

# Minutia-pair spectral representations for fingerprint template protection

Taras Stanko and Boris Škorić  
Eindhoven University of Technology, The Netherlands

## Abstract

We introduce a new fixed-length representation of fingerprint minutiae, for use in template protection. It is similar to the ‘spectral minutiae’ representation of Xu et al. but is based on coordinate differences between pairs of minutiae. Our technique has the advantage that it does not discard the phase information of the spectral functions. We show that the fingerprint matching performance (Equal Error Rate) is comparable to that of the original spectral minutiae representation, while the speed is improved.

## 1 Introduction

### 1.1 Privacy-preserving storage of biometric data

Biometrics-based authentication has become popular because of its great convenience. Biometrics cannot be forgotten or accidentally left at home. While biometric data is not strictly speaking secret (we are after all leaving a trail of fingerprints, DNA etc. behind us), it is important to protect biometric data for various reasons, the most important of which is privacy. Unprotected storage of biometric data would reveal medical conditions and would allow for cross-matching entries in different databases. Furthermore, large-scale availability of biometric data would make it easier for malevolent parties to leave misleading traces at a crime scene. (E.g. artificial fingerprints [10], synthesized DNA [7].)

One of the easiest ways to properly protect a biometric database against breaches and insider attacks is to store biometrics in *hashed* form, just like passwords, but with the addition of an error-correction step to get rid of the measurement noise. To prevent critical leakage from the error correction redundancy data, one uses a *Helper Data System* (HDS) [9, 5, 12], for instance a *Fuzzy Extractor* or a *Secure Sketch* [8, 6, 4].

A HDS typically makes use of an error-correcting code and hence needs a *fixed-length representation* of the biometric. Such a representation is not straightforward when the measurement noise can cause features of the biometric to appear or disappear, due to e.g. occlusion of iris areas or fuzziness of fingerprint minutiae. A very useful fixed-length representation called *spectral minutiae* was introduced by Xu et al. [17, 14, 15, 16]. A Fourier-like spectral function is built up on a fixed discrete grid, in such a way that each detected fingerprint minutia adds a contribution to the function. Com-

parison of spectral functions is robust against changes in the number of available biometric features.

### 1.2 Contributions and outline

We have the following results regarding spectral representations of fingerprint minutiae.

- We introduce spectral functions based on pairs of minutiae. By working with coordinate *differences* we immediately obtain a translation-invariant representation. Whereas Xu et al.’s spectral functions have to discard phase information in order to achieve translation invariance, our method retains phase information.
- We test our pair-based spectral minutiae matching technique on two fingerprint databases. The achieved Equal Error Rate is comparable to Xu et al.
- Our fingerprint matching is faster even though we have to sum over minutia pairs instead of individual minutiae. The speedup is due to the fact that we need fewer grid points on which to compute the spectral function.
- A further speedup can be obtained by skipping one laborious step in the verification procedure: rotating the fingerprint so as to obtain optimal alignment with the enrolled fingerprint. Skipping this step leads only to a minimal penalty in terms of False Acceptance Rate and False Rejection Rate.

In Section 2 we briefly review Helper Data Systems and spectral minutiae functions. In Section 3 we discuss the drawbacks of Xu et al.’s spectral minutiae technique. We introduce our minutia pair approach in Section 4, and we study its fingerprint matching performance in Section 5. Section 6 discusses the computational efficiency of the verification procedure.

## 2 Preliminaries

### 2.1 Notation and terminology

We denote the number of minutiae found in a fingerprint by  $Z$ . The coordinates of the  $j$ ’th minutia are  $x_j, y_j$  and its orientation is  $\theta_j$ . Let  $f$  be a function of two real-valued arguments. The two-dimensional Fourier transform  $\tilde{f} = \mathcal{F}f$  is defined as  $\tilde{f}(k_x, k_y) = \int_{-\infty}^{\infty} f(x, y) e^{-ik_x x - ik_y y} dx dy$ .

The inverse relation  $f = \mathcal{F}^{-1}\tilde{f}$  is given by  $f(x, y) = (\frac{1}{2\pi})^2 \int_{-\infty}^{\infty} \tilde{f}(k_x, k_y) e^{ik_x x + ik_y y} dk_x dk_y$ .

The complex conjugate of  $z \in \mathbb{C}$  is written as  $z^*$ . The hermitean conjugate  $M^\dagger$  of a matrix  $M$  is given by  $(M^\dagger)_{ij} = M_{ji}^*$ . The inner product of two complex vectors  $u, v$  is  $\langle u, v \rangle = u^\dagger v$ . The Pearson correlation coefficient of two length- $n$  vectors is defined as  $\rho(u, v) = \frac{1}{n} \langle \frac{u - u_{av}}{\sigma_u}, \frac{v - v_{av}}{\sigma_v} \rangle$ , where  $u_{av} = \frac{1}{n} \sum_i u_i$  and  $\sigma_u^2 = \frac{1}{n} \sum_i |u_i - u_{av}|^2$ .

We will use the abbreviations FR = False Reject, FRR = False Reject Rate, FA = False Accept, FAR = False Accept Rate, EER = Equal Error Rate, ROC = Receiver Operating Characteristic.

## 2.2 Helper Data Systems

A Helper Data System (HDS) for a (possibly non-discrete) source consists of two functions, **Gen** and **Rec**. Given an enrollment measurement  $X$  of the source, **Gen** produces redundancy data  $W \in \{0, 1\}^*$  called *helper data* and a secret string  $S$ . The helper data is stored. The storage is considered insecure, i.e. attackers learn  $W$ . At some later time, a verification measurement is performed, yielding outcome  $X' \approx X$  which is a noisy version of  $X$ . The **Rec** function takes as input  $X'$  and  $W$ . It outputs an estimator  $\hat{S}$  which should equal  $S$  if the noise was not excessive. In a general HDS, there is no constraint on the distribution of  $S$ . A desirable property is that  $S$  has high entropy given  $W$ .

A HDS is the perfect primitive for privacy protection of biometric databases against inside attackers and intruders, who typically obtain access not only to stored data but also to decryption keys. The HDS creates a noiseless secret and thus makes it possible to protect biometric secrets in the same way as passwords: by hashing. For every enrolled user, the database contains  $W$  and a hash  $\chi(S)$ . In the verification phase, the hash of the reconstructed  $\hat{S}$  is compared against the stored  $\chi(S)$ . Ideally,  $W$  contains just enough information to allow for the error correction, and does not leak any privacy-sensitive information about the raw biometric  $X$ . Furthermore, if  $\chi$  is a properly chosen one-way function and  $S$  has enough entropy given  $W$ , the hash value  $\chi(S)$  does not reveal  $S$ .

HDSs for discrete sources [2, 8, 3, 6, 4] and continuum sources [9, 13, 5, 12] are a well studied topic. Typically a HDS uses an error correcting code, which requires that the biometric measurement is turned into a discrete fixed-length representation.

## 2.3 Spectral representation of minutiae

Subsequent measurements of the same finger may not always result in the same set of observed minutiae. This is problematic if one needs a fixed-length representation of a fingerprint, e.g. when a HDS is used. The technique of *spectral minutiae* was introduced by Xu et al. [17, 14, 15] as a way to obtain a fixed-length representation. The set of enrolled minutiae is turned into a function  $f_\sigma(x, y)$  on the  $xy$ -plane by summing narrow Gaussian peaks (with width  $\sigma$ ) centered on the

minutia locations; then a translation-invariant expression  $g_\sigma$  is obtained by taking the absolute value of the Fourier transform,

$$g_\sigma(k_x, k_y) = |\tilde{f}_\sigma(k_x, k_y)| = e^{-\frac{\sigma^2}{2}(k_x^2 + k_y^2)} \left| \sum_{j=1}^Z e^{-ik_x x_j - ik_y y_j} \right|. \quad (1)$$

In order to get an expression with simple behaviour under rotation and scaling, they sampled  $g_\sigma$  on a log-polar grid. Let  $k_x(\alpha, \beta) = e^\alpha \cos \beta$  and  $k_y(\alpha, \beta) = e^\alpha \sin \beta$  where  $\alpha, \beta$  are sampled with equal spacing. A matrix  $G^\sigma$  is constructed as  $G_{\alpha\beta}^\sigma = g_\sigma(k_x(\alpha, \beta), k_y(\alpha, \beta))$ . Under the combination of

scaling and rotation,  $\begin{pmatrix} x_j \\ y_j \end{pmatrix} \mapsto \begin{pmatrix} \cos \varphi & \sin \varphi \\ -\sin \varphi & \cos \varphi \end{pmatrix} \begin{pmatrix} \lambda x_j \\ \lambda y_j \end{pmatrix}$  for all  $j$ ,

the  $G^\sigma$  transforms as  $G_{\alpha\beta}^\sigma \mapsto G_{\alpha + \ln \lambda, \beta + \varphi}^{\sigma/\lambda}$ . For small  $\sigma$  it holds that  $\sigma/\lambda \approx \sigma$  and hence the transform is almost equal to a shift on the  $\alpha\beta$ -grid.<sup>1</sup> Xu et al. investigated fingerprint matching in the spectral minutiae domain by looking at the Pearson correlation between a freshly obtained  $G^\sigma$  and the enrolled  $G^\sigma$ . Their procedure included a search to find values  $\lambda, \varphi$  that maximise the correlation. It turned out that in practice one can fix  $\lambda = 1$  and that the  $\varphi$ -search can be restricted to the interval from  $-10^\circ$  to  $+10^\circ$ , in steps of  $2^\circ$ .

In order to extract more information from a fingerprint Xu et al introduced a variant of the  $g_\sigma$  function which contains information about the minutia orientations  $\theta_j$ . They inserted a factor  $(k_x \cos \theta_j + k_y \sin \theta_j)$  or  $e^{i\theta_j}$  into the summation in  $g_\sigma$  (1). Unsurprisingly, using information from both the ordinary  $G^\sigma$  representation and the orientation-containing variant yielded better results (in terms of e.g. ROC curves and EER) than using only a single representation.

Xu et al also investigated a minutiae representation that is fully invariant under translation, rotation and scaling. Let  $H^\sigma = \mathcal{F}G^\sigma$  be the discrete Fourier transform of  $G_{\alpha\beta}^\sigma$  with respect to  $\alpha$  and  $\beta$ ; then scalings and rotations have the effect of merely producing a phase factor multiplying  $H^\sigma$ ; the absolute value  $|H^\sigma|$  is fully invariant. However, it turned out that fingerprint matching in the  $|H^\sigma|$ -domain does not perform well.

## 3 Motivation

The spectral minutiae technique as developed by Xu et al [17, 14, 15] has a number of unsatisfactory aspects.

1. Translation invariance is obtained by taking the absolute value of a Fourier transform. This step discards a lot of information.
2. Xu et al conclude that the scaling factor  $\lambda$  does not have to be taken into account, since it is always close to 1. But in their best fingerprint matching implementation they still apply logarithmic sampling in the radial  $k$ -direction,

<sup>1</sup> The effect on  $\sigma$  was not explicitly mentioned in the work of Xu et al.

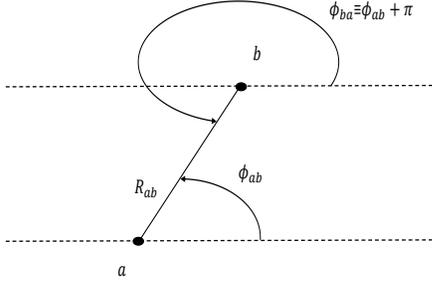


Figure 1: Distance  $R_{ab}$  and angle  $\varphi_{ab}$  for a minutia pair.

$\sqrt{k_x^2 + k_y^2} = e^\alpha$ . Such sampling does not match the radial information density in the fingerprint and hence makes it necessary to take many many samples than in the case of linear sampling.

3. In combination with a HDS, the  $\varphi$ -search is time consuming. This is caused not by the repeated re-computation of the score, but by the fact that in a full HDS every  $\varphi$ -attempt needs an evaluation of the Rec function and the computation of a hash.

We address the first issue by introducing a spectral representation that is based on coordinate differences  $\mathbf{x}_a - \mathbf{x}_b$  only. The advantage is immediate translation invariance without information loss, enabling us to work with fewer samples. The drawback is that each summation over  $Z$  minutiae is replaced by a summation over  $\binom{Z}{2}$  pairs. The overall effect on the computation time during reconstruction is a tradeoff between these two. In Section 6 we show that the tradeoff works in our advantage.

We address the second issue by performing a Fourier transform *only in the angular direction*. In the radial direction our sampling occurs in the spatial domain and is linear.

The third issue could be addressed by developing a method to quickly determine the global orientation of a captured fingerprint image. (Knowledge of the global orientation, even if inaccurate, reduces the search space. Furthermore, storing the global orientation during enrolment as helper data does not leak sensitive information.) However, with our pair-based spectral representation it turns out that executing the  $\varphi$ -search yields only a very modest performance improvement; the search may as well be omitted. In Section 5.3 we show the difference in performance.

## 4 The minutia-pair approach

### 4.1 Definitions and properties

Let  $R_{ab} = |\mathbf{x}_a - \mathbf{x}_b|$  and let  $\tan \varphi_{ab} = (y_a - y_b)/(x_a - x_b)$  for minutiae  $a, b \in \{1, \dots, Z\}$ . See Fig. 1. We define two

translation-invariant spectral functions as follows

$$L_{\mathbf{x}}(q, w) \stackrel{\text{def}}{=} \sum_{\substack{a, b \in \{1, \dots, Z\} \\ a \neq b}} e^{iq\varphi_{ab}} e^{iw \ln R_{ab}} \quad (2)$$

$$L_{\mathbf{x}\theta}(q, w) \stackrel{\text{def}}{=} \sum_{\substack{a, b \in \{1, \dots, Z\} \\ a \neq b}} e^{iq\varphi_{ab}} e^{iw \ln R_{ab}} e^{i(\theta_a - \theta_b)}. \quad (3)$$

Here the subscript  $\mathbf{x}$  denotes the set of minutia locations, and likewise  $\theta$  stands for the set of minutia orientations. We call the functions  $L_{\mathbf{x}}, L_{\mathbf{x}\theta}$  ‘spectral’ because (2) is the Fourier transform (with respect to the radial coordinate  $\ln R$  and the angle  $\varphi$ ) of a sum of delta functions centered on the values  $\mathbf{x}_a - \mathbf{x}_b$  in the plane.

Let  $\Phi = \begin{pmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{pmatrix}$  be a rotation matrix. Our spectral functions (2),(3) have simple behaviour under the combined scaling and rotation  $\mathbf{x}_j \mapsto \lambda \Phi \mathbf{x}_j, \theta_j \mapsto \theta_j + \varphi$ ,

$$L_{\lambda \Phi \mathbf{x}}(q, w) = e^{iq\varphi} e^{iw \ln \lambda} L_{\mathbf{x}}(q, w) \quad (4)$$

$$L_{\lambda \Phi \mathbf{x}, \theta + \varphi}(q, w) = e^{iq\varphi} e^{iw \ln \lambda} L_{\mathbf{x}\theta}(q, w). \quad (5)$$

Note that the absolute values  $|L_{\mathbf{x}}(q, w)|, |L_{\mathbf{x}\theta}(q, w)|$  are invariant under translation, scaling and rotation. Without giving details we mention that, unfortunately, fingerprint matching based on  $|L_{\mathbf{x}}|, |L_{\mathbf{x}\theta}|$  without the phase information performs badly.

Similar to Xu et al we need to sample  $w$  at equally spaced steps in order to exploit the phase behaviour (4),(5) under scaling. However, if we choose to ignore scaling entirely (see point 2 in Section 3), then there is no reason to Fourier transform the radial direction, and we introduce an alternative spectral function,

$$M_{\mathbf{x}}(q, R) \stackrel{\text{def}}{=} \sum_{\substack{a, b \in \{1, \dots, Z\} \\ a \neq b}} e^{iq\varphi_{ab}} \exp \left[ -\frac{(R - R_{ab})^2}{2\sigma^2} \right] \quad (6)$$

$$M_{\mathbf{x}\theta}(q, R) \stackrel{\text{def}}{=} \sum_{\substack{a, b \in \{1, \dots, Z\} \\ a \neq b}} e^{iq\varphi_{ab}} \exp \left[ -\frac{(R - R_{ab})^2}{2\sigma^2} \right] e^{i(\theta_a - \theta_b)}. \quad (7)$$

In the radial direction, the functions  $M_{\mathbf{x}}$  and  $M_{\mathbf{x}\theta}$  consist of a sum of  $\binom{Z}{2}$  Gaussian peaks centered on the values  $R_{ab}$ . The width  $\sigma > 0$  reduces the scheme’s sensitivity to small perturbations in the minutia properties.

Under a rotation ( $\mathbf{x}_j \mapsto \Phi \mathbf{x}_j, \theta_j \mapsto \theta_j + \varphi$ ) we have  $M_{\mathbf{x}}(q, R) \mapsto e^{iq\varphi} M_{\mathbf{x}}(q, R)$  and  $M_{\mathbf{x}\theta}(q, R) \mapsto e^{iq\varphi} M_{\mathbf{x}\theta}(q, R)$ . We want all our spectral functions to be single-valued.<sup>2</sup> Hence  $q$  always has to be integer.

**Lemma 4.1.** *For odd  $q$  it holds that  $L_{\mathbf{x}}(q, w) = 0$  for all  $w$ , and  $M_{\mathbf{x}}(q, R) = 0$  for all  $R$ .*

*Proof.* In (2) every pair of indices  $a, b$  gives two terms in the summation. Using  $R_{ba} = R_{ab}$  and  $\varphi_{ba} \equiv \varphi_{ab} + \pi \pmod{2\pi}$  (see Fig. 1), we write  $e^{iq\varphi_{ab}} e^{iw \ln R_{ab}} + e^{iq\varphi_{ba}} e^{iw \ln R_{ba}} = e^{iq\varphi_{ab}} e^{iw \ln R_{ab}} [1 + e^{iq\pi}] = e^{iq\varphi_{ab}} e^{iw \ln R_{ab}} [1 + (-1)^q]$ . This vanishes when  $q$  is odd. The proof for  $M_{\mathbf{x}}$  is analogous.  $\square$

<sup>2</sup> Invariant under rotations  $\varphi$  that are an integer multiple of  $2\pi$ .

## 4.2 Choosing the grid points

We have to choose a discrete  $(q, w)$ -grid of points on which to evaluate  $L_x$  and  $L_{x\theta}$ . On the one hand, the grid should contain many points so that the spectral functions contain sufficient information about the fingerprint. On the other hand, having too many grid points results in an inefficient scheme. Lemma 4.1 tells us that we do not have to compute  $L_x$  for odd  $q$ . Furthermore, we know that, at a given  $q$ , the spectral functions detect angular periodic features of size  $\approx 2\pi/q$  radians. This leads to a natural cutoff at large  $q$  where the length scale becomes smaller than the feature size in a typical fingerprint, and noise starts to dominate. Similarly, there is a natural maximum for  $w$ , namely where  $2\pi/w$  matches  $\min_{ab:a \neq b} \ln R_{ab}$ . Finally we note that  $L_x(-q, -w) = L_x^*(q, w)$  and  $L_{x\theta}(-q, -w) = (-1)^q L_{x\theta}^*(q, w)$ . This means that the grid point  $(-q, -w)$  contains exactly the same information as  $(q, w)$  and hence can be omitted. The considerations listed above are the only theoretical guidelines for choosing the grid; the best choice must be found by trial and error.

The considerations for  $M_x, M_{x\theta}$  are similar. The grid is a  $(q, R)$ -grid. The maximum  $q$  should be roughly the same as for the  $L$ -functions. The natural cutoffs for  $R$  are given by  $\min_{ab:a \neq b} R_{ab}$  and  $\max_{ab} R_{ab}$ . It holds that  $M_x(-q, R) = M_x^*(q, R)$  and  $M_{x\theta}(-q, R) = (-1)^q M_{x\theta}^*(q, R)$ . Hence it suffices to look at positive  $q$  only.

## 4.3 Introducing weights

In the computation of a spectral function at enrollment, it is possible to introduce a weight factor for each of the  $(a, b)$ -pairs in the summation. It is advantageous to set a low weight for minutia pairs which are unlikely to be recovered later. A low recovery likelihood may occur e.g. when a minutia has low quality. Another reason can be a very large value of  $R_{ab}$ , in which case the recovery is sensitive to noise at the edge of the image, or a very small  $R_{ab}$  which may cause later minutia misidentification in case of noise. In our experiments we have not used weights other than 0 or 1.

## 4.4 Choosing the score function

Let  $F$  denote one of the four spectral functions  $L_x, L_{x\theta}, M_x, M_{x\theta}$  obtained at enrollment, and  $F'$  the noisy version of  $F$  obtained later, in the verification phase. We need a metric or ‘score’ function which quantifies how close  $F'$  is to  $F$ . As  $F$  and  $F'$  are complex-valued, there are quite some options. We have experimented with correlation functions for the radial and phase part of the complex numbers, as well as the real and imaginary part. Furthermore we have tried distance in the complex plane, with and without normalisation of the function  $F$  as a whole. In our experiments it turns out that a complex correlation-like quantity is best able to discriminate between genuine fingerprint matches and impostors. We define our score  $S$  as

$$S(F, F') = |\rho(F, F')| \quad (8)$$

where  $\rho$  stands for the correlation as defined in Section 2.1, and the matrices  $F, F'$  are treated as vectors.

## 4.5 Fusion of scores

The spectral functions  $L_x$  and  $L_{x\theta}$  together contain more information about the fingerprint than each one separately. The information is partially overlapping. We construct a ‘fused’ score by adding the two scores (8) in the same way as [17]:  $S(L_x, L'_x) + S(L_{x\theta}, L'_{x\theta})$ . Analogously, for the  $M$ -functions we work with the fused score  $S(M_x, M'_x) + S(M_{x\theta}, M'_{x\theta})$ .

# 5 Experimental results

We have applied our minutia-pair approach to the Verifinger database and the MCYT database [11]. The Verifinger database contains fingerprints from six individual persons, ten fingers per individual, eight images per finger. The size of each image is  $326 \times 357$  pixels. The MCYT database contains fingerprints from 100 individuals, 10 fingers per individual, 12 images per finger ( $256 \times 400$  pixels). The fingerprints are generally of higher quality than in the Verifinger database.

We extracted minutia coordinates and orientations from the images by using the VeriFinger software [1].

## 5.1 Optimal parameter choices

Good results were obtained with the following parameter settings. For the  $L$ -functions,  $|q| \in \{1, \dots, 24\}$  and  $w \in [0.2, 37.7]$  with 32 equally spaced values. For the  $M$ -functions,  $q \in \{1, \dots, 16\}$ ;  $R \in [16, 130]$  with 20 equally spaced points (MCYT database);  $R \in [16, 160]$  with 25 equally spaced points (Verifinger database). For the  $L_x$  and  $M_x$  functions we take only even  $q$ , as explained in Lemma 4.1. We set  $\sigma = 2.3$  pixels.

A minutia extracted by VeriFinger is labeled with a quality  $Q \in [0, 100]$ . We took only minutiae with  $Q \geq 45$ . Furthermore we used an additional selection rule that turns out to improve overall results a bit: a minutia pair is discarded from the  $\sum_{ab}$  summation in (2,3,6,7) if  $2R_{ab}$  exceeds the horizontal size of the image.

In Fig. 2 we show an example of the  $M_x$  and  $M_{x\theta}$  spectral function. Entirely different fingers obviously produce very different results. The two leftmost columns correspond to the same finger. Noisy images of the same finger do not produce results that, to the human eye, are clearly correlated. However, it turns out (Section 5.2) that the similarities are enough to distinguish between the enrolled user from an impostor.

## 5.2 ROC curves and Equal Error Rates

We work in a *verification* setting, i.e. a stated identity has to be verified. We determine the False Rejection Rate (FRR) by comparing, for each finger in the database, all the pairs of

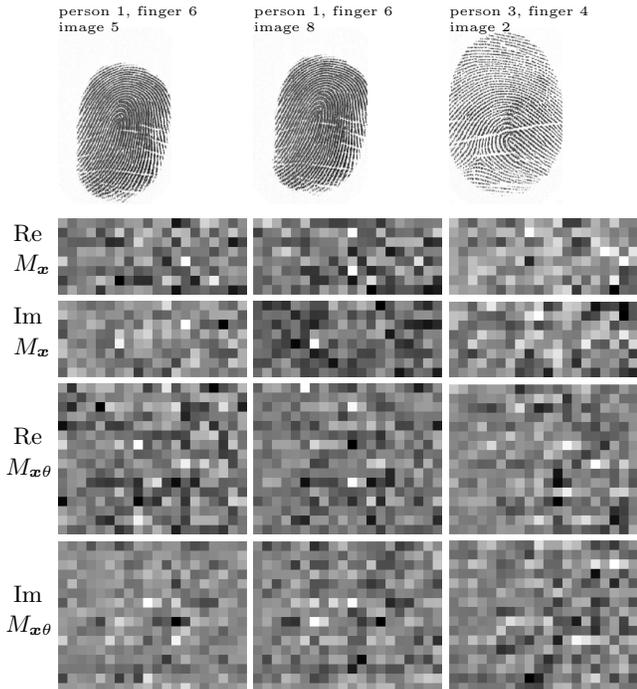


Figure 2: Example of the spectral functions  $M_{\mathbf{x}}$  and  $M_{\mathbf{x}\theta}$ . MCYT database. The vertical axis is the  $q$ -axis, with  $q$  increasing upward. In each image, black represents the most negative value on the grid, and white the most positive.

images. We determine the False Acceptance Rate (FAR) by looking at each pair of different fingers, where one image is drawn at random for each finger (independently per pair).<sup>3</sup> We draw Receiver Operating Characteristic (ROC) curves as FAR plotted against FRR. Each point in the ROC curve corresponds to one threshold setting. The Equal Error Rate (EER) is the error rate in the point where FRR equals FAR.

Table 1 lists the EER values that we obtained. The ROC curves are shown in Fig. 3. We see that the  $M$ -functions consistently outperform the  $L$ -functions, and that the  $L_{\mathbf{x}\theta}$ ,  $M_{\mathbf{x}\theta}$  spectral functions outperform the location based functions. Furthermore we see that fusion of  $M_{\mathbf{x}}$  and  $M_{\mathbf{x}\theta}$  yields only a modest improvement over  $M_{\mathbf{x}\theta}$ . We conclude that, in our pair-based approach, the best option is to work either with  $M_{\mathbf{x}\theta}$  or the fusion of  $M_{\mathbf{x}}$  and  $M_{\mathbf{x}\theta}$ .

We benchmark our system against results reported by Xu et al. [17], which are based on ten individuals in the MCYT database who have high-quality fingerprint images. The ROC curves are shown in Fig. 4, and Table 2 contains the EER comparison.<sup>4</sup> We conclude that our pair-based spectral function  $M_{\mathbf{x}\theta}$  has a discrimination performance comparable to Xu et al.’s spectral function.

<sup>3</sup> This includes pairs of unlike fingers, e.g. thumb vs index finger. The statistics do not change much when only pairs of like fingers are compared.

<sup>4</sup> Unfortunately, [17] does not mention which ten individuals were selected.

Table 1: Equal Error Rates obtained with the parameter settings given in Section 5.1. The notation ‘ $F$ ’ stands for either  $L$  or  $M$ . No rotation of the verification image.

Database	Function $F$	$F_{\mathbf{x}}$	$F_{\mathbf{x}\theta}$	Fusion
MCYT	$L$	5.3%	3.5%	3.0%
	$M$	4.0%	2.5%	2.2%
Verifinger	$L$	11%	4.9%	5.7%
	$M$	8.0%	3.3%	3.2%

Table 2: Equal Error Rates for a subset of ten individuals in the MCYT database who have high-quality fingerprints. No rotation of the verification image. The last row is from Table VI in [17]. The  $L$  and  $M$  function were computed for individuals 16,24,26,32,34,35,46,53,80,94.

Function $F$	$F_{\mathbf{x}}$	$F_{\mathbf{x}\theta}$	Fusion
$L$	1.1%	0.73%	0.31%
$M$	0.65%	0.35%	0.15%
Xu et al	0.47%	0.42%	0.22%

### 5.3 Rotation of the verification image

The results of Section 5.2 were obtained without Xu et al.’s procedure of trying out several image rotations so as to optimise the matching score. Now we discuss what happens when we do try a number of different rotation angles  $\varphi$ .

First we checked for the MCYT and the VeriFinger database how a rotation  $\varphi \in (-10^\circ, +10^\circ)$  affects the  $M_{\mathbf{x}}$  and  $M_{\mathbf{x}\theta}$ -based score in case of a genuine image pair. At some optimal angle  $\varphi_0$  the score is maximal. For all genuine pairs we determined  $\varphi_0$ , for  $M_{\mathbf{x}}$  and  $M_{\mathbf{x}\theta}$ . The histograms of  $\varphi_0$  are shown in Fig. 5. We see that typically  $|\varphi_0| < 6^\circ$ .

In Fig. 6 we present ROC curves that show the impact of trying multiple rotation angles  $\varphi$  in a limited range; we set the range based on Fig. 5. In the case of the MCYT database we see a consistent though small improvement. For the VeriFinger database the change is not always favourable; the ROC curves intersect. For both databases, the effect on the EER is minimal.

Increasing the range of  $\varphi$  does not improve the matching of genuine pairs; it does however increase the FAR. Hence the ROC curves become worse when we increase the range of  $\varphi$ . These results allow for a very interesting trade-off: instead of opting for a minimal improvement of matching accuracy, we can skip the  $\varphi$ -search and thus significantly reduce the computation time. Note that Xu et al.’s method has a  $\varphi$ -search with 11 different values of  $\varphi$ .

## 6 Computational efficiency

*In this analysis we do not use the potential speedup that can be gained by skipping the  $\varphi$ -search.*

Speed is important predominantly in the verification phase. From a freshly captured image the spectral function has to be computed on a number of grid points which we denote as  $N_{\text{gr}}$ . The spectral function has to be computed not once but several times, because  $N_{\varphi}$  different image orientations have to be tried. Fortunately this does not multiply the total effort<sup>5</sup> by a factor  $N_{\varphi}$ , as the spectral function has a simple transform under rotation. (This holds for Xu et al as well as our  $L$  and  $M$  functions.)

Let  $Z$  be the number of minutiae. Let us denote the cost of computing one summation term of the spectral function in one grid point as  $T_s$ , and the cost of applying a rotation transform in one grid point as  $T_{\text{rot}}$ . The cost of computing the score can be written as  $c \cdot N_{\text{gr}}$  where  $c$  is some small constant. The superscript ‘ $G$ ’ will refer to Xu et al’s spectral function; the superscript ‘ $M$ ’ to our function  $M$ . The total cost for the verification phase (not counting the secure sketch) is

$$\begin{aligned} \text{Xu et al: } & N_{\text{gr}}^G Z T_s^G + (N_{\varphi} - 1) N_{\text{gr}}^G T_{\text{rot}}^G + N_{\varphi} c N_{\text{gr}}^G \\ \text{pair-based: } & N_{\text{gr}}^M \binom{Z}{2} T_s^M + (N_{\varphi} - 1) N_{\text{gr}}^M T_{\text{rot}}^M + N_{\varphi} c N_{\text{gr}}^M. \end{aligned}$$

We have  $T_s^G \approx T_s^M$ ,  $T_{\text{rot}}^G \approx T_{\text{rot}}^M$ ,  $T_{\text{rot}} < T_s$ . The main difference between the two approaches lies in the first term:  $N_{\text{gr}}^G Z$  versus  $N_{\text{gr}}^M \binom{Z}{2}$ , i.e.  $N_{\text{gr}}^G$  versus  $\frac{1}{2} N_{\text{gr}}^M (Z - 1)$ . Xu et al report a  $128 \times 256$  grid, yielding  $N_{\text{gr}}^G = 32768$ . In contrast, our  $M_{\mathbf{x}\theta}$ -function is evaluated on a grid of size  $N_{\text{gr}}^M \leq 16 \cdot 25 = 400$ . Given that typically  $Z \approx 35$ , we have  $\frac{1}{2} N_{\text{gr}}^M (Z - 1) \approx 6800$ . Hence our verification is faster than [17, 14, 15].

Note that [16] introduces a reduced template size by applying Principal Component Analysis or a Discrete Fourier Transform to select informative features. This selection reduces the template size by roughly a factor 10. However, these methods still require computation of the spectral function on many grid points.

## 7 Discussion

Achieving translation invariance by looking at *minutia pairs* seems to be advantageous compared to taking the absolute value of a Fourier transform. The minutia-pair approach is able to extract information from a fingerprint using fewer grid points. We conjecture that this is due to the fact that our spectral functions retain phase information instead of discarding it. Of the four functions that we studied, the  $M_{\mathbf{x}\theta}$  performs best. Fusion of the matching scores from  $M_{\mathbf{x}}$  and  $M_{\mathbf{x}\theta}$  leads to an EER comparable to Xu et al.

Due to the reduction of the number of grid points our method is faster than the verification described by Xu et al., in spite of the increased number of summation terms. As an unexpected bonus, it turns out that we can omit the search for an optimal rotation angle; this gives an additional speed improvement.

<sup>5</sup> Here we look only at the computation of the spectral function and the score; not at the cost of  $N_{\varphi}$  Secure Sketch reconstruction attempts.

As topics for future work we mention (i) further speedup by discarding grid points that have a bad signal-to-noise ratio; (ii) applying Principal Component Analysis and similar techniques to improve the EER; (iii) constructing a HDS based on  $M_{\mathbf{x}}$  and  $M_{\mathbf{x}\theta}$ .

## References

- [1] VeriFinger SDK. Available online, [www.neurotechnology.com](http://www.neurotechnology.com).
- [2] C.H. Bennett, G. Brassard, C. Crépeau, and M. Skubiszewska. Practical quantum oblivious transfer. In *CRYPTO*, pages 351–366, 1991.
- [3] X. Boyen. Reusable cryptographic fuzzy extractors. In *ACM Conference on Computer and Communications Security*, pages 82–91, 2004.
- [4] R. Canetti, B. Fuller, O. Paneth, L. Reyzin, and A. Smith. Reusable fuzzy extractors for low-entropy distributions. In *Eurocrypt 2016*, 2016. [eprint.iacr.org/2014/243](http://eprint.iacr.org/2014/243).
- [5] J. de Groot, B. Škorić, N. de Vreede, and J.P. Linnartz. Quantization in Zero Leakage Helper Data Schemes. *EURASIP Journal on Advances in Signal Processing*, 2016. 2016:54.
- [6] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith. Fuzzy Extractors: how to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.*, 38(1):97–139, 2008.
- [7] D. Frumkin, A. Wasserstrom, A. Davidson, and A. Grafit. Authentication of forensic DNA samples. *FSI Genetics*, 4(2):95–103, 2010.
- [8] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *ACM Conference on Computer and Communications Security (CCS) 1999*, pages 28–36, 1999.
- [9] J.-P. Linnartz and P. Tuyls. New shielding functions to enhance privacy and prevent misuse of biometric templates. In *Audio- and Video-Based Biometric Person Authentication*. Springer, 2003.
- [10] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. Impact of artificial “gummy” fingers on fingerprint systems. In *Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques IV*, volume 4677, pages 275–289, 2002.
- [11] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez, V. Espinosa, A. Satue, I. Hernaez, J.J. Igarza, C. Vivaracho, D. Escudero, and Q.I. Moro. MCYT baseline corpus: A bimodal biometric database. In *Vision, Image and Signal Processing, Special Issue on Biometrics on the Internet*, volume 150, pages 395–401. IEEE, 2003.

- [12] T. Stanko, F.N. Andini, and B. Škorić. Optimized quantization in Zero Leakage Helper Data Systems, 2016. <https://eprint.iacr.org/2016/325>.
- [13] E.A. Verbitskiy, P. Tuyls, C. Obi, B. Schoenmakers, and B. Škorić. Key extraction from general nondiscrete signals. *IEEE Transactions on Information Forensics and Security*, 5(2):269–279, 2010.
- [14] H. Xu and R.N.J. Veldhuis. Spectral minutiae representations of fingerprints enhanced by quality data. In *Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS) 2009*. IEEE, 2009.
- [15] H. Xu and R.N.J. Veldhuis. Spectral representations of fingerprint minutiae subsets. In *Image and Signal Processing (CISP) 2009*, pages 1–5, 2009.
- [16] H. Xu and R.N.J. Veldhuis. Complex spectral minutiae representation for fingerprint recognition. In *Computer Vision and Pattern Recognition Workshop*. IEEE, 2010.
- [17] H. Xu, R.N.J. Veldhuis, A.M. Bazen, T.A.M. Kevenaar, A.H.M. Akkermans, and B. Gokberk. Fingerprint verification using spectral minutiae representations. *IEEE Transactions on Information Forensics and Security*, 4(3):397–409, 2009.

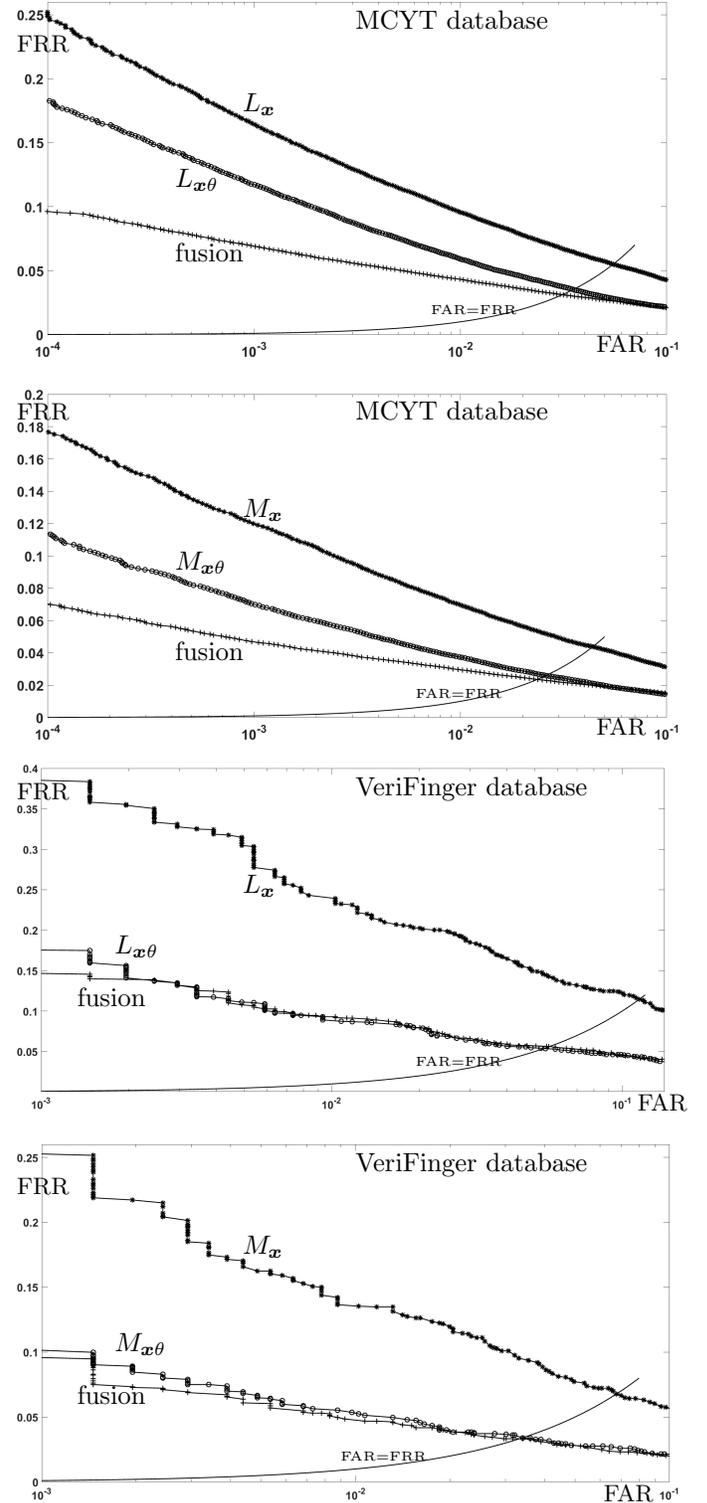


Figure 3: ROC curves for our pair-based spectral functions applied to two databases. No rotation of the verification image.

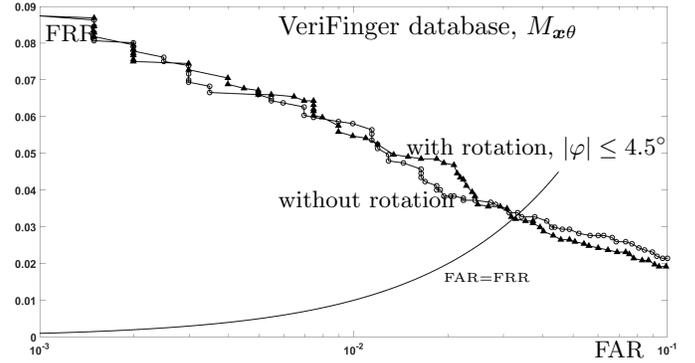
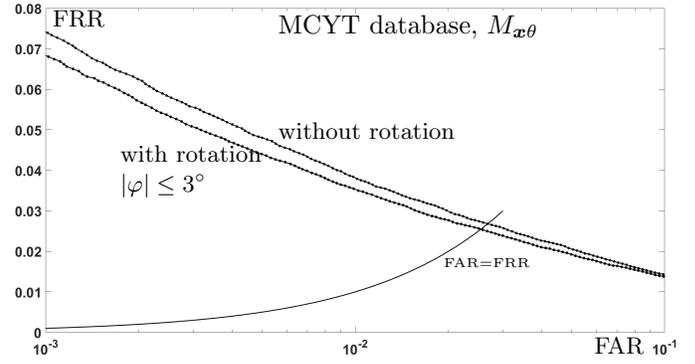
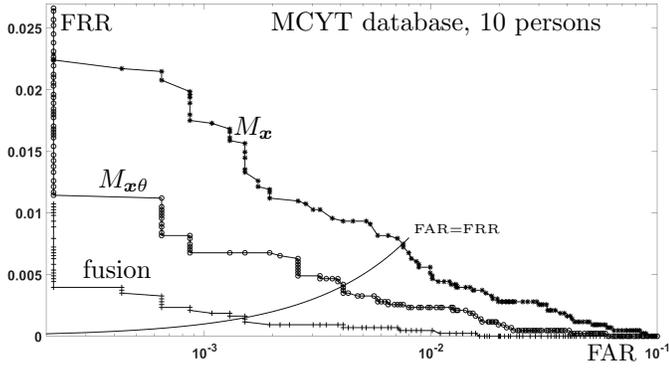
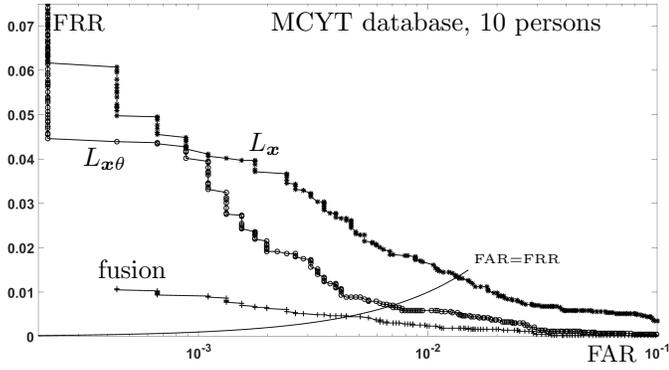


Figure 4: ROC curves for the ten-person subset of the MCYT database. No rotation of the verification image.

Figure 6: ROC curves with and without rotation of the verification image.

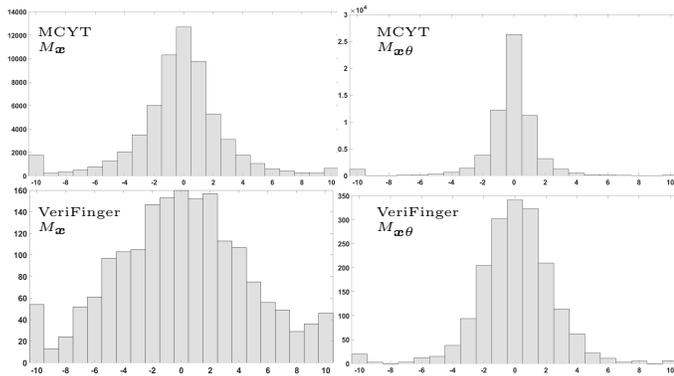


Figure 5: Histograms of the optimal rotation angle  $\varphi_0$  (degrees).