A template privacy protection scheme for fingerprint minutiae descriptors

Leila Mirmohamadsadeghi and Andrzej Drygajlo

leila.mirmohamadsadeghi@epfl.ch, andrzej.drygajlo@epfl.ch

Abstract: It is important in biometric person recognition systems to protect personal data and privacy of users. This paper introduces a new mechanism to revoke and protect fingerprint minutiae information, which can be used in today's security-aware society. The recently developed minutiae cylinder code (MCC), which provides rotation and translation invariant descriptors for accurate fingerprint recognition by describing minutiae neighborhoods with respect to each other, is used as baseline fingerprint descriptor. A hybrid scheme combining a transformation and a user key is designed to provide the MCC-based fingerprint representation with revocability and irreversibility properties for template privacy protection across multiple applications. Furthermore, using the publicly available FVC datasets, it is demonstrated that the designed scheme improves the baseline accuracy of fingerprint recognition using the MCC method.

1 Introduction

Biometric template privacy protection is gaining importance with the widespread use of biometric person recognition and an increase in the awareness on related privacy issues. Biometric template privacy protection should ensure that an individual's biometric characteristic is only available in the form of a template which is diverse and thus revocable if the template is compromised. Furthermore, the template must be irreversible to the original capture and must preserve the accuracy of the underlying recognition system [JNN08].

In the past decade, researchers have proposed various template protection solutions for different biometric modalities. Template protection techniques can be grouped into two categories: 1) Feature transformation, which is divided into two sub-categories of a) reversible and b) irreversible transformations; 2) Biometric cryptosystems which are categorized into a) key binding systems and b) key generation systems [JRN11]. Feature transformation methods apply a transformation function to the biometric representations, both during enrollment and verification. Comparison is performed in the transformed domain. Examples of these methods include the irreversible transformation [RCCB07] and the biohashing salting methods [TLG04]. Biometric cryptosystems use a biometric characteristic to create a concealing combination of the trait with a cryptographic key or to generate a cryptographic key from the characteristic. Fuzzy commitment [TAK$^+$05] and fuzzy vaults [JS02] are pioneering examples of key binding systems and fuzzy extractors are examples of key generating systems [DRS04]. Hybrid schemes not belonging to any group, have been investigated as well [BSW07].

In the particular case of the fingerprint modality, several approaches have been proposed for various representations such as minutiae, ridge information, texture, etc. The minu-

tiae representation is of interest in this paper because of its standardization [ISO05] and widespread real-world usage [MMJP09]. In one existing template protection scheme, powers of minutiae coordinates are combined into a hash [TFMG07]. In another, minutiae triplet characteristics are randomized through binning and permutation [FBTYR07]. Binning and binarization of minutiae pair characteristics has been proposed as well [ZTTT10]. Another approach consists of quantizing the coordinates of a set of aligned minutiae [YBBG10]. Minutiae vicinities, which self align, are proposed as well in combination with a random offset to achieve revocability [YHSB10]. These vicinities are found to be more robust when decomposed into invariant triplet features, and added a random offset [ZT11]. Another approach applied to minutiae pairs is the Biotope^{TM}approach, which consists of breaking the datum into an invariant part, which is encrypted, and a varying part, which is left to support approximate matching [BSW07]. A different method consists of encoding the spatial distribution of minutiae with respect to a reference minutia and to apply a permutation based on a user key [LK10]. Revocability is obtained by changing the reference minutia. Another mapping scheme involves a pair-polar transformation including a radial random user key [AHW11]. A different mapping consists of transforming the minutiae in a polar manner with respect to every minutia as reference and quantizing minutiae attributes to create a bit-string which is then permuted with a user-specific token [ZTTT11]. This scheme is referred to as polar grid based 3-tuple quantization (PGTQ). Exploiting the Delaunay triangulation of minutiae in combination with a fuzzy extractor is also explored [YHW12]. Recently, a specific scheme was designed to provide irreversibility for the minutiae cylinder code (MCC) representation, which involves the quantization of the Karhunen-Loeve transform [FMC12]. However, this scheme is not designed to provide diversity and revocability. Another approach for protecting minutiae maps binarized histograms of minutiae pair attributes in a many-to-one manner using a randomly generated matrix in order to provide irreversibility and revocability [WH12]. This scheme is referred to as the densely infinite-to-one mapping (DITOM). A minimum distance graph (MDG) scheme is also recently proposed to use distances to the core point as invariant features in a fingerprint hash [DKG12].

In the present paper, a novel method is proposed to provide template privacy protection for the minutiae cylinder code (MCC) representation [CFM10], which provides diversity, revocability and irreversibility properties, without degrading the baseline recognition accuracy. Fingerprint recognition using the MCC representation is chosen because it is alignment-free and computationally light.

The remainder of this paper is organized as follows. In Section 2, a brief description of the baseline fingerprint recognition system is provided. In Section 3, the proposed privacy protection scheme is presented. Experiments to assess performance of the protection scheme in terms of accuracy are depicted in Section 4, while security aspects are addressed in Section 4.2. Conclusions are drawn in Section 5.

2 Fingerprint minutiae descriptors based on the minutiae cylinder code (MCC)

The minutiae cylinder code (MCC) [CFM10] is a recent fingerprint description method, which presents the advantages of both nearest-neighbor-based and fixed-radius-based minu-

tiae description methods and is considered as the state-of-the-art in minutiae descriptor design [FZ11].
This method takes as input a set of standard ISO minutiae [ISO05], and creates for each minutia, a descriptor based on its distance to neighboring minutiae and their angular differences. This descriptor is of fixed length, robust to rotations and translations and skin distortions and is computed in a fast manner. The output consists of a template, which contains a descriptor for each minutia. This descriptor is a linearized cylinder whose discretized volume represents weighted spatial and angular distances of each minutiae to its neighbors. In order to compare two such templates within a recognition system, several comparison measures were originally introduced. In this paper, the local similarity sort (LSS) method is chosen among the others because it requires the least extra information about the original minutiae set when performing cylinder set comparison. The LSS comparison method computes all two by two distances of the cylinders and provides a similarity score based on the closest cylinder matches and angular distances of minutiae pairs.
A slightly different version of the MCC method is used in this work. With respect to the original method, cylinder and cell validities are not considered and the weighting functions used to compute the spatial and angular contributions of neighboring minutiae are discretized.

3 A privacy protection scheme for the MCC templates

According to template privacy protection requirements, it is desirable to create from a raw biometric sample, several diverse and revocable templates which are irreversible to the original biometric characteristic and support accurate recognition. The baseline accuracy corresponds to recognition without template protection. It is thus required that template protection does not degrade this accuracy. Revocability is achieved when including a revocable component into the template, as original biometric characteristics are not revocable. Therefore, the privacy protection scheme presented in this paper is a hybrid two-factor scheme which transforms the template with a user key in a revocable and non-reversible manner. The key is assumed secret in the baseline protected system, but it is shown that even if the key is compromised or lost, the original biometric characteristic remains protected. The proposed solution takes root from cryptographic primitives such as the hard problem of square root modulo a composite number [HPS08]. During the modulo operation the quotient is dismissed, it is impossible to reconstruct accurately the original value. Also, as in filtering techniques, e.g., mean filtering, where the underlying operation replaces one value by a value inferred from several original values, the output is more homogeneous with respect to the input and removes small variations such as noise. For this reason, the transformation presented here includes a step in which two original values are added to each other. The reduced intra-class variations are a positive step in working with biometric data, which suffer from inherent variations.
The output of the MCC descriptor creation is a template T for every fingerprint, which contains a fixed length descriptor, referred to as cylinder TC, for each minutia. In order to dismantle the original structure of the cylinders, two-by-two elements are summed based on a user key, which is a permutation of the cylinder indexes. The remainder of the division of the square of this sum by a given parameter is then considered as a new revocable

value as summarized in Equation 1. A binarization step is performed on the transformed values to introduce irreversibilty and quantization, which is necessary in presence of the intrinsic intra-class variations of biometric data. Because of the small values of the baseline MCC template, a multiplication factor A is used to adapt the size of the argument. A user key k, which is a random permutation of the cylinder indexes, is employed to specify the order of the summations of two-by-two elements. Changing this key ensures that it is possible to create several diverse instances of one biometric characteristic and allows to implement revocability through key managment. The revocable template, which is the output of the method presented in this paper, is denoted by RT and its cylinders as $RTCs$. The parameters of the protection operation include the multiplication factor A, the user key k and the divisor n.

$$\begin{aligned} &RTC[i] = B((A(TC[k(2i-1)] + TC[k(2i)]))^2 \mod n) \\ &\text{for } i = 1, ..., nb_{elements}(TC)/2, \text{ and } \forall TC \in T, \end{aligned} \tag{1}$$

where $B(v)$ binarizes each element of the descriptor by means of a threshold:

$$B(v) = \begin{cases} 1, & \text{if } v > t \\ 0, & \text{if } v \leq t. \end{cases} \tag{2}$$

The values of A and n must be in accordance with each other in order for the modulo operation to be meaningful and although they are presented as two different parameters, they are dependent on each other. It is observed that $max(TC[k(i)] + TC[k(i+1)]) = 2$, because the output of the MCC method yields descriptors whose values are normalized between 0 and 1. In order for the modulo operation to yield meaningful results, A and n must be chosen such that $n < (2A)^2$. Furthermore, if the argument (i.e., $(2A)^2$) is very large compared to the divisor n, the discriminatory power of the biometric information is lost. Empirically, it is observed that the argument must not be more than three orders of magnitude larger than the divisor, i.e., $n < (2A)^2 < 10^3 n$. The threshold t is determined based on the values of the transformed descriptors (which in turn depend on A and n) and is empirically fine-tuned.

Given that the same transformation is applied on every cylinder in the template, it is possible to use the original LSS comparison measure of the MCC method [CFM10] . The LSS matching is based on computing the Euclidean distance of two by two cylinders. Given that by using the same key, the elements of the cylinders are shuffled in the same manner, their element by element distance does not vary. Due to the properties of Euclidean spaces and the nature of the transformation in Equation 1, a correlation exists between the distance of two descriptors before and after the transformation. This correlation is later observed in the obtained results.

The transformation presented in this article, is evaluated in three aspects: accuracy, revocability and irreversibility. The accuracy of the recognition system with the transformation must not be lower than that of the recognition system without the transformation. It must be possible to generate several instances of one MCC template which are unlinkable and thus diverse and revocable. Finally, it must not be possible to accurately derive the original biometric trait from the transformed template, even when all parameters are known.

In this case, it must not be possible to re-create the MCC descriptor, and thus the minutiae information from a transformed template.

4 Experiments, performance results and discussion

In order to evaluate the proposed privacy protection scheme, the public and widely used FVC2002 [MMC+02] and 2004 [MMC+04] databases are used, which contain each, 8 impressions from 100 fingers. The minutiae of every fingerprint, formatted according to the ISO standard [ISO05], are extracted using the open source FingerJetFX$_{\text{OSE}}$ software by DigitalPersona [dig].
The original FVC protocol is used to generate genuine and impostor scores. Each template is compared against the remaining templates of the same finger to generate genuine scores and the first template of each finger is compared with the first template of all other fingers to generate impostor scores.
The MCC algorithm is implemented according to Section 2 and is hereafter referred to as the "baseline MCC". The MCC double-valued cylinder creation and matching parameters are $n_s = 16$, $n_d = 8$, $R = 75$, $\sigma_s = 6$, $\mu_\psi = 0.005$, $\sigma_D = 0.4363$, $min_{VC} = 20$, $min_M = 1$, $min_{ME} = 20\%$, $min_{n_p} = 3$, $max_{n_p} = 10$, $\mu_P = 10$, $\tau_P = 0.4$ and $\Delta\Theta = 2.35$. The size of each descriptor in the template using these parameters is 2048 elements. The minutiae extractor is modified to allow template creation for images with any number of minutiae.

4.1 Accuracy of the transformed templates

In order to assess accuracy changes after applying the template privacy protection method introduced in this paper, the genuine and impostor distributions are displayed in Figure 1 for the two cases of recognition using the baseline MCC templates and recognition using the protected MCC templates on the FVC2002 DB1 in the case where each identity is assigned a different key. On the corresponding detection error trade-off (DET) curves in Figure 2, it can be observed that recognition using protected MCC templates yields better overall separation and lower false accept rates (FAR) and false rejection rates (FRR) than recognition using the baseline MCC templates. Consequently, the equal error rate (EER) (the operating point at which FAR = FRR) is lowered as well. Corresponding error rates are reported in Table 1 for three operating points (EER point, the 1% FAR point and the 0.1% FAR point), as well as genuine/impostor class separation computed using the characteristics of Gaussian curves fitted to the actual distributions [MR05]. The EERs for the FVC2002 and 2004 databases (unseen data) are reported in Table 3. The parameters A and n (Equation 1) are set to 5×10^3 and 10^6 respectively in order for the modulo operation to be meaningful while preserving the discriminatory power of the biometric information. Furthermore, in order to verify the validity of the conditions given for the values of A and n with respect to each other, several combinations were empirically chosen and tested. It must be noted that for variations smaller than an order of magnitude in the values of A and n, the performance results vary marginally and in a negligible way with respect to the size of the databases used in this study. It can be observed that if A is too large compared to n, the recognition results are considerably lowered, which means that too much discriminative information is lost. Cases where A is too small compared to n are not

considered, as the modulo operation becomes meaningless in these ranges. The threshold t is set to 10^5. However, this value is not optimal and other values within the range of n are empirically tested in Table 2.

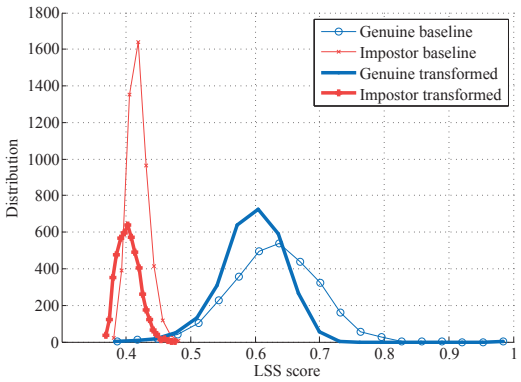

Figure 1: Genuine and impostor distributions for the cases of recognition using the baseline MCC templates and the transformed MCC templates. FVC2002 DB1 images.

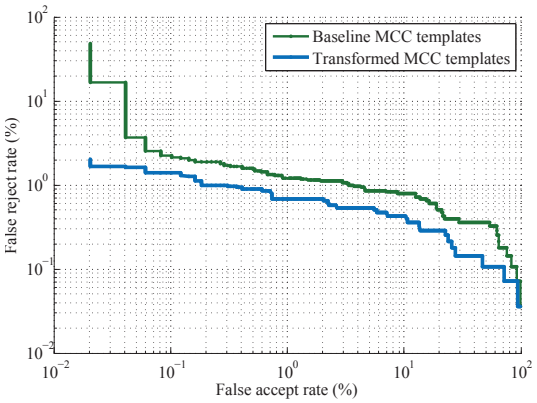

Figure 2: DET curves for recognition using the baseline MCC templates and the transformed MCC templates. FVC2002 DB1 images.

Although the values of the template as well as the chosen transformation parameters A and n are too small to qualify in the typical hard problem in cryptography of finding a square root modulo a composite, it can be observed that results of applying the transformation in Equation 1 are quite interesting with respect to the particular issues of template protection. From the results presented in Figures 1 and 2, it can be concluded that the protection scheme presented in this paper improves the overall verification performance. This observation is made through the lowered error rates as well as an increased genuine/impostor class separation. This phenomenon is explained by the two-factor authentication. The user key provides extra discriminative information to the templates. It must be noted that experiments further in this paper (Section 4.2) show that by setting all keys to one unique and

Method	EER	FRR@FAR 1%	FRR@FAR 0.1%	Class separation
Baseline MCC	1.21%	1.21%	2.25%	0.89
Protected MCC	0.72%	0.67%	1.39%	1.43

Table 1: Recognition results. FVC2002 DB1 images.

Threshold t	10^5	2×10^5	4×10^5	6×10^5	8×10^5
EER	0.72%	0.65%	0.49%	0.28%	0.36%

Table 2: Recognition results for different values of the binarization threshold t. FVC2002 DB1 images.

universal key, it is the biometric information being recognized and not the key. Another positive aspect of this privacy protection scheme is that the transformation reduces the size of the template by half. This property is beneficial when considering large databases as well as applications with reduced resources such as smart cards.
The proposed method is presented along side other state-of-the-art methods in fingerprint minutiae template protection with published results in Table 4. It must be noted that a fair comparison is near impossible since not all methods use the same data and the same testing protocol. Methods such as presented in [YBBG10, ZTTT10] use several enrollment samples. Methods such as in [ZT11] explicitly do not use the FVC testing protocol. Furthermore, different minutiae extractors are used by different researchers which may introduce non-negligible differences in the final performance absolute values. It is important to avoid binary comparisons and instead, to consider various methods with respect to each other based on both their positive and negative aspects with respect to a particular application.

4.2 Diversity and revocability of transformed templates

In targeted working conditions of the biometric recognition system, where the protection scheme is implemented and working in its normal mode, each user has his own key. This key is first used to enroll (enr) his template in the database and is later reused to reproduce the transformation during verification (ver). The operating point decision thresholds are determined in this scenario, which is referred to as *same key enr/ver*.
If a template is revoked, the corresponding key is black-listed and a new template is generated using a different key. The two templates must be different in order for the old template to be nullified. This scenario is referred to as *different key enr/ver* and corresponds to the case where a user needs several different instances of his biometric for use in different applications. Given that the original template consists of descriptors with $m = nb_{elements}(TC)$ elements ($m = 2048$ in this paper), $m!$ different keys can be generated. However, since the two elements of TC specified by k are added to each other before undergoing any other operations, the order of the elements does not matter. For example, if $nb_{elements}(TC) = 8$, then keys $k_1 = 37814256$ and $k_2 = 73814256$ yield the same protected template. They are equivalent to all other keys which have the same indices in the consecutive odd and even positions, regardless of the order of the indices within the

	FVC2002				FVC2004			
	DB1	DB2	DB3	DB4	DB1	DB2	DB3	DB4
Baseline MCC	1.21%	1.15%	6.45%	5.35%	6.19%	10.06%	7.00%	7.96%
Protected MCC	0.72%	0.42%	3.84%	1.39%	1.95%	6.78%	1.35%	2.36%

Table 3: Recognition results for the FVC 2002 and 2004 databases.

pair. A "pair" here refers to an odd and even position in the key, for example $k[1]$ and $k[2]$ are a pair, as well as $k[3]$ and $k[4]$. If k has m elements, then there are $\frac{m}{2}$ pairs. There are $2^{m/2}$ possible permutations within the pairs since every pair has two permutations. The $2^{m/2}$ permutations yield equivalent keys as only the position within a pair varies from one key to another, not affecting the outcome of the transformation. These $2^{m/2}$ keys are a category of equivalent keys. Therefore in order to compute the number of distinct keys (which yield different protected templates through the transformation), the total number of permutations must be divided by the number of categories of equivalent keys, which results in $\frac{m!}{2^{m/2}}$ different keys. In order to ensure two diverse templates of one person are not similar, the pseudo-impostor accept rate (PIAR) is introduced to evaluate the proportion of successful pseudo-impostor attempts. A pseudo-impostor comparison is the comparison of two templates of one individual, which are generated using two distinct keys. It can be seen in Table 5 and Figure 3, that it is difficult to use a template generated with the wrong key for positive verification. If a user loses his key, it is known by an adversary. This scenario is simulated by using the same key for enrollment and verification, for all users, and is referred to as the *stolen-token* scenario. Furthermore, this scenario shows that it is the biometric information being verified, and not the key. These diversity and security testing scenarios are implemented according to [WH12].

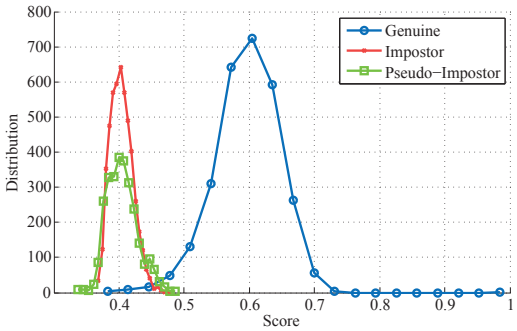

Figure 3: Genuine, impostor and pseudo-impostor distributions (in the *different key enr./ver.* scenario to evaluate diversity). FVC2002 DB1 images.

It can be concluded from the observations in Table 5, that it is possible to define an operating point for the privacy protection scheme presented in this paper, such that, a very limited number of impostors (and pseudo-impostors) gain access to the system with an unauthorized key. It must be noted that the security of this scheme is dependent on the decision threshold and offers flexibility in various operational scenarios.

Scheme	EER	Database	+	-
biotope [BSW07]	2.9%	FVC2000 DB1, 2; FVC2002 DB1, 2; FVC2004 DB1, 2	no alignment, revocable, no decrease in performance	security depends on encryption (secrecy of key)
minutiae hash [TFMG07]	3%	FVC2002 DB1	no alignment, revocable	secrecy of key needed, decrease in performance
triangulation, binning and randomization [FBTYR07]	0	1000 fingerprints, 2 samples	revocable	security based on crypto. encryption or hash
pairs, binning and randomization [ZTTT10]	0	FVC2004 DB1	revocable	5 samples/ enr.; pseudo-irreversible, security depends on secrecy of the key
robust minutiae hash [YBBG10]	2.23%	FVC2002 DB2	revocable	2 samples/ enr.
minutiae vicinity [YHSB10]	2.6%	FVC2002 DB2	revocable, public parameters	alignment, dependence of template size on security
mapping and permutation [LK10]	0	FVC2004 DB1, 2, 3	no alignment	pseudo-irreversible, limited instances
minutiae vicinity decomposition [ZT11]	0	FVC2002 DB2	no alignment	2 out of 8 samples removed from dataset, pseudo-irreversible
delaunay triangulation and fuzzy extractor [YHW12]	13%	FVC2002 DB2	no alignment	not revocable
pair-polar mapping [AHW11]	6% (stolen token)	FVC2002 DB1, 2, 3	no alignment, revocable	decreases baseline performance
irreversible MCC [FMC12]	0	FVC2002 DB1,2,3,4; FVC2006 DB2	no alignment	not revocable
DITOM [WH12]	3.5% (stolen token)	FVC2002 DB1, 2, 3 (2 images per finger)	no alignment, revocable	decreases baseline performance
PGTQ [ZTTT11]	1.19% (stolen token)	FVC2002 DB1, 2	revocable	unproven security
MDG [DKG12]	4% (stolen token)	FVC2002 DB1, 2	no alignment, revocable	core point detection
Method proposed in this paper	0.28%	FVC2002 DB1, 2, 3, 4; FVC2004 DB1, 2, 3, 4	no alignment, no decrease in performance, reduced (fix) template size	decrease in performance when key is public

Table 4: Comparison of state-of-the-art fingerprint minutiae template protection schemes.

Threshold	*same key enr./ver.*		*different key enr./ver.*		*stolen token*	
	FAR	FRR	FAR	PIAR	FAR	FRR
0.4489	1%	0.67%	1.03%	5.1%	41.57%	0.75%
0.4518	0.72%	0.72%	0.66%	3.32%	35.91%	0.78%
0.4673	0.1%	1.39%	0.06%	0.57%	13.37%	1.2%
0.4710	0.04%	1.6%	0.06%	0.46%	0.24%	2.53%
0.4934	0	2.71%	0	0	1.01%	2.82%

Table 5: Error rates at different operating points under different diversity and security assumptions. FVC2002 DB1 images.

4.3 Irreversibility of the transformed templates

In order to effectively protect a person's biometric characteristic, it must not be possible to deduce said characteristic from the transformed template, even when all parameters, including the key, are known. In the transformation presented in this paper, non-reversibility is provided by the fact that during the transformation in Equation 1, part of the data is discarded through the modulo and quantization, which does not allow exact reconstruction even if all parameters are known. However, it is possible to create an approximation of a binary MCC template given a transformed template and the corresponding key as described in Equation 3:

$$
\begin{aligned}
TC_R[k(2i)] &= \begin{cases} 1, & \text{if } RTC[i] = 1 \\ 0, & \text{otherwise and} \end{cases} \\
TC_R[k(2i+1)] &= \begin{cases} 1, & \text{if } RTC[i] = 1 \\ 0, & \text{otherwise.} \end{cases} \\
i = 1, ..., nb_{elements}(RTC), \quad & and \quad \forall RTC \in RT.
\end{aligned} \tag{3}
$$

TC_R denotes the approximated MCC templates and is compared to the baseline binary MCC template, for all users of a database in Figure 4. It can be seen and concluded that these approximated templates do not resemble the baseline MCC templates and thus cannot be systematically used to extract useful minutiae information. In fact, when compared with genuine templates, the reconstructed templates are similar to impostor templates.

5 Conclusions and Future Work

In this paper, a novel template privacy protection technique for the MCC representation of fingerprint minutiae templates was presented. The proposed hybrid, two-factor technique combining a transformation and a user key, provides diversity, revocability, and irreversibility for the MCC descriptors with respect to the original minutiae information while improving the accuracy in recognition. Furthermore, the proposed technique reduces the template size by half.

Future work will include study and modification of the transformation in order to extend of the ideas presented in this paper to other modalities than fingerprints.

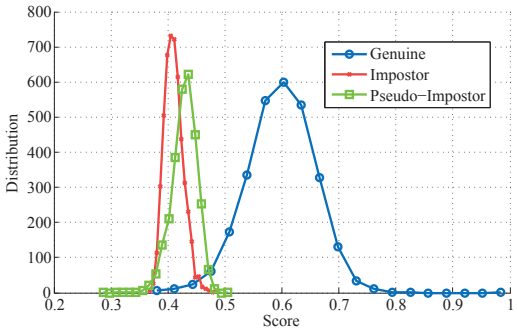

Figure 4: Genuine, impostor and pseudo-impostor distributions (approximated MCC templates to evaluate non-reversibility). FVC2002 DB1 images.

References

[AHW11] T. Ahmad, J. Hu, and S. Wang. Pair-polar coordinate-based cancelable fingerprint templates. *Pattern Recognition*, 44(10-11):2555–2564, 2011.

[BSW07] T. E. Boult, W. J. Scheirer, and R. Woodworth. Revocable fingerprint biotokens: accuracy and security analysis. In *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 1–8, 2007.

[CFM10] R. Cappelli, M. Ferrara, and D. Maltoni. Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32:2128– 2141, 2010.

[dig] digitalPersona. FingerJetFXOSE Fingerprint Feature Extractor, Open Source Edition, http://www.digitalpersona.com/fingerjetfx.

[DKG12] P. Das, K. Karthik, and B. C. Garai. A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs. *Pattern Recognition*, 45(9):3373–3388, 2012.

[DRS04] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In *Advances in Cryptology - EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 523–540. Springer Berlin / Heidelberg, 2004.

[FBTYR07] F. Farooq, R.M. Bolle, J. Tsai-Yang, and N. Ratha. Anonymous and Revocable Fingerprint Recognition. In *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 1–7, 2007.

[FMC12] M. Ferrara, D. Maltoni, and R. Cappelli. Non-invertible Minutia Cylinder-Code Representation. *IEEE Transactions on Information Forensics and Security*, 7(6):1727 –1737, 2012.

[FZ11] J. Feng and J. Zhou. A Performance Evaluation of Fingerprint Minutia Descriptors. In *International Conference on Hand-Based Biometrics (ICHB)*, 2011.

[HPS08] J. Hoffstein, J. Pipher, and J. H. Silverman. Chapter 2: Discrete Logarithms and Diffie-Hellman. In *An Introduction to Mathematical Cryptography*, page 86. Springer, 2008.

[ISO05] ISO/IEC 19794-2:2005. *Information Technology– Biometric Data Interchange Formats– Part 2: Fingerprint Minutiae Data*. 2005.

[JNN08] A. K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP Journal of Advanced Signal Processing*, pages 1–17, 2008.

[JRN11] A. K. Jain, A. Ross, and K. Nandakumar. Security of Biometric Systems. In *Introduction to Biometrics*, pages 259–306. Springer, 2011.

[JS02] A. Juels and M. Sudan. A fuzzy vault scheme. In *IEEE International Symposium on Information Theory*, page 408, 2002.

[LK10] C. Lee and J. Kim. Cancelable fingerprint templates using minutiae-based bit-strings. *Journal of Network and Computer Applications*, 33(3):236–246, 2010.

[MMC+02] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, and A.K. Jain. FVC2002: Second Fingerprint Verification Competition. In *16th International Conference on Pattern Recognition*, volume 3, 2002.

[MMC+04] D. Maio, D. Maltoni, R. Cappelli, J. Wayman, and A. Jain. FVC2004: Third Fingerprint Verification Competition. In D. Zhang and A. Jain, editors, *Biometric Authentication*, volume 3072 of *LNCS*, pages 31–35. Springer Berlin / Heidelberg, 2004.

[MMJP09] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition*. Springer, 2nd edition, 2009.

[MR05] G. L. Marcialis and F. Roli. Fusion of multiple fingerprint matchers by single-layer perceptron with class-separation loss function. *Pattern Recognition Letters*, 26(12):1830 – 1839, 2005.

[RCCB07] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle. Generating Cancelable Fingerprint Templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):561–572, 2007.

[TAK+05] P. Tuyls, A. Akkermans, T. Kevenaar, G. J. Schrijen, A. Bazen, and R. Veldhuis. Practical Biometric Authentication with Template Protection. In *Audio- and Video-Based Biometric Person Authentication*, volume 3546 of *LNCS*, pages 1–53. Springer Berlin / Heidelberg, 2005.

[TFMG07] S. Tulyakov, F. Farooq, P. Mansukhani, and V. Govindaraju. Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recognition Letters*, 28(16):2427–2436, 2007.

[TLG04] A. B. J. Teoh, D. N. C. Ling, and A. Goh. BioHashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, 37(11):2245–2255, 2004.

[WH12] S. Wang and J. Hu. Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach. *Pattern Recognition*, 45(12):4129–4137, 2012.

[YBBG10] B. Yang, C. Busch, P. Bours, and D. Gafurov. Robust minutiae hash for fingerprint template protection. volume 7541, page 75410R. SPIE, 2010.

[YHSB10] B. Yang, D. Hartung, K. Simoens, and C. Busch. Dynamic random projection for biometric template protection. In *4th IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS)*, pages 1–7, 2010.

[YHW12] W. Yang, J. Hu, and S. Wang. A Delaunay Triangle-Based Fuzzy Extractor for Fingerprint Authentication. In *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 66–70, 2012.

[ZT11] J. Zhe and A. B. J. Teoh. Fingerprint template protection with Minutia Vicinity Decomposition. In *International Joint Conference on Biometrics (IJCB)*, pages 1–7, 2011.

[ZTTT10] J. Zhe, A. B. J. Teoh, S. O. Thian, and C. Tee. Generating revocable fingerprint template using minutiae pair representation. In *2nd International Conference on Education Technology and Computer (ICETC)*, volume 5, pages 251–255, 2010.

[ZTTT11] J. Zhe, S. O. Thian, C. Tee, and A. B. J. Teoh. Generating revocable fingerprint template using polar grid based 3-tuple quantization technique. In *IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 1–4, 2011.