# GENERALIZED OPTIMAL THRESHOLDING FOR BIOMETRIC KEY GENERATION USING FACE IMAGES

*Wende Zhang and Tsuhan Chen*

Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, USA
{wendez, tsuhan}@andrew.cmu.edu

## ABSTRACT[1]

In this paper, we study biometric key generation using face images. Given a face image, a set of biometric features are extracted. Each feature is compared with a threshold to generate a key-bit. By cascading the key-bits from all the features, we obtain one bio-key that can be used for security applications. The performance of a biometric key generation system, determined by the chosen thresholds, can be evaluated according to reliability and security. A generalized optimal thresholding method is proposed in this paper to improve the reliability by minimizing the authentication error rate and the security by maximizing the entropy of the generated key.

## 1. INTRODUCTION

Security applications often need certain private information to authenticate the user's privilege. Digital keys are widely used to serve such a purpose. For example, we use a PIN number as the key to access ATM accounts; we use a password as the key to login to a computer system; we also use keys for data encryption or decryption.

Given certain input from the user, a traditional key generator often generates a long key [1][2] to achieve a high key entropy. Such strategy can defer a hacker's attack as the hacker has to search the entire key space exhaustively. However, a long key is easily forgotten and not user-friendly. Hence it usually results in a high false reject rate (FRR).

Instead of asking users to memorize long keys, some recent key generation systems [3]-[9] try to generate keys based on the users' biometric information.

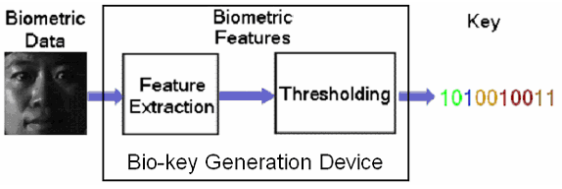



**Figure 1.** Biometric key generation

A flowchart of a general bio-key generation device is shown in Figure 1. First, the biometric features are extracted from the biometric data based on the feature extraction module. Then, the biometric features are thresholded into a bio-key by the thresholding module. A bio-key generation system can be either *user-independent* [3][4][5] or *user-dependent* [6][7][8].

A user-independent bio-key generation system creates a single device, which can be used to generate keys for all subjects. This is similar to the traditional key generation systems.

Monrose *et al.* [3][4][5] proposed a secret sharing method to generate the bio-key. First, the distinguishing biometric features [3] are selected based on the separation between the authentic and imposter data, and then binarized by some thresholds. The key is released under the secret sharing scheme by matching all the bits of the input biometrics with the authentic bits, which are computed from the distinguishing features.

A user-dependent bio-key generation system, however, contains multiple devices, one for each subject. A subject can only gain access using the device created specifically for the same subject, and will be denied if he/she wants to access a device belonging to another subject.

Soutar *et al.* [6] proposed a biometric encryption method. In this method, the input biometric image is correlated with a pre-designed user-dependent filter to create the correlation output. The key is then generated based on this binarized output pattern.

Based on Monrose *et al.*'s [4] bio-key generation approach, Chang *et al.* [7] extended the distinguishing feature selection to user-dependent feature transformation in order to generate more distinguishing features using the cascaded two-class classification scheme. They also extended the binary values of each feature to multiple values so that each feature may contribute multiple bits rather than one bit to improve the security of the bio-key generation system.

However, both Monrose *et al.* [4] and Chang *et al.* [7] did not address the issue of setting the thresholds for the features. Zhang *et al.* [8] proposed a method to minimize the authentication error rate in terms of the false accept rate (*FAR*) and the false reject rate (*FRR*) of the bio-key generation system by setting the optimal thresholds for each extracted feature.

Zhang *et al.* [10] presented a comprehensive analysis on the security of general bio-key generation systems. They classified the hacker's attacks into three categories, and showed how robust a bio-key generation system is under these attacks.

[1] Work supported in part by Industrial Technology Research Institute, Taiwan.

A biometric key generation system should be evaluated on both authentication performance and security. However, in [8], the thresholds are chosen to optimize only authentication performance regardless of security of the bio-key generation system. In this paper, we propose a generalized optimal thresholding method to optimize both authentication performance and security of the bio-key generation system.

This paper is organized as follows: In Section 2, we detail the generalized optimal thresholding method for the bio-key generation system. In Section 3, we describe the biometric face image database used in the experiment and present the performance of the proposed bio-key generation system. Our conclusions are given in Section 4.

## 2. GENERALIZED OPTIMAL THRESHOLDING

A bio-key generation system is evaluated based on authentication error rate in terms of *FAR* and *FRR* and on security in terms of guessing entropy [11][12] of the generated key. *FAR* is defined as the rate that imposter users generate the same bit-sequence as the claimed users. *FRR* is defined as the rate that an authentic user generates a bit-sequence other than the correct key. Guessing entropy is the expected number of guesses a hacker needs to make to get the authentic key.

In this paper, we want to find the optimal threshold for each feature to minimize *FAR* and *FRR* and maximize the guessing entropy.

Assuming that a random vector $\mathbf{k}$ has $m$ states and that the probability distribution of $\mathbf{k}$, say $\mathbf{p_k} = [p_1, p_2, ..., p_m]$, satisfies $p_1 \geq p_2 \geq ... \geq p_m$, the guessing entropy $G(\mathbf{k})$ is defined as:

$$G(\mathbf{k}) = \sum_{i=1}^{m} i p_i$$

Guessing entropy $G(\mathbf{k})$ is lower-bounded by the Shannon entropy $H(\mathbf{k})$ [11] as follows:

$$G(\mathbf{k}) \geq \frac{1}{4} 2^{H(\mathbf{k})} + 1$$

Since it is not easy to maximize the guessing entropy directly, we maximize its lower bound in the optimization. That is, we maximize the Shannon entropy.

Therefore, we propose a generalized method to determine the optimal threshold for each feature, thereby minimizing *FAR* and *FRR* as well as maximizing the Shannon entropy of the generated key with trade-off parameters $\alpha$ and $\beta$:

$$\max_{thresholds} [\log(1 - FRR) - \alpha \log(FAR) + \beta H(\mathbf{k})] \quad (1)$$

where $FAR = \int_{R_A} p(\mathbf{x} \mid w_I) d\mathbf{x}$, $FRR = \int_{R_I} p(\mathbf{x} \mid w_A) d\mathbf{x}$, and $p(\mathbf{x} \mid c)$ is the probability density function of the feature vector $\mathbf{x} = [x_1, x_2, ..., x_n]$, given the authentic class $c = w_A$ or the imposter class $c = w_I$. The number of the features is $n$. $R_A$ is the classification decision region for the authentic $w_A$, and $R_I$ is the classification decision region for the imposter $w_I$.

The authentic decision region $R_A$ is defined by the threshold for each feature $x_i$ in the feature vector $\mathbf{x}$. The decision region $R_A$ can be rewritten as in Equation (2), since it is separated from the imposter decision region $R_I$ by thresholding each feature individually.

$$R_A = \{x_1 \in R_1 \wedge x_2 \in R_2 \ ... \wedge x_n \in R_n\} \quad (2)$$

In order to generate one-bit from each feature as shown in Figure 2, we assume that the authentic decision region $R_i$ of feature $x_i$ is on one side of the threshold $T_i$. The threshold $T_i$ separates the authentic decision region $R_i$ from the imposter decision region of feature $x_i$. We can easily extend this one key-bit generation with a single threshold to multiple key-bits generation with multiple thresholds for each feature using the approach proposed in [8].

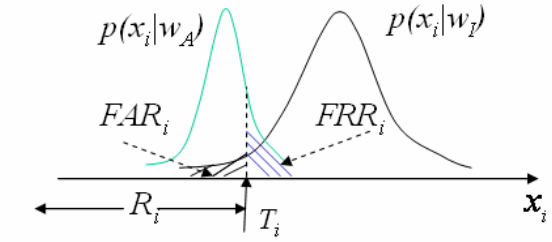



**Figure 2.** The $i^{th}$ feature for one-bit generation

*Assumption 1*: assuming all the features are conditionally independent given the class labels, we have

$$p(\mathbf{x} \mid w_A) = p(x_1 \mid w_A) p(x_2 \mid w_A) ... p(x_n \mid w_A)$$
$$p(\mathbf{x} \mid w_I) = p(x_1 \mid w_I) p(x_2 \mid w_I) ... p(x_n \mid w_I)$$

Therefore, the overall *FAR* and *FRR* can be derived as the functions of the individual $FAR_i$ and $FRR_i$ as follow:

$$\begin{aligned} FAR &= \int_{R_A} p(\mathbf{x} \mid w_I) d\mathbf{x} \\ &= \int_{R_1} p(x_1 \mid w_I) dx_1 \int_{R_2} p(x_2 \mid w_I) dx_2 ... \int_{R_n} p(x_n \mid w_I) dx_n \\ &= FAR_1 \cdot FAR_2 \cdots FAR_n \end{aligned} \quad (3)$$

$$\begin{aligned} 1 - FRR &= \int_{R_A} p(\mathbf{x} \mid w_A) d\mathbf{x} \\ &= \int_{R_1} p(x_1 \mid w_A) dx_1 \int_{R_2} p(x_2 \mid w_A) dx_2 ... \int_{R_n} p(x_n \mid w_A) dx_n \\ &= (1 - FRR_1) \cdot (1 - FRR_2) \cdots (1 - FRR_n) \end{aligned} \quad (4)$$

*Assumption 2*: assuming all the key-bits $k_i$ from each feature are generated independent, the key entropy of the key-bit sequence $\mathbf{k} = [k_1, k_2, ..., k_n]$ can be derived as follows:

$$H(\mathbf{k}) = H(k_1, k_2, ..., k_n) = H(k_1) + H(k_2) + ... + H(k_n)$$
$$H(k_i) = -\sum_j p_j(k_i) \log p_j(k_i)$$

where $p_j(k_i)$ is the probability of the $j^{th}$ key bit among all the subjects on feature $x_i$. Since $p_j(k_i)$ is a function of the threshold $T_i$ of feature $x_i$, $H(k_i)$, and hence $H(\mathbf{k})$, is also a function of $T_i$.

Instead of maximizing (1) using an exhaustive search over all the features, we search for the threshold on each feature individually as follows:

$$\begin{aligned} &\max_{T_1, T_2, ..., T_n} [\log(1 - FRR) - \alpha \log(FAR) + \beta H(\mathbf{k})] \\ &= \max_{T_1, T_2, ..., T_n} \sum_{i=1}^{n} [\log(1 - FRR_i) - \alpha \log(FAR_i) + \beta H(k_i)] \\ &= \sum_{i=1}^{n} \max_{T_i} [\log(1 - FRR_i) - \alpha \log(FAR_i) + \beta H(k_i)] \end{aligned} \quad (5)$$

Note that based on the two assumptions, by maximizing $\log(1-FRR_i)-\alpha\log(FAR_i)+\beta H(k_i)$ with the same tradeoff parameters $\alpha,\beta$ on each feature individually, we can find the optimal point ( $\log(FAR_i)$ , $\log(1-FRR_i)$ , $H(k_i)$ )for each feature, which results in optimal value for (1). By tuning different $\alpha,\beta$ 's, we can find the solution for any optimal point with different tradeoffs among *FAR*, *FRR* and $H(\mathbf{k})$.

## 3. EXPERIMENTAL RESULTS

We conduct experiments to evaluate the biometric key generation systems on the AMP face database as shown in Figure 3. As the face images of each subject contain a significant amount of expression variation and registration errors, this is a relatively challenging database. We take 20 subjects in this database for performance evaluation. Each subject has 137 face images of size 64×64. In order to compare with the system proposed in [10], we use 25 images of each user to train the feature extraction module. Principal Component Analysis (PCA) [13] is performed on all the training images to form a 100-dimensional user-independent global PCA subspace to reduce the features' dimensionality. The first $n$ ($n$ = 5, 17 in our experiments) distinguishing features [3] of each user are taken as the output of the feature extraction module. We use another 25 images of each user to determine one user-dependent threshold for each feature to generate a user-dependent biometric key generation device using the proposed method. While Shannon entropy $H(\mathbf{k})$ is optimized in the design stage, we evaluate the security of the biometric key generation system using the guessing entropy $G(\mathbf{k})$ in the test stage. The remaining 87 images of each user are used as test images to evaluate the average *FAR*, *FRR* and the average expected number of guesses, $G(\mathbf{k})$, of these 20 user-dependent biometric key generators.

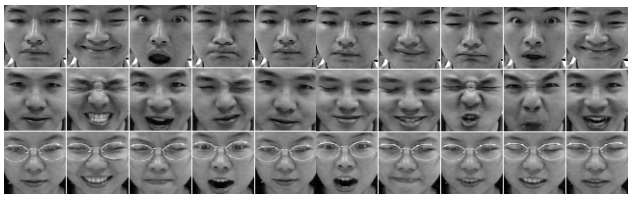


**Figure 3.** Sample images of the AMP face database

We evaluate the authentication performance (*FAR, FRR*) and security of the biometric key generation system $G(\mathbf{k})$ for different emphases ($\beta$) on $H(\mathbf{k})$ with a fixed $\alpha$ on *FAR* in (1) for feature number $n$ = 5 and feature number $n$ = 17. The resulting average *FAR*, *FRR*, $H(\mathbf{k})$ and $G(\mathbf{k})$ are listed in Table 1-Table 5. We show that although $H(\mathbf{k})$ and $G(\mathbf{k})$ are small in the tables due to the small number of users in the database, we can reach the upper bound [10] of $G(\mathbf{k})$=10.5 for this 20-user system as shown in Table 5. In a real system, $G(\mathbf{k})$ can be large with a large number of users in the system.

In all experiments, both the Shannon entropy $H(\mathbf{k})$ and the guessing entropy $G(\mathbf{k})$ increase, as $\beta$ increases. *FAR* decreases and *FRR* increases, as α increases. Therefore, our optimization method can adjust the thresholds to find the best operation point that strikes the balance among the authentication error rate *FAR*, *FRR* and the guessing entropy $G(\mathbf{k})$.

When $\beta$ = 0, the proposed method degenerates to the optimal thresholding method proposed in [8], which optimizes the authentication performance only. The resulting entropy in such a case is relatively small.

**Table 1.** Authentication performance and security of the system for feature number $n$ = 5, and $\alpha$ = 0.035

| $\beta$ | *FAR* | *FRR* | $H(\mathbf{k})$ | $G(\mathbf{k})$ |
|---|---|---|---|---|
| 0 | 2.0% | 0.46% | 3.21 | 4.23 |
| 0.015 | 1.9% | 0.46% | 3.32 | 4.52 |
| 0.031 | 1.6% | 0.46% | 3.39 | 4.71 |
| 0.049 | 1.9% | 0.46% | 3.66 | 5.80 |
| 0.070 | 1.7% | 0.46% | 3.69 | 5.95 |
| 0.095 | 1.6% | 0.52% | 3.78 | 6.70 |
| 0.131 | 1.6% | 0.75% | 3.82 | 6.79 |
| 0.187 | 1.7% | 0.75% | 3.99 | 7.53 |

**Table 2.** Authentication performance and security of the system for feature number $n$ = 5, and $\alpha$ = 0.087

| $\beta$ | *FAR* | *FRR* | $H(\mathbf{k})$ | $G(\mathbf{k})$ |
|---|---|---|---|---|
| 0 | 1.10% | 6.67% | 3.14 | 4.00 |
| 0.015 | 0.92% | 6.67% | 3.15 | 4.07 |
| 0.031 | 0.80% | 6.72% | 3.15 | 4.08 |
| 0.049 | 0.84% | 6.55% | 3.18 | 4.19 |
| 0.070 | 0.67% | 6.55% | 3.32 | 4.53 |
| 0.095 | 0.51% | 6.61% | 3.31 | 4.54 |
| 0.131 | 0.52% | 6.32% | 3.50 | 4.98 |
| 0.187 | 0.60% | 6.26% | 3.56 | 5.27 |

**Table 3.** Authentication performance and security of the system for feature number $n$ = 17, and $\alpha$ = 0.035

| $\beta$ | *FAR* | *FRR* | $H(\mathbf{k})$ | $G(\mathbf{k})$ |
|---|---|---|---|---|
| 0 | 1.04% | 1.3% | 4.19 | 8.27 |
| 0.015 | 0.81% | 1.9% | 4.27 | 9.36 |
| 0.031 | 0.57% | 2.5% | 4.28 | 9.44 |
| 0.049 | 0.53% | 3.6% | 4.29 | 9.78 |
| 0.070 | 0.25% | 5.6% | 4.30 | 9.90 |
| 0.095 | 0.13% | 6.7% | 4.32 | 10.45 |
| 0.131 | 0.06% | 9.3% | 4.32 | 10.45 |
| 0.187 | 0.02% | 13.8% | 4.32 | 10.45 |

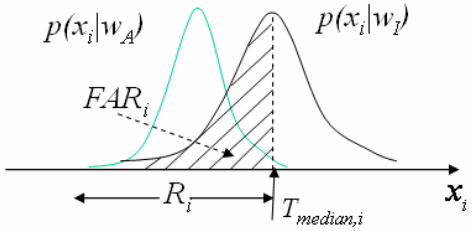
**Table 4.** Authentication performance and security of the system for feature number $n$ = 17, and $\alpha$ = 0.087

| $\beta$ | *FAR* | *FRR* | $H(\mathbf{k})$ | $G(\mathbf{k})$ |
|---|---|---|---|---|
| 0 | 0.0% | 22.9% | 4.25 | 8.94 |
| 0.015 | 0.0% | 22.9% | 4.25 | 8.94 |
| 0.031 | 0.0% | 23.8% | 4.29 | 9.68 |
| 0.049 | 0.0% | 24.4% | 4.31 | 9.84 |
| 0.070 | 0.0% | 25.3% | 4.32 | 10.30 |
| 0.095 | 0.0% | 26.8% | 4.32 | 10.45 |
| 0.131 | 0.0% | 28.6% | 4.32 | 10.45 |
| 0.187 | 0.0% | 31.0% | 4.32 | 10.50 |

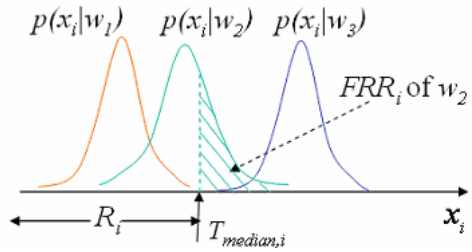
**Table 5.** Authentication performance and security of the system for $\beta = \infty$

| Feature Number | *FAR* | *FRR* | $H(\mathbf{k})$ | $G(\mathbf{k})$ |
|---|---|---|---|---|
| 5 | 1.9% | 12.9% | 4.02 | 7.33 |
| 17 | 0.0% | 69.3% | 4.32 | 10.50 |

When $\beta = \infty$, it is effectively ignoring the authentication performance (*FAR*, *FRR*) in the optimization. The thresholds are optimized for the Shannon entropy $H(\mathbf{k})$ only. The resulting threshold for each feature is the median point $T_{median,i}$ of all the subjects of that feature to achieve maximal $H(k_i)$. Note that in this case, the thresholds, and hence the whole system, become user-independent.




(a) Authentic and imposter data distribution




(b) Each subject's data distribution

**Figure 4.** Maximal Shannon entropy on the $i^{th}$ feature

Since the number of subjects in the database is large, the median point $T_{median,i}$ of all the subjects is close to the median point of the imposter subjects for $x_i$. Therefore, with the threshold $T_{median,i}$, it results in $FAR_i \approx 0.5$ for all the subjects as shown in Figure 4(a). Based on Equation (3), we can roughly estimate $FAR \approx (0.5)^n$, which is consistent with the experimental results in Table 5.

There is very likely to be at least one subject's data points distributed around the threshold $T_{median,i}$ of $x_i$ since the number of subjects in the database is large. Then, the $FRR_i$ of that subject ($w_2$) turns out to be bad because the imposter region covers a substantial portion of authentic data as shown in Figure 4(b). Based on Equation (4), we can prove that $FRR \geq FRR_i$. Therefore, the average *FRR* of all the subjects in Table 5 is large.

## 4. CONCLUSIONS

In this paper, we propose a bio-key generation system using face images with a generalized optimal thresholding approach to reach the balance between the authentication error rate and security. The experimental results show that the proposed generalized optimal thresholding approach optimizes both the authentication performance and the guessing entropy of the generated key.

## REFERENCES


[1] S. Burnett and S. Paine, *RSA Security's Official Guide to Cryptography*, RSA Press, McGraw-Hill/Osborne Media, 2001.

[2] A. Menezes, P. Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[3] F. Monrose, M.K. Reiter, and S.G. Wetzel, "Password hardening based on keystroke dynamics," *International Journal on Information Security* 1(2), February 2002. pp. 69–83.

[4] 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*, 2001, pp. 202-213.

[5] F. Monrose, M.K. Reiter, Q. Li and S. Wetzel, "Using voice to generate cryptographic keys," *Proceedings of 2001: A Speaker Odyssey, The Speaker Recognition Workshop*, June 2001, pp. 237–242.

[6] 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 R.K. Nicholls, 1999, pp.649-675.

[7] Y. Chang, W. Zhang and T. Chen, "Biometric-based cryptographic key generation," *IEEE Conference on Multimedia and Expo,* 2004.

[8] W. Zhang, Y. Chang and T. Chen, "Optimal thresolding for key generation based on biometrics," *IEEE Conference on Image Processing,* 2004.

[9] J. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15(11), 1993, pp. 1148-1161.

[10] W. Zhang, C. Zhang and T. Chen, "Security analysis for key generation systems using face images," *IEEE Conference on Image Processing,* 2004.

[11] J.L. Massey, "Guessing and entropy," *Proceedings of the 1994 IEEE International Symposium on Information Theory*, Trondheim, Morway, 1994, pp.204.

[12] C. Cachin, *Entropy measures and unconditional security in cryptography*, Ph. D. Thesis, ETH Zurich, Hartung-Gorre Verlag, Konstanz, 1997.

[13] I.T. Jolliffe, *Principle Component Analysis*, Spring-Verlag, New York, 1986.