Received: 20 May 2020 | Revised: 5 January 2021 | Accepted: 12 February 2021

DOI: 10.1049/bme2.12043

IET Biometrics

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH PAPER

Towards better and unlinkable protected biometric templates using label-assisted discrete hashing

Kiran Raja[1,2] | **R. Raghavendra**[2] | **Christoph Busch**[2]

[1]Department of Computer Science, The Norwegian Colour and Visual Computing Laboratory, Norway

[2]Norwegian Biometrics Laboratory, NTNU, Gjøvik, Norway

Correspondence

Kiran Raja, Department of Computer Science, The Norwegian Colour and Visual Computing Laboratory, Norway.
Email: kiran.raja@ntnu.no

Abstract

The growth of biometrics-based authentication in various services raises the need to protect biometric data at the storage level. Specifically, biometric templates need to be protected after features are extracted to avoid the leakage of biometric data and subsequent linkability issues. An approach based on discrete hashing is presented with the assistance of semantic labels to generate discriminative and privacy preserving protected templates in this work. The proposed approach can easily be adopted for a closed-enrolment set in which enrolment images are known a priori whereas the challenge of learning templates for a single subject remains open. To extend this approach for individual subject, the concept of auxiliary pseudouser enrolment data is introduced, through which a protected template can be generated at the user level. Through the use of a moderately sized multimodal biometric database of 94 subjects, the effectiveness of the proposed approach is illustrated to achieve a robust and secure template protection with *irreversibility*, *unlinkability* and *renewability*. With the set of experiments, the performance of the template protection approach is established and benchmarked against the popular bloom-filter technique. The proposed approach results in a high genuine match rate (≈100% at a false accept rate of 0.01%) and low equal error rate (EER ≈ 0%) and outperforms traditional approaches while satisfying other requirements of biometric template protection when the closed enrolment set is known. With auxiliary pseudousers, the performance of the proposed approach for user-level protected template creation results in an EER of 2.5%, indicating very low performance degradation compared with the known enrolment dataset. Along with the set of experimental validation of the proposed approach, a security analysis of the proposed approach is presented to demonstrate the unlinkability of the biometric templates using a state-of-art unlinkability metric.

1 | INTRODUCTION

The automated recognition of individuals based on physiological characteristics such as the face, fingerprints, or iris or behavioural traits such as the gait, keystrokes, or mouse dynamics is termed biometric recognition. The reliability of such an approach in recognizing an individual with high confidence has resulted in numerous applications such as border control and access control to personal devices (e.g., smartphones), establishing and verifying identity using biometrics. This success has resulted in heavily focused research to make techniques and algorithms robust enough to achieve higher accuracy. However, there are a few major challenges when adapting biometrics to everyday authentication scenarios using smartphones owing to the sensitivity of biometric data.

1.1 | Background and related works

As the number of instance of a biometric characteristics owned by an individual is limited (e.g. 1 face, 2 irises, 10 fingerprints), unlike passwords, biometric data cannot be regenerated if leaked. It is therefore essential to store biometric data in a secure and protected manner in which the privacy and sensitivity of the biometric data are preserved. The process of securing biometric data is popularly referred to as biometric

template protection (BTP). Due to the limited number of biometric characteristics, one can be forced to use same characteristic for multiple services, for example, the face can be employed in banking applications as well as in border control application. Thus, it is necessary to unlink biometric templates across multiple services. Along with unlinkability, when a template is compromised, it should be irreversible and templates should be renewed. Thus, an ideal BTP should provide unlinkability, irreversibility and renewability to secure biometric data, preserve privacy and protect the data of subjects according to international standard ISO/IEC IS 24745 [1] and European Union (EU) General Data Protection Regulation (GDPR) 2016/679 [2].

To fulfill the requirements laid out by ISO/IEC IS 24745 [1] while complying with EU-GDPR 2016/679 [2], a number of earlier works proposed various techniques for BTP. These techniques can be categorised under biometric cryptosystems [3] and cancellable biometric systems [4–7]. Generally, the template protection scheme can be enforced at the service level where all enrolment biometric data are protected within the database (e.g. protecting biometric data in civilian ID management) or at a user level benefiting the service (e.g. protecting biometric data of banking users at the device level in accordance with the European Payment Services Directive [8]). Whereas most previous work has proposed template protection schemes at a service level where enrolment data are known a priori [6, 7, 9], some work has also proposed user-level template protection [10, 11]. Of the popular approaches, random projections-based template protection [6] and biohashing schemes [7, 9] are based on projections and hashing on the enrolment dataset. In another category of user-level template protection, bloom filter-based template protection was proposed employing private keys at the service level to avoid linkability challenges [10, 11]. In a similar direction of hashing, two other works were reported exploiting a kernel approach with hashing specifically designed for spectral data consisting of a number of images to create better kernel representations [12, 13]. Despite these advances, the challenge of obtaining a stable template under variation of biometric sample data (owing to pose, illumination and expression) remains open for biometric modalities. Although earlier works provide a good basis for BTP, no specific works provides a common strategy for both service-level (i.e. fully available enrolment set) and user-level template protection, which motivates our current work to obtain stable hash representation and also provide protected biometric templates at the service and user levels.

1.2 | Challenges and our contributions

We first consider the problem of arriving at stable hash representation of biometric features. As with a traditional biometric system, we first extract the features from biometric data. We then address the problem of obtaining stable hash templates. Furthermore, it has to be noted with caution that hashing methods generally partition the entire dataset and derive a single hash from each partition. Thus, the learned templates can be optimal when the training or enrolment data (features) are known a priori. Therefore, we acknowledge that hashing approaches may not be effective when the entire enrolment is not known, or for each user independently (irrespective of the enrolment set). Such challenges hinder arriving at stable hash for each user, which motivated the second part of the current work. We therefore address the problem of creating stable hash when the entire enrolment set is unavailable in the second part, as explained in Section 1.2.2.

1.2.1 | Stable hash representation

To address the problem of arriving at stable hash, we propose employing semantic label-assisted discrete hashing to derive protected templates. Our assertion is that the biometric feature similarity relationship is preserved while deriving the hash function by using labels from enrolment samples (also referred to as similarity labels or semantic similarity labels). The use of such labels aids as metadata to address performance limitations posed by unsupervised hashing, specifically for biometric data. The four major steps in our proposed approach consist of (1) extracting features from biometric images, (2) learning a hash projection for a given enrolment set and obtaining a protected enrolment template, (3) using the projection matrix to create a template for a probe (verification) image, and (4) comparing the protected templates to arrive at decision to accept or reject the claimed identity. Our first contribution comes in Step 2 for this sequence by employing enrolment labels (semantic similarity labels), as explained in Section 1.2.1. The approach can be tailored to obtain a chosen length of features in protected templates (e.g. 32, 64, 128, or 256 bits), making it compact and applicable for biometric applications.

Renewability and unlinkability requirement

Although the use of semantic labels to derive a biometric feature relation preserving hash function provides good biometric performance, template protection demands the need for *renewability*, *reversibility* and *unlinkability*, as discussed earlier [1]. To meet these criteria, we incorporate a novel component of induced protected keys before deriving hashing templates to ensure the renewability and unlinkability of the generated protected templates motivated by Bringer et al. [14]. Because the keys are application- or service-specific, we induce the unlinkability and reduce the guessability/brute force attacks by employing keys randomly drawn from a *normal distribution* while generating the hash function as another novel contribution. To this end, our approach has universal protected keys that can be applied at a service level. The specific details of each of these components are presented in Section 2. The new and robust end-to-end template protection approach is based on (1) the concept of leveraging the labels of enrolment samples to achieve a stable hash function to derive the biometric template, and (2) optimization of the hash function by using a private key guaranteeing optimal performance along with the goals of template protection.

1.2.2 | User-level protected template creation

Although our approach is well-engineered for a known enrolment set in which enrolment labels can be used as semantic similarity labels, there is an inherent problem of deriving templates for each user irrespective of other subjects in an unknown enrolment set (i.e. the absence of a semantic label matrix). We therefore propose another strategy for creating user-level protected templates in which the entire enrolment set is unknown (i.e. unavailable semantic label matrix). To this end, we employ the auxiliary data of nonexistent biometric users (pseudousers) inspired by Gunasinghe et al. [15] to scale our approach to cases in which the enrolment set is unknown. Motivated by earlier work [15], we create a pseudoauxiliary similarity label matrix for creating efficient protected templates for each user in a specific service. With the newly adopted strategy, the proposed approach also scales to cases in which the enrolment set is not fully available when creating the templates.

1.2.3 | Contributions

This work therefore presents a complete framework for privacy-preserving protected biometric template creation using texture features (binarized statistical image features [BSIF]) [16, 17] and semantic label-assisted hashing in which the templates are irreversible, unlinkable and renewable. To validate the approach proposed in this work, we present experimental evidence for three independent biometric features (face and periocular images) by employing a biometric database captured in the visible spectrum using a smartphone. Furthermore, as detailed earlier, we present an approach to generating protected biometric templates for each user independently of others in the enrolment set using the auxiliary pseudouser biometric dataset such that it can be employed for user-level template protection. The main contributions of this work are therefore:

1. That it presents a new framework for BTP using texture features and semantic label-assisted hashing through a randomly generated application or service specific key (drawn from *normal distribution*).
2. That it presents a framework to generate the hash-function/hash-projection matrix during enrolment and employs it while comparing the probe attempt based on an available enrolment set. The protected templates vary in size (as compact as 32 bits), depending on the application, while maintaining good accuracy.
3. That it presents an additional strategy for learning a user-level protected template through an auxiliary pseudouser enrolment set to create protected templates at the user level to exemplify the scalability of the proposed approach.
4. An extensive set of experiments is provided to validate the proposed approach using face and periocular images along with a detailed illustration of robustness for security aspects (unlinkability and renewability) of template protection.

In the remainder of this article, Section 2 describes the proposed BTP and Section 4 presents experiments, including a brief discussion of the database in Section 3. In Section 5, we present a detailed security analysis of the protection method, and Section 6 presents concluding remarks and lists potential future work.

2 | PROPOSED BTP FRAMEWORK

Under the assumption that the entire enrolment dataset is available (e.g. civilian ID management), we first present the proposed template protection framework as depicted in Figure 1. Given a biometric image (face or periocular image), we generate protected templates using the approach described subsequently. The proposed approach consists of four steps illustrated in Figure 1. The four main components (marked with numbers in Figure 1) are:

[1] Feature extraction from the biometric sample (e.g. a face or periocular image).
[2] Generation of a hash projection matrix (function) based on the full set of enrolment samples and application-specific key (universal secret key for an application or database).
[3] Generation of protected templates for enrolment set using the generated global and application-specific hash projection matrix.
[4] Generation of protected templates for probe sample using the hash transformation matrix and subsequent comparison of protected templates to derive biometric performance.

We present the details of each step in the following subsections.

2.1 | Texture feature extraction

We employ BSIF [16] to extract the textural features from the biometric samples. BSIF encodes binary features as the result of convolving an input image with a set of independent filters learned on natural images. The key motivation for using BSIF is to leverage high performance for biometric verification by using independently learned natural filters [16] and then to provide a fair benchmark of the proposed approach for earlier works that employed the same feature extraction technique [18]. However, unlike the ensemble approach of earlier work [18], in our work we simply employ one single filter in a block-based manner to extract histogram features resulting from the BSIF-based filtering operation. Therefore, unlike the high feature dimension (65,536) in previous work, we use only 8192

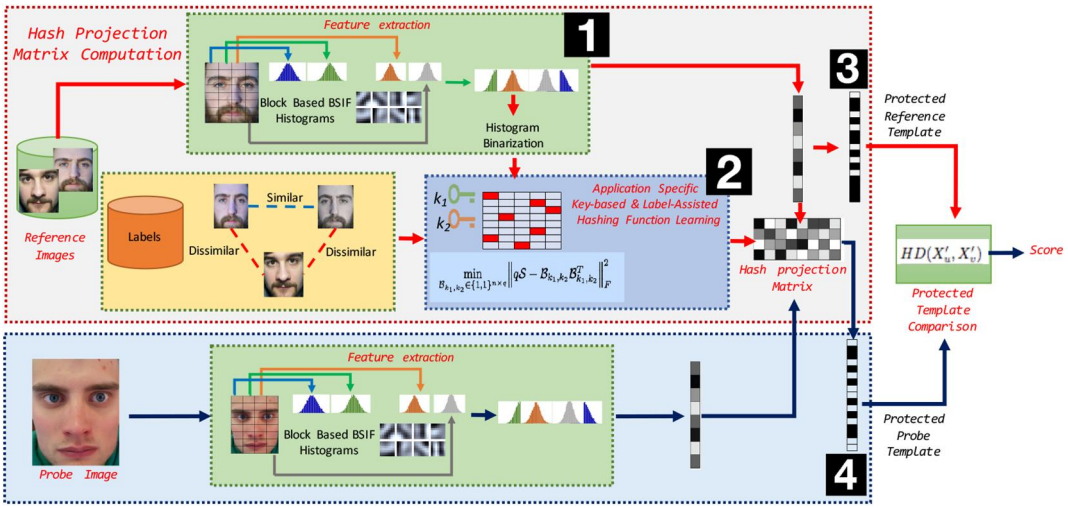

FIGURE 1 Proposed approach for protected template creation. The hash representation with the embedded key is learned for the set of all enrolment samples (i.e., subjects), as shown in the grey block. The learned hash projection matrix is then used to obtain the protected template for any biometric samples, as indicated in the blue block

features in our work, reducing feature space and thus the computational complexity of the approach.[1]

2.2 | Learning protected hash-projection matrix using private keys

Considering a set of n number of samples (enrolment samples) with d dimensional features, all enrolment samples can be represented as $\{x_i \in \Re^d\}_{i=1}^n$, where x_i corresponds to the feature at point i (i.e. x_i is the feature vector). Furthermore, they can be equivalently denoted as $\mathcal{X} \in \Re^{n \times d}$ for the sake of simplicity, where $\mathcal{X}_{i*}^T = x_i$. Alongside the feature vectors, the enrolment set (training set) of supervised hashing accompanies a semantic similarity matrix $\mathcal{S} \in \{-1, 1\}^{n \times n}$, where $S_{ij} = 1$ indicates the similarity between point x_i and point x_j, whereas $S_{ij} = -1$ indicates dissimilarity between points x_i and x_j. In other words, these correspond to the label of the enrolment samples of a particular biometric characteristic.[2] From the set of feature vectors represented by $\mathcal{X}$, we learn the optimized binary code matrix $\mathcal{B} \in \{0, 1\}^{n \times q}$, where q represents the bit length of the template and $\mathcal{B}_{i*}$ denotes q-bit code for a training (enrolment) sample i while preserving the similarity of feature vectors with the help of $\mathcal{S}$ or semantic labels. For computational reasons, we represent the binary array $\mathcal{B} \in \{0, 1\}$ in terms of $\{-1, 1\}$, where 0 is replaced by -1.

The derivation of hash function can simply be translated to an optimization problem, as defined by Equation (1) [19]:

$$\min_{\mathcal{B} \in \{-1,1\}^{n \times q}} \left\| q\mathcal{S} - \mathcal{B}\mathcal{B}^T \right\|_F^2 \tag{1}$$

where norm $|.|_F$ represents the Frobenius norm of the matrix and q is the bit-length of the template. Equation (1) can be written as Equation (2):

$$\left|\left| q\mathcal{S} - \mathcal{B}\mathcal{B}^T \right|\right|_F^2 = \sum_{i=1}^{n} \sum_{j=1}^{n} \left(qS_{ij} - B_{i*}B_{j*}^T \right)^2 \tag{2}$$

Equation (1) and subsequently Equation (2) can be noted as optimization problems to minimize loss using the square loss [20]. Inspired by Kang et al. [19], demonstrating the theoretical guarantee of obtaining a stable hash function, we adopt the same optimization approach to derive a hash function that serves the purpose of BTP and also improves recognition accuracy. Thus, the optimization problem in Equation (1) is solved by using a column sampling strategy to obtain stable hash with performance guarantees [19].

Furthermore, for the case of BTP, the problem of *irreversibility*, *unlinkability* and *renewability* has to be considered while achieving good biometric performance. The goal is thus to achieve a simple yet robust, renewable template while ensuring *unlinkability* to avoid the linkage of two databases [21]. To comply with this requirement, we present an approach with a private key that is unique and application-specific, inspired by security analysis provide in Bringer et al. [14]. This application-specific private key is induced while generating and optimizing the binary matrix $\mathcal{B}$. Although one specific key can be used to achieve good unlinkability, to guarantee a high degree of *irreversibility and unlinkability*, we employ two keys, k_1 and k_2, to derive the initial binary matrix with label constraints such that $\mathcal{B}$ is a result of two private keys and can be represented as $\mathcal{B}_{k_1,K_2}$.[3] The role of number of keys is further discussed in Section 2.3.

$$\mathcal{B}_{k_1,k_2} = \mathcal{B}^{k_1} \oplus \mathcal{B}^{k_2} \tag{3}$$

where $\mathcal{B}^{k_1}$ and $\mathcal{B}^{k_2}$ are two normally distributed random matrices, which are further binarized based on simple thresholding through keys k_1 and k_2.

The protected binary matrix to generate the hash function is a *bitwise XOR* of two distributions satisfying conditions imposed by keys, which are further presented as:

$$\mathcal{B}_i^{k_1} = \begin{cases} 1, & \text{if } i \geq k_1 \\ -1, & \text{otherwise} \end{cases} \tag{4}$$

$$\mathcal{B}_i^{k_2} = \begin{cases} 1, & \text{if } i \geq k_2 \\ -1, & \text{otherwise} \end{cases} \tag{5}$$

Thus, optimization problem in Equation (1) can be represented as:

$$\mathcal{W}_{k_1,k_2} = \min_{\mathcal{B}_{k_1,k_2} \in \{-1,1\}^{n \times q}} \left\| q\mathcal{S} - \mathcal{B}_{k_1,k_2} \mathcal{B}_{k_1,k_2}^T \right\|_F^2 \tag{6}$$

We simply adopt the column sampled optimization proposed in Kang et al. [19] to derive the hash matrix based on private keys. The final binary projection/hash matrix, satisfying constraints laid by the keys, is used to transform the features to templates as provided by:

$$\mathcal{X}'_q = \mathcal{X}\mathcal{W}_{k_1,k_2} \tag{7}$$

$$(\mathcal{X}'_q)_i = \begin{cases} 1, & \text{if } i \geq 0 \\ 0, & \text{otherwise} \end{cases} \tag{8}$$

where $\mathcal{X}'$ represents the transformed and protected binary template of length q bits.

2.3 | Role of keys in proposed approach

As indicated in Equation (3), the proposed approach relies on private keys. It can be intuitively noted that the number of keys can be chosen to be any number p in a space of $1 < p < \infty$, as indicated in Equation (9):

$$\mathcal{B}_{k_1,k_2,\ldots k_p} = \mathcal{B}^{k_1} \oplus \mathcal{B}^{k_2} \cdots \oplus \mathcal{B}^{k_p} \tag{9}$$

where $p \in 1, 2, \ldots \infty$.

Because the keys are used to generate binary vectors from normal distribution, in theory the keys can span to ∞ space. However, because the drawn random normal distribution is thresholded to get the binary vectors, the binary vectors can start colliding. Because the proposed approach is designed for a q-bit protected template, the binary vector derived using key k can be represented as $\mathcal{B}_k$. If b is the number of possible bits (i.e. 0 or 1), the number of possible combinations for the q length binary vector can be represented as:

$$\frac{b!}{q!(p-q)!} \quad for\ q > p. \tag{10}$$

However, because the binary vectors derived using private keys are employed for *XOR* operation, having a large number of keys may result in sparse binary vectors. The sparsity introduced in the binary vectors may result in colliding binary vectors. Specifically, suppose $\mathcal{B}_{k_{x1}}$ has m non-zero entries in the binary vector derived using key k_{x1} and $\mathcal{B}_{k_{x2}}$ has m non-zero entries in the binary vector derived using key k_{x2}, and they differ in m places. The probability that the ith entry of $\mathcal{B}_{k_x}$ is non-zero is equal to probability that a random variable with distribution binomial (m, r) (with the vector being binary) is even. The upper-bound probability P_{up} of both binary vectors being exactly same therefore can be represented as given by Equation (11):

$$P_{up} = \left(\frac{1}{2}(1 + (1-2r)^m)\right)^r \tag{11}$$

Thus, although the maximum number of private keys is unbounded, the binary vectors by themselves colliding are bounded by the probability in Equation (11). When the binary vectors start colliding, *XOR* operation involved in Equation (9) starts nullifying multiple features, which results in underoptimized protected template creation. An optimal selection can be made under such upper bounds while keeping the template protection approach superior.

2.4 | Protected template at user level using auxiliary pseudousers

As acknowledged earlier, the proposed approach is challenged when the entire dataset corresponding to enrolment is unavailable. At the same time, regulations require that biometric data verification occurs at the device level without biometric data transfer to the remote verification infrastructure [8]. To address this challenge considering both of these aspects, we propose a strategy to derive a protected template for each user independently of the enrolment set by employing a pseudouser set inspired by Gunasinghe et al. [15]. In this extension of the proposed approach, an unrelated biometric enrolment set is employed with p number of users, which corresponds to p semantic labels. Thus, for a specific user m of interest, we construct the enrolment set with p pseudousers and the mth user. With this strategy, we create protected templates independently of the entire enrolment set of a particular service, such as a banking service. The strategy of creating an auxiliary pseudouser-based protected template is provided in Figure 2. The proposed approach scales easily for any number of users without depending on the rest of the real enrolment dataset. In case a particular template for a user is compromised, a new template can easily be created by changing the key, and can be replaced.

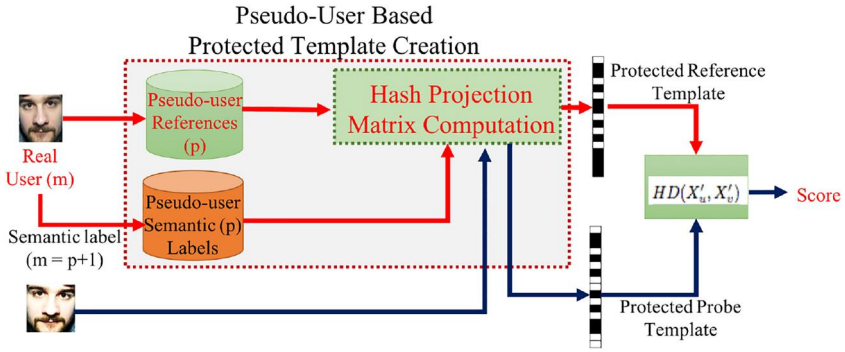

FIGURE 2 Auxiliary pseudouser enrolment-based template creation at the user level. The protected template in this case is created for each biometric sample (for instance, a face image) for reference and probe. The reference biometric sample is inserted into the pseudouser enrolment set to derive the hash projection matrix and the learned projection matrix is used to obtain the protected template for the probe image

2.5 | Protected template similarity

For a protected template of size q-bit length, we use the Hamming distance (HD) to measure dissimilarity between templates owing to the binary nature of templates and the robustness of the HD. Dissimilarity between two protected binary templates, $\mathcal{X}'_u$ and $\mathcal{X}'_v$, is provided by $HD(\mathcal{X}'_u, \mathcal{X}'_v)$, which measures the number of disagreeing pairs of bits.

3 | DATASET AND EVALUATION PROTOCOL

In this section, we present the dataset and the corresponding experimental protocols. A multimodal biometric dataset of face and periocular images (left and right eye) captured from a Samsung Galaxy S5 smartphone is employed [18]. The dataset consists of data obtained from 94 unique subjects in 15 different attempts, in which 5 attempts correspond to high-quality enrolment samples and 10 correspond to probe samples with various lighting and environmental conditions. The database is divided into a *development* and *testing/evaluation* set, in which the *development* set consists of 21 subjects and the *testing* set consists of 73 subjects. The *development* dataset is used to tune the parameters of the proposed approach. The testing dataset of 73 subjects has a total of 73 *subjects* × 15 *samples* = 1095 images for face and similarly, 1095 left periocular images and 1095 right periocular images.

3.1 | Evaluation protocol

To demonstrate the applicability of the proposed approach, we evaluate it for the face and left and right periocular images independently. However, we acknowledge that the creation of protected templates for multimodal biometric is fully possible when the features are combined. With five enrolment samples and 10 probe samples for 73 subjects, a total of 3650 genuine comparisons and 262,800 impostor comparisons are obtained for each biometric modality, which agrees with the protocols provided by earlier work using the same dataset for template protection [18]. Furthermore, to provide recognition performance of the template protection scheme, we provide the baseline evaluation on unprotected templates using multiscale block-based BSIF features and benchmark them against single-scale block-BSIF features with proposed template protection.

4 | EXPERIMENTS AND RESULTS

We present the experiments and corresponding results obtained with the database for both unprotected and protected templates. Details for each approach are presented in the following subsections.

4.1 | Unprotected templates and bloom-filter templates

In the case of unprotected templates, we employ multiscale BSIF filters of sizes 3 × 3, 5 × 5, 7 × 7, 9 × 9, 11 × 11, 13 × 13, 15 × 15 and 17 × 17, each size corresponding to eight layers. Each image (face or periocular) is partitioned into 32 different blocks of size 8 × 20 pixels and 15 × 22 for face and periocular images, respectively. Furthermore, the features are represented as histograms, resulting in a feature vector of size 8 × 256 for a total of eight separate filters. For 32 unique blocks, the total feature size for an image is 65,536 features. For the sake of simplicity and to provide a fair comparison with earlier work [18], we binarize the features as 1 if the histogram feature is greater than 0, and 0 otherwise. Furthermore, the HD is employed to measure the dissimilarity between templates in the unprotected domain.

The same set of features is further employed to obtain a Bloom filter-based template in which the feature vector is restructured into a matrix of dimensions 256 × 256, in which

each row corresponds to an extracted histogram [10, 22]. In line with the unprotected templates, a simple binarization is carried out on histogram features before the bloom filter transformation is carried out. Again, we employ the HD to measure dissimilarity between templates (bloom filters) in the protected domain.

4.2 | Proposed template protection

We divide the image into 32 unique blocks of size 8 × 20 pixels and 15 × 22 for face and periocular images, respectively. However, unlike the previous approaches, we employ single-scale BSIF features to obtain protected templates and thus significantly reduce the length of the feature vectors. For the sake of simplicity, we present the results of template protection achieved using a BSIF filter of 8 bits for a 3 × 3 filter.[4] However, the results for different sizes of filters ranging from 3 × 3, 5 × 5, 7 × 7, 9 × 9, 11 × 11, 13 × 13, and 15 × 15 to 17 × 17 pixels are further presented to illustrate the effect of filter size on template protection in Figure 3. Furthermore, we experimentally demonstrate the ability of the compact size of protected templates by setting q bits to $q = \{32, 64, 128, 256\}$.[5]

4.3 | Results

For all experiments, the disjoint dataset is employed as reported in Stokkenes et al. [18]. We measure the recognition performance on the *testing* set of the database in terms of the genuine match rate (GMR) at particular false match rates (FMR) and report the results for both protected and unprotected templates. Furthermore, we present the equal error rate (EER) along with the detection error trade-off (DET) curves and cumulative match curves.

4.3.1 | Results with proposed framework

Table 1 presents results for the proposed approach when the entire enrolment set is known along with current state-of-art approaches. For the sake of simplicity, we present the results of templates with bit lengths $q = 64$ and $q = 256$ bits. The results and Figure 4 (associated identification accuracy is provided in Figure 5), key observations and the analysis show that:

- The proposed approach achieved a high GMR at FMR = 0.01% and a correspondingly low *EER* for all three modalities.
- Although the unprotected templates with multiscale BSIF resulted in GMR = 90% for faces, the protected templates with a bloom filter resulted in a lower of 82% indicating a loss of accuracy when templates are protected. Similar observations can be made for periocular images. The loss of distinctive features owing to the conversion of binary template and functioning of the bloom filter seeking the presence of values in a block of an image leads to the loss of accuracy.
- However, with the proposed approach, we achieved better accuracy of GMR for faces and the periocular region (left and right). The increase in accuracy can be attributed to two primary aspects:
  - Robustness of hash learning from the proposed approach, which results in the choice of a highly discriminative feature matrix for each subject when the enrolment set is known.
  - The use of labels in obtaining discriminative information for each unique subject within the enrolment set, further resulting in optimizing the key protected binary matrix while maintaining similarity imposed by the labels ($\mathcal{S}$ in Equation 1).

4.3.2 | Impact of bit length of templates

For the sake of simplicity, we have presented the performance obtained with $q = 32$ and $q = 256$ bits in Table 1. In this section, we analyse the impact of bit length q of the protected template on performance in terms of both GMR and EER. We employ the set of experimental protocols mentioned in Section 3.1, but change the bit lengths to different values, $q = \{32, 64, 128, 256\}$, with a single BSIF filter of size 3 × 3. Results pertaining to this set of experiments are presented in Table 2.[6] The proposed approach with different lengths does not affect the accuracy to a large degree and the observation holds for the face and periocular region. The primary reason for this observation is the robust nature of learning the discriminative hash matrix through the use of the semantic similarity preserving matrix.

4.3.3 | Impact of filter configuration on feature extraction

The generation of strong biometric templates is closely coupled to feature extraction. Therefore, in this section we analyse the impact of different filter configurations and measure their performance (GMR and EER). While maintaining the evaluation protocol and fixing the bit length to $q = 32$, we change the filter size of BSIF filters in different runs. Figure 3 shows that both EER and GMR vary nominally when the filter size is smaller. A drop in performance can be noted when the features are extracted using the 15 × 15 and 17 × 17 filters in which features are not robustly extracted owing to the size of the block. The filter size becomes closer to the size of BSIF filters, resulting in non-robust features. Nonetheless, performance

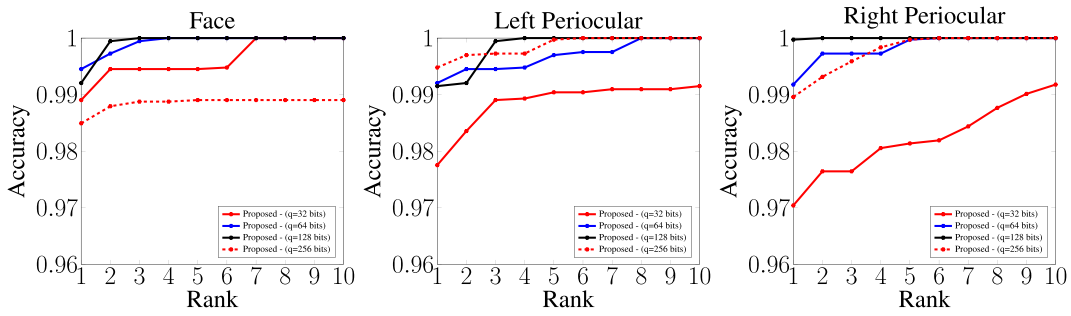

FIGURE 3 Variation of equal error rate and genuine match rate for face characteristics with bit length ($q = 32$) for different size of binarized statistical image feature filters

TABLE 1 Results obtained for unprotected templates, bloom filter template and proposed template protection (BSIF—3 × 3)

	Unprotected		Protected (bloom filter) [18]		Proposed approach ($q = 64$)		Proposed approach ($q = 256$)	
Modality	**GMR (%) @ FMR 0.01%**	**EER (%)**	**GMR (%) @ FMR 0.01%**	**EER (%)**	**GMR (%) @ FMR 0.01%**	**EER (%)**	**GMR (%) @ FMR 0.01%**	**EER (%)**
Face	90.05	1.67	82.63	2.90	**100.00**	**0.00**	**98.88**	**0.03**
Left periocular	83.31	3.20	68.02	5.39	**98.14**	**0.49**	**98.03**	**0.98**
Right periocular	83.78	4.53	72.21	5.48	**98.08**	**0.85**	**97.78**	**0.81**

Abbreviations: BSIF, binarized statistical image feature; EER, equal error rate; FMR, false match rate; GMR, genuine match rate.

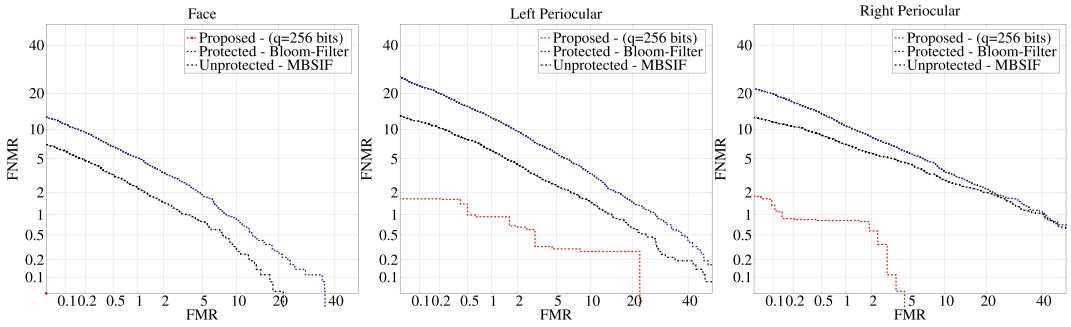

FIGURE 4 Performance (in DET) obtained with unprotected templates, Bloom filter protection and proposed approach (bit length of $q = 256$, binarized statistical image features filter 3 × 3). *Proposed approach results in 0% equal error rate for face modality and therefore is not visible in the DET curve. DET, detection error trade-off

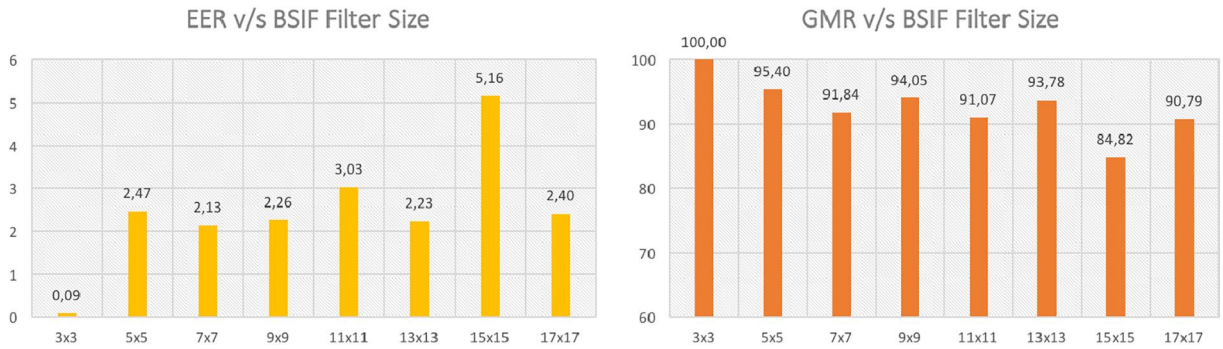

FIGURE 5 Rank identification accuracy (in cumulative match curves) of proposed approach for various bit lengths

TABLE 2 Genuine match rate (GMR) and equal error rate (EER) of proposed protected template protection for various bit lengths (q) of templates (biometric template protection—3 × 3)

	Face		Left periocular		Right periocular	
Bit length	**GMR (%) @ FMR 0.01%**	**EER (%)**	**GMR (%) @ FMR 0.01%**	**EER (%)**	**GMR (%) @ FMR 0.01%**	**EER (%)**
$q = 32$	95.95	2.37	96.08	0.71	97.51	0.69
$q = 64$	**100.00**	**0.00**	98.14	0.49	98.08	0.85
$q = 128$	99.73	0.01	97.29	1.00	98.60	0.80
$q = 256$	98.88	0.03	98.03	0.98	97.78	0.81

reported for the lowest bit length of templates is still observed to be superior to the current state of the art.[7]

4.4 | Results with proposed framework and pseudouser auxiliary data

To address the creation of protected user-level templates independently of the enrolment set, we employ the strategy provided in Section 2.4. In our experiments, we employ the FRGC v2 dataset [23] and randomly choose 50 subjects with 10 facial images for enrolment and 5 facial images for probe, which we refer to as the auxiliary dataset. We follow the same procedure for face detection, cropping and feature extraction as mentioned in the previous section. Furthermore, for each user in the database [18], we create the protected template iteratively by employing the auxiliary dataset. In settings similar to those of the previous experiment, we create templates with various bit lengths in the range 32, 64, 128, and 256 (Figure 6). We present results in the corresponding DET provided in Figure 7. Key observations from this set of experiments are:

- As can be observed from Figure 7, the performance of protected templates using pseudouser auxiliary enrolment data is moderately lower (with EER = 2.5%) compared with protected templates (with EER = 0.03%) when the complete enrolment set is available for the template with $q = 256$ with a BSIF of 3 × 3.
- Intuitively, the moderate degradation can be attributed to suboptimal protected template generation, compared with optimal template generation using the complete enrolment set.
- Despite moderate degradation, the performance remains consistent across different template sizes depicted in Figure 7.

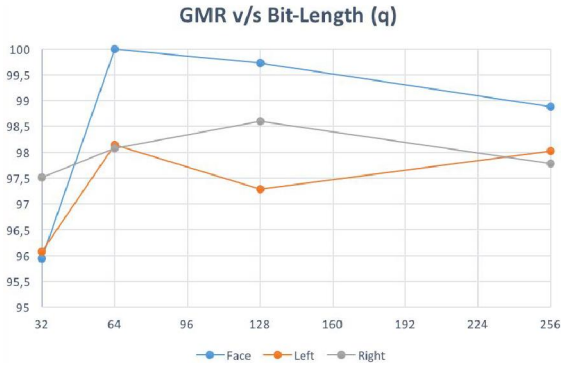

FIGURE 6 Variation of genuine match rate for different bit-lengths (q)

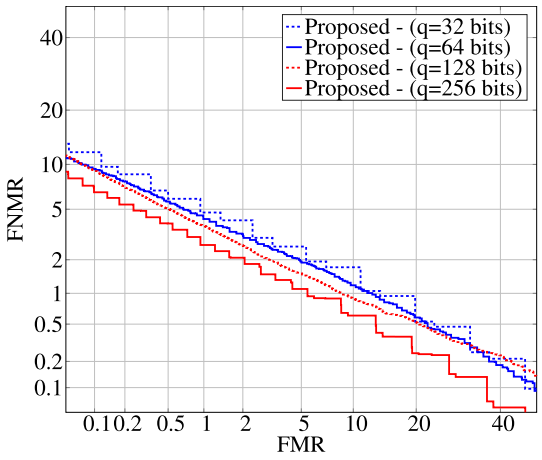

FIGURE 7 Performance (in detection error trade-off) obtained with proposed framework with pseudouser auxiliary data

5 | SECURITY ANALYSIS

Considering three requirements for a template protection scheme, we present the security analysis of the proposed approach. In the first part, we focus on implicit limitations of the proposed approach. Then, we discuss the *renewability* of the template and the *unlinkability* of the BTP.

5.1 | Implications and limitations of proposed approach

The proposed approach relies on the private key and also protecting the auxiliary information of the projection matrix in Equation (6). The inherent failure of the proposed approach can be established not when the private keys are stolen, but when the protected projection matrix in Equation (6) is compromised. As with any biometric operation system, when such an attack is carried out, templates are to be revoked and replaced with new templates. Under such an attack, the performance of the attack

TABLE 3 Unlinkability metric ($D^{sys}_{\leftrightarrow}$) and irreversibility metric ($|\bar{b}|$, and $\overline{rm-rate}$) for various bit lengths of templates

	Face			Left periocular			Right periocular		
Approach	$D^{sys}_{\leftrightarrow}$	$\lvert\bar{b}\rvert$	$\overline{rm-rate}$ (%)	$D^{sys}_{\leftrightarrow}$	$\lvert\bar{b}\rvert$	$\overline{rm-rate}$ (%)	$D^{sys}_{\leftrightarrow}$	$\lvert\bar{b}\rvert$	$\overline{rm-rate}$ (%)
Bloom filter [18]	0.078	7.10	55.00	0.085	8.58	46.00	0.085	8.58	46.00
Proposed ($q = 32$)	0.00	16.60	48.14	0.00	16.67	47.90	0.00	16.57	48.21
Proposed ($q = 64$)	0.00	32.90	48.59	0.00	33.94	46.97	0.00	33.54	47.59
Proposed ($q = 128$)	0.00	68.18	46.73	0.00	68.15	46.76	0.00	68.71	46.32
Proposed ($q = 256$)	0.00	137.11	46.44	0.00	136.30	46.76	0.00	135.67	47.00

Note: The results of the proposed approach can be directly compared with results in Stokkenes et al. [18] for BSIFs 3 × 3.

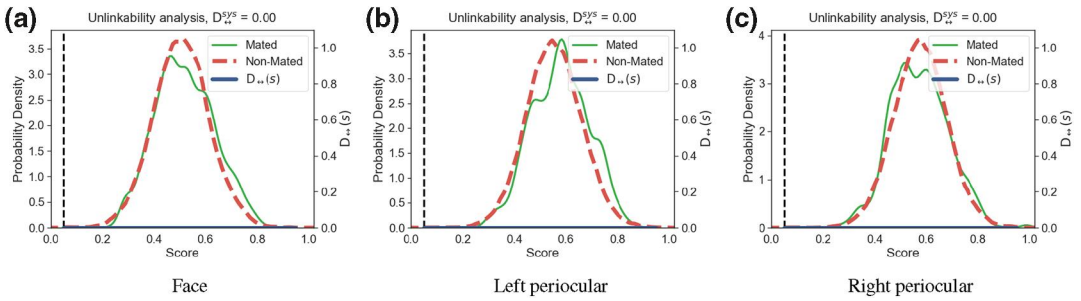

FIGURE 8 Unlinkability analysis with templates of length $q = 32$ for the face and left and right periocular region

success rate equals the performance of a protected biometric system without an attack. The protection of auxiliary information is beyond the scope of this work; thus, we assess the security of the proposed approach for rest of the metrics of template protection, as discussed subsequently.

5.2 | Renewability of templates

Because biometric templates are generated using block-based features from BSIF filtering and the use of private keys to optimize the hash-projection matrix, one can easily renew the templates simply by changing the filters to renew the template. Second, the hash function is based on block-based features, which makes it difficult to compromise the template and reduces the problem for *renewability*.

5.3 | Reversibility and entropy of templates

To evaluate the irreversibility of the templates, we employ the metrics provided by earlier work [10, 24], in which the irreversibility of Bloom filter template protection was previously shown. To estimate the irreversibility of the proposed template protection approach, we measure the probability of guessing the original feature vector from the protected template. Specifically, we employ $|b|$, which is the average number of activated bits in each protected template and is determined empirically for the database. The $|b|$ also represents entropy by indicating on number of bits set to 1 out of the total bits.[8] We also employ $rm-rate$, which is described as the average remapping rate for words, or the chance of reconstructing the template from a given random binary string. Considering that no word construction is involved in the proposed approach, we simply use the metric to present the rate of reversibility with respect to the length of the protected template. Table 3 shows that the reconstructing probability is around 46% for all three modalities.

5.4 | Unlinkability analysis and metrics

We achieve unlinkability through private key embedding, as given in Equation (6) in which templates are based on keys. Furthermore, these keys are used to generate the random distributed binary matrix before optimizing the hash function. With this background, we present the experimental evaluation of the unlinkability of the templates generated using two separate keys. The results are presented in accordance with a proposed *unlinkability* metric [22] with two measures: $D_{\leftrightarrow}$ and $D^{sys}_{\leftrightarrow}$, in which $D_{\leftrightarrow}$ describes unlinkability for different score values within the system and $D^{sys}_{\leftrightarrow}$ estimates the overall unlinkability of the system. Thus, the results of *unlinkability* analysis is presented by the score distribution of two separate templates and genuine-impostor distribution, as presented in Figure 8. The Figure 8 shows that the genuine and impostor distributions have high overlap, making it impossible for the attacker to link the template to a service.

5.4.1 | Unlinkability of protected templates

With the compromise of biometric templates, it must be ensured that the template cannot be linked to other biometric

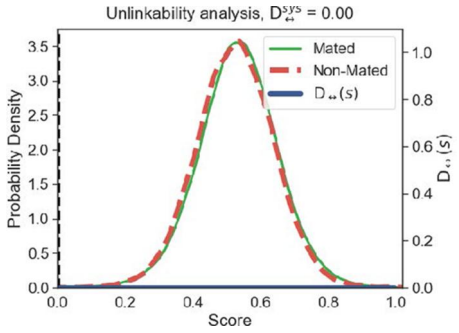

FIGURE 9 Unlinkability of protected templates ($q = 256$) with pseudouser auxiliary enrolment data

services. We achieve unlinkability through private key embedding, as given in Equation (6), in which the templates are based on keys. These keys are used to generate the random distributed binary matrix before optimizing the hash function. With this background, we present an experimental evaluation of the unlinkability of the templates generated using two separate keys. The results are presented in agreement with a proposed *unlinkability* metric [22, 25], in which the measure is indicated by $D^{sys}_{\leftrightarrow}$, which reports whether it is possible to say with a degree of certainty that two protected templates stem from the same subject. Given two score distributions, one generated by mated comparisons with different private keys and one generated by non-mated comparisons with different keys, the degree of unlinkability is measured depending on the overlap of the distribution. A perfect overlap indicates a fully unlinkable system whereas two disjoint distributions indicate a fully linkable system. For unlinkability, the two measures used are $D_{\leftrightarrow}$ and $D^{sys}_{\leftrightarrow}$, where $D_{\leftrightarrow}$ describes the unlinkability for different score values within the system and $D^{sys}_{\leftrightarrow}$ estimates the overall unlinkability of the system. Thus, the results of *unlinkability* analysis is presented by the score distribution of two separate templates and genuine-impostor distribution, as presented in Figure 8. Figure 8 shows that the genuine and impostor distributions have high overlap, making it impossible for the attacker to link the template across different services. Also, the template protection scheme is robust against attacks for both face and periocular images. In addition to the analysis of the template of length $q = 32$, we present the variation in the unlinkability metric $D^{sys}_{\leftrightarrow}$ for different template lengths in Table 3. The metric indicates a low probability of linkability attacks even with the compromise of protected templates.

5.5 | Unlinkability of templates with pseudouser auxiliary data

In the previous analysis, we provided the unlinkability analysis for the known enrolment set to demonstrate the applicability of proposed method. In this section, we present the unlinkability of protected templates at the user level using the strategy presented in Section 2.4. For the sake of simplicity, we present the unlinkability analysis of protected templates for face templates with $q = 256$, as seen in Figure 9, in which $D^{sys}_{\leftrightarrow} = 0$ indicates near ideal unlinkability. The obtained unlinkability indicates suitability for the application of the proposed approach in real scenarios of biometrics.

6 | CONCLUSIONS

BTP is crucial for the success and adoption of biometrics in various applications because of the sensitivity of the biometric data. While keeping the performance of biometric system at par without protected templates, one has to ensure that a strong template protection scheme will provide *irreversibility*, *unlinkability* and *renewability*. We have presented a framework for generating biometric templates using semantic label-assisted discrete hashing. Experimental trials on different modalities including the face and periocular region indicated promising recognition performance of the proposed approach, resulting in a GMR ≈100% at an FMR = 0.01% (Table 2) for the face. The templates can vary in length and the performance is not compromised even under different compact lengths of templates. The proposed template protection scheme is antagonistic to the size of filters in feature extraction, indicating stable performance. With a new strategy of pseudouser auxiliary enrolment set, we have also demonstrated scalability at user level template protection for applicability in a real biometric scenario.

ORCID

Kiran Raja https://orcid.org/0000-0002-9489-5161
Christoph Busch https://orcid.org/0000-0002-9159-2923

END NOTS

[1] The approach can be used with any chosen filter and the configurations do not have major performance variations, as illustrated with the experimental evaluation in Section 4.3.3.

[2] The binary semantic similarity matrix is constructed for known enrolment samples with manual effort. The semantic label matrix for a specific enrolment sample is a set of ones whereas the semantic label matrix for all other samples, excluding the one considered for hash learning, is set to 0.

[3] The experimental results are provided with single key and dual key-based approaches in the Supporting Information Materials (Figure A.1.9). Although the single key achieves good biometric performance, the dual key-based proposed approach induces high randomness and thus low linkability, as observed in the Supporting Information Materials (Figure A.1.8).

[4] The number of independent filters can be chosen to be specific to the application, as noted in Section A.1.4 in the Supporting Information Materials, as long as the extracted feature length is larger than length of intended protected templates.

[5] The length of the bits can be further changed if needed.

[6] The results can be visualized in Supporting Information Materials in Figures S6 and A.1.5 accompanying results presented in Table 2.

[7] Higher GMR and lower EER are obtained on different template lengths (q); however, because of limited space, all results are not presented here.

[8] Alternatively, Figure A.1.10 presents the measured entropy for templates created using the proposed approach.

REFERENCES

1. ISO/IEC JTC1 SC27 Security Techniques: ISO/IEC 24745:2011. information technology—security techniques—biometric information protection. (2011)

2. European Council: Regulation of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation). (2016)
3. Uludag, U., et al.: Biometric cryptosystems: issues and challenges. Proc IEEE. 92(6), 948–960 (2004)
4. Ratha, N.K., Connell, J.H., Bolle, R.M.: Enhancing security and privacy in biometrics-based authentication systems. IBM Syst. J. 40(3), 614–634 (2001)
5. Ratha, N.K., et al.: Generating cancelable fingerprint templates. IEEE Trans. Pattern Anal. Mach. Intell. 29(4), 561–572 (2007)
6. Pillai, J.K., et al.: Secure and robust iris recognition using random projections and sparse representations. IEEE Trans. Pattern Anal. Mach. Intell. 33(9), 1877–1893 (2011)
7. Patel, V.M., Ratha, N.K., Chellappa, R.: Cancelable biometrics: a review. IEEE Signal Process Mag. 32(5), 54–65 (2015)
8. Steennot, R.: Reduced payer's liability for unauthorized payment transactions under the second Payment Services Directive (PSD2). Comput. Law Secur. Rep. 34(4), 954–964 (2018)
9. Jin, A.B., Ling, D.C., Goh, A.: Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recogn. 37(11), 2245–2255 (2004)
10. Rathgeb, C., Breitinger, F., Busch, C.: Alignment-free cancelable iris biometric templates based on adaptive bloom filters. In: 2013 International Conference on Biometrics,Madrid, Spain, 4–7 June 2013
11. Rathgeb, C., et al.: Towards cancelable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris. In: 3rd International Workshop on Biometrics and Forensics (IWBF 2015), Gjovik, Norway, 3–4 March 2015
12. Raja, K.B., Raghavendra, R., Busch, C.: Towards protected and cancelable multi-spectral face templates using feature fusion and kernalized hashing. In: 2018 21st International Conference on Information Fusion (FUSION), pp. 2098–2106. (2018)
13. Raja, K.B., Raghavendra, R., Busch, C.: Anchored kernel hashing for cancelable template protection for cross-spectral periocular data. In: International Conference on Pattern Recognition, pp. 103–116. Springer, Cham (2018)
14. Bringer, J., Morel, C., Rathgeb, C.: Security analysis of bloom filter-based iris biometric template protection. In: 2015 International Conference on Biometrics (ICB), pp. 527–534. IEEE (2015)
15. Gunasinghe, H., Bertino, E.: Privbiomtauth: privacy preserving biometrics-based and user centric protocol for user authentication from mobile phones. IEEE Trans. Inf. Forensics Secur. 13(4), 1042–1057 (2018)
16. Kannala, J., Rahtu, E.: BSIF: binarized statistical image features. In: Proceedings of the 21st International Conference on Pattern Recognition (ICPR2012), pp. 1363–1366. ICPR (2012)
17. Raja, K.B., et al.: Multi-modal authentication system for smartphones using face, iris and periocular. Proceedings of 2015 International Conference on Biometrics, pp. 143–150. ICB (2015)
18. Stokkenes, M., et al.: Multi-biometric template protection—a security analysis of binarized statistical features for bloom filters on smartphones. In: Sixth International Conference on Image Processing Theory, Tools and Applications, pp. 1–6. IEEE (2016)
19. Kang, W.C., Li, W.J., Zhou, Z.H.: Column sampling based discrete supervised hashing. In: Proceedings of the 30th AAAI Conference on Artificial Intelligence, pp. 1230–1236. AAAI (2016)
20. Lin, G., et al.: Fast supervised hashing with decision trees for high-dimensional data. In: 2014 IEEE Conference on Computer Vision and Pattern Recognition, pp. 1963–1970 (2014)
21. Hermans, J., Mennink, B., Peeters, R. 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. IEEE (2014)
22. Gomez-Barrero, M., et al.: Multi-biometric template protection based on bloom filters. Inf Fusion. 42, 37–50 (2018)
23. Phillips, P.J., et al.: Overview of the face recognition grand challenge. In: 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), pp. 947–954. IEEE (2005)
24. Gomez.Barrero, M., et al.: Unlinkable and irreversible biometric template protection based on bloom filters. Inf. Sci. 370–371, 19–32 (2016)
25. Gomez-Barrero, M., et al.: General framework to evaluate unlinkability in biometric template protection systems. IEEE Trans. Inf. Forensics Secur. 13(6), 1406–1420 (2018)

How to cite this article: Raja, K., Raghavendra, R., Busch, C.: Towards better and unlinkable protected biometric templates using label-assisted discrete hashing. IET Biom. 11(1), 51–62 (2022). https://doi.org/10.1049/bme2.12043