Personal based authentication by face recognition

Yung-Wei Kao, Hui-Zhen Gu, and Shyan-Ming Yuan
Department of Computer Science and Engineering
National Chiao Tung University, 1001 Ta Hsueh Rd., Hsinchu 300, Taiwan
{ywkao, hcku}@cs.nctu.edu.tw, smyuan@cis.nctu.edu.tw

Abstract

Authentication is a significant issue in system control. Traditional account based authentication doesn't guarantee the exact person of the account. It also suffers from the easily guessed problem. On the other hand, the camera is more and more popular. Personal based authentication via cameras becomes possible for mobile users. In the paper, we propose the PBAS, which conducts the authentication depends on both face image and password. We claim that the password information can be used to enhance face recognition rate, which is the most significant benchmark for identification system. Finally, we simulate the PBAS by PCA method based on both database we constructed and a subset of FERET. The result of experiment shows that our system performs much better than the PCA method without password integration.

1. Introduction

Authentication is a significant issue in system control. Traditionally, the account based authentication is applied to recognize who is the current user. The users login to the system by their accounts and passwords. After the login, the consequent actions can be logged as belonging to a specific user.

However, the account does not exactly represent the user himself. One user can own several accounts in a system, and one account can be used by several users. In many scenarios, it is significant to know who the user is, such as the critical business transactions. Many systems solve the problem by maintaining additional personal information while requesting the account. However, the account can still be used by those people knowing the password. Moreover, the account often composed by several characters or numbers, which is easily guessed.

On the other hand, the camera is more and more popular. A lot of mobile devices and notebooks are equipped with built-in cameras. There are products (Lenovo Y510, IdeaPad Y510) even support face image recognition for authentication via cameras. The concept of face recognition for authentication has been implemented in products. However, most of them only depend on face images. We know that face image is public information; it is easy to be acquired. For example, we can login to the notebook owned by the president of the United States simply by showing his picture in front of the camera.

Face recognition has been developed for a long time [1][2][3]. The most significant issue of face recognition is that the recognition rate is difficult to be 100%. The recognition rate of face recognition should be as high as possible.

In our research, we propose the personal based authentication system (PBAS). PBAS conducts the authentication depends on both face image and password. PBAS has several advantages. First, the account factors of account based authentication are replaced by face images. Hence, the person who he is will be guaranteed. Second, only the face images are not enough to login, the passwords are still needed. Third, the accounts can be easily guessed, but the face images are not easily fabricated if you don't know who the owner is. Finally, we will show that, the password is able to be utilized to enhance the face recognition rate.

The paper is organized as followings: chapter 2 describes the system overview. Chapter 3 introduces the system design. Chapter 4 reviews the PCA method. Chapter 5 illustrates the evaluation of our simulation program. Finally, the conclusion is drawn.

2. System Overview

Figure 1 represents the system overview of our research. The figure illustrates that a user is buying

978-0-7695-3322-3/08 $25.00 © 2008 IEEE
DOI 10.1109/NCM.2008.167

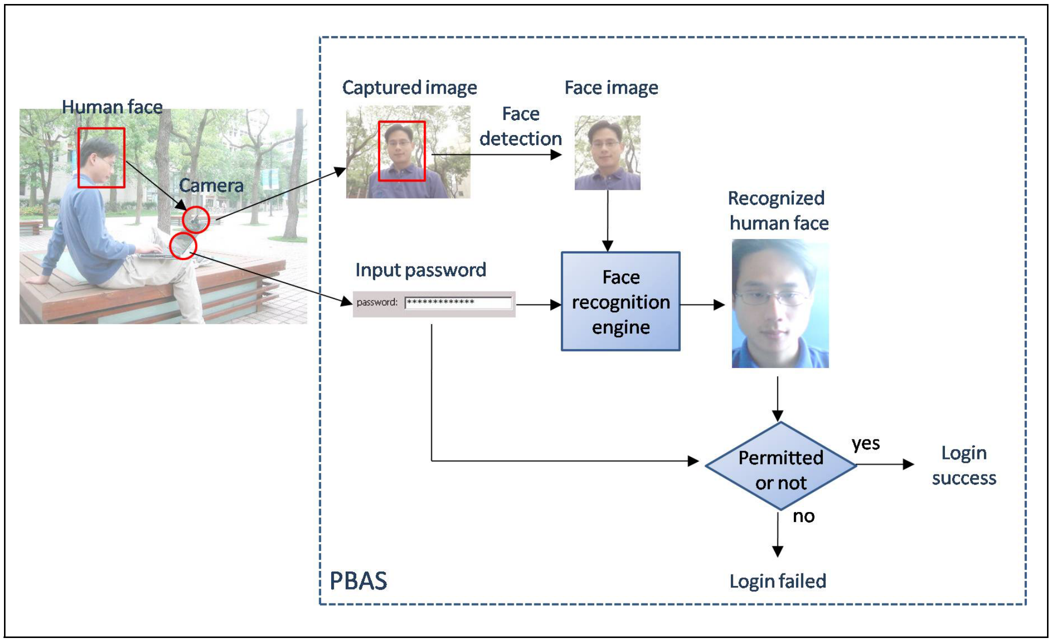


Figure 1. System overview

something on the Internet. He has to login to the PBAS before making the purchase decision. In order to login the system, the camera on his notebook takes a picture of his face. After that, the captured image and input password are sent to PBAS. In PBAS, the captured image should be preprocessed first, and the face image is extracted. The extracted face image will be sent to the face recognition engine, and the recognized face is identified. During the recognition process, the input password can be utilized to enhance the recognition rate. Finally, PBAS will check whether the identified person is permitted to login. We claim that the face recognition rate can be improved by password. The recognition rate is improved by eliminating impossible candidates based on password.

For face recognition, there are a lot of technologies can be adopted as the recognition engine, such as PCA (Principal Component Analysis) [4], HMM (Hidden Markov Model) [5], AdaBoost [6], ANN (Artificial Neural Network) [7], etc. Although the recognition technologies are different, most of them follow the basic concept of pattern recognition. The basic pattern recognition concept is to derive several liner/nonlinear lines to separate the feature space into multiple clusters. For example, Figure 2 has nine clusters, from C1 to C9.

If point *p* belongs to C5 in Figure 1 actually, it will be recognized to be in C4 incorrectly. However, if we dynamically reduce some impossible clusters by additional information, such as password, the result will be different. For example, in Figure 3, there are five clusters remaining.

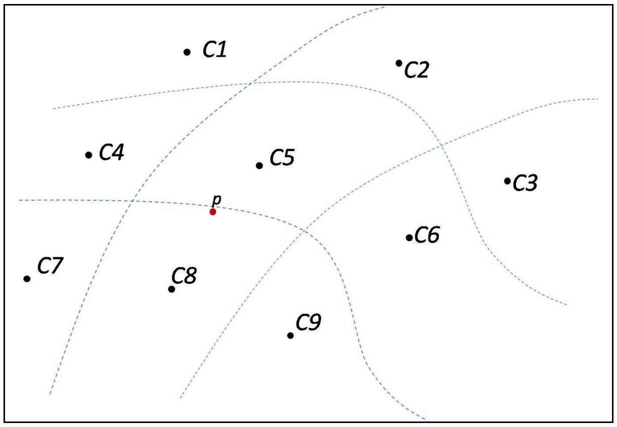


Figure 2. Nine clusters in feature space

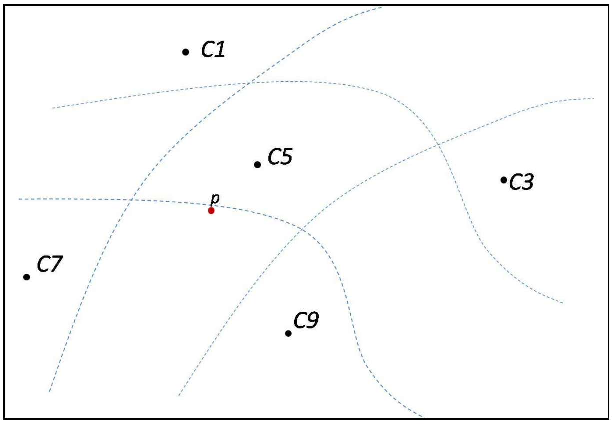


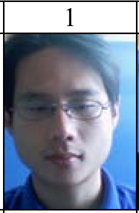
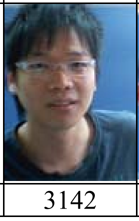
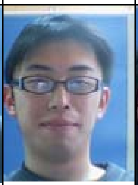
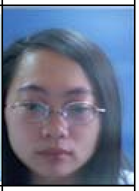
Figure 3. Five clusters in feature space

In this case, although *p* belongs to no cluster, the distance between *p* and the center of C5 is the smallest, so it can be correctly clustered into C5. This example provides the intuition of how the recognition rate can be improved.

3. System Design

PBAS maintains the mapping between the user faces and passwords, as shown in table 1. It can be noticed that, different person can choose the same password, although it is rare. For example, the first person and the second person choose the same password "4398"; the third person and the fourth person choose the same password "3142".

Table 1. Face and password mapping example

	1	2	3
Faces			
passwords	4398	4398	3142
	4	5	6
Faces			
passwords	3142	3933	5915

We integrate the password with the recognition engine to improve recognition rate. The integration point takes place at the final stage of face recognition engine. The integration process is shown in figure 4. First of all, we take input password, and check the available face password mapping. If this password is not available for any candidate, such candidate will be eliminated before the final stage of recognition process. After that, the remaining processes of traditional face recognition are conducted.

For example, in figure 4, the average correctly guesses rate is 1/5 without the elimination. On the other hand, after integration, the average correctly guesses rate is 1/2, which is 2.5 times higher than the previous one. It is the main idea that how the face recognition rate can be improved. The recognition rate can be enhanced if the error recognized face symbol is eliminated.

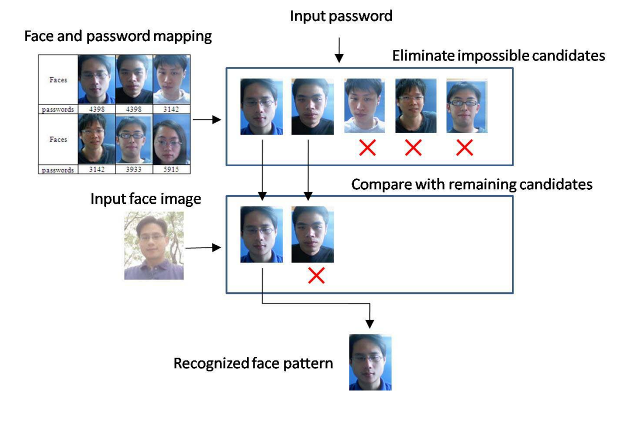


Figure 4. Integration process

4. PCA (Principal Component Analysis)

This section reviews the PCA method [4], which has been widely used in applications such as face recognition and image compression. PCA is a common technique for finding patterns in data, and expressing the data as eigenvector to highlight the similarities and differences between different data. The following steps summarize the PCA process.

1. Let $\{D_1, D_2, \ldots D_M\}$ be the training data set. The average *Avg* is defined by:

$$Avg = \frac{1}{M}\sum_{i=1}^{M} Di$$

2. Each element in the training data set differs from *Avg* by the vector $Y_i = D_i - Avg$. The covariance matrix *Cov* is obtained as:

$$Cov = \frac{1}{M}\sum_{i=1}^{M} Yi \cdot Yi^T$$

Since the covariance matrix *Cov* is square, we can calculate the eigenvectors and eigenvalues for this matrix.

3. Choose M' significant eigenvectors of *Cov* as E_K*'s*, and compute the weight vectors W_{ik} for each element in the training data set, where *k* varies from 1 to M'.

$$W_{ik} = E_k^T \bullet (D_i - Avg),\ \forall\, i\, ,k$$

Based on PCA, many face recognition techniques have been developed, such as *eigenfaces* [1]. The following steps summarize the *eigenface* recognition process:

1. Initialization: Acquire the training set of face images $I_1,I_2,...I_M$. Calculate each face difference vector from the average face *Avg* by (1), and the covariance matrix *Cov* is obtained by (2). Then compute the eigenvectors E_k of *Cov*, which define the face space. Finally, compute the weights W_{ik} by (3) for each image in the training set.
2. Input querying: When a new testing face image is encountered, calculate a set of weights W_{testK} depending on the same steps mentioned above. The weights W_{testk} forming a vector T_p $=[w_1,w_2,...,w_{M'}]^T$ describes the contribution of each *eigenface* in representing the input face image
3. Recognition: A simplest technique to classify the weight pattern is to compute the minimum distance of $\mathrm{W}_{\mathrm{testK.}}$ from $\mathrm{T}_{\mathrm{P.}}$ It means that the test image can be classified to be in class *p* when $min(Dp) < \Theta i$, where $Dp=|| W_{testK} - T_P ||$ and Θi is the threshold.

Figure. 6 shows a simplified version of face space to illustrate the projecting results of three training face images W_1, W_2, W_3 and a testing image W_{testk}. We can recognize W_{testk}. as one of the three known individuals W_1, W_2 and W_3 by the projecting distance between W_{testk} with each training images. In this case, there are two *eigenfaces* $\mathrm{e}_1,\mathrm{e}_2$ to construct the face space. The distance between W_{testk} and W_2 is larger than the threshold Θ_i, they are not considered to be the same person consequently. Furthermore, the projecting location of W_{testk} in the face space is more close to the projecting location of W_1 than W_2. Therefore, we believe that W_{testk}. and W_1 are the same person.

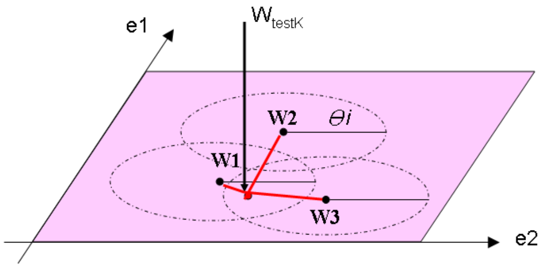
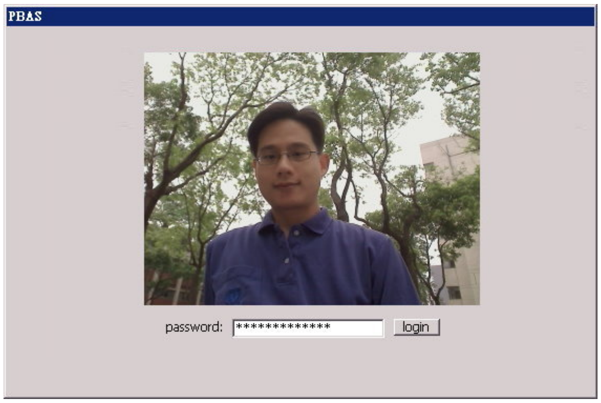


Figure 5. A simplified version of face space

5. Evaluation of simulation

We simulate the PBAS with C++ program. The screenshot of PBAS is shown in figure 6. The face recognition is performed by the basic PCA method. In the paper, we conduct two experiments. In the first experiment, the face database we used is constructed by our self, which contains twenty face patterns and ten images per pattern.


PBAS

password: *************

Figure 6. The screenshot of PBAS

Table 2 and figure 7 illustrate the recognition rate of original face recognition *P* (Probability without integration), and integrated face recognition P_i (Probability with integration). We analyze the recognition rate if there are one to five training images of these two recognition method. In general, P_i is always higher than *P*.

Table 2. Recognition rate of *P* and P_i (1)

	training data				
	1	2	3	4	5
P	0.83	0.88	0.885	0.9	0.915
P_i	0.98	0.985	0.99	0.99	0.995

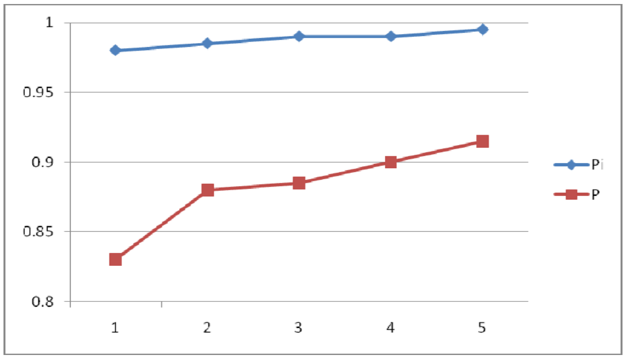


Figure 7. Recognition rate of *P* and P_i (1)

In the second experiment, the face database we used is a subset of gray FERET database [8], which contains twenty face patterns and ten images per pattern. Table 3 and Figure 8 show the recognition rate of original face recognition and integrated face recognition. In this experiment, P_i is also always outperforms than *P*.

Table 3. Recognition rate of P and P_i (2)

	training data				
	1	2	3	4	5
P	0.46	0.53	0.615	0.665	0.745
P_i	0.765	0.88	0.945	0.985	0.985

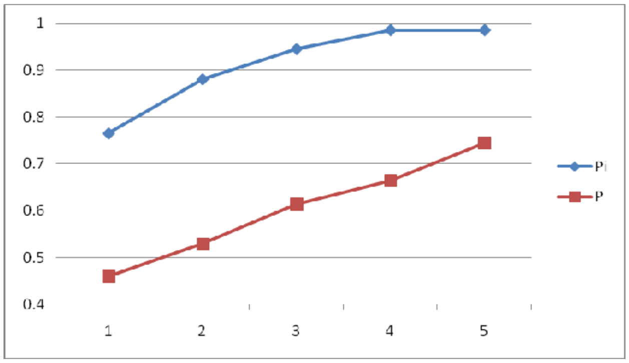


Figure 8. Recognition rate of P and P_i (2)

6. Conclusion

In conclusion, we propose the PBAS solution which conducts the authentication depends on both face image and password. The system focus on personal based authentication and has several advantages. First, the account factors of account based authentication are replaced by face images. Hence, the person who exactly he is will be guaranteed. Second, only the face images are not enough to login, the passwords are still needed. Thus, the system will not be easily cracked by simply showing a picture of the owner in front of camera. Third, the accounts can be easily guessed, but the face images are not easily fabricated if you don't know who the owner is. Finally, we show that the password is able to be utilized to enhance the face recognition rate dramatically.

7. References

[1] Turk, M. A. and A. P. Pentland, "Face recognition using eigenfaces", in Proc. IEEE Conf. CVPR, June 3-6, 1991, pp.586-591.

[2] Brunelli, R. and T. Poggio, "Face recognition: features versus templates," IEEE Trans. Pattern Analysis and Machine Intelligence, Vol.15, No.10, pp.1042-1052, 1993.

[3] A.M. Burton, S. Wilson, M. Cowan, V. Bruce, "Face recognition in poor-quality video: Evidence From Security Surveillance", Psychological Science, Vol. 10, No. 3, May 1999, pp. 243-248

[4] Fukunaga, Keinosuke, "Introduction to Statistical Pattern Recognition," Elsevier,1990

[5] L. R. Rabiner and B. H. Juang, "An introduction to hidden Markov models", IEEE ASSP Mag., pp 4--16, Jun. 1986.

[6] Yoav Freund and Robert E. Schapire, "A short introduction to boosting", Journal of Japanese Society for Artificial Intelligence, 14(5):771--780, September, 1999.

[7] Gurney K., An Introduction to Neural Networks, UCL Press, 1997, ISBN 1 85728 503 4

[8] FERET database, http://www.itl.nist.gov/iad/humanid/feret/feret_master.html