Fingerprint Authentication Based on Matching Scores with Other Data

Koji Sakata[1], Takuji Maeda[1], Masahito Matsushita[1], Koichi Sasakawa[1], and Hisashi Tamaki[2]

[1] Advanced Technology R&D Center, Mitsubishi Electric Corporation, 8-1-1, Tsukaguchi-Honmachi, Amagasaki, Hyogo, 881-8661, Japan
[2] Faculty of Engineering, Kobe University, 1-1, Rokkodai, Nada, Kobe, Hyogo, 657-8501, Japan

Abstract. A method of person authentication based on matching scores with the fingerprint data of others is proposed. Fingerprint data of others is prepared in advance as a set of representative data. Input fingerprint data is verified against the representative data, and the person belonging to the fingerprint is confirmed from the set of matching scores. The set of scores can be thought of as a feature vector, and is compared with the feature vector already enrolled. In this paper, the mechanism of the proposed method, the person authentication system using this method are described, and its advantage. Moreover, the simple criterion and selection method of the representative data are discussed. The basic performance when general techniques are used for the classifier is FNMR-3.6% at FMR-0.1%.

1 Introduction

Generally, biometric authentication systems either use the biometric data as is or use some processed version of the biometric as feature data. There is a real danger with this kind of authentication that if the enrolled data is leaked, the leaked data could be used to impersonate the legitimate user for illegitimate purposes. When a password is used for authentication, all you need do is to change the password in the event that the password is leaked, but biometric data cannot generally be changed. Then, the method of making former data not restorable is proposed as a protection method of the enrolled data. Biometric data is transformed by one way function or geometrical conversion[1]. Moreover, biometric data is protected by using the cryptology, and there is a method of correcting swinging of the input image by using helper data[2].

Now we use fingerprint authentication scheme using features extracted from fingerprint images[3]. We propose a method of fingerprint matching based on matching scores with other data[4]. A set of representative data is prepared in advance, and the set of scores obtained by verifying the input data against the set is regarded as a feature vector.

First we will provide an overview of conventional matching and proposal methods. Moreover, the person authentication system using this method is described,

D. Zhang and A.K. Jain (Eds.): ICB 2006, LNCS 3832, pp. 280–286, 2005.

and it explains the advantage. Next, we consider what feature data is suitable for the representative data, and a simple criterion is discussed. Finally, general techniques are applied to the classifier, and the basic performance of the correlation matching is clarified.

2 Conventional Matching and Correlation Matching

In this section we describe differences of conventional matching and correlation matching.

2.1 Conventional Fingerprint Matching

In conventional matching, features extracted from fingerprint image or the image are verified. Important to note is that, while there are some differences in the data being verified, there is no difference in the enrollment of his fingerprint data to the system (Fig. 1).

Since having the user's biometric data is required for conventional matching, this means that the data has to be stored somewhere in an authentication system. If the user's biometric data is retained, then there is an inherent risk that the data could be leaked. Various schemes have been proposed for encrypting or somehow transforming the enrollment data to reduce the risk, but that does not alter the fact that the individual's biometric data enrolled in the system. Since biometric data cannot readily be changed, a user whose data had been leaked might be compelled to use a different finger for authentication or some other equally inconvenient tactic.

2.2 Correlation Matching

Here we present an overview of correlation matching, a fingerprint matching technique that does not require enrollment of biometric data. Fig. 2 shows a schematic overview of correlation matching. Correlation matching requires that a number of fingerprint data used for matching are prepared in advance. This

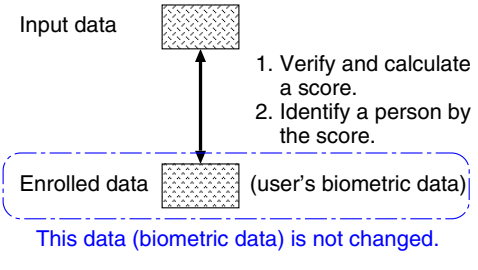

Fig. 1. Conventional matching method. The individual's own data is necessary for verification.

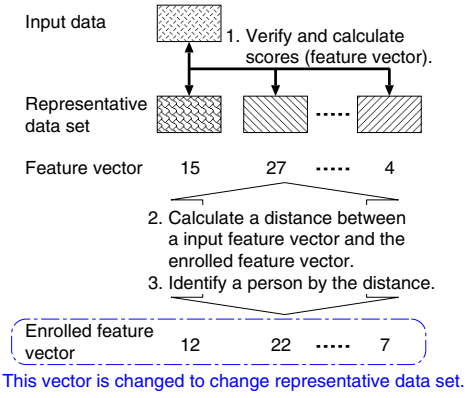

Fig. 2. Overview of correlation matching. Input data is verified with individual data items in the representative data set to derive a feature vector. The most simple matching method is to calculate the distance between the input feature vector and previous enrolled feature vector.

set of fingerprint data is called a set of representative data. Input data of a user is not verified with his enrolled biometric data, but rather is verified against his representative data items. The set of scores obtained by verifying the input data against his representative data items can be thought of as a feature vector. The distance is then calculated between this feature vector and other enrolled feature vectors derived previously by the same procedure, and the person is identified by the distance.

Here, it explains the calculation time. In this method, it is assumed to the verification of input data and representative data to use the conventional matching. If it takes n second for the verification in the conventional matching, it will take the $M \times n$ second in the correlation matching to calculate the feature vector. M is assumed to be a number of representative data. In addition, the time that hangs in the comparison between the input vector and the enrolled vector will add.

An advantage of correlation matching is that it does not require the enrollment of users' biometric data. Rather, the information that is enrolled in the system is feature vectors indicating the relationship with the representative data items. The risk of a leak thus comes to focus on the sets of representative data and feature vectors. Note however that the set of representative data readily changed by transposing the data items themselves or by changing the number of data items. The feature vectors are determined by the number and type of representative data. Though the searching method for the enrolled data by the steetest descent method in a face recognition system[5] is reported, it might be difficult to search for the number of elements and the element value at the same time.

Here, one example of the person authentication system that uses the correlation matching is shown in Fig.3. In this authentication system, user's fingerprint data is enrolled nowhere and doesn't flow in the network. This is an advantage of the correlation matching.

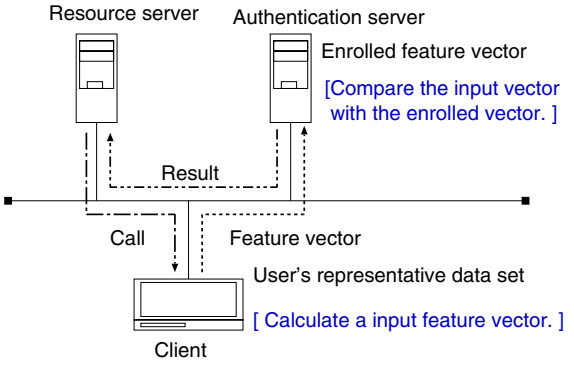

Fig. 3. Overview of the authentication system. A fingerprint data is taken on the client and a feature vector is calculated for the data. In the Authentication server, the input feature vector and the enrolled feature vector are compared.

3 Correlation Matching Scheme

Next let us consider the criterion for selecting the representative data items. Moreover, it thinks about the classifier when the fingerprint is matching.

3.1 Representative Data

We observed earlier that correlation matching requires that representative data be prepared in advance. Here we will consider the criterion by which this representative data should be prepared.

we assume here that representative data sets are set up for each enrollee. Consider that the set of representative data is selected for a fingerprint F_{i^*}. Here we assume that each representative data item incorporates fingerprint data enabling F_{i^*} to be distinguished from $\mathrm{F}_{j\neq i^*}$. Thus the group of scores x_{p,d_1} yielded by verifying fingerprint data $p \in \mathcal{D}$ with $d_1 \in \mathcal{D}_{i^*}$ is called class ω_1, and the group of scores x_{p,d_2} obtained by verifying with $d_2 \in \mathcal{D}_{j\neq i^*}$ is called class ω_2. Here $\mathcal{D}$ is a fingerprint data set, and $\mathcal{D}_i \subset \mathcal{D}$ is the fingerprint data set for fingerprint F_i.

The value of p is based on the within-class variance between-class variance ratio between these two classes ω_1 and ω_2. The within-class variance between-class variance ratio J_σ represents the extent or degree of separation between the classes. In other words, the bigger the J_σ score, the greater the distance between classes. Here x_{p,d_i} belonging to ω_i is $\mathcal{X}_i$, the $\mathcal{X}_i$ element number is n_i, and the average score is m_i. The total number of element is n and the total average score is m. Here the within-class variance is represented by σ_W^2, the between-class variance is represented by σ_B^2, and can be written

$$\sigma_W^2(p) = \frac{1}{2}\sum_{i=1}^{2}\sum_{x_{p,d_i}\in\mathcal{X}_i}(x_{p,d_i} - m_i)^2 \tag{1}$$

$$\sigma_B^2(p) = \frac{1}{2}\sum_{i=1}^{2} n_i(m_i - m)^2. \tag{2}$$

Therefore, based on Equations (1) and (2), the p score $J_\sigma(p)$ is given by

$$J_\sigma(p) = \frac{\sigma_B^2(p)}{\sigma_W^2(p)}. \tag{3}$$

Next, we consider how sets of representative data are constructed using representative data. First, a large number of fingerprint data samples are prepared to serves as candidates of representative data. The values of these candidates are derived based on the criterion described earlier. If a set of representative data consists of M number of representative data samples, then M number of samples are chosen from among these candidates, and arranged in the order to highest value first to make up the set of representative data.

3.2 Adopting Classifier

In this section we consider the procedure for identifying fingerprints. A set of representative data can be prepared by above method. The following problem is a classifier. In a word, the method of matching the fingerprint from the feature vector. The easiest method is to match the fingerprint from the distance of the input vector and the enrolled vector. Moreover, there is the one using the KL expansion and the linear discriminant method. The one using the neural net work is a superior method, too. In addition, there is a method of the combination of these classifier. For example, there is bagging[6] that studies the data set where distribution is different, and there is boosting[7] that increases the weight of the instance of the mis-classification and repeats study. Moreover, there are cascading[8] and stacking[9, 10] that controls the combination of the classification machine by study.

Here, the KL expansion and the linear discriminant method that is the standard way will be used. Moreover, the method of combining these two methods is applied. Therefore, the basic performance of the correlation matching is confirmed.

4 Computer Experiments

In this section, the basic performance of the correlation matching is confirmed.

4.1 Experimental Procedures

Four basic experiments are conducted in which the matching is done

(a) using feature space,
(b) using space whose dimensionality is reduced by KL expansion (KL),
(c) using discriminate space based on the linear discriminant method (LD), and
(d) using discriminate space based on a combination of KL and LD.

In the experiments we use a database of 30,000 fingerprints compiled by scanning 2,000 fingers 15 times each. Essentially, the 2,000 fingers are divided into three groups as follows: 500 fingers are used to calculate the performance (Group A), 500 different fingers are used to calculate the values of the candidates (Group B), and the remaining 1,000 fingers are used as candidates for the representative data (Group C).

The experiments are conducted in the following order:

(1) A set of representative data is defined for each finger in Group A. Using the first 10 data samples out of 15 and the data in Group B, values are derived for the candidate data in Group C. M number of candidates are selected forming his set of representative data in the order of highest values.
(2) Enrolled feature vectors are calculated for each finger in Group A. Ten feature vectors are derived from his set of representative data defined in (1) and from the first ten data samples. This average vector is regarded as his enrolled feature vector.
(3) When KL and LD are applied, conversion matrix and vector were calculated. These matrix and vector are derived using his feature vectors calculated in (2) and another-person feature vectors calculated from the Group B data and his set of representative data defined in (1).
(4) For each finger in Group A we obtain a genuine distribution calculated from the distance and frequency between the enrolled feature vectors calculated in (2) and the feature vectors derived from the remaining 5 data. Imposter distributions are then obtained calculating the distance and frequency of the feature vectors derived from the remaining 5 data of the other fingers. In other words, the distance calculations are performed between 2,500 pairs of the same finger, and between 1,247,000 pairs of different fingers, and the frequencies are derived from these calculations.

4.2 Experimental Results

In experiment (a), we change M from 100 to 1000. In experiment (b), the results are obtained when 1000-dimension feature space is converted to L reduced-dimension subspace by KL expansion. L is changed from 100 to 1000. In experiment (c), we show the results for discriminant space derived by the linear discriminant method for M-dimension feature space. The range of M is from 100 to 900. In the last experiment (d), we show the results when matching is done using discriminate space derived by applying the linear discriminant method to the L-dimension subspace. Here $L = 100$ to 900. The result of each experiment is

Table 1. The best FNMR when a threshold is set up in FMR = 1% and FMR = 0.1%

Experiment	(a)	(b)	(c)	(d)
FMR= 1%	12.2%	10.9%	3.2%	1.6%
FMR= 0.1%	33.7%	27.0%	7.7%	3.6%

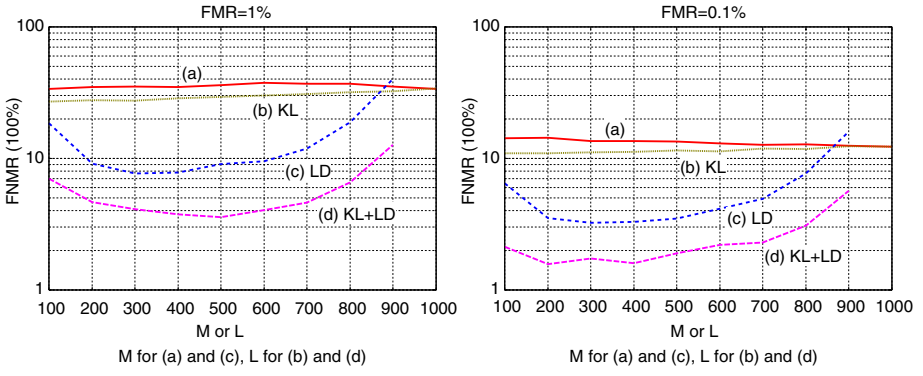

Fig. 4. FNMR in the each experiment is shown. The left figure is a result in FMR= 1%, and a right figure is a result in FMR= 0.1%.

shown in Fig. 4. And, the best result is shown in Table. 1. The best performance is FNMR= 3.6% at FMR= 0.1% when the combining classifier is applied.

5 Conclusions

In this paper, we showed the overview of the correlation matching and examined the basic performance. To realize better performance, we will improve the method to prepare representative data, construct them, and adopt more advanced classifiers in the future study.

References

1. Ratha N., Connell J., Bolle R., "Enhancing security and privacy in biometrics based authentication systems", IBM Systems Journal40, pp.61-634, 2001.
2. Soutar C., Roberge D., Stoianov A., Gilroy R., Kumar V., "Biometric Encryption", http://www.bioscrypt.com/assets/Biometric_Encryption.pdf
3. K. Sasakawa, F. Isogai, S. Ikebata, "Personal Verification System with High Tolerance of Poor Quality Fingerprints", in Proc. SPIE, vol. 1386, pp. 265-272, 1990.
4. M. Matsushita, T. Maeda, K. Sasakawa, "Personal verification using correlation of score sets calculated by standard biometrics data", Technical Paper of the Inst. of Electronics and Communication Engineers of Japan, PRMU2000-78, pp. 21-26, 2000.
5. Adler A., "Sample images can be independently restored from face recognition template", Can. Conf. Electrical Computer Eng., pp.1163-1166, 2003.
6. Breiman, L "Bagging Predictors", Machine Learning, 24(2), pp. 123-140, 1996.
7. Freund, Y. Schapire, R. E. "Experiments with a new boosting algorithm", in Proc. of Thirteenth International Conference on Machine Learning, pp. 138-156, 1996.
8. Gama, J. and Brazdil, P. "Cascade Generalization", Machine Learning, 41(3), Kluwer Academic Publishers, Button, pp. 315-343, 2000.
9. Wolpert, D. "Stacked Generalization", Neural Network 5(2), pp.241-260, 1992.
10. Dzeroski S., and Zenko B., "Is combining classifiers better than selecting the best one?", Machine Learning, 54, pp.255-273, 2004.