Finger-Vein Template Protection based on Alignment-Free Hashing

Simon Kirchgasser, Andreas Uhl
Department of Computer Sciences
University of Salzburg
{skirch, uhl}@cs.sbg.ac.at

Yen-Lung Lai, Jin Zhe
School of Information Technology
Monash University, Malaysia
{yenlung.lai, jin.zhe}@monash.edu

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 suboptimal in the one or other way. In this study we propose an alignment-free 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 IoM hashing to fulfil mandatory privacy and security based characteristics. The proposed method is compared to block-remapping and warping regarding recognition performance and is analysed with respect to security and privacy aspects.

1. 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 implies 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 fulfil four requirements as defined in ISO/IEC Standard 24745: 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 (cancelable biometrics - CB) and biometric cryptosystems (BCS) [22]. Another class of BTP schemes is discussed as an alternative for CB, Homomorphic Encryption (HE [29]). HE allows computations performed in the encrypted domain without using helper data and receiving the same comparison results as done in the decrypted domain, however, the computational cost is often prohibitive.

CB rely on the application of a transformation function to a biometric template or a biometric trait. 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 authentication of subjects can be done directly in the transformed domain.

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. Thus, the template comparison is done not 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 paper, we propose a CB scheme, namely Alignment-Free Hashing (AFH) 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 [13], insensitivity to skin condition changes and high security [14]). Second, there are no template protection schemes

978-1-7281-1522-1/19/$31.00 ©2019 IEEE

available originally designed for finger-vein biometrics which results in some problems regarding the application of adopted template protections methods as follows. Most finger-vein recognition systems relying on binary vascular patterns are using a correlation based strategy to compare provided templates. Shifting the templates against each other during template comparison is required to compensate e.g. displacement introduced during the image acquisition. Unfortunately, after applying template protection a 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 [21] or Indexing-First-One (IFO) hashing [15] (both are adoptable for finger-vein biometrics) suffer from alignment problems. As a consequence there are two strategies to overcome this problem: a) all shifted variations of a template must be stored during the enrolment (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 computational 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-free descriptor which is combined with IoM hashing [11] to fulfil the ISO/IEC Standard 24745 template protection requirements without an increase in template size or higher computational costs. The AFH-based method is analysed regarding recognition performance, security and privacy aspects. The analysis also includes a comparison to other non-invertible transformations, namely block re-mapping and warping, which have been used to protect finger-vein templates before [19].
The rest of this paper is organised as follows: In Section 2 a brief discussion about finger-vein biometrics is given before we provide a compact literature review on related BTP techniques in Section 3. Subsequently, the proposed template protection scheme is explained and the applied concepts are described in detail in Section 4. Section 5 illustrates the experimental set-up (including the used datasets) and the recognition performance results of the analysis. The experimental evaluation regarding non-invertibility and unlinkability is presented in Sections 6 and 7, respectively. Finally, Section 8 concludes this paper along with an outlook on future work.

2. Finger-Vein Biometrics

Finger-vein biometric based systems rely on the structure of vascular patterns which are formed by the blood vessels inside the human finger tissue. According to the fact that the blood vessels lie beneath the human skin it is necessary to use near-infrared (NIR) light based scanners to make the structure visible as dark lines on the resulting images which are 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. [26]. The system may contain an optional template protection module, applied either after the preprocessing module (image domain) or after the feature extraction module (feature domain). The proposed template protection scheme is applied in the feature domain.

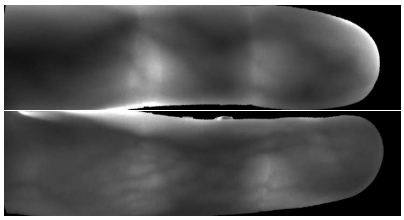


Figure 1: Two finger-vein images using palmar view.

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) [31], Circular Gabor Filter (CGF) [30] and CLAHE (local histogram equalisation). After the visibility was enhanced vein feature extraction methods are applied. We selected six techniques based on the binary vessel structure (however, there exist also minutiae-related extraction methods e.g. [3]). The extraction schemes are Gabor Filter (GF) [14], Isotropic Undecimated Wavelet Transform (IUWT) [23], Maximum Curvature (MC) [18], Principal Curvature (PC) [2], Repeated Line Tracking (RLT) [17], and Wide Line Detector (WLD) [10]. Further details regrading these methods are given in [12]. Example images of binary feature representations extracted by the before mentioned schemes are displayed in Figure 2. The BTP techniques discussed in this work are applied to these extracted features.

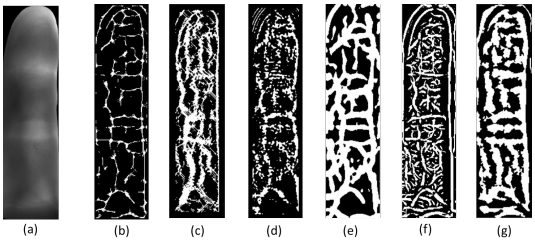


Figure 2: Features taken from an example finger-vein image: (a) Original FV image (b) MC, (c) RLT, (d) WLD, (e) PC, (f) GF and (g) IUWT.

3. Finger-Vein Template Protection

An analysis of two CB schemes was conducted by Piciucco et al. [19]. They applied block re-mapping and block based warping in the image domain, while all techniques described 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.

A direct application of BCS, i.e. a fuzzy Commitment Scheme (FCS), to binary finger vein data is demonstrated in [7]. In a similar approach, [4] also apply the FCS, but they tackle the issue of a bias in the binary data (as non-vein pixels are in clear majority as compared to vein pixels) by applying no vein detection but a simple thresholding scheme using the median. We find 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 schemes close to BioHashing is used employing random projections. The obtained coefficients are binarised and subjected to a fuzzy commitment scheme (FCS), which is a particular CBS approach based on helper data. This approach is used to secure medical data on a smartcard [28]. A second approach combining CB and BCS is suggested in [27], 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 [16], 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 suffer from the drawback that they are no fixed length representations (which is a prerequisite for the application of several template protection schemes) – techniques developed in the context of finger print minutiae-representations have been transferred to vein minutiae representations, i.e. vein minutiae cylinder-codes [9] and vein spectral minutiae representations [8]. The latter representations are subjected to binarisation and subsequently fed into Bloom filters to result in a CB scheme thereby avoiding position correction during template comparison as required by many techniques based on vascular structure representation [6].

A BCS approach based on quantisation is proposed in [25]: 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 quantisation-based key generation where the quantisation parameters (helper data) depend in the distribution of the generated stable features. Another quantisation-based BCS is proposed in [1], where vein intersection points are located by considering a neighbourhood connectivity criteria, after Gabor-based enhancement with subsequent thresholding. However, the generation of a stable key is not discussed as it is just suggested to use a subset of the identified feature points as key material.

4. An Alignment-Free 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. Thus, a proper alignment of the templates is a crucial step to obtain a suitable 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 shift has to be carried out in both vertical and horizontal directions due to the arbitrary placement of finger during image acquisition [17, 18]. The computationally costly comparison strategy leads to high computational load, especially for carrying out identification over a large database. This computational time 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-free property that also enables a faster template comparison as it is done by bit-by-bit shifting.

4.1. Alignment-Free Feature Descriptor

Let $d(i, j)$ be the local distance between the i-th and j-th locations in a binary vector $V = (v_1, , v_n)$ where

$v_i, v_j \in [0, 1]$. In particular:

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

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

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

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

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

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 utilise the local feature (e.g. local distance) to replace the prior alignment required by global features as used in other algorithms (e.g. [18]). Thus, the employment of local distance measures as invariant feature descriptor eliminates the requirement of alignment from finger-vein recognition.

4.2. Alignment-Free Hashing (AFH) and Template Comparison

In this section, we introduce our feature extraction scheme, the Alignment-Free Hashing (AFH), in detail. The proposed method is based on the feature descriptor described in Section 4.1. We extend AFH from 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 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 algorithmical five-step procedure described in Algorithm 1.

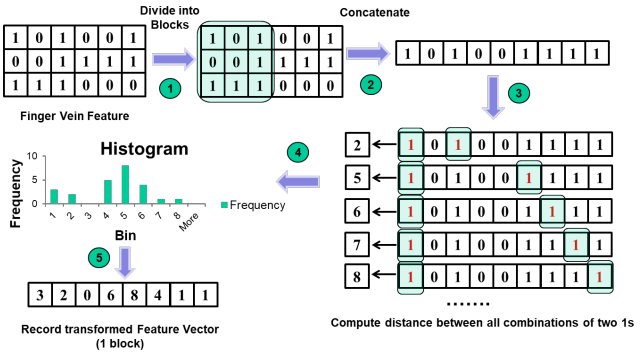


Figure 3: The overall flow of the AFH protection scheme.

Algorithm 1 Alignment-Free Hashing (AFH)

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

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:

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

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 $\binom{\min_{N_1,\ldots,N_b}}{2}$ number of combina-

tions representing collisions of 1's. However, according to the fact that 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. it is difficult to determine the value of $\min_{N_1,\ldots,N_b}$ precisely. However, AFH 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 [11] to achieve a full set of BTP requirements as defined in the Introduction. A detailed discussion regarding irreversibility is presented in Section 6.

4.3. IoM Hashing applied in AFH

IoM hashing, as introduced by Jin et al. in [11], 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 only with low probability.
The IoM hashing uses a feature vector (the extracted AFH template) $x \in \mathbb{R}^n$ and a n-dimensional Gaussian vector, $r \in \mathbb{R}^n$ as input argument. Thus, the IoM hashing operates as follows:

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 [11].
As we want to introduce revocability and unlinkability by adding IoM to the AFH, 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 [11], q has no significant influence on the recognition performance thus we have set $q = 2$ as suggested by [11].

5. Experimental Set-up and Performance Analysis

The experiments have been carried out using the PLUSVein-FV3 Dorsal-Palmar finger-vein database [13] and the University of Twente Finger Vascular Pattern Database (UTFVP) [24]. As PLUSVein-FV3 contains 4 subsets, Laser/LED DORSAL and Laser/LED PALMAR, we selected the latter subsets because the UTFVP database contains palmar images only. Thus, a direct comparison between the databases is possible. In the following we name the considered datasets UTFVP, PLUS LED and PLUS Laser.
After pre-processing the resulting binary features are used to perform the baseline experiments without applying template protection schemes. After the baseline experiments, the extracted templates are protected by the use of the proposed AFH method, and by block re-mapping and warping as a comparison. Note that the latter techniques are applied in the feature domain contrasting to [19]). Block re-mapping 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 higher amount of privacy protection as would be given by just permuting the blocks. Warping is based on deforming the vein patterns' structures contained in non-overlapping blocks using piece-wise linear interpolation. As block sizes $16, 32, 48$ 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 [19], thus we have selected them for the sake of comparability.
For AFH different equidistant m values in the range of $[20, 200]$ have been selected as key parameters. Furthermore, for the non-overlapped blocks formulation (as needed for Step 1 of the proposed algorithm), several block sizes are taken into account as well. We have selected $b_n \in 10, 20, 30$ and $b_m \in 20, 30, 40, 50, 60$. The recognition accuracy on the selected datasets is evaluated by using the equal error rate (EER).

5.1. Baseline Performance

Table 1 lists the performance results of the baseline experiments in percentage for the UTFVP and the PLUSVein-FV3 datasets, respectively. Overall, the performance on the UTFVP dataset is slightly superior compared to the PLUSVein-FV3 dataset for most of the evaluated recognition schemes.
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

	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

Table 1: Baseline performance in terms of EER. The best performing results are highlighted in bold numbers.

other schemes on both subsets. Nevertheless, each of the evaluated recognition schemes achieves a competitive performance on all of the tested datasets.

5.2. Recognition Performance applying Template Protection

Table 2 presents the EER by using the mean ($\bar{x}$) and the standard deviation (σ) for all datasets and applied template protection schemes. These results are calculated by randomly choosing 10 different keys (system-specific, i.e. identical keys for all users) as suggested by [5] to subsequently perform a suitable unlinkability analysis.

Due to the length of the paper 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. 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 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 AFH-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 it has to be mentioned that the observed results are a) similar for all other parameter configurations of block re-mapping and AFH and b) are strongly depending on the particular feature extraction method used and the selected dataset. Thus, the AFH-based method did not work well using WLD on the PLUSVein-FV3 data and further 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 only small, while a larger amount of displacement, e.g. longitudinal rotation as reported by [20], seems to be the reason for the performance issues concerning UTFVP.

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 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 AFH-based protected templates must be compared only once (by counting the number of collisions of 1's, which is extremely fast). As a consequence, the computational cost using AFH-based template protection is reduced to a high extent compared to the other template comparson methods.

6. Non-invertibility Analysis

First of all, the pair-wise local distance representation of AFH (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

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

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

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

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 subjected 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 to $E(\min N_1, N_2, \ldots, N_b) = 29$

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
AFH_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
	PLUS 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
AFH_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
	PLUS 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
AFH_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

Table 2: Recognition performance results (%). The best result for each feature extraction method is highlighted in bold numbers.

and $E(\max N_1, N_2, \ldots, N_b) = 234$, while $P_d = 0.0557$ is calculated by taking the normalised 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 maximise 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:

$$E(\binom{\min N_1, N_2, \ldots, N_b}{2} \times (1 - (P_d)^b)) \leq E(combinations) \leq E(\binom{\max N_1, N_2, \ldots, N_b}{2} \times (1 - (P_d)^b)) \quad (7)$$

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 bounding for the expected number of combinations representing collisions of 1's. The AFH-based transformation implicitly provides irreversibility by the argument of an expected guess complexity from 2^9 to 2^{15}, but the CB scheme only provides further requirements like revocability and unlinkability after the application of IoM hashing. The latter requirement is discussed in the following Section 7, while the property of revocability is fulfilled by the design of IoM hashing. As described in Section 4.3, 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).

7. Unlinkability Analysis

ISO/IEC Standard 24745 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 et al. [5] present a universal framework to evaluate the unlinkability of a biometric template protection system based on the comparison scores. They proposed the so called D_{sys} measurement as a global measure to evaluate a given biometric recognition and template protection system. The D_{sys} ranges normally from 0 to 1, where 0 represents the best achievable unlinkability score. We shifted the range from $[0, 1]$ to values in $[0, 100]$ to improve the readability of the results presented in Table 3. Furthermore, the authors of [5] 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 have also selected 10 different keys for our performance, see Section 5.2, and unlinkability analysis, respectively.

The D_{sys} values are shown for all three template protection schemes in Table 3. 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 property of unlinkability is exhibited by warp_16_6. From a security point of view warping is not really a proper template protection scheme using the given parameters.

Compared to the recognition performance, see Table

2, the unlinkability of our proposed AFH-based template protection technique, independently of the parameter selection, outperformed warping and is similar to the results obtained for block re-mapping, especially if compared to remp_16. Nevertheless, it also needs to be mentioned that AFH-based method's σ is much higher in several cases. 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 [5]). 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 [5]. The red coloured distribution correspond to the non-mated samples scores, which yielded by templates generated from samples of different instances using different keys. According to [5] 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. The presented distribution plots of Figure 4 show nearly full unlinkability in all cases as the D_{sys} values are close to 0. As a consequence, the distributions of mated and non-mated samples scores are highly overlapping.
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 the most cases as well. Thus, the proposed 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).

8. Conclusion

The proposed AFH-based template protection scheme shows a slightly lower recognition performance compared to warping, but exhibits a much better unlinkability. Bock re-mapping was outperformed in most cases regarding recognition performance and unlinkability as well. Another advantage of the proposed method are 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 AFH feature descriptor design implicitly ensures non-invertibility of the entire template protection system. The revocability requirement is fulfilled as well because a new template can be regenerated by using a different random Gaussian vector during the IoM hash code computation. Thus, the main requirements of a template protection scheme are achieved.
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. One possibility for future work includes the combination of warping and the proposed alignment-free hashing based template protection scheme to possibly maintain the recognition performance obtained by warping, while improving unlinkability at the same time.

9. Acknowledgements

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

References

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

[2] J. H. Choi, W. Song, T. Kim, S.-R. Lee, and H. C. Kim. Finger vein extraction using gradient normalization and principal curvature. volume 7251, pages 7251 – 7251 – 9, 2009.

[3] S.-J. Chuang. Vein recognition based on minutiae features in the dorsal venous network of the hand. Signal, Image and Video Processing, 12(3):573–581, 2018.

[4] M. Favre, S. Picard, J. Bringer, and H. Chabanne. Balancing is the key - performing finger vein template protection using fuzzy commitment. In ICISSP 2015 - Proceedings of the 1st International Conference on Information Systems Security and Privacy, ESEO, Angers, Loire Valley, France, 9-11 February, 2015., pages 304–311, 2015.

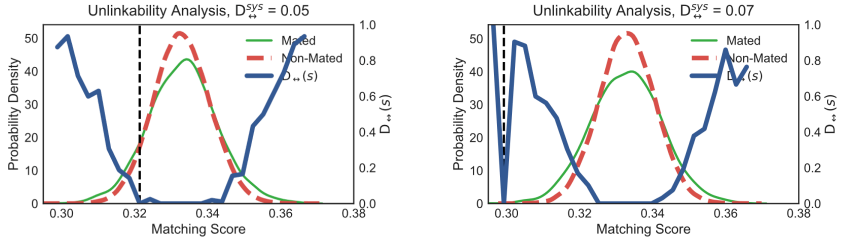
[5] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch. General framework to evaluate unlinkability in biometric template protection systems. IEEE Transactions on Information Forensics and Security, 13(6):1406–1420, 2018.

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

[7] D. Hartung and C. Busch. Why vein recognition needs privacy protection. In Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'09), pages 1090–1095, 2009.

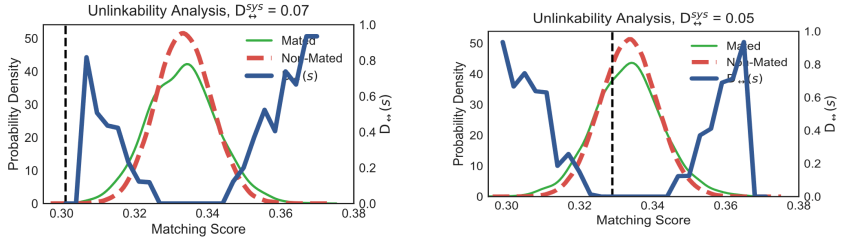
tempProt	Dsys											
	GF		IUWT		MC		PC		RLT		WLD	
	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ	$\bar{x}$	σ
	UTFVP											
remp_16	3.43	0.52	3.02	0.58	3.91	0.97	2.90	0.32	3.09	0.46	4.35	0.53
remp_64	25.67	18.69	20.03	21.95	29.72	22.93	20.81	22.36	16.32	19.89	27.24	22.93
warp_16_6	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_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
AFH_180_20_60	5.40	45.00	7.20	21.80	6.30	48.60	5.20	44.1	7.20	26.80	6.60	24.80
	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_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_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
AFH_180_20_60	6.10	13.10	7.40	46.60	7.10	24.80	7.20	51.80	6.30	21.60	6.61	24.40
	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_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_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
AFH_180_20_60	5.20	13.10	7.40	46.60	7.10	24.80	7.20	51.80	6.30	21.60	6.60	24.40

Table 3: D_{sys} unlinkability scores for block re-mapping and warping. The best results (low values, representing unlinkability) for each template protection method are highlighted in bold numbers.



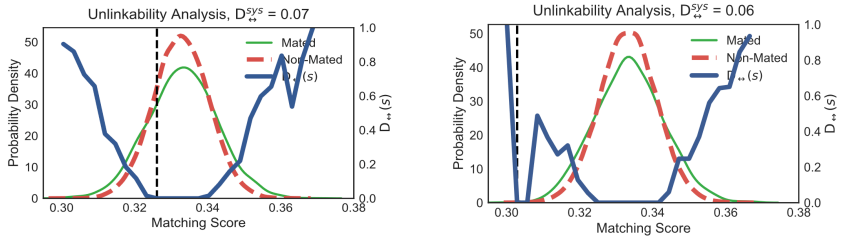
(a) UTFVP + GF

(b) PLUS LED + IUWT



(c) PLUS Laser + MC

(d) PLUS Laser + PC



(e) UTFVP + RLT

(f) PLUS LED + WLD

Figure 4: Example images which display unlinkability trend using AFH-based scheme.

[8] D. Hartung, M. A. Olsen, H. Xu, H. T. Nguyen, and C. Busch. Comprehensive analysis of spectral minutiae for vein pattern recognition. IET Biometrics, 1(1):25–36, 2012.

[9] D. Hartung, M. Tistarelli, and C. Busch. Vein minutia cylinder-codes (V-MCC). In International Conference on Biometrics, ICB 2013, 4-7 June, 2013, Madrid, Spain, pages 1–7, 2013.

[10] B. Huang, Y. Dai, R. Li, D. Tang, and W. Li. Finger-vein authentication based on wide line detec-

tor and pattern normalization. In Pattern Recognition (ICPR), 2010 20th International Conference on, pages 1269–1272. IEEE, 2010.

[11] 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 Transactions on Information Forensics and Security, 13(2):393–407, 2018.

[12] C. Kauba, E. Piciucco, E. Maiorana, P. Campisi, and A. Uhl. Advanced variants of feature level fusion for finger vein recognition. In Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG'16), pages 1–12, Darmstadt, Germany, 2016.

[13] 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 Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG'18), pages 1–8, Darmstadt, Germany, 2018.

[14] A. Kumar and Y. Zhou. Human identification using finger images. IEEE Transactions on Image Processing, 21(4):2228–2244, 2012.

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

[16] Y. Liu, J. Ling, Z. Liu, J. Shen, and C. Gao. Finger vein secure biometric template generation based on deep learning. Soft Comput., 22(7):2257–2265, 2018.

[17] N. Miura, A. Nagasaka, and T. Miyatake. Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification. Machine vision and applications, 15(4):194–203, 2004.

[18] N. Miura, A. Nagasaka, and T. Miyatake. Extraction of finger-vein patterns using maximum curvature points in image profiles. IEICE TRANSACTIONS on Information and Systems, 90(8):1185–1194, 2007.

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

[20] B. Prommegger, C. Kauba, M. Linortner, and A. Uhl. Longitudinal finger rotation - deformation detection and correction. IEEE Transactions on Biometrics, Behavior, and Identity Science, pages 1–17, 2019.

[21] C. Rathgeb, F. Breitinger, and C. Busch. Alignment-free cancelable iris biometric templates based on adaptive bloom filters. In Biometrics (ICB), 2013 International Conference on, pages 1–8. IEEE, 2013.

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

[23] J.-L. Starck, J. Fadili, and F. Murtagh. The undecimated wavelet decomposition and its reconstruction. IEEE Transactions on Image Processing, 16(2):297–309, 2007.

[24] B. T. Ton and R. N. Veldhuis. A high quality finger vascular pattern dataset collected using a custom designed capturing device. In Biometrics (ICB), 2013 International Conference on, pages 1–5. IEEE, 2013.

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

[26] L. Yang, G. Yang, Y. Yin, and L. Zhou. A survey of finger vein recognition. In Chinese Conference on Biometric Recognition, pages 234–243. Springer, 2014.

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

[28] W. Yang, S. Wang, J. Hu, Z. Guanglou, J. Chaudhry, E. Adi, and C. Valli. Securing mobile healthcare data: A smart card based cancelable finger-vein bio-cryptosystem. IEEE Access, 06:36939 – 36947, 2018.

[29] S. Ye, Y. Luo, J. Zhao, and S.-C. S. Cheung. Anonymous biometric access control. EURASIP Journal on Information Security, 2009:2, 2009.

[30] J. Zhang and J. Yang. Finger-vein image enhancement based on combination of gray-level grouping and circular gabor filter. In Information Engineering and Computer Science, 2009. ICIECS 2009. International Conference on, pages 1–4. IEEE, 2009.

[31] J. Zhao, H. Tian, W. Xu, and X. Li. A new approach to hand vein image enhancement. In Intelligent Computation Technology and Automation, 2009. ICICTA'09. Second International Conference on, volume 1, pages 499–501. IEEE, 2009.