21st International Conference on Pattern Recognition (ICPR 2012)
November 11-15, 2012. Tsukuba, Japan

A Cross-device Matching Fingerprint Database from Multi-type Sensors

Xiaofei Jia, Xin Yang, Yali Zang, Ning Zhang and Jie Tian, *Fellow, IEEE*
Institute of Automation, Chinese Academy of Sciences
{*jiaxiaofei, yx, zangyali, zhangning*}*@fingerpass.net.cn, tian@ieee.org*

Abstract

Databases play an important role in evaluating the performance of fingerprint identification algorithms. But which can be used to test the interoperability? That is to say, few of databases can test the performance of an algorithm on images acquired by different sensors. In order to solve the problem, we create the FingerPass cross-device matching fingerprint database which consists of almost 80 thousand fingerprint images from 90 subjects on nine different fingerprint sensors. We take both technology type and interaction type into consideration when choosing the sensors, totally different from other databases. It can test the interoperability of an algorithm at both the sensor level and the sensor type level. So we can use the FingerPass to test the performance of a cross-device matching algorithm for sensors of a specific type or different types . We apply the VeriFinger fingerprint recognition algorithm on it, and the experimental results indicate that the FingerPass cross-device matching database is a challenge for fingerprint algorithms.

1 Introduction

Owing to reliability and stability, biometric identification is rapidly developed and widely used all over the world. Fingerprint recognition is one of the most popular biometrics identification due to its high accuracy and low cost [5][10]. At the same time with the development of hardware, numerous fingerprint sensors are currently present. The consequence is that fingerprint images using for enrollment and verification may be acquired by different sensors. It would be in the best interests of researchers in the field to develop the fingerprint recognition algorithm which has satisfied performance even for images acquired by different sensors. In this way we will have more freedom to select products. We can also use a more specialized term "Interoperability" [8] to describe cross-device matching. But to the best of our knowledge, most of the current fingerprint recognition algorithms can only operate well on a specific kind of sensors, enduring poor performance on others. Without an algorithm that could match fingerprint images acquired by different capture sensors in enrollment and verification, all the clients attached to the same system have to be equipped with the same sensors. Now it has become an attractive challenge that how to match fingerprint images captured by multi-type sensors. What' worse, it greatly hinders technological innovation in this area that there is none reliable database for cross-device matching released till now.

In order to evaluate the performance of a fingerprint algorithms for the cross-device matching, we build the FingerPass database which is acquired by nine different scanners. The sensors we chose covers two different technology types and two different interaction types. We can use the FingerPass to test the interoperability of an algorithm for a specific type of sensors or different types of sensors, totally different from other databases. What's more important, our database is free to acquire for scientific research.

The rest of the paper is organized as follows: Section 2 details the FingerPass database. Section 3 explains interoperability. Section 4 provides the performance of the VeriFinger fingerprint recognition algorithm on the FingerPass database. Section 5 discusses the research and points out to some potential biases of the FingerPass. Section 6 concludes the paper.

2 Details of the FingerPass database

2.1 Sensors of the database

Nowadays, there are many ways to distinguish fingerprint sensors. According to technology type, these sensors can be divided into optical, capacitive, thermal or ultrasonic ones. And according to interaction type, they can be classified into press, sweep and non-contacted ones. As for the FingerPass, it contains nine sub-databases collected from nine biometric sensors

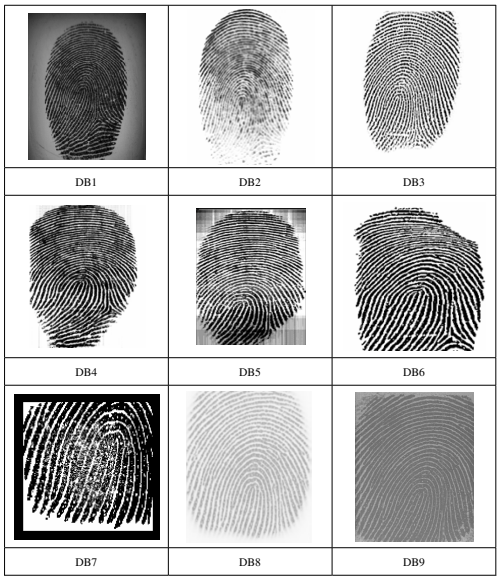

Figure 1. Image examples of the FingerPass database.

(Biometrika FX3000, CrosssMatch Verifier 300, Digital Persona URU4000B, Authentec Aes2501, ATRU-A, Aymware Sw6888, Authentec AES3400, FPC1011C and UPEK-TCRU2C). The details of sensors are shown in Table 1. The FingerPass covers optical sensors and capacitive sensors according to technology type, and covers the press and the sweep according to interaction type. In this way the sub-databases of the FingerPass can be classified into several groups. We can test the performance of an algorithm on the fingerprint images which are collected by different sensors of the same type or different type. This characteristic distinguishes the FingerPass from most of current released cross-device matching databases, such as the GUC [7]. The FingerPass database is publicly available for scientific research [1].

2.2 Acquisition of the database

Acquisition of the cross-device matching database are conducted in an outdoor environment. Environmental conditions (e.g. lighting) are not controlled in order to simulate a realistic situation. There are nine sub-databases corresponding to nine sensors. The example images of each subset are shown in Figure 1, respectively. All the nine subsets are acquired by the same eight fingers (thumb, index finger, middle finger and ring finger of both hands) of the same 90 people and 12 impressions per finger. So there are 720 fingers and the total number of impressions in the FingerPass cross-device matching database is 90*8*12*9 = 77,760 images.

The fingerprint images are named in the format of DBName-X-Y.bmp, where DBName represents the sensor type. X has four digits, which represents the finger serial number (0001-0720). And Y has two digits (01-12), which represents the serial number of impressions of the same finger.

3 Interoperability

Interoperability of the different fingerprint scanners can be considered from three levels, interface, data format and algorithm, according to [8]. The standard to specify the interoperability of interface are provided by CBEFF [2]and BioAPI [3]. The standard data formats is intended to evaluate the interoperability among various fingerprint scanner modules. As for the algorithm point of view, the interoperability is the ability to recognize the fingerprint images when the images are collected by different sensors and invariable in resolution, distortion, image size and Dots Per Inch (DPI) [4]. Ross et al. [13] regarded the sensor interoperability as the ability of a biometric system to adapt raw data acquired by different sensors. Poh et al. [11] [12] proposed to do cross-device matching at the score level and it is applicable to any biometric matching algorithm. In a word, high interoperability performance of a fingerprint verification algorithm leads to a better choice on selecting fingerprint scanners and reduces the dependency on a specific type of sensor. The reason of creating the FingerPass database is to provide a measurement to test the interoperability of a fingerprint algorithm.

4 Experiments

We apply a commercial fingerprint verification software named Verifinger 6.1 SDK to show our database is a challenge for the fingerprint recognition algorithm in cross-device matching. The sequence of the compared fingerprints in cross-device matching is arranged as follows: in genuine match, each impression is matched against all the rest impressions of the same finger to compute the False Non-Match Rate (FNMR) [6][9]. In imposter match, the first impression of each finger is matched against the first sample of the remaining fingers to compute the False Match Rate (FMR) [6][9]. To sum up, a total 95,040 (90*8*12*11) genuine matching and 517,680 (90*8*719) imposter matching are conducted for each sub-database.

The interoperable EER matrices are shown in Table 2. The diagonal cells indicate that the fingerprint images for enrollment and verification are acquired by the

Table 1. Sensors and image details in FingerPass Cross-device matching database.

Sub-database	Sensor	Technology Type	Interaction Type	Image Size	Image Resolution
DB1	FX3000	Optical	Press	400*560(224Kpixels)	569dpi
DB2	V300	Optical	Press	640*480(307Kpixels)	500dpi
DB3	URU4000B	Optical	Press	500*550(275Kpixels)	700dpi
DB4	AES2501	Optical	Sweep	unfixed	500dpi
DB5	ATRUA	Capacitive	Sweep	124*400(48Kpixels)	250dpi
DB6	SW6888	Capacitive	Sweep	288*384(111Kpixels)	500dpi
DB7	AES3400	Capacitive	Press	144*144(21Kpixels)	500dpi
DB8	FPC1011C	Capacitive	Press	152*200(30Kpixels)	363dpi
DB9	TCRU2C	Capacitive	Press	208*288(60Kpixels)	500dpi

same sensor. Other cells indicate that the fingerprint images for enrollment and verification are acquired by the different sensors. The sensor datasets in the columns represent the sensors for enrollment and the sensor datasets in the rows represent the sensors for verification. All the native EERs are lower than cross-device matching datasets except for {DB7, DB2}, {DB7, DB3}, {DB7, DB8} and {DB7, DB9}. The EERs of the above datasets are 13.39%, 9.40%, 8.58% and 8.97%, respectively. And the native EER of DB7 is 13.56%. The above sensors are all press ones. What's more, DB7, DB8 and DB9 are all collected from capcative press sensors. So we conduct an experiment about the evaluation of interoperability by grouping the datasets into the following categories: datasets collected by optical press sensors, datasets collected by optical sweep sensors, datasets collected by capacitive sweep sensors, and datasets collected by capacitive press sensors. The native EERs of each group mean the interoperability of the same type of sensors. And other EERs represent the interoperable performance of different types of sensors. In this way, the evaluation of interoperability is at the acquisition and interaction level, not the sensor level. DB1, DB2 and DB3 are placed in the optical press group. DB4 is placed in the optical sweep group. DB5 and DB6 are placed in the capacitive sweep group. DB7, DB8 and DB9 are placed in the capacitive press group. As there is just one sub-database in the optical sweep group, the native EER for the optical sweep group is meaningless to the interoperability of the optical sweep sensors. So we just calculate the interoperability of the other three groups. And the results of interoperability at sensor type level are shown in Table 3.

As can be seen from Table 3, the sensors of the same type have a lower EER than interoperable ones. The {Optical Press, Capacitive Press} interoperable dataset has a much lower EER than both the {Capacitive Sweep, Optical Press} and {Capacitive Sweep, Capacitive}. It indicates a high level of interoperability between optical press group and capacitive press group. And the native EER for capacitive sweep datasets is much larger than the native EER for optical press datasets and the native EER for capacitive press dataset. Actually the sweep sensors generate more distorted fingerprints than the press ones during acquisition because the motion of sweep is difficult to be controlled in unbiased direction and uniform speed. What's more, the sweep methods produce more distortion during the construction of the entire fingerprint image based on overlapping slices. Though the datasets generated by the press sensors has a high level of interoperability, fingerprints generated from them have obvious variance in resolution and noise patterns. In this way, the EERs of images acquired by different sensors are much higher than those of images acquired by same sensor.

5 Discussion

It seems like a little difficult to develop a cross-device matching algorithm which has a perfect performance on every sensors. It would be better if we developed an algorithm for a specific types of sensors. The FingerPass database contains the mainstream sensor types. What's more, there are more than one sensor in some sensor type. So we can use the FingerPass to test the interoperability of a cross-device matching algorithm for a specific type of sensors or different types of sensors.

There are still some drawbacks in the FingerPass cross-device matching database. There are just one optical sweep sensor in the FingerPass. Therefore, the optical sweep type can not be added into the comparison of different types. The number of scanners are limited. So the experimental result might be different for other types of fingerprint sensors.

Table 2. EERs (%) of the FingerPass

	DB1	DB2	DB3	DB4	DB5	DB6	DB7	DB8	DB9
DB1	0.06	1.10	0.71	5.12	50.00	8.46	17.78	1.52	1.00
DB2	1.10	0.13	0.33	2.16	47.38	4.30	13.38	1.05	0.37
DB3	0.71	0.34	0.01	2.69	48.28	4.47	9.40	0.74	0.20
DB4	5.12	2.16	2.69	0.01	47.31	1.08	17.22	2.69	2.73
DB5	50.00	47.38	48.28	47.31	0.18	46.27	49.57	47.10	49.13
DB6	8.46	4.30	4.47	1.08	46.27	0.28	20.33	4.35	4.26
DB7	17.78	13.39	9.40	17.22	49.57	20.33	13.56	8.58	8.97
DB8	1.52	1.05	0.74	2.69	47.10	4.34	8.58	0.09	1.01
DB9	1.00	0.37	0.20	2.73	49.13	4.26	8.98	1.01	0.05

Table 3. EER(%) at sensor type level

		Test Group		
		Optical Press	Capacitive Sweep	Capacitive Press
Enroll Group	Optical Press	0.50	27.15	5.05
	Capacitive Sweep	27.15	23.25	29.12
	Capacitive Press	5.05	29.12	5.65

6 Conclusion

Different types of sensors have great differences in resolution, image size, number of pixels and distortion. These differences lead to superior difficulty for a fingerprint verification in cross-device matching. In order to test the performance of a fingerprint recognition algorithm for cross-device matching, we present the FingerPass cross-device matching database. The FingerPass database consists of nearly 80 thousand fingerprint images of 8 fingers from 90 subjects which are acquired by 9 scanners. It contains two different technology types and two different interactions types of sensors. It can test the interoperability of an algorithm at sensor level and sensor type level. The FingerPass database furnishes a reliable measure to evaluate the performance of a fingerprint recognition algorithm for cross-device matching.

References

[1] *http://www.fingerpass.csdb.cn*.

[2] *http://www.itl.nist.gov*.

[3] *http://www.bioapi.org/*.

[4] Iso/iec 19794-2:2005, information technology-biometric performance testing and reporting-part 4: Interoperability performance testing, 2007.

[5] Biometric market and industry report 2009-2014. *http://www.biometricgroup.com/reports/public/market report.php*, 2008.

[6] R. Cappelli, D. Maio, D. Maltoni, J. Wayman, and A. Jain. Performance evaluation of fingerprint verification systems. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 28(1):3–18, 2006.

[7] D. Gafurov, P. Bours, B. Yang, and C. Busch. Guc100 multisensor fingerprint database for in-house (semipublic) performance test. *EURASIP Journal on Information Security*, 2010:3, 2010.

[8] Y. Han, J. Nam, N. Park, and H. Kim. Resolution and distortion compensation based on sensor evaluation for interoperable fingerprint recognition. pages 692–698, 2006.

[9] D. Maio, D. Maltoni, R. Cappelli, J. Wayman, and A. Jain. Fvc2000: Fingerprint verification competition. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 24(3):402–412, 2002.

[10] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar. *Handbook of fingerprint recognition*. Springer-Verlag New York Inc, 2009.

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

[12] N. Poh, R. Wong, J. Kittler, and F. Roli. Challenges and research directions for adaptive biometric recognition systems. *Advances in Biometrics*, pages 753–764, 2009.

[13] A. Ross and A. Jain. Biometric sensor interoperability: A case study in fingerprints. *Biometric Authentication*, pages 134–145, 2004.