Finger Vein Template Protection Based on Alignment-Robust Feature Description and Index-of-Maximum Hashing

Simon Kirchgasser, *Student Member, IEEE*, Christof Kauba, *Student Member, IEEE*, Yen-Lung Lai, Jin Zhe, *Member, IEEE*, and Andreas Uhl, *Senior Member, IEEE*

***Abstract*—Privacy preserving storage and secure processing of biometric data is a key issue that has to be addressed in finger vein recognition systems as well. Various template protection approaches originally proposed for well established biometric modalities have been adopted to the domain of finger vein authentication. However, these adopted methods have the disadvantage that they are not designed for finger vein patterns in particular and are thus, sub-optimal in several ways. In this study we propose an alignment-robust template protection scheme that is based on an efficient binary representation of finger vein patterns on the one hand and is further using the advantages of Index-of-Maximum (IoM) hashing to fulfill mandatory privacy and security based characteristics on the other hand. The proposed method is compared to block re-mapping and warping regarding recognition performance and is analyzed with respect to security and privacy aspects. The analysis is further extended to robustness against misalignment of the finger vein data and a combination of block re-mapping/warping and the proposed method is investigated as well.**

***Index Terms*—Finger vein template protection, cancellable biometrics, alignment-robust feature description, index-of-maximum hashing, performance evaluation, non-invertibility analysis, unlinkability analysis.**

I. Introduction

DESPITE the excellent usability of biometrics in authentication, privacy invasion and impersonation may occur if the biometric template is compromised or stolen. This is further complicated by the fact that biometric traits are irrevocable and irreplaceable. Hence, templates compromised once imply a permanent loss of identity. Biometric template protection (BTP) techniques were invented to tackle these and further challenges. An effective biometric template protection scheme should fulfill four requirements as specified in ISO/IEC Standard 24745 [1] and 30136 [2]: *Non-invertibility or Irreversibility*, *Revocability or Renewability*, *Non-linkability or Unlinkability* and *Performance preservation*.

The current BTP methods proposed in literature can be broadly divided into feature transformations (cancellable biometrics - CB) and biometric cryptosystems (BCS) [41]. Another class of BTP schemes is discussed as an alternative to CB, Homomorphic Encryption (HE) [53]. HE allows template comparisons to be performed in the encrypted domain without using helper data and receiving the same comparison results as done in the decrypted domain. However, the computational costs often prohibit its practical application.

CB rely on the application of a transformation function to a biometric template or a biometric sample. This can be done by applying invertible (salting) or non-invertible transformations. If an adversary gets access to the key used in the context of salting, the original data can be restored by inverting the salting method. This drawback can be solved by applying non-invertible transformations as they are based on one-way functions which can not be reversed in polynomial time (NP hard problems). The main advantage of CB is that the necessary comparisons to authenticate subjects can be done directly in the transformed domain.

A BCS is a process that either securely binds a secret key (e.g., PIN, private keys) to a biometric template and thus, generates the protected biometric template, or directly generates the cryptographic key from biometric features so that neither the key nor the biometric template can be retrieved from the protected biometric template. Hence, the template comparison is not done directly on the biometric templates. In particular, only if a genuine biometric trait is presented during the authentication process the corresponding correct key is retrieved.

In this work, we propose a CB scheme, namely Alignment-Robust Hashing (ARH) for finger vein biometrics. This scheme was developed for finger vein biometrics because of two main reasons: first, finger vein biometrics exhibit several advantages compared to other well established ones (high accuracy [21], insensitivity to skin condition changes and high security [23]). Second, there are no template protection schemes available originally designed for finger vein biometrics which results in some problems regarding the application

Manuscript received October 15, 2019; revised January 8, 2020; accepted March 9, 2020. Date of publication March 23, 2020; date of current version September 23, 2020. This work was supported in part by the European Union's Horizon 2020 Research and Innovation Program under Grant 700259 (PROTECT) and Grant 690907 (IDENTITY), and in part by FWF Project regarding finger vein recognition under Grant P32201_P. This article was recommended for publication by Associate Editor I. Kakadiaris upon evaluation of the reviewers' comments. *(Corresponding author: Simon Kirchgasser.)*

Simon Kirchgasser, Christof Kauba, and Andreas Uhl are with the Department of Computer Scienes, University of Salzburg, 5020 Salzburg, Austria (e-mail: skirch@cs.sbg.ac.at; ckauba@cs.sbg.ac.at; uhl@cs.sbg.ac.at).

Yen-Lung Lai and Jin Zhe are with the School of Information Technology, Monash University, Subang Jaya 47500, Malaysia (e-mail: yenlung.lai@monash.edu; jin.zhe@monash.edu).

Digital Object Identifier 10.1109/TBIOM.2020.2981673

of adopted template protections methods as follows. Most finger vein recognition systems relying on binarized vascular patterns are using a correlation based strategy to compare the templates. Shifting the templates against each other during template comparison is required to compensate displacements introduced during the image acquisition. After applying a template protection scheme, shifting of the protected templates is not possible as the used transformation is typically not shift invariant. Thus, recently developed non-invertible transforms that are providing good recognition performance and privacy protection, e.g., Bloom Filters [39] or Indexing-First-One (IFO) hashing [24] (both are adoptable for finger vein biometrics in principle) suffer from alignment problems. As a consequence, there are two strategies to overcome this problem: *a)* all shifted variations of a protected template must be stored during the enrollment (results in a very large "master-template") or *b)* during the comparison of the templates all shifted variations must be transformed and compared to each other (very high computational costs). Both presented strategies can not be applied in real world applications as processing speed is crucial. In this work we propose a new feature extraction process mitigating the need for displacement compensation during template comparison. The proposed method computes local distances among vein patterns from vein feature blocks to form an alignment-robust descriptor which is combined with IoM hashing [19] to fulfill the ISO/IEC Standard 24745/30136 template protection requirements without an increase in template size or computational costs. The proposed method is analyzed regarding recognition performance, security and privacy aspects. The analysis also includes a comparison to other non-invertible CB transformations, namely *block re-mapping* and *warping*, which have already been utilized to protect finger vein templates [32].

The current work is mainly based on a previously published study [22] and extends this study by additional experiments and insights, including a runtime analysis. These experiments are on the one hand focusing on how robust the proposed method is to coarsely aligned input images and on the other hand a combination of block re-mapping/warping and the proposed feature descriptor is analyzed as well. The first question regarding the alignment issue is important as in our previous publication [22] we claimed to establish an alignment-free finger vein feature descriptor and template protection method. Nevertheless, in the aforementioned work no discussion was done on how robust the scheme is against misalignment which is *a)* frequently present in finger vein data and *b)* a crucial aspect regarding the performance of a template protection scheme. A recognition performance degradation is expected if template protection is applied but it should be kept at a minimum level. The combination of the two well-established CB schemes block re-mapping and warping and the newly proposed feature descriptor have the potential to maintain the recognition performance obtained by warping [22], while improving the unlinkability at the same time. Thus, the main focus of these experiments will be on the combination of warping and the ARH feature descriptor, but we also present results obtained for the combination of block re-mapping and the proposed descriptor to have comparable results.

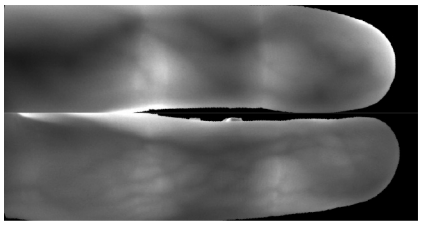


Fig. 1. Two finger vein images captured from the palmar view (PLUSVein-FV3 LED subset).

The rest of this paper is organized as follows: in Section II a brief discussion about finger vein biometrics is given before we provide a compact literature review on related BTP techniques in Section III. Subsequently, the proposed template protection scheme is explained and the applied concepts are described in detail in Section IV. Section V illustrates the experimental set-up (including the used datasets) and describes the methodology of the extended experiments. The recognition performance results, introduced in [22] are discussed in Sections V-A and V-B. This evaluation is extended by a runtime analysis, which is presented in Section V-C. The corresponding experimental evaluation regarding non-invertibility and unlinkability is presented in Sections V-D and V-E, respectively. The experimental results for the extended experiments are described and discussed in Sections V-F and V-G. Finally, Section VI concludes this study along with an outlook on future work.

II. Finger-Vein Biometrics

Finger-vein based biometric systems rely on the structure of vascular patterns which are formed by the blood vessels inside the human finger tissue. The blood vessels lie beneath the human skin and the haemoglobin contained in the blood absorbs near-infrared light. Hence, it is necessary to use NIR light based scanners to make their structure visible as dark lines on the resulting images. These images are then further processed by the recognition system. Example images are given in Figure 1.

There are several studies focusing on the presentation and discussion of finger vein recognition systems, e.g., [50]. The system may contain an optional template protection module, applied either after the pre-processing module (image domain) or after the feature extraction module (feature domain). Our proposed template protection scheme is applied in the feature domain.

During pre-processing the ROI (region of interest), which contains the finger vein patterns, is extracted first in our used tool-chain. After the ROI extraction, the vein pattern's visibility is enhanced by applying High Frequency Emphasis Filtering (HFE) [55], Circular Gabor Filter (CGF) [54] and CLAHE (local histogram equalisation). After the visibility was enhanced, vein feature extraction methods are applied. We selected six techniques outputting the binary vessel structure (however, there are minutiae-related extraction methods,

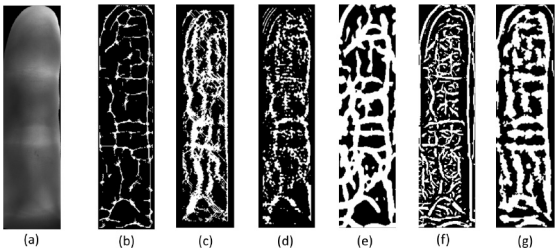


Fig. 2. Features taken from an example finger vein image: (a) Original FV image (b) MC, (c) RLT, (d) WLD, (e) PC, (f) GF and (g) IUWT.

e.g., [6] as well). The employed extraction schemes are *Gabor Filter (GF)* [23], *Isotropic Undecimated Wavelet Transform (IUWT)* [43], *Maximum Curvature (MC)* [31], *Principal Curvature (PC)* [5], *Repeated Line Tracking (RLT)* [30], and *Wide Line Detector (WLD)* [17]. Further details regrading these methods are given in [20]. Example images of binary feature representations extracted by the aforementioned schemes are shown in Figure 2. The BTP techniques discussed in this work are applied to these extracted features.

Using the unprotected templates, these binary feature templates are subsequently compared using an approach proposed by Miura *et al.* [31], the Miura matcher. In most cases input images are not registered and only coarsely aligned to each other. Thus, the method is based on the correlation between the input image and x- and y-direction shifted versions of the reference image. The maximum of the determined correlation values is normalized and then used as final comparison score. This method can be applied both during baseline experiments conducted on the original, non protected input templates and during the experiments performed on the protected templates generated by block re-mapping and warping. The protected templates generated by the proposed alignment-robust scheme are compared in a different manner (see Section IV-B for details).

III. Finger-Vein Template Protection

The main research objective of this work are CBs, which belong to the class of non-invertible transforms [18]. CBs have been successfully applied to many traditional biometric characteristics, including fingerprint ([3], [8], [36], [37], [38], [46], [49]), face ([3], [36], [42], [44]), iris ([13], [33], [34], [40], [56]), palmprint ([7], [25]) and online signature ([27], [28], [29]), among others. However, as this study is proposing and analysing a template protection scheme, which was designed for finger vein biometrics we will give a more detailed literature review on template protection for this specific biometric modality.

An analysis of two CB schemes was conducted by Piciucco *et al.* [32]. They analyzed applicability and security aspects of block re-mapping [36] and block based warping [47] which originally have not been proposed for finger veins, but for fingerprints and face biometrics [36]. The authors applied the aforementioned approaches in the image domain, while all techniques we apply and describe subsequently operate in the feature (i.e., template) domain. We use their approach for comparison purposes. However, we apply it to generated binary templates after feature extraction and therefore in the current study block re-mapping and warping are conducted in the feature domain instead of the image one as done by Piciucco *et al.* [32].

A direct application of BCS, i.e., a Fuzzy Commitment Scheme (FCS), which is a particular CBS approach based on helper data, to binary finger vein data is demonstrated in [14]. In a similar approach, in [9] an FCS is applied too, but the authors tackle the issue of bias in the binary data (as non-vein pixels are in clear majority compared to vein pixels) by applying no vein detection/extraction but a simple thresholding scheme using the median. There are techniques, which apply both CB and BCS to binary features: after applying a set of Gabor filters for feature extraction and subsequent dimensionality reduction using PCA, a CB scheme close to *BioHashing* is used to employ random projections [52]. The obtained coefficients are binarized and subjected to an FCS. This approach is used to secure medical patients' health records on a smartcard [52]. A second approach combining CB and BCS is suggested in [51], where bio-hashing is also applied to features generated by applying Gabor filters and subsequent LDA. The binary string is then subjected to FCS and also to a fuzzy vault scheme (where the binary string is somewhat artificially mapped into points used in the vault). Another approach to combine CB and BCS is proposed in [26], where finger vein minutiae are extracted and random projections are used to achieve revocability and dimensionality reduction. Afterwards, a so-called deep belief network architecture learns irreversible templates.

Minutiae-based feature representations exhibit an important drawback: they are no fixed length representations, which is a prerequisite for the application of several template protection schemes. Therefore, techniques developed in the context of finger print minutiae-representations have been transferred to vein minutiae representations, i.e., vein minutiae cylinder-codes [16] and vein spectral minutiae representations [15]. The latter representations are subjected to binarization and subsequently fed into Bloom filters to result in a CB scheme which avoids position correction during template comparison as required by many techniques based on vascular structure representation [12].

A BCS approach based on quantization is proposed in [48]: based on multiple samples per subject (i.e., class), features with low intra-class scatter and high inter-class scatter (found by Fisher discriminant analysis (FDA)) are generated, which are finally subjected to a quantization-based key generation where the quantization parameters (helper data) depend on the distribution of the generated stable features. Another quantization-based BCS is proposed in [4], where vein intersection points are located by considering a neighborhood 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. According to [14] it is possible to extract information regarding the presence or absence of various diseases like arteriovenous malformation from finger vein patterns. Thus, the authors examined the necessity of finger vein data privacy protection

methodologies and established a privacy enhancing scheme that allows a robust authentication while preserving the capture subject's privacy. The recognition process is based on the use of a hash and Gaussian error functions which are applied by selecting reliability bit vectors containing helper data and describing the presence or absence of a disease.

IV. An Alignment-Robust CB Scheme

It is known that vein feature templates contain a majority of black background pixels, thus the binary finger vein feature is usually sparse. Consequently, slight displacements between an enrolled vein template and a query vein template would lead to a significant row-wise or column-wise dissimilarity. Hence, a proper alignment of the templates is a crucial step to obtain a sufficient recognition performance. The common strategy to alleviate alignment issues is to perform multiple comparisons with bit-by-bit shifts among binary templates. Moreover, the bit-by-bit shifts have to be carried out in both vertical and horizontal directions due to the arbitrary placement of finger during image acquisition [30], [31]. This computationally costly comparison strategy leads to high computational load, especially for carrying out identification on a large database. This computational load is further increased if BTP schemes need to be applied as well. Thus, we designed a BTP scheme for finger vein template protection with an alignment-robust property that also enables a faster template comparison than achieved using by bit-by-bit shifting. A runtime evaluation is presented in Section V-C.

A. Alignment-Robust Feature Descriptor

Let $d(i,j)$ be the local distance between the i-th and j-th locations in a binary vector $V = (v_1, \ldots, v_n)$ where $v_i, v_j \in \{0, 1\}$. In particular:

$$d(i,j) = |i - j| \tag{1}$$

and Kronecker delta functions $\delta(v_i, v_j)$:

$$\delta\big(v_i, v_j\big) = \begin{cases} 0 & \text{if } v_i \neq v_j \\ 1 & \text{if } v_i = v_j \end{cases} \tag{2}$$

Then we combine Eq. (1) and Eq. (2). This leads to the alignment-robust transformation, denoted as $\mathbf{T}$ over a vector V which is described as:

$$\mathbf{T}_k(V) = \sum_{i>j} \delta(d(i,j) - k)\delta(v_i, 1)\delta\big(v_j, 1\big) \tag{3}$$

where n represents the length of the given binary vector V and $k \in \{1, 2, \ldots, n\}$. Eq. (3) shows us that $\mathbf{T}$ in fact is designed to measure the number of pairs of 1s (representing vein information) in the binary feature template that have a local distance k. We utilize the local feature (e.g., local distance) to replace the prior alignment required by global features as used in other algorithms (e.g., [31]). Thus, the employment of local distance measures as invariant feature descriptor eliminates the requirement of alignment from finger vein recognition.

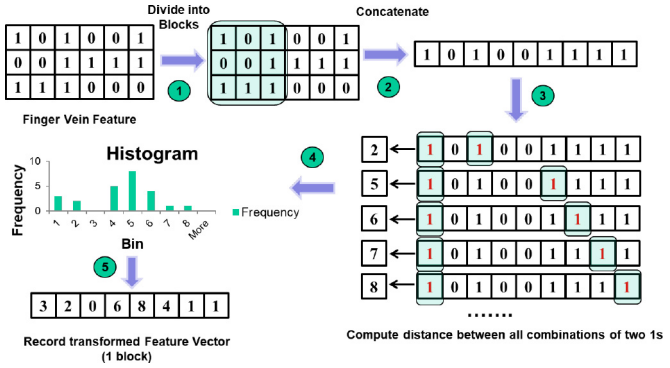


Fig. 3. The overall flow of the ARH protection scheme.

Algorithm 1 Alignment-Robust Hashing (ARH)

Input: Finger-Vein Feature Template $\mathbf{x} \in \{0, 1\}^{n \times m}$
Output: Hashed Code $\mathbf{x_{hash}}$

Step 1: Non-Overlapped Blocks Formulation
Let $x_{block} \in \{0, 1\}^{b_n \times b_m}$ be a block
$x_{block(1,1)} \leftarrow x[1 : b_n, 1 : b_m]$

for $i \leftarrow 2$ to $\left\lfloor \frac{n}{b_n} \right\rfloor$ and $j \leftarrow 2$ to $\left\lfloor \frac{m}{b_m} \right\rfloor$ **do**
$\mathbf{x_{block(i,j)}} \leftarrow x[i \times b_n + 1 : (i+1) \times b_n, j \times b_m + 1 : (j+1) \times b_m]$

Step 2: 1-Dimensional Binary Vector Generation
for $i \leftarrow 1$ to b_n **do**
$\mathbf{x_{bin}} = [x_{block(i)} | x_{block(i+1)} | \ldots | x_{block(b_n)}]$
where | denotes a concatenation function

Step 3: Invariant Feature Computation
for any two 1s (all combinations) in x_{bin} **do**
Compute distance $d(i,j) = |i - j|$
between $x_{bin(i)}$ and $x_{bin(j)}$,
where $x_{bin(i)} = x_{bin(j)} = 1$
Store the computed distances in $x_{dis(i)}$

Step 4: Histogram Formulation from x_{dis}
$\mathbf{h} = [h(1), \ldots, h(n_{blocks})]$, where
$h(i) = \sum_{j=1}^{b_n \times b_m - 1} x_{dis(j)}$

Step 5: ARH Code Generation from h
$\mathbf{x_{hash}} \leftarrow \mathbf{h}$, thus $\mathbf{x_{hash}} = [h(1), \ldots, h(n_{blocks})]$

B. Alignment-Robust Hashing (ARH) and Template Comparison

In this section, we introduce our feature transformation scheme, the *Alignment-Robust Hashing (ARH)*, in detail. The proposed method is based on the feature descriptor described in Section IV-A. We extend ARH from a mathematical notation to a complete procedure for the sake of readability. Let $\mathbf{x} \in \{0, 1\}^{n \times m}$ be a binary finger vein feature template, extracted using any of the six utilized feature extraction schemes (GF, IWUT, MC, PC, RLT and WLD), that can be interpreted as a matrix, with a size of $n \times m$. In Figure 3 the feature descriptor's building process is displayed according to the algorithmic five-step procedure described in Algorithm 1.

During template comparison of a gallery template $X_{hash} = [X_{hash(1)}, \ldots, X_{hash(n_{block})}]$ and a newly acquired probe template $X'_{hash} = [X'_{hash(1)}, \ldots, X'_{hash(n_{block})}]$ the cosine similarity

(mean) between these two hashed codes is calculated using Eq. (4) where $\|.\|$ represents Euclidean norm:

$$S\left(X_{hash}, X'_{hash}\right) = \frac{1}{n_{block}} \sum_{i=1}^{n_{block}} \frac{X_{hash(i)} \times X'_{hash(i)}}{\left\|X_{hash(i)}\right\| \times \left\|X'_{hash(i)}\right\|} \quad (4)$$

As $S(X_{hash}, X'_{hash}) \in [0, 1]$, a high S indicates a high probability that two hashed codes are from the same subject and otherwise from different subjects.

Furthermore, the pair-wise (pairs of 1's) local distance representation implicates strong irreversibility. Let $N_1, \ldots, N_b$ be the number of bit 1's that can be found in the binary vectors $x_{bin(1)}, \ldots, x_{bin(b)}$. For any $k \in \{1, 2, \ldots, b\}$, there are at most $\binom{N_k}{2}$ possible combinations to describe the pair-wise relation for each binary vector, which contains local distances k. In view of this, recovering a single binary vector x_{bin} would require at least $\binom{\min_{N_1,\ldots,N_b}}{2}$ combinations representing collisions of 1's. However, the number of bit 1's present in the vectors $x_{bin(1)}, \ldots, x_{bin(b)}$ are subjected to uncertainty due to external environmental factors, i.e., noise, finger movements, etc. Thus, it is difficult to determine the value of $\min_{N_1,\ldots,N_b}$ precisely. Unfortunately, ARH does not offer revocability and unlinkability, which are crucial requirements for a template protection scheme. These requirements are not covered so far as no key is involved in the template generation process and to distinguish between different instances of generated protected templates. Hence, we adopted IoM hashing [19] to achieve a full set of BTP requirements as defined in the introduction. A detailed discussion regarding irreversibility is presented in Section V-D.

C. IoM Hashing Applied in ARH

IoM hashing, as introduced by Jin *et al.* [19], possesses the property that if two similar feature vectors X and X' are given, their hashed values will be the same with high probability. Opposed to this, if X and X' are distinct it can be expected that their IoM hashed output will be the same with low probability only.

Ideally, IoM operates on the ordered and fixed-length feature vector. If there is an alignment issue, IoM has to perform a left/right shift based alignment during the comparison which is done in the original paper [19]. Due to the structure of the generate vascular features IoM cannot be used directly on them as they are binary images. Thus, a feature comparison is not possible. Furthermore, a potentially necessary alignment compensation can also not be done. From this point of view, the benefit of using both ARH and IoM enables the compatibility of IoM and the used vascular features while standalone IoM can not processed on them. An additional alignment compensation can be performed as well (presented in the robustness section). Apart from the applicability of ARH there is another reason why a combination of ARH and IoM is beneficial. The combined usage of ARH and IoM is much faster as using ARH only (for details see Section V-C).

The IoM hashing uses a feature vector (the extracted ARH template) $x \in \mathbb{R}^n$ and an n-dimensional Gaussian vector, $r \in \mathbb{R}^n$ as input argument. The IoM hashing operates as follows:

TABLE I
BASELINE PERFORMANCE IN TERMS OF *EER*. THE BEST PERFORMING RESULTS ARE HIGHLIGHTED IN BOLD NUMBERS

	EER [%]					
dataset	GF	IUWT	MC	PC	RLT	WLD
UTFVP	0.64	0.36	**0.09**	0.14	0.60	0.46
PLUS LED	0.61	0.63	**0.28**	0.35	0.79	0.53
PLUS Laser	0.74	1.49	**0.33**	1.47	1.71	1.38

1) Randomly generate q n-dimensional Gaussian vectors $r_1, \ldots, r_q$.
2) Record the indices of the maximum value as $\psi = \arg\max_i \langle r_i, x \rangle$, where $\langle \cdot, \cdot \rangle$ is the inner product and $i \in \{0, 1, \ldots q\}$.
3) Repeat step 1-2 m number of times and yield the IoM output vector $(\psi_1, \ldots, \psi_m)$.

The similarity of two IoM hashed vectors $(\psi_1, \ldots, \psi_m)$ and $(\psi'_1, \ldots, \psi'_m)$ can be measured by counting the number of collisions, i.e., $\psi_i = \psi'_i$ among their size of m as discussed in [19].

As we want to introduce revocability and unlinkability by adding IoM to the ARH, it is necessary to define the key of the system, which is represented by the q n-dimensional Gaussian vectors $r_1, \ldots, r_q$. While q controls the number of generated Gaussian vectors (not their concrete specifications), m is responsible for the number of iterations conducted. According to [19], q has no significant influence on the recognition performance. Thus, we set $q = 2$ as suggested in [19].

V. EXPERIMENTAL SET-UP AND ANALYSIS

The experiments have been carried out using the PLUSVein-FV3 Dorsal-Palmar finger vein database (PLUSVein-FV3) [21] and the University of Twente Finger Vascular Pattern Database (UTFVP) [45]. As PLUSVein-FV3 contains 4 subsets, Laser/LED DORSAL and Laser/LED PALMAR, we selected the latter subsets to enable a direct comparison between the databases because the UTFVP database contains palmar images only. In the following we name the considered datasets UTFVP, PLUS LED and PLUS Laser.

In addition to the baseline and template protection experiments (presented in the following two subsections) we performed several other experiments which are dedicated to answer the additional questions introduced in Section I. These experiments will be discussed in detail in the subsequent subsections as well.

A. Baseline Performance Analysis

After pre-processing the resulting binary features are used to perform the baseline experiments without applying template protection schemes. We conducted these experiments with the help of the PLUS OpenVein Finger- and Hand-Vein Toolkit (http://www.wavelab.at/sources/OpenVein-Toolkit/).

Table I lists the performance results of the baseline experiments for the UTFVP and the PLUSVein-FV3 datasets. Overall, the performance on the UTFVP dataset is slightly superior compared to the PLUSVein-FV3 dataset for most of the evaluated recognition schemes.

TABLE II
RECOGNITION PERFORMANCE RESULTS (%). THE BEST RESULT FOR EACH FEATURE EXTRACTION METHOD IS HIGHLIGHTED IN BOLD NUMBERS

tempProt	EER											
	GF		IUWT		MC		PC		RLT		WLD	
	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ
	UTFVP											
remp_64	8.43	2.23	3.94	0.77	3.27	0.83	3.81	0.97	4.68	0.89	3.72	0.67
warp_16_6	**3.36**	0.74	**0.74**	0.18	**0.78**	0.23	**0.71**	0.21	**1.20**	0.24	**1.16**	0.25
ARH_180_20_60	10.98	0.04	4.43	0.06	4.77	0.03	7.18	0.16	3.89	0.11	3.90	0.12
	PLUSVein-FV3 Laser											
remp_48	11.55	3.47	6.86	1.71	10.45	2.03	14.10	3.42	12.51	3.41	5.52	2.04
warp_16_6	**6.33**	0.99	**2.21**	0.20	8.78	0.10	**3.30**	0.41	**4.27**	0.39	**2.02**	0.18
ARH_180_20_60	6.66	0.06	6.30	0.10	**3.79**	0.14	7.11	0.04	6.56	0.03	5.67	0.12
	PLUSVein-FV3 LED											
remp_48	10.32	3.08	6.68	1.57	7.71	2.47	13.43	4.00	12.21	2.92	4.42	1.27
warp_16_6	**5.27**	0.99	**1.33**	0.17	**2.01**	0.52	**2.30**	0.53	**3.88**	0.58	**1.00**	0.17
ARH_180_20_60	5.44	0.05	5.94	0.11	4.08	0.03	6.61	0.41	6.11	0.57	5.27	0.39

On the UTFVP, the best recognition performance result with an EER of 0.09% is achieved by MC, followed by PC with an EER of 0.14%, then IUWT, WLD and RLT follow while GF has the worst performance with an EER of 0.64%. On PLUS Laser and PLUS LED the best results are achieved by using MC as well, with an EER of 0.28% and 0.33% on the LED and laser subset, respectively. RLT performed worst compared to the other schemes on both subsets. Nevertheless, each of the evaluated recognition schemes achieves a competitive performance on all of the tested datasets.

B. Recognition Performance Applying Template Protection

After the baseline experiments, the extracted templates are protected by the use of the proposed ARH method, and by block re-mapping and warping as a comparison (http://wavelab.at/sources/Kirchgasser19d/). Note that the latter techniques are applied in the feature domain contrasting to [32]. Block re-mapping [36] divides an input template into non-overlapping blocks which are rearranged in a lossy manner (not all blocks of the input template are contained in the protected template) to achieve a certain level of irreversibility which would not be given by just permuting the blocks. Warping [47] is based on deforming the vein patterns' structures contained in non-overlapping blocks using piece-wise linear interpolation. Block sizes of 16, 32, 48 and 64 pixel have been chosen, while the offset parameter, controlling the warping based geometrical distortions is set to be maximal 6, 12, 18 or 24, respectively. These values have been used in [32] as well. Thus, we selected them for the sake of comparability.

For ARH different equidistant m values in the range of $[20, 200]$ have been selected as key parameters. Furthermore, for the non-overlapped blocks formulation (needed for Step 1 of the proposed algorithm), several block sizes are taken into account as well. We selected $b_n \in \{10, 20, 30\}$ and $b_m \in \{20, 30, 40, 50, 60\}$. The recognition accuracy on the selected datasets is again quantized in terms of the equal error rate (*EER*).

Table II presents the *EER* by using the mean ($\bar{x}$) and the standard deviation (σ) for each of the datasets and applied template protection schemes. For all following performance related experiments the results are presented by using $\bar{x}$ and σ as well. These results are calculated by randomly choosing 10 different keys (system-specific, i.e., identical keys for all users) as suggested by [10] to subsequently perform a suitable unlinkability analysis.

To keep the paper at a reasonable length, we will only present the best performing results and discuss the trend of the other experimentally considered cases without a detailed presentation of the EER values. These detailed results together with the reference implementation of the ARH scheme can be found on our aforementioned website (http://wavelab.at/sources/Kirchgasser19d/). Not surprisingly, the overall best recognition performance is observed for warping in almost all cases using a block size of 16 pixels and a maximal offset of 6 pixels. The remaining warping experiments based on other parameters resulted in a slightly worse EER, but still outperform the best EER values of the other schemes. The only exception to this trend is obtained by our proposed ARH-based scheme ($m = 180$, $b_n = 20$ and $b_m = 60$) on the PLUS Laser dataset applying MC for feature extraction ($EER = 3.79\%$). In all other cases using the PLUSVein-FV3 dataset the newly introduced technique achieved better results compared to block re-mapping but was outperformed by warping. In general the observed results are *a)* similar for all other parameter configurations of block re-mapping and ARH and *b)* are strongly depending on the particular feature extraction method and the dataset used. The ARH-based method did not work well using WLD on the PLUSVein-FV3 dataset. Furthermore, a poor EER must be reported for the UTFVP. In case WLD is considered the difference to the second best method (i.e., block re-mapping) is marginal. For the UTFVP a larger amount of displacement, e.g., longitudinal rotation is reported by [35]. This seems to be the reason for the performance issues concerning UTFVP as compared to the PLUSVein-FV3.

C. Runtime Analysis

Apart from recognition performance results the aspect of computational costs needs to be discussed. Considering the number of performed comparisons, which are conducted during the comparison of two templates, it is possible to state the following: regardless if baseline or template protected experiments applying block re-mapping/warping are performed, the number of template comparisons for each pair is always the

TABLE III
RUNTIMES FOR ALL PERFORMED PARTS OF THE EXPERIMENTS (AVERAGE VALUES OF 10 KEYS)

	Runtime (in sec)	
method	*UTFVP*	*PLUS_LED*
	baseline	
GF	7381	10957
MC	3024	2234
RLT	12738	17797
	remap_64	
GF	7562	11144
MC	3205	2421
RLT	12919	17984
	warp_16_6	
GF	7585	11169
MC	3228	2446
RLT	12942	18009
	ARH scheme	
ARH without IoM	4934	6194
ARH with IoM (m=20)	2584	3541
ARH with IoM (m=200)	2779	3748

same. As a maximum of vertically 30 pixel-wise shifts and horizontally 80 pixel-wise shifts are done for the probe finger vein template, a total of 2400 different shifted versions of two templates need to be compared to each other. Opposed to this computational costly process, two ARH-based protected templates have to be compared only once (by counting the number of collisions of 1's, which is quite fast).

For the concrete runtime analysis each process was run 10 times at a desktop computer equipped with an Intel Core i7-6700 CPU3.40 GHz and 32 GB RAM using Ubuntu 19.04 and MATLAB 2019a. Table III shows the mean values of all runs. As there is nearly no difference between PLUS_Laser and PLUS_LED, we only discuss results for PLUS_LED as they have been slightly better. The corresponding results presented in the first part of Table III are describing the baseline experiments for GF, MC and RLT. We have selected these three feature extraction methods as they include several different runtime representatives. It can be clearly seen that the differences between the single methods are varying. Not only the feature extraction was slowest for RLT, but also the feature comparison took longest, while MC performed best in both categories, which results in the lowest combined runtime. Furthermore, a difference between the used datasets must be reported as well. GF and RLT performed better on the UTFVP data, while for MC the opposite can be observed.

The reference template protection methods block re-mapping and warping showed only small differences between the datasets. The evaluated block re-mapping method using a block size of 64 pixel was slightly faster than the warping scheme exhibiting a block size of 16 pixel and an offset of 6 pixel. We have selected these two parameter settings as they resulted in the best recognition performance results (see Table II). Subsequently, we selected the best performing settings for ARH as well ($b_n = 20$ and $b_m = 60$, while for $m = [20, 200]$ the minimal and maximal key parameters were chosen).

For the proposed ARH method we present the results of two different runtime experiments. The first experiments focus on the application of ARH only, while the second ones include IoM hashing as well. The higher computational costs are obtained if ARH only is considered. Thus, the usage of IoM is beneficial for the runtime. This can be explained by the feature comparison step, which is much faster if IoM hashes are used as their comparison is based on the Jaccard distance. All experiments conducted on the PLUS_LED or PLUS_Laser dataset achieved worse results compared to the corresponding UTFVP dataset's experiments. This difference can possibly be explained by the different sizes of the images contained in the datasets. Interestingly the selection of m does not seem to have a high impact on the computational costs. Depending to which baseline feature extraction method combined with block re-mapping or warping the ARH scheme including IoM hashing is compared to, our scheme is outperforming the reference template protection experiments. Opposed to the basic procedure of ARH excluding IoM, the experiments described in Section V-G are very costly and much slower than all other experiments involving template protection.

D. Non-Invertibility Analysis

First of all, the pair-wise local distance representation of ARH (considering the pairs of 1's) implicitly introduces non-invertibility. In detail, let $N_1, N_2, \ldots, N_b$ be the number of 1's that can be found in the binary vectors $x_{bin(1)}, x_{bin(2)}, \ldots x_{bin(b)}$, respectively. For any $k \in 1, 2, \ldots, b$ there are at most $\binom{N_k}{2}$ possible combinations to describe the pair-wise relation for each binary vector, which contains a certain distance k. Further, the minimal number of combinations representing collisions of 1's between different finger vein binary feature vectors $x_{bin(1)}, x_{bin(2)}, \ldots x_{bin(b)}$ can be described formally as

$$\binom{\min N_1, N_2, \ldots, N_b}{2} \times \left(1 - (P_d)^b\right) \tag{5}$$

where P_d refers to the minimum dissimilarity between two different binary vectors. The maximum number of combinations representing collisions of 1's can therefore be described as

$$\binom{\max N_1, N_2, \ldots, N_b}{2} \times \left(1 - (P_d)^b\right) \tag{6}$$

However, it is difficult to determine the value of $\min N_1, N_2, \ldots, N_b$ and $\max N_1, N_2, \ldots, N_b$ precisely. The reason is based on the fact that the number of 1's detected in the vectors $x_{bin(1)}, x_{bin(2)}, \ldots x_{bin(b)}$ is subject to uncertainty due to external environmental factors, i.e., noise, finger misplacement like longitudinal rotation and several others. Nonetheless, the expected number of $\min N_1, N_2, \ldots, N_b$ and $\max N_1, N_2, \ldots, N_b$ can be estimated numerically for all given finger vein templates. This yields $E(\min N_1, N_2, \ldots, N_b) = 29$ and $E(\max N_1, N_2, \ldots, N_b) = 234$, while $P_d = 0.0557$ is calculated by taking the normalized minimum non-zero Hamming distance between different binary vectors of the same template across the whole dataset (the estimated results are presented only for PLUS Laser). According to the low value of P_d it is implied that the correlation between two binary finger vein feature vectors is high enough to maximize the number of combinations representing collisions

of 1's, reported by Equations (5) and (6), by approaching $\binom{\min N_1, N_2, \ldots, N_b}{2}$ and $\binom{\max N_1, N_2, \ldots, N_b}{2}$ for the minimum and maximum number of combinations representing collisions of 1's, respectively. Subsequently, the expected number of combinations representing collisions of 1's can be estimated by using the following inequality:

$$\begin{aligned} & E\left(\binom{\min N_1, N_2, \ldots, N_b}{2} \times \left(1-(P_d)^b\right)\right) \\ & \leq E(combinations) \\ & \leq E\left(\binom{\max N_1, N_2, \ldots, N_b}{2} \times \left(1-(P_d)^b\right)\right). \end{aligned} \tag{7}$$

After selecting the best performing parameters $b_n = 20$ and $b_m = 60$ we have $b = 29$ and calculated $2^9 \leq E(combinations) \leq 2^{15}$ as bounds for the expected number of combinations representing collisions of 1's.

The ARH-based transformation implicitly provides irreversibility by the argument of an expected guess complexity from 2^9 to 2^{15}, but the CB scheme provides further requirements like revocability and unlinkability only after the application of IoM hashing. The latter requirement is discussed in the following Section V-E, while the property of revocability is fulfilled by the design of IoM hashing. As described in Section IV-C, randomly constructed Gaussian vectors are used to generate the IoM hash codes. Thus, a new template can be generated to replace a compromised one by re-generating an IoM hash code using a different random Gaussian vector (revocability is assured).

Additionally, the application of IoM provides some separate level of non-invertibility itself. IoM protected templates are generated to solve the problem that real-value features can be guessed from their discrete indices form. Let's assume the adversary gained a protected template (discrete indices), the auxiliary data (i.e., permutation seeds or random matrices) as well as the hashing algorithm and the corresponding parameters (e.g., m, k, p, q [19]). There is no direct clue that an adversary can recover the biometric vector x information (real-value features) from the compromised protected template (discrete indices form) alone. Furthermore, the auxiliary data is completely independent from the biometric vector. Therefore, knowing the auxiliary data does not provide enough information to recover the real-value features as well. Thus, the only way for the adversary to extract a recovered template is to guess the real-value directly. Further details on this specific aspect including a more thorough analysis of IoM's non-invertibility is given in [19].

E. Unlinkability Analysis

ISO/IEC Standard 24745/30136 defines various criteria to ensure a proper protection of templates, one of those criteria is the unlinkability. Unlinkability guarantees that stored and protected biometric information can not be linked across various different applications or databases.

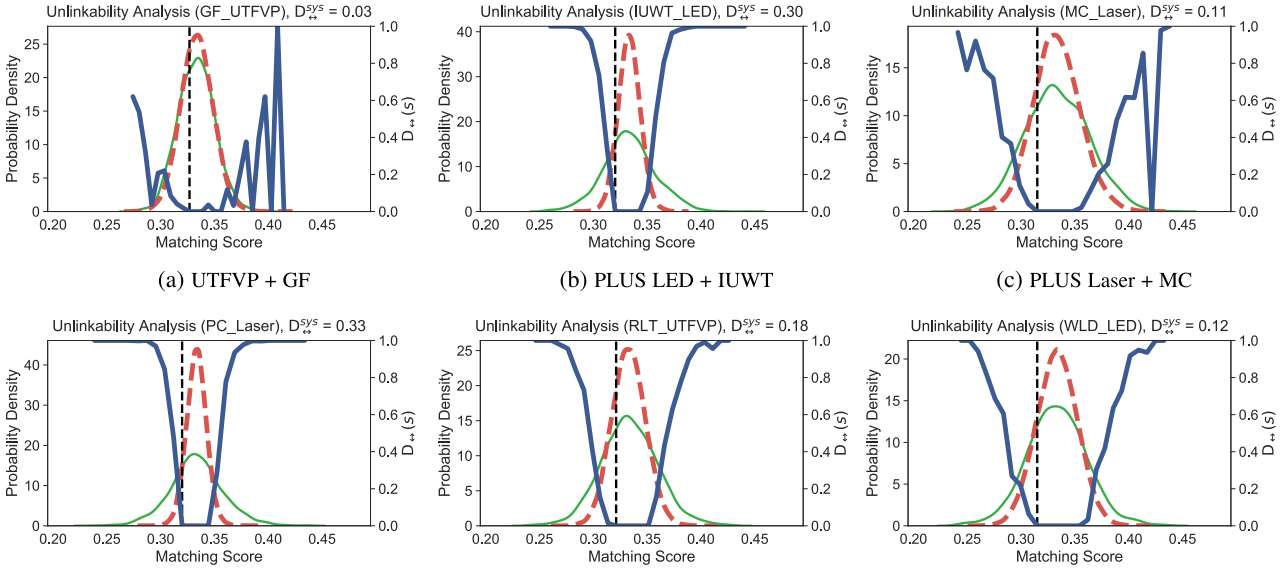
However, the standard only defines what unlinkability means but gives no generic way of quantifying it. Gomez-Barrero *et al.* [10] present a universal framework to evaluate the unlinkability of a biometric template protection system based on the comparison scores. They proposed the so called D_{sys} 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. A value of 0.5 refers to the mated and unmated scores being separated in a way that 50% of the comparisons can be clearly linked to each other despite different keys were used to protect the templates. This does not relate to 50% of the templates being linkable as it depends on the number and distribution of comparisons used to calculate the unlinkability. Only if each template is involved in the same number of comparisons, a D_{sys} value of 0.5 refers to 50% of the templates being linkable. To provide a reasonable level of unlinkability, the D_{sys} values should be as low as possible (for practical reasons at least below 0.15). According to Figure 1 of [11] good D_{sys} values around 0.14 are called semi-unlinkable, while D_{sys} results around 0.32 are named semi-linkable which is not preferable.

TABLE IV
D_{sys} UNLINKABILITY SCORES FOR BLOCK RE-MAPPING, WARPING AND THE PROPOSED ARH SCHEME. A VALUE OF 100 INDICATES FULL LINKABILITY, HENCE THE WORST UNLINKABILITY VALUE THAT CAN BE ACHIEVED WHILE A D_{sys} VALUE OF 0 INDICATES NO LINKABILITY, THUS THE BEST POSSIBLE UNLINKABILITY. THE BEST RESULTS FOR EACH TEMPLATE PROTECTION METHOD ARE HIGHLIGHTED IN BOLD NUMBERS

tempProt	D_{sys}					
	GF	**IUWT**	**MC**	**PC**	**RLT**	**WLD**
	UTFVP					
remp_16	3.4	3.0	3.1	**2.9**	3.1	4.4
remp_64	25.7	20.0	29.7	20.8	16.3	27.2
warp_16_6	56.4	85.0	82.6	79.6	81.7	74.9
warp_64_24	42.4	**41.2**	53.1	48.8	44.7	43.4
ARH_180_20_60	5.4	7.2	6.3	**5.2**	7.2	6.6
	PLUSVein-FV3 Laser					
remp_16	4.1	2.7	3.4	2.8	**2.6**	4.3
remp_64	19.6	14.4	24.5	10.1	7.4	17.8
warp_16_6	63.4	81.3	86.4	84.0	68.2	82.1
warp_64_24	33.3	35.3	44.0	34.3	**28.8**	47.2
ARH_180_20_60	**6.1**	7.4	7.1	7.2	6.3	6.6
	PLUSVein-FV3 LED					
remp_16	3.8	2.9	3.3	2.6	**2.3**	4.0
remp_64	19.4	13.6	23.5	10.1	7.7	16.9
warp_16_6	67.0	82.0	86.7	84.4	67.5	82.6
warp_64_24	32.8	33.0	45.1	33.9	**27.7**	48.5
ARH_180_20_60	**5.2**	7.4	7.1	7.2	6.3	6.6

We shifted the range from $[0, 1]$ to values in $[0, 100]$ to improve the readability of the results presented in Table IV. Furthermore, the authors of [10] stipulated that 10 different keys should be considered during the unlinkability analysis as this simulates a real world case where the same subjects are enrolled in ten different applications and an attacker aims at linking the templates of the corresponding datasets to each other. Thus, we also selected 10 different keys for our performance and unlinkability analysis.

The D_{sys} values are shown for all three template protection schemes in Table IV. For block re-mapping almost full unlinkability is achieved in the most cases (especially for *remp_16*), while for the warping scheme almost full linkability can be reported. The worst result regarding the ISO/IEC Standard 24745/30136 property of unlinkability is exhibited by *warp_16_6*. From a security point of view, warping is not a proper template protection scheme based on the evaluated parameters.



(a) UTFVP + GF (b) PLUS LED + IUWT (c) PLUS Laser + MC

(d) PLUS Laser + PC (e) UTFVP + RLT (f) PLUS LED + WLD

Fig. 4. Example images which display unlinkability trend using ARH-based scheme.

The unlinkability of our proposed ARH-based template protection technique (see Table II), independently of the parameter selection, outperformed warping and is similar to the results obtained for block re-mapping, especially if compared to *remp_16*. Corresponding distribution plots are presented in Figure 4. The blue line represents the D_{sys} values for all threshold selections done during the computation (see [10]). The green distribution describes the so called *mated* samples scores. These comparison scores are computed from templates extracted from samples of a single instance of the same subject using different keys [10]. The red colored distribution corresponds to the *non-mated* samples scores, which is yielded by templates generated from samples of different instances using different keys. According to [10] a *fully unlinkable* scenario can be observed if both colored distributions are identical, while *full linkability* is given if mated and non-mated distributions can be fully separated from each other. The presented distribution plots of Figure 4 show nearly full unlinkability in all cases as the distributions of mated and non-mated samples scores are highly overlapping. As a consequence, the D_{sys} values are close to 0.

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 and the severe recognition performance drop restricts the use of block re-mapping schemes in most cases as well. Thus, the proposed ARH method offers a promising trade-off between recognition performance loss and unlinkability in most cases, while the other two investigated template protection schemes either have a low recognition performance loss but bad unlinkability (warping), or have a relatively high performance loss but good unlinkability (block re-mapping).

F. Robustness of the Proposed Feature Descriptor

The first type of additional experiments is focusing on the *robustness* characteristic of the proposed scheme. As mentioned in Section II, in most cases finger vein images presented to dedicated recognition systems are not registered and only coarsely aligned to each other. Thus, the used comparison methods are usually based on the calculation of the correlation between the input image and x- and y-direction shifted versions of the reference image. The proposed template protection scheme relies on the usage of a new finger vein feature descriptor which was designed to be less sensitive to the non-aligned character of the presented input images. The feature descriptor uses local block based information as described in Section IV-B. A visualization of the block based principle is presented in the first two images located in the upper left corner of Figure 3. The local block based information is used to form a distance based representation of each image. Due to alignment differences between images of the same subject it is possible that certain vascular structures which are identical do not appear in the corresponding blocks of the same subject's images as they are misplaced to each other. An example for this misplacement is presented in the first row of Figure 5. The reader should focus on the triangle shape structure in the left upper corner. This structure highly varies among the given examples. Not only the shape changes but also the position of important characteristics like the vein crossing indicated by the right vertex is altered. We corrected these misalignments to examine the influence of the detectable misplacements on the proposed feature descriptor.

For pre-aligning the extracted templates a modified version of the Miura matcher [31] is used. This modified version of the discussed method (see Section II) returns the determined shifts in x- and y-direction as well as the rotational shift in steps of 0.5° for the optimal found alignment together with the comparison score. The comparison score is compared against a pre-defined threshold and an alignment is only performed if it is above this threshold. Hence, for a set of genuine templates from the same subject and finger, the shifts between all pairs of templates are determined which results in a set of relative

TABLE V
RECOGNITION PERFORMANCE (%) RESULTS OF THE ROBUSTNESS EXPERIMENTS USING PROPOSED TEMPLATE PROTECTION SCHEME. THE BEST RESULT FOR EACH DATASET IS HIGHLIGHTED IN BOLD NUMBERS

dataset	EER											
	GF		**IUWT**		**MC**		**PC**		**RLT**		**WLD**	
	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ
UTFVP	9.32	0.75	**1.36**	**0.22**	1.84	0.29	2.27	0.40	3.40	0.53	1.64	0.32
PLUS_Laser	4.75	0.43	3.72	0.38	**1.58**	**0.18**	3.64	0.31	5.32	0.64	2.80	0.27
PLUS_LED	3.93	0.49	2.71	0.32	**1.31**	**0.25**	2.20	0.28	4.72	0.65	2.10	0.27

shifts. Based on those shifts, a reference template is selected in a way that all the remaining shifts are minimized in order to avoid large black areas at the template boundaries which are introduced by shifting the templates. Afterwards, the proposed ARH scheme was applied in the same manner like introduced in Section V-B. An example of the misplacement correction is presented in the second row of Figure 5. The most prominent correction can be seen in example image (e), while the others (d) and (f) remained almost stable.

The results presented in Table V summaries the performance evaluation after the application of the proposed template protection scheme on alignment corrected input templates. Once more 10 different system-based keys have been used to secure the biometric information contained in the extracted feature templates. Thus, for each EER value the mean ($\bar{x}$) and the standard deviation (σ) for all datasets and feature extraction methods were obtained.

In most cases these results have been observed for $b_n = 20$, $b_m = 60$ and $m = 60$. In the other cases m was different; $m = 180$ for UTFVP: MC and PC or $m = 200$ for PLUS_LED: MC and PC. Except for the use of GF as feature extraction method, the recognition performance is significantly better than the performance described in Table II for the same method applied to non-aligned data resulting in an approximate EER reduction by half. In case of GF the EER is lower as well, but the reduction is not that pronounced. Nevertheless, even in the worst performing experimental setting the prior alignment correction is highly beneficial. The difference between the baseline experiments without template protection and the recognition performance after applying template protection is much less than expected. This observation proves that pre-alignment enhances the recognition performance of the ARH template protection scheme. Important vascular structures can be located in the same block-areas which is mandatory for a good quality of the extracted features.

Additionally to the recognition performance experiments we also conducted an unlinkability analysis once more. Interestingly, the obtained *Dsys* values resulted in full unlinkability (*Dsys* $= 0$). This indicates that no subject's image, protected by a certain key, can successfully be compared to the same subject's image protected by a different key.

Summarising it can be stated that our proposed template protection method is not that insensitive to displacements as expected. The detectable misplacement between images of the same capture subject affects the proposed scheme. The same observation can be made for basically all template protection methods applied to finger vein data.

G. Combination of Either Block Re-Mapping or Warping With the Proposed Feature Descriptor

The goal of these experiments was to successfully combine either block re-mapping or warping with the ARH feature descriptor introduced in Section IV-A. In [22] it was assumed that especially the combination of warping and the proposed feature descriptor could maintain the recognition performance obtained by warping, while improving the unlinkability at the same time. The unlinkability enhancement would especially be beneficial for warping while the recognition performance of this scheme was promising on the used finger vein data. Thus, we want to prove or disprove this assumption and investigate the combination of either block re-mapping or block warping and the alignment-robust descriptor as well.

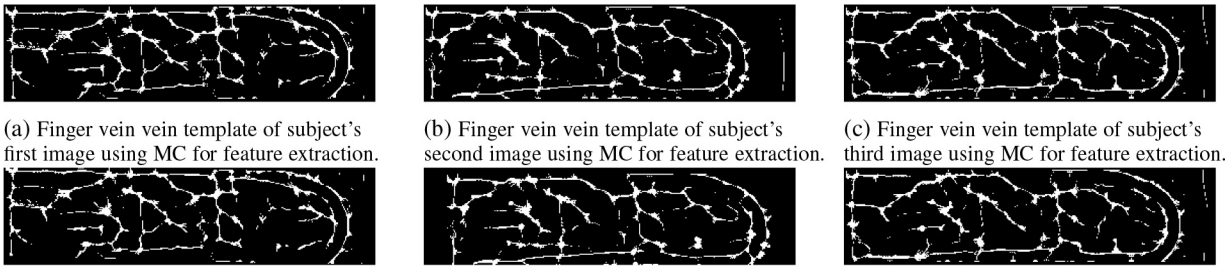
The application of IoM hashing to achieve revocability and unlinkability is not necessary any longer as it is possible to use the proposed ARH feature descriptor to extract features from the protected templates (generated by block re-mapping or warping). Block re-mapping and warping are ensuring both important properties by design. Furthermore, the ARH extracted features are represented as feature vectors and thus, it might be able to compare them much faster than if the protected templates are compared by using the Miura approach.

We did not only conduct performance related experiments for this methodology but did an analysis regarding unlinkability as well. The corresponding experimental results are described and discussed in the following. For the experiments we selected the best performing block re-mapping and warping parameters out of the template protection experiments (see Section V-B) as described in Table II. For the sake of simplicity, we selected remap_64 for all three datasets as there was almost no difference between remap_64 and remap_48 in datasets PLUS_Laser and PLUS_LED. In case of warping a block size of 16 and offset of 6 was selected once again.

Unfortunately, the experimental results presented in Table VI do not follow the assumption as expected. Compared to the results obtained for the original template protection experiments (see Tables II and IV) the recognition performance was reduced drastically. The reported EER values for warping highly increased for all datasets and feature extraction methods while for block re-mapping especially the results using GF got worse. Thus, the expectation to maintain the recognition performance was clearly not met. Neither the combination of block re-mapping and the ARH feature descriptor nor the combination using warping and ARH resulted in similar EER values as obtained by the template protection experiments using block re-mapping or warping only.

TABLE VI
RECOGNITION PERFORMANCE (%) AND UNLINKABILITY (%) RESULTS OF THE EXPERIMENTS USING A COMBINATION OF BLOCK RE-MAPPING/WARPING AND THE PROPOSED ARH FEATURE DESCRIPTOR. THE BEST RESULT FOR EACH DATASET IS HIGHLIGHTED IN BOLD NUMBERS

dataset	EER											
	GF		**IUWT**		**MC**		**PC**		**RLT**		**WLD**	
	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ
	remap_64 combined with the ARH feature descriptor											
UTFVP	18.74	2.04	8.39	1.17	9.64	1.95	12.36	1.76	9.41	1.82	**7.65**	**1.24**
PLUS Laser	10.17	0.92	10.56	0.60	**8.29**	**1.34**	12.31	0.73	12.62	1.01	10.96	0.92
PLUS LED	9.19	1.05	11.61	1.25	**8.65**	**1.40**	12.89	0.61	13.15	1.31	11.86	0.75
	warp_16_6 combined with the ARH feature descriptor											
UTFVP	20.40	0.71	9.52	0.64	10.26	0.62	11.41	0.46	**6.37**	**0.32**	10.06	0.53
PLUS Laser	10.07	0.30	9.14	0.43	**5.89**	**0.20**	9.53	0.31	8.19	0.22	8.39	0.48
PLUS LED	9.92	0.46	10.13	0.48	**6.47**	**0.25**	9.94	0.38	8.35	0.26	9.15	0.41
	$Dsys$											
	remap_64 combined with the ARH feature descriptor											
UTFVP	10.7	3.4	11.1	4.7	11.7	5.1	10.4	3.4	**8.9**	**1.2**	10.4	3.7
PLUS Laser	13.7	6.7	11.8	5.2	14.5	8.1	11.8	5.2	**9.3**	**2.3**	12.7	6.4
PLUS LED	15.2	7.8	10.7	4.1	13.7	6.7	11.9	5.2	**9.8**	**2.5**	12.6	6.3
	warp_16_6 combined with the ARH feature descriptor											
UTFVP	**34.4**	**2.0**	63.6	2.0	67.7	2.4	66.5	1.2	67.3	2.5	67.9	1.8
PLUS Laser	**68.3**	**1.5**	72.6	2.2	82.8	7.9	76.5	7.5	71.1	2.2	76.1	1.5
PLUS LED	**67.4**	**1.7**	70.6	2.1	82.4	1.02	75.6	1.0	71.3	2.3	75.0	1.6



(a) Finger vein vein template of subject's first image using MC for feature extraction.

(b) Finger vein vein template of subject's second image using MC for feature extraction.

(c) Finger vein vein template of subject's third image using MC for feature extraction.

(d) Alignment corrected finger vein vein template of subject's first image (a) using MC for feature extraction.

(e) Alignment corrected finger vein vein template of subject's second image (b) using MC for feature extraction.

(f) Alignment corrected finger vein vein template of subject's third image (c) using MC for feature extraction.

Fig. 5. Example images which display alignment variances within the same subject. The first row presents 3 original templates of one subject. The second row visualises the alignment corrected templates.

However, the other goal of enhancing the unlinkability capability was partly achieved for warping. The linkability was reduced for IUWT, MC, PC and WLD by nearly 20%, while for GF a reduction of approximately 30% could be achieved. Nevertheless, this enhancement is not enough to compensate the recognition performance degradation which is introduced by the application of the ARH feature descriptor.

Summarising it can be stated that the combination of block re-mapping/warping and the proposed feature descriptor is not promising. It seems that the distortions introduced by the applied template protection schemes block re-mapping and warping do not allow to extract robust features which can compensate these distortions and allow to maintain the recognition performance and enhance the unlinkability at the same time. Nonetheless, this experiment can be interpreted as an extension of the previous one, which investigated the aspect of robustness.

VI. CONCLUSION

The proposed ARH-based template protection scheme shows a slightly lower recognition performance compared to warping, but exhibits a much higher unlinkability. Bock re-mapping was outperformed in most cases regarding recognition performance and unlinkability as well. Another advantage of the proposed method are the much lower computation costs due to a highly reduced number of template comparisons which are conducted for two templates. Furthermore, security based aspects like irreversibility and revocability were discussed. The ARH feature descriptor design implicitly ensures non-invertibility of the entire template protection system. The revocability requirement is fulfilled as well as a new template can be re-generated by using a different random Gaussian vector during the IoM hash code computation. Thus, the main requirements of a template protection scheme are met.

The proposed scheme offers a promising trade-off between recognition performance loss and unlinkability, while especially block re-mapping is not able to perform well in terms of recognition performance and unlinkability at the same time. Similar to other template protection schemes the proposed method suffers from displacements detectable between different images of the same biometric subject, but to a much lower extent than others.

Experiments regrading the combination of block re-mapping and warping resulted in an unlinkability enhancement for

warping, but a recognition performance degradation for all investigated cases. The positive aspect of the combination experiments is the confirmation that the reduction of distortions or misplacements of the data is beneficial for the application of the proposed scheme. Otherwise, the additional distortion introduced by block re-mapping or warping would have been compensated to a certain degree at least.

One possibility for future work includes the usage of user-specific keys instead of system-based ones like done in the present study. Different distance measures for the ARH feature vector could be investigated as well as the applied cosine measure might not be the best performing choice. Furthermore, it would also be interesting to evaluate the obtained performance reduction regarding recognition performance and unlinkability with respect to the application of those template protection schemes in real-world deployments of finger vein recognition systems, i.e., is the performance still suitable for daily use.

REFERENCES

[1] *Information Technology Security Techniques Biometric Information Protection, 2011*, Standard ISO/IEC 24745:2011, 2011.

[2] *Information Technology Performance Testing of Biometric Template Protection Schemes, 2018*, Standard ISO/IEC 30136:2018, 2018.

[3] T. E. Boult, W. J. Scheirer, and R. Woodworth, "Revocable fingerprint biotokens: Accuracy and security analysis," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Minneapolis, MN, USA, Jun. 2007, pp. 1–8.

[4] J. Chavez-Galaviz, J. Ruiz-Rojas, A. Garcia-Gonzalez, and R. Fuentes-Aguilar, "Embedded biometric cryptosystem based on finger vein patterns," in *Proc. 12th Int. Conf. Elect. Eng. Comput. Sci. Autom. Control (CCE)*, Mexico, MO, USA Oct. 2015, pp. 1–6.

[5] J. H. Choi, W. Song, T. Kim, S.-R. Lee, and H. C. Kim, "Finger vein extraction using gradient normalization and principal curvature," in *Proc. SPIE*, 2009, pp. 7251–7259.

[6] S.-J. Chuang, "Vein recognition based on minutiae features in the dorsal venous network of the hand," *Signal Image Video Process.*, vol. 12, no. 3, pp. 573–581, 2018.

[7] T. Connie, A. Teoh, M. Goh, and D. Ngo, "PalmHashing: A novel approach for cancelable biometrics," *Inf. Process. Lett.*, vol. 93, no. 1, pp. 1–5, 2005.

[8] P. Das, K. Karthik, and B. C. Garai, "A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs," *Pattern Recognit.*, vol. 45, no. 9, pp. 3373–3388, 2012.

[9] M. Favre, S. Picard, J. Bringer, and H. Chabanne, "Balancing is the key: Performing finger vein template protection using fuzzy commitment," in *Proc. Int. Conf. Inf. Syst. Security Privacy (ICISSP)*, Angers, France, Feb. 2015, pp. 304–311.

[10] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General framework to evaluate unlinkability in biometric template protection systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 6, pp. 1406–1420, Jun. 2018.

[11] M. Gomez-Barrero, C. Rathgeb, J. Galbally, C. Busch, and J. Fierrez, "Unlinkable and irreversible biometric template protection based on bloom filters," *Inf. Sci.*, vols. 370–371, pp. 18–32, Nov. 2016.

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

[13] J. Hämmerle-Uhl, E. Pschernig, and A. Uhl, "Cancelable iris biometrics using block re-mapping and image warping," in *Information Security*, Heidelberg, Germany: Springer, 2009, pp. 135–142.

[14] D. Hartung and C. Busch, "Why vein recognition needs privacy protection," in *Proc. 5th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP'09)*, Kyoto, Japan, 2009, pp. 1090–1095.

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

[16] D. Hartung, M. Tistarelli, and C. Busch, "Vein minutia cylinder-codes (V-MCC)," in *Proc. Int. Conf. Biometr. (ICB)*, Madrid, Spain, Jun. 2013, pp. 1–7.

[17] B. Huang, Y. Dai, R. Li, D. Tang, and W. Li, "Finger-vein authentication based on wide line detector and pattern normalization," in *Proc. 20th Int. Conf. Pattern Recognit. (ICPR)*, Istanbul, Turkey, 2010, pp. 1269–1272.

[18] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, 2008, Art. no. 113

[19] Z. Jin, J. Y. Hwang, Y.-L. Lai, S. Kim, and A. B. J. Teoh, "Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 393–407, Feb. 2018.

[20] C. Kauba, E. Piciucco, E. Maiorana, P. Campisi, and A. Uhl, "Advanced variants of feature level fusion for finger vein recognition," in *Proc. Int. Conf. Biometr. Special Interest Group (BIOSIG'16)*, Darmstadt, Germany, 2016, pp. 1–12.

[21] C. Kauba, B. Prommegger, and A. Uhl, "The two sides of the finger—An evaluation on the recognition performance of dorsal vs. palmar finger-veins," in *Proc. Int. Conf. Biometr. Special Interest Group (BIOSIG'18)*, Darmstadt, Germany, 2018, pp. 1–8.

[22] S. Kirchgasser, Y.-L. Lai, J. Zhe, and A. Uhl, "Finger-vein template protection based on alignment-free hashing," in *Proc. IEEE 10th Int. Conf. Biometr. Theory Appl. Syst. (BTAS2019)*, Tampa, Florida, USA, 2019, pp. 1–9.

[23] A. Kumar and Y. Zhou, "Human identification using finger images," *IEEE Trans. Image Process.*, vol. 21, no. 4, pp. 2228–2244, Apr. 2012.

[24] Y.-L. Lai*et al.*, "Cancellable iris template generation based on indexing-first-one hashing," *Pattern Recognit.*, vol. 64, pp. 105–117, Apr. 2017.

[25] L. Leng and J. Zhang, "PalmHash code vs. PalmPhasor code," *Neurocomputing*, vol. 108, pp. 1–12, May 2013.

[26] 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.

[27] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri, "Cancelable templates for sequence-based biometrics with application to on-line signature recognition," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 40, no. 3, pp. 525–538, May 2010.

[28] E. Maiorana, P. Campisi, J. Ortega-Garcia, and A. Neri, "Cancelable biometrics for HMM-based signature recognition," in *Proc. 2nd IEEE Int. Conf. Biometr. Theory Appl. Syst. (BTAS)*, Arlington, VA, USA, 2008, pp. 1–6.

[29] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, and A. Neri, "Template protection for HMM-based on-line signature authentication," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW'08)*, Anchorage, AK, USA, 2008, pp. 1–6.

[30] N. Miura, A. Nagasaka, and T. Miyatake, "Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification," *Mach. Vis. Appl.*, vol. 15, no. 4, pp. 194–203, 2004.

[31] N. Miura, A. Nagasaka, and T. Miyatake, "Extraction of finger-vein patterns using maximum curvature points in image profiles," *IEICE Trans. Inf. Syst.*, vol. E90-D, no. 8, pp. 1185–1194, 2007.

[32] E. Piciucco, E. Maiorana, C. Kauba, A. Uhl, and P. Campisi, "Cancelable biometrics for finger vein recognition," in *Proc. 1st Int. Workshop Sens. Process. Learn. Intell. Mach. (SPLINE)*, Aalborg, Denmark, 2016, pp. 1–5.

[33] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Sectored random projections for cancelable iris biometrics," in *Proc. Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Dallas, TX, USA, 2010. pp. 1838–1841.

[34] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Secure and robust iris recognition using random projections and sparse representations," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 9, pp. 1877–1893, Sep. 2011.

[35] B. Prommegger, C. Kauba, M. Linortner, and A. Uhl, "Longitudinal finger rotation—Deformation detection and correction," *IEEE Trans. Biometr. Behav. Identity Sci.*, vol. 1, no. 2, pp. 1–17, Apr. 2019.

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

[37] N. Ratha, J. Connell, R. M. Bolle, and S. Chikkerur, "Cancelable biometrics: A case study in fingerprints," in *Proc. 18th Int. Conf. Pattern Recognit. (ICPR)*, vol. 4. Hong Kong, China, 2006. pp. 370–373.

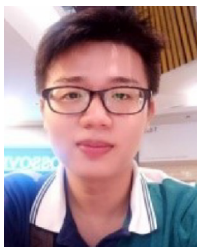
[38] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[39] C. Rathgeb, F. Breitinger, and C. Busch, "Alignment-free cancelable iris biometric templates based on adaptive bloom filters," in *Proc. IEEE Int. Conf. Biometr. (ICB)*, Madrid, Spain, 2013, pp. 1–8.

[40] C. Rathgeb and A. Uhl, "Secure iris recognition based on local intensity variations," in *Image Analysis and Recognition*. Heidelberg, Germany: Springer, 2010, pp. 266–275.
[41] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. Inf. Security*, vol. 2011, Sep. 2011, Art. no. 3.
[42] M. Savvides, B. V. K. V. Kumar, and P. K. Khosla, "Cancelable biometric filters for face recognition," in *Proc. 17th Int. Conf. Pattern Recognit. (ICPR)*, vol. 3. Cambridge, U.K., Aug. 2004, pp. 922–925.
[43] J.-L. Starck, J. Fadili, and F. Murtagh, "The undecimated wavelet decomposition and its reconstruction," *IEEE Trans. Image Process.*, vol. 16, no. 2, pp. 297–309, Feb. 2007.
[44] 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 Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 12, pp. 1892–1901, Dec. 2006.
[45] B. T. Ton and R. N. Veldhuis, "A high quality finger vascular pattern dataset collected using a custom designed capturing device," in *Proc. IEEE Int. Conf. Biometr. (ICB)*, Madrid, Spain, 2013, pp. 1–5.
[46] S. Wang and J. Hu, "Design of alignment-free cancelable fingerprint templates via curtailed circular convolution," *Pattern Recognit.*, vol. 47, no. 3, pp. 1321–1329, 2014.
[47] G. Wolberg, "Image morphing: A survey," *Vis. Comput.*, vol. 14, no. 8, pp. 360–372, 1998.
[48] 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," *Inf. Sci.*, vols. 433–434, pp. 431–447, Apr. 2018.
[49] B. Yang, D. Hartung, K. Simoens, and C. Busch, "Dynamic random projection for biometric template protection," in *Proc. 4th IEEE Int. Conf. Biometr. Theory Appl. Syst. (BTAS)*, Washington, DC, USA, Sep. 2010, pp. 1–7.
[50] L. Yang, G. Yang, Y. Yin, and L. Zhou, "A survey of finger vein recognition," in *Chinese Conference on Biometric Recognition*. Cham, Switzerland: Springer, 2014, pp. 234–243.
[51] W. Yang, J. Hu, and S. Wang, "A finger-vein based cancellable bio-cryptosystem," in *Proc. 7th Int. Conf. Netw. Syst. Security (NSS)*, Madrid, Spain, Jun. 2013, pp. 784–790.
[52] W. Yang *et al.*, "Securing mobile healthcare data: A smart card based cancelable finger-vein bio-cryptosystem," *IEEE Access*, vol. 6, pp. 36939–36947, 2018.
[53] S. Ye, Y. Luo, J. Zhao, and S.-C. S. Cheung, "Anonymous biometric access control," *EURASIP J. Inf. Security*, vol. 2, Nov. 2009, Art. no. 865259.
[54] J. Zhang and J. Yang, "Finger-vein image enhancement based on combination of gray-level grouping and circular gabor filter," in *Proc. IEEE Int. Conf. Inf. Eng. Comput. Sci. (ICIECS)*, Wuhan, China, 2009, pp. 1–4.
[55] J. Zhao, H. Tian, W. Xu, and X. Li, "A new approach to hand vein image enhancement," in *Proc. 2nd Int. Conf. Intell. Comput. Technol. Autom. (ICICTA'09)*, Changsha, China, vol. 1, 2009, pp. 499–501.
[56] J. Zuo, N. K. Ratha, and J. H. Connell, "Cancelable iris biometric," in *Proc. 19th Int. Conf. Pattern Recognit. (ICPR)*, Tampa, FL, USA, Dec. 2008, pp. 1–4.

Simon Kirchgasser (Student Member, IEEE) received the M.Sc. degree in applied image and signal processing from the University of Salzburg and University of Applied Sciences, Salzburg, in 2016. He is currently pursuing the Ph.D. degree with the Department of Computer Sciences, University of Salzburg, where he is working as a Research Assistant. His main research interest is in fingerprint and vascular biometrics, especially focusing on ageing related aspects in fingerprint biometrics, and template protection in vascular biometrics.

Christof Kauba (Student Member, IEEE) received the B.Eng. and M.Sc. degrees and the Ph.D. degree in applied information technology from the University of Salzburg, Austria, in 2013, 2015, and 2018, respectively, where he is a Postdoctoral Researcher with the Department of Computer Sciences. His research interests include image and video processing, image forensics and biometrics, especially biometric sensor design as well as finger and hand vein biometrics.



Yen-Lung Lai received the B.Sc. degree in physics from University Tunku Abdul Rahman, Malaysia, in 2015. He is currently pursuing the Ph.D. degree with Monash University, Malaysia. His research interests include biometrics and information security.

Jin Zhe (Member, IEEE) received the BIT degree (Hons.) in software engineering, the M.Sc. (I.T.) degree from Multimedia University, Malaysia, in 2007 and 2011, respectively, and the Ph.D. degree in engineering from University Tunku Abdul Rahman, Malaysia, in 2016. He is currently a Lecturer with the School of Information Technology, Monash University, Malaysia. His research interest is biometric template security.

Andreas Uhl (Senior Member, IEEE) is a Professor with the Department of Computer Sciences, University of Salzburg, where he heads the Multimedia Processing and Security Laboratory. His research interests include image and video processing and compression, wavelets, media security, medical imaging, biometrics, and number-theoretical numerics.