Chapter 16

Cancellable Biometrics for Finger Vein Recognition—Application in the Feature Domain

Simon Kirchgasser, Christof Kauba and Andreas Uhl

Abstract Privacy preservation is a key issue that has to be addressed in biometric recognition systems. Template protection schemes are a suitable way to tackle this task. Various template protection approaches originally proposed for other biometric modalities have been adopted to the domain of vascular pattern recognition. Cancellable biometrics are one class of these schemes. In this chapter, several cancellable biometrics methods like block re-mapping and block warping are applied in the feature domain. The results are compared to previous results obtained by the use of the same methods in the image domain regarding recognition performance, unlinkability and the level of privacy protection. The experiments are conducted using several well-established finger vein recognition systems on two publicly available datasets. Furthermore, an analysis regarding subject- versus system-dependent keys in terms of security and recognition performance is done.

Keywords Finger vein recognition · Template protection · Cancellable biometrics · Biometric performance evaluation · Block re-mapping · Warping

16.1 Introduction

Various methods exist to protect the subject-specific information contained in biometric samples and/or templates. According to several studies, e.g. Maltoni et al. [16], and ISO/IEC Standard 24745 [7] each method should exhibit four properties: *Security, Diversity, Revocability and Performance*. These shall ensure that the capture subject's privacy is protected and at the same time a stable and sufficient recognition

S. Kirchgasser · C. Kauba · A. Uhl (✉)
Department of Computer Sciences, University of Salzburg, Jakob-Haringer-Str. 2,
5020 Salzburg, Austria
e-mail: uhl@cs.sbg.ac.at

S. Kirchgasser
e-mail: skirch@cs.sbg.ac.at

C. Kauba
e-mail: ckauba@cs.sbg.ac.at

performance during the authentication process is achieved. The first aspect deals with the computational hardness to derive the original biometric template from the protected one (*security-irreversability*). *Diversity* is related to the privacy enhancement aspect and should ensure that the secured templates cannot be matched across different databases (*unlinkability*). The third aspect, *revocability*, should ensure that a compromised template can be revoked without exposing the biometric information, i.e. the original biometric trait/template remains unaltered and is not compromised. After removing the compromised data, a new template representing the same biometric instance can be generated. Finally, applying a certain protection scheme should not lead to a significant recognition performance degradation of the whole recognition system (*performance*).

One possibility to secure biometric information, cancellable biometrics, are introduced and evaluated on face and fingerprint data by Ratha et al. in [22]. The applied template protection schemes, *block re-mapping* and *warping*, have also been applied in the image domain and evaluated on iris [5, 14] and finger vein [20] datasets, respectively. Opposed to the latter study we want to investigate these schemes not in the image domain, but in the feature domain as several advantages and disadvantages exist in both spaces. These positive and negative aspects will be described in Sect. 16.2.

A detailed discussion on finger vein related template protection schemes, that can be found in literature, is given in Chap. 1 [26]. Thus, the interested reader is referred to this part of the handbook.

The rest of this chapter is organised as follows: The considered experimental questions are discussed in Sects. 16.2, 16.3 and 16.4 respectively. The employed non-invertible transform techniques are described in Sect. 16.5. Section 16.6 introduces the datasets utilised during the experimental evaluation, the finger vein recognition tool-chain as well as the evaluation protocol. The performance and unlinkability evaluation results are given and discussed in Sect. 16.7. Section 16.8 concludes this chapter and gives an outlook on future work.

16.2 Application in the Feature or Image Domain

If a template protection scheme is applied in the image/signal domain immediately after the image acquisition, the main advantage is that the biometric features extracted from the transformed sample do not correspond to those features computed from the original image/signal. So, the “real” template is never computed and does occur at no stage in the system and further, the sample is never processed in the system except at the sensor device. This provides the highest level of privacy protection for the capture subject. The main disadvantage of the application in the image/signal domain is that the feature extraction based on the protected image/signal might lead to incorrect features and thus, to inferior recognition performance. Especially in finger vein recognition, most of the well-established feature extraction schemes rely on tracking the vein lines, e.g. based on curvature information. By applying

template protection methods like block re-mapping in the image domain right after the sample is captured, connected vein structures will become disconnected. These veins are then no longer detected as continuous vein segments which potentially causes problems during the feature extraction and might lead to an incomplete or faulty feature representation of the captured image. Consequently, the recognition performance of the whole biometric system can be negatively influenced by the application of the template protection scheme.

On the contrary, if template protection is conducted in the feature domain, the feature extraction is finished prior to the application of the template protection approach. Thus, the extracted feature vector or template is not influenced by the template protection scheme at this stage and represents the biometric information of the capture subject in an optimal way.

16.3 Key Selection: Subject- Versus System-Specific

There are two different types of key selection, subject- and system-specific keys. In the subject-specific key approach, the template of each subject is generated by a key which is specific for each subject while for a system-specific key, the templates of all subjects are generated by the same key.

Subject dependent keys have advantages in terms of preserving the capture subjects' privacy compared to system-dependent keys. Assigning an individual key to each capture subject ensures that if an adversary gets to know the key of one of the capture subjects, he can not compromise the entire database as each key is individual. A capture subject-specific key also ensures that insider attacks performed by legitimate registered subjects can not be performed straight forward. Such an attack involves a registered capture subject, who is been granted access to the system and has access to the template database as well. This adversary capture subject wants to be legitimated as one of the other capture subjects of the same biometric system. So he/she could just try to copy one of his/her templates over the template belonging to another capture subject and claim that this is his/her identity, thus trying to get authenticated as this other, genuine capture subject. If capture subject-specific keys are used, this is not easily possible as each of the templates stored in the database has been generated using an individual key. However, it remains questionable if such an insider attack is a likely one. In fact, it would probably be easier for an adversary who has access to the entire template database to simply create and store a new genuine capture subject that exhibits his/her biometric information together with a key he sets in order to get the legitimation he wants to acquire. Another advantage of capture subject-specific keys is that the system's recognition performance is enhanced by introducing more inter-subject variabilities and thus impacting the performed impostor comparisons. The additional variability introduced by the subject-specific key in combination with the differences between different biometric capture subjects leads to a better separation of genuine and impostor pairs which enhances the overall system's performance.

One drawback of using capture subject-specific keys is that the system design gets more complex, depending on how the capture subject-specific keys are generated and stored. In contrast to a system-specific key, which is valid for all capture subjects and throughout all components of the biometric recognition system, the individual capture subject-specific keys have to be generated and/or stored somehow. One possibility is to generate the key based on the capture subject's biometric trait every time the capture subject wants to get authenticated. This methodology refers to the basic idea of Biometric Cryptosystems (BCS), which have originally been developed for either securing a cryptographic key applying biometric features or generating a cryptographic key based on the biometric features [9]. Thus, the objective to employ a BCS is different but the underlying concept is similar to the one described earlier. The second option can be used to generate the capture subject specific key once and then store this key which is later retrieved during the authentication process. This key can either be stored in a separate key database or with the capture subject itself. Storing the keys in a key database of course poses the risk of the key database getting attacked and eventually the keys getting disclosed to an adversary. Storing the keys with the capture subject is the better option in terms of key security, however it lowers the convenience of the whole system from the capture subjects' perspective as they have to be aware of their key, either by remembering the key or by using smart cards or similar key storage devices.

16.4 Unlinkability

The ISO/IEC Standard 24745 [7] defines that irreversibility is not sufficient for protected templates, as they also need to be unlinkable. Unlinkability guarantees that stored and protected biometric information can not be linked across various different applications or databases. The standard defines templates to be *fully linkable* if a method exists which is able to decide if two templates protected using a different key were extracted from the same biometric sample with a certainty of 100%. The degree of linkability depends on the certainty of the method which decides if two protected templates originate from the same capture subject. However, the standard only defines what unlinkability means but gives no generic way of quantifying it. Gomez-Barrero et al. [4] 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. Further details are given in Sect. 16.6.3 where the experimental protocol is introduced.

The application of the proposed framework [4] allows a comparison to previous work done on the aspect of key-sensitivity using the same protection schemes by Piciuccio et al. [20]. Protected templates generated from the same biometric data by using different keys should not be comparable. Thus, the authors of [20] used the so-called Renewable Template Matching Rate (RTMR) to prove a low matching rate between templates generated using different keys on both protection schemes.

This can also be interpreted as a high amount of unlinkability as the RTMR can be interpreted as a restricted version of the D_{sys} measure.

16.5 Applied Cancellable Biometrics Schemes

The two investigated non-invertible transforms, block re-mapping and warping, are both based on a regular grid. Some variants of them have been investigated and discussed in [21, 22]. The input (regardless if a binary matrix or image) is subdivided into non-overlapping blocks using a predefined block size. The constructed blocks are processed individually, generating an entire protected template or image. As we aim to utilise the same comparison module for the unprotected and protected templates, there is one preliminary condition that must be fulfilled for the selected schemes: The protected template must exhibit a structure similar to the original input template. In particular, we interpret the feature vector (template) as binary image, representing vein patterns as 1s and background information as 0s. Based on this representation, each x-/y-coordinate position (each pixel) in the input image can be either described as background pixel or as vein pattern pixel. Thus, our approach can be used in the signal domain as well as in the feature domain and the template protection performance results obtained in image domain can be directly compared to results obtained in the feature domain. Note that in the signal domain the input as well as the protected output images are no binary but greyscale ones, which does not change the way the underlying cancellable biometrics schemes are applied (as they only change positions of pixels and do not relate single pixel values to each other). In the following, the basic block re-mapping scheme as well as the warping approach are described.

16.5.1 Block Re-mapping

In block re-mapping [22], the number of predefined blocks is separated into two classes, where the total number of blocks remains unaltered. The blocks belonging to the first class are randomly placed at different positions to the ones they have been located in the original input. This random allocation is done by assigning random numbers generated by a number generator according to a predefined key. This key must be stored, such that a new image acquired during authentication can be protected using the same number generator specification. The blocks belonging to the second class are dismissed and do not appear in the output. This aspect ensures the irreversibility property of the block re-mapping scheme. The percentage of blocks belonging to each of the two classes is set by a predefined value. The more blocks in the second class, the less biometric information is present in the output. Usually, the percentage of blocks in the first class is between 1/4 and 3/4 of the total blocks.

Fig. 16.1 Schematic block re-mapping scheme

Figure 16.1 shows the block re-mapping scheme which has been implemented in a slightly adopted version compared to the original one done by Piciuccio et al. [20]. The main difference is the randomised block selection: We introduce an additional parameter, which controls the number of blocks that remain in the transformed template. To enable comparable results, we fixed the number of blocks that remain in the transformed templates to be at 75% of the original blocks. The required key information consists of the two set-up keys for the random generator and the block-size information for the grid construction. By comparing Fig. 16.1 (a) and (b) the following can be observed: While the blocks 4, 6 and 8 are present in (a) they do not occur in the protected, re-mapped image. All the other blocks are used to construct the re-mapped version (b) that has the same size as the original unprotected image or feature representation (a). It also becomes obvious that the blocks 3 and 5 are inserted multiple times into (b) in order to compensate for the absence of the non-considered blocks 6 and 8.

Due to the random selection, it is possible that some blocks are used more than once and others are never used. Otherwise, the re-mapping would resemble a permutation of all blocks, which could be reverted by applying a brute-force-attack testing all possible permutations or some more advanced attacks based on square jigsaw puzzle solver algorithms, e.g. [2, 19, 23].

The bigger the block size, the more biometric information is contained per block and thus, the higher the recognition performance is assumed to be after the application of block re-mapping. Of course, this argument also might depend on the feature extraction and comparison method as well as if it is done in signal or feature domain. Block re-mapping creates discontinuities at the block boundaries which influences the recognition performance if applied in the image domain as several of the feature extraction schemes try to follow continuous vein lines, which are not there any longer. This gets worse with decreasing block sizes. If block re-mapping is applied in the feature domain, this is not an issue as the feature extraction was done prior to applying the block re-mapping. However, due to the shifting process involved during comparison, the re-mapping of blocks can cause problems as a normalised region-of-interest is considered, especially for blocks that are placed at the boundaries of the protected templates. This might eventually lead to a degradation in the biometric systems performance because the information contained in those blocks is then “shifted out” of the image and the vein lines present in the blocks do not

Fig. 16.2 Finger vein templates displaying the variations that can occur during the re-mapping process using a block size of 64×64 pixel and MC as feature extraction method. The red dashed lines represent the grid

contribute to the comparison score anymore. In addition, blocks that share a common vein structure in the original template might be separated after performing the block re-mapping, posing a more severe problem due to the shifting applied during the comparison step. The vein structures close to the block borders are then shifted to completely different positions and cannot be compared any longer, leading to a decrease in the genuine comparison scores. Furthermore, it can also happen that the block re-mapping introduces new vein structures by combining two blocks that originally do not belong to each other. Both of the aforementioned possibilities have a potentially negative influence on the recognition performance. These problems due to the shifting applied during the comparison step are visualised in Fig. 16.2. It clearly can be seen that most of the vein structures visible in the original—left template, are not present in the protected—right template, but other structures have been newly introduced.

On the other hand, the larger the block size, the more of the original biometric information is contained per single block, lowering the level of privacy protection. Hence, we assume that a suitable trade-off between loss of recognition accuracy and level of privacy protection has to be found. Furthermore, the block size also corresponds to the irreversibility property of the transformation. The bigger the block size, the more information is contained per single block and the lower is the total number of blocks. The lower the number of blocks and the higher the information per block, the more effective are potential attacks on this protection scheme as discussed in the literature, e.g. [2, 19, 23].

16.5.2 Block Warping

Another non-invertible transformation in the context of cancellable biometrics is the so called “warping” (originally named “mesh warping” [27]). Warping can be applied in the image as well as in the template domain. 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. The warping

Fig. 16.3 Block Warping scheme including resize enhancement displayed schematically

Fig. 16.4 Finger vein templates displaying the variations that can occur during the warping process using a block size of 32×32 pixel and PC as feature extraction method

approach utilised in this chapter is a combination of using a regular grid, as in the block re-mapping scheme, and a distortion function based on spline interpolation. The regular grid is deformed per each block and adjusted to the warped output grid. The number of blocks in the output is the same as in the input, but the content of each individual block is distorted in the warped output.

This distortion is introduced by randomly altering the edge positions of the regular grid, leading to a non-predictable deformation of the regular grid. Spline based interpolation of the input information/pixels is applied to adopt the area of each block with respect to the smaller or larger block area obtained after the deformation application (warping might either stretch or shrink the area of the block as the edge positions are changed). This distortion is key dependent and the key defines the seed value for the random generator responsible for the replacement of the grid edges. This key needs to be protected by some cryptographic encryption methods and stored in a safe place. However, if the key gets disclosed, it is not possible to reconstruct all of the original biometric data in polynomial time due to the applied spline based interpolation. Figure 16.3 shows the basic warping scheme, while in Fig. 16.4 an example of a original—left template and its protected—right template is given.

The application of interpolation does increase the template protection degree as the relation between original vein structures is distorted. However, these transformations might destroy dependencies between the vein lines which are necessary in the feature extraction step in order to enable the same recognition performance as on the original, unprotected data. On the one hand, the application of warping transformations increases the capture subject's privacy but on the other hand the recognition performance is likely to decrease. For more information about other warping methods, the interested reader is referred to [3], where a review of several different possible solutions including the use of parametric and non-parametric functions can be found.

16.6 Experimental Set-Up

In the following, the experimental set-up, including the datasets, the finger vein recognition tool-chain as well as the experimental protocol are explained.

16.6.1 Finger Vein Datasets

The experiments are conducted on two datasets: The first one is the University of Twente Finger Vascular Pattern Database (UTFVP) [25]. It consists of 1440 images, which were acquired from 60 subjects in a single session. Six fingers were captured, including the index, ring and middle finger of both hands with 4 images per finger. The finger vein images have a resolution of 672×380 pixels and a density of 126 pixels/cm, resulting in a width of 4–20 pixels for the visible blood vessels.

The second dataset we utilise here is the PLUSVein-FV3 Dorsal–Palmar finger vein dataset and which has been introduced in [10] and is partly discussed in Chap. 3 [12]. To enable a meaningful comparison with the UTFVP results, we only use the palmar subset. Region-Of-Interest (ROI) images containing only the centre part of the finger where most of the vein pattern information is located have been extracted from the captured images as well. Some example images of the PLUSVein-FV3 subsets are given in Fig. 16.5.

16.6.2 Finger Vein Recognition Tool-Chain

In this subsection an overview of the most important parts of a typical finger vein recognition tool-chain is given. There are several studies about finger vein recognition

Fig. 16.5 Finger vein images of the PLUSVein-FV3 finger vein laser (first two rows) and LED subset (last two rows) showing 8 different fingers

systems, e.g. [8], that present and discuss different designs, but they all include a few common parts or modules. These main modules consist of: the finger vein scanner (image acquisition), the preprocessing module (preprocessing), the feature extraction module (feature extractor), the template comparison module (matcher) and the decision module (final decision). The system may contain an optional template protection module, either after the preprocessing module (image domain) or after the feature extraction module (feature domain). As the main focus of this chapter is on template protection applied in the feature domain, the system used during the experiments contains the template protection as part of the feature extractor. For feature extraction we selected six different methods: Gabor Filter (GF) [13], Isotropic Undecimated Wavelet Transform (IUWT) [24], Maximum Curvature (MC) [18], Principal Curvature (PC) [1], Repeated Line Tracking (RLT) [17] and Wide Line Detector (WLD) [6].

To calculate the final comparison scores an image correlation based comparison scheme as introduced by Miura et al. in [17] is applied to the baseline (unprotected) templates (features) as well as to the templates protected by block re-mapping and block warping. As the comparison scheme is correlation based, including a necessary pixel wise shifting, we selected a shift range of 80 pixels in x- and 30 pixels in y-direction, respectively. Further details on the deployed recognition tool-chain can be found in Chap. 4 [11] of this handbook.

16.6.3 *Experimental Protocol and Types of Experiments*

The necessary comparison scores are calculated using the correlation based comparison scheme described before and the comparison to be performed are based on the Fingerprint Verification Contests' (FVC) protocol [15]. To obtain the genuine scores, all possible comparisons are performed, i.e. the number of genuine scores is $60 * 6 * \frac{4*3}{2} = 2160$ (UTFVP) and $60 * 6 * \frac{5*4}{2} = 3600$ (PLUSVein-FV3), respectively. For the impostor scores, only a subset of all possible comparisons is performed. The first image of each finger is compared against the first image of all other fingers. This results in $\frac{60*6*(60*6-1)}{2} = 64,620$ impostor comparisons for each dataset (as both of them contain 60 subjects and 6 fingers per capture subject). As the employed comparison scheme is a symmetric measure, no symmetric comparisons (e.g. 1–2 and 2–1) are performed. The FVC protocol reduces the number of impostor comparisons in order to keep the computation time low for the whole performance evaluation while ensuring that every finger is compared against each other finger at least once. To quantify the recognition performance, several well-known measures are utilised: The equal error rate (EER, point where the FMR and the FNMR are equal), FMR_{100} (the lowest false Non-Match Rate (FNMR) for false match rate (FMR) $\leq 1\%$), FMR_{1000} (the lowest FNMR for FMR $\leq 0.1\%$) as well as the *ZeroFMR* (the FNMR for FMR = 0%).

We conduct four sets of experiments:

1. In the first set of experiments the unprotected templates are considered. The first experiments provide a baseline to compare the recognition performance of the protected templates to
2. The second set of experiments deals with the protected templates, generated by applying one of the aforementioned cancellable biometrics schemes to the same templates that have been used during the first set of experiments. For score calculation, these protected templates are compared against each other. For both employed cancellable schemes, 10 runs using different system keys are performed to assess the recognition performance variability and key dependency of the recognition performance.
3. The third set of experiments compares capture subject specific and system-specific keys. Therefore, a different key (note: the key is controlling the random selection of blocks or the repositioning of the grid) is assigned to each finger, thus resulting in 360 virtual subjects (not only the 60 physical ones). Again, 10 runs with different keys per run are performed and averaged afterwards. These capture subject-specific key results are then compared to the system-specific key ones as obtained in the second set of experiments.
4. The last set of experiments is committed to the unlinkability analysis. The approach by Gomez et al. [4], introduced in Sect. 16.4 describes the extent of linkability in the given data, with a range of D_{sys} from [0, 1]. The higher the value, the more linkable are the involved templates. Thus, the resulting measure represents a percentage of linkability that is present. Of course, full unlinkability is given if the score is 0. D_{sys} is based on the local $D(s)$ value, which is calculated based on the comparison scores of several mated (genuine) as well as non-mated (impostor) comparison between templates protected by the same template protection system but using different keys, thus originating from different applications or systems. We utilise this measure to assess the unlinkability of the presented cancellable biometric schemes for finger vein recognition (block re-mapping and warping).

To comply with the principles of reproducible research we provide all experimental details, results as well as the used vein recognition SDK, settings files and scripts to run the experiments for download on our website: <http://www.wavelab.at/sources/Kirchgasser19b/>. The used datasets are publicly available as well, hence it is possible to reproduce our results for anyone who is interested to do so.

16.6.4 Selecting the Processing Level to Insert Template Protection

If template protection is done in the signal domain cancellable biometrics schemes are applied directly after the image acquisition and before the feature extraction. Otherwise, template protection is applied to the extracted binary vein features in

order to protect the contained private biometric information right after the feature extraction is finished (feature domain).

The main purpose of this chapter and the experiments performed here is to provide a recognition performance comparison to the previous results obtained by Piciuccio et al. [20]. The authors used the same cancellable methods on the UTFVP finger vein images, but as opposed to this chapter, not in the feature domain, but in the image domain. To ensure that our results are comparable with the previous ones by Piciuccio et al. [20], we use the same block sizes during our experiments and select the same maximum offset for the block warping approach. Thus, we select block sizes of 16×16 , 32×32 , 48×48 , and 64×64 for block re-mapping and block warping. For block warping, maximum offset values of 6, 12, 18, and 24 pixel are considered. In the following result tables block re-mapping is abbreviated using *remap_16* (block size: 16×16) till *remap_64* (block size: 64×64), while all warping experiments correspond to *warp_16_6* (block size: 16×16 , offset: 6) till *warp_64_24* (block size: 64×64 , offset: 24).

In contrast to the work of Piciuccio et al. [20], we do not perform an analysis of the renewability and the key-sensitivity of the employed cancellable biometrics schemes. The key-sensitivity and renewability are expected to be similar for the schemes applied in the feature domain and in the image domain. Instead, we consider different issues like the comparison of capture subject vs. system-dependent keys, and a thorough unlinkability analysis.

16.7 Experimental Results

This section presents and discusses all relevant results concerning the various template protection methods' impact on the recognition performance and unlinkability in the four sets of experiments that have been considered. As we aim to compare the experimental results to the corresponding results reported in [20], we first summarise their main results:

- (a) The best performance results regarding EER were found for the block re-mapping scheme using a block size of 64×64 .
- (b) The best achieved EER was 1.67% for the protected data and 1.16% for the unprotected templates of the UTFVP dataset (using GF features).
- (c) Block re-mapping outperformed block warping.

16.7.1 Baseline Experiments

Table 16.1 lists the performance results of the baseline experiments in percentage terms for the UTFVP and the PLUSVein-FV3 dataset. Overall, the performance on the UTFVP dataset is slightly superior compared to the PLUSVein-FV3 dataset for most of the evaluated recognition schemes.

Table 16.1 Baseline performance on the UTFVP and PLUSVein-FV3 database in terms of *EER*, *FMR*₁₀₀, *FMR*₁₀₀₀ and *ZeroFMR*. The best performing results are highlighted in bold numbers

Features	GF	IUWT	MC	PC	RLT	WLD
<i>UTFVP</i>						
<i>EER</i> (%)	0.64	0.36	0.09	0.14	0.60	0.46
<i>FMR</i> ₁₀₀ (%)	0.60	0.27	0.04	0.13	0.32	0.27
<i>FMR</i> ₁₀₀₀ (%)	1.00	0.55	0.09	0.13	1.15	0.60
<i>ZeroFMR</i> (%)	1.00	1.34	0.23	0.87	1.89	1.43
<i>PLUSVein-FV3 Laser</i>						
<i>EER</i> (%)	0.74	1.49	0.33	1.47	1.71	1.38
<i>FMR</i> ₁₀₀	0.63	1.66	0.22	1.50	1.91	1.44
<i>FMR</i> ₁₀₀₀	1.47	2.08	0.44	2.19	2.52	1.75
<i>ZeroFMR</i>	1.75	2.77	0.72	2.75	3.77	1.94
<i>PLUSVein-FV3 LED</i>						
<i>EER</i> (%)	0.61	0.63	0.28	0.35	0.79	0.53
<i>FMR</i> ₁₀₀	0.52	0.52	0.27	0.33	0.72	0.52
<i>FMR</i> ₁₀₀₀	0.63	0.97	0.27	0.38	1.16	0.55
<i>ZeroFMR</i>	1.00	3.05	0.30	0.66	1.77	0.69

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 while GF has the worst performance with an *EER* of 0.64%. On both subsets of the PLUSVein-FV3 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. The other performance figures, i.e. *FMR*₁₀₀, *FMR*₁₀₀₀ and *ZeroFMR* are in line with the *EER* values and support the general trend that most of the applied feature extraction methods perform reasonably well on the given data sets using the baseline, unprotected templates.

16.7.2 Set 2—Protected Template Experiments (System Key)

As mentioned before, there are several parameters that have an essential influence on the recognition performance results obtained by applying the different cancellable biometrics schemes.

Table 16.2—feature domain and 16.3—signal domain, respectively, present the *EER* by using the mean ($\bar{x}$) and the standard deviation (σ) for both datasets. These results are calculated by randomly choosing 10 different keys and running the experiments first before the presented results are obtained by calculating $\bar{x}$ and σ of the performed computations.

Table 16.2 Recognition performance results (%) for template protection in the feature domain using system keys. The best performing results for each template protection method are 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											
rem _p _16	13.76	1.58	6.29	0.51	8.41	1.09	8.31	0.56	5.77	0.71	6.71	0.37
rem _p _32	9.12	2.08	4.85	1.25	4.52	1.46	4.79	1.54	5.06	0.94	4.34	1.34
rem _p _48	7.18	4.20	4.07	2.33	3.62	2.61	4.55	3.38	4.26	2.07	3.59	1.98
rem _p _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
warp_32_12	3.00	1.11	1.24	0.60	0.96	0.47	1.01	0.46	1.56	0.42	1.52	0.66
warp_48_18	2.45	1.15	1.15	0.60	0.87	0.42	0.92	0.47	1.44	0.45	1.34	0.67
warp_64_24	3.38	1.51	1.30	0.65	1.02	0.58	1.00	0.55	1.55	0.64	1.28	0.63
	PLUSVein-FV3 Laser											
rem _p _16	14.29	0.80	9.00	0.34	9.63	0.27	15.50	0.96	11.87	0.61	9.43	0.52
rem _p _32	12.02	1.12	7.72	0.97	10.24	0.57	12.38	2.07	11.54	1.42	6.60	0.94
rem _p _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
rem _p _64	10.79	5.10	7.20	2.19	10.60	0.88	14.82	6.78	15.90	11.24	5.60	2.90
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
warp_32_12	6.20	2.26	3.00	0.75	8.80	0.10	4.29	1.38	5.09	1.67	2.66	0.70
warp_48_18	4.38	1.38	2.50	0.61	8.75	0.15	3.53	1.13	4.22	1.10	2.20	0.58
warp_64_24	4.59	1.59	2.86	0.73	8.73	0.30	3.76	1.38	4.16	1.22	2.32	0.68
	PLUSVein-FV3 LED											
rem _p _16	14.03	1.03	10.01	0.47	14.57	0.62	16.50	1.10	12.64	0.73	10.67	0.57
rem _p _32	11.84	1.68	8.12	1.14	9.72	2.00	12.81	2.51	12.18	1.85	6.79	1.05
rem _p _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
rem _p _64	10.08	5.76	7.21	2.20	9.73	8.87	14.48	7.78	16.11	11.32	5.14	3.08
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
warp_32_12	5.67	2.29	2.51	0.92	3.32	1.92	3.76	1.66	4.87	1.86	1.84	0.72
warp_48_18	3.95	1.45	1.81	0.72	2.23	1.11	3.05	1.39	3.84	1.36	1.36	0.57
warp_64_24	4.07	1.69	2.48	1.15	2.27	1.06	3.51	1.66	3.90	1.65	1.55	0.90

At first we will discuss the results given by Table 16.2. Not surprisingly, the worst performance is observed for block re-mapping (*rem_p_16*, *rem_p_32*, *rem_p_48* and *rem_p_64*) using 16×16 as smallest block size while GF was applied (UTFVP). This trend is in line with the findings of Piciuccio et al. [20], which have been observed in the signal domain. It has to be mentioned that the observed results are strongly depending on the particular feature extraction method. As in [20] only the GF method was used for feature extraction, a direct comparison can only be done based on the GF results using the UTFVP dataset. This direct comparison shows that our best results on GF are worse compared to the results presented in [20] as we used a different implementation of the scheme. However, the best results using UTFVP are obtained by MC using a block size of 64×64 (*EER* 3.27). In general *rem_p_48* and *rem_p_64*

always resulted in the best performance for all datasets and not only on UTFVP (best *EER* of 5.52/4.42 for Laser/LED was achieved by applying WLD and *remap_48*). The only exception to this trend is given by RLT on the Laser/LED dataset. In this particular case, *remap_64* was performing worst, but this is a feature extraction type based observation.

In contrast to the block re-mapping based methods, the recognition performance of the warping based experiments (*warp_16_6* till *warp_64_24*) is better as observed for block re-mapping. This is in line with results reported for warping based experiments done in other biometric applications, e.g. [22] but opposed to the result of [20]. The best result on UTFVP is obtained for using PC and *warp_16_6* (*EER* 0.71). Nevertheless, there is not a big difference to the *EER* given by *warp_32_12*, *warp_48_18* and *warp_64_24*. It seems that the parameter choice has not a very high influence on the reported performance. For the other two datasets using WLD is resulting in the best *EER* values (Laser: 2.02, LED: 1.00).

As we want to compare the recognition performance of the feature domain template protected data to the same experiments which have been considering the transformations in the signal domain we will discuss the corresponding results now. The *EER* values applying template protection in the signal domain using system based keys are presented in Table 16.3.

The most important aspect using block re-mapping in the signal domain instead of applying the template protection schemes in the feature domain is a quite high-performance degradation in most of the conducted experiments. As mentioned in Sect. 16.2 it is likely that the feature extraction of the vein patterns after the template protection done in the signal domain might cause problems. This overall trend is confirmed by the observed *EER* results presented in Table 16.3. On UTFVP data, IUWT and PC resulted in the same trend that bigger block sizes are favourable in terms of performance (best average *EER*, 12.84, is given by IUWT using *remap_64*). For all other extraction schemes the *EER* values for *remap_16* or *remap_32* are better compared to *remap_64*. However, the performance difference is quite small.

Using warping, the influence on extracting the finger vein based features in the signal domain as compared to conducting the extraction in the feature domain is not so high as reported for block re-mapping. Hence, the overall performance trend using warping regardless of which dataset is considered, is similar to the results given in Table 16.2 (feature domain). IUWT again performs best in terms of *EER*. For *warp_16_6* the best performance can be reported. Surprisingly, the best average *EER*, 1.08, and the other performance values which are achieved applying IUWT on the template protected images are very similar for UTFVP and the LED dataset among each other.

Table 16.3 Recognition performance results (%) for template protection in the signal domain using system keys. The best performing results for each template protection method are 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											
rem _p _16	14.66	0.66	15.43	0.80	15.04	0.58	15.67	0.62	16.09	1.04	15.02	0.58
rem _p _32	15.14	1.35	13.75	1.54	14.67	1.65	14.17	1.32	14.25	1.54	14.58	1.31
rem _p _48	17.88	1.63	13.24	1.16	16.03	1.25	13.91	1.16	15.29	1.37	15.34	1.31
rem _p _64	17.68	1.52	12.84	1.11	16.33	1.46	13.01	1.06	15.27	1.79	14.95	1.51
warp_16_6	4.13	0.48	1.08	0.16	2.28	0.39	1.23	0.20	1.35	0.16	2.00	0.34
warp_32_12	3.49	0.64	2.31	0.55	3.35	0.62	2.70	0.64	1.81	0.29	3.04	0.53
warp_48_18	3.93	0.81	2.53	0.72	3.44	0.84	2.79	0.82	2.33	0.61	3.05	0.76
warp_64_24	3.40	0.83	2.15	0.67	2.66	0.95	2.11	0.82	2.04	0.40	2.47	0.72
	PLUSVein-FV3 Laser											
rem _p _16	9.87	0.54	9.43	0.49	9.74	0.41	10.61	0.38	10.47	0.62	9.24	0.45
rem _p _32	9.44	0.77	8.30	0.60	8.46	0.35	10.07	0.71	9.53	0.60	8.42	0.59
rem _p _48	10.36	1.05	9.14	0.89	9.04	0.85	10.15	0.69	10.49	0.75	9.17	0.99
rem _p _64	11.40	0.87	9.67	0.81	9.04	0.76	11.16	1.28	10.78	0.63	9.38	0.99
warp_16_6	6.94	0.82	2.61	0.20	7.01	0.19	5.84	0.95	4.80	0.62	2.72	0.20
warp_32_12	8.38	1.01	3.99	0.52	6.63	0.19	9.37	0.92	6.58	0.67	3.83	0.56
warp_48_18	6.12	1.49	3.49	0.66	6.84	0.26	7.71	1.49	5.70	1.17	3.38	0.79
warp_64_24	6.00	1.60	3.39	0.65	6.96	0.27	7.52	1.66	5.67	1.39	3.07	0.70
	PLUSVein-FV3 LED											
rem _p _16	14.99	0.89	15.29	0.71	15.27	0.57	16.24	1.05	16.79	1.37	15.02	0.58
rem _p _32	15.88	1.43	13.75	1.54	15.49	1.60	15.20	1.34	15.28	1.60	14.58	1.31
rem _p _48	18.97	2.18	13.21	1.23	17.01	1.86	14.51	1.77	16.49	1.73	15.34	1.31
rem _p _64	19.15	2.51	12.84	1.11	17.23	2.31	13.90	1.77	15.46	2.59	14.95	1.51
warp_16_6	4.85	0.51	1.08	0.16	3.13	0.46	2.04	0.26	2.59	0.22	2.00	0.34
warp_32_12	5.06	0.86	2.33	0.58	4.63	1.02	4.05	0.86	3.09	0.38	3.04	0.53
warp_48_18	5.05	0.94	2.53	0.72	4.71	0.88	4.49	0.69	3.56	0.65	3.05	0.76
warp_64_24	4.46	0.92	2.15	0.67	3.93	1.09	3.71	0.82	3.38	0.51	2.47	0.72

16.7.3 Set 3—Subject Dependent Versus System-Dependent Key

In this subsection, the capture subject-specific key experiments and their results are described and compared to the performance values obtained by using a system-dependent key. For the capture subject specific key experiments, a different and unique key for each finger is selected, compared to only one system-specific key, which is the same for all fingers. This should lead to a better differentiation of single capture subjects as the inter-subject variability is increased. Considering the subject dependent template protection experiments the results are summarised in Tables 16.4—feature domain, and 16.5—signal domain, respectively. As expected,

Table 16.4 Recognition performance results (%) for template protection in the feature domain using subject-specific keys. The best performing results for each template protection method are 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											
rem _p _16	3.28	0.20	4.82	0.38	4.70	0.29	7.68	0.47	3.19	0.24	5.79	0.31
rem _p _32	2.83	0.35	3.49	0.29	2.63	0.30	4.65	0.40	2.74	0.20	3.31	0.24
rem _p _48	2.93	0.28	3.18	0.41	2.27	0.25	3.41	0.36	2.90	0.33	2.31	0.15
rem _p _64	4.35	0.41	2.28	0.27	2.09	0.27	2.35	0.29	2.27	0.41	1.90	0.27
warp_16_6	2.74	0.23	0.72	0.18	0.68	0.20	0.82	0.13	1.00	0.10	1.24	0.16
warp_32_12	3.01	0.26	1.35	0.16	1.12	0.13	1.23	0.15	1.54	0.15	1.63	0.24
warp_48_18	2.20	0.24	1.16	0.19	0.90	0.16	1.08	0.16	1.26	0.20	1.33	0.15
warp_64_24	2.72	0.26	1.39	0.18	0.99	0.29	1.37	0.27	1.33	0.18	1.45	0.30
	PLUSVein-FV3 Laser											
rem _p _16	12.83	0.53	5.58	0.30	3.44	0.17	14.95	0.52	6.58	0.27	6.11	0.37
rem _p _32	9.50	0.40	3.46	0.28	3.60	0.23	10.96	0.45	6.58	0.38	3.81	0.21
rem _p _48	8.30	0.43	3.27	0.22	3.94	0.14	12.53	0.53	7.72	0.52	3.31	0.27
rem _p _64	5.15	0.31	1.84	0.17	3.93	0.26	11.09	0.93	6.93	0.62	2.52	0.15
warp_16_6	5.14	0.19	1.81	0.10	6.04	0.15	2.78	0.15	3.82	0.16	1.95	0.12
warp_32_12	6.07	0.28	2.41	0.16	5.83	0.12	4.54	0.33	5.02	0.27	2.41	0.15
warp_48_18	4.31	0.33	2.12	0.18	6.05	0.10	3.63	0.32	3.93	0.30	2.02	0.17
warp_64_24	4.42	0.35	2.26	0.24	4.71	0.23	4.35	0.22	3.96	0.40	2.18	0.19
	PLUSVein-FV3 LED											
rem _p _16	12.23	0.54	5.90	0.32	13.13	0.43	15.30	0.46	6.85	0.27	6.70	0.37
rem _p _32	9.08	0.42	3.67	0.36	8.02	0.38	11.00	0.65	6.79	0.28	3.81	0.25
rem _p _48	7.61	0.31	3.58	0.16	5.65	0.34	12.69	0.64	8.01	0.39	2.95	0.29
rem _p _64	4.64	0.33	1.93	0.15	5.51	0.40	10.35	0.80	7.32	0.73	2.15	0.26
warp_16_6	4.10	0.22	0.90	0.09	1.42	0.14	1.78	0.23	3.18	0.29	0.85	0.09
warp_32_12	5.85	0.41	2.00	0.21	3.36	0.28	4.22	0.27	4.83	0.19	1.65	0.23
warp_48_18	3.83	0.43	1.54	0.17	2.39	0.32	3.44	0.26	3.69	0.44	1.32	0.24
warp_64_24	3.88	0.30	1.85	0.29	2.54	0.43	4.00	0.31	3.66	0.33	1.50	0.44

it becomes apparent that the overall performance of all experiments using subject dependent keys is much better compared to the system-specific key results. This can be explained as the usage of subject dependent keys provides a better separation of genuine and impostor score distributions after applying the transformation.

The best feature domain based performance (see Table 16.4) is obtained on UTFVP using WLD during rem_p_64 (EER 1.90) and MC during warp_16_6 (EER 0.68), on the Laser dataset using IUWT (EER 1.84 for rem_p_64, EER 1.81 for warp_16_6) and finally on the LED dataset using IUWT/WLD (EER 1.93/0.85) applying rem_p_64/warp_16_6. According to the EER values highlighted in Table 16.5 (signal domain) the overall best recognition performance is achieved by applying the template protection schemes in the signal domain using subject-specific

Table 16.5 Recognition performance results (%) for template protection in the signal domain using subject-specific keys. The best performing results for each template protection method are 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_16	0.98	0.15	0.59	0.09	0.78	0.10	0.98	0.13	1.13	0.13	0.53	0.04
remp_32	0.50	0.09	0.48	0.07	0.69	0.12	0.86	0.18	0.96	0.18	0.41	0.09
remp_48	0.39	0.04	0.46	0.07	0.54	0.05	0.77	0.14	0.52	0.10	0.45	0.08
remp_64	0.48	0.12	0.44	0.15	0.57	0.13	0.60	0.13	0.57	0.10	0.41	0.08
warp_16_6	1.39	0.16	0.57	0.07	0.64	0.12	0.42	0.09	0.80	0.06	0.43	0.10
warp_32_12	2.16	0.22	1.31	0.28	1.65	0.19	1.66	0.17	1.22	0.20	1.47	0.16
warp_48_18	2.15	0.19	1.55	0.14	1.64	0.20	1.70	0.15	1.51	0.14	1.76	0.16
warp_64_24	1.80	0.23	1.64	0.25	1.50	0.20	1.68	0.31	1.44	0.18	1.77	0.17
	PLUSVein-FV3 Laser											
remp_16	3.44	0.17	0.96	0.11	0.69	0.06	3.04	0.16	3.6	0.25	1.08	0.10
remp_32	3.21	0.33	1.29	0.20	0.96	0.08	4.29	0.26	4.34	0.29	1.38	0.20
remp_48	3.95	0.33	1.47	0.20	1.09	0.12	4.71	0.27	5.48	0.20	1.68	0.16
remp_64	4.09	0.31	1.88	0.19	1.11	0.10	5.45	0.40	4.89	0.38	2.17	0.24
warp_16_6	5.62	0.24	2.35	0.06	2.82	0.14	5.65	0.15	4.57	0.21	2.12	0.10
warp_32_12	6.74	0.27	2.87	0.10	2.88	0.12	8.46	0.26	5.74	0.26	2.65	0.11
warp_48_18	6.23	0.26	3.02	0.19	3.23	0.14	8.17	0.31	5.76	0.28	2.77	0.23
warp_64_24	5.71	0.30	2.81	0.14	3.87	0.20	7.61	0.31	5.54	0.34	2.45	0.12
	PLUSVein-FV3 LED											
remp_16	1.93	0.20	0.59	0.09	1.54	0.10	1.93	0.21	2.27	0.19	0.53	0.04
remp_32	1.06	0.16	0.48	0.07	1.51	0.20	2.53	0.27	2.14	0.21	0.41	0.09
remp_48	1.08	0.09	0.46	0.07	1.76	0.13	2.50	0.25	1.25	0.18	0.45	0.08
remp_64	0.88	0.16	0.44	0.15	1.46	0.23	1.87	0.25	1.21	0.21	0.41	0.08
warp_16_6	3.64	0.23	0.57	0.07	2.7	0.27	1.78	0.22	2.25	0.25	0.43	0.10
warp_32_12	4.81	0.28	1.31	0.28	4.05	0.22	3.95	0.24	2.83	0.23	1.47	0.16
warp_48_18	4.07	0.22	1.55	0.14	3.61	0.33	3.89	0.25	3.03	0.32	1.76	0.16
warp_64_24	3.72	0.30	1.64	0.25	3.37	0.25	3.77	0.29	3.06	0.13	1.77	0.17

keys. This observation is interesting because it seems that in most cases subject-specific keys have a more positive effect on the protected features’ performance if the corresponding transformation was applied in the signal domain. However, there are also some cases where the subject-specific keys’ signal domain performance is lower compared to the best results obtained in the feature domain, e.g. Laser dataset using WLD and *warp_16_6*. Compared to [20] the recognition performance presented in Table 16.5 using GF is outperforming the findings stated by Piciucco et al. no matter if block re-mapping or warping is considered. All other results obtained for UTFVP are better as well.

16.7.4 Set 4—Unlinkability Analysis

The unlinkability analysis is performed to ensure that the applied template protection schemes meet the principles established by the ISO/IEC 24745 standard [7], in particular the unlinkability requirements. If there is a high amount of linkability for a certain template protection scheme, it is easy to match two protected templates from the same finger among different applications using different keys. In that case, it is easy to track the capture subjects across different applications, which poses a threat to the capture subjects’ privacy. The unlinkability is likely to be low (linkability high) if there is too little variation between protected templates based on two different keys (i.e. the key-sensitivity is low) or the unprotected and the protected template in general. Tables 16.6, 16.7, 16.8 and 16.9 lists the global unlinkability scores, D_{sys} ,

Table 16.6 D_{sys} unlinkability scores for the selected template protection schemes applied in feature domain using system dependent keys. The best results (low values, representing unlinkability) for each template protection method are highlighted in bold numbers

tempProt	Dsys											
	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_16	3.43	0.52	3.02	0.58	3.91	0.97	2.90	0.32	3.09	0.46	4.35	0.53
remp_32	13.96	13.89	10.32	16.79	15.83	16.09	9.34	17.09	8.21	5.88	16.71	19.25
remp_48	18.72	22.27	14.92	23.90	21.49	25.76	13.86	23.66	10.65	17.60	18.54	26.33
remp_64	25.67	18.69	20.03	21.95	29.72	22.93	20.81	22.36	16.32	19.89	27.24	22.93
warp_16_6	56.35	8.94	85.01	6.92	82.61	6.31	79.54	8.02	81.66	6.00	74.87	8.19
warp_32_12	37.54	17.97	40.18	21.74	55.86	17.66	40.18	21.45	44.37	18.8	43.19	19.43
warp_48_18	36.15	22.52	39.08	27.65	52.76	22.89	37.17	26.75	42.92	25.3	41.56	25.20
warp_64_24	42.43	29.21	41.21	32.14	53.13	28.26	48.81	32.36	44.68	31.45	43.43	21.12
	PLUSVein-FV3 Laser											
remp_16	4.07	0.50	2.73	0.44	3.42	0.70	2.79	0.53	2.64	0.49	4.28	0.81
remp_32	20.16	17.10	13.77	18.96	21.00	20.97	10.40	18.23	8.80	9.95	17.13	21.00
remp_48	14.00	17.39	9.18	17.69	14.53	20.09	7.18	16.55	5.26	8.39	12.75	20.81
remp_64	19.58	22.01	14.37	22.48	24.51	22.42	10.06	18.07	7.38	10.77	17.77	21.53
warp_16_6	63.42	10.55	81.26	10.17	86.37	4.36	83.99	6.77	68.19	9.82	82.1	8.65
warp_32_12	34.62	17.86	35.90	20.96	53.34	17.51	44.14	18.82	29.83	13.38	46.36	18.48
warp_48_18	44.30	21.56	42.61	23.67	58.42	18.86	47.80	21.23	34.44	18.93	52.10	20.69
warp_64_24	33.33	26.48	35.28	28.94	43.99	28.59	34.27	27.20	28.83	24.97	47.23	17.95
	PLUSVein-FV3 LED											
remp_16	3.81	0.42	2.86	0.46	3.34	0.62	2.55	0.35	2.34	0.45	4.04	0.65
remp_32	19.67	17.36	13.07	18.9	21.71	20.47	10.62	18.32	8.69	10.20	17.03	21.01
remp_48	14.06	17.78	9.18	17.51	14.99	20.62	7.42	16.15	5.56	9.35	13.23	21.38
remp_64	19.44	22.26	13.58	22.05	23.53	22.61	10.13	17.94	7.71	10.23	16.91	21.19
warp_16_6	67.02	10.53	81.95	10.31	86.66	6.62	84.38	7.23	67.51	10.59	82.58	8.37
warp_32_12	37.51	17.38	35.27	20.74	56.52	16.52	44.58	18.94	28.62	12.99	47.66	18.31
warp_48_18	45.41	22.65	42.56	24.21	60.46	19.33	48.14	21.48	34.10	19.43	52.99	21.83
warp_64_24	32.81	26.35	32.99	28.49	45.09	28.34	33.88	27.47	27.70	24.25	48.52	19.11

Table 16.7 D_{sys} unlinkability scores for the selected template protection schemes applied in signal domain using system dependent keys. The best results (low values, representing unlinkability) for each template protection method are highlighted in bold numbers

tempProt	Dsys											
	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											
rem _p _16	2.97	0.63	2.97	0.66	3.05	0.59	2.77	0.33	2.86	0.51	3.34	0.81
rem _p _32	6.03	12.42	6.17	12.76	6.07	12.19	5.80	12.48	5.84	12.55	6.46	12.39
rem _p _48	6.74	12.04	6.70	13.94	6.91	12.34	6.93	13.81	6.00	13.35	7.58	13.07
rem _p _64	6.43	11.24	6.56	13.61	6.37	11.53	6.63	13.79	6.16	12.94	7.30	13.04
warp_16_6	73.00	4.02	87.21	2.49	82.97	3.05	84.81	2.82	83.14	2.60	84.17	2.89
warp_32_12	42.85	14.28	50.90	14.94	52.36	12.40	47.03	15.45	55.01	12.49	49.88	14.39
warp_48_18	32.64	17.20	33.24	19.71	42.26	16.50	33.26	20.97	36.79	18.98	37.10	18.63
warp_64_24	26.00	17.83	17.92	11.65	28.71	14.28	23.11	20.41	26.72	19.19	26.40	18.45
	PLUSVein-FV3 Laser											
rem _p _16	2.68	0.44	2.30	0.34	2.41	0.40	2.25	0.32	2.57	0.38	3.59	1.03
rem _p _32	8.83	16.19	6.96	16.48	7.20	16.63	6.32	16.16	6.74	16.63	9.66	16.12
rem _p _48	9.12	15.05	7.27	15.86	8.52	14.69	6.71	15.86	6.30	16.13	8.90	15.21
rem _p _64	9.78	15.43	7.76	15.97	8.88	15.36	7.83	16.08	7.43	15.97	10.50	15.92
warp_16_6	76.36	5.87	89.06	2.95	87.14	1.66	77.23	2.55	80.01	2.64	86.3	1.51
warp_32_12	42.37	20.44	44.63	12.57	51.05	12.38	35.13	14.56	42.47	14.04	53.03	7.96
warp_48_18	29.59	16.50	31.37	18.84	41.96	18.63	24.50	16.14	27.83	19.52	47.16	23.77
warp_64_24	27.99	20.84	25.37	21.61	37.85	20.00	20.92	17.16	23.03	18.72	21.00	4.95
	PLUSVein-FV3 LED											
rem _p _16	2.97	0.63	3.00	0.5	3.00	0.56	2.80	0.60	2.86	0.51	3.34	0.81
rem _p _32	6.20	12.78	6.37	13.12	6.07	12.19	6.02	12.44	2.88	0.44	6.46	12.39
rem _p _48	6.74	12.04	7.05	14.79	6.91	12.34	6.99	13.62	6.38	14.16	7.58	13.07
rem _p _64	6.43	11.24	6.56	13.61	6.37	11.53	6.74	13.87	6.16	12.94	7.30	13.04
warp_16_6	78.42	5.77	90.04	3.05	88.48	1.96	78.32	3.05	81.22	3.46	88.02	1.94
warp_32_12	41.32	21.14	45.32	12.85	52.04	11.89	36.03	15.06	44.86	15.21	53.97	8.69
warp_48_18	30.55	17.05	31.34	19.79	41.58	19.25	23.99	15.12	28.66	20.12	48.86	24.97
warp_64_24	27.89	21.00	25.27	20.99	37.92	19.53	21.45	18.10	24.26	19.27	20.95	6.01

for all datasets using block re-mapping and warping, similar to the tables that have been used to describe the recognition performance. 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.

The D_{sys} ranges reveal that there are several block re-mapping configurations leading to a low linkability score, indicating that the protected templates cannot be linked across different applications (high unlinkability). This can be observed not only for applying block re-mapping in the feature domain using system-specific keys but also for the application in all other feature spaces and key selection strategies. The lowest D_{sys} scores can be detected for the usage of *rem_p_16*. For most block sizes

Table 16.8 D_{sys} unlinkability scores for the selected template protection schemes applied in feature domain using subject dependent keys. The best results (low values, representing unlinkability) for each template protection method are highlighted in bold numbers

tempProt	Dsys											
	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											
rem _p _16	3.43	0.52	3.02	0.58	3.95	0.96	2.90	0.32	3.09	0.46	4.35	0.53
rem _p _32	13.93	13.48	10.32	16.79	15.83	16.09	9.34	17.09	8.21	5.88	15.75	17.80
rem _p _48	18.72	22.27	14.92	23.90	21.49	25.76	13.86	23.66	11.82	17.72	18.78	25.23
rem _p _64	24.41	18.90	20.03	21.95	30.95	22.85	20.81	22.36	15.54	19.52	25.92	22.94
warp_16_6	58.04	1.07	83.14	0.75	82.94	0.85	79.15	0.62	79.77	0.73	74.92	1.05
warp_32_12	31.73	11.71	35.67	11.85	49.61	8.56	33.63	12.28	38.96	1.45	37.93	11.00
warp_48_18	39.17	10.46	41.63	10.63	53.54	7.86	40.12	10.94	44.94	1.53	44.28	9.66
warp_64_24	35.15	11.68	32.15	12.61	44.85	9.88	37.82	11.54	36.36	1.57	36.56	10.85
	PLUSVein-FV3 Laser											
rem _p _16	4.07	0.50	2.73	0.44	3.41	0.75	2.79	0.53	2.65	0.51	4.29	0.84
rem _p _32	20.38	17.60	13.77	18.96	21.00	20.97	10.40	18.23	9.08	10.21	17.95	21.35
rem _p _48	14.61	17.73	9.18	17.69	14.53	20.09	7.18	16.55	5.26	8.39	12.75	20.81
rem _p _64	19.58	22.01	14.37	22.48	24.51	22.42	10.48	18.53	7.38	10.77	17.77	21.53
warp_16_6	67.33	0.71	84.02	0.88	87.14	0.92	85.30	0.67	70.99	0.97	83.39	0.93
warp_32_12	32.71	12.16	34.82	13.06	49.23	9.01	41.37	10.71	29.76	0.94	44.48	10.19
warp_48_18	38.73	11.35	39.00	11.80	50.29	9.14	40.83	11.08	34.65	1.93	46.5	10.38
warp_64_24	31.46	13.65	32.65	13.16	41.79	11.84	31.79	13.04	28.76	1.34	43.25	10.12
	PLUSVein-FV3 LED											
rem _p _16	3.81	0.42	2.86	0.46	3.34	0.62	2.55	0.35	2.34	0.45	4.04	0.65
rem _p _32	19.67	17.36	13.07	18.90	21.71	20.47	10.62	18.32	8.69	10.20	17.03	21.01
rem _p _48	14.06	17.78	9.18	17.51	14.99	20.62	7.42	16.15	5.56	9.35	13.23	21.38
rem _p _64	19.44	22.26	13.58	22.05	23.53	22.61	10.13	17.94	7.71	10.23	16.91	21.19
warp_16_6	71.08	0.81	83.99	0.87	88.52	0.64	86.55	0.66	70.93	1.10	84.96	0.80
warp_32_12	34.39	11.73	33.42	12.73	51.79	8.49	41.2	10.74	28.42	0.75	45.48	9.75
warp_48_18	39.69	11.23	38.46	11.82	51.87	8.79	40.85	11.3	34.03	1.65	46.56	9.92
warp_64_24	31.96	12.91	31.72	13.33	43.29	10.78	31.66	13.12	28.79	1.73	44.34	9.68

48 × 48 or 64 × 64 the unlinkability values are higher compared to the schemes using lower block sizes. Thus, the linkability is increased.

For warping the situation is different. First, the obtained D_{sys} is mostly quite high which indicates a high linkability regardless the choice of key selection strategy or the domain. Second, warp_32_12 or warp_48_18 exhibit the lowest unlinkability scores, clearly the highest amount of linkability detected for warp_16_6. The reason for this is given by the applied warping scheme. If small block sizes are used the offset, which is responsible for the amount of introduced degradation during the transformation, is small as well. Thus, for an offset of 6 only a little amount of variation in the original image (signal domain) or extracted template (feature domain) is caused. Of course,

Table 16.9 D_{sys} unlinkability scores for the selected template protection schemes applied in signal domain using subject dependent keys. The best results (low values, representing unlinkability) for each template protection method are highlighted in bold numbers

tempProt	Dsys											
	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											
<i>remp_16</i>	2.97	0.63	2.97	0.66	3.05	0.59	2.77	0.33	2.86	0.51	3.34	0.81
<i>remp_32</i>	6.16	12.79	6.17	12.76	6.07	12.19	5.80	12.48	5.84	12.55	6.67	12.74
<i>remp_48</i>	6.74	12.04	6.70	13.94	6.91	12.34	6.93	13.81	6.00	13.35	7.58	13.07
<i>remp_64</i>	6.43	11.24	6.56	13.61	6.37	11.53	6.63	13.79	6.16	12.94	7.30	13.04
<i>warp_16_6</i>	75.41	0.56	88.16	0.35	84.89	0.55	87.22	0.52	85.51	0.53	85.8	0.43
<i>warp_32_12</i>	46.76	8.57	54.42	7.20	55.75	6.54	51.39	7.64	58.88	6.22	54.15	6.97
<i>warp_48_18</i>	33.87	12.06	33.68	12.37	41.34	10.28	32.58	12.28	38.74	11.10	36.49	11.48
<i>warp_64_24</i>	29.82	13.06	25.12	14.42	34.74	12.11	25.41	14.21	30.16	13.12	29.96	13.16
	PLUSVein-FV3 Laser											
<i>remp_16</i>	2.68	0.44	2.30	0.34	2.41	0.40	2.25	0.32	2.57	0.38	3.59	1.03
<i>remp_32</i>	8.83	16.19	6.96	16.48	7.20	16.63	6.32	16.16	6.74	16.63	9.66	16.12
<i>remp_48</i>	9.12	15.05	7.27	15.86	8.52	14.69	6.71	15.86	6.30	16.13	8.90	15.21
<i>remp_64</i>	9.78	15.43	7.76	15.97	8.88	15.36	7.83	16.08	7.43	15.97	10.50	15.92
<i>warp_16_6</i>	78.38	0.56	90.26	0.46	87.71	0.51	78.41	0.58	80.34	0.48	88.56	0.43
<i>warp_32_12</i>	42.94	0.86	49.98	1.11	54.95	1.50	36.00	0.99	42.75	1.14	56.58	1.22
<i>warp_48_18</i>	29.25	0.95	29.10	0.97	37.86	1.20	21.38	0.70	25.02	1.17	37.98	1.07
<i>warp_64_24</i>	23.59	1.18	19.47	1.44	31.20	1.64	15.97	0.98	18.19	1.08	29.28	1.29
	PLUSVein-FV3 LED											
<i>remp_16</i>	2.97	0.63	3.00	0.5	3.00	0.56	2.80	0.60	2.86	0.51	3.34	0.81
<i>remp_32</i>	6.03	12.42	6.17	12.76	6.07	12.19	6.02	12.44	5.84	12.55	6.46	12.39
<i>remp_48</i>	6.74	12.04	7.05	14.79	6.91	12.34	6.99	13.62	6.38	14.16	7.58	13.07
<i>remp_64</i>	6.43	11.24	6.56	13.61	6.37	11.53	6.74	13.87	6.16	12.94	7.30	13.04
<i>warp_16_6</i>	79.05	0.78	91.02	0.59	88.45	0.89	79.88	0.75	81.45	0.75	89.16	0.66
<i>warp_32_12</i>	43.65	1.22	50.25	1.89	55.66	1.87	36.99	1.36	43.83	2.04	57.39	1.77
<i>warp_48_18</i>	29.85	1.36	30.02	1.48	38.58	1.67	22.22	1.12	26.28	1.99	38.75	1.39
<i>warp_64_24</i>	24.58	1.77	20.23	2.06	32.52	2.24	16.28	1.25	19.12	1.89	30.42	1.58

this results in a high linkability score as the transformed biometric information is minimally protected.

In Fig. 16.6 4 examples exhibiting score distributions and corresponding D_{sys} values are shown for block re-mapping: First row—*remp_16* (a) and *remp_54* (b), and warping: Second row—*warp_16_6* (c) and *warp_64_24* (d). The blue line represents the process of D_{sys} for all threshold selections done during the computation (see [4]). The green distribution corresponds to 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 [4]. The red coloured distribution describes the *non-mated* samples scores, which are yielded by templates generated

Fig. 16.6 Example images which display unlinkability scores. In all four examples signal domain, PC features on the PLUSVein-FV3 Laser dataset and subject-specific key selection was applied

from samples of different instances using different keys. According to [4] a *fully unlinkable* scenario can be observed if both coloured distributions are identical, while *full linkability* is given if mated and non-mated distributions can be fully separated from each other. For block re-mapping, (a) and (b) almost full unlinkability is achieved in both cases, while for the warping examples, (c) and (d) the distributions can be partly separated from each other. The worst result regarding the ISO/IEC Standard 24745 [7] property of unlinkability is exhibited by example (c) as both distributions are separated quite well, which leads to a high amount of linkability. Thus, in *warp_16_6* it is possible to decide with high probability to which dataset a protected template belongs. Furthermore, from a security point of view warping is not really a suitable template protection scheme using the given parameters. As the amount of linkability decreases using bigger block sizes and more importantly larger offsets it seems to be possible to select a parameter set-up that is providing both a good recognition performance and a quit low linkability at the same time.

According to these results, it is possible to summarise the findings taking the recognition performance and unlinkability evaluation into account:

- (a) Only a very low amount of capture subject's privacy protection for configurations exhibiting a low *EER* is obtained for the application of warping schemes.
- (b) A high *EER* is observed for the configurations that exhibit a high unlinkability (e.g. detected during the application of block re-mapping schemes in most cases).

Additionally, it must be mentioned that the template protection application in feature or signal domain shows differences regarding the unlinkability aspect. For both, block re-mapping and warping, it is better to apply template protection in the signal domain as the D_{sys} values are lower for almost all cases. If the recognition performance is taken into account as well the best obtained experimental setting is the template protection application in the signal domain using subject-specific keys.

However, the provided level of privacy protection, especially if it comes to unlinkability is clearly not enough for a practical application of warping based cancellable schemes in the feature domain and several signal domain settings using the selected parameters. Furthermore, the worse recognition performance restricts the use of block re-mapping schemes for real-world biometric systems in the most cases as well.

16.8 Conclusion

In this chapter, template protection schemes in finger vein recognition with a focus on cancellable schemes and their application in the feature domain were presented and evaluated. The focus was hereby on cancellable schemes that can be applied in both the signal and the feature domain in the context of finger vein recognition. Two well-known representatives of those schemes, namely, block re-mapping and block warping were evaluated in signal and feature domain on two different publicly available finger vein data sets: the UTFVP and the palmar subsets of the PLUSVein-FV3. These schemes are the same ones that have been applied in the image domain in the previous work of Piciuccio et al. [20].

Compared to the previous results obtained in [20], none of the block re-mapping methods performed well in the feature and signal domain using system-specific keys. The experiments considering a capture subject-specific key instead of a system specific one lead to an improvement regarding the recognition performance, especially in the signal domain. Warping performed much better in both domains but further results on the unlinkability revealed that the privacy protection amount is very limited. Thus, an application in real-world biometric systems is restricted for the most experimental settings according to the fact that it is possible to track a subject across several instances generated with various keys.

Nevertheless, it was possible to observe the following trend that leads to an optimistic conclusion. Of course, both template protection schemes have their weaknesses, block re-mapping exhibits recognition performance problems, while warping lacks in terms of unlinkability, but according to the results it seems that the selection of a larger offset could reduce the unlinkability issue for warping in the signal domain. In particular, the larger the offset was selected the better the unlinkability

performed, while the recognition performance was hardly influenced. According to this observation, we claim that warping is a suitable cancellable template protection scheme for finger vein biometrics if it is applied in the signal domain using subject-specific keys and a large offset to achieve sufficient unlinkability.

References

1. Choi JH, Song W, Kim T, Lee S-R, Kim HC (2009) Finger vein extraction using gradient normalization and principal curvature. *Proc SPIE* 7251:9
2. Gallagher AC (2012) Jigsaw puzzles with pieces of unknown orientation. In: 2012 IEEE Conference on computer vision and pattern recognition (CVPR). IEEE, pp 382–389
3. Glasbey CA, Mardia KV (1998) A review of image-warping methods. *J Appl Stat* 25(2):155–171
4. Gomez-Barrero M, Galbally J, Rathgeb C, Busch C (2018) General framework to evaluate unlinkability in biometric template protection systems. *IEEE Trans Inf Forensics Secur* 13(6):1406–1420
5. Hämmerle-Uhl J, Pschernig E, Uhl A (2009) Cancelable iris biometrics using block re-mapping and image warping. In: Samarati P, Yung M, Martinelli F, Ardagna CA (eds) *Proceedings of the 12th international information security conference (ISC'09)*, volume 5735 of LNCS. Springer, pp 135–142
6. Huang B, Dai Y, Li R, Tang D, Li W (2010) Finger-vein authentication based on wide line detector and pattern normalization. In: 2010 20th International conference on pattern recognition (ICPR). IEEE, pp 1269–1272
7. ISO/IEC 24745—Information technology—Security techniques—biometric information protection. Standard, International Organization for Standardization, June 2011
8. Jadhav M, Nerkar PM (2015) Survey on finger vein biometric authentication system. *Int J Comput Appl* (3):14–17
9. Jain AK, Nandakumar K, Nagar A (2008) Biometric template security. *EURASIP J Adv Signal Process* 2008:113
10. Kauba C, Prommegger B, Uhl A (2018) The two sides of the finger—an evaluation on the recognition performance of dorsal vs. palmar finger-veins. In: *Proceedings of the international conference of the biometrics special interest group (BIOSIG'18)*, Darmstadt, Germany (accepted)
11. Kauba C, Prommegger B, Uhl A (2019) An available open source vein recognition framework. In: Uhl A, Busch C, Marcel S, Veldhuis R (eds) *Handbook of vascular biometrics*. Springer Science+Business Media, Boston, MA, USA, pp 77–112
12. Kauba C, Prommegger B, Uhl A (2019) Openvein—an open-source modular multi-purpose finger-vein scanner design. In: Uhl A, Busch C, Marcel S, Veldhuis R (eds) *Handbook of vascular biometrics*. Springer Science+Business Media, Boston, MA, USA, pp 77–112
13. Kumar A, Zhou Y (2012) Human identification using finger images. *IEEE Trans Image Process* 21(4):2228–2244
14. Lai Y-L, Jin Z, Teoh ABJ, Goi B-M, Yap W-S, Chai T-Y, Rathgeb C (2017) Cancellable iris template generation based on indexing-first-one hashing. *Pattern Recognit* 64:105–117
15. Maio D, Maltoni D, Cappelli R, Wayman JL, Jain AK (2002) FVC2002: second fingerprint verification competition. In: 16th international conference on pattern recognition, 2002. *Proceedings*, vol 3. IEEE, pp 811–814
16. Maltoni D, Maio D, Jain AK, Prabhakar S (2009) *Handbook of fingerprint recognition*, 2nd edn. Springer

17. Miura N, Nagasaka A, Miyatake T (2004) Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification. *Mach Vis Appl* 15(4):194–203
18. Miura N, Nagasaka A, Miyatake T (2007) Extraction of finger-vein patterns using maximum curvature points in image profiles. *IEICE Trans Inf Syst* 90(8):1185–1194
19. Paikin G, Tal A (2015) Solving multiple square jigsaw puzzles with missing pieces. In: *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp 4832–4839
20. Piciuccio E, Maiorana E, Kauba C, Uhl A, Campisi P (2016) Cancelable biometrics for finger vein recognition. In: *2016 First international workshop on sensing, processing and learning for intelligent machines (SPLINE)*. IEEE, pp 1–5
21. Ratha NK, Chikkerur S, Connell JH, Bolle RM (2007) Generating cancelable fingerprint templates. *IEEE Trans Pattern Anal Mach Intell* 29(4):561–572
22. Ratha NK, Connell J, Bolle R (2001) Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst J* 40(3):614–634
23. Sholomon D, David O, Netanyahu NS (2013) A genetic algorithm-based solver for very large jigsaw puzzles. In: *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp 1767–1774
24. Starck J-L, Fadili J, Murtagh F (2007) The undecimated wavelet decomposition and its reconstruction. *IEEE Trans Image Process* 16(2):297–309
25. Ton BT, Veldhuis RNJ (2013) A high quality finger vascular pattern dataset collected using a custom designed capturing device. In: *2013 International conference on biometrics (ICB)*. IEEE, pp 1–5
26. Uhl A (2019) State-of-the-art in vascular biometrics. In: Uhl A, Busch C, Marcel S, Veldhuis R (eds) *Handbook of vascular biometrics*. Springer Science+Business Media, Boston, MA, USA, pp 3–62
27. Wolberg G (1998) Image morphing: a survey. *Vis Comput* 14(8):360–372

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.