Biometric Symmetry: Implications on Template Protection

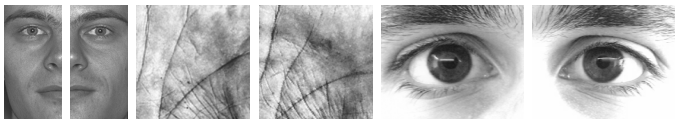
M. Gomez-Barrero*, C. Rathgeb*, K. B. Raja†, R. Raghavendra†, C. Busch*
*da/sec - Biometrics and Internet Security Research Group, Hochschule Darmstadt, Germany
Email: {marta.gomez-barrero,christian.rathgeb,christoph.busch}@h-da.de
†Norwegian Biometrics Laboratory, NTNU, Gjøvik, Norway
Email: {kiran.raja,raghavendra.ramachandra}@ntnu.no

***Abstract*—In the past, many efforts have been directed to develop biometric template protection schemes to guard biometric reference data, i.e. templates. One fundamental premise in the design of such schemes is that the average entropy of the templates should be maximised in order to improve the level of protection. In parallel, several works have addressed the difficult problem of measuring the average entropy of biometric characteristics. However, the impact of the correlation present in different regions of a single biometric characteristic (e.g., left and right part of the face) or within two instances of a single subject (e.g., left and right palmprints) on the joint entropy of a multi-biometric template has been overlooked os far. In this paper, we address this issue and propose a way to measure such correlation from an information theoretical perspective. We then apply the proposed measure to a particular case study based on periocular biometrics, using the MobBIO database. The results show that up to 70% of the information comprised in both periocular regions of a given subject is correlated. Finally, we analyse the implications of such average mutual information loss on biometric template protection schemes.**

I. Introduction

The continuously increasing deployment of biometric recognition systems in the past decades has raised some privacy concerns regarding the storage and use of biometric data. Whereas PINs or passwords may be replaced in case of leakage or theft, the link between individuals and their biometric characteristics, e.g. fingerprints or iris, is strong and permanent. As a consequence, biometric templates need to be protected in order to safeguard individuals' privacy and biometric systems' security. In particular, the activities of a given subject can be tracked without consent if unprotected biometric templates are stored in different databases, or presentation attacks can be launched employing specific inversion techniques [1], [2], [3].

In order to tackle those security and privacy issues, different *biometric template protection* (BTP) schemes have been proposed in the recent past [4], [5]. These systems are designed to meet two major requirements of biometric information protection, as established in the ISO/IEC IS 24745 [6]: i) *irreversibility*: knowledge of a protected template can not be exploited to reconstruct a biometric sample which allows a positive verification of the subject; and ii) *unlinkability*: different versions of protected biometric templates can be generated based on the same biometric data (renewability), while protected templates should not allow cross-matching.



(a) (b) (c) (d) (e) (f)

Fig. 1. Examples of biometric symmetry: (a) right and (b) left sides of the face [9], (c) right and (d) left palmprint [10] (e) right and (f) left periocular regions [11].

In addition to satisfying these main properties, an ideal BTP scheme shall not cause a decrease in biometric performance (i.e., recognition accuracy) or verification speed with respect to the corresponding unprotected system [4]. However, in spite of the efforts directed to developing such systems, to date the vast majority of the proposed approaches does not meet the aforementioned requirements in practice, mostly resulting in a trade-off between privacy protection and biometric performance. To overcome this issue, the incorporation of multiple biometric sources to BTP schemes has recently received significant attention [7]. Such multi-biometric template protection schemes have been found to improve biometric performance [7]. However, the protection of multi-biometric templates is especially crucial, as they contain information regarding multiple characteristics of the same subject [8].

In contrast to conventional biometric systems, where fusion may take place at score or decision level [12], feature level fusion has been identified as the most suitable for BTP schemes. This is due to the fact that a separate storage of two or more protected biometric templates would enable parallelized attacks. On the other hand, a single protected template including the information extracted from two or more characteristics is expected to improve privacy protection, since the fused template is expected to comprise more information [8]. This is analogous to an access control system which requires multiple low strength (few bits) keys, where each key can be attacked individually. Such a system is less secure than one which uses a single key with a larger number of bits.

To maximise the verification accuracy, uncorrelated characteristics should be fused in a multi-biometric system. In this regard, some biometric characteristics have been found to be uncorrelated, e.g. the left and right iris patterns of a subject [13]. However, as shown in Fig. 1, due to the natural symmetry, which we refer to as *biometric symmetry*, some biometric characteristics are expected to exhibit significant correlation

ISBN 978-0-9928626-7-1

within the extracted template itself (e.g., left and right half of a subject's face image) or across multiple templates (e.g. left and right palmprint of a single subject [14]). Focusing on multi-biometric template protection, compact templates revealing high entropy are desired [4]. Hence, the use of symmetric biometric sources might have a severe impact on information protection due to a loss of average entropy of the fused template with respect to the ideal fusion based on uncorrelated characteristics. Whereas some techniques have been proposed to exploit such symmetry to increase verification accuracy [15], this issue is frequently ignored in existing approaches to multi-biometric template protection.

In this paper we provide a theoretical analysis of the aforementioned issue caused by biometric symmetry from an information theory perspective, and focus on quantifying its impact on the biometric information of the fused template (Sect. II). Furthermore, we provide a case study in which we empirically quantify the correlation caused by biometric symmetry (Sect. III). This case study is conducted for left and right periocular regions of single subjects, i.e., the externally visible skin regions of the face that surround the eye sockets. Periocular biometric recognition is of particular interest since it represents an emerging biometric technology, which has been recently used in diverse fields, such as surveillance or mobile applications [16]. Based on the obtained results, we provide a thorough discussion on potential implications of biometric symmetry on (multi-)biometric template protection schemes, Finally, according conclusions are drawn (Sect. IV).

II. Biometric Information and Symmetry

The term *biometric information* is defined as "the decrease in uncertainty about the identity of a person due to a set of biometric measurements" in [17]. Since for a given biometric characteristic, different systems compare different sets of features, the problem of determining the amount of information contained in a specific biometric characteristic is a complex one: the question ultimately depends on the selected feature representation of the biometric data and the comparison algorithm used [18]. In fact, a considerable effort has been directed to solve this problem [17], [18], [19], [20].

It was shown in [20] that the decrease in the uncertainty about the identity of an unknown biometric characteristic can be formulated in terms of mutual information:

$$I\left(Y;X\right)=H\left(X\right)-H\left(X|Y\right) \tag{1}$$

where $H\left(X|Y\right)$ is the conditional entropy, i.e., uncertainty of X after the observation of Y. In addition, the authors show that $I\left(X;Y\right)$ can be approximated by the Kullback-Leibler divergence of the mated $p_m\left(s\right)$ and non-mated $p_{nm}\left(s\right)$ score probability distributions, where $\left\{s^1,\ldots,s^N\right\}$ denotes the mated and non-mated observed scores:

$$I\left(X;Y\right)\approx D_{KL}\left(p_m\|p_{nm}\right)=\sum_{i=1}^{N}p_m\left(s^i\right)\log_2\left(\frac{p_m\left(s^i\right)}{p_{nm}\left(s^i\right)}\right) \tag{2}$$

The problem now lies on how to model the probability densities from a limited number of scores. To that end, a Nearest Neighbor (NN) estimator can be used to calculate the value of $D_{KL}\left(p_m\|p_{nm}\right)$ from the mated and non-mated scores, without computing any probability models [19]. Let $\left\{s_m^1,\ldots,s_m^{N_m}\right\}$ and $\left\{s_{nm}^1,\ldots,s_{nm}^{N_{nm}}\right\}$ be i.i.d. samples drawn from the mated and non-mated densities $p_m\left(s\right)$ and $p_{nm}\left(s\right)$, respectively (i.e., the computed mated and non-mated similarity scores). Then, the NN estimator of the KL-divergence is defined as [21]:

$$\hat{D}_{KL}\left(p_m\|p_{nm}\right)=\frac{1}{N_m}\sum_{1=1}^{N_m}\log\frac{\nu_{nm}\left(i\right)}{\rho_m\left(i\right)}+\log\frac{N_{nm}}{N_m-1} \tag{3}$$

where $\rho_m\left(i\right)=\min_{j\neq i}\left\|s_m^i-s_m^j\right\|$ is the distance of s_m^i to its nearest neighbour in $\left\{s_m^j\right\}_{j\neq i}$, and $\nu_{nm}\left(i\right)=\min_j\left\|s_m^i-s_{nm}^j\right\|$ is the distance of s_m^i to its nearest neighbour in $\left\{s_{nm}^j\right\}$.

In spite of the great value of these techniques, such approaches can only be used to globally quantize the average entropy provided by (multi-)biometric feature vectors, i.e., local information of correlation is ignored. To provide a more concrete estimate of the joint entropy caused by correlation factors such as biometric symmetry, one part of a multi-biometric template (X_l) could be used to gain some knowledge about the other part (X_r).

Focusing on unprotected multi-biometric systems, the use of two (or more) biometric characteristics has been found to generally improve the overall recognition accuracy [12]. Such improvement can be expected if the joint entropy of the used biometric characteristics is clearly larger than that of each individual one, $H\left(X_l,X_r\right)>\max\left\{H\left(X_l\right),H\left(X_r\right)\right\}$. However, in the presence of biometric symmetry, the joint entropy of the used biometric characteristics is clearly smaller than the sum of that of each individual one, $H\left(X_l,X_r\right)<H\left(X_l\right)+H\left(X_r\right)$. We assume that the same holds for extracted biometric templates and, hence, the average entropy of the multi-biometric template is expected to be lower than the desired maximum.

Therefore, the question to answer now is: "what is the decrease in uncertainty about one biometric characteristic (or instance), due to a set of biometric measurements on the other correlated characteristic (or instance)?". In other words, can we employ the template associated to a particular instance (X_l) to gain some knowledge about the other instance (X_r)? To answer that question, we should first note that the joint entropy of X_l and X_r can be defined as

$$H\left(X_l,X_r\right)=H\left(X_l\right)+H\left(X_r\right)-I\left(X_l;X_r\right) \tag{4}$$

Thus, we would like to minimise the mutual information between X_l and X_r: $I\left(X_l;X_r\right)$. In analogy to [19], [20],

$$I\left(X_l;X_r\right)\approx\hat{D}_{KL}\left(p_m\|p_{lr}\right) \tag{5}$$

where $p_{lr}\left(s\right)$ denotes the probability density of the similarity scores between both characteristics or instances from a single subject (left and right).

ISBN 978-0-9928626-7-1 © EURASIP 2017

The degree of biometric symmetry can thus be measured in terms of $\hat{D}_{KL}(p_m \| p_{lr})$, which is bounded between the following values:

$$\hat{D}_{KL}(p_m \| p_{lr}) \geq H(X_l) + H(X_r) - \max\{H(X_l, X_r)\} = 0 \quad (6)$$

$$\hat{D}_{KL}(p_m \| p_{lr}) \leq H(X_l) + H(X_r) - \min\{H(X_l, X_r)\} = \min\{H(X_l), H(X_r)\} \quad (7)$$

since $I(X_l; X_r) = H(X_l) + H(X_r) - H(X_l, X_r)$ (see Eq. 4).

However, in order to have a comparable measure across different characteristics or feature extraction techniques, we need a relative value with respect to the original amount of information of the biometric source. Therefore, in order to evaluate the degree of correlation between the templates, and the corresponding amount of mutual information loss, we should analyse the relative decrease of $\hat{D}_{KL}(p_m \| p_{lr})$ with respect to $\hat{D}_{KL}(p_m \| p_{nm})$:

$$\hat{D}_{KL}^{\text{fused}} = 1 - \frac{\hat{D}_{KL}(p_m \| p_{lr})}{\hat{D}_{KL}(p_m \| p_{nm})} \approx 1 - \frac{I(X_l; X_r)}{I(Y; X)} \quad (8)$$

This way, $\hat{D}_{KL}^{\text{fused}}$ achieves a maximum value of one when both left and right templates are uncorrelated (Eq. 6):

$$\hat{D}_{KL}^{\text{fused}} \leq 1 - \frac{0}{I(X; Y)} = 1 \quad (9)$$

Conversely, $\hat{D}_{KL}^{\text{fused}}$ yields a minimum value of zero when the average joint entropy is minimised (i.e., X_r and X_l are fully correlated):

$$\begin{aligned} \hat{D}_{KL}^{\text{fused}} &\geq 1 - \frac{\min\{H(X_l), H(X_r)\}}{I(X; Y)} \\ &\geq 1 - \frac{H(X)}{I(Y; X)} \geq 1 - \frac{H(X)}{H(X)} = 0 \end{aligned} \quad (10)$$

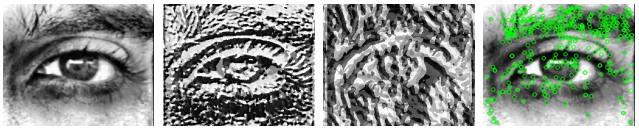
where the first inequality is derived from Eq. 7, the second from $\min\{H(X_l), H(X_r)\} \leq H(X)$ (i.e., the average entropy of one half of the characteristic X_l is at most as high as that of the complete characteristic X), and the third from $I(Y; X) = H(X) - H(X|Y) \leq H(X)$.

In summary, $\hat{D}_{KL}^{\text{fused}}$ gives an estimation of how uncorrelated X_l and X_r are. Or in other words, the higher $\hat{D}_{KL}^{\text{fused}}$, the higher the average joint entropy of the fused template.

III. Case Study: Periocular Biometrics

A particular case study, based on periocular regions, is analysed in this section. The experiments are conducted on the training set of the MobBIO iris corpus [11], acquired at visible wavelength, which can be used to benchmark periocular recognition systems [16]. The database comprises color images of 300×200 pixels of 200 periocular instances (100 subjects). For each region, four images are available, resulting in a total number of unconstrained 800 images.

At preprocessing, each image is converted to grayscale and Contrast Limited Adaptive Histogram Equalization (CLAHE) is applied to obtain an enhanced image, as shown in Fig. 2 (a).



(a) Enhanced (b) LBP (c) BSIF (d) SIFT

Fig. 2. An (a) enhanced image and (b-d) features extracted from (a).

Subsequently, two types of features are extracted, namely: i) generic texture descriptors and ii) keypoint-based features.

With respect to generic texture descriptors, Uniform Local Binary Patterns (LBP) [22] and Binarized Statistical Image Features (BSIF) [23] are extracted from the enhanced images. Images are then divided into 25×25 sub-blocks to retain local information and one feature histogram, comprising the obtained feature values, which are computed per texture block. While LBP simply processes neighbouring values of 9×9 pixel multi-scale blocks, BSIF utilizes 15×15 pixel filters with a filter length of 8 bits learned from a set of images. The extracted templates from a given image are depicted in Fig. 2 (b) and 2 (c), respectively. In order to obtain a similarity score from the templates, pairs of corresponding histograms are compared using the χ^2-distance. The final score is estimated as the normalized average distance of all histogram comparisons. For more details on these texture descriptors the reader is referred to [22], [23].

On the other hand, regarding keypoint-based features, Scale Invariant Feature Transform (SIFT) [24] and Speeded Up Robust Features (SURF) [25] extract sets of local keypoints and the corresponding keypoint descriptors. As a consequence, the extracted feature vectors are of variable size. The aforementioned generic algorithms can be applied to various types of input images. In this case, both methods are applied to enhanced images, and an efficient trimming of false positive keypoint correspondences using geometrical constraints is carried out. The keypoints detected in Fig. 2 (a), based on which SIFT and SURF descriptors are extracted, are shown in Fig. 2 (d). In order to compare the feature vectors, given two sets of keypoint descriptors, the resulting correspondences are obtained from the according comparator using a cross-checking procedure. False positive matches are detected and erased by comparing the distance of x and y coordinates of corresponding keypoints to adequate thresholds. In particular, matched keypoints have to lie within 16×16 pixel regions. The final comparison score is estimated as the number of retained matches normalized by the minimum number of keypoints detected in both images. For details on keypoint detection, the extraction of keypoint descriptors and keypoint matching, the reader is referred to [24], [25].

To obtain the baseline accuracy, the mated score distribution $p_m(s)$ is estimated by performing all genuine (i.e., mated) comparisons. For uncorrelated impostor (i.e., non-mated) scores, $p_{nm}(s)$, the first image of each subject is used. In addition, to quantify the correlation, all possible comparisons between left and right periocular regions of single subjects are performed, $p_{lr}(s)$, where the right periocular regions are horizontally mirrored prior to feature extraction.

ISBN 978-0-9928626-7-1 © EURASIP 2017

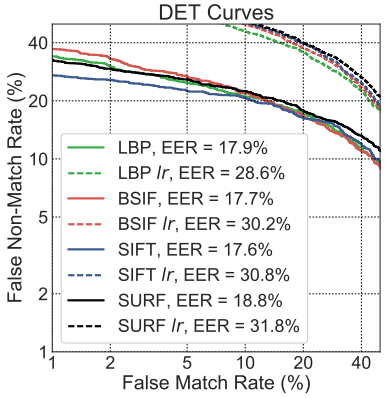


Fig. 3. DET curves for all features considered, where the FNMR is computed from mated (solid curves) or left *vs* right comparisons (dashed curves).

The Detection Error Trade-off (DET) curves for each feature extraction method are depicted in Fig. 3. The solid curves represent the normal accuracy evaluation, and the dashed curves represent the correlation study - i.e., left *vs* right comparisons are computed for the False Non-Match Rate (FNMR) estimation. As it can be observed, the Equal Error Rate (EER) increases approximately from 18% to 30% in all cases, indicating that the features extracted from periocular regions are not exactly symmetric, and therefore can not be indistinguishably used for recognition purposes. On the other hand, if there were no correlation or symmetry between them, the EER would be that of random comparisons: 50%. However, values around 30% are achieved, confirming that there is a significant correlation between both periocular regions of the subject, regardless of the features considered.

Let us now quantify the degree of correlation, following the methodolofy proposed in Sect. II. The score distributions for all feature extractors considered are shown in Fig. 4, where $p_m(s)$ is depicted in dashed green, $p_{nm}(s)$ in dashed red and $p_{lr}(s)$ in solid blue. Table I shows the corresponding values of $\hat{D}_{KL}(p_m \| p_{nm})$, $\hat{D}_{KL}(p_m \| p_{lr})$ and $\hat{D}_{KL}^{\text{fused}}$.

As it can be observed in Fig. 4, regardless of the feature extractor considered, the left-right distribution is closer to the mated distribution than the non-mated one. This shows that such comparisons give away more information about the biometric sample than random non-mated comparisons with instances belonging to other individuals, thereby resulting in a decrease in the average joint entropy of the fused template with respect to the fusion of fully uncorrelated characteristics. This fact is reflected on the decrease of $\hat{D}_{KL}(p_m \| p_{lr})$ with respect to $\hat{D}_{KL}(p_m \| p_{nm})$, as shown in Table I: in all cases, $\hat{D}_{KL}^{\text{fused}} < 1$, indicating that both periocular regions are somehow correlated. More specifically, only 44% of the ideal maximal joint entropy is retained for the SIFT based templates ($\hat{D}_{KL}^{\text{fused}} = 0.44$), whereas the BSIF features show the lowest correlation (i.e., $\hat{D}_{KL}^{\text{fused}} = 0.70$). Hence, the amount of joint entropy also depends on the employed feature extractor.

IV. Discussion and Conclusions

As shown in Sect. III, biometric symmetry results in a considerable degree of correlation between the corresponding

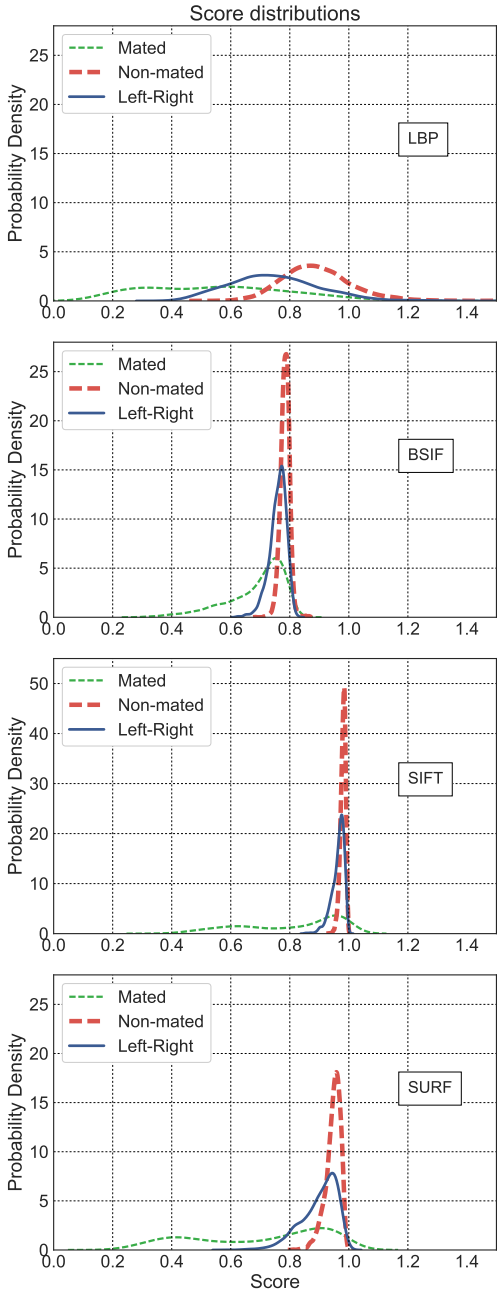


Fig. 4. Mated $p_m(s)$ (dashed green), non-mated $p_{nm}(s)$ (dashed red) and lef-right $p_{lr}(s)$ (solid blue) score distributions for each feature extractor.

biometric templates, thereby decreasing their joint entropy (only up to 70% of the maximal joint entropy is retained for both periocular regions). While a decrease in average entropy might not cause any issue from a verification accuracy perspective, it can negatively affect the privacy protection offered by multi-biometric template protection schemes. In particular, regarding biometric cryptosystems, e.g. the fuzzy commitment scheme [26], secret keys are bound to and retrieved from biometric templates, where biometric variance is overcome by means of error correction. The general idea for achieving error correction is to add some redundancy. To that end, biometric templates are bound to non-random data of

ISBN 978-0-9928626-7-1 © EURASIP 2017

TABLE I
$\hat{D}_{KL}\left(p_m \| p_{nm}\right)$, $\hat{D}_{KL}\left(p_m \| p_{lr}\right)$ AND $\hat{D}_{KL}^{\text{FUSED}}$ FOR ALL FEATURES.

	LBP	BSIF	SIFT	SURF
$\hat{D}_{KL}\left(p_m \| p_{nm}\right)$	5.45	5.07	7.08	6.07
$\hat{D}_{KL}\left(p_m \| p_{lr}\right)$	2.07	1.50	3.94	2.51
$\hat{D}_{KL}^{\text{fused}}$	0.62	0.70	0.44	0.59

rather low entropy. For instance, in a $[2^k, k+1, 2^{k-1}]$ linear code, k bits are encoded to 2^{k-1} bits. It has been shown that information leakage increases within biometric cryptosystems if the average entropy provided by the biometric template is reduced [27]. When an attacker is aware of the biometric symmetry of two or more biometric templates used in a multi-biometric cryptosystem, his guessing entropy is significantly reduced. In particular, in case of statistical attacks, where the symmetry between different template parts might be utilized to filter out faulty keys.

Within cancelable multi-biometric systems feature, transforms are applied in the signal of feature domain using specific parameters, allowing a reliable comparison in the transformed domain [28]. In any case, a decrease in the average entropy of biometric templates results in a reduction of the feature space, and, hence, also in the parameter space of the cancelable multi-biometric system. Moreover, biometric symmetry will facilitate the reconstruction of an approximation of the original biometric templates, due to a reduced guessing entropy [29].

In summary, for both types of biometric template protection schemes, the presence of biometric symmetry is expected to reduce the level of privacy protection. In other words, naïve assumptions about provided security levels in multi-biometric template protection schemes could be misleading and (even worse) utilized by an adversary to attack the system. In order to increase the security offered by multi-biometric template protection systems, it is suggested to choose biometric sources in a way that the joint entropy and, hence, the average entropy of multiple templates (or within a single template) are maximised. This corresponds to a minimization of mutual information between biometric sources, $I\left(Y; X\right)$, which could be easily achieved by choosing totally uncorrelated modalities, e.g., a combination of fingerprint and iris. However, when designing a multi-biometric system, biometric performance as a result of biometric fusion should always be weighed against the associated overhead involved, such as additional sensing cost. That is, it is preferred to combine biometric sources that can be acquired in a single presentation [30], e.g., both irises of the subject.

ACKNOWLEDGMENTS

This work was partly supported by the German Federal Ministry of Education and Research (BMBF) as well as by the Hessen State Ministry for Higher Education, Research and the Arts (HMWK) within the Center for Research in Security and Privacy (CRISP), and by the Research Council of Norway (IKTPLUSS 248030/O70).

REFERENCES

[1] A. Adler, "Sample images can be independently restored from face recognition templates," in *Proc. CCECE*, vol. 2, 2003, pp. 1163–1166.

[2] J. Galbally, R. Cappelli *et al.*, "An evaluation of direct and indirect attacks using fake fingers generated from ISO templates," *Pattern Recognition Letters*, vol. 31, pp. 725–732, 2010.

[3] J. Galbally, A. Ross *et al.*, "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms," *Computer Vision and Image Understanding*, vol. 117, no. 10, pp. 1512–1525, 2013.

[4] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Proc. Magazine*, vol. 32, no. 5, pp. 88–100, 2015.

[5] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, no. 3, 2011.

[6] ISO/IEC JTC1 SC27 Security Techniques, *ISO/IEC 24745:2011. Information Technology - Biometric Information Protection*, 2011.

[7] C. Rathgeb and C. Busch, "Multibiometric template protection: Issues and challenges," in *New Trends and Developments in Biometrics*. In-Tech, 2012, pp. 173–190.

[8] A. Nagar, K. Nandakumar, and A. Jain, "Multibiometric cryptosystems based on feature-level fusion," *Trans. on Information Forensics and Security*, vol. 7, no. 1, pp. 255–268, 2012.

[9] P. J. Phillips, H. Moon *et al.*, "The FERET evaluation methodology for face-recognition algorithms," in *Proc. CVPR*, 1997, pp. 137–143.

[10] A. Kummar, "Incorporating cohort information for reliable palmprint authentication," in *Proc. ICVGIP*, 2008, pp. 583–590.

[11] A. F. Sequeira, J. C. Monteiro *et al.*, "MobBIO: A multimodal database captured with a portable handheld device," in *Proc. VISAPP*, vol. 3, 2014, pp. 133–139.

[12] A. Ross and A. K. Jain, "Information fusion in biometrics," *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2115–2125, 2003.

[13] J. Daugman, "How iris recognition works," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, 2004.

[14] A. Kumar and K. Wang, "Identifying humans by matching their left palmprint with right palmprint images using convolutional neural network," in *Proc. DLPR*, 2016.

[15] K. Papachristou, A. Tefas, and I. Pitas, "Symmetric subspace learning for image analysis," *IEEE Trans. on Image Processing*, vol. 23, no. 12, pp. 5683–5697, 2014.

[16] F. Alonso-Fernandez and J. Bigun, "A survey on periocular biometrics research," *Pattern Recognition Letters*, vol. 82, pp. 92 – 105, 2016.

[17] A. Adler, R. Youmaran, and S. Loyka, "Towards a measure of biometric information," in *Proc. CCECE*, 2006, pp. 210–213.

[18] Y. Sutcu, E. Tabassi *et al.*, "What is biometric information and how to measure it?" in *Proc. HST*, 2013, pp. 67–72.

[19] Y. Sutcu, H. T. Sencar, and N. Memon, "How to measure biometric information?" in *Proc. ICPR*, 2010, pp. 1469–1472.

[20] K. Takahashi and T. Murakami, "A measure of information gained through biometric systems," *Image Vision and Computing*, vol. 32, pp. 1194–1203, 2014.

[21] Q. Wang, S. R. Kulkarni, and S. Verdu, "Divergence estimation for multidimensional densities via k-nearest-neighbor distances," *IEEE Trans. on Information Theory*, vol. 55, no. 5, pp. 2392–2405, 2009.

[22] S. Liao, X. Zhu *et al.*, "Learning multi-scale block local binary patterns for face recognition," in *Proc. ICB*, 2007, pp. 828–837.

[23] J. Kannala and E. Rahtu, "BSIF: Binarized statistical image features," in *Proc. ICPR*, 2012, pp. 1363–1366.

[24] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *Int. J. Comput. Vision*, vol. 60, no. 2, pp. 91–110, 2004.

[25] H. Bay, A. Ess *et al.*, "Speeded-Up Robust Features (SURF)," *Computer Vision and Image Understanding*, vol. 110, no. 3, pp. 346 – 359, 2008.

[26] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. ACM CCS*, 1999, pp. 28–36.

[27] T. Ignatenko and F. M. J. Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Trans. on Information Forensics and Security*, vol. 4, no. 4, pp. 956–973, 2009.

[28] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Proc. Magazine*, vol. 32, no. 5, pp. 54–65, 2015.

[29] C. Rathgeb and C. Busch, "Irreversibility analysis of feature transform-based cancelable biometrics," in *Proc. CAIP*, 2013, pp. 177–184.

[30] A. Jain, B. Klare, and A. Ross, "Guidelines for best practices in biometrics research," in *Proc. ICB*, 2015.