Expert Systems with Applications 42 (2015) 6286–6294

Contents lists available at ScienceDirect

Expert Systems with Applications

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

Intelligent biometric pattern password authentication systems for touchscreens

Orcan Alpar [*]

Center for Basic and Applied Research, Faculty of Informatics and Management, University of Hradec Kralove, Rokitanskeho 62, Hradec Kralove 50003, Czech Republic

ARTICLE INFO

Article history:
Available online 30 April 2015

Keywords:
Biometric authentication
Touch pattern
Neural networks
Adaptive neurofuzzy
RGB Histograms

ABSTRACT

Given the recent developments in alternative authentication interfaces for smartphones, tablets and touchscreen laptops, one of the mostly selected method is the pattern passwords. Basically, the users that prefer this method, draw a pattern between the nodes to open the lock in lieu of entering an alphanumeric password. Although drawing a pattern seems easier than typing a password, it has a major security drawback since it can be very easy to be stolen. Therefore, this paper proposes some novel theoretical ideas with artificial intelligence methods, to improve security of pattern password authentication, using touching durations as biometric traits. What we put forward is the utilization of three different neural network based algorithms to verify logins with one novel histogram-based technique in a hidden interface for enrollment, training and verification.

Inspired by the keystroke recognition models, the touch time and durations are extracted to create a ghost password. Moreover, the nodes are colored depending on the touch duration in the hidden interface and subsequently the colored images are exported. As a result of training session, the system discriminates real attempts from frauds using artificial neural networks (ANN), adaptive neuro-fuzzy inference systems (ANFIS) and Red–Green–Blue (RGB) Histogram methods in verification phase. The results are greatly encouraging that we reached 0% of false accept rate (FAR) for 80 fraud attacks with 16.5% false reject rate (FRR) of unsuccessful authentication for the 80 real attempts when started with interval checking algorithm. Moreover, to reduce this FRR, we utilized neural network based systems and consequently with ANN, we achieved 8.75% equal error rate (EER), with ANFIS, 2.5% EER for 85% proximity and finally with RGB Histogram method, we attained 7.5% EER.

© 2015 Elsevier Ltd. All rights reserved.

1. Introduction

In recent years, the pattern password authentication interfaces have introduced subsequent to emergence of touchscreen devices such as phones, tablets and touchscreen computers. Since some keyboard interfaces are certainly very small to enter a password, nowadays pattern password is one of the commonly used authentication method. Due to its imitability, pattern passwords however have some security issues, regardless how complicated the passwords may be. Even without paying special attention, pattern passwords could easily be recognized since the authentication programs generally have a kind of weakness that the password patterns are shining brightly or at least changing colors. Considering this salient effect, the password with cyan color as an example of colorization and illumination could be seen in Fig. 1.

Additionally, the pattern password authentication is supposed to have medium security according to the security options of Samsung Duos 8262, the basic model for this research, where the alternatives vary from swiping (no security) to alphanumeric password authentication (maximum security). Therefore, enhancing the pattern password authentication system seems to be a crucial requirement without altering the dynamics. Considering the dynamics of pattern password authentication, what we put forward is a novel idea that utilizes the touching durations on the nodes of the pattern password as the main biometric trait, with several classification methods based on artificial intelligence tools.

Biometrics is the term introduced in 1890s (El-Abed & Charrier, 2012) that is originated from fingerprint classification systems (Cole, 2004) and dealing with the unique physical, biological, behavioral and habitual characteristics of human-beings. Biometric authentication systems refer to intelligent recognition and identification of individuals, to discriminate real and fake attempts based on unique characteristics of users. In the past decade, it is possible to find numerous researches in various subtopics

[*] Tel.: +420 732 764683.
E-mail address: orcanalpar@hotmail.com

http://dx.doi.org/10.1016/j.eswa.2015.04.052
0957-4174/© 2015 Elsevier Ltd. All rights reserved.

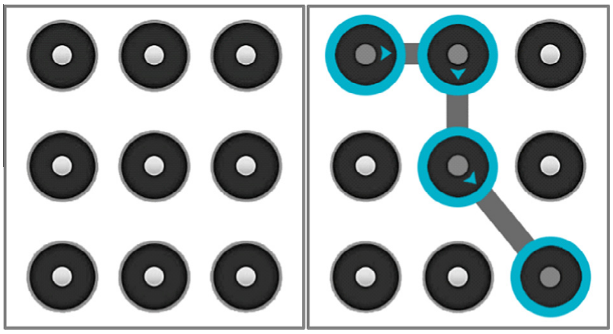

Fig. 1. Password patterns (left: idle pattern, right: recorded pattern).

consisting of biometrics, intelligent recognition and authentication such as Clarke and Furnell (2007a, 2007b), Fan and Lin (2009), Jain and Nandakumar (2012), Shen, Cai, Guan, Du, and Maxion (2103), Feher, Elovici, Moskovitch, Rokach, and Schclar (2012) and Simoens, Bringer, Chabanne, and Seys (2012).

One of the common biometric recognition system is keystroke recognition that extracts inter-key durations as a feature with an assumption of no other can enter a password like the owner. From it has been introduced by Spillane (1975) the keystroke authentication algorithms are researched and a great number papers are published such as Karnan, Akila, and Krishnaraj (2011), Karatzouni and Clarke (2007), Clarke and Furnell (2007a, 2007b), Kang, Hwang, and Cho (2007), Cho, Han, Han, and Kim (2000), Haidar, Abbas, and Zaidi (2000), Umphress and Williams (1985), Joyce and Gupta (1990), Bleha, Silvinsky, and Hussien (1990), Leggett, Williams, Usnick, and Longnecker (1991), Obaidat and Sadoun (1997), Monrose and Rubin (1997), Monrose and Rubin (2000), Araujo, Sucupira, Lizarraga, Ling, and Yabu-Uti (2005), Gunetti and Picardi (2005) and Ahmed, Traore, and Almulhem (2008). As the recent studies of keystroke authentication (Alpar, 2014; Campisi, Maiorana, Bosco, & Neri, 2009; Crawford, 2010; Dholi & Chaudhari, 2013; Garg & Meena, 2012; Hwang, Lee, & Cho, 2009; Jamil & Khan, 2011; Li et al., 2011; Messerman, Mustafic, Camtepe, & Albayrak, 2011; Rudrapal & Das, 2013; Saevanee & Bhattarakosol, 2009; Syed, Banerjee, Cheng, & Cukic, 2011; Teh, Teoh, Tee, & Ong, 2010; Zhong, Deng, & Jain, 2012) are the most remarkable articles in the literature.

Even though the subject of this paper is inspired by keystroke authenticating algorithms, the core of this research is slightly different that we investigated touching durations instead of inter-key durations. However, it is not plausible to state that everyone's touching times are as unique as keystrokes, therefore we concentrated on invisible ghost passwords which can be created intentionally. Briefly, we wrote an interface that collects touching durations from first touch to release, and saves the intervals as biometric data. Afterwards, we checked the future logins by comparing with the saved data, as the first simple interval checking method. However this process resulted in a very strict authentication, with 0% false accept rate (FAR) which is flawless, while with an unexpected false reject rate (FRR) as 16.5%, since the intervals were extremely narrow. Therefore, to lower the FRR, we proposed several artificial intelligence based algorithms such as ANN, ANFIS and RGB Histogram technique.

In the literature, there are several papers which are close to our research regarding touchscreen authentication such as Zheng, Bai, and Huang (2012), Kwapisz, Weiss, and Moore (2010), Chang, Tsai, and Lin (2012), Sae-Bae, Ahmed, Isbister, and Memon (2012), De Luca, Hang, Brudy, Lindner, and Hussmann (2012), Angulo and Wästlund (2012), Shahzad, Liu, and Samuel (2013), Schaub, Deyhle, and Weber (2012), Shahzad, Zahid, and Farooq (2009), Maiorana, Campisi, González-Carballo, and Neri (2011) and Rao, Aparna, Akash, and Mounica (2014). Since it is a very fresh field, there are a few papers published in recent years, similar to principal of ours, regarding touchscreen authentication. Briefly, Sae-Bae et al. (2012) proposed a novel multi-touch and gesture-based authentication method that combines biometric techniques with gestural input. Using five-finger touch gestures, based upon classifying movement characteristics of the center of the palm and fingertips, they collected biometric data with the pattern recognition techniques. They also established a classifier to recognize unique biometric gesture characteristics and check the future logins.

Chang et al. (2012) introduced a new graphical-based password keystroke authentication system for touch screen handheld mobile devices. In their paper, they enlarged the password space size and utilized keystroke system for touch screen handheld mobile devices with a pressure feature. The paper of De Luca et al. (2012) seems the most close paper to ours since they researched the pattern passcodes, as well. They introduced an authentication approach that enhances password patterns with an additional security layer, transparent to the user. Therefore users authenticated by the pattern and by the way they press the pattern nodes. Moreover they introduced a novel method of dynamic time warping borrowed from speech recognition for the analysis of biometric data.

Shahzad et al.'s (2013) paper, which is also relevant to our research, presented a biometric authentication for touchscreen smartphones, however without patterns. In their paper they introduced a user authentication scheme for the secure unlocking of touch screen devices. They focused on finger velocity, device acceleration as novel features as well as stoke durations. Angulo and Wästlund (2012) proposed the usage of lock pattern dynamics as a secure and user-friendly authentication method with developing an application for the Android mobile platform to collect data, with the way that individuals draw lock patterns on a touchscreen. The achieved 10.39% EER with a Random Forest machine learning clasier method using finger-in-dot and finger-in-between nodes features. Maiorana et al. (2011) also proposed a method of keystroke recognition for keypads of mobile devices. The novelty in their research is the new statistical classifier with Manhattan and Euclidean distances.

Moreover, regarding the very recent studies of biometric keystroke authentication for touchscreens, the most noticeable papers currently published are as follows; Tasia, Chang, Cheng, and Lin (2014) proposed a twelve key virtual keypad as an interface for users to enter their pins. They extracted 6 features including pressure and size as rarely used traits in the literature, and utilized statistical classifiers. Kang and Cho (2014) designed three different interfaces for touchscreens and one for pc keyboards to collect biometric data. They used several statistical methods to classify the authentication data and reached 5.64% EER for 1000 reference and test set sizes. Furthermore, Kambourakis, Damopoulos, Papamartzivanos, and Pavlidakis (2014) implemented a keystroke system for Android touchscreens and presented two novel traits: speed and distance besides two known features: hold-time and inter-time. Using KNN and Random Forest algorithms, they classified the attempts according to two different methodologies and scenarios.

When compared with these papers, what we introduce a novel pattern password authentication systems with neural network based ANFIS and RGB Histogram methods as the new classifiers. Furthermore, we manipulated the standard learning process in ANN to fit our requirements by introducing a separation rate. Additionally, we used Levenberg–Marquardt algorithm consisting of Jacobian matrix to train the network in RGB Histogram method since there was not 1–1 correspondence between inputs and

Download English Version:

https://daneshyari.com/en/article/384902

Download Persian Version:

https://daneshyari.com/article/384902

Daneshyari.com