3D Gesture Base Authentication of Smart Phone

Author’s Details:

(1) Wenjun Hu – Professor - Information Engineering Department Huzhou University
huwenjun@zjhu.edu.cn  
(2) Bigyan Poudel - Information Engineering Department Huzhou University
bindasbiku@yahoo.com  
(3) Minmin Miao – Professor, Information Engineering Department Huzhou University
miaomin2@gmail.com

Abstract

In today’s world mobile device has been a basic need of life. People use their mobile devices daily basis works. Due to this, their information data along with bank information, payment information, social media information, and password are saved in the mobile phone which creates security threads. Those important data can be stolen easily and can be misused by other people.

In this study, we are introducing a new method of authentication for the smartphone which includes the user interaction on their smartphone. In other words, we can say 3D gesture base authentication process where the user will use their hand motion in the air and can do authentication easily. The help of an embedded 3D accelerometer and gyroscope which is in the smartphone along with unsupervised machine learning algorithms called Dynamic Time Warping and Hidden Markov models has been used to make the authentication more secure and user friendly.

KeyWords: Accelerometer, Gyroscope, Authentication, Hidden Markov model, Dynamic time warping

1. Introduction

Mobile phone helps us in our daily lives. The fundamental advantage of these gadgets is that we can carry them around with us and use them nearly anywhere and at any time: we can check our e-mails, read online news, chat via social networks, and do a variety of other things while on the go. Mobile devices generate and retain a large amount of sensitive personal data in order to assist their owners. Recently, two factors have emerged as critical to the success of mobile devices: competent hardware and mobile internet connection. Mobile devices are becoming widespread; however they may be accessed by unauthorized individuals. It is critical to build and deploy trustworthy authentication techniques to avoid misuse. PINs and passwords, which are widely used knowledge-based techniques, are not well suited for mobile devices due to the restricted capabilities of user interfaces.

Mobile phone helps us in our daily lives. The fundamental advantage of these gadgets is that we can carry them around with us and use them nearly anywhere and at any time: we can check our e-mails, read online news, chat via social networks, and do a variety of other things while on the go. Mobile devices generate and retain a large amount of sensitive personal data in order to assist their owners. Recently, two factors have emerged as critical to the success of mobile devices: competent hardware and mobile internet connection. Mobile devices are becoming widespread; however they may be accessed by unauthorized individuals. It is critical to build and deploy trustworthy authentication techniques to avoid misuse. PINs and passwords, which are widely used knowledge-based techniques, are not well suited for mobile devices due to the restricted capabilities of user interfaces.

2. Methodology

To assess the gesture-based user authentication system, user research was undertaken. The user research was separated into two parts in order to properly investigate different dimensions. Stage 1 investigated the
feasibility, usability, and user perception. This stage is known as Proof-of-Concept-Study. This stage's participants all played the role of genuine users. The primary purpose of this stage is to investigate feasibility and usefulness. The participants attempted to create selected motions from the Proof-of-Concept-Study in the second step. This stage is known as Forgery-Study.

2.1 Gesture Recording

The user authentication system based on gestures is intended for use on mobile devices. In this case, we're using Android Studio and Java to create an application that collects data for the patterns. The data acquired when sketching the pattern in the air will use the x, y, and z coordinates from the embedded accelerometer and gyroscope sensors. The user can use one handed to draw the patterns as they required. This application was installed and run to collect data in Huawei NZONE, HONOR and xiaomi which was mostly used by the users in the recent time. Here the data starts to collect after the application was started and different patterns were drawn various times continuously and those data were collected in the phone storage memory of the smartphone.

Fig 1: App to show and record the accelerometer and gyroscope data

The accelerometer sensor of that smart phone collects the value of acceleration of the device along each axis, while as the gyroscope sensor of the device records the values while the device rotate around the axis. The accelerometer values include the entire measured acceleration, which takes gravity into account. Because the gesture is built such that the rear of the device points primarily to the floor, the influence of gravity is primarily stored in the z-axis.

Figure2 :X,Y,Z accelerometer (up) and gyroscope (down) record for triangular gesture.
2.2 Used Pattern and Data
The patterns we used to collect the data were circle, triangle, wave, eight. We collect these data. For taking the data we use the mobile phone in one hand and move the phone and draw the circle, triangle, wave and eight once at a time and collects those data given by the accelerometer and gyroscope sensor. When authentication is necessary, the user is likely to hold the device in this manner. Following it, the user is likely to continue interaction in the same posture. As a result, this posture was chosen as the starting and end position of all planned gestures, ensuring that authentication does not need any extra motions prior to contact that are not part of the gesture.

To make the result better different users were used to draw the similar patterns by making the difference in the timing of drawing the pattern, size of the pattern also far from the body and near to the body.

First 15 data which was recorded while drawing the circle pattern in the air are as follow.

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>285</td>
<td>-6.389555</td>
<td>-6.343307</td>
<td>3.508835</td>
<td>0.072617</td>
</tr>
<tr>
<td>2</td>
<td>289</td>
<td>-6.331200</td>
<td>-6.302841</td>
<td>3.494553</td>
<td>0.068878</td>
</tr>
<tr>
<td>3</td>
<td>294</td>
<td>-6.276200</td>
<td>-6.324625</td>
<td>3.489792</td>
<td>0.067810</td>
</tr>
<tr>
<td>4</td>
<td>299</td>
<td>-6.292892</td>
<td>-6.279037</td>
<td>3.530258</td>
<td>0.062469</td>
</tr>
<tr>
<td>5</td>
<td>304</td>
<td>-6.285751</td>
<td>-6.281418</td>
<td>3.427962</td>
<td>0.061935</td>
</tr>
<tr>
<td>6</td>
<td>309</td>
<td>-6.259567</td>
<td>-6.269516</td>
<td>3.537399</td>
<td>0.056595</td>
</tr>
<tr>
<td>7</td>
<td>314</td>
<td>-6.242905</td>
<td>-6.245712</td>
<td>3.523117</td>
<td>0.052322</td>
</tr>
<tr>
<td>8</td>
<td>319</td>
<td>-6.228622</td>
<td>-6.281418</td>
<td>3.613571</td>
<td>0.045914</td>
</tr>
<tr>
<td>9</td>
<td>324</td>
<td>-6.238144</td>
<td>-6.324625</td>
<td>3.597672</td>
<td>0.040573</td>
</tr>
<tr>
<td>10</td>
<td>330</td>
<td>-6.228622</td>
<td>-6.293320</td>
<td>3.482651</td>
<td>0.033896</td>
</tr>
<tr>
<td>11</td>
<td>334</td>
<td>-6.271469</td>
<td>-6.326645</td>
<td>3.563583</td>
<td>0.026154</td>
</tr>
<tr>
<td>12</td>
<td>339</td>
<td>-6.285751</td>
<td>-6.383774</td>
<td>3.568344</td>
<td>0.015472</td>
</tr>
<tr>
<td>13</td>
<td>344</td>
<td>-6.316696</td>
<td>-6.367111</td>
<td>3.454086</td>
<td>0.007996</td>
</tr>
<tr>
<td>14</td>
<td>349</td>
<td>-6.342880</td>
<td>-6.457565</td>
<td>3.451766</td>
<td>0.005157</td>
</tr>
<tr>
<td>15</td>
<td>355</td>
<td>-6.347641</td>
<td>-6.436142</td>
<td>3.389816</td>
<td>-0.002151</td>
</tr>
</tbody>
</table>

All the data measure by the acceleration and gyroscope are as follow:

\[
A^t = \{(X^1_t, Y^1_t, Z^1_t), \ldots, (X^j_t, Y^j_t, Z^j_t), \ldots, (X^n_t, Y^n_t, Z^n_t)\} \quad (2.1)
\]

\[
G^t = \{(X^1_t, Y^1_t, Z^1_t), \ldots, (X^j_t, Y^j_t, Z^j_t), \ldots, (X^n_t, Y^n_t, Z^n_t)\} \quad (2.2)
\]

Where, 
\( t \) = time for drawing pattern,
\( j \) = total repetition pattern,
\( n \) = end time for the pattern

3. Result
The suggested 3-D gesture basis authentication system achieves four of the eight qualities that uses behavioral biometrics should satisfy, including universality, collectability, acceptability, and minimality. Our experimentation aims to confirm the other four criteria: originality, permanence, circumvention, as well as accuracy, and speed of performance. We used the smartphone's 3D accelerometer and 3D gyroscope sensor to do in-field studies for this purpose. The outcomes of the tests are discussed and shown briefly here in this section.

3.1 Valid Sample Enrollment
During the thesis work four patterns were targeted and done by this 1200 users. Every one has given the six times to draw the pattern. The participants were thought to be legitimate users of the established mechanism. The samples from the third iteration of the real interpretation were chosen as the best enrollment samples. Because the user got average training in this iteration, those should be the most representative of all iterations. Only samples from iterations 3, 5, and 6 were utilized for validation. The first iteration was
omitted entirely since it was thought that these samples were prone to becoming outliers owing to the impact of training. As a result, 7200 samples were available for testing.

3.2 Used Forgery
Here we have used the Naive, Semi-Naive and Visual Forgery. For naive, the other persons except who draws the pattern were given to guess and drawn the pattern in random way. But for semi-naive the patten what the user drawn for the authentication was told to them and tell them to use that and try to draw the pattern which help little bit to the attack. While as the total different method was adopted for the visual forgery for this visual forgery the pattern drawn by the users were shown to them and tell them to draw same as they draw for authentication.

3.2.1 Hidden Markov Model
The result for the hidden markov model has been presented. The relevant levels for the HMM Model Acceptance Function range between 9 and 17. As predicted, the performance of First-order HMMs is affected by the number of states. Raising the number of states from 4 to 8, and then from 8 to 12, significantly increases overall performance, although models with 14 states perform just marginally better than models with 12 states. For First-order HMMs with 12 and 14 states, depicts the ROC diagram of all genuine interpretations vs Naive Forgery and SemiNaive Forgery.

HMMs show promise for authentication against Naive Forgery. A FRR of 23% can generate a FAR of 2%. Unfortunately, Semi-naive Forgery HMMs did not fare well, as even a FRR of 40% results in a FAR of 3%. A FAR of 3% may be considered safe enough for non-critical authentication applications, but the large FRR renders HMMs useless. It should be noted that Semi-naive Forgeries rely solely on visuals and description. An attacker was unaware of the individual interpretation.

Two constraints are placed on potential pathways by a first-order HMM: the path must begin in the first state, and only state transitions to the immediate successor are permitted. Nonetheless, a huge variety of potential pathways are still open due to these limitations. Imagine an attacker can generate a sample with constant values for each stream, and that the constant values are highly accurate representations of the emission distribution of a particular state. The most likely route would include a series of state changes to get to the desired state and then a series of changes to go back to that state.

3.2.2 Dynamic Time Warping
The DTW results are shown in the section below. To provide a certain degree of fairness for various scaled dimensions, the cost functions employed in the analyzed variations of DTW for the developed gesture-based authentication method are based on the Minkowski Norm. The table below displays the 3-dimensional accelerometer and 3-dimensional gyroscope's minimum and maximum values throughout the user research.
In every dimension, the rotating measurements range much outweighs the acceleration readings range. Nevertheless, there was no a priori information on the significance of the various sensors or the axis to discriminate between genuine and non-genuine samples. Consequently, it was assumed that each dimension was equally significant. The acceleration dimensions are scaled down by a factor of 6 to ensure fairness. Using factor 1, the rotational dimensions were rescaled. The Weighted Minkowski Norm takes these variables into account. Both the Euclidian Norm (k = 2) and the Manhattan Norm (k = 1) were researched for the gesture-based authentication technique. Whereas the Euclidian Norm determines the length of the vector that would link the compared feature vectors to a triangle, the Manhattan Norm determines the absolute difference for each dimension individually and adds the findings. The Manhattan Norm consistently outperforms the Manhattan Norm, according to the analysis of the findings. The Euclidian Norm is therefore inappropriate and is not included in the following. This might be because the Manhattan Norm's calculation of the distance between two vectors is always higher than or equal to the Euclidian Norm's calculation of the same distance. The enrollment samples' mean and standard deviation are used to compute the DTW threshold, although utilizing just the mean produces superior results. It was discovered that the range from 1.3 to 3.0 is adequate. Nevertheless, the performance of the DTW variations for the same Q varies greatly, necessitating a separate evaluation of this parameter for each version. Also, it was discovered that the DTW variations' authentication performance varies greatly. The table below displays the parameters of the three variations with the best performance. It was discovered that just one version performed comparably, and that variants with no slope limitation, i.e. (P = 0), outperformed nearly all others.

<table>
<thead>
<tr>
<th>Variant</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slope constrain</td>
<td>0 (R=30)</td>
<td>0(R=30)</td>
<td>1</td>
</tr>
<tr>
<td>Train mode</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Non-digononal alignment (H)</td>
<td>5</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Minkowski parameter (K)</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Selecting the least low enrollment sample (Training Mode 0) or computing the model based on integrating all enrollment samples (Training Mode 1 and 2) were two very distinct methods used to develop a model. Using DTW to locally align the data, Training Modes 1 and 2 compute the model based on the enrollment samples. Although Training Mode 2 employs expansion by distribution and compression by summation, Training Mode 1 uses duplication for expansion and averaging for compression. If no slope limitation was used, both methods performed remarkably similarly. Training Mode 1 performed somewhat better when a slope limitation was applied. Using the least expensive sample had unsatisfactory results. Another intriguing finding was that the comparable variants without a penalty beat all variants with an enforced slope constraint and a non-diagonal alignment penalty of 5. The ROC diagram for the three Nave Forgery and Semi-Nave Forgery variations that performed the best is displayed in Figure below. All variations perform quite similarly in terms of Naive Forgery for a FRR larger than 20%. At a FAR < 20%, variation 3, or slope constraint 1, performed quite well. With a FRR larger than 20%, the performance of variants 1 and 2 for semi-naive forgery is extremely comparable. Variant 3 performs a little less well in this range. With variation 2 showing a modest advantage, the results of variants 1 and 2 for naive forgery and semi-naive forgery are extremely comparable. These variations only differ in their Training Mode.
Due to variation 2's apparent superiority for a low FRR, Training Mode 2 appears to be better suited in this constellation for DTW without a slope limitation.

3.3 Comparing Both Model Together
The effectiveness of the DTW variation 2 and the 14-states HMM are compared in the sections that follow. Due to its apparent somewhat improved performance, DTW variation 2 was chosen. Figure following depicts the ROC diagram for various DTW and HMM variations.

3.4 Infulance Training:
The forger eventually produced the first batch of forgeries. To capture the second repetition, same method was repeated. The second iteration should thus perform better as there was more time for learning and training.

After training the model, we find that the combination of the Hidden Markov model and Dynamic Time Warping provides very high performance, with an attack probability of practically 0%. Our research shows that this concept is really practical. There are a number of potential causes for this, including ignorance, underestimating of hazards, access to services, and exposure of data. Moreover, authentication methods are frequently seen as hurdles that may be avoided. Although the current gesture-based authentication technique appears to be more suitable for mobile devices owing to the restrictions of the user interface and the interaction style, users are not always made aware of hazards and risks. The implemented gesture-based authentication mechanism's broad viability was established.
4. Conclusion

During this thesis we work through the authentication system mechanism called Gesture based authentication regarding the smart phones present in today's world using its embedded 3-dimensional accelerometer sensors combining with the 3-dimensional gyroscope sensors. We worked and came with the solution that using those embedded sensors its very continent, feasible also the user freely.

The 3-dimensional accelerometer and gyroscope sensors can capture precise and detailed information about the user's physical movements in three dimensions, providing a high level of accuracy and reliability in the authentication process. This allows the mechanism to detect and verify subtle variations and patterns in the user's movements, making it much harder for unauthorized users to mimic or spoof the user's gestures.

Moreover, the use of gesture-based authentication mechanism can offer several advantages over traditional authentication methods, such as passwords or PINs. For example, the mechanism can be more user-friendly and accessible, as it does not require the user to remember complex passwords or enter them repeatedly. Instead, the user can simply perform a pre-defined set of gestures, such as swipes or taps, to unlock their device or access specific applications or services.

Yet, this thesis's implementation and study of gesture-based user authentication employing a 3-dimensional accelerometer and a 3-dimensional gyroscope show promise for application with mobile devices. The gesture-based authentication method is particularly suited for mobile devices because it gets over the restrictions that the form factor of mobile devices places on the currently existing authentication techniques. Moreover, authentication may be carried out naturally and without the need of eyes. Also, the technique enables quick entry of a difficult secret, and a real user prefers to train rather than memorize.

5. Reference


x. Guerra-Casanova,Sanchez-Avila “Application of LCS Algorithm to Authenticate Users within Their Mobile Through In-Air Signatures.” Advanced Biometric Technologies. 256-280

