Cancelable biometrics for better security and privacy in biometric systems

Sanjay Ganesh Kanade, Dijana Petrovska-Delacrétaz, Bernadette Dorizzi

Cancelable Biometrics for Better Security and Privacy in Biometric Systems

Sanjay Ganesh Kanade*, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi

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

Abstract. We present a simple scheme with three main features: (1) it induces revocability in biometrics based user authentication systems, (2) protects the biometric information, and (3) improves the verification performance. The user's biometric feature vector is shuffled with a user specific shuffling key to transform into a revocable template. Comparison between different templates is carried out in the transformed domain. If the template is compromised, it can be replaced with another template obtained by changing the shuffling key. This scheme makes cross-matching between databases impossible by issuing different templates for different applications. The performance evaluation of the system is carried out on two modalities: iris and face using publicly available databases. This scheme significantly improves the verification performance of the underlying biometric system, e.g., it reduces the Equal Error Rate (EER) from 1.67% to 0.23% on the NIST-ICE iris database. The EER on the NIST-FRGCv2 face database reduces from 8.10% to zero.

Keywords: Revocability, Cancelable biometrics, Iris, Face, Security and privacy

1 Introduction

Biometrics is defined as automatic recognition of persons based on their physical or behavioral characteristics (such as fingerprint, iris, face, etc.). Since the biometric characteristics are implicitly associated with a user, they provide a strong proof of his identity. In the existing biometric systems that we denote as 'classical biometric systems' (shown in Fig. 1), the information needed for further comparisons, denoted as biometric reference or template, is stored in a database. However, because of the permanent association of biometric characteristics with the user, these templates remains substantially similar across databases if the

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

modality and the biometric algorithm are the same, e.g., for minutiae based fingerprint systems, minutiae sets extracted from the same fingerprint in different systems are similar. If such template is compromised, it is not possible to replace it with a new one because the biometric characteristics (from which this information is extracted) are permanently associated with their owners. In other words, it is not possible to revoke or cancel a template. This phenomenon is called as lack of revocability.

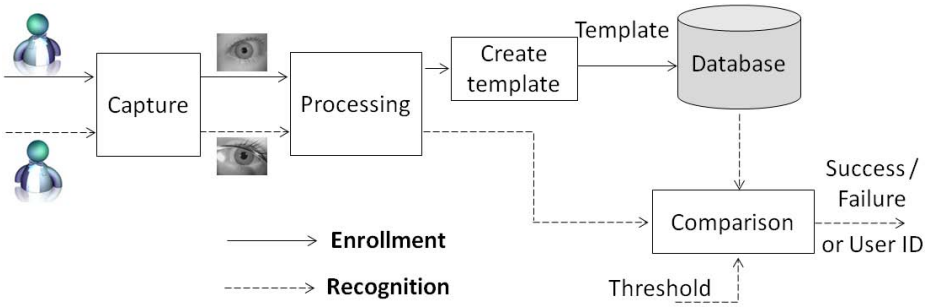


Fig. 1. Basic idea of a biometric based person recognition system. In verification mode, the result of the comparison is either success or failure. In identification mode, the result of comparison is the User ID.

The permanent association of biometric data with the user leads to another problem. Since the templates in all the systems based on the same biometric characteristic and using same biometric algorithms are similar, a compromised template from one biometric database can be used to access information from another system. This can be referred to as cross-matching between databases and is a threat to privacy. Moreover, in some cases, the stored information can be used to create a dummy representation of the biometric trait which can be used to access the system [2, 6, 25, 7]. For example, a dummy finger can be constructed from a fingerprint image.

Because of these reasons, the property of cancelability or revocability is becoming a necessity. In order to induce revocability into biometric systems, cryptographic techniques are a good candidate. Many systems that induce these characteristics are proposed in literature. A summary of such systems is presented in Section 2. In this paper, we present a simple shuffling scheme to create cancelable templates from biometric data. This system was first proposed in our earlier paper on crypto-biometric key regeneration [12]. This scheme involves two factors: biometrics and a shuffling key. Because of this additional parameter, the proposed scheme significantly improves the verification performance of the baseline biometric system.

In general, an authentication system should possess following characteristics:

1. **Identity verification and non-repudiation:** The system should be able to confirm the identity of the user with high degree of confidence. It also indicates that the system should resist repudiation attempts carried out by the users. Involvement of biometrics helps achieve this property.
2. **Revocability:** If the stored user template is compromised, it should be possible to cancel that template and reissue a new one. Additionally, the newly issued template should not match with the previously compromised template. Thus revocability does not mean just to cancel the old template and issue a new one; it also means that, the authentication rights of the old authenticator are revoked. The system should be able to reject a person if he provides the authenticator linked with the old template. Note that, biometrics alone cannot provide this property because biometric characteristics cannot be changed while systems using passwords and tokens have excellent revocability.
3. **Template diversity:** It should be possible to issue different templates for different applications related to the same user. These templates should not match with each other and should make cross-matching impossible. Password and token based systems are good at that, though practically, password diversity can be argued. Biometrics, by itself, cannot have template diversity.
4. **Privacy protection:** These systems should protect the privacy of biometric data, privacy of information protected by the system, and user identity privacy.

The system presented in this paper satisfies all these desired characteristics. In this scheme, the biometric features are combined with a user specific random key to obtain a revocable template. The scheme improves the biometric system performance in an ideal case when the user specific keys are kept secrete. If the keys for all the users are stolen, the system is as secure as the underlying biometric system.

The reminder of the paper is organized as follows: recent developments in the field of revocable biometrics based authentication are given in section 2. In section 3, the algorithm to obtain revocable iris template is described. The experimental setup for the performance evaluation, including baseline biometric systems, databases and experimental protocols are explained in section 4 and results are reported in section 5 along with experimental security analysis. Finally, the conclusions and perspectives are given in section 6.

2 Cancelable Biometrics: Related Work

There are many solutions found in literature which aim at inducing cancelability/revocability in biometric systems. These systems apply some sort of (one-way) transformation on the biometric data. Some of these transformation methods include, Cartesian, polar and functional transformations of Ratha et al. [23, 24], BioHashing of Jin et al. [10], cancelable filters of Savvides et al. [26], improved BioHashing of Lumini and Nanni [17], Revocable biotokens of Boult et al. [4], and transformations proposed by Maiorana et al. [18].

The drawback of many of these cancelable biometric systems is that their performance degrades compared to the baseline biometric system. In some cases, the performance improves, however, the improvement is because of the additional parameter (such as password, PIN, key, token, etc.). Such systems should be analyzed for their verification performance in the stolen key (also called as stolen token) scenario. Such analysis is not reported in most of these works. For BioHashing based systems, the performance in the stolen key scenario degrades compared to the baseline biometric system.

Biometric-based cryptographic key (re)generation systems [11, 27, 9, 28, 5, 19, 12, 14, 13] can provide cancelable templates based on biometrics, but their main aim is to obtain a cryptographic key. Hence we will not discuss these schemes here.

Our previous work on cryptographic key regeneration [12] incorporates the shuffling scheme, presented in this paper, to have better separation between genuine and impostor users. But in that work, we do not analysis the scheme from a revocable biometrics point of view which we present in this paper. The biometric data shuffling scheme is described in the following section.

3 A Biometric Data Shuffling Scheme to Create Cancelable Biometric Templates

The shuffling scheme described in this section can work with any biometric modality provided the biometric features are represented as an ordered set. In this scheme, a randomly generated shuffling key is used to shuffle the biometric data. The shuffled biometric data represents the cancelable template. It is not feasible to recover the original biometric data from this cancelable template. This scheme can be considered analogous to classical symmetric encryption technique because, as in encryption, a key is used to protect the biometric data. But contrary to classical encryption, the user discrimination properties of biometric data are retained by the transformed data, and hence, comparison between two such transformed biometric data can be carried out in the transformed domain. The shuffling technique is explained in details in the next subsection.

3.1 The Shuffling Technique

The shuffling scheme that we introduce requires a binary shuffling key $\mathbf{K}_{sh}$ of length L_{sh}. Since this key is a long bit-string, it is stored on a secure token or it can be obtained using a password. The biometric feature vector is divided into L_{sh} blocks each of which has the same length. To start the shuffling, these L_{sh} blocks of the feature vector are aligned with the L_{sh} bits of the shuffling key $\mathbf{K}_{sh}$. In the next step, two distinct parts containing biometric features are created: the first part comprises all the blocks corresponding to the positions where the shuffling key bit value is one. All the remaining blocks are taken into the second part. These two parts are concatenated to form the shuffled biometric feature

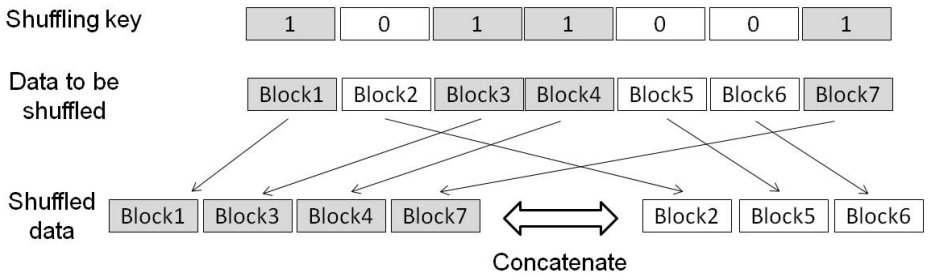


Fig. 2. The shuffling scheme.

vector which is treated as a revocable template. Figure 2 shows a schematic diagram of this shuffling scheme.

The original and shuffled feature vectors have one-to-one correspondence. A block from the original vector is placed at a different position in the shuffled vector. Thus, only the alignment of the feature blocks is changed by the scheme with no change in the actual values of the features. The length of the biometric feature vector does not change because of the shuffling. Hence, the matching algorithms used for calculating the similarity (or dis-similarity) score between two biometric feature vectors are still applicable for the shuffled data.

Note that the effectiveness of this scheme is because it changes the alignment of the feature vectors. If the feature vectors do not require any particular order (e.g., fingerprint minutiae sets), this system is ineffective. This system can work only if the biometric data is in form of an ordered set.

3.2 Advantages of Using the Proposed Shuffling Scheme

The proposed shuffling scheme has the following advantages:

1. **Revocability:** The shuffled feature vector, which is treated as a cancelable template, is a result of combination of an intrinsic identifier (i.e., a biometric characteristic) and an assigned identifier (the shuffling key). Therefore, in case of compromise, it can be canceled and a new template can be generated by changing the shuffling key $\mathbf{K}_{sh}$ (the assigned credential).
2. **Performance improvement:** Another advantage of using the shuffling scheme is that it improves the verification performance. The shuffling process changes the alignment of the feature vector blocks according to the shuffling key. When two biometric feature vectors are shuffled using the same shuffling key, the absolute positions of the feature vector blocks change but this change occurs in the same way for both of the biometric feature vectors. Hence, the Hamming distance (in case of binary vectors) between them does not change. On the other hand, if they are shuffled using two different keys, the result is randomization of the feature vectors and the Hamming distance

increases. In fact, the shuffling process acts like a randomizer and moves the average Hamming distance for such cases close to 0.5.
A unique shuffling key is assigned to each subject during enrollment and he has to provide that same key during every subsequent verification. This means, in ideal case, that the genuine users always provide the correct shuffling key and hence, the Hamming distance for genuine comparisons remain unchanged. On the contrary, in case of random impostor attempts where an impostor tries to get verified with his own credentials, he provides his biometric data along with his shuffling key (or a random shuffling key) to match against other users. The feature vectors for such impostor comparisons are shuffled with two different shuffling keys and the result is that the Hamming distances increase. This effect can be seen in Fig. 3. The separation between the genuine and impostor Hamming distance distributions shows the ability of the system to distinguish genuine users from impostors. As can be seen from Fig. 3, shuffling increases the separation between the two distributions. In this way, the shuffling scheme improves the verification performance of the system.

3. **Template diversity:** With the help of the shuffling technique, different templates can be issued for different applications by using different shuffling keys with the same biometric data. This particularly helps to avoid cross-database matching. In order to make the template-diversity effective, it is suggested that the shuffling key should be generated randomly and protected by a password.
4. **Protection against stolen biometric data:** If a feature vector is shuffled using two different shuffling keys, the resulting shuffled vectors appear to be originating from two different subjects. They can be seen as comparing two random sequences and hence they do not match. Therefore, if a stolen biometric data of a legitimate person is used by an impostor to get verified, the system can still resist such attack due to the use of shuffling key.
5. **Biometric data protection:** It is not computationally feasible to recover the original biometric feature vector from the shuffled data without the proper shuffling key. However, as in classical encryption, the security depends on the secrecy of the shuffling key.

These effects can be better understood from the experimental results and analysis presented in the next section.

4 Experimental Setup

The cancelable biometric system is based upon an underlying baseline biometric system. Therefore, for fair comparison, first the biometric verification performance of the baseline biometric system is reported followed by the performance of the proposed cancelable system.

The proposed cancelable biometric system is evaluated on two biometric modalities: iris and face. For iris, the Open Source Iris Recognition System

(OSIRIS) described in [22] and available online at [1] is used to extract binary iris code features from the iris images. The CBS database [22] (BiosecureV1 OKI device subset) is used for development in order to find out the optimum length of the shuffling key. The system is then evaluated on the NIST-ICE database [21]. As described in the ICE evaluation, we carried out two experiments: ICE-Exp1 involving comparisons between right-eye images whereas ICE-Exp2 involving left-eye images. In total, 12,214 genuine and 1,002,386 impostor comparisons are carried out in ICE-Exp1, whereas in ICE-exp2, 14,653 genuine, and 1,151,975 impostor comparisons are performed.

For face, a Gabor filter based approach is applied to extract features from the face image [16]. The face image is first geometrically normalized using the CSU Face Recognition System [3], and then processed using log-Gabor filters having four scales and eight orientations using the MATLAB source code available at [15]. Magnitude of the filtered output is calculated, downsampled, and concatenated to form a 3,200-element feature vector. The values in this vector are then binarized to obtain a 3,200-bit string called face code. The binarization process used is fairly simple. The median of the values in a feature vector is taken as a threshold. The elements having higher value than the threshold are made one while the remaining are made zeros.

The development and evaluation data sets for face experiments are from a subset of the NIST-FRGCv2 database [20]. This subset is composed of 250 subjects each of which has 12 images. Data from the first 125 subjects are used for development and the remaining 125 subjects are used for evaluation. For each subject, there are eight images captured in controlled lighting conditions while four images in uncontrolled conditions.

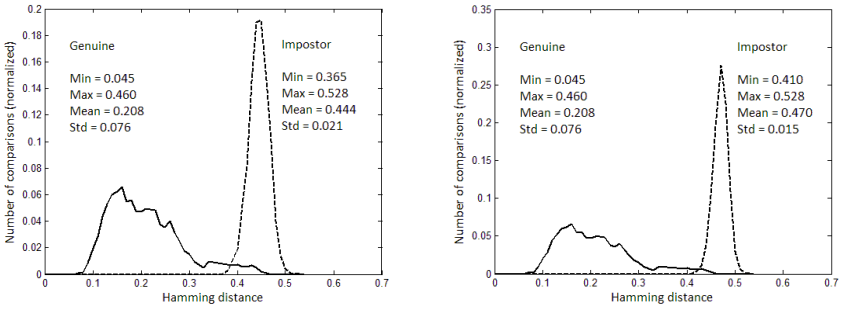
Two separate experiments are carried out during development as well as evaluation: FRGC-Exp1* – where the enrollment as well as test images are captured under controlled conditions, and FRGC-Exp4* – in which the enrollment images are from controlled conditions while the test images are from uncontrolled conditions. For the FRGC-Exp1*, 3,500 genuine and 496,000 impostor comparisons are carried out while for FRGC-exp4*, 4,000 genuine and 496,000 impostor comparisons are performed.

5 Experimental Results and Security Analysis

5.1 Results and Security Analysis on Iris Modality

Results on Iris Modality The genuine and impostor Hamming distance distributions for the CBS-BiosecureV1 data set before and after shuffling are shown in Fig. 3. As described in Section 3.2, the shuffling process increases the impostor Hamming distances while the genuine Hamming distances remain unchanged. This can be seen from the Fig. 3. In this figure, the mean of the impostor Hamming distance distribution of the baseline system shifts from 0.44 to 0.47 when the shuffling scheme is applied. Note that, the genuine Hamming distance remains unchanged. This reduces the overlap between the genuine and impostor

distribution curves which improves the user discrimination capacity of the system thereby increasing the verification accuracy.



(a) Baseline iris biometric system

(b) Proposed cancelable biometric system (baseline iris system with shuffling)

Fig. 3. Normalized Hamming distance distributions for genuine and impostor comparisons on the CBS-BioSecureV1 [22] development data set.

The better separation between genuine and impostor Hamming distance distribution curves improves the verification performance of the system. The verification performance in terms of Equal Error Rate (EER) on the development database (CBS database) is reported in Table 1.

Table 1. Verification results of the baseline biometric system (which is based on the OSIRISv1) and the proposed cancelable system on iris modality; in terms of EER in %. Values in bracket indicate the error margins for 90% confidence intervals.

Experiment	**CBS-BiosecureV1**	**ICE-Exp1**	**ICE-Exp2**
Baseline	2.63[±0.34]	1.71[±0.11]	1.80[±0.10]
Proposed cancelable	0.93[±0.20]	0.23[±0.04]	0.37[±0.05]
OSIRISv1 [22]	2.83[±0.35]	1.52[±0.12]	1.71[±0.12]
Stolen biometric scenario	1.50[±0.26]	0.27[±0.08]	0.44[±0.09]
Stolen key scenario	2.63[±0.34]	1.71[±0.11]	1.80[±0.10]

The system is then evaluated on the evaluation (NIST-ICE) database. These results are also reported in Table 1. As noted before, we carried out separate experiments according to the common protocol for ICE evaluation for right (ICE-Exp1) and left (ICE-Exp2) iris comparisons. A clear improvement in performance can be seen by comparing the EER of the baseline system with the proposed cancelable system. For example, in case of ICE-Exp1, the EER for the

baseline system is 1.71% which reduces to 0.23% when the cancelable scheme is applied. Similarly, for the ICE-Exp2, the EER reduces from 1.80% to 0.37% because of the shuffling scheme. For the sake of comparison, the EER values reported in the documentation of the OSIRISv1 on these two data sets are also reported in this table.[1]

Security Analysis on Iris Modality The cancelable biometric system proposed in this chapter has two factors: biometrics and a shuffling key. In order to test the robustness of the system, we carried out the performance evaluation in two extreme hypothetical impostor scenarios: (i) stolen biometric and (ii) stolen key.

In the stolen biometric scenario, we consider a hypothetical extreme situation when the biometric information for all the users is stolen. Here, an impostor will try to provide the stolen biometric data along with a wrong shuffling key. In this situation, the EER increases compared to that of the cancelable system with both factors secret. But, it is still less than the EER of the baseline biometric system. For example, as shown in Table 1, for the ICE-Exp1, the EER of the cancelable system is 0.23% when both the factors are secret. Considering that the iris image is stolen for all the users, the EER increases to 0.27% which is still less than the EER for baseline system (1.71%). Thus, use of the shuffling scheme prevents the impostors from being successfully verified using stolen biometric data.

In the stolen key scenario, we consider another extreme situation when the shuffling keys of all the users are compromised. As in the stolen biometric scenario, the EER increases compared to that of the cancelable system having both parameters secret. But, the EER is equal to the EER of the baseline biometric system meaning that the system in this stolen key scenario is still as good as the baseline biometric system (see Table 1). In fact, the proposed shuffling scheme is such that, it increases the Hamming distance between two iris codes if and only if they are shuffled with different keys. If the same key is used to shuffle two codes, the Hamming distance remains intact. Thus in the stolen key scenario, the Hamming distance distribution is exactly the same as that for the baseline system, and hence, yields the same result as that of the baseline biometric system. This is a distinct advantage of our system over other cancelable systems found in literature. For most of the cancelable systems found in literature, the performance degrades if the keys (or the cancelable parameters used) are compromised. Only the Farooq et al. [8] system is shown to have the performance equal to the baseline biometric system in the stolen key scenario.

Detection Error Tradeoff (DET) curves for the proposed cancelable system along with the security threats are shown in Fig. 4 for the iris modality. These curves show the performance on the evaluation database – the NIST-ICE database – for the ICE-Exp1 experiment. The DET curves for the baseline system and that for the stolen key scenario overlap with each other which indicates

[1] The baseline iris system is based on OSIRISv1; the difference is that the matching module is re-implemented to cope with the iris rotations.

that the performance of the system in stolen key scenario is same as the baseline system.

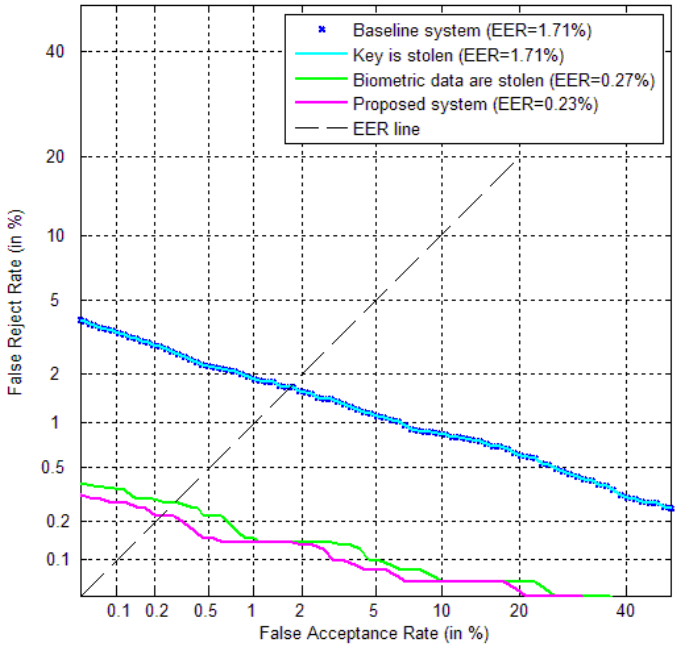


Fig. 4. DET curves for the proposed system performance along with the possible security threats for iris modality on the NIST-ICE database(evaluation data set) [21]; ICE-Exp1.

The stolen biometric scenario also proves the template diversity property. It shows that, if the biometric feature vector is shuffled with two different keys, the two shuffled codes appear to be random and do not match. In order to prove our point, we carried out an additional test. We shuffled one iris code with 100,001 randomly generated shuffling keys. The first shuffled iris code is compared with the remaining 100,000 shuffled iris codes. The distribution of Hamming distances obtained from these comparisons is shown in Fig. 5. This distribution is also close to the random impostor distribution which validates our claim of template diversity.

In case of compromise, the cancelable template can be revoked. In order to revoke the template, the user is asked to re-enroll into the system. The fresh biometric data is shuffled with a newly generated random shuffling key. Since this shuffling key is different than the one used earlier in enrollment, the old template and the newly issued template cannot match with each other. If an attacker obtains an iris code of the user from previously compromised template

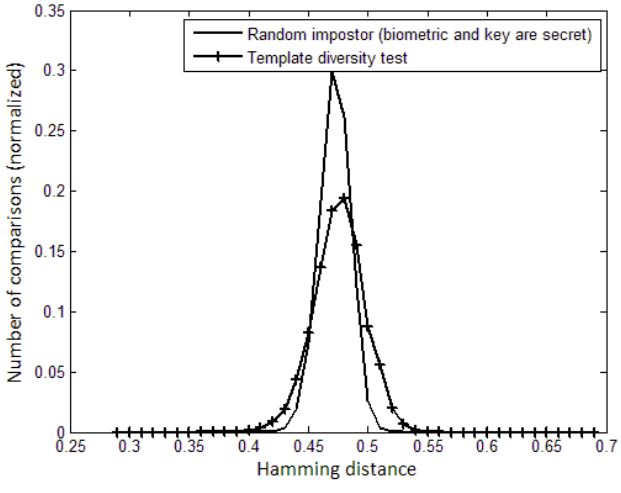


Fig. 5. Impostor Hamming distance distributions for the proposed system along with the Hamming distance distributions for the template diversity test on iris modality on the NIST-ICE database [21] (ICE-Exp1).

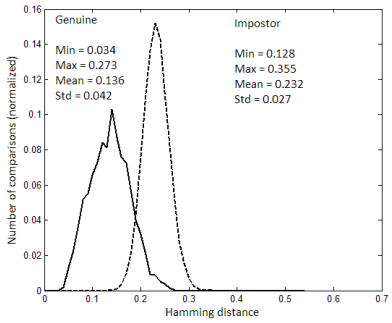
or from another biometric system, that iris code cannot be used by the impostor to get verified because the new shuffling key resists such attacks.

5.2 Results and Security Analysis on Face Modality

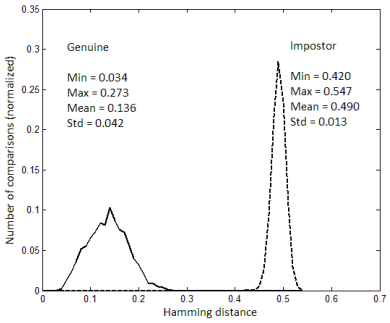
Results on Face Modality The Hamming distance distribution curves for genuine and impostor comparisons before and after shuffling on the development data sets are shown in Fig. 6. The curves for both, FRGC-Exp1* and FRGC-Exp4*, experiments are shown.

As was observed in case of iris, the impostor Hamming distances increase because of the shuffling process. Note that the genuine Hamming distances remain unchanged. A clear separation between genuine and impostor Hamming distance distributions is observed for both the experiments. This complete separation results in zero EER. The results of the proposed cancelable system for the FRGC-Exp1* and FRGC-Exp4* on the development data sets are reported in Table 2.

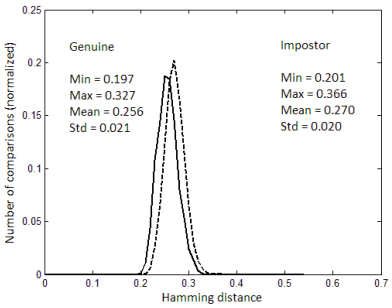
Note that, the improvement in performance is because of the increase in impostor Hamming distances. The shuffling scheme works as a randomization process which shifts the mean of the impostor Hamming distance distribution close to 0.5. Therefore, if the mean of the original (un-shuffled) impostor Hamming distance distribution is small, the improvement in performance will be more prominent. This can be visualized by comparing the improvements for iris and face modalities. For example, on the development data set CBS-BiosecureV1 for



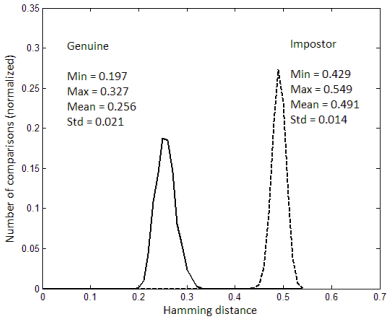
(a) Baseline face biometric system (FRGC-Exp1*)



(b) Baseline face system with shuffling (FRGC-Exp1*)



(c) Baseline face biometric system (FRGC-Exp4*)



(d) Baseline face system with shuffling (FRGC-Exp4*)

Fig. 6. Normalized Hamming distance distributions for genuine and impostor comparisons on the NIST-FRGCv2 development data set for FRGC-Exp1* and FRGC-Exp4*.

Table 2. Verification results of the proposed cancelable system on face modality along with the security analysis in terms of EER in %. Values in bracket indicate the error margins for 90% confidence intervals.

Test	**Development set**		**Evaluation set**	
	FRGC-Exp1*	**FRGC-Exp4***	**FRGC-Exp1***	**FRGC-Exp4***
Baseline	8.10[±0.41]	35.90[±0.68]	7.65[±0.40]	35.00[±0.68]
Proposed cancelable	0	0	0	0
Stolen biometric	0	0	0	0
Stolen key	8.10[±0.41]	35.90[±0.68]	7.65[±0.40]	35.00[±0.68]

iris, as shown in Fig. 3, the average impostor Hamming distance for iris is 0.44, which after shuffling, increases to 0.47. Similarly, for face, on the development

data set Exp1 (Fig. 6), the average impostor Hamming distance is 0.23, which moves to 0.49 after shuffling. Thus, the increase in the separation between genuine and impostor Hamming distance curves is more in case of face than for iris. Therefore, the improvement in performance is higher in case of face than in case of iris.

The proposed cancelable system is then evaluated on the evaluation data sets. As it is seen for the experiments on development sets, a clear separation is obtained on the evaluation sets also. The outcome of this separation is zero EER as reported in Table 2.

Security Analysis on Face Modality The experimental security analysis of the proposed system carried out for the iris modality is also performed for the face modality. The two scenarios: (i) stolen biometric scenario and (ii) stolen key scenario, are followed. During these tests, it is observed that the proposed cancelable system behaves in a similar way as it did on iris. The performance in case of the stolen biometric case remains unchanged. In the stolen key scenario, the performance is exactly the same as that of the baseline biometric system. The results for these tests in terms of EER are reported in Table 2.

6 Conclusions and Perspectives

Classical biometric systems lack the important properties of revocability and template diversity because the biometric traits are permanently associated with the user. Cancelable biometric systems overcome these drawbacks of classical biometric systems. The shuffling scheme proposed in this paper employs a randomly generated shuffling key to randomize the biometric feature codes. The shuffled feature vectors act as cancelable templates. The system can issue different templates for different applications using the same biometric which preserves privacy. If the stored template is compromised, it can be canceled and a new template can be issued by changing the shuffling key. Such use of shuffling key prevents an attacker from getting verified by providing the compromised template or stolen biometric data. One distinct advantage of this system is that the performance of the baseline system increases by more than 80% due to shuffling. And even if one of the two secret factors, the biometric data and the shuffling key, is compromised, the EER of the system in such scenario still remains less than or equal to that of the baseline biometric system.

The drawback of this shuffling scheme is that it is not noninvertible. Practically, it works as a classical symmetric encryption where data can be encrypted by a key and the encrypted data can be decrypted by providing the same key. If an attacker succeeds to obtain the shuffling key, he can de-shuffle the cancelable template to obtain the reference biometric data. However, when such compromise is detected, the system can revoke the old template and issue a new one and the earlier attack becomes irrelevant.

A limitation of this shuffling scheme in its current form is that it can only be applied to biometric systems when the templates are in form of an ordered set. It cannot be applied to unordered sets such as a set of fingerprint minutiae.

The proposed shuffling scheme is very effective and therefore can be used as a means to induce revocability in other key regeneration systems.

References

1. Online: http://svnext.it-sudparis.eu/svnview2-eph/ref_syst/
2. Adler, A.: Sample Images Can be Independently Restored from Face Recognition Templates. In: Canadian Conference on Electrical and Computer Engineering (CCECE) (2003)
3. Beveridge, J.R., Bolme, D., Raper, B.A., Teixeira, M.: The CSU Face Identification Evaluation System. Machine Vision and Applications 16(2), 128–138 (2005)
4. Boult, T.E., Scheirer, W.J., Woodworth, R.: Revocable fingerprint biotokens: Accuracy and security analysis. In: IEEE Conference on Computer Vision and Pattern Recognition. pp. 1–8 (June 2007)
5. Bringer, J., Chabanne, H., Cohen, G., Kindarji, B., Zémor, G.: Optimal Iris Fuzzy Sketches. In: IEEE Conference on Biometrics: Theory, Applications and Systems (2007)
6. Cappelli, R., Lumini, A., Maio, D., Maltoni, D.: Can Fingerprints be Reconstructed from ISO Templates? In: 9th International Conference on Control, Automation, Robotics and Vision (ICARCV) (2006)
7. Cappelli, R., Maio, D., Lumini, A., Maltoni, D.: Fingerprint Image Reconstruction from Standard Templates. IEEE Transactions on Pattern Analysis and Machine Intelligence 29(9), 1489–1503 (September 2007)
8. Farooq, F., Bolle, R.M., Jea, T.Y., Ratha, N.: Anonymous and Revocable Fingerprint Recognition. In: IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2007)
9. Hao, F., Anderson, R., Daugman, J.: Combining crypto with biometrics effectively. IEEE Transactions on Computers 55(9), 1081–1088 (2006)
10. Jin, A.T.B., Ngo, D., Ling, C., Goh, A.: Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognition 37(11), 2245–2255 (November 2004)
11. Juels, A., Wattenberg, M.: A fuzzy commitment scheme. In: Proceedings of the Sixth ACM Conference on Computer and communication Security (CCCS). pp. 28–36 (1999)
12. Kanade, S., Camara, D., Krichen, E., Petrovska-Delacrétaz, D., Dorizzi, B.: Three Factor Scheme for Biometric-Based Cryptographic Key Regeneration Using Iris. In: The 6th Biometrics Symposium (BSYM) (September 2008)
13. Kanade, S., Petrovska-Delacrétaz, D., Dorizzi, B.: Generating and Sharing Biometrics Based Session Keys for Secure Cryptographic Applications. In: IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS) (2010)
14. Kanade, S., Petrovska-Delacrétaz, D., Dorizzi, B.: Obtaining Cryptographic Keys Using Feature Level Fusion of Iris and Face Biometrics for Secure User Authentication. In: IEEE CVPR Workshop on Biometrics (June 2010)
15. Kovesi, P.: Matlab and octave functions for computer vision and image processing. Online: http://www.csse.uwa.edu.au/∼pk/Research/MatlabFns/ (2005)

16. Lades, M., Vorbrüuggen, J.C., Buhmann, J., Lange, J., v.d. Malsburg, C., Wüurtz, R.P., Konen, W.: Distortion Invariant Object Recognition in the Dynamic Link Architecture. IEEE Transactions on Computers 42(3), 300–311 (March 1993)
17. Lumini, A., Nanni, L.: An improved biohashing for human authentication. Pattern Recognition 40(3), 1057–1065 (March 2007)
18. Maiorana, E., Campisi, P., Ortega-Garcia, J., Neri, A.: Cancelable Biometrics for HMM-based Signature Recognition. In: IEEE Conference on Biometrics: Theory, Applications and Systems (BTAS) (2008)
19. Nandakumar, K., Jain, A.K., Pankanti, S.: Fingerprint-based fuzzy vault: Implementation and performance. IEEE Transactions of Information Forensics and Security 2(4), 744–757 (December 2007)
20. National Institute of Science and Technology (NIST): Face Recognition Grand Challenge (2005), http://www.frvt.org/FRGC/
21. National Institute of Science and Technology (NIST): Iris Challenge Evaluation (2005), http://iris.nist.gov/ice
22. Petrovska-Delacrétaz, D., Chollet, G., Dorizzi, B. (eds.): Guide to Biometric Reference Systems and Performance Evaluation. Springer-Verlag (2009)
23. Ratha, N.K., Connell, J.H., Bolle, R.M.: Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal 40(3), 614–634 (2001)
24. Ratha, N.K., Chikkerur, S., Connell, J.H., Bolle, R.M.: Generating cancelable fingerprint templates. IEEE Transactions on Pattern Analysis and Machine Intelligence 29(4), 561–572 (April 2007)
25. Ross, A., Shah, J., Jain, A.K.: From template to image: Reconstructing fingerprints from minutiae points. IEEE Transactions on Pattern Analysis and Machine Intelligence 29(4), 544–560 (April 2007)
26. Savvides, M., Kumar, B.V., Khosla, P.: Cancelable biometric filters for face recognition. In: Proceedings of the 17th International Conference on Pattern Recognition (ICPR04). vol. 3, pp. 922–925 (August 2004)
27. Soutar, C., Roberge, D., Stoianov, A., Gilroy, R., Kumar, B.V.: Biometric encryption. In: ICSA guide to Cryptography. McGraw-Hill (1999)
28. Uludag, U., Jain, A.: Securing fingerprint template: Fuzzy vault with helper data. In: Proc. of the 2006 Conference on Computer Vision and Pattern Recognition Workshop. pp. 163–170 (June 2006)