Journal of Network and Computer Applications 53 (2015) 128–139

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Implementing multiple biometric features for a recall-based graphical keystroke dynamics authentication system on a smart phone

Chao-Liang Liu [a,b], Cheng-Jung Tsai [c], Ting-Yi Chang [d,*], Wang-Jui Tsai [d], Po-Kai Zhong [d]

[a] Department of Applied Informatics and Multimedia, Asia University, Lioufeng Rd., Wufeng, Taichung 500, Taiwan, ROC
[b] Department of Medical Research, China Medical University Hospital, China Medical University Taichung, Taiwan, ROC
[c] Department of Mathematics, National Changhua University of Education, No.1, Jin-De Road, 500 Changhua City, Taiwan, ROC
[d] Department of Industrial Education and Technology, National Changhua University of Education, No.1, Jin-De Road, 500 Changhua City, Taiwan, ROC

ARTICLE INFO

Article history:
Received 25 June 2014
Received in revised form
16 December 2014
Accepted 2 March 2015
Available online 14 April 2015

Keywords:
Authentication
Biometric
Keystroke dynamics
Touch screen
Graphical password
Android pattern lock

ABSTRACT

Keystroke Dynamics-based Authentication (KDA) is a type of behavioral biometric method. It verifies user identity via the keystroke features gathered from the keystroke events provided by users on a QWERTY keyboard. With the growing use of smart phones, the traditional keypad on mobile phones has been replaced by touch screen devices. The keypad-based KDA is no longer suitable for smart phones. This paper proposes a KDA system implemented using multiple biometric features applied to the pattern lock layout on a smart phone. Except for the time, pressure and size of the keystroke features presented in previous research, we additionally adopted a novel angle keystroke feature and determined the best combination of these features in a series of experiments. As the results show, with 10 training samples involved, the combination of time, pressure and angle offers the best utility (Equal Error Rate of 3.03%).

1. Introduction

With the development of mobile devices and the 3G mobile network, smart phones have assumed an important role in our life. Mobile phones allow Internet surfing, website login, gaming, stock investing, etc. Meanwhile, due to their convenience, most people store their personal information in their mobile phone. Once the phone is stolen or lost, the information can be accessed for malicious purposes by others. In the situations stated above, developing a reliable authentication mechanism for mobile devices becomes an essential research issue.

Authentication can be divided into three different types (Clarke and Furnell, 2007), specifically, knowledge-based, token-based and biometric-based authentication. Knowledge-based authentication verifies user identity by the information in the user memory (something-we-know), such as a password or PIN. This kind of authentication is convenient to use, but vulnerable to brute force attacks, dictionary attacks, shoulder-surfing attacks (Goucher, 2011) and smudge attack (Aviv et al., 2010). The token-based authentication identifies users via an object carried by the user (something we have), for instance, a SIM card or credit card. Biometric-based authentication identifies the user through the biometric characteristics of the user (something we are). There are two types of biometrics: physical and behavioral. Physical biometrics includes palm, fingerprint, and iris recognition. On the other hand, behavioral biometrics include the signature (Syukri et al., 1998), and keystroke dynamics (Araújo et al., 2005; Giot et al., 2011; Gunetti and Picardi, 2005; Hwang et al., 2009). Biometric features are difficult to lose, steal, or imitate due to their uniqueness. Among the biometric authentications, physical biometrics shows the best identification performance. Unfortunately, it requires advanced support of devices to achieve high discriminability, such as a fingerprint or iris scanner. In contrast, keystroke dynamics can be used to provide additional protection for password authentication due to their advantages of unobtrusiveness and the ability to adopt without any other supporting devices.

According to different verified sessions, KDA can be recognized as a static (Araújo et al., 2005; Chang et al., 2012; Clarke and Furnell, 2007; Haider et al., 2000; Hwang et al., 2009; Killourhy and Maxion, 2009) or continuous (Monrose and Rubin, 2000; Patrick, 2012; Zahid et al., 2009) KDA. Static KDA only verifies user identity at specific phases, such as the login phase. Continuous KDA verifies all the keystroke features generated during the session between the login and logout phase. It observes every operation of the user after the login phase by the keylogger, which might lead to privacy issues (Banerjee and Woodard, 2012).

Keystroke dynamics is a pattern recognition application. Like pattern recognition, they include feature gathering, sampling, and classification. Gaines et al. (1980) built the KDA system with a keystroke time feature. They also proposed that the structure of KDA should include feature gathering in the enrollment phase, classifier building in the training phase, and feature verification at

* Corresponding author.
E-mail address: tychang@cc.ncue.edu.tw (T.-Y. Chang).

http://dx.doi.org/10.1016/j.jnca.2015.03.006
1084-8045/

the authentication phase. For the enrollment phase, many studies have tried to reinforce the utility of KDA by improving the quality of keystroke features or using various features which could be gathered during keystroke behavior. Araújo et al. (2005) reported four time features that could be generated according to the key press time and key release events. We refer to the time between a key being pressed and released (Down–Up time, DU), the time elapsed between two successive keys being pressed (Down–Down time, DD), the time between a key being released to the next key pressed (Up–Down time, UD), and the time between two successive keys being released (Up–Up time, UU), respectively. Their experiment showed the best utility occurred when adopting the combination of DU, DD, and UD.

Before determining the feature used in the enrollment phase, the quality of the keystroke features should be considered. Cho and Hwang (2005) reported three characteristics of keystroke features, namely, uniqueness, consistency, and discriminability. The definitions are shown below:

- *Uniqueness*: The difference between the sample of legitimate users and imposters.
- *Consistency*: The similarity of the sample provided by legitimate users in the enrollment phases and authentication phases.
- *Discriminability*: The ability to identify legitimate users and imposters.

Cho et al. proposed a method of inserting pauses and cues into password input on a QWERTY keyboard. They asked users to enter the password with several pauses included in order to form an artificial rhythm. A metronome was adopted as a cue to make the keystroke features maintain their uniqueness and consistency.

After data gathering, the KDA system was able to build the classifier in the training phase using the collected samples. Many research papers applied various algorithms to implement their classifier using statistical (Boechat et al., 2006), fuzzy logic (Haider et al., 2000), neural network (Ahmed and Traore, 2014; Killourhy and Maxion, 2009; Uzun and Bicakci, 2012), Euclidian distance (Killourhy and Maxion, 2009; Monrose and Rubin, 2000), support vector machine (Giot et al., 2011) algorithm methods. In order to avoid burdening the user, the number of training samples (or training size) used to finish the classifier training should be considered. Therefore, Araújo et al. (2005) recommended that the number of training samples should not be larger than ten.

In the authentication phase, a well-trained classifier is adopted in order to verify user identity. For obtaining the accuracy of the authentication system, it is important to estimate both the imposter acceptance rates and the legitimate user rejection rates. The former should be estimated under the situation of assuming that the imposter possesses the password of the legitimate user. For comparing the utility of different KDAs, Golfarelli et al. (1997) suggested that every biometric authentication system should be evaluated by the following two criteria, where the values of these criteria would change according to the threshold value of the system:

- *False Rejection Rate* (FRR): The percentage of the system rejecting legitimate users while they attempt to login.
- *False Acceptance Rate* (FAR): The percentage of imposters accepted by the system while they attacked.

These two criteria can form the following three:

- *Equal Error Rate* (EER): EER value is obtained when FRR equals FAR. This value is usually used to present the entire system utility, which serve as the criterion for comparing various authentication systems.
- *Zero False Rejection Rate* (ZeroFRR): ZeroFRR indicates the FAR value when FRR equals zero. If the system modifies the threshold to meet ZeroFRR, then no legitimate user should be treated as an imposter at the same time.
- *Zero False Acceptance Rate* (ZeroFAR): ZeroFAR represents the FRR value as FAR equals zero. This value shows the probability that the system rejects the legitimate user while it can resist every imposter.

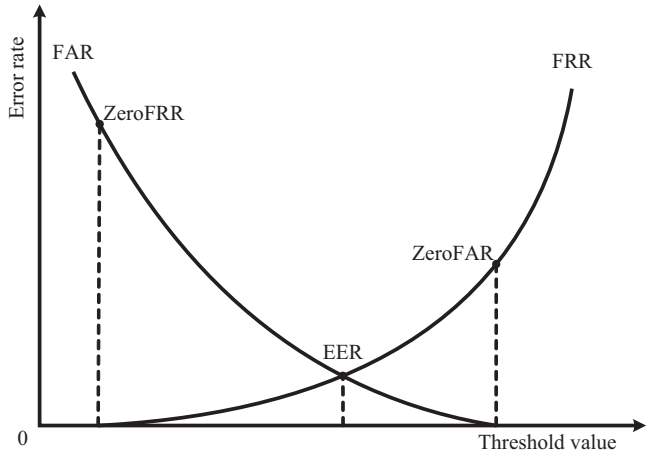

Fig. 1. Five evaluation criteria.

Observing the five evaluated criteria in Fig. 1, ZeroFRR and ZeroFAR can only represent the ability of the system to judge user identity. However, the EER value is generated by modifying FAR and FRR. This value shows both the abilities of rejecting legitimate users and of accepting imposters for the entire system. Thus, this paper adopted the EER value to evaluate our system utility.

Except for the QWERTY keyboard, many research papers (Clarke and Furnell, 2007; Clarke et al., 2003; Hwang et al., 2009; Karnan and Krishnaraj, 2012; Maiorana et al., 2011; Tsai et al., 2014) adopted keystroke dynamics for handheld mobile devices. However, with the popularity of smart phones and touch screens, mobile phones no longer provide keypads on the device. The alternative touch screen has a virtual keyboard to perform keystroke dynamics. Consequently, users tend to choose simple text-based passwords on the smart phone, which has a relatively smaller screen (Nauman and Ali, 2010). This practice leads to the bad performance of KDA on mobile phones. Therefore, many research papers proposed a graphical password to replace the traditional text-based password on handheld mobile devices (Angulo and Wästlund, 2012; Chang et al., 2012; Jansen, 2004). The *Picture Superiority Effect* (PSE) indicates that humans have a stronger ability to memorize and recognize pictures than text. Shepard (1967) prepared a pair of pictures or sentences to ask participants to recognize which one of the pictures or sentences had been presented in previous experiments. He discovered that the recognition rate of pictures is higher than sentences by a recognition experiment. Even when the experiment was hosted again in the following week, the recognition rate was 87% for hundreds of pictures. Standing (1973) adopted 10,000 pictures in the experiment and reported only a 17% rate of misrecognition. These experiments proved that the human recognition ability for pictures is better than text.

Jansen (2004) proposed a graphical password authentication method on a *Personal Digital Assistant* (PDA). A picture is equally divided into 30 blocks on a screen for the user to click. The password is generated according to the click order. This kind of graphical password authentication is called recognition-based, and it makes the user produce the same input result from their memory of the picture location. Once the preference of the user is well-known by the imposter, the password may be obtained by a guessing attack. Another type of graphical password authentication is termed as