Biometric Template Protection in the Image Domain Using Non-invertible Grey-scale Transforms

Luca Debiasi, Simon Kirchgasser,
Bernhard Prommegger and Andreas Uhl
Department of Computer Sciences, University of Salzburg
Jakob-Haringer-Str. 2, 5020 Salzburg, Austria
Email: {ldebiasi, skirch, bprommeg, uhl}@cs.sbg.ac.at

Artur Grudzień and Marcin Kowalski
Institute of Optoelectronics
Military University of Technology
Gen. W. Urbanowicza 2, 00-908 Warsaw, Poland
Email: {artur.grudzien, marcin.kowalski}@wat.edu.pl

***Abstract*—Various template protection schemes are providing solutions to fulfil privacy preservation in biometric recognition systems, among them Cancellable Biometrics (CB). In this paper we propose two CB schemes, so called non-invertible many-to-one transforms, that alter the image's grey values in key-dependent manner. The obtained recognition performance and unlinkability results are compared to other signal domain cancellable transformation schemes proposed earlier in literature (block re-mapping and warping). Experiments are conducted on a multi-biometrics dataset including finger-vein, hand-vein and thermal face images. In particular, for thermal face biometrics this represents the first study concerning uni-modal template protection techniques and their respective evaluation.**

I. Introduction

Cancellable Biometrics (CB), also known as feature transformations, have been introduced and evaluated in the image (signal) domain by Ratha et al. in [1]. The two applied transformations, **block re-mapping** and **warping**, have been evaluated to protect iris [2], [3] and finger-vein [4] datasets. However, since [1] no further signal domain CB techniques have been proposed and most recent template protection methods, e.g. Bloom Filters [5] and Indexing-First-One hashing [3], apply template protection in the feature domain.

The main advantage of applying template protection in the image domain immediately after image acquisition as compared to template protection operating in the feature domain is that the original biometric template is never generated. Therefore, the original template cannot be compromised in principle which constitutes the highest level of privacy protection for the capture subject. Only the transformed features (i.e. protected template), which obviously differ from the original ones, are extracted and further processed during template comparison by the recognition systems' authentication procedure. The main disadvantage is that feature extraction based on the transformed image might lead to incorrectly detected features and thus results in a recognition performance decrease as confirmed by [2], [4].

In this work we present and analyse a new class of image domain CB schemes based on non-invertible many-to-one grey value transformations with respect to the performance and unlinkability properties defined in ISO/IEC Standard 24745 [6] (details given in Section V). As a particular instance of this class, we investigate sine-based transformations. Thus, compared to block re-mapping and warping no shape or structure information of the biometric trait get geometrically changed, disconnected or disrupted. In particular, this geometrical-structure preserving property is expected to be beneficial if the recognition process relies on the detection of landmarks to identify regions-of-interest for feature extraction which get distorted by the applied CB methods. Vascular and thermal face biometrics have been selected as real-world applications to prove this assumption because features from vascular biometrics are mostly based on the extraction of geometrical-structures while in thermal face recognition landmarks are of importance for the feature extraction.

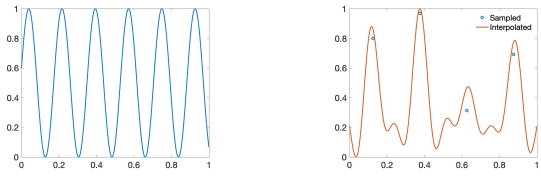
The remainder of this paper is organised as follows: A review on template protection schemes in vascular and (thermal) face biometrics is given in Section II. The proposed CB schemes together with the earlier proposed counterparts are described in Sections III and IV, respectively. The vascular and thermal face biometric dataset utilised during the experimental evaluation, the conducted biometrics' specific recognition tool-chain, the evaluation protocol, and experimental results are given and discussed in Section V. Section VI concludes the study and gives an outlook on future work.

II. Template Protection in Hand-based Vascular and (Thermal) Face Biometrics

Several proposed techniques are restricted to the feature domain transformation setting. Spectral minutiae representations [7] are subjected to binarisation and subsequently fed into Bloom filters to result in a CB scheme thereby avoiding position correction during template comparison as required by many techniques based on vascular structure representation [8]. We find techniques, which apply both CB and biometric crypto systems (BCS), the second important class of template protection schemes: After applying a set of Gabor filters for feature extraction and dimensionality reduction using PCA, a CB schemes close to *BioHashing* is used employing random projections. The obtained coefficients are binarised and subjected to a fuzzy commitment scheme (FCS), which is a particular CBS approach based on helper data. This approach is used to secure medical data on a smart-card [9]. A second approach combining CB and BCS is suggested in [10], where bio-hashing is applied to features generated by applying Gabor

978-1-7281-3217-4/19/$31.00 ©2019 IEEE

filters, LDA and FCS as well as the fuzzy vault scheme. Another approach to combine CB and BCS is proposed in [11], where finger vein minutiae are extracted and random projections are used to achieve revocability and dimensionality reduction while a so-called deep network architecture ensures irreversible templates. In [12], features with low intra-class scatter and high inter-class scatter (found by Fisher discriminant analysis (FDA)) are generated from multiple samples per subject. These features are finally subjected to a quantisation-based key generation where the quantisation parameters (helper data) depend in the distribution of the generated stable features. Another quantisation-based BCS is proposed in [13], where vein intersection points are located by considering a neighbourhood connectivity criteria, after Gabor-based enhancement with subsequent thresholding. However, the generation of a stable key is not discussed as it is just suggested to use a subset of the identified feature points as key material.



(a) GM-R (b) GM-I

Fig. 1: Examples for GM-R and GM-I key-dependent transformation functions.

With respect to *hand vein* template protection schemes, previous literature is sparse: Besides the proposal of a fuzzy vault scheme using dorsal hand vein data [14], only a multimodal template protection approach involving both *hand and palm vein data* exists: It suggests to fuse feature sets of both modalities [15] (where stable vein points extracted from multiple enrolment samples act as feature sets) to create a fuzzy vault where chaff-points are added as in the original scheme. However, the use of dual encryption involving both AES and DES in the second paper remains entirely unclear.

According to Jindal et al. [16] the existing approaches for *face template protection* can also be divided into three major types: BCS, CB, and hybrid approaches which combine CB and BCS. The most prominent face BCS make use of a FCS [17] or a fuzzy vault scheme [18]. They achieve a high level of security, but their weakness lies in dealing with high intra-class variations. Face recognition CB approaches are seen less often [19]. Hybrid methods, representing a combination of both previous approaches, also have limitations for data with high intra-class variability and exhibit high performance losses in such cases, but different CNN-based approaches have been proposed to overcome these limitations e.g. [16]. A template protection scheme for multi-biometrics using a FCS and chaotic system approach was applied on iris, thermal face and visible face images in [20] - this work constitutes the only template protection approach involving thermal face data. A FCS is generated from the corporation of error correcting codes (ECC) and binary features extracted from the facial images. Further, iris feature vectors are extracted and encrypted by the use of a chaotic system. Both parts are finally used in a score level fusion based performance evaluation.

III. Non-invertible Grey-scale Transformation: Many-To-One-Mapping

In this work, we propose a novel template protection approach in the signal domain: grey value many-to-one (GM) mappings. The basic principle of this approach is to transform the grey values of an input image based on an underlying non-injective surjective function, which maps multiple grey values from the input image to one or multiple values in the output image. Many functions are able to satisfy this constraint, however we chose to use the sine function since it offers smooth transitions between neighbouring grey values and helps to better preserve areas of similar grey values in the images. In the following, we project all grey values (0 to 255) to the range $[0, 1]$, thus the adopted functions perform the mapping $[0, 1] \rightarrow [0, 1]$.

Other applicable transformation based privacy protection schemes are proposed by [21] or [22]. These methods have in common that the performed projections prohibit the usage of well-established and well-performing feature extraction schemes in the transformed domain. Thus, the methods cannot be applied in the signal domain and they would result in higher computational costs as well. For these reasons they have not been considered as alternative transformations. Instead, we investigated two different sine-based functions: a regular sine function (*GM-R*) and an irregular sine function based on interpolation of sampled random points (*GM-I*).

For GM-R, the sine function $\sin$ has been adopted to allow the adjustment of two parameters, frequency (f) and phase (p). The adopted sine function is defined as

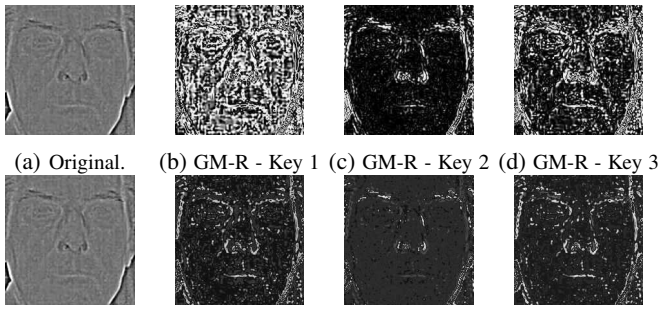
$$\text{GM-R}(x) = \frac{1}{2}\sin(f 2\pi x + p) + \frac{1}{2} \tag{1}$$

where f is the frequency factor and p is the phase factor. The values of these two parameters are then set based on the selected template protection key. An example transformation of a thermal face image is shown in Figure 1. For GM-I, the cardinal sine function sinc is used to interpolate N points randomly sampled in the interval $[0, 1]$. The sinc function is defined as $\text{sinc}(x) = \frac{\sin(\pi x)}{\pi x}$. We can then reconstruct the randomly sampled points S by the countably infinite set of shifted sinc functions, which spans the space of functions limited in the frequency range $\omega = (-\pi, \pi]$. For our function GM-I, we define 1000 integer shifts N in the range $[0, 1]$. Thus, GM-I can be defined as:

$$\text{GM-I}(x) = \frac{1}{1000}\sum_{n=N} S(n)\,\text{sinc}(x - n) \tag{2}$$

where the function GM-I can be reconstructed from the sample points S at integer spacings. The only parameter for GM-I is the seed for the random number generator, which is used to generate the randomly sampled points S. This leads to a highly aperiodic function, as illustrated in Figure 1, which illustrates an exemplary transformation using 4 sample points. Compared

to block re-mapping and block warping no shape or structure information of the biometric trait is distorted. This can be beneficial when the recognition process relies on geometrical features, e.g. landmark based face recognition. Furthermore, these techniques can be applied to every biometric modality if images of the biometric trait are acquired.



(a) Original. (b) GM-R - Key 1 (c) GM-R - Key 2 (d) GM-R - Key 3

(e) Original. (f) GM-I - Key 1 (g) GM-I - Key 2 (h) GM-I - Key 3

Fig. 2: Example of using different template protection keys for GM-R (top row) and GM-I (bottom row).

It is difficult to estimate from a theoretical point of view how the proposed grey value one-to-many mappings will behave in terms of irreversibility, performance and unlinkability aspects. The irreversibility of the proposed approaches is given by design, since multiple grey values are mapped to the same one in the transformed image. However, the irreversibility is highly dependent on the frequency of the underlying sine functions: the higher the frequency, the more grey values are mapped to the same one in the transformed image and thus it is more difficult to fully reconstruct the original image. The performance impact is even harder to assess and is also dependent on the frequency of the underlying function. Especially for GM-I this is highly dependent on the selected template protection key, since the function is highly aperiodic. Therefore, we will focus on an experimental evaluation of these aspects later on in the paper. Figure 2 depicts an example of applying the GM-R and GM-I functions using different template protection keys on the same image.

IV. Block Re-Mapping and Warping

In block re-mapping [1], a number of pre-defined blocks is randomly placed at different positions as they have been located in the original sample. Some blocks that are present in the original sample are dismissed and do not appear in the transformed output. This aspect ensures the irreversibility property of the block re-mapping scheme. To enable comparable results, we fixed the number of blocks that remain in the transformed templates to be at 75% of the original blocks.

Another non-invertible transformation in the context of cancellable biometrics is the so called "warping" (originally named "mesh warping" [23]). Using this transformation, a function is applied to each pixel in the image which maps the pixel of the input at a given position to a certain position in the output (can also be the same position as in the input again). Thus, this mapping defines a new image or template containing the same information as the original input but in a distorted representation, introduced by a piece-wise linear interpolation. For more information about other warping methods the interested reader is referred to [24], where a review of several different possible solutions including the use of parametric and non-parametric functions can be found.

V. Experiments

Dataset: In this work, biometric template protection on hand- and finger veins as well as thermal face is analysed. The data used in the experiments is part of the PROTECT Multimodal DB Dataset (PMMDB) [25]. The PMMDB includes different biometric modalities, namely iris, face (visual light, NIR, 3D and thermal), periocular, anthropometrics and hand- and finger veins of 69 different subjects. It was acquired in two data acquisition events with one year between the two. In the experiments only data acquired in the 2nd event is utilised. Figure 3 visualises some samples of the captured images from all datasets under investigation. The database is available for download at http://projectprotect.eu/.

Fig. 3: Dataset samples - Top (from left to right): *FV-LED-Dorsal*, *FV-Laser-Dorsal*, *Thermal-Face*; bottom: *HV-RL850-Palmar* and *HV-RL850-Dorsal*.

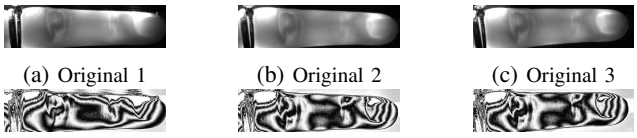
Vascular Based Recognition Tool-Chain: There are several studies about finger vein [26] and hand vein [27] recognition systems that present and discuss different designs, but they all include a few common parts or modules. As the focus of this paper is on template protection applied in the signal domain, the system used during the experiments contains the template protection as part of the pre-processing. For feature extraction one of the best performing methods has been selected: Maximum Curvature (MC) [28]. The final comparison scores are obtained by an image correlation based comparison scheme as introduced by Miura et al. in [29] is applied to the baseline (unprotected) templates (features) as well as to the templates protected by the proposed non-invertible grey value transformations, block re-mapping and warping. An implementation of the complete tool-chain as well as the used configuration files and results are available for download at: http://www.wavelab.at/sources/Debiasi19d.

Thermal Face Based Recognition Tool-Chain: A thermal infrared system seems to be a promising way to complement facial recognition systems in visible range [30]. For example, thermal imaging does not need illumination and relies on passive detection of infrared emissions, but is sensitive to changes of emotional, physical, health condition of the subject and several others. The deployed face detection method, Faster-RCNN deep learning, is based on ResNet-50. The architecture

computes candidate regions while a separate sub-network is used to predict the region proposals. After a reshaping, using a RoI pooling layer a Difference of Gaussians filtering has been applied to reduce the fluctuations of temperature of the subject's face and environment visible in the acquired images. Finally, the detected face must be translated into specific patterns which allow to compare one to another. Local features provided higher recognition accuracy, LBP has been selected as the best performing one according to [30]. During the subsequent matching process, the extracted features of two facial samples are compared using the Euclidean distance metric against a threshold calculated on the entire dataset.

A. Evaluation Protocol

In order to evaluate the effects of applying the proposed signal domain template protection approach(es), we evaluate the impact on the recognition performance as well as the unlinkability of the templates generated with distinct keys. The parameters for the different template protection approaches have been selected as follows: *GM-R:* Frequency factor f between 3 and 6, Phase factor p between 0 and 1; *GM-I:* 4 randomly sampled points; *Block Re-Mapping (R):* Block sizes of 16/32/64 pixels; *Warping (W):* Block sizes of 16/32/64 pixels with warping offsets of 6/12/24 pixels, respectively. The values for each parameter are determined by a random selection within the value boundaries above, where the selection is based on the template protection key.



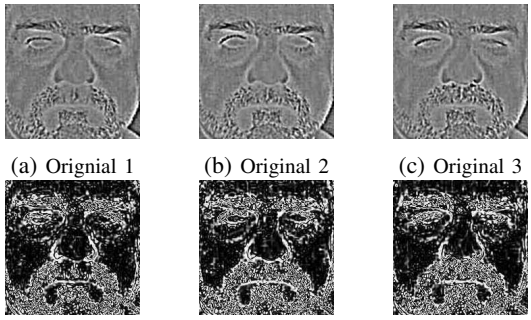
(a) Original 1 (b) Original 2 (c) Original 3

(d) Protected 1 (e) Protected 2 (f) Protected 3

Fig. 4: Applying the GM-R template protection scheme to images of the same subject with different illumination.

Performance: The baseline recognition performance is established by using the original - unprotected data. We calculate the Equal Error Rate (EER) for all comparisons within each dataset for all modalities, i.e. the full range of images is used to compute the genuine and impostor comparison scores. With this baseline numbers the impact of the various template protection approaches on the recognition performance can be assessed by first applying the template protection scheme to the whole dataset (system key) using a fixed but arbitrary key and afterwards computing all genuine and impostor comparison scores. This process is repeated for 10 random keys, where we report the minimum, mean and maximum EER and standard deviation (σ) of all keys.

Unlinkability: This property guarantees that stored and protected biometric information can not be linked across various different applications or databases [6]. Gomez et al. [31] present a universal framework to evaluate the unlinkability of a biometric template protection system based on the comparison scores. They proposed the so called D_{sys} measurement as a global measure to evaluate a given biometric recognition and template protection system. The D_{sys} ranges normally 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. Furthermore, the authors of [31] stipulated that 10 different keys should be considered and thus, we have also selected 10 different keys for our performance and unlinkability analysis.



(a) Orignial 1 (b) Original 2 (c) Original 3

(d) Protected 1 (e) Protected 2 (f) Protected 3

Fig. 5: Applying the GM-R template protection scheme to images of the same subject with consistent illumination.

B. Results

The recognition performance results and the unlinkability evaluation of the conducted experiments are presented in Table I. The first column contains the dataset name and the baseline EER performance computed using the unprotected (original) images. These values are used as reference for the mean recognition performance employing template protected data, which is presented in column three. The table contains only the most interesting results.

It can be observed, that the obtained performance differences vary among the biometric modalities: *a)* The proposed GM schemes perform worse than the other two template protection schemes (warping and block re-mapping) for finger vein data (*FV-LED-Dorsal*and *FV-Laser-Dorsal*). However, all investigated template protection schemes show a very high performance degradation for these finger vein datasets. *b)* For hand vein data (*HV-RL850-Dorsal*and *HV-RL850-Palmar*) and thermal face data (*Thermal-Face*), the lowest performance loss is achieved by warping, though the proposed GM schemes exhibit a very similar performance to warping and a much better performance when compared to block re-mapping. The performance variation among different keys shows a similar behaviour to the other two template protection schemes, thus it is quite low in general.

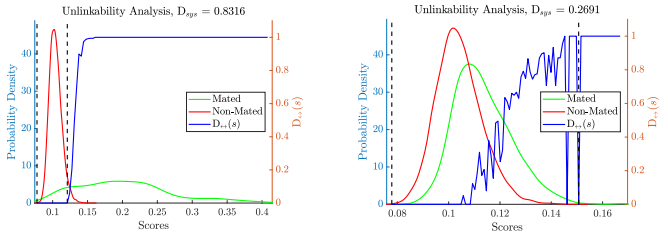
In general, the proposed GM schemes lead to only a slight performance loss for hand vein and thermal face data (comparable to warping), but come with severe performance penalties for finger vein data. This trend can be explained by the differing illumination properties of the finger vein data compared to the hand vein and thermal face data. During the acquisition of the finger vein data, the illumination is adjusted for each image, which leads to inconsistent illumination conditions among the images of a subject and therefore different grey values in the

	Method	Recog. Perf. EER [%]		Unlinkability D_{sys} [%]	
		Mean	σ	Mean	σ
FV-LED-Dorsal Orig. EER: 0.13%	GM-R	7.49	1.91	48.53	18.77
	GM-I	10.74	1.58	61.88	28.92
	R 16	6.47	0.48	3.84	0.65
	R 32	6.87	0.65	4.79	1.14
	R 64	9.81	1.18	6.00	3.04
	W 16	2.67	0.87	92.22	1.55
	W 32	7.07	1.21	52.20	10.73
	W 64	6.12	2.55	33.84	15.19
FV-Laser-Dorsal Orig. EER: 1.67%	GM-R	11.66	1.58	44.53	18.17
	GM-I	13.86	1.51	59.48	25.11
	R 16	7.12	0.41	4.01	0.72
	R 32	7.78	0.74	5.18	1.18
	R 64	11.37	1.35	6.77	2.96
	W 16	5.48	0.90	88.85	1.71
	W 32	8.37	0.96	47.50	10.29
	W 64	7.06	1.54	30.71	14.44
HV-RL850-Dorsal Orig. EER: 6.67%	GM-R	6.77	0.57	52.64	21.63
	GM-I	7.53	0.83	61.06	23.36
	R 16	18.95	1.04	6.96	0.84
	R 32	20.17	1.31	7.25	1.22
	R 64	23.94	2.08	8.61	1.94
	W 16	6.68	0.43	92.20	0.40
	W 32	10.07	0.94	76.66	3.29
	W 64	12.18	2.41	47.92	10.72
HV-RL850-Palmar Orig. EER: 5.65%	GM-R	10.44	2.12	49.03	21.77
	GM-I	11.65	1.75	63.35	22.03
	R 16	15.81	1.02	6.47	0.93
	R 32	19.03	1.27	7.52	1.51
	R 64	22.84	2.00	8.12	2.45
	W 16	8.07	0.61	88.97	0.38
	W 32	9.70	0.58	81.00	1.83
	W 64	11.09	1.64	63.96	7.29
Thermal-Face Orig. EER: 11.52%	GM-R	13.36	1.41	51.48	11.88
	GM-I	11.59	0.54	63.13	11.86
	R 16	15.22	2.36	24.00	2.20
	R 32	15.60	1.72	27.68	3.94
	R 64	15.15	2.33	29.95	8.68
	W 16	12.69	1.22	68.52	2.40
	W 32	10.97	2.11	68.26	3.61
	W 64	11.36	1.15	65.06	4.02

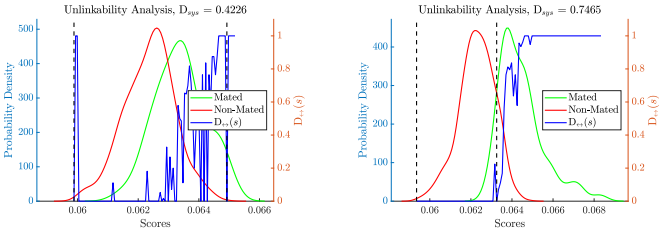
TABLE I: Recognition performance and unlinkability analysis.

same areas of the images. Since the GM schemes transform the grey values, this leads to dissimilar transformed images for a subject, which further leads to failed genuine matches. An example can be seen in Figure 4, which shows three different images of the same subject and the effects of applying the GM-R scheme: the first two with very similar illumination and the third one with different illumination. If the illumination is consistent among the various images of the same subject, as in the hand vein and thermal face datasets where the illumination is fixed for all acquisitions, applying the GM-R scheme also leads to very similar results as presented in Figure 5. Therefore, a consistent illumination plays an important role when the GM schemes are applied in conjunction with geometry or shape based recognition systems, e.g. vascular recognition.

As reported above, warping yields the lowest EER performance degradation, followed by the GM schemes and lastly block re-mapping. Contrary to the performance, the unlinkability evaluation, presented in the last two columns of Table I, reveals a different trend: Block re-mapping yields the best (lowest) D_{sys} scores, followed by the GM schemes and the worst scores are obtained by warping. It is observable that the mean D_{sys} scores of the GM schemes are right in between of warping and block-remapping. The fluctuation of the D_{sys} values of GM, however, is very high compared to the other two template protection schemes, which means that the unlinkability for the GM is highly key dependent. Some examples for this variability are illustrated in Figure 6, where the blue curve represents the process of D_{sys} for all threshold selections, the green curve shows the intra-subject (mated) scores and the inter-subject (non-mated) scores computed between different keys. According to [31], a *fully unlinkable* scenario can be observed if both green and red distributions are identical (low D_{sys} value). A detailed analysis of the key dependency for the various template protection schemes is left for future work.



(a) HV: GM-R Key 1 vs 2 (b) HV: GM-R Key 1 vs 9



(c) TF: GM-I Key 1 vs 7 (d) TF: GM-I Key 2 vs 4

Fig. 6: Examples for D_{sys} variation between different key pairs for *HV-RL850-Dorsal* (HV, top) and *Thermal-Face* (TF, bottom) data sets and GM-R and GM-I transforms.

Summarising, we can report that a low recognition performance loss usually leads to bad unlinkability. The proposed GM schemes show comparable performance to warping, but exhibit a much better unlinkability. They offer a trade-off between performance loss and unlinkability in most cases, while the other two investigated template protection schemes either have a low performance loss but bad unlinkability (warping), or have a relatively high performance loss but good unlinkability (block re-mapping). However, the provided level of privacy protection, especially if it comes to unlinkability is clearly not sufficient for a practical application of warping based cancellable schemes. Furthermore, the severe performance drop restricts the use of block re-mapping schemes for real world biometric systems in the most cases as well. Finally, a potential combination of warping and a GM scheme could *i)* still maintain the recognition performance, while *ii)*

D_{sys} might be reduced to an acceptable amount. This would probably enable the usage of a combined warping and non-invertible grey-scale transform template protection scheme in practical applications.

VI. Conclusion

In this study two well-established (block re-mapping, warping) and a newly proposed non-invertible grey-value based template protection schemes are evaluated on a multi-biometrics datasets including finger-vein, hand-vein and thermal face images in the signal domain. The evaluation process regarding performance and unlinkability aspects revealed that the proposed grey-value based techniques, GM-R and GM-I, show comparable recognition performance to warping, but exhibit a much better unlinkability. The proposed scheme offers a trade-off between recognition performance loss and unlinkability in most cases, while block re-mapping and warping are not able to perform well in terms of recognition performance and unlinkability at the same time. Future work will include combining warping and the proposed non-invertible grey-scale transform template protection scheme to possibly maintain the recognition performance, while reducing the unlinkability to an acceptable level. Furthermore, a detailed key dependency, irreversibility and security analysis is planed as well as the evaluation of the proposed method on other image based biometric modalities.

Acknowledgements: This project received funding from the European Union's Horizon 2020 research and innovation program under grant agreements No. 700259 (PROTECT) and 690907 (IDENTITY).

References

[1] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[2] J. Hämmerle-Uhl, E. Pschernig, and A. Uhl, "Cancelable iris biometrics using block re-mapping and image warping," in *Proceedings of the 12th International Information Security Conference (ISC'09)*, ser. LNCS, P. Samarati, M. Yung, F. Martinelli, and C. Ardagna, Eds., vol. 5735. Springer Verlag, 2009, pp. 135–142.

[3] Y.-L. Lai, Z. Jin, A. B. J. Teoh, B.-M. Goi, W.-S. Yap, T.-Y. Chai, and C. Rathgeb, "Cancellable iris template generation based on indexing-first-one hashing," *Pattern Recognition*, vol. 64, pp. 105–117, 2017.

[4] E. Piciucco, E. Maiorana, C. Kauba, A. Uhl, and P. Campisi, "Cancelable biometrics for finger vein recognition," in *Sensing, Processing and Learning for Intelligent Machines (SPLINE), 2016 First International Workshop on*. IEEE, 2016, pp. 1–5.

[5] C. Rathgeb, A. Uhl, and C. Busch, "Ageing effects and implications for biometric template protection," in *Age Factors in Biometric Processing*, M. Fairhurst, Ed. London, UK: IET, 2013, ch. 4.3, pp. 321–341.

[6] "Security techniques – biometric information protection," International Organization for Standardization, Standard, June 2011.

[7] D. Hartung, M. A. Olsen, H. Xu, H. T. Nguyen, and C. Busch, "Comprehensive analysis of spectral minutiae for vein pattern recognition," *IET Biometrics*, vol. 1, no. 1, pp. 25–36, 2012.

[8] M. Gomez-Barrero, C. Rathgeb, G. Li, R. Ramachandra, J. Galbally, and C. Busch, "Multi-biometric template protection based on bloom filters," *Information Fusion*, vol. 42, pp. 37 – 50, 2018.

[9] W. Yang, S. Wang, J. Hu, Z. Guanglou, J. Chaudhry, E. Adi, and C. Valli, "Securing mobile healthcare data: A smart card based cancelable finger-vein bio-cryptosystem," *IEEE Access*, vol. 06, pp. 36 939 – 36 947, 2018.

[10] W. Yang, J. Hu, and S. Wang, "A finger-vein based cancellable bio-cryptosystem," in *Network and System Security - 7th International Conference, NSS 2013, Madrid, Spain, June 3-4, 2013. Proceedings*, 2013, pp. 784–790.

[11] Y. Liu, J. Ling, Z. Liu, J. Shen, and C. Gao, "Finger vein secure biometric template generation based on deep learning," *Soft Comput.*, vol. 22, no. 7, pp. 2257–2265, 2018.

[12] Z. Wu, L. Tian, P. Li, T. Wu, M. Jiang, and C. Wu, "Generating stable biometric keys for flexible cloud computing authentication using finger vein," *Information Sciences*, vol. 433-434, pp. 431–447, 2016.

[13] J. Chavez-Galaviz, J. Ruiz-Rojas, and A. Garcia-Gonzalez, "Embedded biometric cryptosystem based on finger vein patterns," in *12th International Conference on Electrical Engineering, Computing Science and Automatic Control, CCE 2015, Mexico City, Mexico, October 28-30, 2015*, 2015, pp. 1–6.

[14] V. Brindha, "Biometric template security using dorsal hand vein fuzzy vault," *Biometrics & Biostatistics*, vol. 3, no. 4, p. 1000145, 2012.

[15] N. Lalithamani and M. Sabrigiriraj, "Palm and hand vein-based fuzzy vault generation scheme for multibiometric cryptosystem," *The Imaging Science Journal*, vol. 63, no. 2, pp. 111–118, 2015.

[16] A. K. Jindal, S. Chalamala, and S. K. Jami, "Face template protection using deep convolutional neural network," in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. IEEE, 2018, pp. 575–5758.

[17] H. Lu, K. Martin, F. Bui, K. N. Plataniotis, and D. Hatzinakos, "Face recognition with biometric encryption for privacy-enhancing self-exclusion," in *2009 16th International Conference on Digital Signal Processing*. IEEE, 2009, pp. 1–8.

[18] Y. Wu and B. Qiu, "Transforming a pattern identifier into biometric key generators," in *2010 IEEE International Conference on Multimedia and Expo*. IEEE, 2010, pp. 78–82.

[19] A. B. Teoh, A. Goh, and D. C. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 1892–1901, 2006.

[20] N. Wang, Q. Li, A. A. A. El-Latif, J. Peng, X. Yan, and X. Niu, "A novel template protection scheme for multibiometrics based on fuzzy commitment and chaotic system," *Signal, Image and Video Processing*, vol. 9, no. 1, pp. 99–109, 2015.

[21] P. Boufounos and S. Rane, "Secure binary embeddings for privacy preserving nearest neighbors," in *2011 IEEE International Workshop on Information Forensics and Security*. IEEE, 2011, pp. 1–6.

[22] B. Razeghi, S. Voloshynovskiy, D. Kostadinov, and O. Taran, "Privacy preserving identification using sparse approximation with ambiguization," in *2017 IEEE Workshop on Information Forensics and Security (WIFS)*. IEEE, 2017, pp. 1–6.

[23] G. Wolberg, "Image morphing: a survey," *The visual computer*, vol. 14, no. 8, pp. 360–372, 1998.

[24] C. A. Glasbey and K. V. Mardia, "A review of image-warping methods," *Journal of applied statistics*, vol. 25, no. 2, pp. 155–171, 1998.

[25] 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 multimodal db: a multimodal biometrics dataset envisaging border control," in *Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG'18)*, Darmstadt, Germany, 2018, pp. 1–8.

[26] M. Jadhav and P. RavaleNerkar, "Survey on finger vein biometric authentication system," *International Journal of Computer Applications*, no. 3, pp. 14–17, 2015.

[27] H. Luo, F.-X. Yu, J.-S. Pan, S.-C. Chu, and P.-W. Tsai, "A survey of vein recognition techniques," *Information Technology Journal*, vol. 9, no. 6, pp. 1142–1149, 2010.

[28] N. Miura, A. Nagasaka, and T. Miyatake, "Extraction of finger-vein patterns using maximum curvature points in image profiles," *IEICE TRANSACTIONS on Information and Systems*, vol. 90, no. 8, pp. 1185–1194, 2007.

[29] ——, "Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification," *Machine vision and applications*, vol. 15, no. 4, pp. 194–203, 2004.

[30] A. Grudzien, N. Palka, and M. Kowalski, "Simple thermal to thermal face verification method based on local texture descriptors," in *12th Conference on Integrated Optics: Sensors, Sensing Structures, and Methods*, vol. 10455. International Society for Optics and Photonics, 2017, p. 104550C.

[31] 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*, vol. 13, no. 6, pp. 1406–1420, 2018.