Information Sciences 352–353 (2016) 188–202

Contents lists available at ScienceDirect

Information Sciences

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

Two strategies to optimize the decisions in signature verification with the presence of spoofing attacks

Shilian Yu[a,b], Ye Ai[a,b], Bo Xu[a,b], Yicong Zhou[c], Weifeng Li[a,b,*], Qingmin Liao[a,b], Norman Poh[d]

[a] Department of Electronic Engineering/Graduate School at Shenzhen, Tsinghua University, China
[b] Shenzhen Key Laboratory of Information Science and Technology, Shenzhen, China
[c] Department of Computer and Information Science, University of Macau, Macau, China
[d] Department of Computer Science, University of Surrey, Guildford, Surrey, United Kingdom

ARTICLE INFO

Article history:
Received 19 January 2015
Revised 23 February 2016
Accepted 4 March 2016
Available online 10 March 2016

Keywords:
Biometric authentication
Spoofing attack
Liveness score
Brute-force
Probabilistic

ABSTRACT

A conventional biometric authentication system is often designed to distinguish genuine accesses from zero-effort impostor attacks. However, when operating in an adversarial environment, the system has to be robust against presentation attacks such as spoofing. An effective solution to reduce the impact of spoofing attack is to consider both the matching score and liveness score when making the accept/reject decision. In this paper, we consider the joint decision space of matching and liveness scores in the presence of *both* spoofing attack and zero-effort attack, with application to signature verification. Our investigation aims to understand how decision thresholds in the above space should be optimized. This leads to two dichotomies of methods, namely brute-force approach versus probabilistic approach; and single threshold versus double-threshold approach. This view leads to three novel methods that have never been reported. Based on the experimental results carried out on an off-line signature database, the novel methods turn out to outperform simpler methods with only matching score.

1. Introduction

Biometric authentication now permeates our daily lives, from automatic border control to unlocking our smart phones. Along with its convenience, potential vulnerabilities and various kinds of attacks have been reported. One of the most commonly reported attacks is *spoofing* attack, which is also called *non-zero effort* attack. In a spoofing attack, an attacker tries to cheat the biometric system to gain illegitimate access by producing fake biometric traits of the victim that he/she tries to impersonate. Since a conventional biometric authentication system is designed to distinguish genuine samples from *zero-effort* impostor samples, the system is often unable to judge whether a submitted sample is a *live* one or is made from a spoofed material. Examples of spoofing attack abound for various biometric modalities: gummy fingers in fingerprint authentication [15], face prints in 2D face authentication [13], masks in 3D face authentication [8], synthesized voice forgery [17], etc.

[*] Corresponding author at: Shenzhen Key Laboratory of Information Science and Technology, Shenzhen, China. Tel.: +86 755 26036564.
E-mail address: li.weifeng@sz.tsinghua.edu.cn (W. Li).

http://dx.doi.org/10.1016/j.ins.2016.03.005
0020-0255/© 2016 Elsevier Inc. All rights reserved.

Signature as one of the most popular biometric traits plays an important role in person recognition. It has many applications such as bank cheques authentication, attendance monitoring, and endorsement or confirmation of documents, often in a legally binding manner. For some applications, especially those where the identity of the signer needs to be ascertained, automatic signature verification is indisputably the most natural biometric modality that can fulfil this role.

According to the data acquisition mechanism, signature verification systems can be divided into online verification and off-line verification. Online systems have a higher signature recognition rate because of the dynamic information including writing speed, stroke length and pen pressure. However, the system requires special electronic devices to capture these information at the same time of writing. On the other hand, off-line systems are designed to compare a static image with a template stored in the database without any dynamic information. Compared to the online systems, off-line systems are more practical because they do not require the presentation of signers or any equipment. Thus, we focus on the off-line signature verification in this paper.

Saikia and Sarma [21] define three basic types of forgeries in signature verification systems; they are random forgery, simple forgery and skilled forgery. “Spoofing” in this paper is associated with *skilled* forgery, where the forger has access to the samples of the genuine signature and thus he/she is able to reproduce it.

To deal with the spoofing attacks in biometric systems, we use two very common threshold-based schemes to make the final decision. One of them simply makes the decision from the matching score d and the liveness score s by thresholding the two measurements:

$$\text{decision}(d,s) = \begin{cases} accept & \text{if } d < T_d \quad \text{and} \quad s > T_s \\ reject & \text{otherwise}, \end{cases} \tag{1}$$

where T_d is a threshold applied to d and T_s is a threshold applied to s. Since we consider the distance between the template and the query sample as our matching score d, the less d is, the higher the degree of matching is.

An alternative way is to estimate the posterior probability that the sample is genuine or a *match* comparison, and that it is also from a live sample, $P(M=1, L=1|d,s)$ based on the measurements d and s. It is then straightforward to apply a threshold to this posterior probability in order to make the final decision:

$$\text{decision}(d,s) = \begin{cases} accept & \text{if } P(M=1, L=1|d,s) > P_T \\ reject & \text{otherwise}, \end{cases} \tag{2}$$

where $M=1$ and $L=1$ synergistically represent the traits of this sample being genuine and authentic. More details about our terminology will be discussed in Section 3. This approach is also referred to as *single threshold probabilistic approach*.

A similar variant, which is referred to as *double threshold probabilistic approach*, is to optimize two thresholds for $P(M=1|d)$ and $P(L=1|s)$ respectively, as shown in Eq. (3).

$$\text{decision}(d,s) = \begin{cases} accept & \text{if } P(M=1|d) > P_{Td} \quad \text{and} \\ & P(L=1|s) > P_{Ts} \\ reject & \text{otherwise}. \end{cases} \tag{3}$$

Although the methodology is general, we will conduct our experiments on off-line signature authentication as a case study.

In order to make the final accept/reject decision in biometric systems using a matching score and a liveness score, from the introductory presentation so far, we can identify two decision schemes to optimizing the decision threshold, namely, brute-force and probabilistic optimization. The first strategy consists of exhaustively searching for an optimal solution by minimizing a performance criterion. The second capitalizes on the logic construct of Eq. (1) but in probabilistic sense. Although both strategies rely on the same logic construct, the brute-force optimization does not commit to an assumption that its probabilistic version does; that is, the latter assumes that both the matching score and the liveness score are independent of each other. Since there are two approaches, i.e. single threshold and double threshold in the probabilistic strategy, we have to systematically investigate all three different methods, as represented by the three equations above. The effectiveness of these methods will be systematically compared in the presence of both spoofing attack and zero-effort attack.

In this paper, we argue that although complicated methods have been proposed in the literature, one should not dismiss simple, yet straightforward strategies such as threshold-based methods because they are extremely easy to implement. Therefore, the key question is not about implementation, but about finding out if there is an optimal way to optimize the thresholds. Our key contribution is, therefore, to advance the understanding of the nature of thresholds optimization; and to provide recommendations and practices with regards to their implementation. Our second contribution is to propose two probabilistic variant of thresholding schemes. We conjecture that these variants are useful and should compare them favourably with the plain thresholding strategy because probability axioms can handle the inherent uncertainty in the choice of thresholds.

This paper is organized as follow: Section 2 describes related work in signature verification and the liveness detector used in some biometric traits. Section 3 illustrates some concepts and the notation used in our study. Section 4 presents our study methodology. Section 5 presents a case study on signature verification followed by conclusions in Section 6.