Applied Soft Computing xxx (2017) xxx–xxx

Contents lists available at ScienceDirect

Applied Soft Computing

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

Improving the performance of free-text keystroke dynamics authentication by fusion

Arwa Alsultan [a,*], Kevin Warwick [b], Hong Wei [c]

[a] Information Technology Department, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia
[b] Vice Chancellors Office, Coventry University,Priory Street, Coventry CV1 5FB, UK
[c] Computer Science Department, School of Mathematical, Physical and Computational Sciences, University of Reading, Reading RG6 6AH, UK

ARTICLE INFO

Article history:
Received 29 September 2016
Received in revised form 18 October 2017
Accepted 12 November 2017
Available online xxx

Keywords:
Free-text keystroke dynamics
authentication
Feature-level fusion
Decision-level fusion
SVMs
ACO
Decision tree

ABSTRACT

Free-text keystroke dynamics is invariably hampered by the huge amount of data needed to train the system. This problem has been addressed in this paper by suggesting a system that combines two methods, both of which provide a reduced training requirement for user authentication using free-text keystrokes. The two methods were fused to achieve error rates lower than those produced by each method separately. Two fusion schemes, namely: decision-level fusion and feature-level fusion, were applied. Feature-level fusion was done by concatenating two sets of features before the learning stage. The two sets of features were: a timing feature set and a non-conventional feature set. Moreover, decision-level fusion was used to merge the output of two methods using majority voting. One is Support Vector Machines (SVMs) together with Ant Colony Optimization (ACO) feature selection and the other is decision trees (DTs). Even though the classifiers using the parameters merged at feature level produced low error rates, its results were outperformed by the results achieved by the decision-level fusion scheme. Decision-level fusion was employed to achieve the best performance of 0.00% False Accept Rate (FAR) and 0.00% False Reject Rate (FRR).

© 2017 Elsevier B.V. All rights reserved.

1. Introduction

Keystroke dynamics is an effortless behaviour-based method for authenticating users, which employs the person's typing patterns for validating his/her identity. As mentioned by [1], keystroke dynamics is "not what you type, but how you type." In this approach, the user types in text, as usual, without any extra work to be done for authentication. Moreover, it only involves the user's own keyboard and no other external hardware. These criteria make keystroke dynamics an excellent alternative or add on to the conventional ID/password authentication scheme.

Unfortunately, passwords are prone to social engineering and can be easily cracked using methods such as dictionary attack and brute force attack. Therefore, users are obliged to use extreme measures to safeguard their passwords, a procedure which includes remembering long and complex passwords in addition to the need for changing their passwords periodically [2]. This causes frustration and apprehension for users, especially when a single user is most likely responsible for more than a hand-full of ID/passwords spread over multiple systems.

However, the main drawback of keystroke dynamics authentication is the large amount of training data it requires. Typing large amounts of text in the enrolment phase is time consuming and not user-friendly. A key-pairing method, which is based on the keyboard's key-layout, has been suggested as a way to enable one user's typing pattern to be distinguished from another user's. The method extracts several timing features from specific key-pairs. This technique was developed to use the smallest amount of training data in the best way possible. In addition, non-conventional features were also defined and extracted from the input stream typed by the user in order to understand typing behaviours based on limited input data.

As fusion was proven to reduce the error rate in classification tasks compared with single classifiers [3], these two techniques were fused in order to increase the performance of keystroke recognition whilst using a small amount of training data. In this study, we apply two different types of fusion techniques, namely: feature-level fusion and decision-level fusion. Specifically, this work attempts to implement both kinds of fusion and then compare between the two methods in order to find the fusion technique that

* Corresponding author.
E-mail address: afalsultan@ksu.edu.sa (A. Alsultan).

https://doi.org/10.1016/j.asoc.2017.11.018
1568-4946/© 2017 Elsevier B.V. All rights reserved.

Please cite this article in press as: A. Alsultan, et al., Improving the performance of free-text keystroke dynamics authentication by fusion, Appl. Soft Comput. J. (2017), https://doi.org/10.1016/j.asoc.2017.11.018

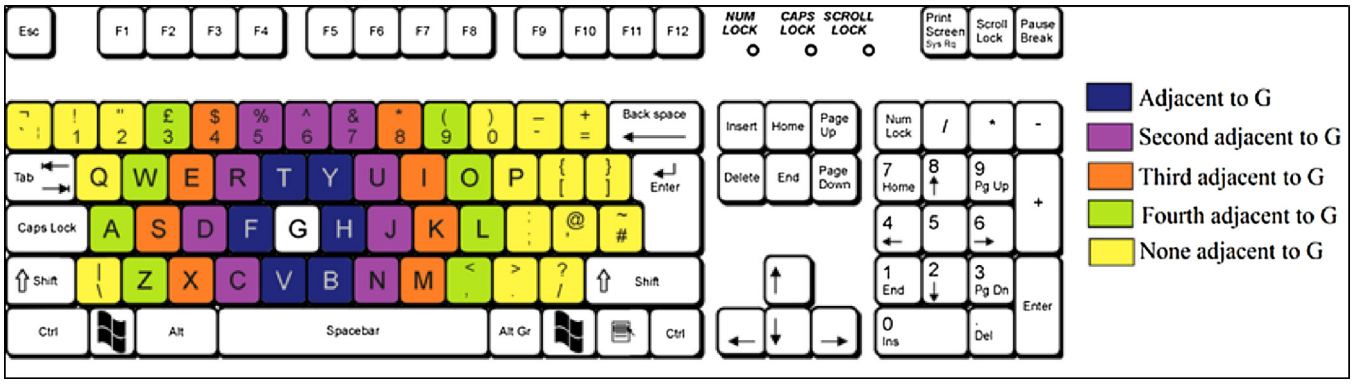

Fig. 1. Key-pair classification.

produces the best recognition rate in free-text keystroke dynamics systems with limited training.

The feature-level fusion is done by joining keystroke timing features and non-conventional typing features before the learning phase. Meanwhile the decision-level fusion is done by combining the output of a method involving timing features and SVMs/ACO and another method utilizing non-conventional features and decision trees. Both SVMs and DTs are classifiers that follow non-iterative approaches.

The rest of this paper proceeds as follows. Section 2 introduces keystroke dynamics theory and describes some of the work previously carried out in the area of keystroke dynamics user authentication. Section 3 discusses the feature sets used in this experiment. Section 4 describes the different fusion techniques. In Section 5, we point to the experimental results and discussion, in which the data space and the experimental results are indicated. A discussion about our results and some comparisons with previous studies is also performed in this section. The final section concludes the topic and points out our research contributions and future work.

2. Keystroke dynamics

There are two basic classes of keystroke dynamics, namely: fixed-text and free-text [4]. The fixed-text keystroke dynamics method uses the typing pattern of the user while entering a predefined text. This text has been previously used to train the system and is delivered by the user at log-in time. Contrariwise, the free-text keystroke method is considered easier for the user as it overcomes the problem of memorizing the text, something that fixed-text keystrokes suffers from. As its name suggest in free-text keystrokes, the text used for enrolment does not have to be the same as the text used for log-in. Moreover, free-text keystroke dynamics is used for enhancing security through continuous and nonintrusive authentication [5]. This is done by authenticating users based on freely typed keystrokes [6]. Thus, the latter method is the one that has been considered in this paper as it can be applied in many useful settings to aid in real life situations in addition to the benefit it provides in balancing between security and usability [4]. Nonetheless, long text is provided by the user to train the system at the enrolment phase [5].

Keystroke dynamics is utilized in user's authentication by extracting timing features at the log-in session and comparing them with the timing features extracted at the enrolment session. These features include, among others: typing latency [7], keystroke duration [1], typing speed and shift key usage patterns [8]. Another feature which requires a specific keyboard for its measurement is typing pressure [9]. If the extracted features are adequately similar, the user is authenticated and if not the user might be denied access or at least asked to provide further identity information.

A large amount of research has been carried out over the years to investigate how keystroke dynamics can aid in user authentication. Joyce and Gupta [7] used a statistical method that employs the absolute distances between the means of the signature data and test data; each of which consists of a fixed-text that includes username, password, first name, and last name.

Moreover, Gunetti and Picardi [10] introduced an effective method for free-text authentication which was further explored by many other researchers. Their method was based on two measures: relative (R) measure and absolute (A) measure. These measures were used to calculate the degree of disorder and the absolute distance between two samples that share some n-graphs, i.e. n-characters-long letter combinations.

Other researchers relied on pattern recognition classifying methods such as the work done by Hu et al. [11]. They used the k-nearest neighbor approach together with the distance measurement proposed by Gunetti and Picardi [10] in order to classify the users' keystroke dynamics profiles.

Neural Networks have also been used for keystroke pattern classification; such as the research conducted by Raghu et al. [12] in which they incorporated a three-layered back propagation neural network to verify the identity of users.

Furthermore, a research that has considered fusion in keystroke dynamics is that conducted by Teh et al. [13]. The authors of this research proposed a fusion between two methods. The first being the Gaussian similarity score between a reference template and a test data template. The second being the Direction Similarity Measure (DSM) for comparing the typing patterns of the user. The two scores were fused by using a weighted sum rule. Fifty participants were requested to type-in their username, password and a special fixed phrase repeatedly ten times. The performance achieved using only the Gaussian probability density function yielded an EER of 11.6897%, while the performance of using only the Direction Similarity Measure produced an EER of 19.74%. Combining the two methods delivered the best result of an EER of 6.36%.

Hocquet et al. [14] performed a study for authenticating users using a fusion of three methods in. The first used the mean and the variance of each latency time and compared it to a threshold. The second method used a measure of typing rhythm disorder where the time was classified into five different classes according to the speed. The difference between the numbers of the classes in the profile data and in the test data was calculated and then the sum of all these differences was compared to a threshold. The third and last method was based on the ranks of the latencies; this was performed by ordering the latencies based on their speed. The latency time of each observation was ordered from the slowest to the fastest for each user's profile. The Euclidean distance between the user's profile and the new data was then used to guess if the new observation belonged to that user. Even though these methods work well on

Please cite this article in press as: A. Alsultan, et al., Improving the performance of free-text keystroke dynamics authentication by fusion, Appl. Soft Comput. J. (2017), https://doi.org/10.1016/j.asoc.2017.11.018

Download English Version:

https://daneshyari.com/en/article/11002717

Download Persian Version:

https://daneshyari.com/article/11002717

Daneshyari.com