Chapter 15
Biometric Template Protection on Smartphones Using the Manifold-Structure Preserving Feature Representation

Kiran B. Raja, R. Raghavendra, Martin Stokkenes and Christoph Busch

Abstract Smartphone-based biometrics authentication has been increasingly used for many popular everyday applications such as e-banking and secure access control to personal services. The use of biometric data on smartphones introduces the need for capturing and storage of biometric data such as face images. Unlike the traditional passwords used for many services, biometric data once compromised cannot be replaced. Therefore, the biometric data not only should not be stored as a raw image but also needs to be protected such that the original image cannot be reconstructed even if the biometric data is available. The transforming of raw biometric data such as face image should not decrease the comparison performance limiting the use of biometric services. It can therefore be deduced that the feature representation and the template protection scheme should be robust to have reliable smartphone biometrics. This chapter presents two variants of a new approach of template protection by enforcing the structure preserving feature representation via manifolds, followed by the hashing on the manifold feature representation. The first variant is based on the Stochastic Neighbourhood Embedding and the second variant is based on the Laplacian Eigenmap. The cancelability feature for template protection using the proposed approach is induced through inherent hashing approach relying on manifold structure. We demonstrate the applicability of the proposed approach for smartphone biometrics using a moderately sized face biometric data set with 94 subjects captured in 15 different and independent sessions in a closed-set scenario. The presented approach indicates the applicability with a low Equal Error Rate,

This chapter is an extended version of our earlier work [1].

K. B. Raja (✉)
University of South-Eastern Norway, Kongsberg, Norway
e-mail: kiran.raja@usn.no; kiran.raja@ntnu.no

K. B. Raja · R. Raghavendra · M. Stokkenes · C. Busch
Norwegian Biometrics Laboratory, NTNU, Gjøvik, Norway
e-mail: raghavendra.ramachandra@ntnu.no

M. Stokkenes
e-mail: martin.stokkenes@ntnu.no

C. Busch
e-mail: christoph.busch@ntnu.no

A. Rattani et al. (eds.), *Selfie Biometrics*, Advances in Computer Vision and Pattern Recognition, https://doi.org/10.1007/978-3-030-26972-2_15

$EER = 0.65\%$ and a Genuine Match Rate, $GMR = 92.10\%$ at False Match Rate (FMR) of 0.01% for the first variant and the second variant provides $EER = 0.82\%$ and $GMR = 89.45\%$ at FMR of 0.01%. We compare the presented approach against the unprotected template performance and the popularly used Bloom filter template.

15.1 Introduction

The use of biometrics as an authentication mechanism for a number of secure access services such as banking, border control or civilian identity management has resulted in the popularity of new generation biometric sensors in devices such as smartphones. A number of real-world applications using a smartphone for biometric authentication have demonstrated the success for corporations and convenience to the customers [2, 3]. Complementing the success from industry, there have been a number of academic works investigating various aspects of biometrics usage on the smartphone. A set of works have investigated the use of face biometrics [4, 5], periocular biometrics [6] and a few on the iris biometrics [4, 7]. Another set of works have indicated the use of a multi-modal approach for smartphone authentication to compensate the performance losses due to non-standard biometric data on smartphone [4, 5, 7]. While the use of biometrics provides versatility and convenience, the challenge of storing the biometric data on smartphones is not addressed to a greater extent. Unlike the password mechanisms, the original biometric characteristics are limited (one face, two irises, ten fingerprints) and thus cannot be replaced for a user if compromised, especially if the smartphone with biometric data is stolen or lost making the data available to maligned parties. It is therefore essential to store the biometric data in a protected manner such that the original biometric image (e.g. face image) cannot be reconstructed under the loss of a smartphone, leading to a need for *irreversibility*.

As an impact of protecting the biometric data, one can expect performance degradation in biometric authentication as the protected templates are typically a result of a number of transformations which may suffer a loss of information [8, 9]. The loss in biometric performance implies either rejecting the genuine subject repeatedly (corresponding to false reject rate—FAR) or accepting the subjects falsely (corresponds to false accept rate—FAR). While it is desired to have FAR and FRR simultaneously at very low values in an ideal biometric system, it is at least expected to prevent no false accepts in practical application with minimal possible false rejects, especially in the use case such as personalized banking applications to prevent monetary loss [2, 10]. The template protection schemes for smartphones thus need to consider performance factor and maintain the performance as equivalent to performance without template protection, or better performance than no-template protection. Given that smartphone is a personal device, it can be generalized that the same device is used to access a number of different services by the user. A direct implication of using the same biometric data (e.g. face) also enforces the need to make the biometric template *unlinkable* between different services from both user and the service provider perspective.

Although the requirements of template protection have been laid out in ISO-24745 [11], there are not many works reported on the smartphone biometric template protection. In this chapter, we present a new approach of protecting biometric templates on the smartphone by exploiting the feature space and using it to the advantage of creating protected templates. Specifically, we employ structure preserving manifold representation to keep the relational features intact prior to creation of the template. The creation of a protected template itself is based on the hashing approach to derive robust representation. While hash-based representation aids in deriving secure transformed template, there are a number of practical considerations in obtaining a stable hash for biometric data.

- The biometric data (e.g. face or fingerprint) varies across different captures, different sessions, different capture conditions and different camera/smartphones. The change in the captured biometric data under these conditions influences the biometric features proportionally. As a direct implication, the hash template representation will be impacted, resulting in lower biometric performance.
- The biometric features can provide high performance when the structural and relational neighbourhood features are preserved. For instance, minutia vicinity plays an important role in obtaining higher performance as compared to unordered fingerprint features. In a similar manner, one can argue that the features from the face can be highly reliable when the structural neighbourhood is preserved in the feature space.
- Our assertion is that hashing-based template protection can provide better performance if the extracted features preserve the neighbourhood and relational structure information making them stable against variations introduced due to capture process.

In this chapter, we present a new approach such that the structure of biometric features is preserved through the use of manifold representation and further use this representation to derive robust protected template via hashing. The proposed approach being computationally simple and efficient is suitable to be deployed on the low-power computational devices such as smartphones. Further, the cancelability is introduced by adopting an entropy-based sampling method to choose the features to obtain the manifold embedding. Through the properties of manifolds, i.e. inductive manifold and Stochastic Neighbourhood Embedding (SNE), we ensure the *irreversibility, unlinkability and revocability*. Further, the proposed approach is validated through the set of experiments on a moderate-sized database of 94 subjects with real biometric data captured using the smartphone. The key contributions of this chapter are:

1. A new approach for creating protected biometric templates is proposed which is based on the neighbourhood relation/structure preserving manifold representation of textural features and hash representation.
2. An experimental performance evaluation is presented to illustrate the validation of proposed approach through the use of smartphone biometric database. The proposed approach is compared against biometric performance of unprotected

template and Bloom filter-based protected template. All of our experiments correspond to the closed-set protocol as the work is addressed towards verification scenarios.
3. This chapter also presents a systematic discussion of the proposed approach for template protection and subsequently discusses unlinkability analysis. In the end, this chapter presents the merits and the limitations of the proposed approach to provide possible direction for future works.

In the rest of this chapter, Sect. 15.2 presents the related works followed by the Sect. 15.3 that discusses proposed approach for biometric template protection. The Sect. 15.4 provides the details on the employed database and the corresponding protocols for experiments. The experiments and the obtained results are discussed in Sect. 15.5 along with the brief discussion on unlinkability analysis in the Sect. 15.5.2 to demonstrate the security level of the proposed template protection method. A set of concluding remarks and a list of potential future work is provided in Sect. 15.6.

15.2 Related Works

A number of approaches can be adopted to deal with this problem of biometric template protection[11] which are either cancellable biometrics or biometric cryptosystems [8, 9, 12–17]. In this work, we adopt the *template protection approach through cancellable biometrics*. The goal of cancellable biometrics is to derive a biometric template that is irreversibly distorted while keeping the uniqueness for all biometric purposes such as identification and verification. Cancellable biometrics can be achieved through methods from simple mathematical transformations to approaches based on hashing. In this work, we adopt hashing-based template protection scheme with a set of key constraints to fulfil the properties required for biometric template protection while still achieving high biometric accuracy in a protected domain biometric comparison [1].

15.3 Proposed Approach for Protected Biometric Templates

The proposed approach of protected template creation is presented in Fig. 15.1. As depicted in Fig. 15.1, the features from biometric data are first extracted using texture descriptors. Specifically, we utilize widely employed Binarized Statistical Image Features (BSIF). The set of extracted features are represented using the manifold representation such that the neighbourhood representation is preserved. Given the set of enrolment images for the subjects, the proposed approach derives the hash projection matrix from the manifold representation of features. Through the projection matrix, we create the protected templates for each subject in the enrolment set. In a similar

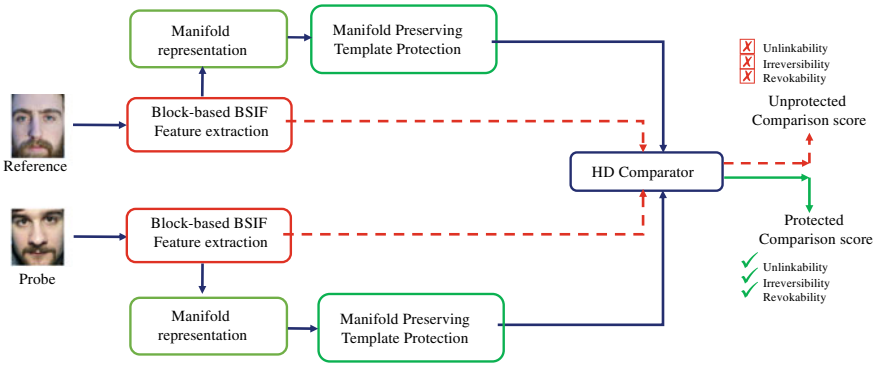


Fig. 15.1 Biometric system with proposed template protection is indicated by the path followed by solid lines which also satisfies the properties of biometric template protection

manner, when a verification attempt is made by the subject, the textural features are extracted using BSIF followed by the manifold representation. The features are then projected using learnt hash projection matrix to derive the protected template representation for probe data. The templates in the protected domain for both enrolment and the probe are compared using a simple Hamming distance measure to establish the biometric performance. The details of each component of the proposed approach are presented in the section below.

15.3.1 Feature Vector from Binarized Statistical Image Features

Given the preprocessed biometric image, we first extract the textural descriptors using the Binarized Statistical Image Features (BSIF)[18]. The descriptors are obtained by convolving the image with the set of filters in the BSIF filter bank which is learnt using the independent component analysis of natural image patches. The choice of BSIF filters to extract the descriptors is motivated by high biometric performance reported in many earlier works [5, 18, 19]. Further, to make the descriptors highly unique, we employ both block-based feature extraction and multi-scale representation through the use of a number of filters from BSIF. Specifically, we employ the filters that correspond to 3×3, 5×5, 7×7, 9×9, 11×11, 13×13, 15×15 and 17×17 pixels with eight orientations. The pixel-wise response from the convolution of different orientation filters within a chosen filter is combined to obtain a final response through the thresholding and binarization approach such that a value between $0 - -255$ is obtained for every pixel [18]. The extracted features are further represented using histogram representation in the subsequent steps. Further, the uniqueness of the features from biometric images is enhanced through block-based approach where prior to extracting the BSIF features, each image is divided into a

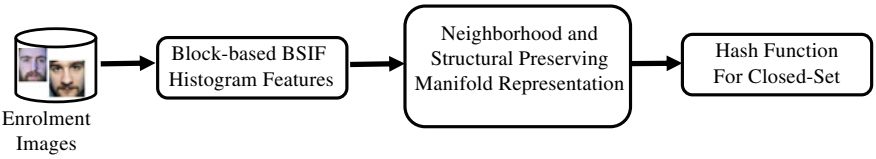


Fig. 15.2 Schematic representation of learning hash function for closed enrolment set

number of blocks and BSIF features extracted thereon. In this chapter, we employ 32 blocks of size 8×20 pixels from a resized biometric image of size 64×80 pixels. The set of all resulting histograms are concatenated to form a feature vector. The feature vector is further binarized using a simple zero thresholding [20, 21] to form a binary feature vector such that Hamming distance can be easily employed to derive biometric performance. Figure 15.2 presents the number of steps involved in extracting the final feature vector in this chapter.

15.3.2 Structure Preserving Biometric Feature Representation and Template Protection

As argued in the introduction, preserving the neighbourhood structure results in better biometric performance and thus in this section, we discuss the approach for preserving structure and neighbourhood within the feature vector of biometric data. Learning compact and effective hash codes can be achieved through embedding the original data into a low-dimensional space while simultaneously preserving the inherent neighbourhood structure [22]. In the line of the same argument, a set of works have demonstrated that nonlinear manifold learning methods are more powerful than linear dimensionality reduction techniques as they can effectively preserve the local structure of the input data without the explicit knowledge of global linearity [22, 23]. Motivated by such argument, we represent the features using the manifold representation using the t-Distributed Stochastic Neighbour Embedding (t-SNE) such that the structural relation of biometric data is preserved [23].

Given the binary feature vector Bx for a subject x within the set of enrolment samples, we attempt to learn the hash projection function and the details are provided herewith. The manifold representation for a given enrolment set $\mathbf{X}$ such that:

$$\mathbf{X} := \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n\}$$

can be given by:

$$\mathbf{Y} := \{\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n\}$$

where $\mathbf{Y}$ is the manifold-based representation of corresponding binary feature vectors $\mathbf{X}$.

The key objective in deriving the manifold representation for the enrolment data q represented by $\mathbf{x}_q$ and i by $\mathbf{x}_i$ is that they should preserve both the neighbourhood and the structure in the original space. Thus, the problem can be formulated as a minimization problem that can be represented by Eq. 15.1.

$$min\{\sum_{i=1}^{n} \mathrm{w}(\mathbf{x}_q, \mathbf{x}_i)\|\mathbf{y}_q - \mathbf{y}_i\|^2\} \tag{15.1}$$

where $W_{qi} = w(\mathbf{x}_q, \mathbf{x}_i)$ is the affinity matrix as defined in [22]. Reformulating Eq. 15.1, it can be deduced that there exists $\mathbf{y}_q^\star$ where the solution of objective function is optimal such that:

$$\sum_{i=1}^{n} \mathrm{w}(\mathbf{x}_q, \mathbf{x}_i)(\mathbf{y}_q^\star - \mathbf{y}_i) = 0 \tag{15.2}$$

The assertion of the objective given in Eq. 15.1 is that the minimized distance between the points in embedding implies the distance between the nearest neighbours in the original dimension is preserved. For the sake of simplicity, we skip the details of each step, and the reader is referred to [1, 22].

Solving Eq. 15.2 and rearranging the terms, $\mathbf{y}_q^\star$ can be obtained as:

$$\mathbf{y}_q^\star = \frac{\sum_{i=1}^{n} \mathrm{w}(\mathbf{x}_q, \mathbf{x}_i)\mathbf{y}_i}{\sum_{i=1}^{n} \mathrm{w}(\mathbf{x}_q, \mathbf{x}_i)}. \tag{15.3}$$

Equation (15.3) is a simple formulation of manifold representation using the set of the linear combination of the features from the enrolment set [22].

Further, as the key properties of protected templates in biometrics need to fulfil *irreversibility, revocability and unlinkability* [11, 24, 25], we impose another condition to choose the sub-samples of the features via entropy-based selection to induce the first level of randomness. Given any manifold features $\mathbf{Y} \subseteq \mathbb{R}^r$ and $p \in \mathbb{N}$, the m-th entropy number $\varepsilon_m(\mathbf{Y})$ of Y is defined as

$$\varepsilon_m(Y) := \inf\{\varepsilon > 0 | \mathcal{N}(\varepsilon, Y, \|\cdot - \cdot\|) \leq m\} \tag{15.4}$$

where $\mathcal{N}$ is the covering number. Then, $\varepsilon_m(Y)$ is the smallest radius that Y can be covered by less or equal to m balls [22].

However, the challenge in realizing Equation (15.4) is the difficulty to cover all the wide range $\mathbf{Y}$ and therefore, an alternative possibility would be to use m clusters to cover $\mathbf{Y}$ where the clustering can be performed by *K-means* algorithm. The cluster centres are required to have the largest overall weight with respect to the points from their own cluster, i.e.

$$\sum_{i \in I_j} \mathrm{w}(\mathbf{c}_j, \mathbf{x}_i)$$

indicating the cluster centres as expressed by $\hat{\mathbf{y}}_q$. Using the relation mentioned above, Eq. (15.3) can be written as given by Eq. 15.5 along with the sign function, which translates to hash function. The hash function obtained by binarizing the low-dimensional embedding not only preserves the manifold with neighbourhood but also provides the binary templates [22].

$$h(\mathbf{x}) = \text{sgn}\left(\frac{\sum_{j=1}^{m} \text{w}(\mathbf{x}, \mathbf{c}_j)\mathbf{y}_j}{\sum_{j=1}^{m} \text{w}(\mathbf{x}, \mathbf{c}_j)}\right) \tag{15.5}$$

where $\text{sgn}(\cdot)$ is the sign function and

$$\mathbf{Y_B} := \{\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_m\}$$

is the embedding for the base set

$$\mathbf{B} := \{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_m\}$$

which is the cluster centres obtained by K-means.

The approach formulated by Eq. 15.5 is the manifold representation (a.k.a., embedding) for the enrolment data:

$$\mathbf{Y} = \bar{\mathbf{W}}_{\mathbf{XB}}\mathbf{Y_B}, \tag{15.6}$$

where $\bar{\mathbf{W}}_{\mathbf{XB}}$ is defined using the cluster centres:

$$\bar{\mathbf{W}}_{ij} = \frac{\text{w}(\mathbf{x}_i, \mathbf{c}_j)}{\sum_{i=1}^{m} \text{w}(\mathbf{x}_i, \mathbf{c}_j)} \tag{15.7}$$

for $\mathbf{x}_i \in \mathbf{X}$, $\mathbf{c}_j \in \mathbf{B}$.

In this chapter, we employ two different approaches to derive a manifold representation of the enrolment features. The first approach to derive manifold representation is through Stochastic Neighbourhood preserving Embedding (t-SNE) [23] as proposed in our recent work. It was shown in the preliminary work in [1] that t-SNE based structure preserving manifold is able to preserve both biometric features as well as performance. While in the first approach, the manifold representation and the hashed projection is only based on the optimization of one function given in Eq. 15.5, we explore another similar approach proposed in [22] with a set of relaxations to consider features in the manifold representation and the features in the original space.

$$min\{\sum_{i=1}^{n} \text{w}(\mathbf{x}_i, \mathbf{x}_j)\|\mathbf{y}_i - \mathbf{y}_j\|^2 + \lambda \sum_{\mathbf{x}_i \in \mathbf{Y}, \mathbf{x}_j \in \mathbf{x}}^{n} \text{w}(\mathbf{x}_i, \mathbf{x}_j)\|\mathbf{y}_i - \mathbf{y}_j\|^2\} \tag{15.8}$$

where λ is the relaxation parameter. Through the specific reformulation provided in [22], Eq. 15.8 can be presented as the Laplacian Eigenmap. The first approach relies

on t-SNE and is referred to as ***Manifold-structure Preserving Biometric Template (MaPBiT)*** in our earlier work. The second approach relies on Laplacian Eigenmap (LE), and we hereby refer to it as ***Manifold-structure Preserving via Laplacian Eigenmap for Biometric Template (MaPLEBiT)***.

15.4 Data set and Evaluation Protocol

This section provides the details of the data set employed for the experimental evaluation of the approach presented in this chapter. We employ a face data set captured from smartphone that consists of images corresponding to 94 unique subjects [5, 21]. The composition of the images in the database is provided in Table 15.1.

The images are captured in 15 different attempts where 5 captures correspond to the high-quality enrolment samples and 10 correspond to the probe attempts under varying capture conditions such as illumination and background. We retain the original partition of the database where the complete data set is partitioned to *Development* and *Testing*/*Evaluation*. The *Development* set consists of data captured from 21 different subjects, while the *Testing* set consists of data captured from 73 subjects. The parameters of experiments such as number of filters, size of filters and hashing features are selected on the basis of empirical trials on the *Development* data set. The selected parameters are used for experiments on the *Testing* data set to report the results in this work.

15.4.1 Evaluation Protocols

This section outlines the experimental protocols followed in this chapter. We adopt the protocols corresponding to the earlier works [21] that have 5 images in enrolment set and 10 images in the probe set. The results are presented in the terms of Equal Error Rate (EER %) such that a symmetrical error distribution of False Match Rate (FMR) versus False Non-Match Rate (FNMR) can be visualized. The error rates are accompanied by the Detection Error Trade-off (DET) curves to understand the algorithmic performance.

Table 15.1 Statistics of the smartphone face biometric data set

	Development data set	Testing data set
Subjects	21	73
Device	Samsung Galaxy S5	Samsung Galaxy S5
Reference images	5	5
Probe images	10	10
Genuine comparisons	1050	3650
Impostor comparisons	21,000	262,800

15.5 Experiments and Results

Along with the results from the proposed approach in this chapter, we present the results from two other approaches that correspond to the performance from unprotected biometric templates and another set corresponding to protected templates through Bloom filter approach. A significant difference to be noted in the experimental protocols is that while the unprotected and protected template performance is independent of enrolment samples, the proposed approach relies on the known enrolment set (closed-set biometric scenario).

Unprotected Templates: In order to provide biometric performance, we provide the baseline evaluation with unprotected biometric templates using the multi-scale block-based Binarized Statistical Image Features (BSIF) which are derived using a set of varying filters of size such as 3×3, 5×5, 7×7, 9×9, 11×11, 13×13, 15×15 and 17×17 with each of basis size corresponding to eight layers. Further, the biometric face image is partitioned into 32 different blocks of size 8×20 pixels as discussed earlier in Sect. 15.3.1. The resulting concatenated histograms are binarized using simple zero thresholding, and the distance between two histograms is measured using Hamming distance in the unprotected domain.

Bloom filter Template Protection: In a similar manner to unprotected templates, we employ Bloom filter representation to derive protected templates using the features as discussed in Sect. 15.3.1. Further, Hamming distance is employed to measure the dissimilarity between the protected templates to derive the biometric templates [21].

Proposed Template Protection Schemes: In order to evaluate the proposed approaches, we adopt features as outlined in Sect. 15.3.1. As the features are further represented in binary format, we employ simple Hamming distance to derive the biometric performance. The key difference here compared to unprotected and Bloom filter based template protection is the number of filters employed. *In the proposed approach, we employ block-based approach with only* 9×9 *pixels with* 8 *bits while both unprotected and Bloom filter based templates employ* 8 *different filters along with block-based approach.*

15.5.1 Discussion on Results

As it can be observed from Table 15.2 and Fig. 15.3, the proposed approach (both variants) provide better performance with respect to both FMR and FNMR. The better results compared to unprotected templates can be fully attributed to the optimization procedure in selecting the unique bits for the hash. *While one can argue that the performance is primarily due to optimization from the known set, it can be counter-argued that data from pseudo-users can be used to derive the templates for each user of the smartphone.* Given this argument, we are justified in using this approach to obtain the performance close to unprotected templates. The obtained results have

Table 15.2 Results obtained for unprotected templates, Bloom filter template & proposed template protection (MaPBiT and MaPLEBiT). Genuine Match Rate (GMR) reported at False Match Rate of 0.01%. The results with ± presents the average variance over a number of experimental evaluation

Template	Face	
	EER	GMR
Unprotected-MBSIF	1.65	90.05
Protected-Bloom filter	2.91	82.68
Protected-Proposed-MaPBiT	0.65 ± 0.18	92.10 ± 0.78
Protected-Proposed-MaPLEBiT	0.82 ± 0.12	89.45 ± 0.57

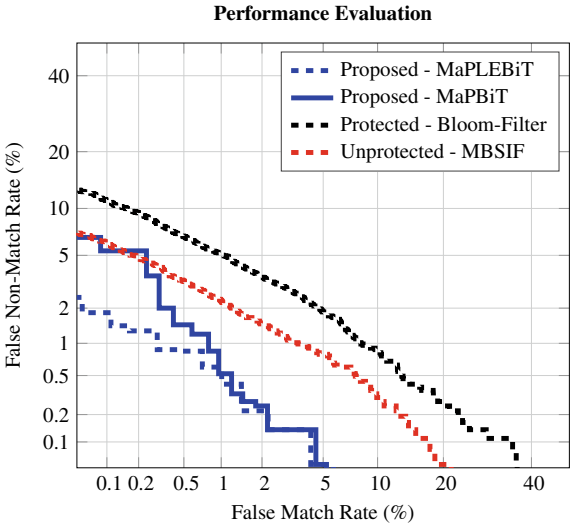
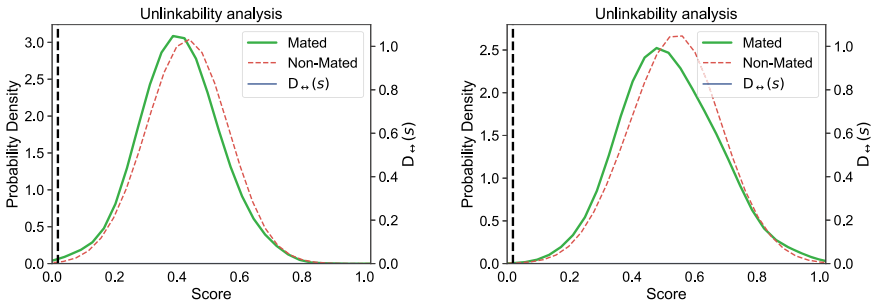


Fig. 15.3 Comparison of biometric performance using DET for smartphone face biometric data set

validated our intuition that retaining the inherent structural similarity of biometric features via neighbourhood preserving embedding improves the protected template performance. Further, the results also suggest that the approach can be used in two different variants with t-SNE and Laplacian Eigenmap based manifolds.

15.5.2 Unlinkability Analysis

This section presents the unlinkability analysis of the proposed approach through the metric proposed in [12, 26]. Here, it is assumed that the same biometric system is deployed for two different applications, and it should not be possible to tell if an individual present in one is also present in the other. The biometric templates from the same individual (one template from each application) are compared to generated



(a) MaPLEBiT (Laplacian Eigenmap) (b) MaPBiT (tSNE)

Fig. 15.4 Unlinkability analysis of proposed template protection

mated score distribution. Similarly, the biometric templates from different individuals are compared to generate the non-mated score distribution. Greater overlap between the two distributions demonstrates greater unlinkability.

The score distributions of two cancellable templates are presented in Fig. 15.4 for two variants of the proposed approach. As observed from Fig. 15.4, both the variants, *MaPBiT* and *MaPLEBiT*, demonstrate a good degree of unlinkability. This can be interpreted through the genuine and the imposter distribution which have a high degree of overlap indicating the low probability of linkability.

15.5.3 Limitations of Current Work and Potential Future Works

The proposed approach in both variants has demonstrated not only good biometric performance but also the applicability for the smartphone biometric scenario. While the performance closely matches the unprotected template biometric performance, the proposed approach inherently needs known enrolment set. Although this limitation can be addressed through employing a set of pseudo-users, real-time analysis with large-scale biometric data needs to be conducted. As a second advantage, the proposed approach results in a compact template size which can be aptly used in smartphone biometric scenario demanding very low memory size.

15.6 Conclusions

In this chapter, an approach for biometric template protection for smartphone data was presented with two variants. The need for preserving the sensitivity of the biometric data while respecting key properties of *irreversibility*, *unlinkability* and *renewability*

has been met through the proposed approach. The chapter has systematically argued the use of manifold preserving feature representation to improve the biometric performance of template protection. The argument has been well illustrated using the two variants of manifold representation with an experimental analysis of the proposed approach. The results obtained on a moderate-sized face biometric database indicate the applicability of proposed approach with a resulting accuracy of $EER \approx 0.65\%$ for the first variant (t-SNE) and the $EER \approx 0.82\%$ for the second variant (Laplacian Eigenmap), both of which are better than the EER (1.65%) of the unprotected biometric system. Unlinkability analysis of the proposed approach has shown very low chance of linkage issues and thereby providing the better cancellable biometric templates in a closed-set scenario.

Acknowledgements This work was partially carried out under the funding of the Research Council of Norway (Grant No. IKTPLUSS 248030/O70).

References

1. Raja KB, Raghavendra R, Busch C (2018) Manifold-structure preserving biometric templates - a preliminary study on fully cancelable smartphone biometric templates. In: Proceedings of the ICME, pp 1–8
2. ZOLOZ Real ID. http://www.zoloz.com, 2017. Accessed on 01 Jan 2018
3. Salesky J (2017) Providing a frictionless banking experience: What banks can learn from apple. Am Bankers Assoc. ABA Bank J, 109(1):38–38,50. Copyright - Copyright Naylor, LLC Jan/Feb 2017; Last updated - 2017-02-07; CODEN - ABAJD5
4. De Marsico M, Galdi C, Nappi M, Riccio D (2014) Firme: face and iris recognition for mobile engagement. Image Vis Comput 32(12):1161–1172
5. Raja KB, Raghavendra R, Stokkenes M, Busch C (2015) Multi-modal authentication system for smartphones using face, iris and periocular. Proceedings of 2015 international conference on biometrics, ICB 2015, pp 143–150
6. Rattani A, Derakhshani R, Saripalle SK, Gottemukkula V (2016) Icip 2016 competition on mobile ocular biometric recognition. In: 2016 IEEE international conference on image processing (ICIP), pp 320–324
7. Raja KB, Raghavendra R, Vemuri VK, Busch C (2015) Smartphone based visible iris recognition using deep sparse filtering. Pattern Recognit Lett 57:33–42
8. Ratha NK, Chikkerur S, Connell JH, Bolle RM (2007) Generating cancelable fingerprint templates. IEEE Trans Pattern Anal Mach Intell 29(4):561–572
9. Ratha NK, Connell JH, Bolle RM (2001) Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J 40(3):614–634
10. Council of European Union. Apple touch id, Accessed on April 2016. http://www.cbsnews.com/news/should-you-fear-apples-fingerprint-scanner/
11. ISO/IEC JTC1 SC27 Security Techniques. ISO/IEC 24745:2011. information technology - security techniques - biometric information protection, 2011
12. Gomez-Barrero M, Rathgeb C, Li G, Ramachandra R, Galbally J, Busch C (2018) Multi-biometric template protection based on bloom filters. Inf Fusion 42:37–50
13. Jutta H-U, Elias P, Andreas U (2009) Cancelable iris biometrics using block re-mapping and image warping. In ISC, vol 9. Springer, pp 135–142
14. Jin ATB, Ling DNC, Goh A (2004) Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognit 37(11):2245–2255

15. Patel VM, Ratha NK, Chellappa R (2015) Cancelable biometrics: a review. IEEE Signal Process Mag 32(5):
16. Pillai JK, Patel VM, Chellappa R, Ratha NK (2011) Secure and robust iris recognition using random projections and sparse representations. IEEE Trans Pattern Anal Mach Intell 33(9):1877–1893
17. Uludag U, Pankanti S, Prabhakar S, Jain AK (2004) Biometric cryptosystems: issues and challenges. Proc IEEE 92(6):948–960
18. Juho K, Esa R (2012) BSIF: binarized statistical image features. 21st ICPR (Icpr):1363–1366
19. Raja KB, Raghavendra R, Busch C (2014) Binarized statistical features for improved iris and periocular recognition in visible spectrum. In: 2014 International Workshop on Biometrics and forensics (IWBF), pp 1–6
20. Stokkenes M, Ramachandra R, Raja KB, Sigaard M, Gomez-Barrero M, Busch C (2016) Multi-biometric template protection on smartphones: an approach based on binarized statistical features and bloom filters. In: Iberoamerican Congress on Pattern Recognition. Springer, pp 385–392
21. Stokkenes M, Ramachandra R, Sigaard MK, Raja KB, Gomez-Barrero M, Busch C (2016) Multi-biometric template protectiona security analysis of binarized statistical features for bloom filters on smartphones. In 6th IPTA. IEEE 2016:1–6
22. Shen F, Shen C, Shi Q, Van Den Hengel A, Tang Z (2013) Inductive hashing on manifolds. In: 2013 IEEE conference on computer vision and pattern recognition (CVPR). IEEE, pp 1562–1569
23. van der Maaten LJP, Hinton GE (2008) Visualizing high-dimensional data using t-sne
24. Marta G-B, Christian R, Javier G, Christoph B, Julian F (2016) Unlinkable and irreversible biometric template protection based on bloom filters. Inf Sci
25. Hermans J, Mennink B, Peeters R (2014) When a bloom filter is a doom filter: security assessment of a novel iris biometric template protection system. In: 2014 International conference of the biometrics special interest group (BIOSIG), pp 1–6
26. Gomez-Barrero M, Galbally J, Rathgeb C, Busch C (2018) General framework to evaluate unlinkability in biometric template protection systems. IEEE Trans Inf Forensics Secur 13(6):1406–1420