Anchored Kernel Hashing for Cancelable Template Protection for Cross-Spectral Periocular Data

Kiran B. Raja[†§]; R. Raghavendra[§]; Christoph Busch[§]

[†]University of South-Eastern Norway (USN), Norway
[§]Norwegian Biometrics Laboratory, NTNU - Gjøvik, Norway
{kiran.raja} @usn.no
{ kiran.raja; raghavendra.ramachandra; christoph.busch} @ntnu.no

Abstract. Periocular characteristics is gaining prominence in biometric systems and surveillance systems that operate either in NIR spectrum or visible spectrum. While the ocular information can be well utilized, there exists a challenge to compare images from different spectra such as Near-Infra-Red (NIR) versus Visible spectrum (VIS). In addition, the ocular biometric templates from both NIR and VIS domain need to be protected after the extraction of features to avoid the leakage or linkability of biometric data. In this work, we explore a new approach based on anchored kernel hashing to obtain a cancelable biometric template that is both discriminative for recognition purposes while preserving privacy. The key benefit is that the proposed approach not only works for both NIR and the Visible spectrum, it can also be used with good accuracy for cross-spectral protected template matching. Through the set of experiments using a cross-spectral periocular database, we demonstrate the performance with $EER = 1.39\%$ and $EER = 1.61\%$ for NIR and VIS protected templates respectively. We further present a set of cross-spectral template comparison by matching the protected templates from one spectrum to another spectra to demonstrate the applicability of the proposed approach.

Keywords: Template protection, cross-spectral periocular recognition, Hashing

1 Introduction

Many of the current day biometric systems are based on the physiological characteristics due to ease of capturing data such as face data in unobtrusive manner. The recent works have investigated the use of periocular region and indicated it's use as a supplementary information [13, 10, 7, 6, 22, 8, 1, 16]. The works have focused on visible spectrum (VIS) periocular recognition, and Near-Infra-Red (NIR) spectrum periocular recognition. A limited number of the recent works have evaluated the cross-spectrum periocular recognition (NIR to Visible spectrum (VIS)) [22, 8, 1].

The variability of the data from NIR and VIS domain introduces a challenge in cross-spectral data verification and this is acknowledged by many existing works, for instance in [22, 8, 1]. An added challenge is to provide a template protection mechanism that can be employed in both the domains. Our key motivation remains that the template protection mechanisms should preserve the privacy of biometric data adhering to recent guidelines enforced by European Union (EU) General Data Protection Regulation (GDPR) 2016/679 [2] which does not discriminate the data from NIR or VIS.

According to guidelines of ISO-24745[3] and GDPR 2016/679 [2], irrespective of the spectrum employed for biometric system , biometric data must be *protected* in a template format where the plain biometric data shall be rendered usable even under the compromise of the entire database. The template protection schemes must also minimize the risks of inverting the templates to biometric raw images adhering to the principles of *irreversibility*. Under the extreme scenarios, the template of same biometric modality from same spectrum or from different spectrum of any compromised database should be rendered unusable to access other services using exactly the same biometric modality. Therefore, it is necessary to make biometric data *unlinkable* irrespective of spectrum employed for same biometric characteristics. While these properties of *irreversibility* and *unlinkability* are accounted for, a biometric system should not compromise in the identification or verification performance, even under the challenging conditions of highly varying data due to cross-spectrum comparison(NIR versus VIS). An inherent need therefore is to preserve the *privacy* of the subject while operating with pre-determined performance of biometric system without any *template protection* mechanisms. Summarizing, the challenge therefore is to protect the data not only in one particular domain (NIR or VIS), but also to maintain the sensitiveness and privacy of biometric data across domains while providing optimal biometric recognition performance.

Motivated by such arguments provided above, in this work, we investigate the template protection scheme that can be adapted across spectrum and provide good comparison performance. To the best of our knowledge, there are no reported works that have provided the template protection schemes for biometric data captured across spectrum. Further, we limit our work to explore the problem in a *closed set biometric system* where the enrolment data of all users in database is known. *The apriori assumption thus remains our primary argument to employ data-dependent hashing to derive protected template.* It has to be noted that there exist a number of data-dependent and data-independent schemes in the earlier works that have been explored for a single spectrum template protection in earlier works. The template protection mechanisms can be classified under (1) biometric cryptosystems [23] and, (2) cancelable biometrics based systems [18], [17], [15], [14],[19], [20],[5], [14].

In this work, we present a new approach for biometric template protection that is *designed for closed set biometric system (i.e., known subjects and enrolment dataset) but independent of spectrum (VIS - NIR).* The approach is based on deriving the protected templates using the data-dependent hashing approach while introducing the cancelability through the use of randomly chosen anchor points. The key feature relies on employability of anchor points for hashing from one particular spectrum (for e.g, VIS spectrum) to data captured in other spectrum. The hashing approach is further supplemented through the kernalization to maximize the separability of hashed templates for two different subjects (inter-subject) while minimizing the distance of hashed templates stemming from same subject (intra-subject). Given the *apriori* known enrolment set (i.e., closed set), we adopt supervised hashing approach to optimize the biometric performance while maintaining the properties of ideal template protection. Further, to validate the applicability of the proposed approach, we present set of results on a recent large scale cross-spectral periocular dataset - Cross-eyed database which consists of periocular images corresponding to 120 subjects (240 unique periocular instances) captured in both NIR and VIS spectrum.

Our contributions from this work can thus be listed as below:

1. Presents a novel approach of cancelable biometric template protection using anchored points and kernalized hashing that can be employed across different spectrum such as NIR and VIS.
2. Demonstrates the use of anchor point based hashing as a mode of achieving cancelability for template protection. The approach is demonstrated to work for both NIR and VIS spectrum template protection.
3. Presents an experimental evaluation of new template protection approach on a large scale closed-set cross-spectral periocular database. To the best of our knowledge, this is the first work attempting at cross-spectral template protection. The obtained results exemplify the performance of the template protection scheme which achieves the performance comparable to unprotected biometric system.

In the remainder of this article, Section 2 describes the proposed biometric template protection system and Section 3 presents the experiments including a brief discussion of the database in Section 3.1. Section 4 presents the concluding remarks and lists potential future work.

2 Proposed Biometric Template Protection

The proposed framework consists of extracting the features from the given periocular image followed by protected template creation as shown in Figure 1. Binarized Statistical Image Features (BSIF) are extracted from each periocular image using a set of filters which serve as unprotected features. These biometric features from the enrolment database is used to learn the hash projection function using anchored kernels. Through the randomly chosen anchor points, the proposed approach obtains the cancelable biometric template for a given biometric image. In the similar manner, the learned hash function is used to transform the biometric features emerging from the probe attempts to obtain the cancelable protected templates. The protected templates are further used in biometric pipeline for verification where they are compared using simple Hamming distance to obtain the comparison score. The obtained comparison score for a particular probe attempt determines the acceptance or rejection of the attempt by the system. Each of the individual step in the proposed framework is provided in the section below.

2.1 Multi-scale Fused BSIF Features

Given the biometric image (periocular image), the first step is to extract the features. We employ multi-scale fused feature representation which consists of the texture features extracted using Binarized Statistical Image Features (BSIF) owing to high performance reported earlier on this database [22]. The textural features are extracted using a set of

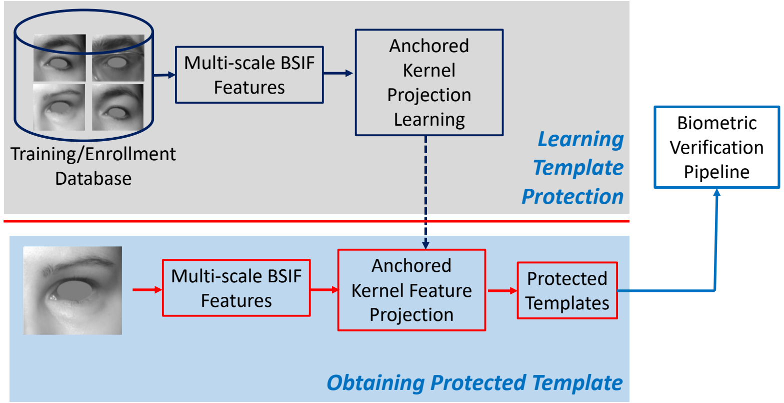
Training/Enrollment Database
Multi-scale BSIF Features
Anchored Kernel Projection Learning
Learning Template Protection
Biometric Verification Pipeline
Multi-scale BSIF Features
Anchored Kernel Feature Projection
Protected Templates
Obtaining Protected Template

Fig. 1: Schematic of the proposed template protection scheme in closed-set biometric verification pipeline.

filters that provide holistic, multi-feature and multi-level feature representation. Following the earlier works [22, 8], we employ BSIF filters of size 9×9, 11×11, 13×13, 15×15, 17×17 with a bit size of 11 leading to 2048 levels of the histogram features. The features are represented as f_1, f_2, f_3, f_4 and f_5 corresponding to 5 different filters respectively. In order to reduce the difference between the features of images of same person and increase the difference between images of different persons, we employ feature fusion leading to a total number of 10240 features for each image. The equivalent representation of the fused features is given by $\mathfrak{f} = \{f_1|f_2|f_3|f_4|f_5\}$ where $|$ operator represents the fusion of the individual histogram features obtained from different filters.

2.2 Anchored Kernel Hash Function

Given the features $\mathfrak{f}$ of an image in an enrolment database of l subjects, to obtain the unique templates, we need to derive r hash functions resulting in r bit representation. Thus, the objective is to learn r hash functions $\{h_k\}_{k=1}^{r}$ for r hash bits given $\mathbf{X}_l$. If $\mathbf{X}_l$ is l labelled samples $\{x_1, x_2, \ldots x_l\}$, the similarity label matrix can be represented by $\mathbf{S}_{ij} = 1$ for $i = j$ and $\mathbf{S}_{ij} = -1$ for $i \neq j$ where i and j are biometric samples. The goal in obtaining the unique hash functions can therefore be interpreted as learning hash function H such that:

$$\begin{aligned} \mathbf{S}_{ij} = 1, D_H(x_i, x_j) = 0 \\ \mathbf{S}_{ij} = -1, D_H(x_i, x_j) \neq 0 \end{aligned} \tag{1}$$

Where $D_H(x_i, x_j)$ is the Hamming distance between hash of two templates $H(x_i)$ and $H(x_j)$, assuming the binary representation of the biometric templates. The practical implication for a system operating on r binary bits is that when $\mathbf{S}_{ij} = -1$, the Hamming distance $D_H(x_i, x_j) \rightarrow r$ as theoretically there can be r differing bits. The generalized conclusion of this observation leads to the fact that the distance between two dissimilar hash of r bits is r [11]. The goal of learning hash representation is therefore to minimize the distance between two hash functions ($= 0$ in ideal case) and maximize the distance between the dissimilar biometric templates ($= r$ for r bit hash representation). One method to achieve such a goal can be through kernalized representation as suggested by [11] which helps in maximizing the Hamming distance between two dissimilar hash and minimizing Hamming distance between two similar hash through employing the inner product as described in earlier work [11]. We therefore adopt the approach of kernalized representation in this work. The Hamming distance between two templates can further be represented as inner product given by $\odot$:

$$H(x_i) \odot H(x_j) = H(x_i)H^T(x_j) \tag{2}$$

where $H(x_i)$ and $H(x_j)$ are hash of two templates.

For a hash representation of r bits, the problem of obtaining best hash codes in a similarity space S can be given as an optimization problem as given by Eqn. 3 [1].

$$\underset{H_l \in -1,1^{l \times r}}{\text{minimize}}\, Q = \left|\left|\frac{H(x_i)H^T(x_j)}{r} - S\right|\right|_F^2 \tag{3}$$

where $||.||_F^2$ represents the Frobenius norm. For a r bit hash code of sample $[h_1(x), h_2(x) \ldots h_r(x)] \in \{1, -1\}^{l \times r}$ for l subjects. The matrix representation of kernalized hashes can be given as:

$$\begin{bmatrix} h_1(x_1)\ h_2(x_1), \ldots\ h_r(x_1) \\ h_1(x_2)\ h_2(x_2), \ldots\ h_r(x_1) \\ \ldots \\ h_1(x_l)\ \ h_2(x_l),\ \ldots\ h_r(x_l) \end{bmatrix} \tag{4}$$

The representation in Eqn.4 can be rewritten as 5 using a set of anchors[11]:

$$\begin{aligned} h_k(x) &= sgn \sum_{j=1}^{m} (k(x_j, x)a_{jk}) \\ &= sgn(\mathbf{k}^T(x)a_k) \end{aligned} \tag{5}$$

where m is the number of anchors chosen from the dataset and $k(x)$ is a kernel function. Considering the Equation 3 and Equation 5, the optimization can be written as:

$$\begin{aligned} \min_{H_l \in -1,1^{l \times r}} Q &= \left|\left|sgn(K_l A)(sgn(K_l A))^T - rS\right|\right|_F^2 \\ &\approx -2sgn(K_l a_k)(sgn(K_l a_k))^T R_{k-1} \end{aligned} \tag{6}$$

The solution of the Equation 6 is provided through Spectral Relaxation and Sigmoid Smoothing as proposed in [11]. As it can be noted from the Equation 5, the use of anchor points provide a basis for the *Anchored Kernel Hashing* [12] which forms the basis for our template extraction framework.

[1] For the sake of simplicity, the detailed derivations of the problem is not presented here. The reader if further referred to [11] and [9] for details.

2.3 Cancelability Through Random Anchors

In order to satisfy the cancelability property, we choose the anchor points corresponding to a specific application where randomized anchors are used for kernel representation as given by Equation 7. The anchor points for m points are chosen according to a specific application or database, for example specific application s_1 or specific application s_2, generally represented by $\mathfrak{s}$. Thus, the anchor points a is replaced by $a^{\mathfrak{s}}$.

$$h_k(x) = sgn \sum_{j_s=1}^{m} (k(x_j, x) a^{\mathfrak{s}}_{jk}) \tag{7}$$

In practicality, choosing these anchor points can be a challenge to make the templates cancelable and therefore, in this work we propose to choose the anchor points based on a subset of samples corresponding to randomly chosen users which reduces the chances of guessability. The underlying argument for the low chances of guessability is that there can be a number of combinations to select the subset of users x in larger sample set X (also, enrolment set). The set of hash function is finally used to transform the unprotected biometric features x to hashed representation x^h simply by employing the following transformation: $x^h = x * H^T$.

2.4 Protected Template Comparison in Same Spectrum

Given a protected biometric reference template corresponding to ${}_{nir}x_r^h$ and the biometric probe template ${}_{nir}x_p^h$ in NIR domain, the Hamming distance between the two biometric templates is computed through measuring the number of differing bits as compared to total number of bits. The obtained Hamming distance $D({}_{nir}x_r^h,{}_{nir} x_p^h)$ is considered as the biometric comparison score.

In the similar manner, given a protected biometric reference template corresponding to ${}_{vis}x_r^h$ and the biometric probe template ${}_{vis}x_p^h$ in VIS domain, the Hamming distance between the two biometric templates is computed through Hamming distance $D({}_{vis}x_r^h,{}_{vis} x_p^h)$ is considered as the biometric comparison score.

2.5 Protected Template Comparison in Cross-Spectrum

In alignment with the motivation of this article, we intend to perform the cross-spectral template comparison in protected domain. Thus, given a protected biometric reference template corresponding to ${}_{vis}x_r^h$ from visible domain and the biometric probe template ${}_{nir}x_p^h$ in NIR domain, the Hamming distance between the two biometric templates is computed through Hamming measure $D({}_{vis}x_r^h,{}_{nir} x_p^h)$ is considered as the biometric comparison score.

3 Experiments and Results

This section presents the database, evaluation protocols and the obtained results using the proposed approach. The proposed approach is also compared against the performance of unprotected template comparison.

Table 1: Details of the cross-spectrum periocular image database

Camera	Subjects	Unique Eye	Samples	Total
(Spectrum)	Subjects	Instances	per Instance	images
NIR - Camera	120	240	8	1920
Visible Camera	120	240	8	1920

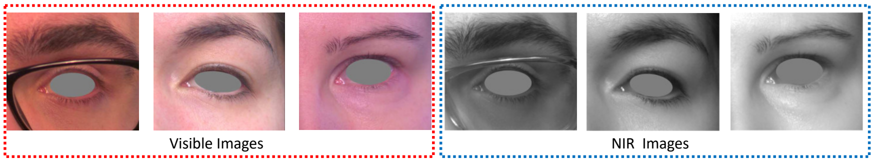

Fig. 2: Sample images from Cross-Eyed periocular subset. Note that the iris and sclera portions of images are masked by the providers of database.

3.1 Cross-spectral Periocular Database

This section presents the details of the database employed in this work for the purpose of evaluating the proposed biometric template protection method. *Reading Cross-Spectral Periocular Dataset* (*Cross-Eyed*) [21][2], was used to benchmark the proposed approach with template protection and the same cross-spectral biometric verification system without template protection. The dataset consists of periocular images captured in both VIS and NIR domain with a custom developed dual spectrum imaging sensor. The unique property of the images in this dataset is that they are captured at the same time through mirror splitting of the images resulting in minimal changes in pairs of NIR-VIS images. The database consists of 120 subjects in total from various nationalities and ethnicities. For each of the 120 subjects, 8 images are captured from eyes in VIS and NIR spectra and the complete distribution of the images are given in the Table 1. A set of sample images from the database are presented in Figure 2.

3.2 Database division

In order to evaluate the proposed approach, we divide the database in three parts constituting *development*, *testing set-1* and *testing set-2* with disjoint subjects and images. The distribution of the database subset is provided in the Table 2. We employ the *development set* consisting of 10 subjects (20 unique periocular instances, a total of 320 samples) to derive the optimal parameters for the hashing approach, number of anchor point and to tune the parameters of the kernalization. The *testing set-1* corresponds to dataset of 20 subjects which is used to validate the parameters obtained for the proposed approach. Finally, the performance of the proposed approach is reported using the *testing set-2* which consists of images from the rest of the 90 subjects who are not present within the development set or testing set-1.

[2] Available by request at www.crosseyed.eu.

Table 2: Division of the database for the experimental validation. The development database is employed for choosing the parameters of the hashing approach, number of anchor point and to tune the parameters of the kernalization.

Description	Development*	Testing Set-1	Testing Set-2
	(Parameter Selection)	(Parameter Validation)	(Performance Evaluation)
Number of Subjects (NIR)	10	20	90
Number of Subjects (VIS)	10	20	90
Number of Unique Ocular Images			
VIS	20	40	180
NIR	20	40	180
Number of samples per eye instance	8	8	8
Total images (NIR)	160	320	1440
Total images (VIS)	160	320	1440

3.3 Performance metrics

As the focus of the current work is to measure the performance of the proposed approach to protect the biometric templates and to provide robust performance, we present the results in two different terms. To denote the robustness in terms of dealing with symmetrical errors of False Accepts and False Rejects, we present the Detection Error Trade-off (DET) which presents the False Accept Rate (FAR) against False Reject Rate (FRR). In order to complement the DET, we also present the Equal Error Rate (EER). The performance is also provided in terms of Genuine Match Rate (GMR) versus False Match Rate (FMR) which is derived on the basis of False Match Rate (FMR) and the False Non-Match Rate (FNMR)[4]. Higher values of GMR at a specified FMR indicate superior recognition accuracy at verification. The GMR is defined using False Non Match Rate (FNMR) (%) at a given False Match Rate (FMR) and is given by:

$$GMR = 1 - FNMR$$

3.4 Experimental Settings

This section presents the specific details of the settings employed in this work for the evaluation. All the periocular images are resized to a common size of 128×128 pixels for the sake of computational complexity. Further, to derive the unprotected and also protected templates, we employ BSIF histograms extracted using 9×9, 11×11, 13×13, 15×15, 17×17 with a bit size of 11 leading to 2048 levels of the histograms. In order to derive the optimal setting for kernels, anchors and hashing, we employ the specific parameter as follows: number of anchor points equal to 100 ($\approx> (number - of - subjects)/2$), kernel - exponential kernel based on the Hamming distance.

3.5 Experiments and Results

In this section, we present the experiments conducted in two specific parts which correspond to unprotected biometric template verification and protected biometric template verification. Further, for the case of protected template verification, we present three cases of protected template verification corresponding to NIR spectrum alone, VIS spectrum alone, NIR versus VIS templates. All the experiments correspond to closed-set verification where the enrolment samples are available prior hand to derive the hash projection and protected templates for enrolment set. We specifically follow three protocols for three separate cases: (1) NIR data alone (2) VIS data alone (3) NIR versus VIS data. In each of these cases, we employ first 4 images for enrolment set and rest of the 4 images for probe set.

Unprotected Biometric Verification Performance Considering the biometric system has no template protection mechanism in-place, we employ the BSIF histograms and χ^2 distance to obtain the performance of unprotected templates [8]. The results from the obtained experimental evaluation on *testing set-2* is presented in the Table 3 for VIS templates and Table 4 for NIR templates. [3] As seen from the results, it can be noted that the EER obtained for NIR and VIS image unprotected comparison results in EER equalling to 2.51% and 2.05% respectively. We also present the unprotected biometric performance when NIR data is enrolled and VIS data is probed in Table 5. As it can be noted, the challenging nature of cross-spectral data verification can be seen from EER equalling to 10.18%.

Schemes	Verification Accuracy	
	EER	GMR @ FMR=0.01%
Unprotected	2.05	96.63
Protected	**1.61**	**93.33**

Table 3: Verification - VIS images

Schemes	Verification Accuracy	
	EER	GMR @ FMR=0.01%
Unprotected	2.51	96.89
Protected	**1.39**	**93.09**

Table 4: Verification - NIR images

Table 5: Verification performance of cross-spectrum (NIR v/s VIS) image comparison for various algorithms

Schemes	Verification Accuracy	
	EER	GMR @ FMR=0.01%
Unprotected	**10.18**	**17.80**
Protected	13.32	11.07

[3] It has to be noted that the performance reported here cannot be directly compared with performance reported earlier due to changes in number of images in enrolment and probe set. A slight change in the performance can be observed as compared to earlier reported results.

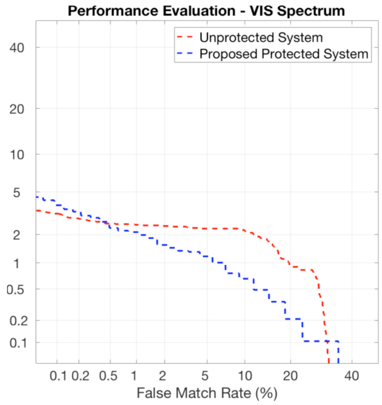

Fig. 3: VIS Templates

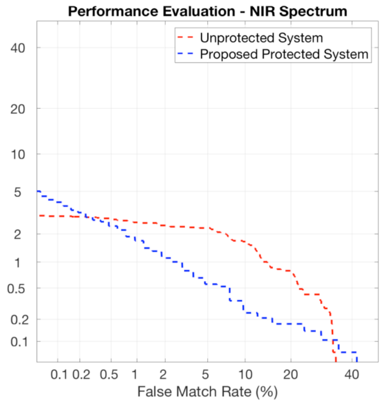

Fig. 4: NIR Templates

Cross-spectral Protected Template Comparison Further, Table 5 and Table **??** presents the results of protected templates when NIR templates are compared against VIS in protected domain.

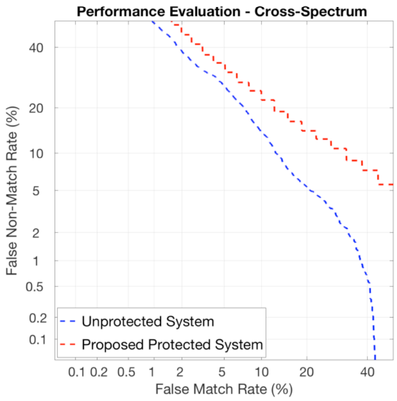

Fig. 5: NIR versus VIS

Protected Biometric Verification Performance This section presents the results and analysis with the proposed template protection scheme. Along the lines of unprotected template comparison, we present the results for NIR template verification alone, VIS template verification alone and NIR versus VIS template verification. The results of the protected templates using the proposed approach is presented in Table 4 for NIR spectrum and in Table 3 for VIS spectrum which correspond to an EER of 1.61% and 1.39% indicating the applicability of the proposed approach. The obtained results are highly comparable to templates without any protection. One can note a slight performance improvement in protected template performance and this is mainly due to optimized hash representation for the closed set of enrolment templates. The DET curves for the experimental evaluation can be seen in Figure 4 and 3.

Similarly, we also validate the proposed approach for protected template comparison for cross-spectral template protection as indicated in Table 5 and correspondingly DET presented in Figure 5. It can be noted that the protected template comparison from NIR against VIS data results in a degraded performance. This is in-line with the unprotected data comparison from NIR to VIS data which is already a challenging task. We provide the arguments for performance in the section below.

3.6 Discussion

The set of observations from the experimental results are listed herewith:

- It can be observed from the obtained results, the proposed approach of template protection is agnostic of the spectrum, i.e., can be used for NIR or VIS spectrum. The template protection scheme performs with better accuracy that is comparable to unprotected templates when both enrolment and probe data emerge from the same spectrum in the closed-set. This can be attributed to optimized hash representation for closed-set enrolment data.
- However, the challenge of verifying the templates from NIR against VIS can be evidently seen with the drop in performance, both in protected and unprotected domain. The performance degradtion is seen in both the cases with a very high EER.
- Although the EER is reasonably high (10.18%, 13.32% for unprotected and protected template comparison respectively), the GMR in the cross-spectral comparison of both unprotected and protected data are very low indicating the need for robust methods and further investigations.

Potential future works can investigate on joint template learning using both NIR and VIS images so that common features across both domain are identified. Another direction is to adapt the approach from closed-set biometric system to open-set biometric system. This implies investigating data-independent template protection mechanisms that can be used in both spectrum and cross-spectrum biometric systems.

4 Conclusion

Template protection in biometric applications are important to preserve the privacy and sensitiveness of the biometric data. The challenge in cross-spectral applications is that they provide different kind of data and thus, a common template protection algorithm may not work for optimally for both NIR and VIS spectrum. Further, it is necessary to obtain good biometric performance even when the templates are compared from different spectrum. In this work, we have presented a new template protection technique based on anchored kernel hashing which works for data from both VIS and NIR spectrum. The proposed approach being highly cancelable, provides privacy protection for biometric templates. The detailed set of experiments on the large scale cross-spectral biometric dataset has demonstrated promising results for template protection for both NIR and VIS spectrum. The obtained protected templates using the proposed approach have provided a performance of EER lesser than 2% for both VIS and NIR spectrum data indicating the applicability of anchored kernel hashing. The limited applicability is also demonstrated for cross-spectral protected template verification which reflected the need for further investigations.

Future works in this direction include in evaluating the strengths of proposed privacy preserving template protection schemes by incorporating new security and privacy analysis. Another future work can be in the direction of open-set biometric data where the enrolment images are not available while learning the hashing space. The scalability of proposed approach can be evaluated for handling the changes due to open-set data or unconstrained data for template protection, especially in cross-spectral imaging scenario.

Acknowledgement

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

References

1. Alonso-Fernandez, F., Mikaelyan, A., Bigun, J.: Comparison and fusion of multiple iris and periocular matchers using near-infrared and visible images. In: Biometrics and Forensics (IWBF), 2015 International Workshop on. pp. 1–6. IEEE (2015)
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) (April 2016)
3. ISO/IEC JTC1 SC27 Security Techniques: ISO/IEC 24745:2011. information technology - security techniques - biometric information protection (2011)
4. ISO/IEC TC JTC1 SC37 Biometrics: ISO/IEC 19795-1:2006. Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework. International Organization for Standardization and International Electrotechnical Committee (Mar 2006)
5. Jin, A.T.B., Ling, D.N.C., Goh, A.: Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern recognition **37**(11), 2245–2255 (2004)
6. Kiran B. Raja, Raghavendra, R., Busch, C.: Binarized statistical features for improved iris and periocular recognition in visible spectrum. In: Proc. IWBF. pp. 1–6 (2014)
7. Kiran B. Raja, Raghavendra, R., Busch, C.: Collaborative representation of deep sparse filtered feature for robust verification of smartphone periocular images. In: 23rd IEEE International Conference on Image Processing (ICIP 2016). pp. 1 –5 (Oct 2016)
8. Kiran B. Raja, Raghavendra, R., Busch, C.: Cross-spectrum periocular authentication for nir and visible images using bank of statistical filters. In: Imaging Systems and Techniques (IST), 2016 IEEE International Conference on. pp. 227–231. IEEE (2016)
9. Kiran B. Raja, Raghavendra, R., Busch, C.: Towards protected and cancelable multi-spectral face templates using feature fusion and kernalized hashing. In: International Conference on Information Fusion (IFIP-FUSION). pp. 1–8. IEEE (2018)

10. Kiran B. Raja, Raghavendra, R., Stokkenes, M., Busch, C.: Smartphone authentication system using periocular biometrics. In: 2014 International Conference on Biometrics Special Interest Group. pp. 27–38. IEEE (2014)
11. Liu, W., Wang, J., Ji, R., Jiang, Y.G., Chang, S.F.: Supervised hashing with kernels. In: Computer Vision and Pattern Recognition (CVPR), 2012 IEEE Conference on. pp. 2074–2081. IEEE (2012)
12. Liu, W., Wang, J., Kumar, S., Chang, S.F.: Hashing with graphs. In: Proceedings of the 28th international conference on machine learning (ICML-11). pp. 1–8. Citeseer (2011)
13. Park, U., Ross, A., Jain, A.K.: Periocular biometrics in the visible spectrum: A feasibility study. In: 3rd IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS'09). pp. 1–6 (2009)
14. Patel, V.M., Ratha, N.K., Chellappa, R.: Cancelable biometrics: A review. IEEE Signal Processing Magazine **32**(5) (2015)
15. Pillai, J.K., Patel, V.M., Chellappa, R., Ratha, N.K.: Secure and robust iris recognition using random projections and sparse representations. IEEE transactions on pattern analysis and machine intelligence **33**(9), 1877–1893 (2011)
16. Raghavendra, R., Kiran B. Raja, Yang, B., Busch, C.: Combining iris and periocular recognition using light field camera. In: 2nd IAPR Asian Conference on Pattern Recognition (ACPR2013). IEEE (2013)
17. 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 (2007)
18. 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)
19. Rathgeb, C., Breitinger, F., Busch, C.: Alignment-free cancelable iris biometric templates based on adaptive bloom filters. Proceedings - 2013 International Conference on Biometrics, ICB 2013 (2013). https://doi.org/10.1109/ICB.2013.6612976
20. Rathgeb, C., Gomez-Barrero, M., Busch, C., Galbally, J., Fierrez, J.: Towards cancelable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris. In: 2015 IWBF. pp. 1–6 (March 2015). https://doi.org/10.1109/IWBF.2015.7110225
21. Sequeira, A.F., Chen, L., Wild, P., Radu, P., Ferryman, J.: Cross-Eyed: Reading Cross-Spectrum Iris/Periocular Dataset (2016), www.crosseyed.eu
22. Sequeira, A., Chen, L., Wild, P., Ferryman, J., Alonso-Fernandez, F., Raja, K.B., Raghavendra, R., Busch, C., Bigun, J.: Cross-eyed-cross-spectral iris/periocular recognition database and competition. In: Biometrics Special Interest Group (BIOSIG), 2016 International Conference of the. pp. 1–5. IEEE (2016)
23. Uludag, U., Pankanti, S., Prabhakar, S., Jain, A.K.: Biometric cryptosystems: issues and challenges. Proceedings of the IEEE **92**(6), 948–960 (2004)