Template Protection on Multiple Facial Biometrics in the Signal Domain under Visible and Near-Infrared Light

Simon Kirchgasser, Luca Debiasi, Rudolf Schraml, Heinz Hofbauer, Andreas Uhl
Multimedia Signal Processing and Security Lab
Department of Computer Sciences
University of Salzburg, Austria
{skirch, ldebiasi, rschraml, hofbauer, uhl}@cs.sbg.ac.at

Jonathan Boyle, James Ferryman
Computational Vision Group
Department of Computer Science
University of Reading, United Kingdom
{j.n.boyle, j.m.ferryman}@reading.ac.uk

***Abstract*—Template protection techniques like cancellable biometrics have been introduced in order to overcome privacy issues in biometric applications. We conduct an ISO/IEC Standard 24745 compliant assessment of block re-mapping and warping focusing on recognition performance issues as well as security and unlinkability aspects. Both of these template protection schemes are applied on a multi-biometrics dataset in the signal (image) domain. The dataset includes 2D face, iris and periocular images which have been acquired not only using visual light (VIS) but also near-infrared light (NIR). With respect to the used data, this is the first study that applies and evaluates cancellable template protection methods in the signal domain on VIS/NIR 2D face, iris and periocular biometrics.**

***Index Terms*—Template Protection, 2D NIR/VIS Face, NIR/VIS Iris, NIR/VIS Periocular, Performance Evaluation, Security, Unlinkability**

I. Introduction

Privacy invasion and impersonation are two possible threats if a biometric template gets compromised or stolen. Thus, methods have been proposed to protect biometric samples and/or templates by fulfilling certain properties e.g. defined in ISO/IEC Standards 24745 [1] and 30136 [2]: *Irreversibility*, *Revocability*, *Unlinkability* and *Performance preservation*. Meeting the requirements of these properties makes biometric template protection challenging especially if the schemes should be applied in a multi-biometric setting. This challenging setting including different biometric modalities gets even more complicated if the considered biometric data was acquired using varying illumination sources.

In the scope of this study the cancellable biometrics schemes block re-mapping [17] and warping [26] are evaluated not only on visible light (VIS) images but also on near-infrared light (NIR) ones. Thus, the main contribution of this work is the usage of both VIS and NIR 2D face, iris and periocular images under the aspect of cancellable biometrics. During the experiments block re-mapping and warping are applied on this multiple face biometrics in the image/signal domain independently from each other and an ISO/IEC Standard 24745/30316 compliant assessment of both schemes focusing on recognition performance issues as well as security and unlinkability aspects is conducted.

Regardless if VIS or NIR images are considered, template protection in the signal domain is preferable for several reasons. The main advantage is that the biometric features are not extracted from the original acquired image/signal, instead the original image/signal is protected after completing the pre-processing and before starting the feature template extraction. Thus, a template, storing the captured subject's original biometric characteristics, is neither processed during feature extraction nor during comparison. Only a template storing the features of the protected biometric characteristics is used during the recognition process. This provides the highest possible level of privacy protection for the capture subject. Another advantage is the compatibility with recent deep-learning based recognition approaches. Deep-learning based approaches often do not compute and store templates in order to perform the biometric comparisons. Instead, these techniques directly process the sample data. Thus, in order to facilitate cancellable template protection techniques (extensively discussed in e.g. [16]), they have to be applied in the signal domain as there are no "templates" available. The main disadvantage of the application in the image/signal domain is that the feature extraction based on the protected image/signal might lead to falsely detected features and thus, to a negative impact on the recognition performance.

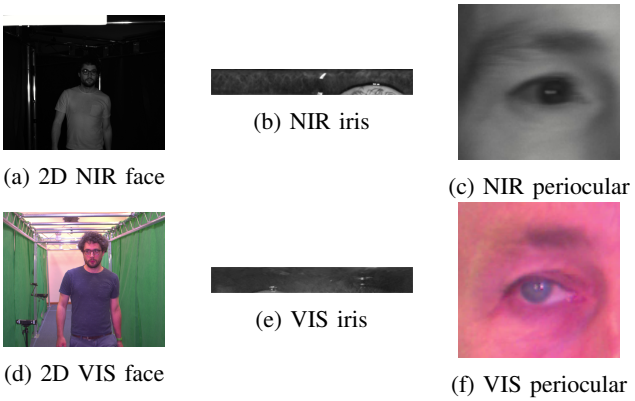
To the best of our knowledge there has been no study so far that discusses template protection methods, in particular our investigated schemes block re-mapping and warping, in the signal domain using VIS/NIR 2D face, iris and periocular data. Furthermore, it must be considered that the applied template protection schemes, block re-mapping [17] and warping [26], tend to change the shape or structure information of the biometric trait they are applied on. This modification in the geometrical structure is expected to be non-beneficial

978-1-7281-6232-4/20/$31.00 ©2020 IEEE

if the feature extraction process relies on the detection and description of landmarks as it is done by the applied methods for the considered face biometric modalities (see Section IV). As a consequence it is assumed that a recognition performance decrease compared to the original unprotected images can be observed especially for block re-mapping, while for warping the difference should be much smaller.
The remainder of this study is organised as follows: The related work with respect to face, iris and periocular biometrics is briefly discussed in Section II. In Section III the used dataset is described, while the experimentally setup is presented in Section IV. The corresponding experimental results are summarised and discussed in Section V while conclusions are drawn in the final Section VI.

II. Template Protection in Face, Iris and Periocular Biometrics

In [19] an overview of multi-biometric template protection issues and challenges is given. One of these issues is the recognition performance reduction after the application of a template protection technique. To overcome this problem employing multi-biometrics is a valid solution. During the experimental evaluation we observe that that the application of a template protection scheme can also lead to an enhancement of the recognition performance instead. This is a unexpected observation as most other studies focusing on the usage of multi-biometric datasets apply several fusion strategies to enhance the recognition performance while maintaining the important aspects like subjects' security and privacy [3], [12], [20].
Several studies have been presented so far that either discuss biometric recognition performance issues using NIR or VIS face, iris or periocular data (e.g. [10], [27]) or focus on template protection aspects that can be described for one of the biometric modalities. So far no paper was published which investigates template protection in periocular biometrics. Nevertheless, there are studies available which discuss the aspect of VIS and NIR light during the recognition process, e.g. [10] stating that VIS may be a better option for periocular recognition than NIR light. Although in face and iris biometrics several template protection studies have been published. Both, cancellable biometrics (CB) as well as biometric cryptosystems have been investigated (e.g. [5], [22]). Especially Bloom filter based CBs have recently grown in importance. In [9] the Bloom filter approach was successfully used on 2D VIS face images and was at least maintaining the baseline biometric performance, while securing the biometric traits, reducing the template size and the computational costs. Similar promising aspects as for face biometrics have been observed on iris data as well [18]. Further details on iris template protection can be found e.g. in [21]. However, all mentioned works performed template protection in the feature domain.



(a) 2D NIR face (b) NIR iris (c) NIR periocular
(d) 2D VIS face (e) VIS iris (f) VIS periocular

Fig. 1: Examplary multi-face data used in the study for NIR and VIS light.

III. Dataset

In this work, biometric template protection on various face biometric modalities is analysed. The images used during the experiments are part of the PROTECT Multimodal DB Dataset (PMMDB) [23]. This collection of biometric data includes iris (VIS, NIR), face (VIS, NIR, 3D and thermal), periocular (VIS, NIR), anthropometrics as well as hand- and finger vein biometric samples of 69 different subjects. The acquired data was captured at two data acquisition events separated by a time-gap of one year. This database is publicly available http://projectprotect.eu/. In our experiments we utilised VIS, NIR iris images as well as VIS, NIR 2D face and VIS, NIR periocular images. Some samples of the investigated biometric modalities are shown in Fig. 1 and further modality specific details can be found in e.g. [23].

IV. Evaluation Protocol

In this work the template protection methods' recognition performance, security and unlinkability of the templates generated with distinct keys is evaluated. Each evaluation scheme, including the applied template protection schemes and the recognition tool-chains are described in more detail in the following, starting with the template protection schemes. Furthermore, we also will briefly discuss irreversibility aspects which should be considered as well if the applied template protection schemes are utilised.

1	2	3	4
5	6	7	8

(a) Initial grid with blocks.

5	2	7	3
4	1	3	5

(b) Blocks after re-mapping.

Fig. 2: Grid displaying the blocks before the re-mapping (a) and after the re-mapping (b).

Block re-mapping [17] (BRMP) partitions the sample image into blocks. Some of the blocks are randomly placed at different positions during the re-mapping while others are removed completely to ensure the irreversibility property and thus, it is likely that several blocks are used more than once.

The block selection is key-dependent. By comparing Fig. 2 (a) and (b) the principle described can be observed: While the blocks 6 and 8 are present in (a) they do not occur in the protected, re-mapped image (b). It becomes obvious that the blocks 3 and 5 are inserted multiple times into (b) in order to compensate for the absence of the non-considered blocks 6 and 8. As parameters for BRMP experiments block sizes of 16, 32 and 64 pixels are chosen. Thus, in Table I the corresponding experimental results are presented in the lines named *BRMP 16*, *BRMP 32* and *BRMP 64*, respectively.

Block or Mesh Warping (WARP) applies a function (based on [26]) which maps each pixel of the input to a certain position in the template protected output, which can remain at the same position as well. Thus, this mapping defines a new image or template containing the same information as the original input but in a distorted representation as shown in Fig. 3. Subsequently, during experiments block sizes of 16, 32 and 64 pixels with maximal warping offsets of 6, 12 and 24 pixels are utilised. The corresponding lines in Table I are named *WARP 16/6*, *WARP 32/12* and *WARP 64/24*. The first number (16, 32 or 64) indicates the block size and the second number refers to the used maximal offset (6, 12, 24).

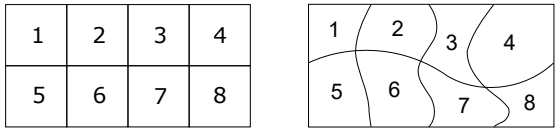


Fig. 3: Block warping scheme: basic grid and warped blocks.

Recognition Tool-Chains: The 2D face experiments are conducted using a commercial deep learning based solution [25]. The utilised visage network is capable of doing the pre-processing as well as the necessary feature extraction and the final comparison. For the iris recognition-based assessment we employ a feature extractor based on quadratic spline wavelet transform (QSW) by Ma et al. [13], from the USIT 2.0 toolkit [22], yielding 10240 bit codes compared using fractional Hamming distance.
During the periocular recognition for each periocular image one single local binary pattern (LBP) [14] histogram for three scales is computed. Hence, the corresponding feature vector has a length of 256 x 3 = 768. The comparison of two feature vectors is done by using a set of distance metrics: Chi-Square, Euclidean, Manhattan and Histogram intersection. In the experimental evaluation the results computed with the different distance metrics showed no significant difference, thus the presented results are those achieved by applying Euclidean distance.

Recognition Performance: We calculate the Equal Error Rate (EER) based on the full range of the genuine and impostor comparison scores. The baseline recognition performance uses the original and unprotected data only. The impact of the various template protection approaches on the recognition performance is assessed by first applying the template protection scheme to the whole dataset using a fixed but arbitrary key (system key) and afterwards computing all comparison scores. This process is repeated for 10 random system-based keys, where we report the mean EER and standard deviation (σ) for all keys.

Security: When the template protection schemes are applied, it must be ensured that a template extracted from an original image cannot be successfully compared against a template extracted from a protected version of the same image. We perform all genuine comparisons among original (unprotected) images, followed by all genuine comparisons between original and protected images (with a specific key). Thus, we obtain two score distributions, where a high security is given if the two score distributions are clearly separable and do not overlap. Hence, a mean EER and σ of 0% can only be obtained, if the protected and unprotected templates do not match.

Unlinkability (Diversity): The ISO/IEC Standards 24745 [1] and 30136 [2] define the criteria of unlinkability. This property shall guarantee that stored and protected biometric information can not be linked across various different applications or databases. Two templates are *fully linkable* if a method exists which is able to decide if these templates protected using a different key were extracted from the same biometric sample with a certainty of 100%. In that case, it is easy to track the capture subjects across different applications, which poses a threat for the capture subjects' privacy. Gomez et al. [8] present a universal framework based on mated (genuine) and non-mated (impostor) comparison scores to evaluate the unlinkability of a biometric template protection system by proposing the so called D_{sys} measurement as a global measure. The D_{sys} normally ranges from 0 to 1, where 0 represents the best achievable unlinkability score. We shifted the range from $[0, 1]$ to values in $[0, 100]$ to improve the readability of the results.

Irreversibility Aspects: The ISO/IEC Standards 24745 [1] and 30136 [2] also define the criteria of irreversibility. This property shall ensure computational hardness to derive the original biometric template from the protected one. We discuss this aspect only from a theoretically point of view and did not conduct explicit experiments to prove this criteria. Both considered template protection schemes can easily fail to meet the irreversibility requirement, because the selected secret keys used are much too short. As a consequence it would be easy to reconstruct the original templates. For example, using jigsaw puzzle solver approaches, e.g. [4], [7], [15], the original positions of the present blocks which have been rearranged by BRMP can be reconstructed. The bigger the block sizes are the easier this brute force attack will be successful. Another attack which could be launched on protected iris data, is based on the idea of employing one of the following two methods [6], [24] to recover the

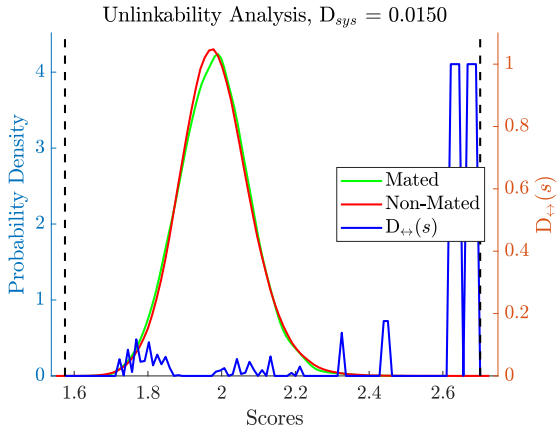
transformed image from which the iris code was extracted. After the application of one of these methods a jigsaw puzzle solver can be applied to reconstruct the original positions of the blocks as mentioned above. Similar approaches exist for WARP as well. Thus, it must be considered how the key is selected: In terms of BRMP it is necessary to think about how big the block sizes should be and how much blocks will be kept after the re-mapping. The critical aspect for WARP relies on the off-set parameter and the corresponding interpolation scheme as those key informations are responsible for the amount of introduced distortions. The block size and off-set parameters which have been selected shall ensure a balanced trade-off between recognition performance, applicability on a multiple biometrics and applicability in the signal domain. We are aware of the fact that the selected keys may not be the best in terms of irreversibility aspects as a better attack protection would need *a)* smaller block size or a *b)* a higher off-set. Nevertheless, this work introduces a first and detailed ISO/IEC Standard evaluation on well-established template protection schemes which have not been applied at several different face-related biometrics at once until now. A higher amount of irreversibility and of protection in general could be ensured by applying Biometric Cryptosystems or Homomorphic Encryption instead. These template protection schemes have been investigated extensively in former studies e.g. [11]. The main disadvantages of these schemes are high computational costs and the fact that a direct comparison of the protected templates is not possible any longer.

V. Experimental Results

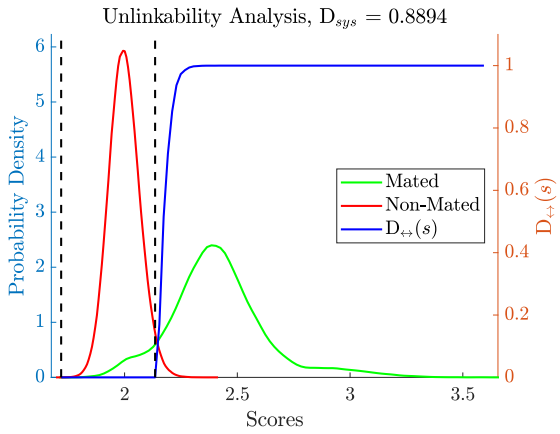
The experimental results of the conducted recognition performance, security and unlinkability analysis are presented in Tab. I and in the subsequent Fig. 4. The first column contains the name of the investigated biometric modality and the corresponding baseline EER performance computed using the unprotected images only. The remaining columns describe either which template protection method was applied (second column) or present the recognition performance, security or unlinkability scores generated using 10 different keys. For several experiments it was not possible to compute meaningful results as the introduced distortions of the template protection methods are too high, thus they will be described by ”-”.

According to the baseline experiments 2D face performed best, followed by iris and periocular. Focusing on the performance only, WARP received good results on 2D face, but BRMP failed in VIS and NIR. We assume that the deployed commercial face recognition system is most likely based on geometric features like facial landmarks, which explains the good results for WARP and bad ones for BRMP schemes. Comparing VIS and NIR face results it must be reported that the VIS face baseline recognition performance outperform the NIR performance, but in the protected domain NIR performed better (best result for NIR WARP 16/6).

Considering iris it was not surprising to observe that the baseline NIR results are better than the VIS as ones. However, it was interesting to observe that after template protection



(a) NIR iris - BRMP 32



(b) NIR iris - WARP 32/12

Fig. 4: Score distributions and corresponding D_{sys} values for unlinkablity for NIR iris images.

BRMP 16 and 32 are worse for NIR compared to VIS, indicating that the BRMP template protection results in less distinctive templates for NIR. Both WARP 64/24 experiments' EERs are the same as the baseline EER.

Finally, there is an interesting observation for periocular as well. The applied template protection schemes lead to a recognition performance improvement. Of course the baseline EER for NIR and VIS is poor, but after applying BRMP 32, 64 as well as WARP 64/24 on the NIR and BRMP 64 on the VIS images the recognition performance remained almost the same (VIS BRMP 64) or was significantly improved (NIR BRMP 32 and 64).

As mentioned in I the observed performance results follow the assumptions: In almost all cases BRMP performed not so good as compared to WARP. We already briefly discussed that for 2D face the deployed network seems to be based on the extraction of local structures which are distorted to a large extend applying BRMP. The features extracted for iris and periocular also rely on the description of local geometrical dependencies. Thus, it was unexpected that for both biometric modalities the recognition performance loss was lower as assumed. Of course the observed degradation is high (higher than for warping) in the most cases, but the parameter selection

Dataset	Method	**Recognition Perf.**		**Security**		**Unlinkability**	
		EER [%]		EER [%]		D_{sys} [%]	
		Avg	σ	Avg	σ	Avg	σ
2D NIR Face *Orig. EER:* 4.75%	BRMP 16	-	-	-	-	-	-
	BRMP 32	-	-	-	-	-	-
	BRMP 64	49.42	0.00	0.00	0.01	0.81	0.60
	WARP 16/6	4.29	1.07	31.50	2.06	52.59	3.48
	WARP 32/12	5.40	1.08	11.82	4.05	61.68	5.67
	WARP 64/24	10.64	3.20	7.28	0.79	72.05	8.93
2D VIS Face *Orig. EER:* 3.18%	BRMP 16	42.04	1.02	3.24	0.15	19.66	3.29
	BRMP 32	41,95	1,73	3.24	0.12	20.54	2.75
	BRMP 64	42.54	2.02	3.30	0.37	20.56	2.83
	WARP 16/6	5.35	1.29	7.04	0.69	48.01	2.54
	WARP 32/12	6.74	1.08	6.24	0.00	52.36	5.36
	WARP 64/24	6.92	1.47	4.99	0.59	47.50	13.08
NIR Iris *Orig. EER:* 4.28%	BRMP 16	15.81	0.98	4.28	0.31	4.18	2.27
	BRMP 32	10.44	1.74	4.84	0.63	7.54	6.34
	BRMP 64	7.60	1.21	6.94	3.77	23.44	20.95
	WARP 16/6	5.58	0.17	26.29	1.53	88.14	1.17
	WARP 32/12	4.92	0.17	20.38	2.18	86.17	4.25
	WARP 64/24	4.28	0.00	49.20	0.00	-	-
VIS Iris *Orig. EER:* 9.76%	BRMP 16	11.60	0.96	9.49	0.55	5.54	2.68
	BRMP 32	10.73	0.92	10.09	1.16	8.58	4.80
	BRMP 64	12.00	1.70	14.76	6.88	21.23	17.14
	WARP 16/6	10.82	0.63	39.86	0.87	76.40	1.21
	WARP 32/12	10.31	0.67	35.93	1.74	75.09	3.85
	WARP 64/24	9.76	0.00	48.45	0.00	-	-
NIR Periocular *Orig. EER:* 13.71%	BRMP 16	17.08	2.12	0.01	0.01	37.03	4.16
	BRMP 32	13.20	1.84	0.70	0.06	25.81	9.07
	BRMP 64	10.40	2.23	1.45	1.48	29.88	12.81
	WARP 16/6	14.04	1.27	5.53	0.59	57.70	2.12
	WARP 32/12	14.26	2.14	4.70	0.92	53.60	4.50
	WARP 64/24	13.83	0.96	6.75	1.12	54.88	9.92
VIS Periocular *Orig. EER:* 18.03%	BRMP 16	24.53	2.78	2.01	0.49	21.34	4.83
	BRMP 32	22.16	2.69	3.09	0.40	17.67	5.82
	BRMP 64	18.38	2.10	3.90	0.90	20.69	7.82
	WARP 16/6	23.44	1.38	5.98	0.58	36.53	3.42
	WARP 32/12	20.58	1.60	5.59	0.30	35.75	5.90
	WARP 64/24	20.14	2.07	7.64	0.99	38.74	11.67

TABLE I: Recognition performance, security and unlinkability analysis presented for all performed warping (WARP) and block re-remapping (BRMP) experiments.

seems to have a high impact on the performance on these particular biometrics. This results in the above mentioned performance improvement using BRMP on the NIR periocular data, while for WARP the parameter selection seems to have only a small impact on the experimental results in the most cases.

The evaluation regarding the security property is resulting in a low EER for all BRMP techniques. This corresponds to a high level of security for the template protection methods. Warping is slightly less secure regardless of the particular biometric modality. Furthermore, these results give a first indication of how the unlinkability performs: BRMP obtains the better unlinkability results compared to WARP across all considered datasets. The difference between BRMP and WARP is especially prominent if one of the both iris datasets is taken into account. An example for this observation is given in Fig. 4. Thus, if unlinkability is considered in real world applications WARP is not sufficiently secure enough as the generated protected data could easily be tracked across several databases and applications.

Summarising, applying BRMP and WARP on the biometric data leads to a trade-off between performance, security and unlinkability for all biometric modalities and used light sources. For 2D face WARP works best, while the BRMP schemes yield the best results for texture-based iris and periocular NIR and VIS recognition, mainly because of the pre-alignment which was performed before the template protection schemes have been applied.

VI. Conclusion

The experimental results confirmed that the applied template protection schemes worked well on the considered datasets. Regarding recognition performance, the application of warping on 2D NIR face images maintains the results compared to the baseline ones, whereas for the 2D VIS face images the performance drops after applying warping in the signal domain. Furthermore, after the application of block re-mapping on periocular images the recognition performance was improved compared to the baseline results which was not expected and needs further investigation. Except for warping applied on iris data, a constant good security level can be reported across all considered experiments, while the unlinkability for warping is generally worse compared to block re-mapping. Thus, block re-mapping offers a better trade-off between recognition performance loss, security and unlinkability in most cases as compared to warping regardless if VIS or NIR data is used. In future work we are planing to extend our presented evaluation regarding irreversibility of the applied template protection techniques.

References

[1] ISO/IEC 24745:2011 information technology — security techniques — biometric information protection, 2011, 2011.

[2] ISO/IEC 30136:2018 information technology — performance testing of biometric template protection schemes, 2018, 2018.

[3] A. M. Canuto, F. Pintro, and J. C. Xavier-Junior. Investigating fusion approaches in multi-biometric cancellable recognition. *Expert Systems with Applications*, 40(6):1971–1980, 2013.

[4] T. S. Cho, S. Avidan, and W. T. Freeman. A probabilistic image jigsaw puzzle solver. 2010.

[5] Y. Feng, P. C. Yuen, and A. K. Jain. A hybrid approach for face template protection. In *Biometric Technology for Human Identification V*, volume 6944. International Society for Optics and Photonics, 2008.

[6] J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia. Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms. *Computer Vision and Image Understanding*, 117(10):1512–1525, 2013.

[7] A. C. Gallagher. Jigsaw puzzles with pieces of unknown orientation. In *Computer Vision and Pattern Recognition (CVPR), 2012 IEEE Conference on*, pages 382–389. IEEE, 2012.

[8] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch. General framework to evaluate unlinkability in biometric template protection systems. *IEEE Transactions on Information Forensics and Security*, 13(6):1406–1420, 2018.

[9] M. Gomez-Barrero, C. Rathgeb, J. Galbally, J. Fierrez, and C. Busch. Protected facial biometric templates based on local gabor patterns and adaptive bloom filters. In *2014 22nd International Conference on Pattern Recognition*, pages 4483–4488. IEEE, 2014.

[10] K. P. Hollingsworth, S. S. Darnell, P. E. Miller, D. L. Woodard, K. W. Bowyer, and P. J. Flynn. Human and machine performance on periocular biometrics under near-infrared light and visible light. *IEEE transactions on information forensics and security*, 7(2):588–601, 2011.

[11] A. K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP Journal on advances in signal processing*, 2008:113, 2008.

[12] E. Kelkboom, X. Zhou, J. Breebaart, R. N. Veldhuis, and C. Busch. Multi-algorithm fusion with template protection. In *2009 IEEE 3rd international conference on biometrics: Theory, applications, and systems*, pages 1–8. IEEE, 2009.

[13] L. Ma, T. Tan, Y. Wang, and D. Zhang. Efficient iris recognition by characterizing key local variations. *IEEE Transactions on Image Processing*, 13:739–750, 2004.

[14] T. Ojala, M. Pietikäinen, and T. Mäenpää. Multiresolution Gray-Scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(7):971–987, July 2002.

[15] G. Paikin and A. Tal. Solving multiple square jigsaw puzzles with missing pieces. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 4832–4839, 2015.

[16] V. M. Patel, N. K. Ratha, and R. Chellappa. Cancelable biometrics: A review. *IEEE Signal Processing Magazine*, 32(5):54–65, 2015.

[17] N. Ratha, J. Connell, and R. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634, 2001.

[18] C. Rathgeb, F. Breitinger, C. Busch, and H. Baier. On application of bloom filters to iris biometrics. *IET Biometrics*, 3(4):207–218, 2014.

[19] C. Rathgeb and C. Busch. Multi-biometric template protection: Issues and challenges. In *New Trends and Developments in Biometrics*. IntechOpen, 2012.

[20] C. Rathgeb, M. Gomez-Barrero, C. Busch, J. Galbally, and J. Fierrez. 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)*, pages 1–6. IEEE, 2015.

[21] C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, 2011(1):3, 2011.

[22] C. Rathgeb, A. Uhl, and P. Wild. *Iris Recognition: From Segmentation to Template Security*, volume 59 of *Advances in Information Security*. Springer Verlag, 2013.

[23] A. F. Sequeira, J. Ferryman, L. Chen, C. Galdi, J.-L. Dugelay, V. Chiesa, A. Uhl, B. Prommegger, C. Kauba, S. Kirchgasser, A. Grudzien, M. Kowalski, L. Szklarski, P. Maik, and P. Gmitrowicz. Protect multi-modal db: a multimodal biometrics dataset envisaging border control. In *Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG'18)*, pages 1–8, Darmstadt, Germany, 2018.

[24] S. Venugopalan and M. Savvides. How to generate spoofed irises from an iris code template. *IEEE Transactions on Information Forensics and Security*, 6(2):385–395, 2011.

[25] Visage Technologies. VisageSDK, June 2019. Available by request at http://visagetechnologies.com/.

[26] G. Wolberg. Image morphing: a survey. *The visual computer*, 14(8):360–372, 1998.

[27] D. Yi, R. Liu, R. Chu, Z. Lei, and S. Z. Li. Face matching between near infrared and visible light images. In *International Conference on Biometrics*, pages 523–530. Springer, 2007.