BIOMETRIC-BASED CRYPTOGRAPHIC KEY GENERATION

Yao-Jen Chang[*]*, Wende Zhang*[+]*, and Tsuhan Chen*[+]

[*]Advanced Technology Center, Computer & Communications Research Laboratories
Industrial Technology Research Institute, Chutung, Hsinchu, Taiwan 310, R.O.C.

[+]Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, USA

ABSTRACT

Instead of using PINs and passwords as cryptographic keys that are either easy to forget or vulnerable to dictionary attacks, easy-to-carry and difficult-to-transfer keys can be generated based on user-specific biometric information. In this paper, a framework is proposed to generate stable cryptographic keys from biometric data that is unstable in nature. The proposed framework differs from prior work in that user-dependent transforms are utilized to generate more compact and distinguishable features. Thereby, a longer and stable bitstream can be generated as the cryptographic key. Experiments are performed on one face database to verify the feasibility of the proposed framework. The preliminary result is very encouraging.

1. INTRODUCTION

Cryptographic keys are widely used in access control to computing resources, bank accounts in ATM systems, and user validation in e-business. Conventionally, system random-selected or user-determined PINs and passwords are utilized to generate unique keys for access control. However, system random-selected keys are easy to forget and user-determined keys are subject to dictionary attacks and also easy to transfer. Biometrics, such as face, voice, iris, and fingerprint, contribute specific characteristics of each individual. Therefore, biometric data potentially can be taken as good alternatives, or supplements, to PINs and passwords.

Numerous researches have been conducted in biometric-based authentication. However, fundamental differences exist between biometric-based authentication and biometric-based cryptographic key generation targeted in this work. The former relies on good classifiers or user-specific templates to distinguish authentic user to potential imposters, while the latter transforms biometric features to a unique key that cannot be regenerated from biometric features of potential imposters. The goal of biometric-based key generation can also be achieved by biometric-based authentication followed by key selection. However, one assumption is made that attackers cannot access any resources related to user-dependent models or templates used by classifiers, which may not be true under all circumstances, especially where the authentication device is not immune to capture or full examination by adversaries. Hence, it is preferred if biometric data can be directly transformed to cryptographic keys and no user-specific models or templates that can be analyzed by reverse engineering techniques are stored on the device.

Based on the above criteria, Monrose *et al.* [1] proposed voice-based cryptographic key generation. In which each biometric feature is conceptually contributed to one bit of the cryptographic key. Similarly, Jermyn *et al.* [2] proposed to use hand-drawn sketch to generate passwords according to the position and timing of the sketch drawing. Soutar *et al.* [3] proposed the Biometric Encrytion™ method based on a specific correlation filter design for image-based biometric feature.

Inspired by conventional biometric-based authentication schemes based on classification, two research directions are conducted in this work. One is to generate more distinguishable features by cascading two-class classifiers. And the other is to extend the feature binarization to be multiple discrete values such that conceptually each feature may contribute multiple bits. In the next section, an overview the proposed framework is introduced. Distinguishable feature generation and stable key generation are detailed in Sections 3 and 4. Some experimental results based on the biometric data generated from face images are presented in Section 5. Finally, Section 6 concludes the paper and states some possible future directions.

2. THE FRAMEWORK

The conceptual diagram of the proposed framework is depicted in Figure 1. Firstly, with a collection of biometric features of authentic user and other users as training data, a user-dependent feature transform is derived such that transformed features of the authentic user are compact in

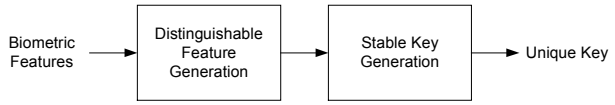


Figure 1. The conceptual diagram of the proposed framework.

the transformed feature space while those of other users presumed as imposters are either diverse or far away from those of the authentic user. Thus, the transformed features of the authentic user are distinguishable from those of imposters. Secondly, a stable key generation mechanism is utilized to generate a stable cryptographic key. According to the degree of distinguishability, each transformed feature may contribute one or more bits of information to the cryptographic key generation. Thereby, not only a stable key can be generated, the key space is also enlarged to hinder imposters from exhaustive search for the correct key from the key space.

3. DISTINGUISHABLE FEATURE GENERATION

The goal of distinguishable feature generation is to find a transformation such that each transformed feature is distinguishable to separate the authentic user from potential imposter users. As stated in the previous section, either the separation of the transformed features between authentic user and imposters or the compactness of the transformed features of authentic user and the diversity of those of the imposters can contribute distinguishability between the authentic user and imposters. Therefore, different criteria can be derived to find optimal transforms given a collection of biometric features as the training data. Some possible criteria explored in this work are addressed in the following subsections.

3.1. Cascaded Linear Discriminant Analysis

Linear discriminant analysis (LDA) [4] has long been used to form discriminative low dimensional features from a high dimensional feature space based on Fisher's discriminant criterion which maximizes the ratio of the determinant of the between-class scatter matrix of the transformed features to the determinant of the within-class scatter matrix of the transformed features. For two-class classification that separates features of the authentic user and all other imposters, the optimal projection vector can be derived as

$$\boldsymbol{w} = \mathbf{S}_w^{-1}\left(\boldsymbol{m}_a - \boldsymbol{m}_t\right) \Big/ \left\| \mathbf{S}_w^{-1}\left(\boldsymbol{m}_a - \boldsymbol{m}_t\right) \right\|, \qquad (1)$$

where $\mathbf{S}_w = 0.5(\mathbf{S}_a + \mathbf{S}_t)$, in which $\mathbf{S}_a$ and $\mathbf{S}_t$ are covariance matrices of features of the authentic user and imposters, respectively. And $\boldsymbol{m}_a$ and $\boldsymbol{m}_t$ are the mean of features of the authentic user and imposters. With Eq. (1), only one optimal projection vector can be found which projects high-dimensional features to one-dimensional feature space. To derive more discriminative projection vectors, the original features are projected to the null-space of the one-dimensional feature space defined by the optimal project vector, and then use Eq. (1) to find the optimal projection vector within the null-space.

By repeating the procedures m times, m projection vectors can be derived to create an m-dimensional discriminative feature space from the original high-dimensional feature space. Each dimension of the transformed features occupies a compact region and the distance between the mean of authentic samples and the mean of imposter samples is maximized, which satisfies the requirements of distinguishability.

3.2. Generalized Symmetric Max Minimal Distance in Subspace (GSMMS) Criterion

When the authentic samples are surrounded by imposter samples in the high-dimensional feature space, it is difficult to find one linear plane to separate authentic samples and imposter samples. Instead of seeking non-linear planes, Zhang and Chen [5] proposed to use two linear planes to resolve the problem. The optimal projection vector is derived iteratively such that the minimal distance of the transformed features between the authentic user and imposters is maximized. That is,

$$\boldsymbol{w}^* = \arg\max_{\boldsymbol{w}} \left\{ \min_{i,j} \left| \boldsymbol{w}^T \boldsymbol{f}_{t,i} - \boldsymbol{w}^T \boldsymbol{f}_{a,j} \right| \right\}, \qquad (2)$$

where $\boldsymbol{f}_{t,i}$ and $\boldsymbol{f}_{a,j}$ are the i-th imposter sample and the j-th authentic sample, respetively. To simplify the optimization, the transformed authentic feature is assumed to be Gaussian or uniformly distributed surrounded the mean of the projected value authentic samples. Hence, the optimal projection vector can be expressed by:

$$\boldsymbol{w}^* = \arg\max_{\boldsymbol{w}} \left\{ \min_{i} \left| \boldsymbol{w}^T \boldsymbol{f}_{t,i} - b \right| - \max_{j} \left| \boldsymbol{w}^T \boldsymbol{f}_{a,j} - b \right| \right\}, \qquad (3)$$

where $b = \text{mean}(\boldsymbol{w}^T \boldsymbol{f}_{a,i})$, the mean of the projected value of authentic samples. However, Eq. (3) is still a non-linear optimization problem. An approximation that converts the max-min problem to weighted mean optimization is utilized to find the optimal projection vector iteratively [5].

To derive multiple projection vectors, either the null-space approach as stated in previous subsections can be applied or a set of m optimal orthogonal vectors can be directly estimated by maximizing the minimal distance of the projected features between the authentic user and imposters in a m-dimensional subspace.

4. STABLE KEY GENERATION

To generate stable cryptographic keys from biometric features, Monrose *et al.* [1] proposed to firstly verify the distinguishability of each feature. For a feature, if the distance between the authentic mean from the global mean

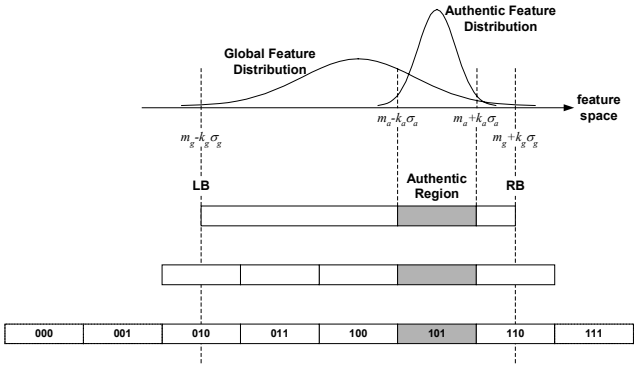


Figure 2. An example of the key generation for one feature.

is larger than k_a times of the authentic standard deviation, this feature is considered to be distinguishable and is binarized to be 0 or 1. Otherwise, the feature is implicitly discarded based on the Shamir's secret sharing scheme [6].

Since the distinguishable feature generation stated in the previous section can generate features with compact and distinguishable distribution, more bits of information can be provided to contribute the cryptographic key rather than just 1-bit for each feature as in [1]. Given an *m*-dimensional feature space, the multi-bit key generation scheme is proposed as follows:

(1) Let the left and right boundaries for each feature be

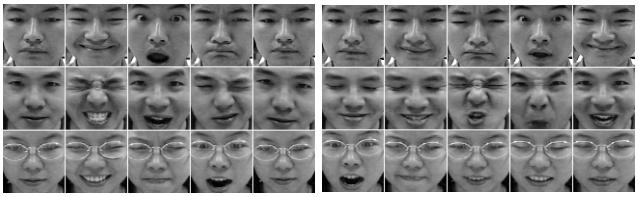
$$LB = \min\left(m_g - k_g\sigma_g, m_a - k_a\sigma_a\right),$$

$$RB = \max\left(m_g + k_g\sigma_g, m_a + k_a\sigma_a\right),$$

where m_a and σ_a are the mean and standard deviation of the authentic feature distribution, and m_g and σ_g are those of global feature distribution. The value of k_g is set to be 5 to cover almost 100% of the global distribution, and k_a is utilized to control the range $\left(m_a - k_a\sigma_a, m_a + k_a\sigma_a\right)$ to be specified as the authentic region.

(2) From *LB* to the left boundary of the authentic region, there are $LS = \left\lceil \left(m_a - k_a\sigma_a - LB\right) / 2k_a\sigma_a \right\rceil$ segments of the same size as the authentic region. Similarly, there are $RS = \left\lceil \left(RB - m_a - k_a\sigma_a\right) / 2k_a\sigma_a \right\rceil$ segments from the right boundary of the authentic region to *RB*. Therefore, there are (*LS*+*RS*+1) segments to cover the range (*LB*, *RB*). At least $\left\lceil \log_2\left(LS + RS + 1\right) \right\rceil$ bits are sufficient to specify each segment with a unique index. An example is illustrated in Figure 2. The top row depicts the approximated authentic and global feature distribution. The second row shows the positions of *LB*, *RB*, and the authentic region. The third row shows three segments with the same size of the authentic region to cover *LB* and one segment to cover *RB*, i.e., *LS*=3 and *RS*=1. Three redundant segments are randomly added to the left or the right side since three bits are required to specify the index of each segment as shown in the last row. Therefore, the index for the authentic region for this feature is 101 in this case.

With the above procedure, the cryptographic key with length $\sum_{i=1}^{m} \left\lceil \log_2\left(LS_i + RS_i + 1\right) \right\rceil$ can be generated by cascading all indices of authentic regions from the *m*-dimensional feature space.



(a) (b)

Figure 3. Sample images of (a) the training set, and (b) the testing set of the face database for performance evaluation.

5. EXPERIMENTAL RESULTS

Experiments are conducted to verify the performance of the proposed framework. One database containing face images of 30 persons with facial expression and slight head motion variations is utilized for evaluation. In this database, each person has 25 images as training data and 112 images for testing. Sample images are shown in Figure 3. Two approaches explored in Section 3 are used, and the performance comparison between our proposed multi-bit scheme and the original 1-bit scheme is also presented.

5.1. Preprocessing

For each face image in the database, the locations of eyes are manually marked such that each face region is normalized to 64×64 pixels. Principal component analysis is performed on all training set images to reduce the feature dimension to 100 dimensions, which are taken as the biometric features in Figure 1.

5.2. Performance Evaluation

In conventional biometric-based user authentication, the performance is evaluated with the false-acceptation-rate (*FAR*) and false-rejection-rate (*FRR*). For cryptographic key generation, the key space is also an important factor to measure the security of the cryptographic key especially when adversaries can perform exhaustive search for the key with powerful computing resources. Thus, the performance is evaluated by the objective function:

$$f_p = c_1 \cdot FAR + c_2 \cdot FRR - c_3 \cdot (\#\ \text{effective bits}), \quad (4)$$

where the (# effective bits) is calculated from the average base-2 logarithm of the reciprocal of the probability that

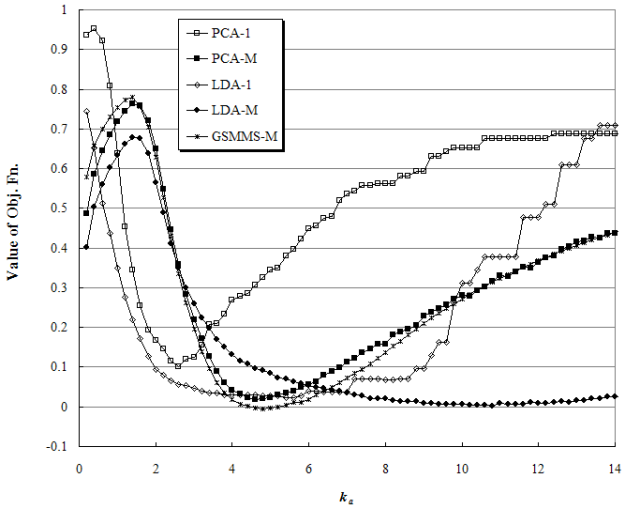


Figure 4. The values of objective function under different criteria with respect to the internal parameter k_a.

Table 1. Best operating point for each method

Method	*FAR*	*FRR*	# Effective Bits
PCA-1	0.046	0.059	5.07
LDA-1	0.001	0.026	3.60
PCA-M	0.010	0.077	67.64
LDA-M	0.004	0.052	51.25
GSMMS-M	0.008	0.074	88.03

an adversary with the knowledge (*LB*, *RB*) of each feature space can correctly guess the positions of the authentic regions from *m* features. Therefore, it will be less than or equal to the actual key length since some redundant segments may be added to the left of *LB* or the right of *RB* as shown in the Figure 2. In the 1-bit scheme [1], the effective bits equal to the number of distinguishable features. Various configurations of c_i's can be used according to the target application. For example, in applications such as e-commerce require extremely low *FAR*, a large c_1 would be chosen. On the contrary, in applications that use the proposed scheme only as supplements to PINs or passwords, a large c_2 is utilized to lower *FRR* to avoid the inconvenience to legitimate users. In our experiments, c_1 and c_2 are both set to be 1, and c_3 is set to be 0.001. Figure 3 shows the performance for different feature generation methods under different stable key generation schemes, where LDA-1 stands for the combination with the cascaded LDA criterion for distinguishable feature generation with the 1-bit scheme for stable key generation while the LDA-M stands for using cascaded LDA with the multi-bit scheme. PCA-1 scheme is taken as the baseline scheme in which no user-dependent transform is performed and stable key generation is based on 1-bit scheme. The parameter k_a in the multi-bit scheme controls the range of the authentic region, while in the 1-bit scheme, it determines how far away the distance is between the authentic mean and global mean, a feature will be considered to be distinguishable. As a result, increasing k_a for both schemes will increase *FAR* and reduce *FRR* and the number of effective bits. The best operation point for each method as listed in Table 1. It can be observed that the user-dependent transform based on cascaded LDA and GSMMS can improve *FAR* and *FRR* since the transformed features are more distinguishable. In addition, the proposed multi-bit approach can create more effective bits than the 1-bit scheme, i.e., with the multi-bit approach, the key space is enlarged.

6. CONCLUSIONS AND FUTURE WORK

In this paper, a framework for biometric-based cryptographic key generation is proposed. Contributions include a general approach for distinguishable feature generation and a stable key generation mechanism. Possible future directions include applying to other person-dependent biometric features (e.g. voices, audio-visual dynamics, iris pattern, etc.) and finding a good approach to set up the authentic range for each feature to achieve the optimal overall performance.

7. ACKNOWLEDGEMENT

This work is a partial result of Project B32BCM1100 conducted by ITRI under sponsorship of the Ministry of Economic Affairs, R.O.C. The authors would also like to thank Michael Reiter, Carnegie Mellon Univ., for discussions of stable key generation.

8. REFERENCES

[1] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice," *Proceedings of the 2001 IEEE Symposium on Security and Privacy*, pp. 202-213, May 2001.

[2] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, A. Rubin, "The Design and Analysis of Graphical Passwords," 8th USENIX Security Symposium, Washington, D.C., August 1999.

[3] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy and B.V.K. Vijaya Kumar, "Biometric Encryption™," *Chapter 22 in ICSA Guide to Cryptography*, edited by Randall K. Nicholls, pp. 649-675, 1999.

[4] R. O. Duda, P. E. Hart, and D. G. Stork, Pattern Classification, Second edition. John Wiley & Sons Inc., New York, 2001.

[5] W. Zhang and T. Chen, "Personal authentication based on generalized symmetric max minimal distance in subspace," *Proceedings of IEEE Conference on Multimedia and Expo*, Baltimore, MD, July 2003.

[6] A. Shamir, "How to share a secret," *Communications of the ACM*, Vol. 22, No. 11, pp. 612-613, November 1979.