ELectronics EXpress

A scheme for predicting recognition performance by using confidence intervals

Aeyoung Kim and Sang-Ho Lee[a)]

Department of Computer Science and Engineering, Ewha Womans University
11–1 Daehyun-dong, Seodaemun-gu, Seoul, Korea
a) *shlee@ewha.ac.kr*

Abstract: We propose a novel scheme for predicting the recognition performance by using confidence intervals. Biometrics is the best solution for preventing illegal sharing of authentication solutions (e.g., password, identity card) in a multi-factor authentication system. However, information acquired using sensors contains considerable noise, which can lead to errors. Our proposed scheme provides an efficient solution for treating noise and the resulting errors. When an image acquired using the sensor includes considerable noise and the estimated matching result is "fail," the proposed scheme offers a short path. Our experimental results show the efficiency of the proposed scheme.

Keywords: recognition result prediction, error tolerance, multi-factor authentication, face sensing

Classification: Sensing hardware

References

[1] P. Grother and E. Tabassi, "Performance of Biometric Quality Measures," *IEEE Trans. Pattern Anal. Mach. Intell.*, pp. 531–543, 2007.

[2] Y. Chen, S. Dass, and A. Jain, "Fingerprint Quality Indices for Predicting Authentication Performance," *LNCS*, vol. 3546, pp. 160–170, 2005.

[3] K. Kryszczuk and A. Drygajlo, "What do quality measures predict in biometrics?," *Proc. 16th European Conf. Signal Processing*, 2008.

[4] W. J. Scheirer and T. E. Bould, "Cracking fuzzy vaults and biometric encryption," *Proc. Biometric Symp.*, pp. 1–6, 2007.

[5] E. Marasco, A. Ross, and C. Sansone, "Predicting identification errors in a multibiometric system based on ranks and scores," *Proc. 4th IEEE Int. Conf. Biometrics: Theory Applications and Systems*, pp. 1–6, 2010.

[6] A. M. Martinez and R. Benavente, The AR Face Database, CVC Technical Report #24, 1998. [Online] http://www.ece.osu.edu/~aleix/ARdatabase.html

1 Introduction

Authentication is carried out using one or more of three authentication factors: something you know (e.g., password, PIN), something you have (e.g.,

DOI: 10.1587/elex.9.133
Received November 10, 2011
Accepted January 03, 2012
Published February 10, 2012

ATM card, Smart card, USIM), and something you are (e.g., biometrics). Traditional single-factor authentication uses only one authentication factor (typically, the first one); however, such systems are easy to compromise. To make systems more difficult to compromise, thus realizing better security, wireless and mobile communication systems commonly use multi-factor (typically, two factors, these being the first two mentioned above) authentication systems. However, such models are not compliant with real strong authentication, because it is still difficult to prevent the illegal sharing of authentication solutions.

Among the three authentication factors mentioned above, the third factor, something you are, is the best solution to realize strong authentication. A real multi-factor authentication scheme based on biometrics affords both strong security and easy usability. While biometric-based multi-factor authentication schemes are quite promising, it is too difficult to adapt biometrics into an existing cryptography-based two-factor authentication system. In particular, it is difficult to obtain high key stability with the use of biometrics because the images acquired using a sensor differ every time.

For increasing the key stability, failure prediction schemes have proved useful. P. Grother *et al.* [1] reported that quality measures predict the authentication performance, and Y. Chen *et al.* [2] proposed two such quality measures. K. Kryszczuk *et al.* [3] reported a method in which classifier decisions and the corresponding reliability information are combined to predict and correct verification decisions. Scheirer *et al.* [4] proposed the concept of post-recognition failure prediction. E. Marasco *et al.* [5] reported the use of a classifier as a predictor using ranks and scores; however, their prediction scheme cannot be applied in authentication systems in real-time because they need matching and decision steps on the server-side.

In this paper, we propose an efficient scheme for predicting the recognition performance by using confidence intervals based on principal component analysis (PCA). This scheme shows promise for realizing a true multi-factor authentication system; it features increased key stability via efficient error management through the use of confidence intervals while reducing the computational cost.

The remainder of this paper is organized as follows. Section 2 describes the overall flow of the proposed scheme in an authentication system and the algorithms for implementing the same. Section 3 presents the experimental results. Finally, section 4 presents our conclusions.

2 Proposed prediction scheme

2.1 A generic model with a prediction scheme

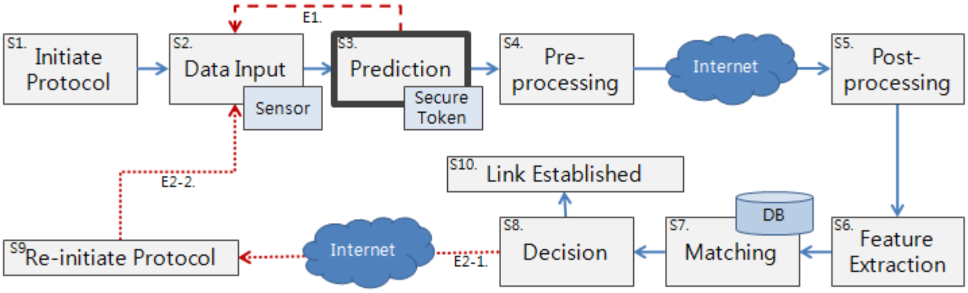
Fig. 1 (a) shows a sample of an efficient authentication model using the proposed prediction scheme. For simplicity and efficiency, the proposed prediction scheme is located between the 2nd stage, *Data Input* ($s2$), and the 4th stage, *Pre-processing* ($s4$). This provides the shortest path for input data that would fail in $s8$.

DOI: 10.1587/elex.9.133
Received November 10, 2011
Accepted January 03, 2012
Published February 10, 2012

© IEICE 2012
DOI: 10.1587/elex.9.133
Received November 10, 2011
Accepted January 03, 2012
Published February 10, 2012

The 1st stage, *Initiate Protocol* ($s1$), is simply an initialization step for the authentication model. The 2nd stage, *Data Input* ($s2$), includes an acquisition algorithm *Acquisition* (v) of a user $v \in \mathcal{U}$ who claims an identity u. *Acquisition* (v) obtains v's measurement B_v. The 3rd stage, *Prediction* ($s3$), is our proposed module with the T-test-based prediction algorithm *Pre_Tci_Prediction* (B_v). This module estimates the decision value of the 8th stage, *Decision* ($s8$), on the server-side by using a decision function. The result of the decision function *Pre_Decision* (B_v) is obtained by using a predetermined threshold $\rho \in \mathbb{R}$ as follows:

$$Pre\_Decision(B_v) = \begin{cases} \text{pass}, & \text{if } Pre\_Tci\_Prediction(B_v) \geq \rho \\ \text{fail}, & \text{if } Pre\_Tci\_Prediction(B_v) < \rho \end{cases}$$



(a) Flow of prediction module

Model-Case	Prediction Module Usage	Decision Result	Steps
I-1	No	Accept	$s1 \rightarrow s2 \rightarrow \rightarrow \rightarrow s4 \rightarrow \hat{\text{W}} \rightarrow s5 \rightarrow s6 \rightarrow s7 \rightarrow s8 \rightarrow s10$
I-2	No	Reject	$s1 \rightarrow s2 \rightarrow \rightarrow \rightarrow s4 \rightarrow \hat{\text{W}} \rightarrow s5 \rightarrow s6 \rightarrow s7 \rightarrow s8 \rightarrow s9 \rightarrow s2$
II-1	Yes	Accept	$s1 \rightarrow s2 \rightarrow s3 \rightarrow s4 \rightarrow \hat{\text{W}} \rightarrow s5 \rightarrow s6 \rightarrow s7 \rightarrow s8 \rightarrow s10$
II-2	Yes	Reject	$s1 \rightarrow s2 \rightarrow s3 \rightarrow s2$

(b) Different steps depending on prediction module usage

Fig. 1. A biometric-based authentication model with the proposed prediction scheme

If the result in $s3$ is "pass," user v will start the next stage. However, if the result is "fail," user v will try $s2$ again. The 4th stage, *Pre-processing* ($s4$), is an important stage for the feature extraction and matching steps. The 5th stage, *Post-processing* ($s5$), is almost the same as $s4$. The 6th stage, *Feature Extraction* ($s6$), computes a feature set $ft_v = \{b'_1, b'_2, \cdots, b'_n\}$ for $b'_j \in M$ ($j = 1, \cdots, n$) with B'_v. Here, n denotes the number of features in ft_v. The 7th stage, *Matching* ($s7$), compares ft_v with the registered information of the user in the DB on the server-side. If $spatial\_distance(b_i, b'_j) \leq \gamma$, the return value of the function $match(b_i, b'_j)$ is 1. The matching score $matching\_score(ft_v, ft_u)$ is $\frac{1}{n \cdot m} \sum_{j=1}^{n} \sum_{i=1}^{m} match(b_i, b'_j)$, and the value lies within the range [0, 1]. The 8th stage, *Decision* ($s8$), includes a decision function *decision*(). The result of $s8$ is obtained by using a predetermined threshold $\tau \in \mathbb{R}$ as follows:

$$decision(ft_v, ft_u) = \begin{cases} \text{accept}, & \text{if } matching\_score(ft_v, ft_u) \geq \tau \\ \text{reject}, & \text{if } matching\_score(ft_v, ft_u) < \tau \end{cases}$$

If the result of $s8$ is "accept," the link in the 10th stage, *Link Established* ($s10$), is established for user u as a successful authentication. However, if the result is "reject," the 9th stage, *Re-initiate* ($s9$), asks the user to go to $s2$ and try again.

Fig. 1 (b) shows the difference between the steps in model I without prediction module $s3$ and model II with $s3$. If the result of $s8$ is "accept," case II-1 is quite similar to case I-1 except for $s3$. However, if the result of $s8$ is "reject," there is a big difference between case I-2 and case II-2. The number of stages that need to be processed in case II-2 is just 3. This short path is possible because of prediction module $s3$, and it is helpful in reducing the process time and cost.

2.2 T-test-based prediction scheme

We now describe the proposed prediction scheme for the biometric-based authentication system. First, we describe the *PRE_TCI_GENERATE* algorithm that is used for the enrollment of a registered user's confidence interval set *CI*. The basic idea behind the generation of *CI* is based on the T-test scheme with some images of the same face. High-quality images should be captured for the enrollment. This algorithm includes methods for calculating a principal component pc_i based on PCA, taking a T-test value t, and generating a confidence interval ci_i. It uses the parameters t, $\bar{x}$, s, u, v, and ci,; a set $B_{(j)} = \{pc_{i(j)}\}$ where $1 < i <$ m and $2 < j < n$ for the input; and a set CI of confidence intervals for the output. This algorithm is given as follows:

```
Algorithm PRE_TCI_GENERATE
    $CI, \bar{x}_i,\ s_i,\ u_i,\ v_i \leftarrow \emptyset$ ;
    $t \leftarrow t_{0.01}(n-1)$ ;
    for $i = 1$ to $m$ do
        $\bar{x}_i \leftarrow \frac{1}{n}\sum_{j=1}^{n} pc_{i(j)}$ ;
        $s_i \leftarrow \frac{1}{n}\sum_{j=1}^{n} (pc_{i(j)})^2 - \bar{x}_i^2$ ;
        $u_i \leftarrow \bar{x}_i - t \cdot s_i \cdot n^{-1/2}$ ;
        $v_i \leftarrow \bar{x}_i + t \cdot s_i \cdot n^{-1/2}$ ;
        $ci_i \leftarrow (u_i, v_i)$ ;
        $CI \leftarrow CI \cup ci_i$ ;
    end
```

The proposed prediction algorithm *PRE_TCI_PREDICTION* is basically used to compare the confidence intervals and m principal components of the input data. It uses the parameters i and j; a set $CI = \{ci_i\}_{i=1}^{m}$,; a set $B_v = \{pc_i\}_{i=1}^{m}$ for the input; and an estimation result ER for the output. This algorithm is given as follows:

© IEICE 2012
DOI: 10.1587/elex.9.133
Received November 10, 2011
Accepted January 03, 2012
Published February 10, 2012

```
Algorithm $PRE\_TCI\_PREDICTION$
    $k, ER \leftarrow \emptyset$ ;
    for $i = 1$ to $m$ do
        if $u_i < pc_i$ & $v_i > pc_i$
        then $\leftarrow k + 1$ ;
    end
    $ER \leftarrow k/m$ ;
```

Given CI and B, as shown in Fig. 2 (a), the algorithm checks whether pc_i in B_v is included in $ci_i = (u_i, v_i)$ of CI; it returns the result 0 if it is not included and 1 if it is. ER, which lies in the range [0, 1], is the estimation rate of the decision result.

3 Experimental results

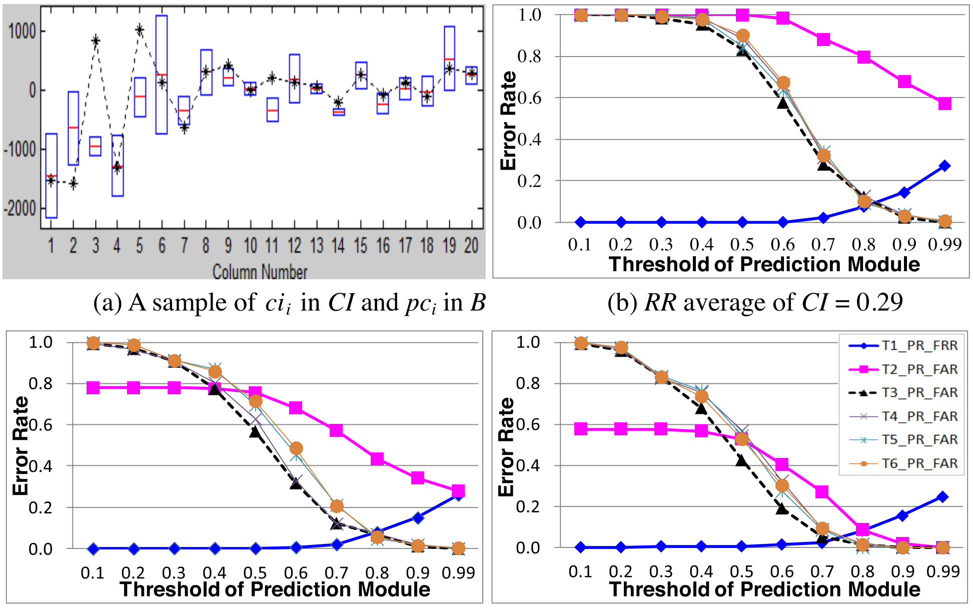
We experimentally evaluated the performance of our prediction scheme. To assess its effectiveness in a biometric-based authentication system, we implemented the algorithms in MATLAB and used grayscale images of faces [6], fingerprints, irises, and eyes. In these experiments, the recognition rate RR of each image in the face DB was already measured as a control. We also used two performance measures, namely, the false rejection rate (FRR) and the false acceptance rate (FAR). In both these measures, a lower value implies better performance. The datasets were divided into control and treatments T1–T6, as listed in Table I.

Table I. Control and treatments for testing the proposed prediction scheme

Control	No prediction scheme	Face (55×45 pixels)
T1	Prediction scheme + same face with $RR \geq \tau$	Face (55×45 pixels)
T2	Prediction scheme + same face with $RR < \tau$	Face (55×45 pixels)
T3	Prediction scheme + another person's face	Face (55×45 pixels)
T4	Prediction scheme + no face 1	Fingerprint (256×256 pixels)
T5	Prediction scheme + no face 2	Eye (226×32 pixels)
T6	Prediction scheme + no face 3	Iris (320×240 pixels)

Fig. 2 (b), (c), and (d) show T1_PR_FRR and T2-6_PR_FAR of the proposed scheme for different prediction thresholds τ and 3 types of CI. T1_PR_FRR is the frequency of a false reject, which occurs when an image of the same face with $RR \geq \tau$ is considered as a "fail" with $ER < \rho$,. T2_PR_FAR is the frequency of a false accept, which occurs when an image of the same face with $RR < \tau$ is considered as a "pass" with $ER \geq \rho$,. T3-6_PR_FAR is the frequency of a false accept, which occurs when each image of another person's face, fingerprint, eye, and iris is considered as a "pass" with $ER \geq \rho$. The RR averages in (b), (c), and (d) are 0.28, 0.50, and 0.70, respectively. Here, the RR average is the mean of the images that are used for calculating CI. If RR average ≈ 1, it is a very strict criterion and it

© IEICE 2012
DOI: 10.1587/elex.9.133
Received November 10, 2011
Accepted January 03, 2012
Published February 10, 2012



(a) A sample of ci_i in CI and pc_i in B

(b) RR average of $CI = 0.29$

(c) RR average of $CI = 0.50$

(d) RR average of $CI = 0.70$

Fig. 2. FRR and FAR of the proposed scheme

makes a sharp distinction between the same face with $RR \geq \tau$ in T1 and others.

If $\rho = 0.8$, we can conclude the following:

- T1_PR_FRR is 0.07 in (b), 0.08 in (c), and 0.08 in (d).
- T2_PR_FAR is 0.80 in (b), 0.44 in (c), and 0.09 in (d). If the RR average of images for CI is over 0.50, the proposed prediction scheme based on CI distinguishes a face with $RR < \tau$.
- T3-6_PR_FAR are 0.12, 0.13, 0.09, and 0.10 in (b); 0.07, 0.07, 0.05, and 0.06 in (c); and 0.01, 0.02, 0.00, and 0.01 in (d), respectively. The proposed prediction scheme based on CI distinguishes between the same face and others.

4 Conclusions

We proposed a novel scheme for predicting the recognition performance by using the confidence interval CI. The proposed scheme attempts to reduce the unstableness of information acquired using sensors. In addition, it can be applied in real-time, thus realizing true multi-factor authentication. The experimental results showed that the RR average of images for CI was higher, implying that the proposed prediction scheme had better performance. Furthermore, it was found that a prediction threshold ρ value of 0.8 realized efficient and true biometric-based multi-factor authentication.

Acknowledgments

This work was supported by Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of

© IEICE 2012
DOI: 10.1587/elex.9.133
Received November 10, 2011
Accepted January 03, 2012
Published February 10, 2012

Education, Science and Technology (2010-0028298).

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2011-0012543).

DOI: 10.1587/elex.9.133
Received November 10, 2011
Accepted January 03, 2012
Published February 10, 2012