Absolute Fingerprint Pre-Alignment in Minutiae-Based Cryptosystems

Benjamin Tams*

Institute for Mathematical Stochastics
University of Goettingen
Goldschmidtstr. 7
D-37077, Goettingen
btams@math.uni-goettingen.de

Abstract: Most biometric cryptosystems that have been proposed to protect fingerprint minutiae make use of public alignment helper data. This, however, has the inadvertent effect of information leakage about the protected templates. A countermeasure to avoid auxiliary alignment data is to protect absolutely pre-aligned fingerprints. As a proof of concept, we run performance evaluations of a minutiae fuzzy vault with an automatic method for absolute pre-alignment. Therefore, we propose a new method for estimating a fingerprint's directed reference point by modeling the local orientation around the core as a tented arch.[1]

1 Introduction

In 2002, Juels and Sudan [JS02] proposed the *fuzzy vault scheme*. It quickly has drawn the attention of biometric researchers as a promising tool for storing fingerprint minutiae templates protected as a part of a security application. While there are other biometric cryptosystems (see [JW99, DORS08, Tru11, JA07]) being considered as a potential tool for protecting fingerprint templates, the fuzzy vault scheme is one of the most dominant one because it well conceptualizes differences of and partial overlap between fingerprints as errors and erasures, respectively, by means of *Reed-Solomon codes*. A common approach to protect a fingerprint template via fuzzy vault is to hide its *genuine minutiae* within a large number of *chaff minutiae*. The *fuzzy fingerprint vault* draws its security from the problem in distinguishing genuine from chaff minutiae (without knowing a matching minutiae template). On authentication, a second minutiae template from the alleged same user is used to distinguish genuine from the chaff. If the candidate minutiae have a significant overlap with genuine minutiae, the protected minutiae template can be recovered using techniques

*The support of the Felix Bernstein Institute for Mathematical Statistics in the Biosciences and the Volkswagen Foundation is gratefully acknowledged.

[1] A program implementing our method for estimating a fingerprint's directed reference point will be provided for download from `http://www.stochastik.math.uni-goettingen.de/biometrics` by the date of the conference.

from the discipline of *error-correcting codes*.

For first implementations of the fuzzy fingerprint vault (e.g., [UJ06, NJP07]) it quickly turned out that brute-force attacks are not only possible but rather easy to perform [SB07, MMT09]. To improve security, the incorporation of minutiae descriptors in addition to mere minutiae has been proposed [NNJ10] which has the potential of providing reasonable brute-force security at a comparably usable authentication performance. However, an intruder having intercepted different application's databases may link genuine vault correspondences across them via correlation, i.e. *cross-matching*. Even worse, given two genuine vault correspondences it can be possible to recover the protected templates at quite a high rate via the *correlation attack* [KY08]. It is known that such *attacks via record multiplicity* are enabled due to the different vault's chaff being generated randomly [SB07] and these attacks can obviously be circumvented by rounding genuine minutiae to a rigid system of which unoccupied elements encode the chaff (e.g., see [MMT09] for a discussion of using non-random chaff). An implementation as well as a performance evaluation (assuming a well-solved alignment framework) of this approach can be found in [Tam13]. There remains the risk of attacks that are yielded by a cryptographically non-negligible false acceptance rate, i.e. *false-accept attacks*. These attacks have the potential of breaking current fingerprint cryptosystems very easily—even if brute-force attacks are impractical to perform. And yet another question remains concerning the information that is leaked from public helper data for assisting in fingerprint alignment on genuine authentication.

On authentication, query fingers have to be pre-aligned such that two vault minutiae matching with query minutiae are of sufficient similarity. Current implementations achieve a reasonably accurate relative pre-alignment by fitting the query fingerprints to auxiliary data publicly stored along with the vault [NJP07, JA07, LYT+08]. This, however, has the inadvertent effect of information leakage about the protected finger from the vault: An adversary having intercepted a vault record may use the additional data to improve off-line attacks. Formal analyses for quantifying the amount of leaked information are missing and may be hard to achieve. Unless analyses yielding negligible information leakage of auxiliary alignment data (given the vault) are available, we should not propagate the use of public alignment helper data.

In [MIK+11] the use of additional data is circumvented. On enrollment, a coarse absolute pre-alignment of the fingerprint is determined before its minutiae are protected. On authentication, as on enrollment, a coarse absolute pre-alignment of the query fingerprint is estimated and then the pre-aligned minutiae are adjusted to well match vault minutiae. The construction, however, does not ensure resistance against cross-matching or the correlation attack. Furthermore, if it is adopted for constructions protecting rounded minutiae to achieve cross-matching resistance (see [JW99, DORS08, KBK+11, Tam13]), refining the alignment of coarsely pre-aligned minutiae will not work anymore. Therefore, absolute fingerprint pre-alignment should not be only coarse but even reasonably robust. Alternatively, constructions using alignment-free features can be considered as in [LYC+10]. However, to date no resistance against cross-matching has been ensured for such constructions. In this paper, we focus on the option of absolute fingerprint pre-alignment to protect minutiae templates in order to avoid the use of additional alignment data.

Minutiae of a fingerprint can be represented w.r.t. a Cartesian coordinate system using

(a) not aligned (b) pre-aligned

Figure 1: A fingerprint and its minutiae (blue) are absolutely pre-aligned w.r.t. a coordinate system given by a directed reference point estimation (red)

well-known techniques from *linear algebra*. There is an evident one-to-one correspondence between Cartesian coordinate systems and points constituted with a direction (also see Figure 1). To implement a robust absolute fingerprint pre-alignment, it is essential to robustly estimate directed reference points or, equivalently, an intrinsic Cartesian coordinate system. There have been proposals for estimating stable reference points such as the *core* [NK98] and the *focal point* [RA00]. For an intrinsic coordinate system, however, the estimation of a robust intrinsic direction is required in addition.

[Hot09] proposed to estimate a fingerprint's intrinsic coordinate system using the global *quadratic differential model* fitted to the fingerprint's orientation field [HHM08]. The fitted model's origin was used as the reference point's coordinate and the direction of the longitudinal axis as its direction. The method requires an estimation of all *singular points* of the finger, i.e. *cores* and *deltas*. This can, however, not be ensured in general—in particular, if some of the singular points are not visible on a fingerprint. Bazen and Gerez [BG01] partitioned a fingerprint into regions containing no singular points and defined hypothetical lines between encompassing regions as the axes of an intrinsic (non-Cartesian) coordinate system. The proposed construction, however, still requires solutions for reliable partitioning the fingerprint into *regular regions*. We argue with [MMJP09] that there have been no definite solutions enabling reliable absolute fingerprint pre-alignment.[2]

The paper is outlined as follows. In Section 2 we describe an implementation based on the fuzzy vault scheme adopted from [Tam13] with minor modifications to protect the minutiae of absolutely pre-aligned fingerprints. In Section 3 we propose a new method for estimating a directed reference point in a fingerprint, which yields an intrinsic Cartesian coordinate system to which minutiae can be absolutely pre-aligned. In Section 4, we incorporate our proposed method into the minutiae fuzzy vault of Section 2. Final discussions are given in Section 5.

[2]To the best of the author's knowledge, no significant advancements have been made in estimating robust absolute pre-alignments of fingerprints since the publication of [MMJP09].

2 Minutiae Cryptosystem Used for Testing

This paper focuses on the potential of biometric cryptosystems to protect absolutely pre-aligned fingerprints. For testing, we used the cross-matching resistant implementation described in [Tam13] of which source code is publicly available. In this section, we briefly describe its functioning in the language of absolutely pre-aligned minutiae.

Given an absolutely pre-aligned minutiae template, each of its minutia is coarsely quantized first. Let $\mathfrak{m} = (a, b, \theta)$ be a minutia at (a, b) and of angle $\theta \in [0, 2\pi)$. Let p_j be a point of a hexagonal grid $\{p_0, \ldots, p_{r-1}\}$ laying within the region in where pre-aligned minutiae can occur. Let p_j be a hexagonal grid point that best approximates (a, b). Furthermore, let $j' = \lfloor \theta/(2\pi) \cdot s \rfloor$ where s denotes a parameter controlling the number of values into which minutiae angles are quantized. Now, the integer $j + r \cdot j'$ encodes the quantization of $\mathfrak{m}$. Let $x_{j,j'} \in \mathbf{F}$ denote the finite field element encoding $j + r \cdot j'$ by a fixed convention. The quantization of the minutia $\mathfrak{m}$ is encoded by $x_{j,j'}$. By $\mathbf{E}$ we denote the subset of $\mathbf{F}$ in where a minutia's quantization $x_{j,j'}$ can occur, i.e. $\mathbf{E} = \{x_{j,j'} \mid j = 0, \ldots, r-1,\ j' = 0, \ldots, s-1\}$.

On enrollment, we assume that the minutiae of an absolutely pre-aligned fingerprint are provided and that they are sorted decreasingly with respect to their quality. The feature set $\mathbf{A}$ is defined as to contain the (at most the first $t_{\max}$) quantizations of the minutiae. The next step is to bind the template quantized as $\mathbf{A}$ to a secret polynomial $f \in \mathbf{F}[X]$ of degree $< k$. This is done as usual by letting the genuine set $\mathbf{G} = \{ (x, f(x)) \mid x \in \mathbf{A} \}$. To achieve resistance against cross-matching via correlation, every element in $\mathbf{E}$ not contained in $\mathbf{A}$ is used to encode a chaff point. More precisely, $\mathbf{C} = \{ (x, y) \mid x \in \mathbf{E} \setminus \mathbf{A} \}$ where the ys are chosen uniformly at random from $\mathbf{F}$ with $y \neq f(x)$. The vault consists of the union of genuine and chaff points. Furthermore, a cryptographic hash value $\mathrm{SHA}(f)$ of the secret polynomial is stored along with the vault. Thus the public vault is the tuple $(\mathbf{V}, \mathrm{SHA}(f))$ where $\mathbf{V} = \mathbf{G} \cup \mathbf{C}$.

An intruder having intercepted $(\mathbf{V}, \mathrm{SHA}(f))$ can recover f as well as the template $\mathbf{A}$ by running off-line attacks. From the difficulty in running such attacks the implementation draws its security.

On authentication, an absolutely pre-aligned query minutiae template is provided. The query feature set $\mathbf{B}$ is extracted from the query template in the same way as $\mathbf{A}$ was extracted from the enrolled template. Using $\mathbf{B}$, the unlocking set is built $\mathbf{U} = \{ (x, y) \in \mathbf{V} \mid x \in \mathbf{B} \}$. $\mathbf{U}$ contains exactly $|\mathbf{A} \cap \mathbf{B}|$ genuine points. Thus, if $|\mathbf{A} \cap \mathbf{B}| \geq k$, the secret polynomial f can potentially be obtained from $\mathbf{U}$ using a systematic decoder. In [Tam13] the implementation uses a randomized decoding procedure. In particular, the higher the overlap $|\mathbf{A} \cap \mathbf{B}|$ the higher is the probability that the correct polynomial f can be recovered.

3 Directed Reference Point Estimation

To date, there have been no definite solutions enabling absolute pre-alignment of fingerprint minutiae for biometric template protection. In this section, we describe a new method for estimating a reference point with a direction from a fingerprint, thus yielding an intrinsic Cartesian coordinate system to which the minutiae can be absolutely pre-aligned. Like in [Hot09], we use the quadratic differential model [HHM08] as an elementary ingredient to estimate a *directed reference point* of a fingerprint but our method only requires the presence of the core on the fingerprint and not the presence of all singular points. Our method is based on the assumption that a fingerprint's orientation field can be modeled as a tented arch in a local neighborhood of its core. Using the quadratic differential model, we fit the orientations of a fixed tented arch to an estimation of the fingerprint's orientation field. Therein, the orientations being close to a predefined distance from the tented arch's core are taken into account with a higher weight which reflects our basic assumption. The position of the fitted tented arch's core serves as the estimated reference point's location and the direction of the fitted arch's longitudinal axis as its direction.

3.1 (Tented) Arch Model

(a) arch (b) tented arch

Figure 2: The orientation field (blue) of an arch (a) and of a tented arch (b). The tented arch is an arch whose orientation field is influenced by a core (green diamond) and a delta (red triangle) on its symmetry axis.

The orientation field of an arch can be modeled as the complex function $\psi(z) = \lambda^2 \cdot (z^2 - R^2)^2$ where $\mathbf{Im}(z) > 0$ and λ, R are real parameters. z is the function's complex variable. The (undirected) orientation $\varphi \in [0, \pi)$ at the location (x, y) with $y > 0$ is given by $\varphi = 0.5 \cdot \mathbf{Arg}(\psi(x + i \cdot y))$. If $y \leq 0$, the orientation is defined to be 0 which can be ensured by letting $\psi(x + i \cdot y) = 1$. A *tented arch model* essentially is an arch of which orientation field is influenced by a core and a delta on its longitudinal axis. We control the positions of the core and the delta by their distance d_{core} and d_{delta}, respectively, to the origin where $0 \leq d_{\mathrm{delta}} \leq d_{\mathrm{core}}$. The orientation field of a tented arch can be modeled as

$\tau(z) = \psi(z) \cdot \frac{(z-i\cdot d_{\text{core}})^2}{(z-i\cdot d_{\text{delta}})^2}$ (see [HHM08]).

The function $\tau(z)$ models the orientation field of a tented arch w.r.t. the origin $0+i\cdot 0$ and abscissa's direction $1+i\cdot 0$. To fit $\tau(z)$ to a fingerprint's orientation field, we may plug an *isometry* $\alpha\cdot z+\beta$ with $|\alpha|=1$. Furthermore, the orientations of the fitted model must be rotated in accordance with the isometry's rotation part α, i.e. a multiplication with α^{-2}. Thus, a tented arch model w.r.t. the origin $\omega = -\alpha^{-1}\cdot\beta$ and abscissa axis' direction α^{-1} is given by $\tau_{\alpha,\beta}(z) = \alpha^{-2}\cdot\tau(\alpha\cdot z+\beta)$.

3.2 Description of the Method

In this section, we describe how we can fit a tented arch model to an orientation field estimation of a fingerprint. Using a *Gaussian function*, the orientations being close to a predefined distance from the core are taken into account with a higher weight. Finally, the core of the adjusted tented arch is used as the reference point's location; its direction is given by the longitudinal axis of the fitted tented arch.

In the following we assume that the parameters of a tented arch (barring translation and rotation) are fixed. These are R, λ, d_{core}, and d_{delta}: R controls the abscissa pole's distance to the origin; λ controls the stretching of the tented arch; d_{core} and d_{delta} control the distance of the core and delta, respectively, from tented arch's origin along the longitudinal axis.

For an isometry $\alpha\cdot z+\beta$, $|\alpha|=1$, we valuate the goodness of $\tau_{\alpha,\beta}(z)$ with the help of a cost function measuring the agreement of $\tau_{\alpha,\beta}(z)$ to a fingerprint's estimated orientation field $\{(z_j, v_j)\}$: Here v_j encodes the estimated orientation at $z_j = x_j + i\cdot y_j$; if $\theta_j \in [0,\pi)$ is the orientation at (x_j, y_j) then $v_j = \cos(2\theta_j) + i\cdot\sin(2\theta_j)$. We can valuate the goodness of $\tau_{\alpha,\beta}(z)$ as $\kappa(\alpha,\beta) = \sum_j w_{\alpha,\beta}(z_j)\cdot\left|\frac{\tau_{\alpha,\beta}(z_j)}{|\tau_{\alpha,\beta}(z_j)|} - v_j\right|^2$ where $w_{\alpha,\beta}(z_j)$ denotes the weight of which the orientation at z_j is taken into account. We design the weight function $w_{\alpha,\beta}(z)$ as follows. Let $\gamma_{\alpha,\beta}$ be the core on the ordinate axis of $\tau_{\alpha,\beta}(z)$, i.e. $\gamma_{\alpha,\beta} = \omega_{\alpha,\beta} + d_{\text{core}}\cdot i\cdot\alpha^{-1}$ where $\omega_{\alpha,\beta} = -\alpha^{-1}\cdot\beta$ is the origin of the coordinate system. Now, the weight function the form $w_{\alpha,\beta}(z) = \exp\left(-\frac{(|z-\gamma_{\alpha,\beta}|-\rho)^2}{2\cdot\sigma^2}\right)$ where $\rho\geq 0$, and $\sigma > 0$.

We can fit a tented arch to $\{(z_j, v_j)\}$ by minimizing the cost function $\kappa(\alpha,\beta)$ where $|\alpha|=1$. The minimization process that we used, consists of three atomic steps: 1. Perform a global search for an initial model: For example, for $\alpha = 1$, we search a complex β such that $\kappa(1,\beta)$ is small, assuming that the tented arch's core $\gamma_{1,\beta}$ is on the fingerprint's foreground; 2. rotate the model around the core such that the cost function $\kappa(\cdot,\cdot)$ is minimized; 3. update the translation part β minimizing the function $\kappa(\alpha,\cdot)$ for fixed α.

The second and third step can be repeated until convergence of α and β. If the core $\gamma_{\alpha,\beta}$ lays on the fingerprint's foreground, it is output as the reference point and $\theta\in[0,2\pi)$ with $\exp(i\cdot\theta) = i\cdot\alpha^{-1}$ as its direction. Otherwise, if $\gamma_{\alpha,\beta}$ is outside the fingerprint's foreground, we repeat the procedure using another initial β. It is possible, that no initial

model yields a core laying on the fingerprint's foreground. Therefore, we should only try a few (20, say) initial models and report a corresponding error message if none yielded a valid reference point. The first step can be realized by an iteration over a grid laid on the fingerprint's foreground. The second and third steps can be solved using a *steepest descent* method for finding local minimums. In the following, we discuss details concerning the three fitting steps.

3.2.1 Initial Model

Let $\mathcal{I} = [0, N) + i \cdot [0, M)$ be the region of the fingerprint image. Furthermore, let $\mathcal{S} \subset \mathcal{I}$ be an estimation of the fingerprint's foreground. To find an initial model $\tau_{1,\beta}(z)$, we can iterate its core $\gamma_{1,\beta}$ over a finite subset of $\mathcal{S}$, e.g., a grid. Therefore, the core $\gamma_{1,\beta}$ and the delta $\delta_{1,\beta}$ must be distinct from the z_j. Otherwise, attempting to evaluate the cost function $\kappa(\alpha, \beta)$ results in a division by zero: $\tau_{\alpha,\beta}(\gamma_{\alpha,\beta}) = 0$ and $\tau_{\alpha,\beta}(\delta_{\alpha,\beta}) = 0$. To ensure that $\gamma_{1,\beta}$ is distinct from the z_j, we can choose them to lay on a grid $z_j \in ([h, h+g, h+2g, \ldots) + i \cdot [h, h+g, h+2g, \ldots)) \cap \mathcal{I}$ with $g > 0$ and $h \geq 0$. Then $\gamma_{1,\beta}$ can be iterated over a grid arranged concurrently to the z_j, e.g., $\gamma_{1,\beta} \in ([h+g/2, h+g/2+g, h+g/2+2g, \ldots) + i \cdot [h+g/2, h+g/2+g, h+g/2+2g, \ldots)) \cap \mathcal{S}$. By choosing d_{delta} carefully, we can ensure that the delta $\delta_{1,\beta}$ is disjoint from the z_j. The model $\tau_{1,\beta}(z) \in ([h+g/2, h+g/2+g, h+g/2+2g, \ldots) + i \cdot [h+g/2, h+g/2+g, h+g/2+2g, \ldots)) \cap \mathcal{S}$ is chosen as the initial model for which $\kappa(1, \beta)$ is minimal.

3.2.2 Fitting the Direction

Given $\tau_{\alpha,\beta}(z)$, we may rotate it around the core for adjustment to $\{(z_j, v_j)\}$. This will change both α and β. Let $\xi = \cos(\theta) + i \cdot \sin(\theta)$ be the complex number describing the rotation by the angle θ. More precisely, the rotated model $\tau_{\alpha',\beta'}(z)$ is given by $\alpha' = \xi \cdot \alpha$ and $\beta' = \gamma_{\alpha,\beta} - i \cdot d_{\text{core}} \cdot \xi \cdot \alpha^{-1}$. To find the adjusting rotation angle θ, we may minimize the function $\theta \mapsto \kappa(\alpha', \beta')$ for $\theta \in (-\pi, \pi)$ where α' and β' define the rotated model $\tau_{\alpha',\beta'}(z)$ as above. A (local) minimum of the function can be found using a steepest descent method starting with $\theta = 0$.

3.2.3 Fitting the Translation Part

For further refinement, we may update the translation part β of $\tau_{\alpha,\beta}(z)$. Therefore, we can minimize the function $(x_1, x_2) \mapsto \kappa(\alpha, x_1 + i \cdot x_2)$. Let (x_1', x_2') be a (local) minimum which can be found using a steepest descent method starting with $(\mathbf{Re}(\beta), \mathbf{Im}(\beta))$. Then the updated model is $\tau_{\alpha,\beta'}(z)$ where $\beta' = x_1' + i \cdot x_2'$.

4 Training and Evaluation

This paper discusses the potential of biometric cryptosystems to protect absolutely pre-aligned fingerprint minutiae. We used the fuzzy vault implementation described in Section 2 to test our proposed method for automatically estimating a directed reference point from a fingerprint and thus for absolutely fingerprint pre-alignment. In this section, we describe how we determined a good configuration for our proposed method. Furthermore, we describe the result of an evaluation. Throughout, we used minutiae templates corresponding to the FVC 2002 DB2 [MMC+02] database (DB2-B for training and DB2-A for evaluation). The minutiae templates have been extracted using a commercial extractor.[3] The orientation fields were estimated using the well-known *gradient method* [KW87] following the description of [MMJP09]. Furthermore, we estimated a fingerprint's foreground by selecting the largest connected region after *Otsu thresholding* and then computing its convex hull via *Graham scan*.

4.1 Training

In [Tam13], the parameters for the vault implementation have been determined during a training in where a good alignment was achieved manually on genuine authentication. We resumed the training to find a good configuration for our tented arch model to implement an automatic absolute pre-alignment. A best configuration observed was $\lambda = 1.81$, $R = 175$, $d_{\text{delta}} = 48$, $d_{\text{core}} = 186$, $\rho = 45$, and $\sigma = 12$ which resulted in 262 (among 280) genuine correspondences with at least $k = 7$ common elements.[4]

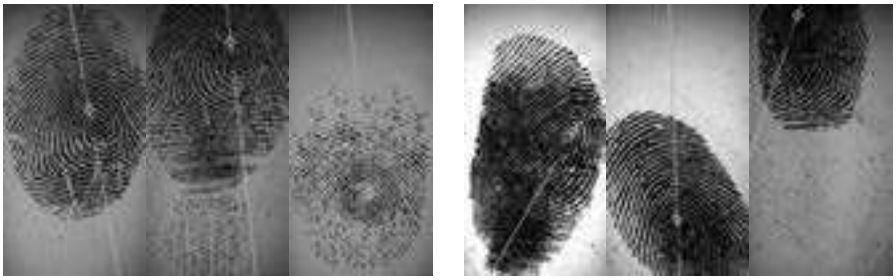
4.2 Evaluation

Table 1: Authentication performances of minutiae-based cryptosystem with absolutely pre-aligned fingerprint with our method on a 3.2 `Ghz` desktop computer using a single processor core. For authentication performances achievable with relative pre-alignment, we refer to [Tam13].

k	sub-GAR (GAR)	FAR	GDT	IDT
$= 7$	$= 91\%$ ($\approx 74.12\%$)	$\approx 0.91\%$	≈ 0.081 *sec*	≈ 0.270 *sec*
$= 8$	$= 88\%$ ($\approx 65.93\%$)	$\approx 0.16\%$	≈ 0.130 *sec*	≈ 0.329 *sec*
$= 9$	$= 85\%$ ($\approx 56.91\%$)	$\approx 0.06\%$	≈ 0.195 *sec*	≈ 0.405 *sec*
$= 10$	$= 80\%$ ($\approx 48.67\%$)	$= 0\%$	≈ 0.263 *sec*	≈ 0.462 *sec*
$= 11$	$= 73\%$ ($\approx 40.20\%$)	$= 0\%$	≈ 0.351 *sec*	≈ 0.539 *sec*
$= 12$	$= 68\%$ ($\approx 32.40\%$)	$= 0\%$	≈ 0.447 *sec*	≈ 0.624 *sec*

[3] Neurotechnology Ltd. Verifinger SDK 5.0, `http://www.neurotechnology.com`.

[4] The minutiae templates were absolutely pre-aligned using the directed reference points estimated by our method. Each pre-aligned minutiae template was quantized as a subset of a finite field with at most $t_{\max} = 44$ elements using a hexagonal grid of distance $\lambda = 29$ centered in $[-559, 559] \times [-559, 559]$, which covers the region in where minutiae locations can occur. The minutiae angles were quantized into $s = 6$ quanta.



(a) (b) (c) (d) (e) (f)

Figure 3: Excerpt from the training — The core (green diamond) and the direction of the longitudinal axis (bold yellow line) give the location and the direction, respectively, of the estimated directed reference point. The blue lines correspond to the orientation of the tented arch. Their transparencies indicate the weight of which the orientations around the core were taken into account.

Using the parameter configuration determined during training, we ran performance evaluations with absolutely pre-aligned minutiae templates following the FVC protocol. We measured the genuine acceptance rate (GAR), false acceptance rate (FAR), avg. time on genuine decoding (GDT), and avg. time on impostor decoding (IDT). In order to allow comparison with other implementations of fingerprint cryptosystems, e.g., [NJP07,NNJ10, LYC$^+$10], we also kept track of the genuine acceptance rate ($\mathrm{sub\text{-}GAR}$) accounting only for the first two impressions of each finger. The results can be found in Table 1. We furthermore observed, that the avg. time for estimating a fingerprint's directed reference point with our implementation (including orientation field estimation and segmentation) was ≈ 3.05 *sec* per fingerprint. If for a fingerprint the estimation of a valid reference point failed, it was not taken into account, neither for enrollment nor for authentication. For 2.5% of the finger a pre-alignment failure were reported while for the sub-database no pre-alignment failure was reported. As a consequence, the GARs and $\mathrm{sub\text{-}GAR}$s have been measured from $2,562$ and 100 observed genuine authentication attempts, respectively. The FARs were measured from $4,950$ impostor authentication attempts.

4.3 Security

In this section, we give a brief security discussion for the above cryptosystem with absolute pre-alignment. For more details, we refer to [Tam13]. First, we note that the implementation is resistant against cross-matching via correlation and the correlation attack. Second, our implementation's resistance against brute-force attacks is at least as in [Tam13]. Thus, for simplicity, we assume the same number of chaff points $n = 1,452$ if we analyze our construction against brute-force attacks. However, analyses of false-accept attacks correspond to a more realistic estimate of the system's overall security. We used the method in [Tam13] to estimate false-accept security. The results can be found in Table 2.

(a) (b) (c) (d) (e) (f)

Figure 4: Excerpt from the evaluation — The estimated directed reference points are quite robust (a)-(c) and our method has the potential to work even for arches (d)-(f).

(a) (b) (c) (d) (e) (f)

Figure 5: (a)–(c) Examples where the estimation of the directed reference point was evidently unstable because of the fingerprint ridge flow being not well tented. (d)–(f) Examples where failures were reported due to the fingers being not well provided by the users.

Table 2: Security evaluation — The times correspond to a 3.2 `Ghz` desktop computer using a single processor core.

secret size k	brute-force security $\binom{44}{k}/\binom{1,452}{k}$	**false-accept security** FAR (for $\mathcal{D}=1$)	expected time for a successful brute-force-attack	**expected time for a successful false-accept attack**
$=7$	$\approx 2^{-36}$	$\approx 2^{-22}$	≈ 2 *days*	≈ 9 *sec*
$=8$	$\approx 2^{-41}$	$\approx 2^{-24}$	3–4 *months*	≈ 1 *min*
$=9$	$\approx 2^{-47}$	$\approx 2^{-27}$	≈ 14 *years*	≈ 11 *min*
$=10$	$\approx 2^{-52}$	$\approx 2^{-30}$	≈ 703 *years*	1–2 *hours*
$=11$	$\approx 2^{-57}$	$\approx 2^{-33}$	$\approx 35,198$ *years*	13–14 *hours*
$=12$	$\approx 2^{-63}$	$\approx 2^{-36}$	$\approx 1,78 \cdot 10^6$ *years*	5–6 *days*

5 Discussion

In this paper, we discussed a countermeasure to information leakage from auxiliary alignment data in minutiae-based cryptosystems. As a proof of concept, we performed test

with a cross-matching resistant cryptosystem protecting absolutely pre-aligned minutiae templates. Therefore, we proposed a new method for automatically estimating a directed reference point from a fingerprint which yields a method for absolutely pre-aligning fingerprints. Another nearby approach is to protect alignment-free features as in [LYC+10] but it is not yet clear how cross-matching resistance can be ensured for such implementations and how this would affect the authentication performances. Currently, the authentication rates that we achieved with absolute pre-alignment are clearly inferior to authentication rates achievable in a well-solved alignment framework (compare Table 1 with Table 5 in [Tam13]). However, the method for estimating a directed reference point and the biometric template protection scheme are building blocks which can be replaced by possibly more robust implementations. The search for methods improving the authentication rates of biometric cryptosystems protecting absolutely pre-aligned minutiae will be part of our future research. Finally, we stress that single-finger cryptosystems are currently not sufficient for providing a reasonable amount of security at a usable genuine acceptance rate (e.g., see Table 2). Our research has the purpose to yield to and to improve multi-finger cryptosystems—or even systems for protecting multiple biometric modalities. First steps have already been made, e.g., see [MIK+11, NNJ12].

References

[BG01] Bazen and Gerez. An Intrinsic Coordinate System for Fingerprint Matching. In *Proc. Int. Conf. on Audio- and Video-based Biometric Person Authentication*, pages 198–204, 2001.

[DORS08] Dodis, Ostrovsky, Reyzin, and Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM J. Comput.*, 38(1):97–139, 2008.

[HHM08] Huckemann, Hotz, and Munk. Global Models for the Orientation Field of Fingerprints: An Approach Based on Quadratic Differentials. *IEEE Trans. Pattern Anal. Mach. Intell.*, 30(9):1507–1519, 2008.

[Hot09] Hotz. Intrinsic Coordinates for Fingerprints Based on their Longitudinal Axis. In *Proc. Int. Symp. on Image and Signal Processing and Analysis*, pages 501–504, 2009.

[JA07] Jeffers and Arakala. Fingerprint Alignment for a Minutiae-Based Fuzzy Vault. In *Proc. Biometrics Symp.*, pages 1–6, 2007.

[JS02] Juels and Sudan. A Fuzzy Vault Scheme. In A. Lapidoth and E. Teletar, editors, *Proc. Int. Symp. Inf. Theory*, page 408, 2002.

[JW99] Juels and Wattenberg. A fuzzy commitment scheme. In *Proc. of ACM Conf. on Computer and Communications Security*, pages 28–36, 1999.

[KBK+11] Kelkboom, Breebaart, Kevenaar, Buhan, and Veldhuis. Preventing the Decodability Attack Based Cross-Matching in a Fuzzy Commitment Scheme. *IEEE Trans. Inf. Forensics Security*, 6(1):107–121, 2011.

[KW87] Kass and Witkin. Analyzing oriented patterns. *Computer Vision, Graphics, and Image Processing*, 37(3):362–385, 1987.

[KY08] Kholmatov and Yanikoglu. Realization of Correlation Attack Against the Fuzzy Vault Scheme. In *Proc. SPIE*, volume 6819, 2008.

[LYC+10] Li, Yang, Cao, Tao, Wang, and Tian. An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. *J. Netw. Comput. Appl.*, 33:207–220, May 2010.

[LYT+08] Li, Yang, Tian, Shi, and Li. Topological structure-based alignment for fingerprint Fuzzy Vault. In *Proc. Int. Conf. on Pattern Recognition*, pages 1–4, 2008.

[MIK+11] Merkle, Ihmor, Korte, Niesing, and Schwaiger. Performance of the Fuzzy Vault for Multiple Fingerprints (Extended Version). *CoRR*, abs/1008.0807v5, 2011.

[MMC+02] Maio, Maltoni, Cappelli, Wayman, and Jain. FVC2002: Second Fingerprint Verification Competition. In *Proc. Int. Conf. on Pattern Recognition*, pages 811–814, 2002.

[MMJP09] Maltoni, Maio, Jain, and Prabhakar. *Handbook of Fingerprint Recognition*. Springer Publishing Company, Incorporated, 2nd edition, 2009.

[MMT09] Mihăilescu, Munk, and Tams. The Fuzzy Vault for Fingerprints is Vulnerable to Brute Force Attack. In *Proc. of BIOSIG*, pages 43–54, 2009.

[NJP07] Nandakumar, Jain, and Pankanti. Fingerprint-Based Fuzzy Vault: Implementation and Performance. *IEEE Trans. Inf. Forensics Security*, 2(4):744–757, 2007.

[NK98] Novikov and Kot. Singular Feature Detection and Classification of Fingerprints Using Hough Transform. In *Proc. SPIE*, volume 3346, pages 259–269, 1998.

[NNJ10] Nagar, Nandakumar, and Jain. A hybrid biometric cryptosystem for securing fingerprint minutiae templates. *Pattern Recogn. Lett.*, 31:733–741, June 2010.

[NNJ12] Nagar, Nandakumar, and Jain. Multibiometric Cryptosystems Based on Feature-Level Fusion. *IEEE Trans. Inf. Forensics Security*, 7(1):255–268, 2012.

[RA00] Krisakorn Rerkrai and Vutipong Areekul. A New Reference Point for Fingerprint Recognition. In *Proc. Int. Conf. on Image Processing*, 2000.

[SB07] Scheirer and Boult. Cracking Fuzzy Vaults and Biometric Encryption. In *Proc. of Biometrics Symp.*, pages 1–6, 2007.

[Tam13] Tams. Attacks and Countermeasures in Fingerprint Based Biometric Cryptosystems. *CoRR*, abs/1304.7386v1, 2013. in revision.

[Tru11] Trugenberger. The Glass Maze: Hiding Keys in Spin Glasses. In *Proc. of BIOSIG*, pages 89–102, 2011.

[UJ06] Uludag and Jain. Securing fingerprint template: fuzzy vault with helper data. In *Proc. Workshop on Privacy Research In Vision*, pages 163–169, 2006.