World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:3, No:3, 2009

# Application of Biometrics to Obtain High Entropy Cryptographic Keys

Sanjay Kanade, Danielle Camara, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi



*Abstract*—In this paper, a two factor scheme is proposed to generate cryptographic keys directly from biometric data, which unlike passwords, are strongly bound to the user. Hash value of the reference iris code is used as a cryptographic key and its length depends only on the hash function, being independent of any other parameter. The entropy of such keys is 94 bits, which is much higher than any other comparable system. The most important and distinct feature of this scheme is that it regenerates the reference iris code by providing a genuine iris sample and the correct user password. Since iris codes obtained from two images of the same eye are not exactly the same, error correcting codes (Hadamard code and Reed-Solomon code) are used to deal with the variability. The scheme proposed here can be used to provide keys for a cryptographic system and/or for user authentication. The performance of this system is evaluated on two publicly available databases for iris biometrics namely CBS and ICE databases. The operating point of the system (values of False Acceptance Rate (FAR) and False Rejection Rate (FRR)) can be set by properly selecting the error correction capacity ($t_s$) of the Reed-Solomon codes, e.g., on the ICE database, at $t_s = 15$, FAR is 0.096% and FRR is 0.76%.

## I. Introduction

Biometrics and cryptography are two technologies widely used for providing security. Biometrics, being strongly associated with the user, ensures his identity; while cryptography provides security to the encrypted data as long as the cryptographic keys are secrete. In a secure authentication system, the user's identity should be verified with high degree of assurance, and at the same time, the system should be revocable, i.e., if the authentication data is found to be compromised, it should be possible to replace that data with a new one which is independent of the data being replaced. Unfortunately, neither biometrics nor cryptography meet these requirements simultaneously: biometrics are non-revocable and cryptography cannot ensure the user identity. Hence researchers have been trying to combine biometrics with cryptography to design a secure authentication system.

In this paper, a two factor scheme is proposed based on iris biometrics that can (re)generate a 94-bit entropy crypto-biometric key using an iris image and a password. The iris image is decomposed using Gabor filters and a 1,188-bit binary string is obtained from the decomposed phase information. This binary string is denoted as an iris code. In the user enrollment step, the key is obtained directly from the iris code by using one-way hash function and a revocable template is created for the user. The user tries to access the system through the authentication step by providing his iris image and password. Since one-way hash functions require exactness in the input to produce the same output, it is necessary to have an iris code exactly the same as the reference iris code at the time of authentication. However, it is well known that two iris codes obtained from two iris images of the same eye always contain some variability. Hence, the proposed system uses the fuzzy sketches idea and error correcting codes to remove the differences between the reference and test iris codes.

The proposed system is an extension of the previous work on cryptographic key regeneration from the same authors [1] which is originally based on Hao et al. [2] system. The system in [1] can obtain variable length keys with 83-bit entropy where the length depends on the accuracy of the system. The scheme proposed in this paper provides increased security to both, the biometric and the key. This scheme uses a well-known cryptosystem – Advanced Encryption Standard (AES) – to protect the shuffling key using a password. The novelty of this scheme is that, it can regenerate the reference iris code of a user by providing another iris image from the same user at the time of authentication. This system provides 94-bit entropy cryptographic keys. The length of the keys obtained using the proposed scheme is independent of the system accuracy. In fact, hash value of the iris code is used as a cryptographic key; hence, the key length can be changed by changing the hash function. This system also uses a random shuffling key which makes the iris template revocable, improves the verification performance, and helps to increase the security of the system.

In this scheme, the biometric matching problem is transformed into an error correction issue. Reed-Solomon codes ($RS$) and Hadamard Codes ($HC$) are used to correct the errors (variability) in iris codes. This system also focuses on the requirement of the password to make such systems truly revocable.

The rest of this paper is organized as follows: related works about combining biometrics and cryptography are briefly summarized in Section II. Section III and Section IV explain, in a more detailed way, the enrollment and authentication steps, respectively. The databases, experimental protocols, and security analysis are given in Section V. Section VI finalizes this paper with conclusions and perspectives.

The first two authors were fully and partially supported by the French "Agence Nationale de la Recherche (ANR)" project BIOTYFUL, (ANR-06-TCOM-018), respectively.

Danielle Camara acknowledges partial support from "Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES)" under Grant No. 1067-07-9.

The authors are with Institut TELECOM: TELECOM & Management SudParis, Départment Electronique et Physique, 9 Rue Charles Fourier, 91011, Evry, France. E-mail: {Sanjay.Kanade,Dijana.Petrovska,Bernadette.Dorizzi}@it-sudparis.eu

## II. Combining Biometrics with Cryptography: Related Works

There are numerous works that suggest combination of biometrics and cryptography. A more detailed description of the related research work in this field can be found in [3]. The related works are divided into two categories based on their main purpose which is: (a) to protect biometric data and make it revocable, such as, [4], [5], [6], [7], and (b) to use biometric data to obtain user specific cryptographic keys, such as, [1], [8], [2], [9], [10], [11], [12].

The systems in the first category are generally referred to as cancelable biometric systems. They use one-way transformation to convert the biometric signal (or feature vector) into irreversible form. Different templates can be issued for different systems using the same biometric. But, these systems require matching of the templates with some kind of distance measure, which means that these templates have variability and cannot be used as cryptographic keys.

The systems related to the second category, key (re)generation systems, possess the properties of cancelable biometrics, and additionally, they can produce stable keys which can be used for cryptographic purposes. These systems either extract some stable bits from the biometric [13], [11], [12], or combine some random information with the biometric data so that a stable string can be extracted using another biometric sample at the time of authentication [1], [8], [2], [9], [10], [14].

## III. Enrollment: Template Generation

This system is based on iris biometric. It uses an Open Source Iris Recognition System (OSIRIS) [15] to extract binary iris codes from iris images. Iris codes extracted from different images of the same eye have two types of errors [2], [1]: (a) Background errors which are random in nature and occur due to camera noise, image capture effects, iris distortions, etc., and (b) Burst errors which result due to eye-lids, eye-lashes, specular reflections, etc. The proposed system treats iris code matching as an error correction problem. A random key is encoded using $RS$ and $HC$. The errors between two iris codes being compared are transferred onto the encoded key and are corrected by the decoding part. Fig. 1 shows the schematic diagram of the enrollment process. The encoding part is discussed in subsection III-A. In order to improve the error correction capacity and security, the iris code modifications suggested in [1] are used, which shuffle the iris code with a shuffling key and then add zeros uniformly to the iris code. These iris code modifications are discussed in subsection III-B.

### A. Random Key Encoding

A user specific random key $K$, having $k_s$ blocks of $m$ bits each, is generated and encoded by $RS(n_s, k_s, t_s)$ to obtain $n_s$ blocks of $m$ bits each. $RS(n_s, k_s, t_s)$ can correct $t_s$ erroneous blocks where, $t_s = (n_s - k_s)/2$. The $HC(k)$ encodes a $(k+1)$-bit block into a $2^k$-bit block. The number of bits in each block is set as $m = k+1$ and the two codes are cascaded such that, the output of $RS$, the $n_s$ blocks, are encoded using $HC(k)$ to obtain $(n_s \times 2^k)$-bit *pseudo-iris code*, $\theta_{ps}$. For these two codes to operate in concatenated form, it is required to set $k = m-1$. The $HC(k)$ can correct at most $2^{k-2}-1$ errors in every block of $2^k$ bits. More details about the error correcting codes can be found in [16].

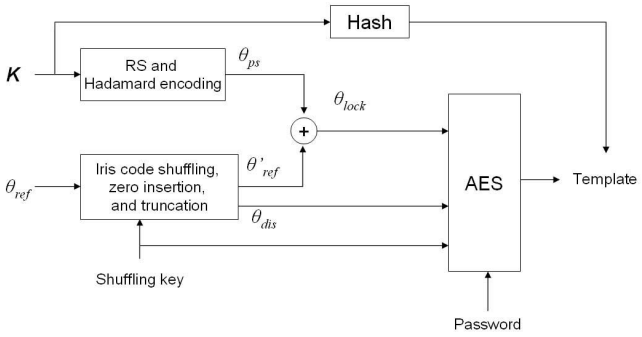


Fig. 1. Schematic diagram for user enrollment phase

### B. Iris Code Modification

The accuracy of any biometric system depends on the ability of that system to separate genuine users from impostors. Genuine and impostor Hamming distance distribution curves show this ability of the system. Larger overlap between the two curves means higher recognition errors such as False Acceptance Rate (FAR) and False Rejection Rate (FRR). The iris code shuffling scheme introduced in [1] is used to increase the separation between the two curves. The iris code is divided into $x$ blocks of $y$ bits each. The iris code blocks are aligned with the $x$-bit shuffling key and the blocks where the key bit is one are sorted first and the remaining blocks are sorted at the end to obtain a shuffled iris code. This scheme increases Hamming distance for impostor comparison, but the Hamming distance for genuine user comparison remains unchanged. Thus it helps in reducing the FAR and FRR of the system. Shuffling also makes the iris code more random which is an added advantage for better security.

Other modification to the iris code is the zero insertion to increase the Hadamard code error correction capacity. Originally, the Hadamard code error correction capacity is 25% (maximum). From the iris code Hamming distance distributions, it was found that, it is required to correct more than 25% errors. So, specific number of zeros are inserted in the iris codes to be compared, which reduces the number of possible errors that can occur in a block, e.g., in a $n$-bit block with $p$ errors, the error ratio $p/n$ can be reduced to $p/(n+q)$ by adding $q$ zeros to the $n$-bit block. Note that, the zero insertion is carried out in reference as well as test iris code. Using this technique, the Hadamard code error correction capacity is changed to 35%. The amount of zeros and the parameters of $RS$ are interdependent and should be selected such that the length of iris code after adding zeros should be either greater than or equal to $(n_s \times 2^k)$. If that length is greater than $(n_s \times 2^k)$, the first $(n_s \times 2^k)$ bits are taken as modified reference iris code $(\theta'_{ref})$, and the remaining bits are called discarded bits $(\theta_{dis})$. The locked iris code, $(\theta_{lock})$, is formed by,

$$\theta_{lock} = \theta_{ps} \oplus \theta'_{ref} \quad . \tag{1}$$

The shuffling key is a long random bit string which is not possible to remember. Hence, the shuffling key, $\theta_{lock}$, and $\theta_{dis}$ are encrypted by a password and the encrypted data along with the hash value of the key $K$, $H(K)$, is stored as a template for the user.

Here, it is worthwhile to point out an important aspect about the use of the password. The password makes the system truly revocable. If the template is found to be compromised, it can be replaced by another template by changing the random key $K$, shuffling key, and password, and using another iris code. The data provided by the user is an iris code and a password. If the system does not employ password, then the only secrete is the iris code (which is compromised), and though the new template is different from the older one, it is no more secure and is directly susceptible to attacks. In this case an attacker does not even need to carry out any cryptanalysis because he will have the iris code from his previous successful attempt which is enough to obtain the cryptographic key. Instead, if the system uses a password along with the iris biometrics, the password can be changed and the attacker will have to carry out the cryptanalysis of the encrypted data again.

## IV. Authentication: Cryptographic Key Regeneration

A cryptographic key can be regenerated from the stored template by providing a genuine iris sample along with the correct password. Fig. 2 shows the schematic diagram of the key regeneration process. Similar to the enrollment stage, OSIRIS is used to extract a test iris code, $\theta_{test}$, from the provided iris sample. The iris code modification steps described in subsection III-B are carried out on the $\theta_{test}$ to obtain a modified test iris code $\theta'_{test}$. This $\theta'_{test}$ is used to unlock the $\theta_{lock}$ and obtain a trial value of the encoded random key $K'$ as explained in the following subsection.

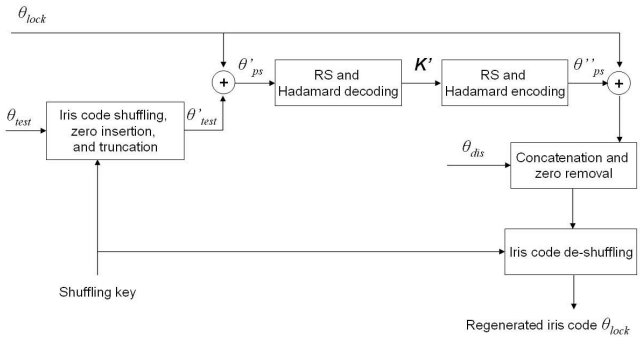


Fig. 2. Schematic diagram for user authentication phase (It is assumed that the template data is already decrypted)

### A. Template Unlocking and Random Key Regeneration

The locked iris code $\theta_{lock}$ is XORed with the modified test iris code $\theta'_{test}$ to get $\theta'_{ps}$, and from (1),

$$\begin{aligned} \theta'_{ps} &= \theta_{lock} \oplus \theta'_{test} \ , \\ &= \theta_{ps} \oplus \theta'_{ref} \oplus \theta'_{test} \ , \\ &= \theta_{ps} \oplus e \ , \end{aligned} \tag{2}$$

where $e$ is the error vector between the two iris codes. The $\theta'_{ps}$ is decoded using the $HC(k)$ to correct background errors. $HC(k)$ operates on blocks having $2^k$ bits each and the blocks having fewer errors than the error correction capacity of $HC(k)$ are decoded correctly and those which have more errors are decoded incorrectly. This results in $n_s$ blocks of $m$ bits each. If the number of blocks that are decoded incorrectly by $HC(k)$ is less than or equal to $t_s$, then those blocks can be corrected by $RS$ to obtain a trial value of the key $K'$. The hash value of $K'$ is compared with $H(K)$, and if found equal, the key $K'$ is processed further to regenerate the reference iris code. If the two hash values are not equal, the normalized test iris image is translated horizontally in both directions (up to 10 times in each direction) to adjust for rotation and next trial value $K'$ is calculated. If the hash values do not match for any of the values of $K'$, a user mismatch is declared. The value of $t_s$ can be tuned to achieve desired accuracy in terms of FAR and FRR.

### B. Regenerating Reference Iris Code and Cryptographic Key

In this step, the reference iris code which was locked at the time of enrollment is regenerated. The regenerated random key $K'$ is re-encoded using $RS$ and $HC(k)$ to obtain $\theta''_{ps}$. This $\theta''_{ps}$ is used to unlock the $\theta_{lock}$ to obtain the regenerated modified reference iris code $\theta''_{ref}$ as:

$$\theta''_{ref} = \theta_{lock} \oplus \theta''_{ps} \ . \tag{3}$$

Since, $H(K) = H(K')$, $K' = K$, and $\theta_{ps} = \theta''_{ps}$. Thus,

$$\theta''_{ref} = \theta_{lock} \oplus \theta_{ps} = \theta'_{ref} \ . \tag{4}$$

The regenerated code $\theta''_{ref}$ is augmented with the discarded bits from the iris code $\theta_{dis}$, to obtain the shuffled reference iris code with zeros. Since the locations of the inserted zeros are known, they can be removed easily to get the shuffled iris code. Iris code de-shuffling is applied on this code to obtain the regenerated reference iris code $\theta_{reg}$. Hash value of this regenerated iris code is used as a cryptographic key. The hash function determines the length of this key, thus the length is independent of the accuracy of the system.

## V. Database, Experimental Results, and Security Analysis

Publicly available and well-known iris-databases, Casia-BioSecure (CBS) database [15] (OKI device subset) and Iris Challenge Evaluation (ICE) database [17], were used to evaluate the system. At first, various tests were carried out on CBS database to find the best performance parameters, and then with these parameters, the system was tested on the ICE database.

The CBS database has two parts: (a) BiosecureV1 containing 1,200 images from 60 eyes of 30 persons with 20 images from each eye, and (b) CasiaV2 - which is a subset of CASIA Version 2 database. It also contains 1,200 images from 60 eyes of 30 persons with 20 images from each eye. Each of these two parts is divided into two datasets as:

1) Reference (enrollment) dataset composed of the first 10 images of each eye, and
2) Test dataset composed by the remaining 10 images.

The benchmarking protocol as described in [15] was followed, which yields 6,000 trials for genuine matches and 6,000 trials for imposter matches for each part of the database. These trials also result in comparison between images obtained in different sessions and different illumination conditions.

In order to show the robustness of the proposed system across databases, the system was tested on the NIST-ICE database [17] with parameters ($m, n_s, k$, etc.) obtained from CBS database tests. This database consists of 2,953 images from 244 different eyes. Two experiments were carried out for this database: Exp-1 – with right eyes, and Exp-2 – with left eyes. All possible comparisons between iris images were carried out for the two experiments, i.e., for Exp-1, 12,214 genuine, and 1,002,386 impostor comparisons, and for Exp-2, 14,653 genuine, and 1,151,975 impostor comparisons.

OSIRIS is used to extract iris codes from these images. OSIRIS has two main parameters: filters and analysis points. The OSIRIS parameters are set to 6 filters and 198 analysis points which yield 1,188 bit iris codes. In order to match the iris code structure, the number of blocks is set to $x = 198$ and number of bits in each block $y = 6$ for the shuffling algorithm. Thus the shuffling key length is set to 198 bits which will be protected with a password of eight characters.

### A. Results

As explained earlier, the parameters of the proposed system such as number of zeros to be added to iris codes, $n_s, t_s, m$, etc., are tuned on the CBS database. Empirically it is found that the best value for the number of zeros to be inserted in the iris codes is 792. These zeros are inserted uniformly in the iris code (e.g., two zeros after every three iris code bits). This increases the iris code length to 1,980 bits, and in order to make it compatible with the coding scheme, the first 1,952 bits are called as $\theta'_{ref}$ and the last 28 bits are called as $\theta_{dis}$. The addition of zeros distributes the iris code bits in such a way that, there can be 20 to 21 iris code bits in a particular 32-bit Hadamard code block. Thus, the maximum error correction capacity of $HC$ becomes $7/20 = 0.35$ (i.e. 35%). After finding the best performance parameters on CBS database, the system was tested on ICE database with the same parameters. The error correction capacity of the Reed-Solomon codes, $t_s$, acts as a threshold, which can be changed to get the desired accuracy in terms of FAR and FRR, e.g., by changing $t_s$ from 9 to 16, the FRR can be reduced from 4.61% to 0.69%, but consequently, the FAR increases from 0% to 0.33%. Table I shows the results on both the databases for various values of $t_s$. Note that, the parameters obtained from CBS database tests are also applicable to the ICE database, which demonstrates the portability of the system.

TABLE I
RESULTS FOR THE PROPOSED SYSTEM; USING PASSWORD AND ZERO INSERTION ($\approx 35\%$ ERROR CORRECTION); $n_s = 61$, $m = 6$.

| $t_s$ | Biosecure V1 | | Casia V2 | | ICE-Exp-1 | | ICE-Exp-2 | |
|---|---|---|---|---|---|---|---|---|
| | FAR | FRR | FAR | FRR | FAR | FRR | FAR | FRR |
| 1 | 0 | 30.53 | 0 | 49.70 | 0 | 49.39 | 0 | 52.99 |
| 2 | 0 | 22.12 | 0 | 35.78 | 0 | 33.26 | 0 | 37.74 |
| 3 | 0 | 16.37 | 0 | 26.27 | 0 | 24.26 | 0 | 25.78 |
| 4 | 0 | 12.88 | 0 | 19.25 | 0 | 16.50 | 0 | 20.10 |
| 5 | 0 | 10.65 | 0 | 14.82 | 0 | 12.67 | 0 | 16.25 |
| 6 | 0 | 8.98 | 0 | 11.70 | 0 | 10.31 | 0 | 11.81 |
| 7 | 0 | 8.35 | 0 | 9.52 | 0 | 7.29 | 0 | 9.42 |
| 8 | 0 | 7.27 | 0 | 7.32 | 0 | 5.93 | 0 | 7.77 |
| 9 | 0 | 6.60 | 0 | 5.97 | 0 | 4.61 | 0 | 6.26 |
| **10** | **0** | **5.87** | **0** | **4.85** | **0** | **3.63** | **0.001** | **4.54** |
| 11 | 0 | 5.28 | 0.02 | 3.77 | 0.001 | 2.48 | 0.002 | 3.49 |
| 12 | 0.02 | 4.57 | 0.08 | 3.13 | 0.005 | 2.13 | 0.033 | 3.05 |
| 13 | 0.03 | 3.97 | 0.12 | 2.12 | 0.021 | 1.46 | 0.018 | 2.12 |
| 14 | 0.32 | 3.25 | 0.52 | 1.57 | 0.055 | 1.04 | 0.13 | 1.41 |
| **15** | **0.70** | **2.67** | **1.15** | **1.07** | **0.096** | **0.76** | **0.21** | **1.09** |
| 16 | 1.38 | 2.00 | 2.50 | 0.63 | 0.33 | 0.69 | 0.31 | 0.94 |
| 17 | 2.77 | 1.43 | 5.30 | 0.30 | 0.95 | 0.47 | 3.14 | 0.61 |
| 18 | 5.55 | 1.00 | 9.68 | 0.25 | 1.81 | 0.38 | 5.62 | 0.46 |
| 19 | 9.57 | 0.63 | 17.52 | 0.15 | 11.37 | 0.26 | 7.62 | 0.39 |
| 20 | 16.18 | 0.42 | 28.20 | 0.05 | 11.77 | 0.15 | 14.77 | 0.29 |
| 21 | 24.42 | 0.23 | 41.32 | 0.03 | 14.20 | 0.13 | 18.38 | 0.20 |
| 22 | 36.22 | 0.13 | 56.72 | 0 | 21.99 | 0.11 | 30.80 | 0.13 |

### B. Security Analysis

The main purpose of the system proposed in this paper is to obtain strong keys from biometric data denoted as crypto-biometric keys. Therefore, it is important to estimate the entropy of these crypto-biometric keys. The secrete information used in this system is iris code and shuffling key. The shuffling key can be re-obtained by decrypting the template data using a password. In order to have high security, it is suggested to use a randomly generated 8-character password which can have 52 bits entropy [18].

There are two ways an attacker can follow to obtain the cryptographic key: (a) by guessing the (un-shuffled) iris code and password separately, or (b) by obtaining modified iris code $\theta'_{test}$ and the password.

In an iris code, all bits are not independent, but there exist some correlations. The number of degrees of freedom in iris codes can be calculated from the experimental data by following the procedure given in [19]. From the current experimental data, the number of degrees of freedom of the un-shuffled iris codes was found to be $N = 561$. The coding scheme allows 35% ($P = 196$) bits to be wrong. Using the similar approach as of Hao et al. [2], the entropy is estimated to be,

$$H' \approx \log_2 \frac{2^N}{\frac{N!}{P!(N-P)!}} \approx 42 \text{ bits} \ . \tag{5}$$

The shuffling key, which is securely encrypted by a password having 52-bit entropy, is required to regenerate the reference iris code. This means that an attacker has to carry out $2^{42} \times 2^{52} = 2^{94}$ trials to successfully regenerate the reference iris code. Hence the total entropy of the final key is $H = 52 + 42 = 94$ bits. Note that the 561 degrees of freedom is a statistical estimate; at present, it is unknown how to find out the uncorrelated iris code bits without knowing the iris code itself [2].

The shuffling scheme makes the iris codes more random. The number of degrees of freedom of the modified iris code ($\theta'_{test}$) can be calculated in a similar way and is found to

be 1,172 bits. If an attacker tries to obtain the modified iris code ($\theta'_{test}$), the security estimate can be calculated using equation (5), which results in 83 bits. These calculations are followed by the de-shuffling phase which requires the cryptanalysis of the encrypted data to obtain the shuffling key. The cryptanalysis requires $2^{52}$ calculations which results in total entropy of $83 + 52 = 135$ bits.

In order to enhance the security, the authors propose to limit the maximum number of login attempts before lockout. Moreover, it is proposed that a smart card should not be used in such systems because it can allow an unlimited number of off-line calculations which can help cryptanalysts. It means that, the templates should be stored on a central database. Note that, the biometric data is not stored in its plain form. The templates contain user specific (and also system specific) random information in encrypted form which makes cross-matching between databases impossible. Thus it also takes care of the user privacy.

## VI. Conclusions and Perspectives

In this paper, a biometric based cryptographic key generation scheme is presented. The keys are strongly bound with the user's identity since the user iris along with the password is required to regenerate the keys. This scheme combines the entropy of iris (42 bits) with the password entropy (52 bits) to have 94-bit entropy keys, which is higher than any other comparable systems [2], [8], [1]. This system uses password which helps in improving the verification performance of the system and increases the security. It was shown that the password is an essential element of the system to make it truly revocable. The experimental results show good performance (e.g., 0.096% FAR at 0.76% FRR for ICE-Exp-1) on different publicly available databases such as CBS and ICE database and also demonstrate the portability of the system.

This scheme can be adopted to other biometric modalities. The requirement for such modification is that the biometric features should be in form of a binary vector and the error correcting codes are chosen to match the error characteristics of those features. This system can be extended to include more biometric modalities to obtain a multi-biometric cryptographic key.

## References

[1] S. Kanade, D. Camara, E. Krichen, D. Petrovska-Delacrétaz, and B. Dorizzi, "Three factor scheme for biometric-based cryptographic key regeneration using iris," in *The 6th Biometrics Symposium*, 2008.

[2] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

[3] A. Cavoukian and A. Stoianov, "Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy," Information and privacy commissioner of Ontario, White Paper, March 2007.

[4] T. E. Boult, W. J. Scheirer, and R. Woodworth, "Revocable fingerprint biotokens: Accuracy and security analysis," in *IEEE Conference on Computer Vision and Pattern Recognition*, June 2007, pp. 1–8.

[5] A. Lumini and L. Nanni, "An improved biohashing for human authentication," *Pattern Recognition*, vol. 40, no. 3, pp. 1057–1065, March 2007.

[6] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 561–572, April 2007.

[7] M. Savvides, B. V. Kumar, and P. Khosla, "Cancelable biometric filters for face recognition," in *Proceedings of the 17th International Conference on Pattern Recognition (ICPR04)*, vol. 3, August 2004, pp. 922–925.

[8] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zmor, "Optimal iris fuzzy sketches," in *IEEE Conference on Biometrics: Theory, Applications and Systems*, 2007.

[9] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proceedings of the Sixth ACM Conference on Computer and communication Security (CCCS)*, 1999, pp. 28–36.

[10] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. IEEE Int. Symp. Information Theory*, A. Lapidoth and E. Teletar, Eds. IEEE Press, 2002, p. 408.

[11] F. Monrose, M. Reiter, and R. Wetzel, "Password hardening based on keystroke dynamics," in *Proceedings of the Sixth ACM Conference on Computer and communication Security (CCCS)*, 1999, pp. 73–82.

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

[13] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proceedings of the Eurocrypt*, 2004.

[14] U. Uludag and A. Jain, "Securing fingerprint template: Fuzzy vault with helper data," in *Proc. of the 2006 Conference on Computer Vision and Pattern Recognition Workshop*, June 2006, pp. 163–170.

[15] E. Krichen, B. Dorizzi, Z. Sun, S. Garcia-Salicetti, and T. Tan, *Guide to Biometric Reference Systems and Performance Evaluation*. Springer-Verlag, 2008, ch. Iris Recognition, pp. 25–50.

[16] F. J. MacWilliams and N. J. A. Sloane, *Theory of Error-Correcting Codes*. North Holland, 1991.

[17] National Institute of Science and Technology (NIST), "Iris Challenge Evaluation," 2005, http://iris.nist.gov/ice.

[18] W. E. Burr, D. F. Dodson, and W. T. Polk, "Electronic authentication guideline: Recommendations of the National Institute of Standards and Technology," April 2006.

[19] J. Daugman, "The importance of being random: Statistical principles of iris recognition," *Pattern Recognition*, vol. 36, no. 2, pp. 279–291, February 2003.