Multi-biometrics based cryptographic key regeneration scheme

Sanjay Kanade, Dijana Petrovska-Delacrétaz, Bernadette Dorizzi

Multi-Biometrics Based Cryptographic Key Regeneration Scheme

Sanjay Kanade* Dijana Petrovska-Delacrétaz Bernadette Dorizzi

Abstract— **Biometrics lack revocability and privacy while cryptography cannot detect the user's identity. By obtaining cryptographic keys using biometrics, one can achieve the properties such as revocability, assurance about user's identity, and privacy. In this paper, we propose a multi-biometric based cryptographic key regeneration scheme. Since left and right irises of a person are uncorrelated, we treat them as two independent biometrics and combine in our system. We propose a novel idea for feature level fusion through weighted error correction to obtain a multi-biometric feature vector which is used to get a secure template. A shuffling key which is protected by a password is used to shuffle the error correcting codes data. The password helps improve revocability, privacy, and security of the system. We succeed to generate 147-bit long keys with as much entropy at 0% FAR and 0.18% FRR on the NIST-ICE database.**

Index Terms— **Multi-biometrics, cryptography, key generation, error correcting codes.**

I. Introduction

Biometric systems recognize a person based on his physiological or behavioral characteristics (e.g., fingerprint, face, iris, signature, voice, etc.). Since these characteristics are strongly bound to the user, biometrics provide high degree of assurance about his identity. But there are some drawbacks associated with biometrics. The biometric data are permanently associated with the user. Hence, if they are compromised, it is not possible to replace them. In this situation, the biometric data become unusable in that system and possibly in all other systems using the same biometric feature. This is called lack of revocability. Another problem associated with biometrics is that it can cause a threat to user privacy. When two information databases are protected by using biometrics, it is possible to track information stored in one database by having access to another database through cross-database matching between biometric databases.

Cryptography, on the other hand, is a widely used technique for secure transmission or storage of sensitive data. In cryptography, the data is encrypted using numerical keys called cryptographic keys. The cryptographic keys are long and generally a user cannot remember them. Hence they are either protected by a comparatively smaller password or stored on a token. The drawback of such a system is that neither the password nor the token is strongly bound to the user. They can be stolen by someone else and used to access the system. The non-association of the token/password with the user identity can also allow a user to falsely repudiate: he can claim that he did not access the system and the token/password was stolen even when it was not. Thus cryptography lacks the assurance needed about the user's identity.

As we discussed in [1], an ideal secure user authentication system should possess the property of revocability, protect user privacy, and provide assurance about the user's identity. Biometric based cryptographic key generation systems can achieve all of these goals. A user specific cryptographic key is randomly generated at the time of enrollment and is stored in the system in form of a secure crypto-biometric template. The key is regenerated with the help of biometrics and can be used for cryptographic purposes. Thus the key is strongly bound to the user. Also, the regenerated key and the original key can be compared using their hash values and result of this comparison can be used for user verification/authentication.

There are many uni-biometric systems found in literature which combine biometrics and cryptography but most of them face the problems of low entropy keys and high rejection rates. Using multiple biometrics is a possible solution to overcome these problems. There are various types of multi-biometric systems such as multi-sensor, multi-algorithm, multi-instance, multi-sample, and multi-modal systems [2]. When such systems are used, there is more discriminating information available per individual which helps to improve the biometric verification performance. There are many different strategies for combining biometric information depending on the level of information fusion such as sensor level, feature level, score level, rank level, etc. [2]. But when it comes to combining multi-biometrics with cryptography, there is not much work done in this regard. Recently, Nandakumar and Jain [3] proposed a multi-biometric template protection scheme which we discuss briefly in Section II.

In this paper, a multi-biometrics based cryptographic key regeneration scheme is proposed. It is a multi-instance system combining information from left and right irises of persons. Daugman [4] has shown that left and right irises of a person are not correlated and thus can be regarded as two independent sources of biometric information. We extract distinctive information from user iris images in form of iris codes. An iris image is decomposed using Gabor filters and the quantized phase information is used to construct an iris code. We combine the iris codes obtained from images of both the eyes of a user to obtain a combined multi-biometric feature vector. Moreover, we propose a novel approach for information fusion in the feature domain through weighted error correction which helps improve the performance. Finally, we introduce a shuffling key (protected

*The first author is supported by the French "Agence Nationale de la Recherche (ANR)" project BIOTYFUL, (ANR-06-TCOM-018).

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

by a password) which helps improve the system accuracy, privacy, and security.

The rest of this paper is organized as follows: some of the works related to combination of biometrics and cryptography are reported in Section II. The proposed multi-biometric based key regeneration system is explained in detail in Section III. The databases and experimental protocols used for performance evaluation are presented in Section IV, whereas the results and security analysis are reported in Section V and VI, respectively. Finally, Section VII sets out the conclusions and perspectives.

II. Combining Biometrics with Cryptography: Related Works

Cavoukian and Stoianov [5] have discussed biometric encryption schemes. We classify these systems in three main categories: (a) *cancelable biometrics* [6], [7], [8], [9], [10], (b) *cryptographic key generation* [11], [12], and (c) *cryptographic key regeneration* [13], [14], [15], [16], [17], [1], [18].

In cancelable biometrics, the biometric feature vector (or signal) is transformed using some kind of (one-way) transformation in such a way that the inter-personal variations are preserved. The transformed templates are compared using some similarity (or dissimilarity) measure followed by a classifier. Some of the works in this category include cancelable filters for face recognition by Savvides et al. [6], cancelable fingerprint templates by Ratha et al. [7], improved BioHashing by Lumini and Nanni [8], revocable fingerprint biotokens by Boult et al. [9], and cancelable iris biometrics by Kanade et al. [10]. Lumini and Nanni [8], Boult et al. [9], and Kanade et al. [10] report improvement in the biometric system performance whereas Savvides et al. [6] report performance invariance. Ratha et al. [7] report degradation in the performance. The cancelable templates generated in these systems need to be compared using some similarity metrics and therefore they cannot be used as cryptographic keys because cryptographic keys require exactness.

In the second category – cryptographic key generation – a stable bit-string is extracted from the biometric sample. *Hardened password* [11] and cryptographic key generation from voice [12] by Monrose et al. fall under this category. The problem associated with these systems is that they still lack revocability. The key is extracted from the biometrics and hence in case of compromise, changing the key is not possible.

In cryptographic key regeneration, some random data is generally assigned to each user and is combined with his biometric features. There are two popular constructs in this category: the *Fuzzy commitment scheme* [14] and the *Fuzzy vault scheme* [19]. The biometric variabilities are treated as errors in these systems and Error Correcting Codes (ECC) are used to correct those errors. The random data can be reobtained by providing another biometric data from the same user. The regenerated random data can be used as a cryptographic key. Summary of some of the systems in this category is given in Table I.

Recently, Nandakumar and Jain [3] proposed a multi-biometric scheme in which they use fingerprint with iris to generate cryptographic keys using the *fuzzy vault* scheme originally proposed by Juels and Sudan [19]. It is basically a feature level fusion scheme which outperforms either of the two uni-modal biometric fuzzy vaults and also results in longer cryptographic keys.

In the next section, we propose a multi-biometric scheme with which we can obtain long keys with higher entropies.

III. Multi-biometrics Based Cryptographic Key Regeneration Scheme

In this section, we provide details of the algorithm for obtaining multi-biometric based cryptographic keys. The basic structure of this scheme is the same as the Hao et al. [15] scheme (Fig. 1). It is well known that the iris codes obtained from different iris images of the same user contain variabilities which are referred to as errors in this paper. There are two types of errors in iris codes: (1) background errors caused by the camera noise, image capture effects, etc., and (2) burst errors which are a result of specular reflections, occlusions, etc. As in [15], Error Correcting Codes (ECC) are used to cope with these errors.

A random bit string $\mathbf{K}$ is generated and assigned to a user and is then encoded using Reed-Solomon (RS) codes, the output of which is further encoded by Hadamard codes. The Hadamard codes correct the background errors and RS codes correct burst errors. Details about these ECC can be found in [20]. The output of the encoder is called *pseudo code* $\mathbf{S}$. In order to cope with the cascading structure of the two ECC, the number of bits in each symbol of RS and that in the input words of Hadamard codes is set to be equal ($m = 7$). The reference iris code $\mathbf{I}_{ref}$ (or in general, a biometric feature vector in binary form) is XOR*ed* with $\mathbf{S}$ to obtain the locked iris code template $\mathbf{I}_{lock}$. In the key regeneration phase, another iris code $\mathbf{I}_{test}$ (the test iris code) is XOR*ed* with $\mathbf{I}_{lock}$. These XOR*ing* operations transfer the errors in the iris codes onto the pseudo code. If the amount of errors is within the error correction capacity of the ECC, the errors are corrected by the ECC decoder part and a key $\mathbf{K}'$ is regenerated which is the same as $\mathbf{K}$. If there are more errors, the regenerated key $\mathbf{K}' \neq \mathbf{K}$.

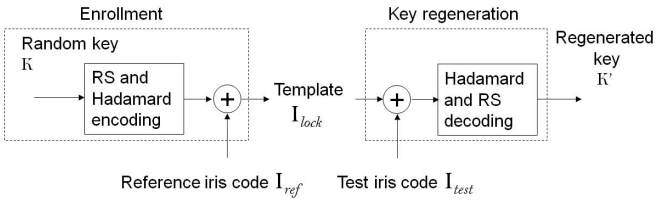


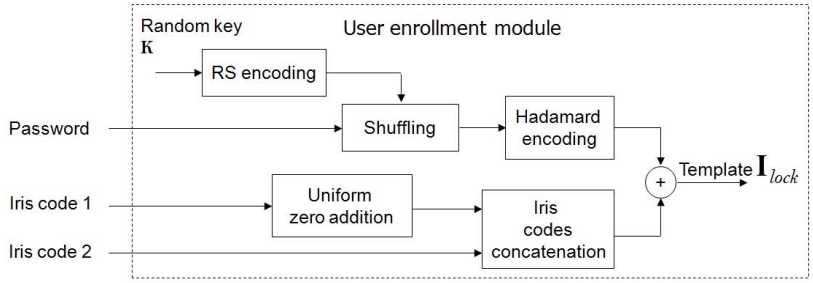
Fig. 1. Schematic diagram for biometric based cryptographic key regeneration system (similar to the Hao et al. [15] scheme).

In the ECC scheme in Fig. 1, there are two levels of error correction: in the first level, the Hadamard codes correct (up to) $2^{(k-2)} - 1$ errors in a 2^k-bit block. If a block has more

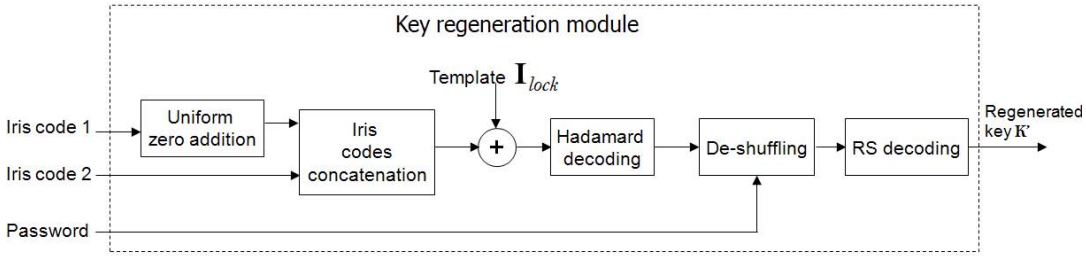
TABLE I

SUMMARY OF SOME OF THE CRYPTOGRAPHIC KEY REGENERATION SYSTEMS FOUND IN LITERATURE; FAR AND FRR VALUES ARE IN %. ECC – ERROR CORRECTING CODES; RSH – REED-SOLOMON AND HADAMARD CODES; RMP – REED-MULLER AND PRODUCT CODES.

Reference	ECC	Length(K) (in bits)	Entropy(K) (in bits)	Password used	FAR	FRR	Database
Hao [15]	RSH	140	44	No	0	0.47	proprietary
Bringer [17]	RMP	42	-	No	10^{-5}	5.62	ICE
Kanade [1]	RSH	234	83	Yes	0.0008	2.48	ICE (right eye)
Kanade [18]	RSH	128/256	94	Yes	0.096	0.76	ICE (right eye)



(a)



(b)

Fig. 2. Schematic diagram of the proposed multi-biometric based cryptographic key regeneration scheme using feature level fusion, weighted error correction, and password – (a) User enrollment phase; (b) Cryptographic key regeneration phase.

than $2^{(k-2)} - 1$ errors, that block is not decoded correctly and results in an error. The second level of ECC consists of the RS codes. The output of the Hadamard decoding stage acts as the input to the RS decoder stage. The RS codes correct the errors caused due to the wrong decoding by the Hadamard codes and generate the key $\mathbf{K}'$.

A. Feature Level Fusion

As discussed earlier in Section I, multi-biometric information fusion can help improve biometric system performance. Moreover, in key regeneration systems, this can lead to improved security by increasing the entropy of the key. In our proposed system, the two iris codes $\mathbf{I}_1$ and $\mathbf{I}_2$ obtained from the images of right and left eye of a person, respectively, are concatenated to form one single feature vector $\mathbf{I}_{ref}$ (or $\mathbf{I}_{test}$ during regeneration). This combined feature vector is used in the key regeneration scheme of Fig. 1. As is obvious, there is double the information available per person and hence, as expected, the key regeneration system using such concatenated feature vector performs better than the system using single iris. But, we found out that, even though there is an improvement in the performance, the False Rejection Rate (FRR) for the key regeneration system is still much high (Table III). In order to further improve the performance of the key regeneration system, we propose a Weighted Error Correction scheme in the next subsection.

B. Weighted Error Correction

In this scheme, we tune the ECC parameters such that, more errors will be corrected in one iris code than in the other. As discussed earlier, there are two levels of error correction in the ECC scheme. We apply different error corrections on the two iris codes at the first level of error correction, i.e., in the Hadamard error correction stage. In [1], we have shown that adding a definite amount of zeros at predetermined locations in the iris codes can help correct a higher amount of errors by the Hadamard codes. We use that technique for the first iris code $\mathbf{I}_1$ so that more errors in that iris code are corrected whereas the other iris code $\mathbf{I}_2$ is not altered. The modified first iris code $\mathbf{I}'_1$ is combined with $\mathbf{I}_2$ to get the final multi-eye iris code $\mathbf{I}'_{ref}$ ($\mathbf{I}'_{test}$ at the time of key regeneration). When the iris code errors are transferred onto

the pseudo code by the XOR*ing* operations and Hadamard decoding is applied, the first iris code part results in more number of correct decodings than the second iris code part. If the number of wrongly decoded blocks is $\leq t_s$ (where t_s is the error correction capacity of the RS codes), they are correctly decoded by the RS decoder to generate the key $\mathbf{K}'$.

Here, the number of correctly decoded blocks after the Hadamard decoding stage can be seen as a similarity score and the RS decoding stage can be considered as a threshold based classifier with t_s as a threshold. Thus the variable error correction acts as a weighting scheme and results in a fusion score having higher weight to the first iris than to the second. The increased error correction for the first iris code helps to increase acceptances while the low error correction for the second iris code increases rejections. The combined effect of the two is the improvement in the key generation performance of the system. If there are two different biometric modalities involved in this scheme, higher weights can be applied to the better performing modality while less weights can be used for the other.

C. Adding Password for Higher Security and Privacy

In order to increase the security of the system (i.e., entropy of the cryptographic key) and to further improve the key generation accuracy, we use the shuffling scheme originally proposed in our previous work [1]. The shuffling key is randomly generated and is protected by a user password using standard security mechanisms such as AES [21]. There is one important difference between the usage of the shuffling scheme in this paper and that in [1] which can be seen in Fig. 2(a). In the scheme proposed in this work, we shuffle the RS encoder output using the shuffling key as opposed to the iris code shuffling in [1].

This change in the location of shuffling is required for security reasons because of the systematic nature of the RS codes. An error correcting code is said to be systematic when portion of the output codeword contains the input data in original form. Put in simple way, the input to the RS code is present in its output. In fact, the output of the RS codes is the input symbols appended with the redundant symbols. This does not pose a security threat to the Hao et al. [15] and Kanade et al. [1] schemes because there is only one error causing part (i.e., the iris code). In our two iris system, an attacker can make use of the systematic nature of the RS codes to break into the system by using only one iris code thus limiting the entropy to that offered by one iris code only. The basic goal of using two irises is to increase the entropy which in this case will not be satisfied. Instead, if the shuffling is applied to the RS codes output, its systematic structure is broken and an attacker has to 'crack' both the iris codes.

The shuffling process is carried out as follows: the output codeword of the RS encoder, denoted as $\mathbf{K}_{RS}$, is in form of blocks. These blocks are first aligned with the shuffling key bits. The shuffling process works as follows: if a particular bit in the shuffling key is one, that corresponding block of $\mathbf{K}_{RS}$ is taken into part 1 and if not then in part 2.

```
N = total number of 1's in the shuffling key;
count1 = 0;
count2 = 0;
for i = 1 to length of the shuffling key,
   if shuffling key(i) = 1,
      count1 = count1 + 1;
      deshuffled_data(i) = shuffled_data(count1);
   else
      count2 = count2 + 1;
      deshuffled_data(i) = shuffled_data(N + count2);
   end if
end for
```

Fig. 3. Pseudo program code for the de-shuffling algorithm.

Concatenation of part 1 and part 2 gives the shuffled data which is further encoded using the Hadamard encoder to obtain the *pseudo code* $\mathbf{S}$. Feature level fusion through weighted error correction is carried out as described in the pervious subsections and the fused iris code is XOR*ed* with the pseudo code to obtain the locked code $\mathbf{I}_{lock}$. This locked code along with the shuffling key encrypted by a password form a template for the person.

The key regeneration phase, shown in Fig. 2(b), also involves similar operations as in enrollment to obtain a fused iris code. This fused iris code is XOR*ed* with the locked iris code of the user stored in the template. This transfers the errors between the reference iris code and test iris code onto the pseudo code. This modified pseudo code is decoded by the Hadamard decoder which results in shuffled $\mathbf{K}_{RS}$ along with some errors. Since the $\mathbf{K}_{RS}$ was shuffled while enrollment, it is required to de-shuffle it before the RS decoder can correct the errors in it. Contrary to this, the shuffling scheme in [1] is applied on the iris codes before XOR*ing* them with the *pseudo code*, and hence, de-shuffling is not required in that system. Hence we developed an algorithm to de-shuffle the data and the pseudo program code of this algorithm is given in Fig. 3.

Other important benefit of using the password is that it protects the user privacy. The password is required to obtain the shuffling key which in turn is required to regenerate the crypto-biometric key $\mathbf{K}$. Without the correct password, it is not possible to obtain the key $\mathbf{K}$. Thus cross-matching between biometric databases is very difficult. This also allows the use of central template database and eliminates the use of a physical token. Moreover, the password provides better revocability. If a password is not involved (e.g., as in [15], [17], [3]), and it is found out that a template is compromised, then in such systems, the template is revoked by changing the crypto-biometric key (and token if involved). But the attacker who has the genuine iris code from his previous successful attempt (we can assume this since the template is compromised), can re-access the system by providing the iris code without needing to carry out the attack. Instead, in the proposed system, the compromised template can be revoked by changing the crypto-biometric key, shuffling key, and the password. In this case, the attacker needs to carry out the attack every time because of the password.

IV. Databases and Experimental Protocols

We use the open source iris recognition system OSIRIS [22] to extract iris codes from the iris images. The iris image is decomposed using Gabor filters at different scales and orientations and then the phase information from the decomposed images is quantized to obtain a 1,188-bit iris code.

The proposed system is evaluated for biometric verification performance on two different iris databases. The Casia-BioSecure (CBS) database [22] is used to tune the system parameters and then using those parameters, the system is tested on the National Institute of Standards and Technology (NIST) – Iris Challenge Evaluation (ICE) database [23].

We selected only a part of the CBS database – the OKI device subset of the BioSecureV1 part, which we refer to as CBS-Bio dataset in this paper. It has 20 images from each eye of 30 persons, i.e., 1200 images. The original CBS protocol reported in [22] is for single eye comparisons. We followed the same structure for our two eye tests thus resulting in exactly half the tests than reported in [22]. Thus there are 3,000 genuine comparisons and 3,000 impostor comparisons.

In the ICE database, 124 persons have recorded their right iris images and there are 120 persons with left iris images. 112 users are common to both these datasets, i.e., 112 persons have recorded both right and left iris images. We select these images of 112 persons for carrying out our tests. The right iris images are coupled with the left iris images for the multi-iris tests. The first such couple of images of a person is considered for enrollment and a template is registered for that person. The genuine comparisons are carried out by comparing the remaining images of that user with the enrollment template which results in 1,099 genuine comparisons. For impostor comparisons, a randomly selected image couple of all the remaining persons is compared with the enrollment template. Thus, for each person, we carry out 111 impostor comparisons. In summary, we carry out 1,099 genuine and 12,432 impostor comparisons on the ICE database. The sample lists of comparisons generated using these protocols are available online [24].

V. Experimental Results

We extensively tested our system on the CBS database to find out the optimum parameters such as the ECC parameters and number of zeros to be added to the iris codes. The system was then evaluated on the ICE database using the same parameters and the results are reported in this section. Since there is a possibility of iris rotations during image acquisition, we move the normalized iris image horizontally in both directions to eliminate the rotation effects.

Since the proposed systems is based on an iris recognition system, it is worthwhile to report the performance of the baseline biometric system for fair comparison. Hence, such performance results are reported in Table II using the protocols described in the previous section. Note that, as expected, the combination of left and right irises results in reduction in Equal Error Rate (EER).

TABLE II

Baseline biometric system (OSIRIS) user verification performance in terms of EER in %.

CBS-Bio dataset			NIST-ICE database		
Left	**Right**	**Both irises**	**Left**	**Right**	**Both irises**
3.23	2.90	2.54	2.44	4.81	1.18

For the cryptographic key regeneration system, we first report the results for our feature level fusion scheme in Table III. For the sake of comparison, the key regeneration results (for CBS database) using single irises are also reported in the same table. It can be observed that the minimum FRR using single iris is 7.37% with a key length of 6 bits. The combination of two irises helps reduce the FRR and also have longer keys such as 35-bit keys at 4.93% FRR. In spite of the improvement, the FRR is still much high and hence we did not carry out these tests on the ICE database.

TABLE III

Key regeneration system results on the CBS-Bio dataset when two iris codes are combined using only feature level fusion; FRR values are in %; length of key $\mathbf{K}$ is in bits; FAR is always zero for all these tests.

t_s	Left iris		Right iris		Both irises	
	FRR	**length(K)**	**FRR**	**length(K)**	**FRR**	**length(K)**
16	9.80	30	14.13	30	4.93	35
17	8.60	18	13.10	18	4.57	21
18	**7.37**	**6**	**12.03**	**6**	**4.27**	**7**

When the proposed feature level fusion approach along with weighted error correction is used, a significant improvement is achieved that can be seen in Table IV. We added 760 zeros to the right iris code so that nearly 39% Hadamard error correction is achieved for it whereas no zeros are added to left iris code. The Hadamard code operates on 64-bit blocks and thus the Hadamard error correction capacity for the left iris is 23%. It also allows us to obtain much longer keys with low error rates, e.g., we can have 175-bit keys at 0.38% False Acceptance Rate (FAR) and 1.64% FRR for ICE database.

Finally, the results for the key regeneration scheme with password are presented in Table IV. These results are better than any previously published results in literature, e.g., we can generate 147-bit keys at 0.18% FRR and 0% FAR for ICE database. In our experiments, the number of blocks at the output of the RS encoder is 49. Hence we use a 49-bit shuffling key to shuffle those blocks. The shuffling key is protected by a password of eight characters. Note that, there is not much decrease in FRR due to the use of password. The main improvement is in the FAR; the FAR becomes zero which means that the systems becomes more secure.

VI. Security Analysis

Since the proposed system is for generating cryptographic keys, it is worthwhile to analyze the security of the system in

TABLE IV

KEY REGENERATION SYSTEM RESULTS WHEN TWO IRIS CODES ARE COMBINED USING FEATURE LEVEL FUSION AND WEIGHTED ERROR CORRECTION; FAR AND FRR VALUES ARE IN %.

t_s	Key length (in bits)	Without password				With password			
		CBS-Bio		NIST-ICE		CBS-Bio		NIST-ICE	
		FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR
6	259	0	8.37	0	13.28	0	8.50	0	13.74
9	217	0	5.37	0	5.19	0	5.63	0	5.46
10	203	0	4.50	0.016	3.37	0	4.60	0	3.28
11	189	0	4.10	0.06	2.09	0	4.10	0	2.09
12	**175**	**0**	**3.63**	**0.38**	**1.64**	**0**	**3.67**	**0**	**1.36**
13	161	0.10	3.40	1.49	0.55	0	3.50	0	1.00
14	**147**	**0.70**	**3.30**	**2.98**	**0.27**	**0**	**3.30**	**0**	**0.18**
15	133	1.87	3.13	10.46	0.18	0	3.03	0	0.18
16	119	6.40	2.80	15.86	0.09	0	2.37	0	0.09
21	49	84.47	0.23	91.37	0	0	0.30	0	0

terms of key entropy. Though the key is generated randomly at enrollment time, a lot of redundancy is added by the ECC and hence its entropy is bound to decrease. Since the key is regenerated using the iris codes and password, we use the same approach as used by Hao et al. [15] to estimate the entropy. The iris codes used in our experiments are 1,188 bits long. Following the procedure given in [4], we estimate the degrees of freedom in the iris code to be 561. Collectively, in two iris codes, we have 1,122 degrees of freedom. In the weighted error correction configuration, the total amount of error correction is $\approx 30\%$. If, $f = 1,122$ and $g = 0.3 \times f \approx 336$, then following the procedure in Hao et al. [15], an impostor needs approximately,

$$BF \approx \frac{2^f}{\binom{f}{g}} \approx \frac{2^{1122}}{\binom{1122}{336}} \approx 2^{140}, \tag{1}$$

brute force calculations to successfully get the cryptographic key. Thus the entropy of the key is 140 bits, which is much higher than any other reported system.

As explained in Section III-C, we add a password protected shuffling key to the system to enhance the security. The shuffling key used in our experiments is 49 bits. This key is randomly generated and is protected by a password. We propose to use a randomly generated 8-character password which can have 52-bit entropy [25]. The shuffling process is embedded into the error correction process and hence the individual entropies add up together resulting in a total key entropy of $140 + 49 = 189$ bits. Thus the minimum entropy of the key is,

$$\text{Entropy} = min(Length(\mathbf{K}), 189)\text{bits}. \tag{2}$$

Another security perspective is the possibility that the password gets stolen. In this situation, the system still has two iris codes which provide the security. The performance in this situation degrades but it is equivalent to that of the system without password. This is a distinct advantage of the proposed system over some of the systems in literature such as the Lumini and Nanni system [8]. The system in [8] improves the biometric verification performance when a hash key is used. But they report that, when such hash key is stolen, the performance generally degrades than that of the baseline biometric system.

In Table V, we present the comparison of the proposed system with the multi-biometric based cryptographic key regeneration system of Nandakumar and Jain [3]. Though the key length reported in [3] is higher than in the proposed system, the entropy of that key is only 49 bits as compared to 147 bits in our system. The FRR value is also nearly ten times higher in their system.

The proposed system can also be compared with the uni-biometric systems reported in Table I. It should be noted that, the performance of Hao et al. [15] system is on a proprietary database having small intra-user variations. Bringer et al. [17] and Kanade et al. [1] report very high FRR when the system in [15] is tested on a comparatively noisy ICE database. Keeping these comments based on re-implementation apart, many of the iris systems report the threshold at EER to be nearly 33% in ICE [23]. Thus it is required for a key generation system using ECC to correct 33% errors but the Hao et al. [15] system can cope up with only 27% errors (maximum).

VII. CONCLUSIONS AND PERSPECTIVES

In this paper, we propose a multi-biometric based cryptographic key regeneration system. Since left and right irises of a person are uncorrelated, we use them as two different biometric sources and combine the information to get a multi-biometric feature vector. We propose a novel method of feature level fusion combined with weighted error correction which significantly improves the verification performance of the system. We also use a shuffling key which randomizes the ECC data which helps make the system more secure. We succeed to generate 147-bit keys with 0% FAR and 0.18% FRR on the ICE database. The entropy of the key is 147 bits. The shuffling key is protected by a password which provides strong revocability. In an event that the password is stolen, the system is still as secure as the one without using password.

The proposed scheme can be adopted to other biometric modalities. The feature level fusion combined with weighted

TABLE V

COMPARISON OF THE PROPOSED SYSTEM WITH THE MULTI-BIOMETRIC BASED CRYPTOGRAPHIC KEY (RE)GENERATION SYSTEM [3]; ECC – ERROR CORRECTING CODES; RSH – REED-SOLOMON AND HADAMARD CODES; BCH+ – BCH CODES FOLLOWED BY POLYNOMIAL RECONSTRUCTION; LENGTH AND ENTROPY OF $\mathbf{K}$ ARE IN BITS.

Reference	ECC	Length(K)	Entropy(K)	Password used	FAR (%)	FRR (%)	Database
Nandakumar [3]	BCH+	208	49	No	0.02	1.80	CasiaV1 Iris + MSU-DBI fingerprint
Proposed	RSH	147	147	Yes	0	0.18	ICE (left eye + right eye)

error correction method proposed in this paper allows the fusion of different biometric modalities having variation in performances (e.g., face+iris). The difficulty is to find appropriate ECC for that modality and the binarization of the feature vector.

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 (BSYM2008)*, September 2008.

[2] A. A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics*, ser. International Series on Biometrics. Springer, 2006.

[3] K. Nandakumar and A. K. Jain, "Multibiometric template security using fuzzy vault," in *IEEE Second International Conference on Biometrics: Theory, Applications and Systems*, 2008.

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

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

[10] S. Kanade, D. Petrovska-Delacrétaz, and B. Dorizzi, "Cancelable Iris Biometrics and Using Error Correcting Codes to Reduce Variability in Biometric Data," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, June 2009.

[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] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. V. Kumar, "Biometric encryption," in *ICSA guide to Cryptography*. McGraw-Hill, 1999.

[14] 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.

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

[16] 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.

[17] 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.

[18] S. Kanade, D. Camara, D. Petrovska-Delacrétaz, and B. Dorizzi, "Application of biometrics to obtain high entropy cryptographic keys," in *Proceedings of World Academy on Science, Engineering, and Technology*, Hong Kong, March 2009.

[19] 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.

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

[21] "Advanced encryption standard (AES)," Federal Information Processing Standards Publication 197, National Institute of Standards and Technology, Standard, November 2001.

[22] E. Krichen, B. Dorizzi, Z. Sun, S. Garcia-Salicetti, and T. Tan, "Iris Recognition," in *Guide to Biometric Reference Systems and Performance Evaluation*, D. Petrovska-Delacrétaz, G. Chollet, and B. Dorizzi, Eds. Springer-Verlag, 2009, pp. 25–50.

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

[24] S. Kanade, D. Petrovska-Delacrétaz, and B. Dorizzi, "Iris Comparison Protocols," http://share.int-evry.fr/svnview-eph/ref_syst/Iris_Osiris/lists/.

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