Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Enhanced template update: Application to keystroke dynamics

Paulo Henrique Pisani [a,*], *Romain Giot* [b], *André C.P.L.F. de Carvalho* [a], *Ana Carolina Lorena* [c]

[a] *Universidade de São Paulo, Instituto de Ciências Matemáticas e de Computação, Av. Trabalhador São Carlense, 400, São Carlos, Brazil*

[b] *Université de Bordeaux, Laboratoire Bordelais de Recherche en Informatique, UMR 5800, F-33405 Talence, France*

[c] *Universidade Federal de São Paulo, Instituto de Ciência e Tecnologia, Rua Talim, 330, São José dos Campos, Brazil*

ARTICLE INFO

Article history:
Received 26 September 2015
Received in revised form 4 April 2016
Accepted 12 April 2016
Available online 20 April 2016

Keywords:
Template update
Biometrics
Keystroke dynamics
Adaptive biometric systems
Data streams

ABSTRACT

With the increasing number of activities being performed using computers, there is an ever growing need for advanced authentication mechanisms like biometrics. One efficient and low cost biometric modality is keystroke dynamics, which attempts to recognize users by their typing rhythm. It has been shown that the biometric features may undergo changes over time, which can reduce the predictive performance of the biometric system. Template update adapts the user model to deal with these changes and, therefore, decreases the predictive performance loss. Most of the studies in the literature only take into account samples classified as genuine to perform adaptation. This paper extends this common approach by proposing an original framework to make use of samples classified as impostors, too. This new approach, named Enhanced Template Update, uses all collected unlabeled samples to support the adaptation process. According to our experimental results, this new approach can improve the predictive performance when compared to current methods depending on the scenario. Some improvements on the visualization of results over time are also proposed during the analysis performed in this study. Although the proposed approach is evaluated on keystroke dynamics, it could also be applied to other biometric modalities.

© 2016 Elsevier Ltd. All rights reserved.

1. Introduction

Keystroke dynamics is a behavioral biometric modality that allows the recognition of individuals based on their typing rhythm on the keyboard. This biometric modality has some advantages over commonly adopted alternatives, like fingerprint or iris recognition systems (Hosseinzadeh and Krishnan, 2008; Peacock et al., 2004). First, keystroke dynamics does not require an additional sensor, since a common keyboard is enough to acquire keystroke data. Second, this biometric modality can be applied in background, during other user daily tasks. These advantages may contribute to a higher acceptability of this technology.

* *Corresponding author.* Tel.: +55 1633739700.
Email addresses: phpisani@icmc.usp.br (P.H. Pisani), romain.giot@u-bordeaux.fr (R. Giot), andre@icmc.usp.br (A.C.P.L.F. de Carvalho), aclorena@unifesp.br (A.C. Lorena).

http://dx.doi.org/10.1016/j.cose.2016.04.004
0167-4048/© 2016 Elsevier Ltd. All rights reserved.

However, as a behavioral modality, keystroke dynamics has a higher tendency to be subject to changes over time (Giot et al., 2012c). Indeed, how the user types a password evolves with time and can be different in a short timespan. The reasons are numerous and cannot always be controlled: increased practice, changes on the environment, etc. For example, users can increase the speed to write the password due to more practice. These modifications increase the intraclass variability which, consequently, can increase the ratio of authentication failure.

A strategy to reduce this performance decrease is to adopt a *template update* mechanism (sometimes referred to as an *adaptive biometric system*) (Poh et al., 2012; Roli et al., 2008). The aim of the template update is to automatically adapt the biometric model/reference of the user to make it closer to the user current biometric data (i.e., decreasing the deviation due to template ageing). However, this update process is done without supervision (i.e., it is totally automatic), and is therefore subject to errors. This may lead to reduced predictive performance, illustrating the difficulty of this task.

There are not many studies on template update for keystroke dynamics, highlighting the need for further investigations. Before introducing the proposed approach, we should clearly specify some terms regarding the biometric samples:

- *True genuine/positive*: a biometric sample which belongs to the genuine user.
- *True impostor/negative*: a biometric sample which belongs to an impostor.
- *Classified as genuine/positive*: a biometric sample classified as genuine by the classifier. It could belong to the genuine user (the classifier returned the correct label) or it could come from an impostor (the classifier returned the wrong label).
- *Classified as impostor/negative*: a biometric sample classified as impostor by the classifier. It could belong to the genuine user (the classifier returned the wrong label) or it could come from an impostor (the classifier returned the correct label).

The majority of the papers in the area updates the user model only with biometric samples classified as genuine/positive, discarding those classified as impostors (negative). They usually employ a *positive gallery*, which is a set of biometric samples classified as genuine/positive. This paper proposes to investigate if taking into account samples classified as impostors can improve the adaptive procedure. Thus, there would be a *negative gallery*, too. This new template update approach, which uses samples classified as both positive and negative for template update, is named here as *Enhanced Template Update* (ETU). The usage of negative samples in the template update process has two main motivations:

- *Reduce False Match Rate (FMR)*[1]: As some impostor samples would be available, they may help to avoid the inclusion of negative samples in the positive gallery. We propose an approach to take advantage of this concept in order to decrease the number of negative samples wrongly included in the positive gallery during adaptation. The proposed approach is named *Positive Gallery Protection* (PGP).
- *Reduce False Non-match Rate (FNMR)*[2]: This can be done by changing the classification decision. Sometimes the positive model alone (induced only from positive samples) may reject a given positive sample, but with the help of a negative model (induced from negative samples), it may be possible to verify whether the sample is closer to the positive model than the negative model. As a result, FNMR can be reduced. We propose some alternatives to change the classification decision based on this reasoning. Four different methods to change the classification decision are proposed, named as ETU 0 to 3.

It must be observed that a reduction of FNMR usually results in an increase of FMR (and vice-versa).

The contributions of this paper are:

- Proposal of a framework for template update using biometric samples classified as positive and the ones classified as negative. This may lead to further studies by the adaptive biometric community using this additional information.
- Study advantages and drawbacks of several configurations of the proposed framework.
- Performance evaluation on public main keystroke dynamics datasets, including different types of feature vectors. To the best of our knowledge, this is one of the first papers to use the passwords part of the GREYC-Web dataset (Giot et al., 2012a).
- Improve the visualization of the performance of adaptive biometric methods over time.

This work does not aim at providing a new keystroke dynamics authentication algorithm neither a performance comparison of various authentication mechanisms linked to our framework. The current study is only interested in the architecture of the template update system and its application with standard authentication algorithms from keystroke dynamics literature, although our methods may be directly applied to other classification algorithms.

This paper is organized as follows: Section 2 introduces previous work on template update for keystroke dynamics; Section 3 presents the enhanced template update framework and the methods investigated in this paper; Section 4 describes the experimental methodology, including datasets, biometric data stream generation and parameters adopted in the experiments; Section 5 shows the experimental results, including a discussion on the performance over time; finally, Section 6 presents the main conclusions of this study and alternatives for future work.

[1] FMR measures the rate in which an impostor is wrongly accepted by the biometric system (it is an error rate, so it must be as low as possible).

[2] FNMR measures the rate in which the genuine user is incorrectly rejected by the biometric system (it is an error rate, so it must be as low as possible).

Download English Version:

https://daneshyari.com/en/article/456386

Download Persian Version:

https://daneshyari.com/article/456386

Daneshyari.com