BHAS: Behavioral Handwriting Authentication System based on Deep Neural Network

Zhu Hongwei

April 20, 2019

Abstract

In this paper, we designed a simple and effective authentication system for smart phones with or without pressure sensor. Users are asked to write a specific Chinese character in order to authenticate. During this process, users' behavioral handwriting habit(such as speed and pressure) will be recorded. With behavioral information, we can overcome problems caused by password forgotten, shoulder surfing attack and feature imitation. We collected a large handwriting dataset collected from 152 subject to capture feature variability. The result shows that handwriting can easily and correctly discern user's data from others'. We also implemented a handwriting recognition demo on Android and did user experiments to evaluate the usability and security of the system.

1 Introduction

Thanks to the development of smart phones and the variability of powerful mobile applications, people can do almost everything they do on personal computer using a smart phone. A small smart phone can store a large amount of user's data, including contact list, chatting records, trade information ,browsing history, and even confidential documents. If a smart phone is stolen or faced to unauthorized access, the data kept in it is easily to get, which can possibly lead to privacy violation, property loss, or more seriously, leak of confidential information. Thus it can be seen that the security of smart phones becomes increasingly important.

As the frequency of people's using smart phones increases rapidly, they probably unlock them dozens of times a day. According to the survey made by Strategy Analytics, a famous statistics institution, Android users unlock their phones on an average of 65.8 times a day. The most frequent time slot to unlock their phones is from 14 p.m to 17 p.m, when most of people are in public places, 14 times on average. So the necessity of designing a secure and user-friendly unlock pattern is obvious. Since smart phone was invented, people have designed textual password, PIN, graphic password, fingerprint unlock, facial unlock, etc. These various unlock patterns tried their best to protect users' security and ensure convenience at the same time, however, they all have some insoluble problems more or less.

Traditionally, textual password has been used in the last few decades and has been proved to be robust enough to resist blind attack. However, the vulnerabilities of textual password are also obvious, if password is too short and simple, it will be easy to guess, if it is too long and complex, it will be easy to forget. So it seems to be difficult for users to achieve a trade-off between security and memorability. To conquer the limitation of textual password, graphic password is devised and put into use for the sake of memorability. Unfortunately, shoulder surfing attack occurs frequently when users unlock their devices in public places. The password can be peeped by other people nearby or recorded by surveillance camera deliberately or unintentionally. This problem is difficult to overcome with such method. A few years ago, TouchID and FaceID, which are based on user's biometric features are proposed by Apple. These two methods are considered to be secure for a long period of time, for biometric features are absolutely unique and are unable to be intimated by anybody else. However, it is reported that with capacitance pen and tape, TouchID can be cracked at an accuracy rate of 95%, according to an experiment carried on by NVIDIA Corporation. Meanwhile, with 3D print technique, a Vietnam Corporation generated fake human face, Apple's FaceID facial recognition system successfully. Therefore, TouchID and FaceID, which are based on biometric features, are not entirely secure as well.

In 2017, Xi'an Jiaotong University designed a multi-touch authentication based on both biometric and behavioral information, and using machine learning algorithms to perform classification. Based on behavioral features, considering both security and usability, we come up with an idea of using user's handwriting trace as behavioral information that is resistant to attacks mentioned above, since everyone's writing habit is not identical and unable to mimic by other people or machines.

Contributions

2 Related Work

With the help of various kinds of sensors embedded on smart phones, more and more biometric and behavioral features can be captured, and these features can be applied in authentication. At present, many researchers and organizations have worked out some authentication methods and put them into practical use.

Touch ID: Touch ID is a fingerprint recognition feature, designed and released by Apple Inc., that allows users to unlock Apple devices, make purchases in the various Apple digital media stores, and authenticate Apple Pay online or in apps. The theory behind it is that the ridges of a person's fingerprint is unique and unchangeable. It can be considered that fingerprints are the natural biological code of human, which cannot be duplicated or counterfeited. The sensors collect features of fingerprints and save them in the form of mathematical expressions. Finally, the system will compare the fingerprint acquired to fingerprints registered before by computing the matching rate between them, and decide whether to unlock the screen. The computing power of smart phones are so powerful that the process above takes less than 0.5 seconds. The authentication is convenient and secure in most cases. However, the sensors will not be able to collect the image correctly when users' hands are wet or sweaty. And with modern technology, the fingerprint image can be counterfeited with a tape and a capacitance pen. In 2017, New York University put forward "MasterPrint" fingerprint, which can unlock smart phones with a 50% success rate. In 2018, GAN made "DeepMasetPrints", the success rate of unlocking smart phones reached up tp 76%. Therefore, Touch ID has its own vulnerabilities, and is not as secure as before.

Face ID: Face ID is a facial recognition system designed and developed by Apple Inc.. The successor to Touch ID, the system allows biometric authentication for unlocking a device, making payments, and accessing sensitive data, as well as providing detailed facial expression tracking for Animoji and other features. When a face is approaching the camera, the dot projector generates 30,000 luminescent spots and projects onto user's face. By returning array formed by spots to infrared camera, the system can construct a 3D model precisely and identify the user by comparing the facial data registered before. This method has a higher security and usability, because the error rate of authentication is less than 1 PPM. However, this authentication is less useful for kids under 10, for their facial features are not fully formed. In 2017, Bkav, a Vietnam Corporation, claimed to crack Face ID successfully by using a mask.

Multi-touch: Multi-touch authentication is a method put forward by Xi-an Jiaotong University. Multi-touch is based on the mixture of biometric features and behavioral features. It collects users' hand geometry, including size of hand and space between fingers, and habits of swipe fingers, including velocity, pressure and angle. Combining biometric and behavioral features, using machine learning algorithms, the accuracy of recognition is very high. However, the method is not easy to perform on a small phone screen. Some screens are not big enough to contain four fingers. So it is unfriendly to users' behavior. To solve the problem, users have to use three or less fingers to swipe across the screen. In this case, the EER will increase from 2% to 7.7%, for the number of biometric features is reduced.

3 Our Scheme

The concrete method is to take users' handwriting habits as features to make identification. Based on the method, we designed an authentication system which is referred as BHAS, the abbreviation of Behavioral Handwriting Authentication System. BHAS contains the following three phases:

- **Register phase:** In this phase, users are asked to write a specified Chinese character on the screen 10 times, the system will capture and record users' behavioral features at fixed intervals and transformed them into data.
- **Training phase:** The data collected in the previous phase will be sent to cloud server as positive samples. The By comparing to other data in database, the system will be able to classify these data into two classes – belong or not belong to the users. Because the database is huge, this process can be time-confusing, so in this phase, users need to wait a little time. After the training finished, the training model will be saved in cloud database for further use.
- **Login phase:** In this phase, users need to write the character which was set in register phase, then the system will record the whole process and determine whether it is performed by the user him/herself. Since the training model has been saved in the previous phase, the login time requires much less time to perform.

Flowchart is here...

3.1 Feature Selection

Because handwriting is a continuous process, the state at one moment is highly relative to that at previous and next moment, it is natural to collect time series data as our dataset. We capture a fixed time spots every $20ms$ and record the information of these time spots to characterize the whole handwriting process approximately. To get as distinct features as possible, we select the following behavioral features:

Relative Position: We define the first recorded touch spot as the origin of coordinates, so all the following spots' positions can be considered as the relative position of the first spot. We use X and Y coordinates to represent each spot's position. Knowing the coordinates and interval, we can figure out the average linear velocity between any two spots.

Fig 1 is here...

Pressure Value: We capture each spot's pressure value. The pressure you use in handwriting process will be recorded and transferred into numerical values. If the user's phone is not pressure-support, the pressure values are all zero.

As mentioned above, each spot includes three numerical values: XY coordinates and pressure value, and the sequential form of data also implicate the time and speed information, which do not manifest directly.

The average time a person takes to write one word is about 3 seconds, so we decide to collect a spot's data every 20ms, and collect 150 times in total. So the whole timescale to write a character is 3 seconds.

Altogether, in one handwriting, we have 3 features in each time spot, and the number of spots is 150. That means one handwriting has 450 features in total. Like normal sequential data, each spot is relative to the adjacent spots, so the data series should be taken as whole.

Fig 2 is here...

3.2 Algorithms

4 Experiments

4.1 Security Experiment

The security experiment aims to examine and analyze the security of the method. It mainly focuses on login success rate of illegitimate users. The experiment contains 4 steps as following:

4.1.1 Experiment Setup

In order to collect data from users, we designed an app based on Android. The APP requires users to register at a nickname and a unique phone number. When a user begin to write a character on the screen, the APP starts to collect the data of one spot every 20ms, and collect 150 times. So the whole timescale to write a character is 3 seconds. If the time is expired but the writing is unfinished, the system will abandon the data after the 3rd second, only recording the first 150 spots. If the writing is finished but time is not expired, the system will automatically complement the data to 150 with the data of last spot recorded.

4.1.2 Dataset

We recruited 152 subjects from NUAA(Nanjing University of Aeronautics and Astronautics) students and some members of the community. We asked them to download the APP mentioned above. First they need to write a specific character "Fang" 10 times. We define this process as ***a writing***. When finishing writing a character, they need to click the "Submit" button and the handwriting data will be recorded. Then they need to write a self-defined character 10 times, and repeat the steps above. Finally the APP will generate a .csv file named after user's nickname, user's phone number and the character the user written for each writing. These two .csv files will be saved and transferred to server side. Some people wrote more than 10 times, but none of them wrote less than 10 times. In total, we collected 1666 writings of the character "Fang" and 1666 writings of the self-defined character as dataset.

Fig 3 is here...

4.1.3 Implementation

First, we checked the dataset, finding that the value of XY-coordinates are much higher than the vale of pressure, and in a few of writings, the 150 pressure values are identical. By examining the source code of APP, we found that some smart phones are not pressure-supporting. To make the classification more accurate, we deleted the data with identical pressure values and regularize the data with the expression below:

Expr 1 is here...

After data cleaning and regularization, we select 151 samples, 30 of them are written by user A, which are considered as positive sample, labeled as 1, the rest are written by other users, considered as negative sample, labeled as 0. Then we randomly split the dataset into training set, containing 113 samples, and test set, containing 38 samples. Then we use KNN, SVM and LSTM and fed the training set to these models respectively. And use the test set to test their performance.

4.1.4 Results

The performance of these three models are in figure 3:

Fig 4 is here...

It is obvious that LSTM performs better than KNN and SVM.