Secure Personnel Authentication Based on Multi-modal Biometrics Under Ubiquitous Environments

Dae-Jong Lee, Man-Jun Kwon, and Myung-Geun Chun*

Dept. of Electrical and Computer Engineering, Chungbuk National University,
Cheongju, Korea
mgchun@chungbuk.ac.kr

Abstract. In this paper, we propose a secure authentication method based on multimodal biometrics system under ubiquitous computing environments. For this, the face and signature images are acquired in PDA and then each image with user ID and name is transmitted via WLAN (Wireless LAN) to the server and finally the PDA receives authentication result from the server. In the proposed system, face recognition algorithm is designed by PCA and LDA. On the other hand, the signature verification is designed by a novel method based on grid partition, Kernel PCA and LDA. To calculate the similarity between test image and training image, we adopt the selective distance measure determined by various experiments. More specifically, Mahalanobis and Euclidian distance measures are used for face and signature, respectively. As the fusion step, decision rule by weighted sum fusion scheme effectively combines the two matching scores calculated in each biometric system. From the real-time experiments, we convinced that the proposed system makes it possible to improve the security as well as user's convenience under ubiquitous computing environments.

1 Introduction

With the advance in communication network, the electronic commerce has been popular according to the rapid spread of Internet. In particular, wireless devices make it possible to enrich our daily lives in ubiquitous environments. Network security, however, is likely to be attacked with intruders and it is faced with the serious problems related to the information security. It is even more difficult to protect the information security under the wireless environment comparing with the wired network. One of the most conventional methods for system security is using password, which is very simple and does not require any special device. However, it can be easily divulged to others. To tackle these problems, biometrics is emerging as a promising technique. In the biometrics, a number of researchers have studied iris, facial image, fingerprint, signature, and voiceprint. Among them, the face recognition is known as the most natural and straightforward method to identity each person.

This face recognition has been studied in various areas such as computer vision, image processing, and pattern recognition. Popular approaches for face recognition

[*] Corresponing author.

I. King et al. (Eds.): ICONIP 2006, Part II, LNCS 4233, pp. 107 – 115, 2006.

are PCA (Principle Component Analysis) [1] and LDA (Linear Discriminant Analysis) [2] methods. However, the major problem with the use of above methods is that they can be easily affected by variations of illumination condition and facial expression. One the other hand, the signature has been a familiar means where it is used for a personal authentication such as making a contact. Online signature recognition methods roughly belong to one of global feature comparison, point-to-point comparison and segment-to-segment comparison methods [3]. For a signature, however, comparing with other features of biometrics, its skilled forgery is more or less easy and system performance is often deteriorated by signature variation from various factors [4].

Though advanced researches based on single biometric modality have been proposed for information security, there are some problems to apply in real life because of lack of confidential accuracy [5-7]. Multimodal biometrics has the advantage of improving security by combination of two biometric modalities such as face and signature [8]. In this paper, we describe an implementation of multimodal biometrics under ubiquitous computing environments. The proposed system is implemented with embedded program in PDA. More specifically, the face images and signatures images are obtained by PDA and then these images with user ID and name are transmitted via WLAN (Wireless LAN) to the server and finally the PDA receives verification result from the server. In our system, face verification system is implemented by conventional PCA and LDA method which calculates eigenvector and eigenvalue matrices using the face image from the PDA at enrollment steps. The signature verification is designed by a novel method based on grid partition, Kernel PCA and LDA. To calculate the similarity between test image and training image, we adopt the selective distance measure determined by various experiments. Here, Mahalanobis and Euclidian distance measures are used for face and signature, respectively. As the fusion step, decision rule by weighted sum fusion scheme is used to effectively combine the two matching scores calculated in each biometric system. The implemented system renders improvements of speed and recognition rate to increase security under ubiquitous computing environments.

This paper is organized as follows. Section 2 describes the system architecture implemented in PDA. In Section 3, we describe the authentication methods for face and signature and fusion method. In Section 4, we presents experiment results obtained by real-time experiment. Finally, some concluding remarks are given in Section 5.

2 System Architecture for PDA Based Personnel Authentication

The proposed system consists of a client module for biometric data acquisition and a server module for authentication. The client module is to register the face and signature image. After then, the acquired user's information is transmitted via WLAN to the server which performs analyzing the transmitted data and sending the authentication result to the client module such as acceptance or rejection. That is, the server deals with image processing and verification algorithm.

For the client module, face images and signatures images are acquired in the PDA program implemented by Microsoft embedded development tool. In the face acquisition process, user's image is obtained from the camera attached to the PDA. Face detection is essential process since the recognition performance directly depends on the quality of acquired face image. Here, we capture a face image by considering the direction and position between two eyes. And then, the captured image is saved in 240x320 pixels BMP format. On the other hand, user's signature is acquired from PDA by stylus pen in acquisition process. Fig 2 shows the user interface environment to acquire the face and signature images. User may select the ID, name, and process step for identity or register from the setup menu.

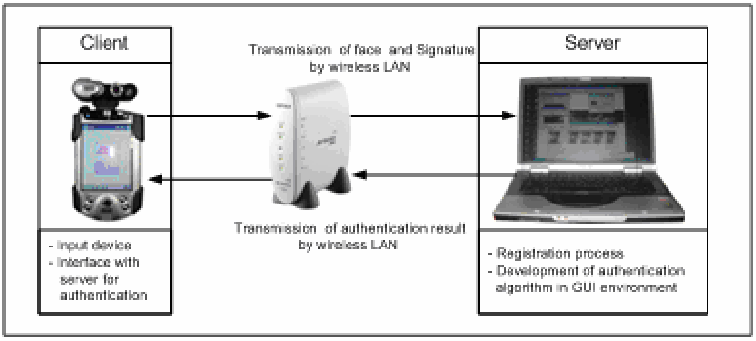
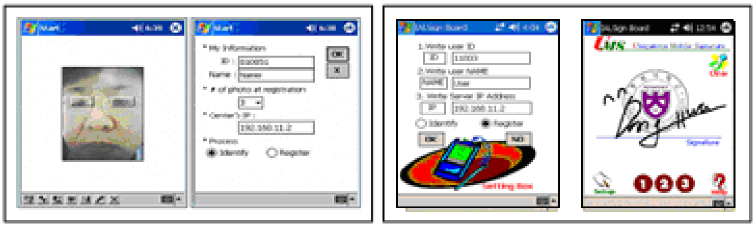

Client
Transmission of face and Signature by wireless LAN
Server
Transmission of authentication result by wireless LAN
- Input device
- Interface with server for authentication
- Registration process
- Development of authentication algorithm in GUI environment

Fig. 1. System architecture for biometric authentication



(a) Face (b) signature

Fig. 2. User interface environment

In the server module, matching score is calculated between input image and registered images in the database. In the registration step for face recognition, feature extraction is performed by PCA and LDA for images transmitted via WLAN from the camera attached to the PDA. And then the calculated features are registered in the database. Authentication is performed by comparing input face with registered face images. For the signature authentication, server receives user's signature from PDA. And then feature extraction is performed by using the algorithm based on grid partition, Kernel PCA and LDA. Finally, decision making for acceptance is performed according to matching scores obtained face and signature module in server, respectively.

3 Multi-modal Biometric Authentication Algorithm

The proposed multi-modal biometric system consists of a face recognition module, a signature recognition module, and a decision module as shown in Fig. 3. Here, the face recognition is designed by PCA and LDA method. The signature recognition is implemented by the grid partition, Kernel PCA, and LDA. As a final step, decision module is implemented with the weighted sum rule. The face recognition system is composed of feature extraction and classification process parts. First, face image is decomposed in each frequency band by wavelet transform to compress it [5]. Then, PCA is applied to reduce the dimensionality of image for low frequency band. Here, we briefly describe the feature extraction based on PCA and LDA used in the face recognition.

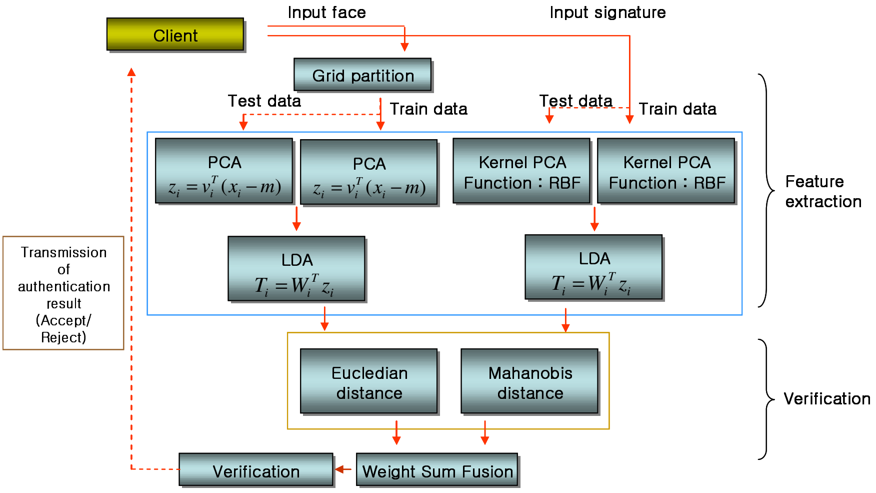


Fig. 3. Proposed multi-modal biometric system

Let a face image be a two-dimensional $n \times n$ array of containing levels of intensity of the individual pixels. An image $\mathbf{z}_i$ may be conveniently considered as a vector of dimension n^2. Denote the training set of N face images by $Z = (\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_N)$. We define the covariance matrix as follows

$$\mathrm{R} = \frac{1}{\mathrm{N}}\sum_{i=1}^{N}(\mathbf{z}_i - \bar{\mathbf{z}})(\mathbf{z}_i - \bar{\mathbf{z}})^T = \Phi\Phi^T \tag{1}$$

$$\bar{\mathbf{z}} = \frac{1}{\mathrm{N}}\sum_{i=1}^{N}\mathbf{z}_i \tag{2}$$

Then, the eigenvalues and eigenvectors of the covariance matrix R are calculated, respectively. Let $E = (\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_r)$ denote the r eigenvectors corresponding to the r largest eigenvalues. For a set of original face images Z, their corresponding reduced feature vectors $X = (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N)$ can be obtained as follows;

$$\mathbf{x}_i = E^T(\mathbf{z}_i - \bar{\mathbf{z}}) \tag{3}$$

The second processing stage is based on the use of the LDA as follows. Consider c classes in the problem with N samples; let the between-class scatter matrix be defined as

$$S_B = \sum_{i=1}^{c} N_i(\mathbf{m}_i - \bar{\mathbf{m}})(\mathbf{m}_i - \bar{\mathbf{m}})^T \tag{4}$$

where N_i is the number of samples in i’th class C_i and $\bar{\mathbf{m}}$ is the mean of all samples, $\mathbf{m}_i$ is the mean of class C_i. The within-class scatter matrix is defined as follows

$$S_W = \sum_{i=1}^{c} \sum_{x_k \in C_i} (\mathbf{x}_k - \mathbf{m}_i)(\mathbf{x}_k - \mathbf{m}_i)^T = \sum_{i=1}^{c} S_{W_i} \tag{5}$$

where, S_{W_i} is the covariance matrix of class C_i. The optimal projection matrix W_{FLD} is chosen as the matrix with orthonormal columns that maximizes the ratio of the determinant of the between-class matrix of the projected samples to the determinant of the within-class fuzzy scatter matrix of the projected sampled, i.e.,

$$W_{FLD} = \arg\max_{W} \frac{|W^T S_B W|}{|W^T S_W W|} = [\mathbf{w}_1 \quad \mathbf{w}_2 \quad \cdots \quad \mathbf{w}_m] \tag{6}$$

where $\{\mathbf{w}_i \mid i = 1,2,\cdots,m\}$ is a set of generalized eigenvectors (discriminant vectors) of S_B and S_W corresponding to the $c-1$ largest generalized eigenvalues $\{\lambda_i \mid i = 1,2,\cdots,m\}$, i.e.,

$$S_B \mathbf{w}_i = \lambda_i S_W \mathbf{w}_i \quad i = 1,2,\ldots,m \tag{7}$$

Thus, the feature vectors $V = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_N)$ for any face images $\mathbf{z}_i$ can be calculated as follows

$$\mathbf{v}_i = W_{FLD}^T \mathbf{x}_i = W_{FLD}^T E^T(\mathbf{z}_i - \bar{\mathbf{z}}) \tag{8}$$

After obtaining the feature vectors, the classification is achieved by finding the minimum distance between the coefficients of test patterns and training patterns. Here, the distance is calculated by Mahalanobis distance measure.

For the signature recognition system, features are calculated by Kernal PCA and LDA. Before projecting the original features by Kernel PCA, a signature image is projected to vertical and horizontal axes by grid partition method [8]. Kernel PCA can be derived using the known fact that PCA can be carried out on the dot product matrix instead of the covariance matrix [9]. Let $\{x_i \in R^M\}_{i=1}^N$ denote a set of data. Kernel PCAfirst maps the data into a feature space F by a function $\Phi : R^M \rightarrow F$, and then performs standard PCA on the mapped data. Defining the data matrix X by $X = [\Phi(x_1)\ \Phi(x_2) \cdots \Phi(x_N)]$, the covariance matrix C in F becomes

$$C = \frac{1}{N}\sum_{1}^{N} \Phi(x_i)^T \Phi(x_i) = \frac{1}{N} X^T X \tag{9}$$

We assume that the mapped data are centered as $1/N \cdot \Sigma_1^N \Phi(x_i) = 0$. We can find the eigenvalues and eigenvectors of C via solving the eigenvalues problem

$$\lambda u = Ku \tag{10}$$

The $N \times N$ matrix K is the dot product matrix defined by $K = 1/N \cdot X^T X$ where

$$K_{ij} = \frac{1}{N}\Phi(x_i) \bullet \Phi(x_i) = \frac{1}{N}k(x_i, x_j) \tag{11}$$

Let $\lambda \geq \cdots \geq \lambda_p$ be the nonzero eigenvalues of K ($P \leq N$, $P \leq M$) and $u^1, \cdots, u^P$ the corresponding eigen-vectors. Then C has the same eigenvalues and there is a one-to-one correspondence between the nonzero eigen-vectors $\{u^h\}$ of K and the nonzero eigenvectors $\{v^h\}$ of C : $v^h = \alpha^h X u^h$, where α^h is a constant for normalization. If both of the eigenvectors have unit length, $\alpha^h = 1/\sqrt{\lambda_h N}$. We assume $\|v^h\| = 1/\sqrt{\lambda_h N}$ so that $\alpha^h = 1$.

For a test data x , its hth principal component y_h can be computed using Kernel function as

$$y_h = v^h \bullet \Phi(x) = \sum_{i=1}^{N} u_i^k k(x_i, x) \tag{12}$$

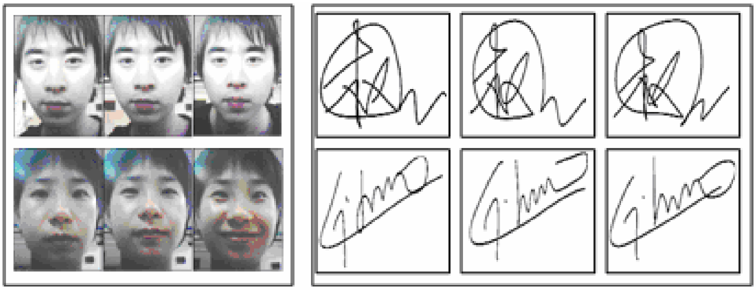
Then the Φ image of x can be reconstructed from its projections onto the first H ($\leq P$) principal components in F by using a projection operator P_H

$$P_H \Phi(x) = \sum_{h=1}^{H} y_h v^h \tag{13}$$

The Kernel PCA allows us to obtain the features with high order correlation between the input data samples. In nature, the Kernel projection of data sample onto the Kernel principal component might undermine the nonlinear spatial structure of input data. Namely, the inherent nonlinear structure inside input data is reflected with most merit in the principal component subspace. To extract feature, we use LDA as well as a Kernel PCA so as to examine the discriminative ability of Kernel principal components. After obtaining the feature vectors, classification is achieved by finding the minimum distance between the coefficients of test patterns and training patterns. Here, the distance is calculated by Euclidean distance measure and finally fusion scheme is implemented by weighted sum rule for similarities obtained from face and signature [8].

4 Experiments and Analysis

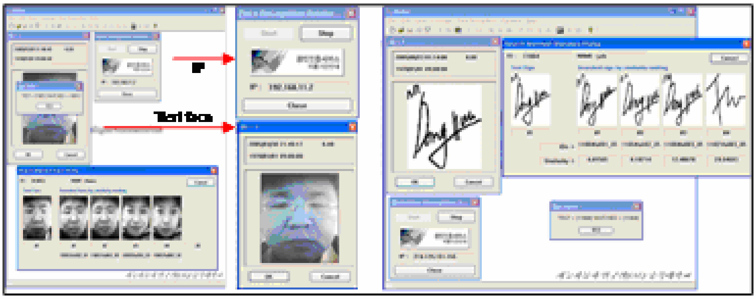
To evaluate the proposed method, face and signature are transmitted via WLAN from PDA. First, three faces and signatures for each user are registered with ID number. Recognition is performed by comparing face and signature images with registered ones. Fig. 4 shows some samples of face or signature images acquired from the PDA. The original size of face image is 240×320. However, it is resized as 128×128 pixel image whose gray level ranges between 0 and 255. Finally, the compressed face image is obtained by performing 4-level wavelet packet transform. On the other hand, the size of signature is 240×100. After applying the PPP matching, 2-dimensional signature is rearranged in vector form having horizontal and vertical information [8]. For the preprocessed face and signature images, feature extraction method is applied to obtain the features such as described in Section 3.



(a) Faces (b) Signatures

Fig. 4. Some samples of faces and signatures acquired from PDA

Figure 5 shows the recognition result executed in the server. As seen in Fig 5, four candidate images are displayed according to the matching score. In this Figure, the leftmost image is the testing one to be authenticated and the others are matched in the server. Among theses images, leftmost image has the highest matching score for the input image. So the server considers him as a genuine person when the matching score is higher than a predefined threshold value.

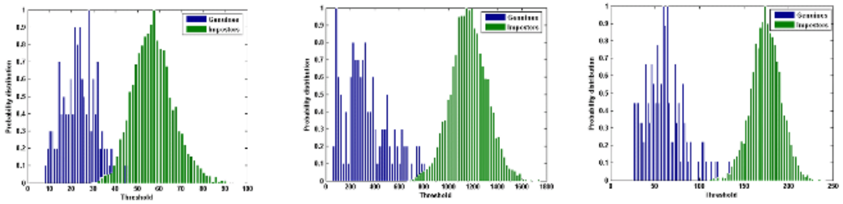


(a) Face recognition (b) Signature recognition

Fig. 5. Recognition process in the server

Figure 6 shows the similarity between genuine and imposter according to the threshold which determines the accept/reject for face and signature, respectively. Here, the number of data is 3 and 44 per person for genuine and imposter. Our experiment uses the 45 person. As seen in Fig. 6-(a) (b), performance shows the best performance when threshold is 38 and 780 for signature and face, respectively. Fig 6-(c) shows the performance applying fusion technique based on weighted sum rule. Final matching degree is calculated by d1+0.1×d2, where d1 is the value obtained

Euclidian distance for signature and d2 is the Mahalanobis distance for face. As seen in Fig. 6-(c), the fusion scheme makes discrimination between genuine and imposter larger than single biometrics.



(a) signature (b) face (c) fusion scheme

Fig. 6. Discrimination between genuine and imposter

Fig 7 shows the ROC curve representing FAR(false acceptance rate) and FRR(false reject rate). As seen in Fig 7, the performance shows best performance when threshold is 122. Table 1 shows recognition rate with respect to EER (error equal rate). The error rates are 5.5% and 3.7% by signature and face verification system, respectively. Finally, the multi-modality makes the error rate lower than single modal system by effectively combining two biometric features. More specifically, the error rate shows 1.1 % and one can find that the proposed method can be used to establish a higher security system.

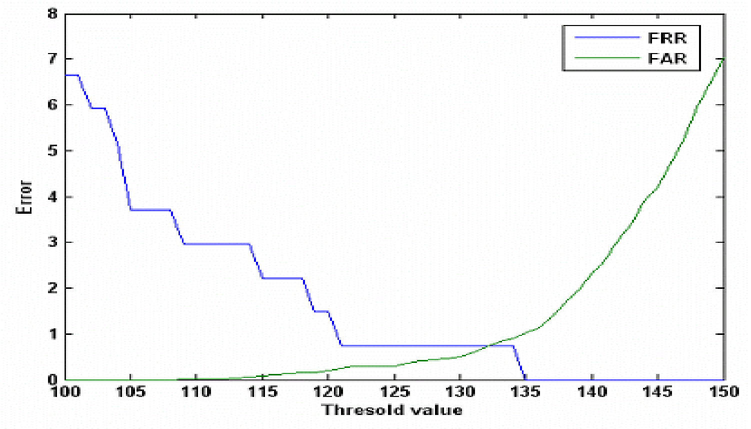


Fig. 7. The ROC curve obtained by applying fusion scheme

Table 1. EER rate according to each applied method

Rate	Signature	Face	Multi-modal
EER	5.5%	3.7%	1.1%

5 Concluding Remarks

In this work, we suggested a multimodal biometrics system under ubiquitous computing environments. Our system consists of face and signature verification system implemented in PDA and server network. Specifically, the face and signature are transmitted to server and PDA receives the verification results via WLAN coming from decision in the server. Face verification system is implemented by conventional PCA and LDA method and signature verification is designed by a novel method based on grid partition, Kernel PCA and LDA. As the fusion step, decision rule by weighted sum fusion scheme is used to effectively combine the two matching scores calculated in each biometric system. From various real-time experiments, we found that the fusion scheme made the error rate lower than single modal system. Therefore, we confirm that the proposed method can be applied to the applications for personnel authentication where higher security is required.

Acknowledgement. This work was supported by ETRI, Korea 2006.

References

[1] M. Turk, A. Pentland, Eigenfaces for Recognition, Journal of Cognitive Neuroscience, Vol. 3 (1991) 72-86

[2] Wenyi Zhao, Arvindh Krishnaswamy, Rama Chellappa, Discriminant Analysis of Principal Components for Face Recognition,Face Recognition from Theory to Application, Springer, (1998).

[3] Kiran G. V., Kunte R. S. R., Saumel S., On-line signature verification system using probabilistic feature modeling, Signal Processing and its Applications, Sixth International Symposium, Vol. 1 (2001) 351-358.

[4] Ma Mingming, Acoustic on-line signature verification based on multiple models, Computational Intelligence for Financial Engineering, Proceedings of the IEEE/IAFE/INFORMS Conference (2000) 30-33

[5] Keun-Chang Kwak, Pedrycz, W., Face Recognition using Fuzzy Integral and Wavelet Decomposition Method, Systems, Man and Cybernetics, Part B, IEEE Trans., Vol. 34 (2004) 1666-1675

[6] Jie Yang, Xilin Chen, Willam Junz, A PDA-based Face Recognition System, Proceeding of the sixth IEEE Workshop on Application of Computer Vision (2002) 19-23

[7] Jong Bae Kim, A Personal Identity Annotation Overlay System using a Wearable Computer for Augmented Reality, Consumer Electronics, IEEE Trans., Vol. 49 (2003) 1457 – 1467

[8] Dae Jong Lee, Keun Chang Kwak, Jun Oh Min, Myung Geun Chun, Multi-modal Biometrics System Using Face and signature, A.Lagana et al.(Eds.): LNCS 3043 (2004) 635-644

[9] B. Scholkopf, A. Smola, Nonlinear Component Analysis as a Kernel Eigenvalue Problem, Neural Computation, Vol. 10 (1998) 1299-1319