

Fingerprint Pre-Alignment based on Deep Learning

Benjamin Dieckmann¹, Johannes Merkle¹, Christian Rathgeb¹

Abstract: Robust fingerprint pre-alignment is vital for identification systems and biometric cryptosystems based on fingerprint minutiae, where computation of a relative alignment by comparison of the fingerprints is inefficient or intractable, respectively. The pre-alignment is achieved through an absolute alignment, i. e. an alignment computed for each fingerprint independently, which can be applied for fingerprint registration to compensate for variations in the placement (translation) and rotation of the fingerprints prior to their comparison.

In this work, a deep learning approach for absolute pre-alignment of fingerprints is presented. The proposed algorithm employs a siamese network (with CNNs as subnetworks) which is trained on synthetically generated fingerprints using horizontal/vertical translation and rotation as three regression coefficients. Evaluations are conducted on the FVC2000 DB2a and the MCYT fingerprint database. Compared to other published fingerprint pre-alignment methods, the presented scheme achieves higher accuracy w. r. t. rotation estimation and overall robustness. In addition, the proposed pre-alignment is applied as a pre-processing step in a Fuzzy Vault scheme.

Keywords: Fingerprint Registration, Deep Learning, Fingerprint Pre-Alignment, Biometric Template Protection

1 Introduction

In recent years, the application of *deep learning*, in particular Convolutional Neural Networks (CNNs), has achieved remarkable success in the field of biometric recognition [SW18]. For different biometric characteristics deep learning approaches have been proposed for various modules in the biometric processing chain. For fingerprint recognition, deep learning solutions have been presented for various tasks, e. g. fingerprint type classification [Pe18], orientation field estimation [CJ15], distortion rectification [Da18] or feature extraction [Ta17, DR17]. More recently, Schuch *et al.* [SMB18] proposed an algorithm for compensating fingerprint rotations based on deep learning; their approach was to interpret the task as a classification problem using the integer degrees ($-90^\circ, \dots, 90^\circ$) of the rotation as the target classes. The authors showed that their approach outperforms other methods in terms of rotation estimation accuracy. However, the algorithm was only trained and evaluated on rotated pairs of the same imprint, while, in real-world applications, it is necessary to compensate the rotation between different imprints of a finger. Furthermore, their algorithm does not allow for translation estimation.

Apart from the aforementioned deep learning-based approach, several handcrafted methods for fingerprint pre-alignment have been published. Most of these schemes are designed to reliably detect reference points based on which an absolute alignment (pre-alignment)

¹ secunet Security Networks, Mergenthaler Allee 77, Eschborn, Germany {firstname.lastname}@secunet.com

can be determined. The most prominent reference points are the *singular points* of the orientation field, i. e. core and delta points. Diverse algorithms have been proposed for singular point detection, e. g. [TK99, NB03]. Since fingerprints of type *arch* do not have any singular points the estimation of more generalized singular points, e. g., highest curvature points, has been suggested, e. g. [Ig06, WBS12]. An alternative approach is the estimation of a so-called *focal point*, e. g. [GZY16, BA09]. However, many of these universal methods do not output a direction which could be used to compensate different rotations of the fingerprints. Another approach to determine directed reference points referred to as *Tented Arch Reference Point* (TARP) was presented in [Ta13] and [TMM15]. In [Me17] different improvements have been applied to TARP resulting in an *Extended Tented Arch Reference Point* (xTARP) algorithm; while xTARP is one of the most accurate reference point detection methods, its computational costs are quite high.

In this publication, we present an algorithm for absolute rotation and translation estimation for fingerprint pre-alignment based on deep learning. A siamese network with CNNs as subnetworks is trained with synthetic fingerprints to output a relative alignment between two imprints of a finger. Subsequently, the output of a single subnetwork which consists of vertical / horizontal translation and rotation is deployed for fingerprint pre-alignment. The introduced algorithm is shown to outperform published approaches in terms of rotation estimation and overall robustness on the widely used FVC2000 DB2a fingerprint database. Additional benchmarks are presented on the MCYT database, based on which the proposed pre-alignment approach is applied in a biometric cryptosystem, i. e. the *Fuzzy Vault scheme*. To the best of our knowledge, this is the first deep learning-based approach for fingerprint pre-alignment.

The remainder of this paper is organized as follows: the fingerprint data used in this work is summarized in Sect. 2. In Sect. 3, the proposed system is described in detail. Experiments are presented in Sect. 4. Finally, conclusions are drawn in Sect. 5.

2 Fingerprint data selection

The definition and selection of suitable data is an essential step for machine learning approaches. Especially, deep learning requires a very high amount of training data. To obtain a sufficient number of fingerprints, we generate synthetic data with the Synthetic Fingerprint Generator (SFinGe) from the University of Bologna [CMM04]. The fingerprints are generated with the default parameter profile, which is pre-configured to create a fingerprint database that contains a realistic feature distribution. As the only changes, the parameters limiting the translation and rotation were set to their maximum. Also the distribution of finger classes is intentionally set to uniform, so that each class occurs equally often. The output image dimension is 256×400 pixel by a resolution of 500 DPI.

The experimental evaluation of the proposed method is performed on the public FVC 2000 DB2a [Ma00] and MCYT [OGFAS03] fingerprint databases. Example fingerprints of these data sets are depicted in Fig. 1. From the MCYT database, only fingerprints of fingers with an index of zero (index fingers) are used. The resulting number of fingerprint images



Fig. 1: Examples of pairs of fingerprints from a single finger of both databases used for testing.

Database	Train	Test	Fingers	Fingerprints
Synthetic Fingerprints	✓		100,000	400,000
FVC2000 DB2a		✓	100	800
MCYT		✓	330	3,960

Tab. 1: Fingerprint databases used for training and testing.

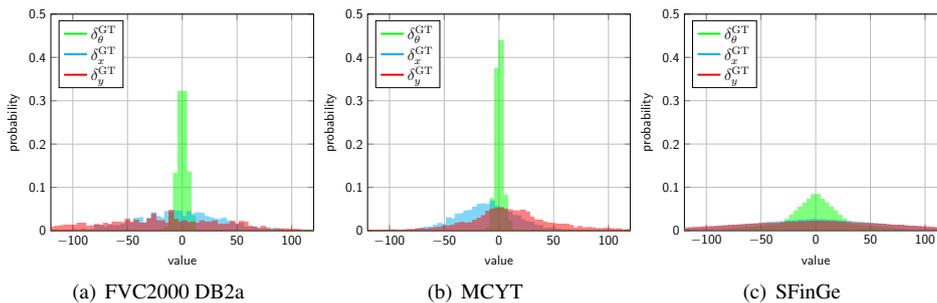


Fig. 2: Target rotation and translation values for all used databases.

employed for training and testing is summarized in Tab. 1. Note that these databases were acquired using different sensor types and image dimensions, i. e. an optical sensor for MCYT (256×400 pixel) and a low-cost capacitive sensor for FVC2000 DBa (256×364 pixel).

The alignment for a fingerprint can be defined as a triple of x , y and θ , where x and y indicate the horizontal/vertical translation and θ represents the rotation. However, there is no generally applicable definition of an absolute alignment, i. e. published works often use the position and direction of a method-specific reference point [BA09, Me17, GZY16]. A method-independent ground-truth can only be defined as relative alignments $(\delta_x, \delta_y, \delta_\theta)$ between pairs of fingerprints of the same finger. Those ground-truth values had been collected by hand for fingerprints of the MCYT database [Me17] and FVC2000 DB2a [GZY16].

The distribution of those target (ground-truth) values $(\delta_x^{\text{GT}}, \delta_y^{\text{GT}}, \delta_\theta^{\text{GT}})$ for all databases are plotted in Fig. 2. These plots clearly show that the translation and rotation between

pairs of (matching) fingerprints vary for each database: In particular, FVC2000 DB2a exhibits higher translation and rotation values than the MCYT database, albeit the variance of rotations is generally rather small in both data sets. The maximum absolute values are $\delta_x^{\text{GT}} = 150$, $\delta_y^{\text{GT}} = 254$ and $\delta_\theta^{\text{GT}} = 19$. In order to cover various translation and rotation values during the training of the neural network, the synthetic fingerprints are generated to exhibit a larger variation of target values compared to the other databases used for testing. The application of a uniformly random translation and rotation to a synthetic fingerprint is intended to enhance the generalization of the network.

3 Proposed system

It is not feasible to train a single CNN directly since method-independent absolute fingerprint alignments cannot be clearly defined (see Sect. 2). Instead, we train a siamese network consisting of two identical CNNs computing absolute alignments, combine their outputs to a relative alignment and compute the error function from the deviation of this relative alignment from the ground truth data. Precisely, each CNN receives as input the orientation field of a different imprint of the same finger, and predicts three regressive values (x, y, θ) which represent an absolute alignment. From these two outputs, the relative alignment $(\delta_x, \delta_y, \delta_\theta)$ representing the horizontal/vertical translation and rotation between the input fingerprints is computed and compared to the ground-truth data $(\delta_x^{\text{GT}}, \delta_y^{\text{GT}}, \delta_\theta^{\text{GT}})$. The computation of the relative alignment from the outputs of the CNNs is not learned but implemented by a fixed function. After the training of the siamese network, a single CNN has learned to predict values for an absolute alignment. These core processing steps of the proposed system are illustrated in Fig. 3. The neural network is implemented with Tensorflow [Ab16]. The following sections describe the extraction of the orientation fields, which are used as input data, the architecture of the basis CNN and the training and testing phases in detail.

3.1 Feature extraction

To minimize the influence of properties from different databases, e. g. compression level or image resolution, only the orientation fields are used as input data. For half of the synthetic fingerprints from Tab. 1, SFinGe is configured to store the generated orientation fields, which are referred to as *ground truth orientation fields*. With all other synthetic and real fingerprints, more realistic input data is created by a modified version of the open source minutiae extractor FingerJetFX [Di11]. For both SFinGe and FingerJetFX the orientation fields are down scaled on a factor 4, resulting on a dimension of 64×100 pixel for synthetic fingerprints and the MCYT database. The height of the images obtained from FVC2000 DB2a is smaller, so that these fingerprints are equally padded with empty background pixels on top and bottom. A single orientation field consists of angle values in the range $[-90, 90)$ degrees. Since the orientation fields are undirected and angle values are cyclic, the sinus and cosinus values of each orientation are used as inputs to the CNNs.

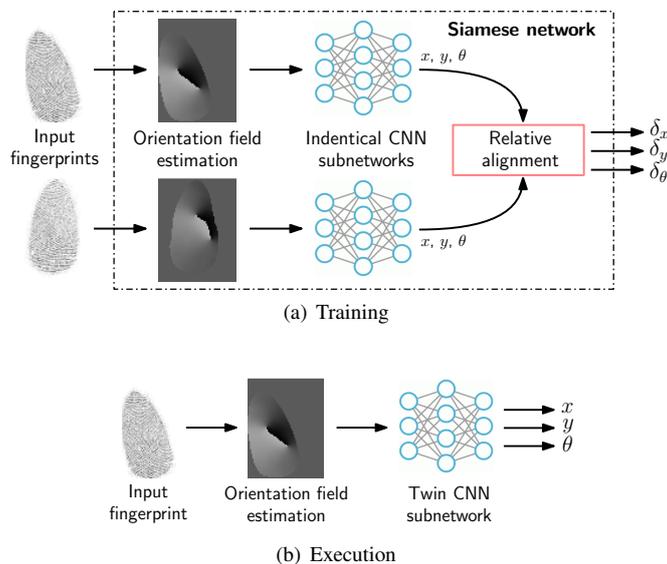


Fig. 3: Overview of the usage of a siamese network for relative fingerprint pre-alignment during training and the execution of one CNN subnetwork for absolute fingerprint pre-alignment.

3.2 Network architecture

The architecture and depth of the CNN subnetworks, as shown in Tab. 2, is inspired by related works on fingerprint processing. Like other publications, e. g. [Da18, CJ15, Pe18], the network architecture is composed of convolutional and fully connected layers. The features of an orientation field are detected by four blocks each consisting of a Convolutional Layer, Batch Normalization and MaxPooling. An absolute alignment is predicted by the following three fully connected layers. The activation of all neurons is calculated by the *Exponential Logarithmic Unit* (Elu) activation function [CUH15], which enables the processing of negative values. Due to the time and resource consuming training operations, the hyperparameters are iteratively chosen and may offer opportunities for further optimization.

3.3 Training and execution of the model

The application of the proposed deep learning model is divided into two stages: the training phases for the siamese network and the execution of a single subnetwork. In a first step, the network learns the most important features of an orientation field, by fitting the random initialized weights with the ground truth orientation fields from SFinGe. Subsequently, the pre-trained network will be refined with real world orientation fields, which are created for the remaining synthetic fingerprints by FingerJetFX. The loss function calculates the relative alignment errors for each fingerprint pair as sum of the rotation and translation error,

Number	Layer	Output
0	Input	(100×64×2)
1	Convolutional Layer (3×3, 32) Batch Normalization Elu	(100×64×32)
2	MaxPooling (2×2)	(50×32×32)
3	Convolutional Layer (3×3, 32) Batch Normalization Elu	(50×32×32)
5	MaxPooling (2×2)	(25×16×32)
6	Convolutional Layer (3×3, 64) Batch Normalization Elu	(25×16×32)
7	MaxPooling (2×2)	(12×16×64)
8	Convolutional Layer (3×3, 64) Batch Normalization Elu	(12×16×64)
9	MaxPooling (2×2)	(6×8×64)
10	Flatten	(3072)
11	Dense Elu Dropout (0.5)	(1024)
12	Dense Elu Dropout (0.5)	(512)
13	Dense Elu	(256)
14	Output	(3)

Tab. 2: Network architecture of CNN subnetworks.

where horizontal and vertical translation are combined as Euclidean distance. After the siamese network learned the relative alignment between two samples of the same finger, the output of one single network is used in the evaluation as absolute alignment values.

4 Evaluation

The predictions of one subnetwork can be used for the pre-alignment of fingerprints, as shown in Fig. 4. Original recordings from the FVC2000 DB2a are pictured in Fig. 4(a) and through the application of the predictions they are pre-aligned in Fig. 4(b). Note that due to the lack of clear definition of a “correct” absolute alignment, the errors of the deep learning-based method cannot be measured on its own. By combining absolute alignments to obtain relative alignments of fingerprint pairs, we can measure the errors for each pair of matching fingerprint as the derivation of the relative alignments $(\delta_x, \delta_y, \delta_\theta)$ derived from the outputs of the CNN from the ground-truth alignment $(\delta_x^{\text{GT}}, \delta_y^{\text{GT}}, \delta_\theta^{\text{GT}})$. The distributions of the errors on the test databases are plotted in Fig. 5.

From Fig. 5 it can be observed that the proposed method achieves slightly higher accuracy on the MCYT database compared to the FVC2000 DB2a database. In order to compare our algorithm with methods based on reference point detection, we apply the metric used in [Me17]: For each finger, all fingerprints are relatively aligned to each other using the ground-truth data $(\delta_x^{\text{GT}}, \delta_y^{\text{GT}}, \delta_\theta^{\text{GT}})$. Ideally, after this relative alignment, the outputs (x_i, y_i, θ_i) of the CNN should be identical for all imprints i of a finger. Consequently, for

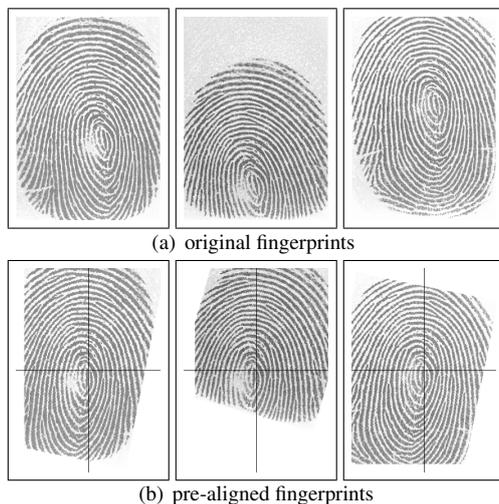


Fig. 4: Examples of pre-aligned fingerprints from the FVC2000 DB2a using deep learning.

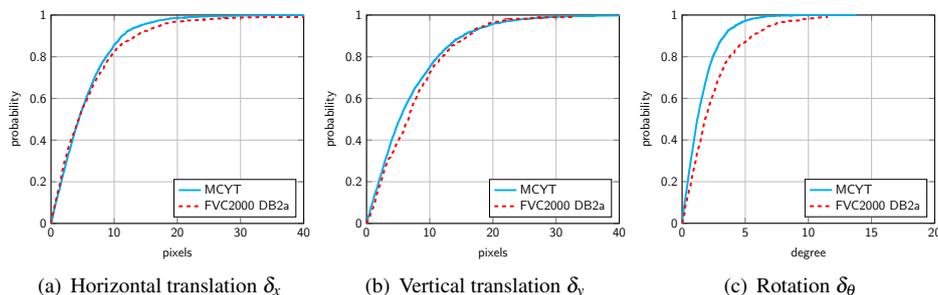


Fig. 5: Cumulative statistics of the obtained translation and rotation errors.

each finger, the distance and rotation errors are then computed as the average Euclidean distance and angle difference, respectively, between the (aligned) outputs for all fingerprints i and their median $(\bar{x}, \bar{y}, \bar{\theta})$. As shown in Tab. 3, the proposed deep learning-based pre-alignment achieves competitive accuracy. It generally provides higher robustness, i. e. large distance or rotation errors are reduced. Focusing on rotation errors, the proposed deep learning-based method clearly outperforms existing approaches.

As an additional feature of a deep learning based pre-alignment method, the concurrent processing of multiple fingerprints is supported by the implementation with tensorflow. With an average execution time of less than 100ms for 256 fingerprints at once, the method is expected to require negligible computational resources within the biometric processing chain. The proposed method is significantly faster than [Me17] (1.5 seconds) but does not reach the performance of [GZY16] (4.88 ms), where comparable methods only support sequentially processing of images. It should be noted that with the graphics card Palit GeForce GTX 1080 TI, stronger hardware was used than in previous works.

Method	$DE < 5$	$DE < 10$	$DE < 20$	$RE < 5$	$RE < 11.25$	$RE < 22.5$	Fail
Proposed	461	761	797	752	798	800	0
[Me17]	612	734	763	610	752	790	5
[TMM15]	624	739	761	607	754	782	13
[GZY16]	569	719	784	n.a.	n.a.	n.a.	0
[BA09]	n.a.	668	769	n.a.	521	657	0
[AB08]	285	640	763	n.a.	n.a.	n.a.	1
[Ig06]	n.a.	712	753	n.a.	n.a.	n.a.	0
[LZH06]	n.a.	654	745	n.a.	690	737	9
[LJK05]	n.a.	659	749	n.a.	n.a.	n.a.	13

Tab. 3: Cumulative statistics of the distance errors (DE), rotation errors (RE), and number of failures of our method and other methods. An entry “n.a.” means that the corresponding value is not provided in the reference or (in the case of RE) that the method does not compute any orientation.

Finally, we evaluate how our deep learning-based pre-alignment affects the performance of a biometric cryptosystem. We used the minutiae-based fuzzy vault scheme of [Bu16], which was also used in [Me17] to evaluate the xTARP pre-alignment algorithm. This scheme protects the confidentiality of the minutiae data by applying a secret polynomial which can be recovered with a sufficiently similar fingerprint and, in contrast to many other biometric cryptosystems (e.g. see [SB07, Ta14, MT13]), it is immune to correlation attacks, where an attacker combines the templates created in different enrolments of the same user.²

We use the implementation from [Bu16] with the same parameters as in [Me17] and apply different pre-alignment algorithms including our deep learning-based method. Tab. 4 lists the resulting False Non-Match Rate (FNMR) for the relevant degrees k of the secret polynomial. Note, that the False Match Rate (FMR) and the security of the protected templates against recovery attacks do not depend on the pre-alignment method. The error rates were estimated on the same test set as in [Me17], i. e. right index fingers of the first 100 subjects of the MCYT database. While the proposed pre-alignment outperforms the original TARP method of [Ta13] for small values of k , it reveals inferior performance compared to the xTARP method of [Me17]. In a fusion where translation is obtained from the xTARP algorithm and the rotation from the proposed deep learning based pre-alignment, respectively, further slight improvements can be observed.

5 Conclusion

In this work, we presented the first deep learning-based approach to absolute fingerprint pre-alignment which has been shown to achieve competitive accuracy. Compared to other published methods, the amount of large deviations from target values is significantly reduced, and with respect to the accuracy of the rotation estimation, our method clearly

² A correlation attack against the scheme of [Bu16] was presented in [NKU16] but, for the parameters used in our evaluation, it is not efficient.

	Method	$k = 5$	$k = 6$	$k = 7$	$k = 8$
FNMR	Original TARP	6.0%	7.4%	9.6%	13.1%
	xTARP (stateless)	0.5%	1.7%	3.8%	6.6%
	Proposed	1.5%	3.9%	9.1%	16.0%
	Proposed + xTARP	0.6%	1.5%	3.7%	6.3%
FMR	all	1.9%	0.3%	0.04%	0%
Security (bits)	all	16.5	20	24	27

Tab. 4: Error rates of the Fuzzy Vault construction of [Bu16] when using different variants of the xTARP and TARP method and the proposed deep learning-based method for pre-alignment.

outperforms all other pre-alignment algorithms. This is essential to achieve practical biometric performance in fingerprint-based cryptosystems as it has been demonstrated for the fuzzy vault scheme.

However, with respect to translation estimation, there is still room for improvement. Possible approaches to improve our method could be to increase the penalty for translation errors in the training, to train separate networks for translation and rotation estimation, to cleverly combine it with other pre-alignment algorithms (e.g. from [Me17] or [GZY16]), or to apply it iteratively multiple times (analogously to [DG08]).

References

- [AB08] Areekul, Vutipong; Boonchaiseree, Natthawat: Fast focal point localization algorithm for fingerprint registration. In: Industrial Electronics and Applications, 2008. ICIEA 2008. 3rd IEEE Conference on. IEEE, pp. 2089–2094, 2008.
- [Ab16] Abadi, M.; Barham, P.; Chen, J. et al.: Tensorflow: A system for large-scale machine learning. In: 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16). pp. 265–283, 2016.
- [BA09] Boonchaiseree, N.; Areekul, V.: Focal Point Detection Based on Half Concentric Lens Model for Singular Point Extraction in Fingerprint. In: Advances in Biometrics, Third International Conference, ICB 2009, Alghero, Italy, June 2-5, 2009. Proceedings. pp. 637–646, 2009.
- [Bu16] Butt, M.; Merkle, J.; Korte, U.; Busch, C.: Correlation-resistant fuzzy vault for fingerprints. In: Proc. of Sicherheit 2016. volume 256 of LNI. GI, pp. 125–136, 2016.
- [CJ15] Cao, K.; Jain, A. K.: Latent orientation field estimation via convolutional neural network. In: 2015 International Conference on Biometrics (ICB). pp. 349–356, 2015.
- [CMM04] Cappelli, R.; Maio, D.; Maltoni, D.: SFinGe: an approach to synthetic fingerprint generation. In: International Workshop on Biometric Technologies (BT2004). pp. 147–154, 2004.
- [CUH15] Clevert, D.-A.; Unterthiner, T.; Hochreiter, S.: Fast and accurate deep network learning by exponential linear units (elus). arXiv preprint arXiv:1511.07289, 2015.
- [Da18] Dabouei, A.; Kazemi, H.; Iranmanesh, S. M.; Dawson, J.; M. Nasrabadi, N.: Fingerprint Distortion Rectification Using Deep Convolutional Neural Networks. In: 2018 International Conference on Biometrics (ICB). pp. 1–8, 2018.

- [DG08] Duffner, Stefan; Garcia, Christophe: Robust Face Alignment Using Convolutional Neural Networks. In: VISAPP (2). pp. 30–37, 2008.
- [Di11] Digital Persona: , FingerJetFX Open Source Edition. <https://github.com/FingerJetFX0SE/FingerJetFX0SE>, 2011. [Online: 21.05.2019].
- [DR17] Darlow, L. N.; Rosman, B.: Fingerprint minutiae extraction using deep learning. In: 2017 IEEE International Joint Conference on Biometrics (IJCB). pp. 22–30, Oct 2017.
- [GZY16] Guo, X.; Zhu, E.; Yin, J.: A fast and accurate method for detecting fingerprint reference point. *Neural Computing and Applications*, pp. 1–11, 2016.
- [Ig06] Ignatenko, Tanya; Kalker, Ton; van der Veen, Michiel; Bazen, Asker M.: Reference point detection for improved fingerprint matching. In: Security, Steganography, and Watermarking of Multimedia Contents VIII, San Jose, CA, USA, January 15, 2006. p. 60720G, 2006.
- [LJK05] Liu, Manhua; Jiang, Xudong; Kot, Alex ChiChung: Fingerprint Reference-Point Detection. *EURASIP J. Adv. Sig. Proc.*, 2005(4):498–509, 2005.
- [LZH06] Liu, Tong; Zhang, Chao; Hao, Pengwei: Fingerprint Reference Point Detection Based on Local Axial Symmetry. In: 18th International Conference on Pattern Recognition (ICPR 2006), 20-24 August 2006, Hong Kong, China. pp. 1050–1053, 2006.
- [Ma00] Maio, D.; Maltoni, D.; Cappelli, R.; Wayman, J.L.; Jain, A.K.: FVC2000: Fingerprint Verification Competition. *IEEE*, pp. 402–412, 2000.
- [Me17] Merkle, J.; Tams, B.; Dieckmann, B.; Korte, U.: xTARP: Improving the Tented Arch Reference Point Detection Algorithm. In: 2017 International Conference of the Biometrics Special Interest Group (BIOSIG). *IEEE*, pp. 1–7, 2017.
- [MT13] Merkle, J.; Tams, B.: Security of the Improved Fuzzy Vault Scheme in the Presence of Record Multiplicity. *CoRR abs/1312.5225*, 2013. available online: <http://arxiv.org/abs/1312.5225>.
- [NB03] Nilsson, K.; Bigün, J.: Localization of corresponding points in fingerprints by complex filtering. *Pattern Recognition Letters*, 24(13):2135–2144, 2003.
- [NKU16] Neu, Matthias; Korte, Ulrike; Ullmann, Markus: Improvement of fuzzy vault for multiple fingerprints with angles. In: 2016 International Conference of the Biometrics Special Interest Group (BIOSIG). *IEEE*, pp. 1–8, 2016.
- [OGFAS03] Ortega-Garcia, J.; Fierrez-Aguilar, J.; Simon *et al.*, D.: MCYT baseline corpus: a bimodal biometric database. *IEE Proc. on Vision, Image and Signal Processing*, 150(6):395–401, 2003.
- [Pe18] Peralta, D.; Triguero, I.; Garc a, S.; Saeys, Y.; Ben atez, J.; Herrera, F.: On the use of convolutional neural networks for robust classification of multiple fingerprint captures. *International Journal of Intelligent Systems*, 33:213–230, 01 2018.
- [SB07] Scheirer, W. J.; Boulton, T. E.: Cracking Fuzzy Vaults and Biometric Encryption. In: *Proc. of Biometrics Symp.* pp. 1–6, 2007.
- [SMB18] Schuch, P.; May, J. M.; Busch, C.: Unsupervised Learning of Fingerprint Rotations. In: 2018 International Conference of the Biometrics Special Interest Group (BIOSIG). pp. 1–6, 2018.

- [SW18] Sundararajan, K.; Woodard, D. L.: Deep Learning for Biometrics: A Survey. *ACM Comput. Surv.*, 51(3):65:1–65:34, May 2018.
- [Ta13] Tams, B.: Absolute Fingerprint Pre-Alignment in Minutiae-Based Cryptosystems. In: *Proc. of BIOSIG 2013*. volume 212 of LNI. GI, pp. 75–86, 2013.
- [Ta14] Tams, Benjamin: Decodability Attack against the Fuzzy Commitment Scheme with Public Feature Transforms. *CoRR*, <http://arxiv.org/abs/1406.1154>, 2014.
- [Ta17] Tang, Y.; Gao, F.; Feng, J.; Liu, Y.: FingerNet: An Unified Deep Network for Fingerprint Minutiae Extraction. In: *Biometrics (IJCB), 2017 IEEE International Joint Conference on*. IEEE, 2017.
- [TK99] Tico, Marius; Kuosmanen, Pauli: A multiresolution method for singular points detection in fingerprint images. In: *Proceedings of the 1999 International Symposium on Circuits and Systems, ISCAS 1999, Orlando, Florida, USA, May 30 - June 2, 1999*. pp. 183–186, 1999.
- [TMM15] Tams, B.; Mihăilescu, P.; Munk, A.: Security Considerations in Minutiae-based Fuzzy Vaults. *IEEE Trans. Inf. Forensics Security*, 10(5):985–998, 2015.
- [WBS12] Wang, L.; Bhattacharjee, N.; Srinivasan, B.: Fingerprint reference point detection based on local ridge orientation patterns of fingerprints. In: *The 2012 International Joint Conference on Neural Networks (IJCNN)*. pp. 1–8, 2012.