and another 3 users (User A, User B and User C) examined the authentication. To compare the strength of security of the combinations of knowledge factor and behavior biometrics with that of only using behavior biometrics, the experiments are conducted without notifying connection pattern, and with notifying connection pattern. Figure 7 shows the registered patterns. For Pattern 1, pattern 2 and pattern 3, four, six and nine points are generated, and the number of feature values used for authentication are three, five and seven respectively. The difference of the authentication results with number of feature points is examined.

Table 1 shows the results using both of the knowledge factor of connection patterns and biometric features of pen speeds without notifying connecting patterns. For all user, the authentications are repeated in ten times. Without notifying connecting patterns, all of non-registered users could not find right connecting patterns, so none of them can successfully authenticated for all patterns. However, the rates of successful authentication decreases with increasing the number of feature points.

Table 2 shows the results using biometric features only with notifying connecting patterns. Without knowledge factor, the strength of security for the non-registered users becomes worse. Especially for Pattern 1 with small number of feature points, almost half of authentication of non-registered users are successful, because too small number of feature values (3 values) is considered to be useless. With increasing the number of feature points, non-registered users become hard to be authenticated. However, for pattern3, the registered user can authenticated only half of trials. Among the non-registered users, the rates of User C is higher than User A and User C, because User C was authenticated just after seeing the successful authentication of registered user.

5.2 Experimental results using HSP

For the comparison, we conducted the authentication experiments using HSP scripting language. HSP is the scripting language which is implemented to multi-platforms such as Windows, Linux, MacOS, and it can be used on the mobile devices such as android and iOS using mobile version of HSPDISH. HSP have many kind of instruction set, and it is relatively easy to make the application which uses system level operations. HSP can even obtain the pen pressures if the device is equipped with the touch panel which can detect pen pressure. However, HSP is basically executed in the local system as application, thus it can not be used for implementing WEB application. As one of script interpreter, we compared the results of HTML with that of HSP.

Table 3 shows the results using both of the knowledge factor of connection patterns and biometric features of pen speeds without notifying connecting patterns using HSP scripts. The users and registered patterns are not identical to those used in the previous experiments. Without notifying connecting patterns, non-registered user can not found connecting patterns as same as in the previous experiments. The rate of acceptance of registered user was better than that of previous experiments.

Table 4 shows the results using biometric features of pen speeds only with notifying connecting patterns using HSP scripts. There is not clear difference between the results using HTML 5 and HSP, however the results of
Table 4: Result of authentication without notifying connecting patterns

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Registered user</th>
<th>User A</th>
<th>User B</th>
<th>User C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern1 (6 points)</td>
<td>1.0</td>
<td>0.3</td>
<td>0.1</td>
<td>0.4</td>
</tr>
<tr>
<td>Pattern2 (7 points)</td>
<td>0.9</td>
<td>0.2</td>
<td>0.0</td>
<td>0.3</td>
</tr>
<tr>
<td>Pattern3 (8 points)</td>
<td>0.7</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
</tbody>
</table>

HSP is considered to be a little biased to acceptance of authentication. The difference comes from the tuning of the parameters. Considering this point, the performance of HTML5 and HSP is considered to be almost same.

6. Conclusion

In this paper, we proposed the biometric authentication method using behavior biometrics in WEB Application. The authentication system generates the feature points automatically, and both of the knowledge factor of the connecting pattern of feature points and the biometric features of the pen speed between feature points are used for authentication. For this system, we proposed the authentication system which comprised of the authentication server and client which measures the biometric feature using HTML 5 in real time. We examined the performance of generating feature points using HTML 5, and conducted authentication experiments. The performance of the authentication is almost same as those of HSP which is implemented natively to the computer. From the experiments, non-registered users can not be authenticated without notifying connecting pattern, and they can be partially authenticated with notifying pattern. However this method may be the abuse to the hacker even if the connecting pattern is known.

As the future work, the authentication accuracy should be more strengthened. In this paper, simple algorithm using threshold is applied for the fair evaluation. The more smart algorithm should be examined as authentication algorithm. And, we use pen speeds only as behavior biometrics. Using another biometrics, such as curvature between feature points, may help to improve the accuracy.

References