Appeared in Proc. of International ECCV Workshop on Biometric Authentication (BioAW), (Prague, Czech Republic), LNCS Vol. 3087, pp. 134-145, Springer Publishers, May 2004.

Biometric Sensor Interoperability: A Case Study In Fingerprints

Arun Ross[1] and Anil Jain[2]

[1] West Virginia University, Morgantown, WV, USA 26506
ross@csee.wvu.edu
[2] Michigan State University, East Lansing, MI, USA 48824
jain@cse.msu.edu

Abstract. The problem of biometric sensor interoperability has received limited attention in the literature. Most biometric systems operate under the assumption that the data (viz., images) to be compared are obtained using the same sensor and, hence, are restricted in their ability to match or compare biometric data originating from different sensors. Although progress has been made in the development of common data exchange formats to facilitate the exchange of feature sets between vendors, very little effort has been invested in the actual development of algorithms and techniques to match these feature sets. In the Fingerprint Verification Competition (FVC 2002), for example, the evaluation protocol only matched images originating from the same sensor although fingerprint data from 3 different commercial sensors was available. This is an indication of the difficulty in accommodating sensor interoperability in biometric systems. In this paper we discuss this problem and present a case study involving two different fingerprint sensors.

1 Introducton

Establishing the identity of a person is becoming critical in our vastly interconnected society. Questions like "Is she really who she claims to be?", "Is this person authorized to use this facility?" or "Is he in the watchlist posted by the government?" are routinely being posed in a variety of scenarios ranging from issuing a driver's licence to gaining entry into a country. The need for reliable user authentication techniques has increased in the wake of heightened concerns about security and rapid advancements in networking, communication and mobility. Biometrics, described as the science of recognizing an individual based on her physiological or behavioral traits, is beginning to gain acceptance as a legitimate method for determining an individual's identity. Biometric systems have now been deployed in various commercial, civilian and forensic applications as a means of establishing identity. These systems rely on the evidence of fingerprints, hand geometry, iris, retina, face, hand vein, facial thermogram, signature, voice, etc. to either validate or determine an identity [1].

A generic biometric system has four important modules: (a) *sensor module* which acquires the raw biometric data of an individual; (b) *feature extraction module* which processes the acquired data to extract a feature set that represents the biometric trait; (c) *matching module* in which the extracted feature set is compared against the templates

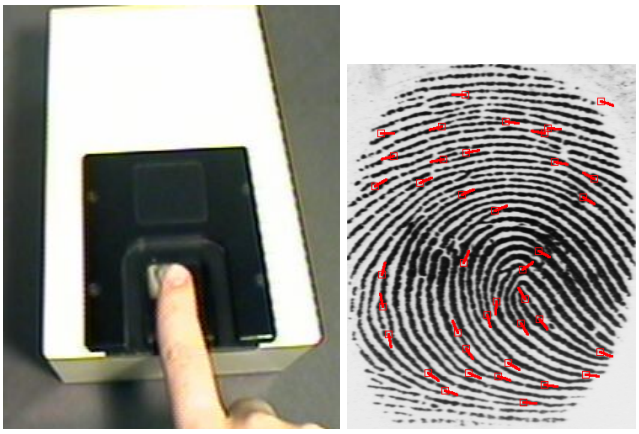
residing in the database through the generation of matching scores; (d) *decision-making module* in which the matching scores are used to either validate the user's claimed identity (verification) or determine her identity (identification). The *template* feature set is typically generated during enrollment when a user first interacts with the system and is refreshed or updated over a period of time in order to account for intra-class variations [2]. Ideally, the feature set extracted from the raw data is expected to be an invariant representation of a person's biometric. However, in reality, the feature set is sensitive to several factors including:

1. change in the sensor used for acquiring the raw data (e.g., optical versus solid-state sensors in a fingerprint system);
2. variations in the environment (e.g., change in lighting in a face recognition system, or dry weather resulting in faint fingerprints);
3. improper user interaction (e.g., incorrect facial pose during image acquisition, or drooping eye-lids in an iris system);
4. temporary alterations to the biometric trait itself (e.g., cuts/scars on fingerprints, or voice altered by respiratory ailments).

Raw data 'corrupted' due to improper user interaction or variations in the environment can be discarded by the application via a quality checking process [3]. Temporary alterations in the biometric trait can be accommodated by the use of a periodic template selection/update procedure [2]. However, the change in sensor scenario introduces challenges that have hitherto not been studied. The quality and nature of the raw data is significantly affected when the sensor used during enrollment and authentication are different. This directly affects the feature set extracted from the data and, subsequently, the matching score generated by the system. Consider a fingerprint matching system that acquires fingerprint images using an optical sensor during enrollment and a solid-state capacitive sensor during verification (at a later time). The raw images obtained at both these time instances will be significantly different (Figure 1) due to variations in imaging technology, resolution of the acquired image, area of the sensor, position of the sensor with respect to the user, etc. Thus, the corresponding feature sets will exhibit variability that cannot be easily handled by the matching module since very few algorithms explicitly account for the variations introduced by different sensors. This problem, known as *sensor interoperability*, has received limited attention in the literature. In this paper we briefly explore this problem and present a case study describing its impact on fingerprint systems.

2 Sensor interoperability

Sensor interoperability refers to the ability of a biometric system to adapt to the raw data obtained from a variety of sensors. Most biometric systems are designed to compare data originating from the same sensor. In some cases the classifiers are trained on data obtained using a single sensor alone thereby restricting their ability to act on data from other sensors. This limitation prevents the use of multiple sensors with different



(a) An optical sensor.

(b) A solid-state sensor.

Fig. 1. Fingerprint images of the same finger acquired using (a) Digital Biometrics' optical sensor and (b) Veridicom's solid state sensor. The number of detected minutiae points in the corresponding images are 39 and 14, respectively.

characteristics in a single biometric system. Martin et al. [4] make the following observation about the effect of the handset type (sensor) on the performance of a speaker recognition system[3]:

> "Microphone differences are one of the most serious problems facing speaker recognition, especially when dealing with the telephone, where Edison's old nonlinear carbon-button microphone still represents a significant fraction of all transducers".

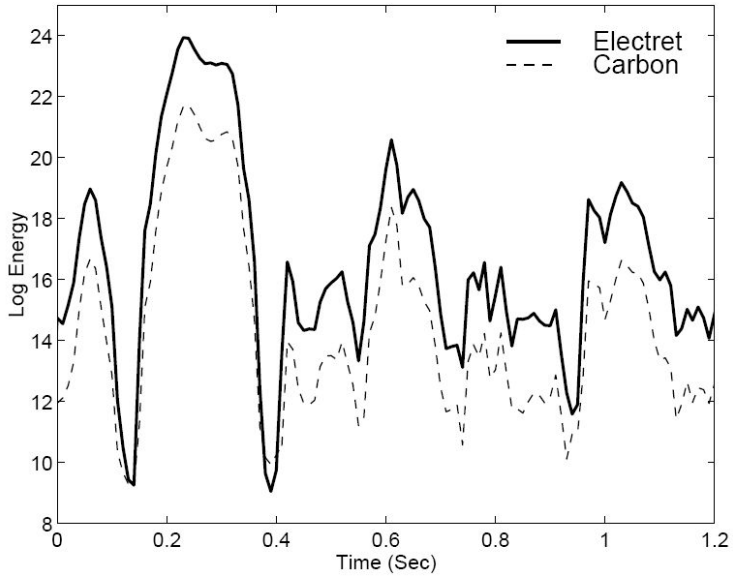


Fig. 2. The logarithmic energy of the same speech segment when passed through carbon-button and electret microphones. The energy corresponds to a specific frequency band (taken from [5]).

They report a significant dip in performance when the carbon-button microphone was used during the training phase and the electret microphone was used during the test phase (and vice-versa) in a speaker biometric system. Malayath [5] suggests the use of oriented principal component analysis (OPCA) in designing a filter to suppress the variabilities introduced by different handsets/channels.

Phillips et al. [6] state the following about the sensitivity of face verification algorithms to camera type:

> "Many face verification applications make it mandatory to acquire images with the same camera. However, some applications, particularly those used in law

[3] The NIST speaker recognition evaluation.

> enforcement, allow image acquisition with many camera types. This variation has the potential to affect algorithm performance as severely as changing illumination. But, unlike the effects of changing illumination, the effects on performance of using multiple camera types has not been quantified".

The International Biometric Group (IBG)[4] recently conducted a battery of tests to evaluate the performance of various sensors (including fingerprint) under different test conditions. BIO-key International, Inc., demonstrated that its fingerprint system could enroll and verify fingerprint images obtained using different sensors[5]. However, this kind of test scenarios are extremely rare as is borne out by the following statement by IBG [7]:

> "Today, there is really very little interoperability among templates and the algorithms that the systems are using for matching. Those are proprietary technologies. So if you as an organization are considering deploying biometric technologies you should be concerned [whether] the vendor you are working with now will be around in 5 years and supporting the product. The cost to you of re-enrolling all your subjects could be significant".

This underscores the need for developing algorithms that are able to seamlessly operate on feature sets originating from different sensors. Note that the problem of sensor interoperability as defined in this paper cannot be solved by adopting a common biometric data exchange format [8]. Such a format merely aids in the *exchange* of feature sets between systems/vendors [9]. It, however, does not provide a method to *compare* feature sets obtained from different sensors.

3 Fingerprint sensors

The advent of small-sized solid-state fingerprint sensors permit these devices to be easily embedded in various applications such as laptops, computer peripherals, cellphones, PDAs, etc. The ease of interacting with fingerprint sensors (compared to, say, iris cameras) has contributed to their increase in popularity. This has resulted in a proliferation of these devices and their subsequent inclusion in a variety of applications (Figure 3). The recently launched US-VISIT[6] program for example, obtains fingerprint (and face) information of certain travellers arriving in airports and seaports. An optical fingerprint sensor is currently being used during the enrollment phase to procure fingerprint images. However, it is not guaranteed that a similar type of sensor will be used at a later time when verifying the same individual. The cost of re-enrolling individuals every time the sensor is changed will be tremendous and will, in fact, defeat the purpose of enrolling individuals at the port of entry in the first place. In cases such as these, the need for sensor interoperability is paramount and will significantly impact the usability of the system.

[4] http://www.biometricgroup.com/index.html
[5] http://www.biometricgroup.com/in_the_news/01_15_04.html
[6] United States Visitor and Immigration Status Indicator Technology.

Fig. 3. A variety of fingerprint sensors with different specifications (e.g., sensing technology, image size, image resolution, image quality, etc.) are now available. These sensors have been embedded in computer peripherals and other devices to facilitate user authentication.

A live-scan fingerprint is usually acquired using the *dab* method, in which the finger is placed on the surface of the sensor without rolling[7]. There are a number of sensing mechanisms that can be used to detect the ridges and furrows present in the fingertip. A brief description of a few of these principles is provided below:

(i) Optical Frustrated Total Internal Reflection (FTIR): This technique utilizes a glass platen, a laser light-source and a CCD (or a CMOS camera) for constructing fingerprint images. The finger is placed on the glass platen, and the laser light-source is directed toward the platen. The CCD captures the reflected light after it has passed through a prism and a lens to facilitate image formation. The light incident on the ridges is randomly scattered (and results in a dark image), while the light incident on the valleys suffers total internal reflection (and results in a bright image). It is difficult to have this arrangement in a compact form, since the focal length of small lenses can be very large. Further, image distortions are possible when the reflected light is not focused properly.

(ii) Ultrasound Reflection: The ultrasonic method is based on sending acoustic signals toward the finger tip and capturing the echo signal. The echo signal is used to compute the range image of the fingerprint and, subsequently, the ridge structure itself. The sensor has two main components: the sender, that generates short acoustic pulses, and the receiver, that detects the responses obtained when these pulses bounce off the fingerprint surface [10]. This method images the sub-surface of the fingerprint and is, therefore, resilient to dirt and oil accumulations that may visually

[7] It is possible to capture a *rolled* live-scan fingerprint, although an elaborate scanner arrangement may be necessary in this case

(a) Fingerprint images of the first user.

(b) Fingerprint images of the second user.

Fig. 4. The fingerprint images of 2 different users (a) and (b) obtained using Precise (left), Ethentica (middle) and Secugen (right) sensors.

mar the fingerprint. The device is, however, expensive, and as such not suited for large-scale production.

(iii) Piezoelectric Effect: Pressure sensitive sensors have been designed that produce an electrical signal when a mechanical stress is applied to them. The sensor surface is made of a non-conducting dielectric material which, on encountering pressure from the finger, generates a small amount of current. (This effect is called the piezoelectric effect). The strength of the current generated depends on the pressure applied by the finger on the sensor surface. Since ridges and valleys are present at different distances from the sensor surface, they result in different amounts of current. This technique does not capture the fingerprint relief accurately because of its low sensitivity.

(iv) Temperature Differential: Sensors operating using this mechanism are made of pyro-electric material that generate current based on temperature differentials. They rely on the temperature differential that is created when two surfaces are brought into contact. The fingerprint ridges, being in contact with the sensor surface, produce a different temperature differential than the valleys that are away from the sensor surface [11]. The sensors are typically maintained at a high temperature by electrically heating them up.

(v) Capacitance: In this arrangement, there are tens of thousands of small capacitance plates embedded in a chip. Small electrical charges are created between the surface of the finger and each of these plates when the finger is placed on the chip. The magnitude of these electrical charges depends on the distance between the fingerprint surface and the capacitance plates [12, 13]. Thus, fingerprint ridges and valleys result in different capacitance patterns across the plates. This technique is susceptible to electrostatic discharges from the tip of the finger that can drastically affect the sensor; proper grounding is necessary to avoid this problem.

While optical sensors have the longest history, the new solid-state capacitive sensors are gaining immense popularity because of their compact size and the ease of embedding them into laptops, cellular phones, smart pens, etc. Figure 4 shows the fingerprint impressions pertaining to two different users acquired using three different sensors. Visually, there are significant differences in the quality of the image corresponding to the three sensors. This clearly illustrates the difficulty in accommodating multiple sensors in a single biometric system. In the recently conducted Fingerprint Verification Competition (FVC2002[8]), only fingerprint images obtained using the same sensor were matched although images from three different types of sensors were available [14].

4 Optical versus solid-state sensors: a case study

In this section we report experiments conducted using two different types of fingerprint sensors. The fingerprint images of 160 different non-habituated cooperative subjects were obtained using an optical sensor manufactured by Digital Biometrics (DBI) and a solid-state capacitive sensor manufactured by Veridicom (Figure 1). The optical sensor had a sensing area of approximately $1" \times 1"$. The images were acquired at a resolution

[8] http://bias.csr.unibo.it/fvc2002/

of 500 dpi and were 480×508 in size. The solid-state sensor had a sensing area of approximately $0.6" \times 0.6"$. The images in this case were also obtained at a resolution of 500 dpi. However, the reduced size of the placement area resulted in 300×300 images.

The subjects mainly consisted of students at Michigan State University, and their relatives and friends. Approximately 35% of the subjects were women. Each individual was asked to provide fingerprint images of four fingers, viz., right index, right middle, left index and left middle fingers. This process was repeated to obtain a second impression of all four fingers. This resulted in a total of $1,280$ ($160 \times 4 \times 2$) fingerprint images per sensor. The subjects were asked to provide their fingerprint images again after a period of 6 weeks. During this time, another $1,280$ ($160 \times 4 \times 2$) fingerprint images per sensor were obtained. Thus, a total of $2,560$ fingerprint images per sensor pertaining to 640 different fingers were made available. The databases corresponding to the optical and solid-state sensors were labelled as MSU_DBI and MSU_VERIDICOM, respectively [15].

We used the minutiae-based fingerprint matcher developed by Hong et al. [16] in order to compare fingerprint images. The matcher uses an adaptive elastic string matching technique to establish correspondences between the minutiae pattern of two images. In this technique, the minutiae points in an image are first represented as a "string" in the polar coordinate system. Two such "strings" are then compared via a dynamic programming algorithm. The similarity between two minutiae patterns is indicated by a score that represents the percentage of matching minutiae pairs. If this score is greater than a threshold then the two minutiae patterns are said to originate from the same fingerprint (a match).

We conducted three different types of experiments in order to study the effect of changing sensors on matching performance.

1. Matching images within the MSU_DBI database.
2. Matching images within the MSU_VERIDICOM database.
3. Matching images from MSU_DBI against those from MSU_VERIDICOM.

The Receiver Operating Characteristics (ROC) curves corresponding to all three cases are shown in Figure 6. Each curve depicts the Genuine Accept Rate (GAR) and the False Accept Rate (FAR) at various matching thresholds. We make the following observations:

1. The optical sensor results in a better matching performance than the solid-state sensor due to the elaborate sensing area of the former. Infact, the average number of minutiae points extracted from the images acquired using the optical sensor is substantially more than that acquired using the solid-state sensor (Figures 1 and 5).
2. When the images being matched originate from two different sensors then the performance of the matcher drastically decreases. The Equal Error Rate (EER) in this case is 23.13% while the EERs for the other two cases are 6.14% (MSU_DBI) and 10.39% (MSU_VERIDICOM). This illustrates the impact of changing sensors on the fingerprint matching performance. As mentioned earlier, the optical sensor results in more minutiae points than the solid-state sensor. Thus, comparing two

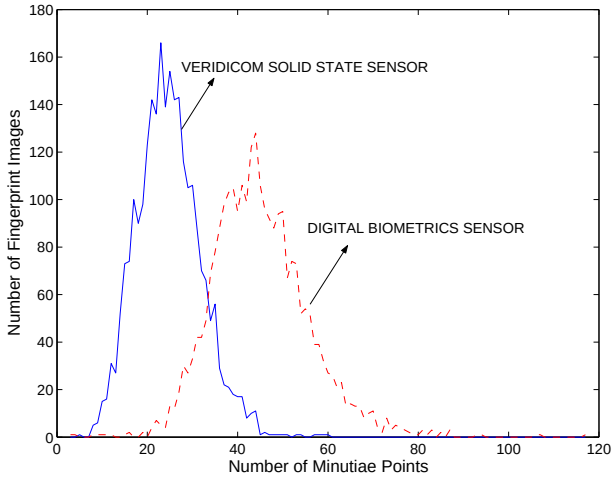


Fig. 5. Histogram of the number of minutiae points extracted from images acquired using the Veridicom and DBI sensors. A total of $2,500$ fingerprint impressions were used to compute these histograms for each sensor. The histograms suggest that substantially fewer minutiae points are available in images obtained using small-sized solid-state sensors.

images - one obtained from the DBI sensor and the other obtained from the Veridicom sensor - is akin to comparing a full print with a partial print, resulting in several incorrect matches (false accepts) that increase the error rate of the system. Similar problems arise if one were to compare rolled prints with dab prints. Seldom does the methodology adopted for one type of input data work on other kinds of data.

There are several ways in which the problem of interoperability can be approached. Typically, it is the matching module that is expected to reconcile feature sets arising from the use of multiple sensors. However, reconciliation has to happen much earlier in a biometric system to mitigate the impact of changing sensors.

1. One of the obvious ways is to store the raw data in its entirety in the database (during enrollment) along with the feature set extracted from it (e.g., a fingerprint image *and* its minutiae set). During verification, the biometric system could extract feature sets from both the database and input images, and then compare them. Here, the onus is on the feature extraction module to generate a 'compatible' feature set from the database image by explicitly taking into account the *differences* between the sensors used during enrollment and verification. However, storing raw data in a central repository would raise security concerns, since compromising this information could have serious repercussions.
2. Canonical representations of the input data might be useful to offset the effect of variability in data. For example, fingerprint images may be viewed as a collection of ridge lines, with the inter-ridge spacing forced to be a constant [17]. Feature values can then be extracted from this canonical representation. Such an approach,

however, presupposes the existence of a canonical form for the raw data. It also preempts the possibility of extracting a *rich* set of features from the original data.

3. In some situations a simple transformation of the template feature set might account for sensor-specific properties. Fingerprint systems could use the ridge count between minutiae pairs in an image, the location of core/delta points, etc. to 'normalize' the spatial distribution of minutiae points. In speaker recognition systems, certain normalization filters may be designed [5] to account for variability due to different handsets.

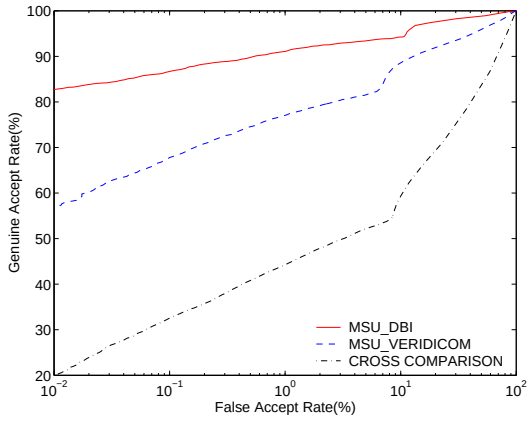


Fig. 6. ROC curves corresponding to the 3 matching experiments that were conducted. The optical sensor is seen to result in the best performance (solid line). The solid-state sensor does not exhibit good performance (dashed line) possibly due to partial prints that present limited number of minutiae points. Cross-comparing images between sensors using the same matching program results in the worst performance (dot-dash line).

5 Summary and future work

The need for biometric sensor interoperability is pronounced due to the widespread deployment of biometric systems in various applications and the proliferation of vendors with proprietary algorithms that operate on a specific kind of sensor. In this paper we have illustrated the impact of changing sensors on the matching performance of a fingerprint system. Almost every biometric indicator is affected by the sensor interoperability problem. However, no systematic study has been conducted to ascertain its effect on real-world systems. Normalization at the raw data and feature set levels of a biometric system may be needed to handle this problem. There is also a definite need to develop matching algorithms that do not implicitly rely on sensor characteristics to perform matching. Biometric vendors and independent test groups (e.g., NIST, IBG)

should begin incorporating interoperable scenarios in their testing protocol. This would help in understanding the effect of changing sensors on a biometric system and would encourage the development of cross-compatible feature extraction (representation) and matching algorithms.

6 Acknowledgements

Thanks to Dr. Naren Malayath for granting permission to use the graph in Figure 2.

References

1. Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. on Circuits and Systems for Video Technology **14** (2004) 4–20
2. Jain, A.K., Uludag, U., Ross, A.: Biometric template selection: a case study in fingerprints. In: Proc. of 4th Int'l Conf. on Audio- and Video-based Biometric Authentication (AVBPA). Volume LNCS 2688., Guildford, UK, Springer (2003) 335–342
3. Ratha, N.K., Bolle, R.M.: Fingerprint image quality estimation. IBM Computer Science Research Report RC21622 (1999)
4. Martin, A., Przybocki, M., Doddington, G., Reynolds, D.: The NIST speaker recognition evaluation - overview, methodology, systems, results, perspectives. Speech Communications **31** (2000) 225–254
5. Malayath, N.: Data-driven methods for extracting features from speech. PhD Thesis, Oregon Graduate Institute of Science and Technology (2000)
6. Phillips, P.J., Martin, A., Wilson, C.L., Przybocki, M.: An introduction to evaluating biometric systems. IEEE Computer **33** (2000) 56–63
7. Moore, S.: Latest tests of biometrics systems shows wide range of abilities. IEEE Spectrum Online (2004)
8. Bolle, R.M., Ratha, N.K., Senior, A., Pankanti, S.: Minutia template exchange format. In: Proc. of IEEE Workshop on Automatic Identification Advanced Technologies, Summit, NJ (1999) 74–77
9. Podio, F.L., Dunn, J.S., Reinert, L., Tilton, C.J., O'Gorman, L., Collier, P., Jerde, M., Wirtz, B.: Common biometric exchange file format (CBEFF). Technical Report NISTIR 6529, NIST (1999)
10. Bicz, W., Gumienny, Z., Kosz, D., Pluta, M.: Ultrasonic setup for fingerprint patterns detection and evaluation. Acoustical Imaging **22** (1996)
11. Edwards, D.G.: Fingerprint sensor. US Patent 4429413 (1984)
12. Tsikos, C.: Capacitive fingerprint sensor. US Patent 4353056 (1982)
13. Young, N.D., Harkin, G., Bunn, R.M., McCulloch, D.J., Wilks, R.W., Knapp, A.G.: Novel fingerprint scanning arrays using polysilicon TFT's on glass and polymer substrates. IEEE Electron Device Letters **18** (1997) 19–20
14. Maio, D., Maltoni, D., Cappelli, R., Wayman, J.L., Jain, A.K.: FVC2002: Fingerprint verification competition. In: Proceedings of the International Conference on Pattern Recognition (ICPR), Quebec City, Canada (2002) 744–747
15. Jain, A.K., Prabhakar, S., Ross, A.: Fingerprint matching: Data acquisition and performance evaluation. Technical Report MSU-TR:99-14, Michigan State University (1999)
16. Hong, L.: Automatic personal identification using fingerprints. PhD Thesis, Michigan State University (1998)
17. Senior, A., Bolle, R.: Improved fingerprint matching by distortion removal. IEICE Transactions on Information and Systems **E84-D** (2001) 825–831