Biometric Person Authentication Method Using Camera-Based Online Signature Acquisition

Daigo Muramatsu[1,2], Kumiko Yasuda[3] and Takashi Matsumoto[3]
[1]Department of Electrical and Mechanical Engineering, Seikei University
3-3-1 Kichijouji-kitamachi, Musashino-shi, Tokyo, Japan
[2]Research Center for Information Security (RCIS)
National Institute of Advanced Industrial Science and Technology (AIST)
1-18-13, Sotokanda, Chiyoda-ku,Tokyo, Japan
[3]Department of Electrical Engineering and Bioscience, Waseda University
3-4-1 Okubo, Shinjuku-ku, Tokyo, Japan
[1]muramatsu@st.seikei.ac.jp
[3]{yasuda06,takashi}@matsumoto.elec.waseda.ac.jp

Abstract

A camera-based online signature verification system is proposed in this paper. One web camera is used for data acquisition, and a sequential Monte Carlo method is used for tracking a pen tip. Several distances are computed from an online signature, and a fusion model trained by using AdaBoost combines the distances and computes a final score. Preliminary experiments were performed by using a private database. The proposed system yielded an equal error rate (EER) of 4.0%.

1. Introduction

It is becoming more important to use person authentication technologies to ensure security. Recently, biometric person authentication technologies have been actively studied, and some of them are being used in real situations [4].

Online signature verification is a biometric person authentication technology that uses data obtained while a signature is being written, and it is a promising candidate for several reasons. First, handwritten signatures are widely accepted as means of authentication in many countries for various purposes, such as authorizing credit cards, banking transactions, and signing agreements or legal documents. Second, because online signature verification can incorporate dynamic information about a handwritten signature, it can achieve higher accuracy than verification using static signatures [9]. Moreover, since it is difficult to extract dynamic information from a static signature, it is easier to detect a forgery with online signature verification compared with verification using a static signature. Finally, a person can modify his or her signature if it is stolen. This is a notable feature because physiological biometrics such as fingerprints or irises cannot be modified or renewed[1].

Several data acquisition devices are used for online signature verification, for example, pen-operated digital tablets [15], Tablet PCs [2], PDAs [1], data acquisition pens [6], and cameras [8]. Among them, pen-operated digital tablets are the most common device for data acquisition in online signature verification. However, because tablets are not ubiquitous, they must be specially provided for online signature verification. On the other hand, web cameras have become relatively widespread these days. Therefore, online signature verification using web cameras for data acquisition is very promising. In this paper, therefore, we propose an online signature verification algorithm using a web camera for data acquisition.

To design a camera-based online signature verification algorithm, the following three items should be considered:

1 The position of the web camera
2 The method for obtaining pen trajectories
3 The limited amount of data that can be obtained

In our proposed algorithm, a web camera is placed to the side of the writing hand (at the left side for a right-handed person and at the right side for a left-handed person). A Sequential Monte Carlo method [3] is applied for pen tip tracking, and online signature data are acquired as time-series data of the pen tip position. Neither pen pressure nor

[1] In order to solve this problem, several template protection methods have been proposed [5, 12]

978-0-7695-3725-2/09 $25.00 © 2009 IEEE
DOI 10.1109/ICDAR.2009.112

pen inclination information is available. Thus, several features extracted from the time-series pen position data are combined to improve performance.

For evaluation of the proposed algorithm, a preliminary experiment was performed using a private online signature database captured by a web camera. The experimental results for this private database showed an equal error rate (EER) of 4.0%.

2. Algorithm

Figure1 depicts our camera-based online signature verification algorithm. There are two phases: an enrollment phase and a verification phase. In the enrollment phase, a user inputs his or her ID and writes several signatures for enrollment. During the writing process, images are captured by the web camera. Then, the pen tip position is tracked, and time-series pen position data are obtained. After preprocessing, several features are extracted, and the time-series data of the extracted features are enrolled as reference signatures and are also used for distance calculation. Then, a mean vector of each user is calculated and stored with the ID.

In the verification phase, a user provides his or her ID and writes a signature (test signature). Images are captured, and time-series data of the pen tip position are obtained. After preprocessing, several features are extracted, and time-series data of the extracted features are compared with the reference signatures to calculate several distances. Then, the calculated distances and the mean vector associated with the user ID are input to a fusion model, and a final score is computed. Based on this score, a decision is made.

The enrollment and verification phases involve some of the following stages: (a) data acquisition, (b) pen tracking, (c) preprocessing, (d) feature extraction, (e) distance calculation, (f) mean vector calculation, (g) fusion, and (h) decision making. These stages are explained in this section.

2.1. Data acquisition

A web camera for data acquisition is placed to the side of the writing hand, as depicted in Figure 2. In this figure, the web camera is placed on the left side of the writing hand because the writer is right-handed. The best position of the web camera for acquiring the online signature data is considered to be just below the writing surface. However, because the writing surface generally is not transparent, the pen tip position cannot be acquired from below the writing surface. Munich et al. set a camera above the surface [7]. In this position, the pen tip is sometimes covered by the hand, and therefore, users need to adjust the camera position in order that the pen tip can be acquired. However, this causes rotation and size variation of the signatures. Thus, we considered placing the camera to the side or in front of the writing hand. It should be noted that the y-coordinate information is compressed when the camera is placed in front of the hand, and the x-coordinate information is compressed when the camera is placed to the side because information along the optical axis is compressed. Y-coordinate information has been shown to be more useful than x-coordinate information in online signature verification [10]. Therefore, we placed the web camera to the side of the writing hand in this study. Using a side camera, images such as those in Figure 3 were captured.

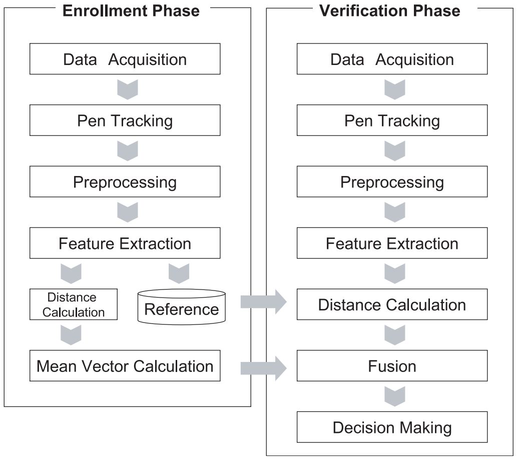

Figure 1. Overall algorithm

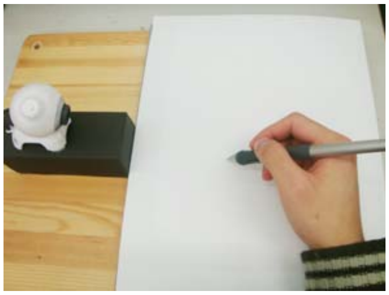

Figure 2. Data acquisition.

2.2. Pen tracking

From the images captured by the web camera, the pen tip was tracked using the Sequential Monte Carlo method [3]. Details of the pen tracking algorithm are described in reference [14]. Using the pen tip position, we obtained the online signature data shown in Figure 4. Figure 5 depicts the obtained online signature data. Though the x-coordinate information was slightly compressed, we can see that online signature data was successfully obtained. The online signature data sig obtained from the images are:

$$sig = (x_t, y_t), t = 1, 2, ..., T, \tag{1}$$

where T is the number of images. Note that only the pen position trajectories are available in camera-based online signature verification.

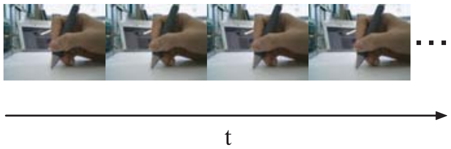

Figure 3. Acquired image data.

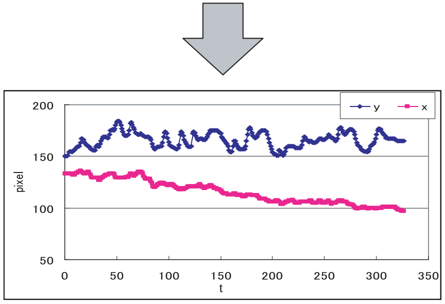

Figure 4. Pen position tracking and obtained data.

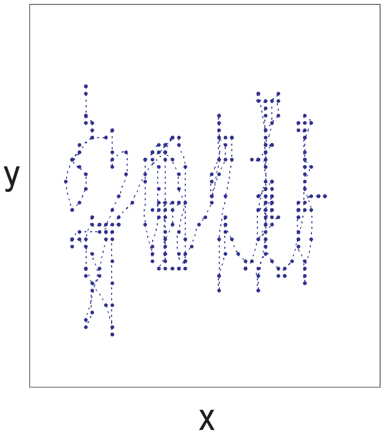

Figure 5. Shape of an acquired signature.

2.3. Preprocessing

The following transformation is performed to obtained the signature data:

$$\bar{x}_t = \frac{x_t - x_g}{x_{max} - x_{min}} \tag{2}$$

$$\bar{y}_t = \frac{y_t - y_g}{y_{max} - y_{min}} \tag{3}$$

where
$$x_g = \frac{1}{T}\sum_{t=1}^{T} x_t, y_g = \frac{1}{T}\sum_{t=1}^{T} y_t$$
$$x_{min} = \min_t x_t, x_{max} = \max_t x_t$$
$$y_{min} = \min_t y_t, y_{max} = \max_t y_t$$

2.4. Feature extraction

The pen movement direction θ and the pen velocity $|V|$ are calculated from the pen position data (x_t, y_t) as follows:

$$\theta_t = \tan^{-1}\frac{y_{t+1} - y_t}{x_{t+1} - x_t} \tag{4}$$

$$|V|_t = \sqrt{(x_{t+1} - x_t)^2 + (y_{t+1} - y_t)^2} \tag{5}$$
$$t = 1, 2, ..., T - 1$$

In the enrollment phase, M items of time-series data of the extracted features are enrolled as reference signatures. Let the enrolled reference signatures $Rsig_m$ be

$$\begin{aligned} Rsig_m &= (rsig_{1,t}^{(m)}, rsig_{2,t}^{(m)}) \\ &= (\theta_t^{(m)}, |V|_t^{(m)}), m = 1, 2, ..., M. \end{aligned} \tag{6}$$

In the verification phase, the time-series data of the extracted feature $Tsig$ is

$$\begin{aligned} Tsig &= ((tsig_{1,t}, tsig_{2,t}) \\ &= (\theta_t^{(0)}, |V|_t^{(0)}). \end{aligned} \tag{7}$$

2.5. Distance calculation

The distances between two sets of time-series data of the extracted features are calculated using dynamic time warping [11]. In the enrollment phase, the distances between reference signatures are calculated, and in the verification phase, extracted features from a test signature and reference signatures are calculated. A distance associated with θ and a distance associated with $|V|$ are calculated independently. The calculated distance vectors in the enrollment phase are

$$\begin{aligned} D(Rsig_n, Rsig_m) &= (D_1^{(n,m)}, D_2^{(n.m)}) \\ &= (dist_\theta^{(n,m)}, dist_{|V|}^{(n,m)}) \qquad (8) \\ n &= 1, 2, ..., M, m = 1, 2, ..., M.(9) \end{aligned}$$

Here, $D(Rsig_n, Rsig_m)$ is a distance vector calculated between the n-th and m-th reference signatures, and the distance vectors calculated in the verification phase are

$$\begin{aligned} D(Tsig, Rsig_m) &= (D_1^{(0,m)}, D_2^{(0,m)}) \\ &= (dist_\theta^{(0,m)}, dist_{|V|}^{(0,m)}) \qquad (10) \\ m &= 1, 2, ..., M, \end{aligned}$$

where $D(Tsig, Rsig_m)$ is a distance vector calculated between the time-series data of the extracted features and the m-th reference signature.

2.6. Mean vector calculation

In the enrollment phase, a mean vector for each user is calculated as follows:

$$Mean = (\bar{D}_1, \bar{D}_2) \tag{11}$$

$$\bar{D}_i = \frac{1}{M(M-1)} \sum_{n=1}^{M} \sum_{m=1, m\neq n}^{M} D_i^{(n,m)}, \tag{12}$$

and this mean vector is stored together with the user's ID.

2.7. Score calculation

A score for decision making is calculated in this stage. A distance vector and associated mean vector are input to a fusion model, and a final score $Score$ is computed:

$$Score(Tsig) = \frac{1}{M} \sum_{m=1}^{M} f(D(Tsig, Rsig_m), Mean; \Theta). \tag{13}$$

Here, Θ is a parameter set of fusion model $f(\cdot)$. L simple perceptrons are randomly generated, and these perceptrons are combined using AdaBoost [13] to generate a fusion model. Thus, a parameter set is composed of weight parameters of simple perceptrons and the confidence level of each perceptron.

2.8. Decision making

A final decision is made based on the following rule:

$$Tsig \text{ is} \begin{cases} \text{Accepted if } Score(Tsig) \geq TRD(c) \\ \text{Rejected if } Score(Tsig) < TRD(c) \end{cases} \tag{14}$$

where $TRD(c)$ is a threshold value, and c is a parameter for adjusting the threshold value.

3. Experiment

3.1. Database

Online signature data from thirteen students was collected. All of the students were right-handed. Each student wrote ten genuine signatures in a first session and ten genuine signatures in a second session, giving a total of twenty genuine signatures from each student. For forgery data, two different students acted as forgers to imitate genuine signatures. The forgers could see video images of genuine signatures previously captured by the web camera, allowing them to see dynamic information of the genuine signatures that they attempted to imitate. Each forger produced 30 forgeries for each genuine user, giving a total of 60 forgeries for each genuine user. All the students were instructed to write their signatures within a predetermined area, and the position of the web camera used for data acquisition was fixed against the writing area.

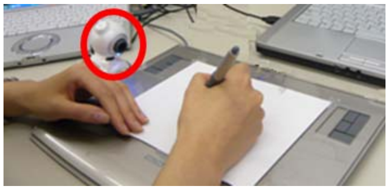

Figure 6. Devices used for data collection

The web camera had a resolution of 320×240 pixels and captured 30 images per second and this camera was . For comparison purpose, a pen-operated digital tablet was also used for data acquisition (Figure 6). Thus, two kinds of signature data, captured by the camera(camera-data) and captured by the tablet(tablet-data), are available in this database.

3.2. Experimental setting

First, five of the genuine signatures collected in the first session were used for enrollment ($M = 5$), and the remaining 15 genuine signatures and 60 forgeries were used for evaluation. A training data set was necessary for generating the fusion model. Therefore, the evaluated data was divided into two groups and two cross-validations were performed.

The number of simple perceptrons L used for the fusion model was set to 2500.

Two threshold settings were considered: a use-dependent threshold parameter (UD TRD) and a global threshold parameter (GL TRD).

3.3. Experimental results

Equal error rates (EERs) of camera-data are summarized in Table 1, and error trade-off curves of caomera-data are illustrated in Figure 7. EERs of θ and $|V|$ in Table 1 represent error rates where each distance calculated from each feature was independently used for verification, and the EER of $\theta+|V|$ is the error where a final score computed by combining these two distances was used for verification. The EERs of θ and $|V|$ were 9.5% and 15.7%, respectively, whereas the EER of $\theta + |V|$ was better, at 4.0%.

Table 1. EER of fusion model [%].

Features	GL TRD	UD TRD
θ	9.5	3.7
$\|V\|$	15.7	11.3
$\theta + \|V\|$	4.0	2.9

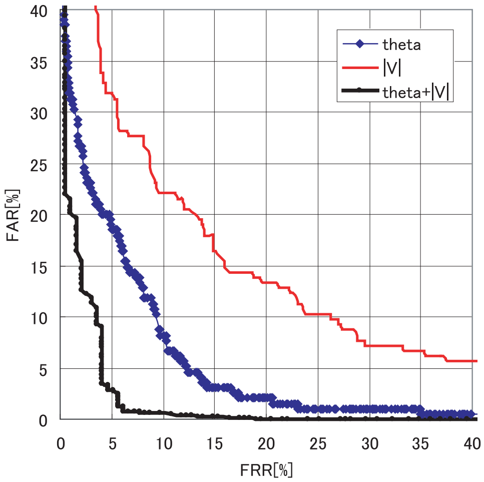

Figure 7. Error trade-off curve of $\theta + |V|$.

4. Conclusions

A camera-based online signature verification algorithm is proposed. A web camera was used for data acquisition, and online signature data was obtained from images captured by the web camera. The Sequential Monte Carlo method was used to track a pen tip in images, and online signature data were obtained as time-series data of the tracked pen tip position. By combining the two features, the accuracy of a camera-based online signature verification system was improved, and achieved EER of 4.0%. However, signature data captured by a web camera were distorted, and this caused accuracy degradation. In fact, an EER of $\theta + |V|$ extracted from tablet-data was 1.0%. Thus, we will attempt to correct the distortion and improve the accuracy. Moreover, we observed several cases where the system lost track of the pen tip when the writer produced an extremely fast stroke, because the images of the pen tip were blurred at that time. In future work, we will attempt to detect these lost points and improve the distance calculation stage so that it can consider lost points. Only two features were used in the current system. In future work, we will also consider other features.

Acknowledgement

This work was supported by the New-Generation Information Security Technologies R&D project (Ministry of Economy, Trade and Industry of Japan).

References

[1] Biosecure multimodal evaluation campaign 2007 (bmec'2007). http://biometrics.it-sudparis.eu/BMEC2007/, 2007.

[2] F. Alonso-Fernandez, J. Fierrez-Aguilar, and J. O.-G. Francisco Del-Velle. On-line signature verification using tablet PC. *Proc. the 4th International Symposium on Image and Signal Processing and Analysis*, pages 245–250, 2005.

[3] A. Doucet, N. de Freitas, and N. Gordon. *Sequential Monte Carlo Methods in Practice*. Springer-Verlag, 2001.

[4] A. K. Jain, P. Flynn, and A. A. Ross. *Handbook of Biometrics*. Springer Science+Business Media, LLC., 2008.

[5] A. K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics*, 2008.

[6] R. Martens and L. Claesen. On-line signature verification: Discrimination emphasised. *Proc. the 4th International Conference on Document Analysis and Recognition*, 2:657–660, 1997.

[7] M. E. Munich and P. Perona. Visual-based id verification by signature tracking. *Proc. 2nd International Conference on Audio- and Video-based Biometric Person Authentication*, 1999.

[8] M. E. Munich and P. Perona. Visual identification by signature tracking. *IEEE Trans. Pattern Analysis and Machine Intelligence*, 25(2):200–217, 2003.

[9] R. Plamondon and G. Lorette. Automatic signature verification and writer identification - the state of the art. *Pattern Recognition*, 22(2):107–131, 1989.

[10] R. Plamondon and M. Parizeau. Signature verification from position, velocity and acceleration signals: A comparative study. *Proc. International Conference on Pattern Recognition*, pages 260–265, 1988.

[11] L. Rabiner and B.-H. Juang. *Fundamentals of speech recognition*. Prentice Hall, 1993.

[12] N. K. Ratha, J. Connell, and R. Bolle. Enhancing security and privacy of biometric-based authentication systems. *IBM Systems Journal*, 40(3):614–634, 2001.

[13] R. E. Schapire and Y. Singer. Improved boosting algorithms using confidence-rated predictions. *Machine Learning*, 37(3):297–336, 1999.

[14] K. Yasuda, D. Muramatsu, and T. Matsumoto. Visual-based online signature verification by pen tip tracking. *Proc. CIMCA 2008*, pages 175–180, 2008.

[15] D.-Y. Yeung, H. Chang, Y. Xiong, S. George, R. Kashi, T. Matsumoto, and G. Rigoll. SVC2004: First international signature verification competition. *Proc. International Conference on Biometric Authentication, LNCS*, 3702:16–22, 2004.