Pattern Recognition 84 (2018) 332–344

Contents lists available at ScienceDirect

Pattern Recognition

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

Distinctiveness, complexity, and repeatability of online signature templates

Napa Sae-Bae[a,*], Nasir Memon[b], Pitikhate Sooraksa[c]

[a] Faculty of Science and Technology, Rajamangala University of Technology Suvarnabhumi, Thailand
[b] Tandon School of Engineering, New York University, USA
[c] Department of Computer Engineering, King Mongkut's Institute of Technology Ladkrabang, Thailand

ARTICLE INFO

Article history:
Received 17 July 2017
Revised 6 July 2018
Accepted 22 July 2018
Available online 26 July 2018

Keywords:
Biometric
Online signature
Biometric template quality
Distinctiveness
Complexity
Repeatability

ABSTRACT

This paper proposes three measures to quantify the characteristics of online signature templates in terms of distinctiveness, complexity and repeatability. A distinctiveness measure of a signature template is computed from a set of enrolled signature samples and a statistical assumption about random signatures. Secondly, a complexity measure of the template is derived from a set of enrolled signature samples. Finally, given a signature template, a measure to quantify the repeatability of the online signature is derived from a validation set of samples. These three measures can then be used as an indicator for the performance of the system in rejecting random forgery samples and skilled forgery samples and the performance of users in providing accepted genuine samples, respectively. The effectiveness of these three measures and their applications are demonstrated through experiments performed on three online signature datasets and one keystroke dynamics dataset using different verification algorithms.

1. Introduction

For the past decade or so, research in biometric verification systems has mostly focused on effective feature sets and recognition algorithms to improve verification performance [1–3]. However, several studies have indicated that characteristics of biometric samples used in the enrollment process to create a verification template can also play a crucial role in the overall accuracy and reliability of biometric systems [4–6]. Specifically, the accuracy of face, fingerprint, and iris biometric systems evaluated on good quality biometric samples is much higher than systems evaluated on poor quality samples [7].

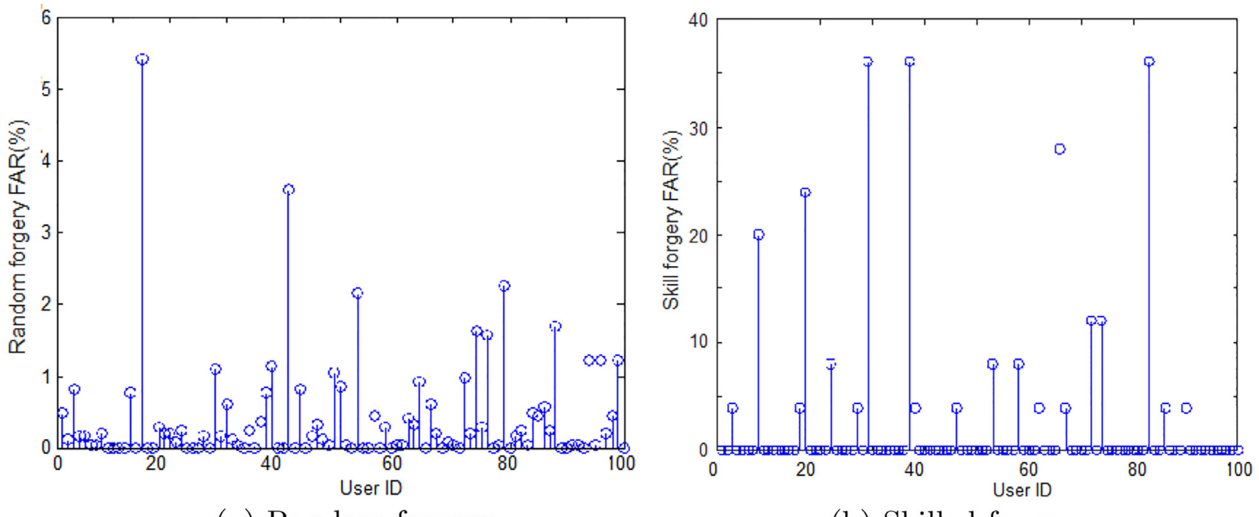
In text password based authentication where users are allowed to choose a password freely, it is known that some users would choose a weak password or a password that could be guessed easily [8]. This problem has led to many studies related to assessing password strength and also the development of mechanisms such as the password strength meter that offers feedback and enforces a policy to reject a weak password during the enrollment stage itself [8].

Similarly, there is a need for the assessment of biometric template characteristics when enrollment is done without supervision [9], e.g., for mobile device authentication, and rejecting samples that could lead to degradation of performance. This is especially true for behavioral biometric based authentication techniques such as online signatures or key stroke dynamics. In behavioral biometric verification systems it is difficult to collect a set of negative samples that could accurately represent a population. Therefore, a user specific template is generally modeled based purely on a small number of enrolled samples, without using imposter samples. Hence, at a given threshold, the verification performance can be profoundly different from one template to another.

For example, in online signature authentication, a user may enroll a template that is very simple. As a result, attackers could easily produce a signature that matches the template, resulting in a compromised account. In this context, an assessment of biometric template characteristics could be used to design proper mechanisms to cope with such weak templates [10–13]. For example, given a template that is predicted to yield high FAR (False Acceptance Rate: the likelihood that forgery samples will be incorrectly accepted by the system) but low FRR (False Rejection Rate: the likelihood that genuine samples will be incorrectly rejected by the system), the system could examine whether a few bad enrolled samples could be safely removed to lower FAR without degrading FRR. Or given a template that is predicted to yield high FRR, the system may prompt users to re-enroll or practice more with their signatures.

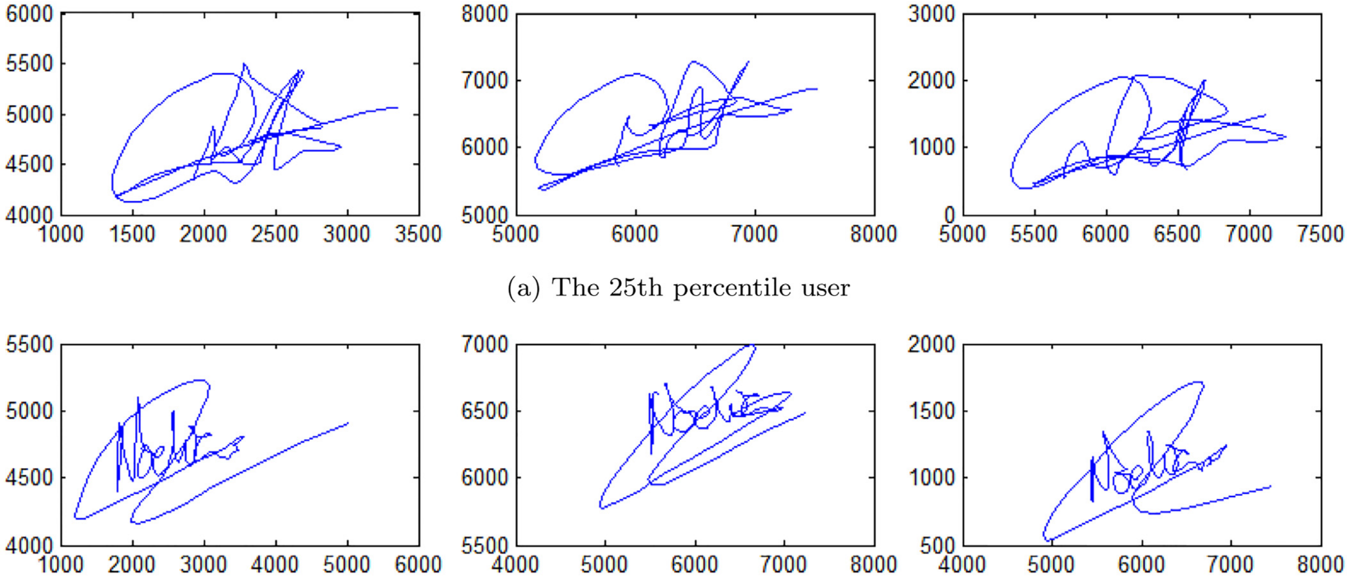
[*] Corresponding author.
E-mail address: napa.s@rmutsb.ac.th (N. Sae-Bae).

https://doi.org/10.1016/j.patcog.2018.07.024
0031-3203/© 2018 Elsevier Ltd. All rights reserved.



(a) Random forgery (b) Skilled forgery

Fig. 1. FAR against random forgery and skilled forgery for each user in MCYT dataset when a user's signature template is derived from the first 10 genuine samples and threshold set at EER with respect to the algorithm described in [2].



(a) The 25th percentile user

(b) The 75th percentile user

Fig. 2. The 3rd, 7th, and 10th samples of two users from MCYT dataset with mean imposter scores at the 25th and 75th percentile.

In this paper we focus on characteristics of one particular type of behavioral biometrics, namely online signatures. We develop three simple assessment characteristics of online signature templates and investigate their ability to predict FAR and FRR. The three characteristics are: **(1) Distinctiveness** refers to how much this user's signature differs from others, which indicates the probability of a user being impersonated by a random signature, **(2) Complexity** refers to how hard to forge this user's signature. This indicates the probability of a user being impersonated by a forged signature, and **(3) Repeatability** refers to how likely this user can repeat her signature which indicates the probability of a genuine sample being rejected by the system.

We show, using experiments, how the assessment of these characteristics for online signature templates can be used to infer security and usability of a particular online signature template. Specifically, distinctiveness and complexity could be indicative of security or FAR of the signature template against random forgeries and skilled forgeries respectively. Also, repeatability could be indicative of usability in terms of FRR, which refers to the ability of the user in gaining access to the system using her signature. Note that this work is an extension of previous work [14] where we presented the metric to measure distinctiveness of online signature templates and preliminary results to demonstrate its efficacy.

1.1. *Performance disparity of signature templates*

To illustrate the disparity in characteristics of online signature templates in terms of distinctiveness and complexity, FAR against random forgery and skilled forgery of each individual in MCYT dataset is plotted in Fig. 1. Note that EER denotes the equal error rate or the rate at which FAR and FRR are equal. Samples of enrolled signatures that lead to the mean imposter score at the 25th and 75th percentile are shown in Fig. 2. It is noticed that, in addition to the intrinsic difference of the two signatures, the