Minimizing the Impact of Low Interoperability between Optical Fingerprints Sensors

Emanuela Marasco, Luca Lugini, Bojan Cukic, Thirimachos Bourlai
West Virginia University, LDCSEE, PO BOX 6109, Morgantown, WV, 26505, U.S.A.
{emanuela.marasco,bojan.cukic,thirimachos.bourlai}@mail.wvu.edu, luligini@mix.wvu.edu

Abstract

In fingerprint recognition, interoperability is the ability of a system to work with a diverse set of fingerprint devices. Variations induced by fingerprint sensors include image resolution, scanning area, gray levels, etc. Such variations can impact (i) the quality of the extracted features, and (ii) cross-device matching performance. This is true even when dealing with fingerprint sensors of the same sensing technology (e.g. optical). Previous research did not provide a model to accommodate sensor distortions to increase cross-device matching performance. In this paper, we propose a method that increases interoperability in systems which deploy optical fingerprint sensors. We design and evaluate a set of characteristics suitable for measuring differences in fingerprint image acquisition. Further, we propose a classification scheme, which combines the defined features with match scores. The classification performance is evaluated on a set of fingerprints acquired using four different optical devices and scanned rolled ink prints, from approximately 500 *subjects. Experimental results confirm the significant impact of low interoperability on match rates and show that the proposed approach is able to reduce cross-device match error rates by a significant margin.*

1. Introduction

Fingerprints can be acquired through different sensing technologies. Among those, optical devices are the most commonly used [8]. The ease of use and low error rates are the main factors that contribute to their success. However, optical technology still presents some challenges. Performance of a fingerprint matcher is affected by variations introduced when acquiring fingerprint images from different devices (see Fig. 1). The ability of a biometric system to handle these variations is referred to as *interoperability*. The need for interoperability is accentuated by the competitive fingerprint sensor market, characterized by many vendors[1]. In optical sensors, the finger is placed on the surface of a transparent prism, typically illuminated from the left side. The light entering the prism is reflected in the valleys and absorbed at the ridges of a fingerprint. Some of the main factors that affect the performance of fingerprint sensing devices are (i) arrangements of sensing elements, (ii) sensor resolution, (iii) scanning area, and (iv) ability of users to properly interact with different sensors, i.e., how users position their fingerprints on the sensor surface. Characteristics of different devices from the same model/vendor can vary (e.g., each prism may distort differently). A realistic operational example is the US VISIT program, deployed at US international airports. There is no guarantee that the same device used for fingerprint acquisition will be used for verification as well [21]. Recently, an interoperability problem was observed in Automated Teller Machines (ATM) [13].

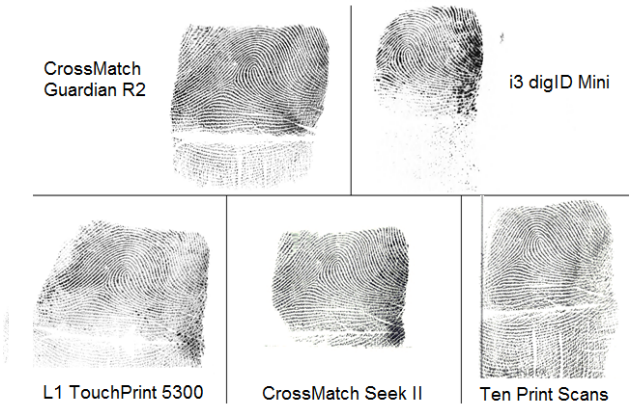


Figure 1. Fingerprint images pertaining to the same subject captured using different optical devices.

Biometric system should be able to handle variations in the biometric data due to the deployment of different capture devices [23]. The matching process accommodates diverse fingerprint images and discriminates genuine and im-

[1] http://pdf.marketpublishers.com/gia/fingerprintbiometrics_gia.pdf

postor presentations. However, performance variations are common. To the best of our knowledge, while previous research considered the problem of designing models for correcting the distortion from fingerprint deformation [3] [20], modeling sensor distortions to increase cross-device matching performance is a challenging area of research. The key question is: How well can we match fingerprints captured by different devices?

In this paper, we propose a methodology that increases interoperability in fingerprint recognition systems. First, we select a set of features to measure differences in fingerprint images captured using different devices; next, we design a fusion scheme that combines the defined features with match scores in order to improve the discrimination between genuine and impostor scores in cross-device matching. The approach is evaluated using a data set from 500 users, collected using four optical-based fingerprint sensors as well as ink rolled prints (baseline) at West Virginia University. The rest of the paper is organized as follows. In Section 2, we describe the state-of-the-art in the fingerprint interoperability accommodation strategies. Section 3 presents the proposed approach. Section 4 discusses the evaluation procedure and experimental results. Section 5 draws conclusions and future research directions.

2. Related Work

Recent work points out the importance of investigating the impact of diverse fingerprints capture platforms on match error rates. Poh *et al.* designed a Bayesian Belief Network (BBN) to estimate the posterior probability of the device d given quality q, referred to as $p(d|q)$ [17] [18]. During testing, the device is unknown and it is identified based on the quality measures extracted from the images. Clustering is applied to each device to explain hidden quality factors. However, limited information about data clustering leaves the impression that cluster content represents the specific pairs of samples used in the study. Quality indices used for experiments included energy concentration in the frequency domain and the spatial coherence in local regions [3].

Jain and Ross considered the interoperability issue as one related to the variability introduced in the feature set when using different sensor technologies (e.g. optical vs. capacitive) [21]. When matching images acquired by Digital Biometrics and Veridicom sensors, they reported an Equal Error Rate (EER) of 23.13%, compared to an EER of 6.14% and 10.39% when using only Digital Biometrics and Veridicom, respectively. Sensors used in this paper are newer and they capture significantly higher quality fingerprints than those used in [21]. Ross and Nadgir subsequently proposed a compensation model which computes the relative distortion between images acquired using different devices [15]. The model is based on a thin-plate spline whose parameters rely on control points manually selected in order to cover representative areas where distortions can occur in the fingerprint image. Their method is, therefore, not completely automated. Campbell and Madden conducted a study to understand the causes of the lack of interoperability by analyzing both native (enrollment and verification using the same device) and non-native (enrollment and verification using different devices) False Match (FM) and False Non-Match Rates (FNMR). They used $60,902$ fingerprint images over 10 products for the evaluation. Their main goal was to test which products could work together at levels of 1% FAR and 1% FRR. Results demonstrated that only 2 products out of 10 were able to interoperate at the specified levels [2].

Recently, Lugini *et al.* analyzed the problem from a statistic perspective in order to measure the degree of change in match scores when devices used for enrollment and verification are different [11]. Results of the Kendall's rank correlation test pointed out that there is a statistically significant difference between sensor pairs and that the change is not symmetric when inverting the two devices. Modi *et al.* observed that optical touch sensors typically present a better image quality across sensors and that similarity of minutiae counts are not related to a specific acquisition technology or interaction type. However, higher minutiae count and quality measures did not have an impact on False Non Match Rates (FNMR).

An interesting study was performed by Kukula *et al.* who investigated the effects of force levels on matching error rates, minutiae count and image quality in order to assess differences between optical and capacitive sensors [9]. Their results report a significant difference in image quality based on force levels and sensor technologies. They showed that increasing the amount of force applied to the optical sensor surface causes an increase in image quality. This is important when instructing individuals on how to interact with the optical devices.

3. The Proposed Approach

Fingerprint sensors aim to obtain a good quality image of the ridge pattern. The quality of a fingerprint image depends on sensor characteristics and the condition of the finger surface [19]. In fact, inherent characteristics of the fingerprint (e.g., the absence of or poorly defined ridges), fingerprint conditions (e.g., wet, dry), poor contact of the finger with the sensor, presence of noise, latent images (e.g., traces from the previous user), ergonomics of the device (e.g., easy of use, alignment) and pressure of the finger during capture are the main factors impacting the quality [14].

This study starts by examining whether fingerprint images captured with different devices exhibit similarity in image quality characteristics, minutiae count, grey-level intensity distribution, etc. The research question we pose is

not only whether such differences in fingerprint images impact the matching performance, but whether they can help us discern the devices used in their capture. If the answer to the later question is yes, then we can use these quality measures to assess whether a match score between two fingerprints represents a genuine or an impostor comparison. The architecture of the proposed approach is described in Fig. 2. A set of suitable features is defined and combined with the match score created by a typical biometric matcher. Used features are described below.

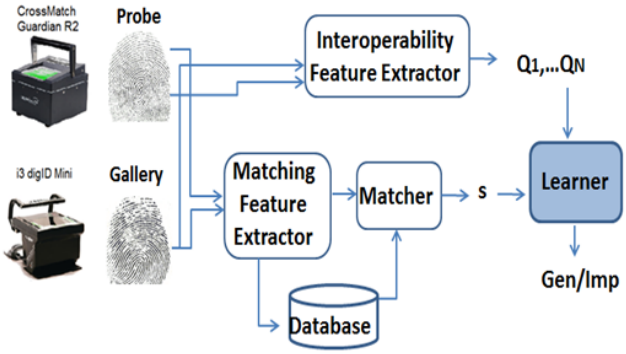


Figure 2. Architecture of the proposed approach. The interoperability analysis is performed in parallel to the typical biometric matching operation. Extracted features are concatenated with the match score to train a pattern classifier.

Image Quality measures the degree of usefulness of a biometric sample for automated recognition. The quality of captured biometric data directly impacts the effectiveness of the matching process. Gother and Tabassi discussed the concept of predicting error rates based on quality values [7], as an indicator of matchability.

Minutiae Count represents the number of minutiae extracted from an image. A minutiae-based matcher might not be accurate if only a few minutiae points can be extracted from the image [5]. Minutia count may vary based on human-sensor interaction [9].

Alignment relates two impressions of a finger. They may be different depending upon the placement of the finger on the sensor. The alignment process geometrically transforms two sets of minutiae points to the same coordinate system. Each minutiae is represented as a triplet **m** = [x,y,θ] that indicates minutiae location co-ordinates and angle [16] [22]. Different methods can be used to align two fingerprints: Generalized Hough Transform, local descriptors, energy minimization, etc. The algorithm used in this work is the descriptor-based Hough Transform which takes as input two sets of minutiae m_g and m_p extracted from the gallery and probe images respectively. Transformation parameters are computed as described in Algorithm 1. In intra-device matching, generally a rigid transformation is sufficient to align fingerprints. Additional problems, such as non-linear deformations, may arise in fingerprint alignment that stems from cross-device acquisition scenarios.

Algorithm 1: Generalized Hough Transform
Input: Two minutiae sets
$m^g = (x_i^g, y_i^g, \Theta_i^g)_{i=1}^M$, and $m^p = (x_j^p, y_j^p, \Theta_j^p)_{j=1}^N$
Output: Transformation parameters Δx, Δy, $\Delta\Theta$.

for i = 1 to M **do**
  for j = 1 to N **do**
    $\Delta\Theta = \Theta_i^g - \Theta_j^p$
    $\Delta x = x_i^g - x_j^p cos(\Delta\Theta) - y_j^p sin(\Delta\Theta)$
    $\Delta y = y_i^g + x_j^p sin(\Delta\Theta) - y_j^p cos(\Delta\Theta)$
    $A[\Delta\Theta][\Delta x][\Delta y] = A[\Delta\Theta][\Delta x][\Delta y] + 1$
  end for
end for
return location of peak in A

Gradient. First-order derivatives of a fingerprint image allow for studying the direction of maximum rate of change in grey-level profiles. The derivative is zero in the constant black and white regions. The gradient of the image is defined as follows:

$$\nabla f = \begin{bmatrix} G_x \\ G_y \end{bmatrix}, \tag{1}$$

where magnitude of this vector is given by

$$\nabla \mathbf{f} = [G_x^2 + G_x^2]^{1/2}. \tag{2}$$

The magnitude of the gradient gives the maximum rate of increase of the grey levels per unit distance in the direction of ∇**f**. G_x corresponds to $\frac{\partial f}{\partial x}$, the differences in x (horizontal) direction. G_y corresponds to $\frac{\partial f}{\partial y}$, the differences in y (vertical) direction [6].

Coherence of Direction. The spatial coherence in local regions indicates whether gradients are pointing consistently in the same direction [10]. If they are all parallel to each other, the coherence is 1 while if they are equally distributed over all directions, the coherence is 0. We first estimate the fingerprint ridge orientation field based the gradient of the image computed using Gaussian filters. The local ridge orientation at each point is estimated by finding the principal axes of variation in the image gradients.

Intensity-based statistics. Statistical parameters can be obtained directly from the histogram of the image. First order statistics measure the likelihood of observing a gray value at a randomly-chosen location in the image. In fact, each $H(n_i)$ can be viewed as an estimate of the probability of occurrence of gray level n_i. Differences in image statistics can be detected from the histogram of pixel intensities. Let n denote a discrete random variable representing discrete gray levels in the range [0, N-1], and let $H(n_i)$ indicate the normalized histogram component for the i^{th} value of n, the

first order statistical properties considered in this study are defined as follows:

$$m = \frac{1}{N}\sum_{i=0}^{N-1}(n_i)H(n_i), \quad (3)$$

where m is the mean value of r (its average gray level)

$$\sigma^2 = \sum_{i=0}^{N-1}(n_i - \mu)^2 H(n_i). \quad (4)$$

Mean, standard deviation and variance are measured over an entire segmented image.

Pattern Noise. During the image capture, different sources of noise are introduced at various stages [1] [12]. One component of noise is random and it is referred to as *photonic noise*, one is deterministic and it is referred to as *pattern noise*. The pattern noise is present in every image acquired by the sensor and it corresponds to a systematic distortion. The dominant part of pattern noise is the Photo-Response Non-Uniformity noise (PRNU) which is caused by diversity in sensitivity of pixels to the light. The image exhibits changes in intensity between pixels even if it is acquired under good illumination conditions. Light refraction on optical surfaces and zoom settings also contribute to the PRNU. First, the algorithm computes an approximation of the sensor reference pattern, then it computes the correlation between this pattern and the noise of the image as follows:

$$\rho = corr(\mathbf{n},\mathbf{r}) = \frac{(\mathbf{n} - \mu_n)(\mathbf{r} - \mu_r)}{||\mathbf{n} - \mu_n||\,||\mathbf{r} - \mu_r||}, \quad (5)$$

where **n** is the residual noise of an image, and **r** is the sensor reference pattern obtained as an average of the residual noise of all the images in the dataset. The information of interest, for the purpose of this study, is the correlation between the fingerprint image and the reference pattern of its acquisition device, indicated as *PRNU feature*.

4. Experimental Results

4.1. Data set

The data set used in this study consists of fingerprints from 494 users. Fingerprints were collected from each participant using multiple devices, all based on optical sensors. Details are provided in Table 1, at the top of next page. The order in which the devices were used for capturing fingerprints was the same for all participants. Participants provided information on age (53% varying between 20 and 29 years old) and ethnicity (57.2% of the participants are Caucasian). Fingerprints were acquired using four live-scan devices and ink-based ten-print cards (D4). Ten-print cards were scanned at resolutions of 500 dpi using a flat-bed scanner, to match the resolution of optical scanners. Ink-based fingerprints were acquired at the end, not to affect the quality of live-scans. For each live-scan device, users provided two sets of fingerprints, in sequence, each consisting of: rolled individual fingers on both hands, left slap, right slap, and thumbs slap. Only one ink-based ten prints card was collected from each user. Fingerprints were collected without controlling the quality in acquisition, i.e., no fingerprint images were rejected and recaptured at that stage.

Table 2. Matching scenarios table.

Matching Scenarios	Subjects	Devices	Match Scores
Intra-device	494	4[a]	Gen: 1,976
	494	5	Imp: 120,855
Cross-device	494	5	Gen: 9,880
	494	5	Imp: 483,420

[a] In intra-device scenario, genuine scores for Ten Print cards are missing since we only have one set of ink-based prints.

Match scores between all image pairs were generated using the Identix BioEngine Software Development Kit. The creation of match scores for this data set leads to four matching scenarios: *i)* intra-device genuine matching, for genuine match scores between fingerprints acquired using the same device for gallery and probe, *ii)* intra-device impostor matching, for impostor match scores between fingerprints acquired by the same device for gallery and probe images, *iii)* cross-device genuine matching, for genuine match scores between gallery and probe fingerprints acquired by different devices, and *iv)* cross-device impostor matching, for impostor match scores between fingerprints acquired by two different devices. Details about the matching scenarios are provided in Table 2. Impostor match scores were generated by dividing users in groups of 100 and matching the fingerprints within the same group. Although the data set contained the prints from all fingers, for this study we limited the matching to the point fingers from the right hand only.

We depict the verification performance of the fingerprint recognition system in the Detection Error Tradeoff (DET) curve, shown in Fig. 3. DET curves are obtained for both intra-device and cross-device matching scenarios.

We further analyzed the data set using the NIST Fingerprint Image Software (NFIS) [2]. The NFIQ function was used to evaluate fingerprint quality. NFIQ scores vary between 1 and 5, with 1 being the highest quality and 5 the lowest. We used MINDTCT function to count the number of minutiae present in each fingerprint image. Additional quality measures were obtained using the IQF software, developed by MITRE[3]. This quality factor (Q) ranges from 0

[2] http://www.nist.gov/itl/iad/ig/nbis.cfm

[3] http://www.mitre.org/tech/mtf/

Table 1. Characteristics of the Live-scan devices used for the fingerprint acquisition carried out in this study.

	Manufacturer	Model	Resolution (dpi)	Image size (pixels)	Capture area (mm)
D0	Cross Match	Guardian R2	500	800 x 750	81 x 76
D1	i3	digID Mini	500	752 x 750	81 x 76
D2	L1 Identity Solutions	TouchPrint 5300	500	800 x 750	81 x 76
D3	Cross Match	Seek II	500	800 x 750	40.6 x 38.1
D4	Ten Print Scans	-	500	800 x 715	-

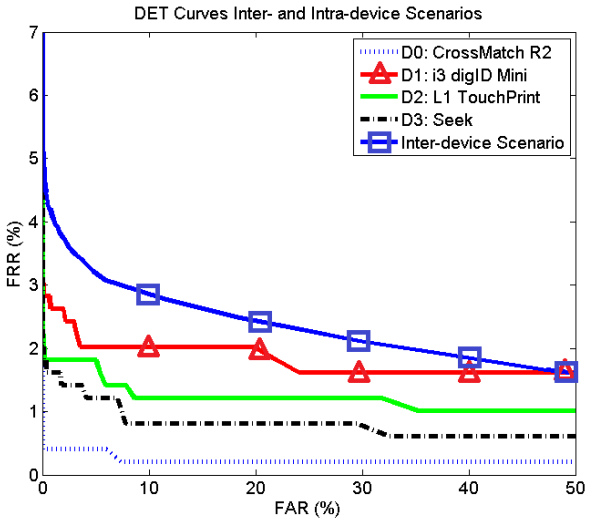


Figure 3. Verification performance of the fingerprint recognition system: DET curves for both intra- and cross-device scenarios.

to 100, with 0 being the lowest and 100 being the highest quality.

4.2. Procedure

In the proposed methodology, a fusion scheme incorporates device-specific characteristics, quality measures with match scores. The features presented in the previous section were used to train a pattern classifier to discriminate genuine from impostor users. The feature vector includes the following measures:

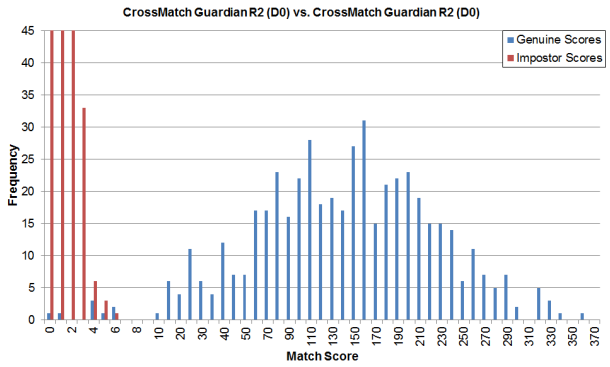
- Characteristics extracted from each *single* image: MITRE and NFIQ quality measures, contrast, average gray-level, minutiae count, PRNU, first order statistics, gradient, device ID and mean of the orientation coherence matrix;
- Characteristics extracted from *pairs* of images: alignment (Δx, Δy, $\Delta\Theta$) and match score.

Depending upon the degree of interoperability between different devices, the selected measures can exhibit more or less discriminative power. High discriminative power for a feature indicates that it is able to capture variations due to device diversity. We implemented tree-based classification schemes, i.e., a Decision Tree and a Random Forest [4], where no assumption is made about the input variables. Additionally, we implemented a Naive Bayes classifier where input variables are assumed to be independent. In order to avoid overfitting, classifiers were trained through a 10-fold cross validation procedure; since the Random Forest exhibited the lowest error rates we also experimented with training it using a subset of 25% of available match scores (cross validation), where the training set was randomly selected at each experimental instance. The features were implemented using the Matlab Version R2012a software. For the classifiers, we used Weka 3.6.

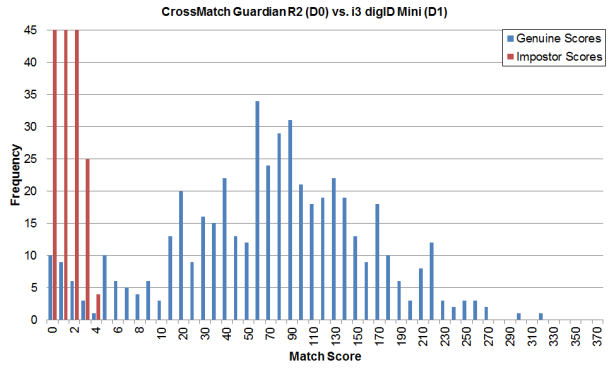
4.3. Results

As expected, we found that genuine match scores were generally higher when fingerprints where captured using the same device, compared to the case where they were captured using different devices. Fig. 4 (a) shows intra-device match scores for the device D0 (CrossMatch Guardian R2), while Fig. 4 (b) shows the cross-device scenario for the device D0 (CrossMatch Guardian R2) and the device D1 (i3 digID Mini). The overlap between genuine and impostor match scores increases substantially when capture devices are different. The mean match score and the range of match scores are lower in the cross-device matching scenario. Score distributions representing other devices reflect similar patterns. A few more observations regarding the trends of other features follow.

NFIQ quality distributions vary across devices (see Fig. 5). Device D0 (CrossMatch Guardian R2) offers the highest number of best quality samples, while device D4 (Ten Print) presents the highest number of low quality samples ($Q \geq 3$). Fig. 6 shows box plot graphs of minutiae counts considering both low and high quality images. We can observe that the lowest number of minutiae points is obtained with device D1 (i3 digID Mini). Although device D0 (CrossMatch Guardian R2) exhibits the lowest error rates in the intra-device scenario (see Fig. 3), it does not offer the highest number of minutia points, contrary to what one would expect. Lower minutiae count may be the consequence of the lack of user habituation given that D0 (CrossMatch Guardian R2) was the first device used during the data acquisition.



(a)



(b)

Figure 4. (a) Histogram of the match scores when both gallery and probe images are obtained using the same device D0 (CrossMatch Guardian R2); (b) Histogram of the match scores when the gallery is obtained using the device D0 (CrossMatch Guardian R2) while the probe image is obtained using the device D1 (i3 digID Mini).

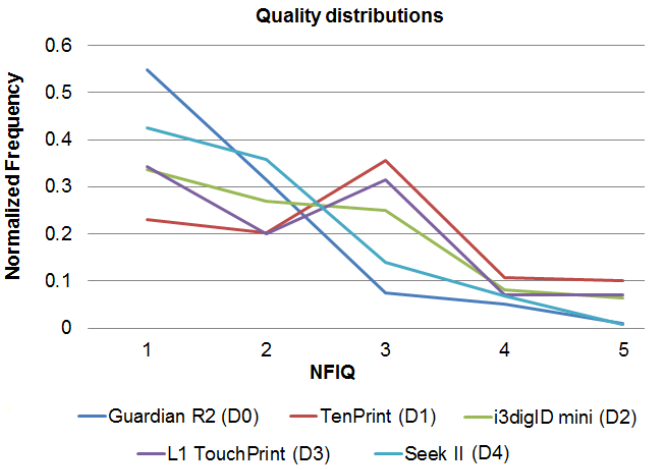


Figure 5. Distribution of NFIQ quality measures for each device analyzed in this study.

Deformations present when considering two fingerprint images acquired using different devices were non-linear. The rotation angle across pairs of minutiae was not uniform.

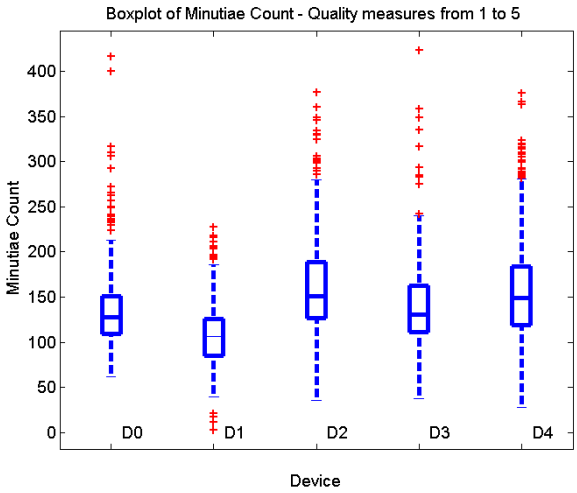


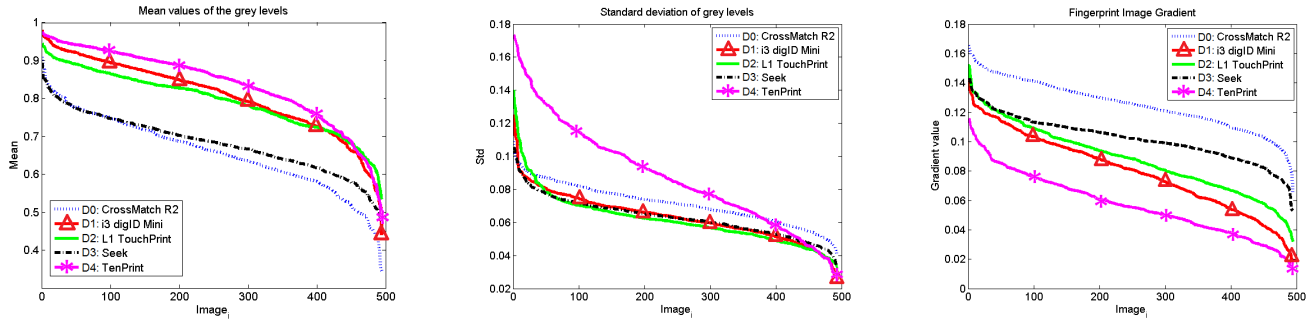
Figure 6. Boxplots of minutiae counts for each device under study in which all the images (of low and high quality) are considered.

Therefore a rigid transformation as computed by Algorithm 1 was not sufficient to align minutiae extracted from the probe and those extracted from the gallery.

Fig. 7 (a) and (b) show mean and standard deviation of grey level values. Mean separates Cross Match devices (D0 and D3) from the other manufacturers; they have a better ridge/valleys contrast. Standard deviation clearly distinguishes Ten Prints cards from images captured using the four optical devices. This may be due to the low robustness of inked fingerprints to variability in user interaction. Observed values of the gradient confirm that the highest values of the variation in grey levels are obtained by Cross Match devices (D0 and D3) (see Fig. 7 (c)). Fig. 8 indicates that the pattern noise introduced by device D2 (L1 TouchPrint) appears more systematic compared to the other devices. In other words, the images acquired by D2 exhibit the maximum correlation with the pattern noise reference of the device.

The previous observations indicate that the differences between optical fingerprint devices are many. Precisely describing the impacts such differences may have to match scores in intra-device matching scenarios is not a simple task. For this reason, we decided to rely on a machine learning approach to alleviate the impact of such complex differences to matching accuracy.

Tables 3 and 4 report the error rates for cross-device matching scenario. All device pairs are included in the classification experiment, whose results are shown in Table 3. Table 4 shows the biometric match error rates without any accommodation for intra-device comparisons. The values of False Match Rates (FMR) and False Non-Match Rates (FNMR) in 4 were selected to be approximately the same as the corresponding performance points in Table 3, for a fair



(a) (b) (c)

Figure 7. First order statistics: (a) mean of the grey level of the fingerprint image; (b) standard deviation of the grey level of the fingerprint image. First derivatives: (c) gradient of the image.

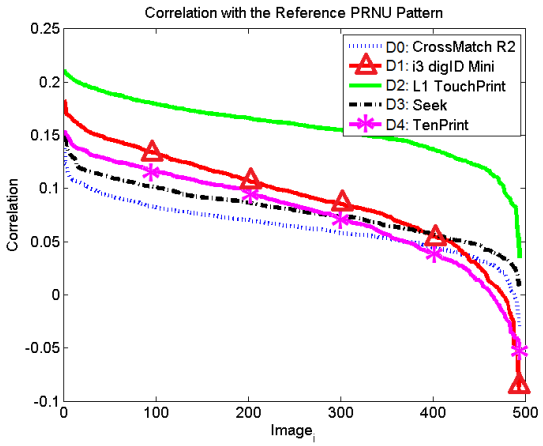


Figure 8. Correlation value with the Pattern Noise reference.

comparison. The results indicate that in cross-device matching scenarios the proposed classification method based on a random forest with 25 trees, the FMR improves from 1.982% to 0.005% at the FNMR of 3.741%. For a fixed FMR of 0.005%, the classification model improves FNMR from approximately 6.7% down to 3.74%. These results reflect the experiment in which not more than 25% of the fingerprint pairs were used for training and the remaining pairs for testing, an approach much more realistic than that in which 90% of the data set is used for training. Further improvement, although not significant, can be obtained by increasing the number of trees in the random forest. We also note that Naive Bayes does not perform the classification task well. The likely reason is the high degree of correlation between the features, which are assumed independent by Naive Bayes algorithm.

5. Conclusions

A repeated observation in biometric literature has been that the error rates of commercial fingerprint matchers increase when the images are captured by different devices.

Table 3. Comparison between different classification approaches used for modeling the scenario in which both devices used for enrollment and verification are unknown.

Performance with the Proposed Method			
Classifier	**Training**	**FMR**	**FNMR**
Decision Tree	10-Fold CV	0.013%	2.470%
Naive Bayes	10-Fold CV	0.135%	6.100%
Random Forest	10-Fold CV 10 Trees	0.006%	3.279%
Random Forest	25% Training CV 10 Trees	0.006%	3.927%
	25 Trees	0.005%	3.741%
	50 Trees	0.005%	3.722%

Table 4. Performance obtained with no classification at two operating points where FMR and FNMR are comparable with those obtained with the proposed approach.

Performance with no Classification	
FMR	**FNMR**
0.005%	6.696%
1.982%	3.741%

The goal of the paper was to improve cross-device fingerprint verification performance. We extracted quality- and intensity-based characteristics of fingerprint images acquired using four different commercial optical devices and scanned ink rolled prints. They were subsequently used as features and combined with match scores via a classifier-based fusion scheme. The model was developed for both intra-device and cross-device matching for all device pairs. Experiments were carried out using a data set pertaining to approximately 500 subjects collected at West Virginia Uni-

versity. Results show that the proposed approach is able to reduce the cross-device match error rates by several orders of magnitude for a fixed false non-match rate of 3.7%. However, the precise performance gains depend on the specific matcher used.

We plan to extend our experiments using additional data sets, different matchers and by involving scenarios in which the device used for testing the enhancement scheme is unknown. We will be considering additional quality measures and image properties as well as different fusion and classification schemes. Further, we plan to model the device influence on image quality and the influence of image quality on match scores by designing suitable graphical models. Finally, we would like to use the proposed method to enhance the interoperability of fingerprint liveness detection algorithms across different devices.

6. Acknowledgement

We would like to thank Alessandra Paulino and Dr. Anil Jain, Michigan State University, for useful discussions about the alignment procedure. The code of the alignment algorithm was written by Dr. Jianjiang Feng. We also appreciate the contribution of Dr. Jeremy Dawson, West Virginia University, for his leadership in data collection and experimental guidance.

References

[1] N. Bartlow, N. Kalka, B. Cukic, and A. Ross. Identifying sensors from fingerprint images. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPR)*, pages 78–84, 2009.

[2] J. Campbell and M. Madden. International Labor Organization (ILO) Seafarers. 2009.

[3] Y. Chen, S. C. Dass, and A. K. Jain. Fingerprint quality indices for predicting authentication performance. *Audio-and Video-Based Biometric Person Authentication*, pages 160–170, 2005.

[4] R. Duda, P. Hart, and D. Stork. *Pattern Classification*. Wiley, New York, 2nd edition, 2001.

[5] S. Elliott, S. Modi, L. Maccarone, M. Young, J. Changlong, and H. Kim. Image quality and minutiae count comparison for genuine and artificial fingerprints. *41st Annual IEEE International Carnahan Conference on Security Technology*, pages 30–36, 2007.

[6] R. Gonzalez and R. Woods. Digital image processing. *Prentice Hall Press*, 2002.

[7] P. Grother and E. Tabassi. Performance of biometric quality measures. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):531–543, 2007.

[8] A. Jain, D. Maltoni, D. Maio, and S. Prabhakar. Handbook of fingerprint recognition. *Springer*, 2003.

[9] E. Kukula, C. Blomeke, S. Modi, and S. Elliott. Effect of human-biometric sensor interaction on fingerprint matching performance, image quality and minutiae count. *International Journal of Computer Applications in Technology*, 34(4):270–277, 2009.

[10] E. Lim, X. Jiang, and W. Yau. Fingerprint quality and validity analysis. *International Conference on Image Processing. Proceedings*, 1:469–472, 2002.

[11] L. Lugini, E. Marasco, B. Cukic, and I. Gashi. Interoperability in fingerprint recognition: a large scale study. *Workshop on Reliability and Security Data Analysis (RSDA), Budapest*, pages 1–6, June 2013.

[12] J. Lukas, J. Fridrich, and M. Goljan. Digital camera identification from sensor pattern noise. *IEEE Transactions on Information Forensics and Security*, 1(2):205–214, 2006.

[13] S. Modi. Analysis of fingerprint sensor interoperability on system performance. *PhD Thesis, Purdue University*, 2008.

[14] S. Modi and S. Elliott. Impact of image quality on performance: Comparison of young and elderly fingerprints. *Proceedings of the 6th International Conference on Recent Advances in Soft Computing (RASC)*, pages 449–54, 2006.

[15] R. Nadgir. Facilitating sensor interoperability and incorporating quality in fingerprint matching systems. *PhD Thesis, West Virginia University*, 2006.

[16] A. Paulino, J. Feng, and A. Jain. Latent fingerprint matching using descriptor-based hough transform. *International Joint Conference on Biometrics (IJCB)*, pages 1–7, 2011.

[17] N. Poh, J. Kittler, and T. Bourlai. Improving biometric device interoperability by likelihood ratio-based quality dependent score normalization. *First IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS)*, pages 1–5, 2007.

[18] N. Poh, J. Kittler, and T. Bourlai. Quality-based score normalization with device qualitative information for multimodal biometric fusion. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 40(3):539–554, 2010.

[19] S. Prabhakar, A. Ivanisov, and A. Jain. Biometric recognition: Sensor characteristics and image quality. *Instrumentation & Measurement Magazine, IEEE*, 14(3):10–16, 2011.

[20] A. Ross, S. Dass, and A. Jain. A deformable model for fingerprint matching. *Pattern Recognition*, pages 95–103, 2005.

[21] A. Ross and A. Jain. Biometric sensor interoperability: A case study in fingerprints. *International ECCV Workshop on Biometric Authentication*, pages 134–145, 2004.

[22] A. Ross, A. Jain, and K. Nandakumar. *Introduction to Biometrics: A Textbook*. Springer, 2011.

[23] A. Ross and R. Nadgir. A calibration model for fingerprint sensor interoperability. *Proceedings of SPIE*, 6202, 2006.