Hindawi Publishing Corporation
EURASIP Journal on Information Security
Volume 2010, Article ID 391761, 11 pages
doi:10.1155/2010/391761

Research Article

GUC100 Multisensor Fingerprint Database for In-House (Semipublic) Performance Test

Davrondzhon Gafurov, Patrick Bours, Bian Yang, and Christoph Busch

Norwegian Information Security Lab, Gjøvik University College, P.O. Box 191, 2802 Gjøvik, Norway

Correspondence should be addressed to Davrondzhon Gafurov, davrondzhon.gafurov@hig.no

Received 5 February 2010; Revised 3 July 2010; Accepted 30 August 2010

Academic Editor: Bernadette Dorizzi

For evaluation of biometric performance of biometric components and system, the availability of independent databases and desirably independent evaluators is important. Both databases of significant size and independent testing institutions provide the precondition for fair and unbiased benchmarking. In order to show generalization capabilities of the system under test, it is essential that algorithm developers do not have access to the testing database, and thus the risk of tuned algorithms is minimized. In this paper, we describe the GUC100 multiscanner fingerprint database that has been created for independent and in-house (semipublic) performance and interoperability testing of third party algorithms. The GUC100 was collected by using six different fingerprint scanners (TST, L-1, Cross Match, Precise Biometrics, Lumidigm, and Sagem). Over several months, fingerprint images of all 10 fingers from 100 subjects on all 6 scanners were acquired. In total, GUC100 contains almost 72.000 fingerprint images. The GUC100 database enables us to evaluate various performances and interoperability settings by taking into account different influencing factors such as fingerprint scanner and image quality. The GUC100 data set is freely available to other researchers and practitioners provided that they conduct their testing in the premises of the Gjøvik University College in Norway, or alternatively submit their algorithms (in compiled form) to run on GUC100 by researchers in Gjøvik. We applied one public and one commercial fingerprint verification algorithm on GUC100, and the reported results indicate that GUC100 is a challenging database.

1. Introduction

The interest in biometric systems is rapidly increasing due to the demands on high security applications. Although various types of human characteristics are observed in biometric authentication, the most popular biometric systems are based on fingerprinting [1, 2]. The two important aspects in performance evaluation of fingerprint recognition algorithms (and other biometrics in general) are the availability of independent databases and desirably testing bodies too. The advantages of such databases and third party testing bodies are that firstly it allows more direct and unbiased benchmarking of different algorithms, and secondly it increases trustworthiness of the performance report, since developers do not have a direct access to the database for tuning algorithm's parameters to adapt to the database. However, creating and distributing large-scale databases publicly is not an easy task because of the involved costs and time as well as jurisdictional limits. Due to the nature of the collected data (i.e., human physiology), creation and distribution of the large scale biometric databases raises privacy concerns and may not be permitted by data protection authorities in some countries (especially in Europe). Even if data collection is permitted, usually it is requested to destroy collected data after the completion of the project, for example, as in [3].

Nevertheless, in the biometric community, several fingerprint databases were established for research purposes [4–10]. A short summary of some reported fingerprint databases is given in Table 1. In this table, the columns #SC, #SB, #FS, #UF, and #NF represent the number of fingerprint scanners, number of volunteers contributing to the data collection, number of fingers per subject, total number of unique fingers, and number of images per finger, respectively. Previously public databases were provided by NIST (National

Table 1: Summary of some fingerprint image databases.

Database	#SC	#SB	#FS	#UF	#NF	Comment
BioFinger [3]	11	30	8	240	9	Not available any more
NIST29 [4]	—	—	—	2160	2	Available for purchase
NIST4 [5]	—	—	—	2000	2	Available for purchase
NIST14 [6]	—		—	27000	2	Available for purchase
FVC2000 [7]	1	19	up to 4	110	8	Available publicly
	1	19	up to 4	110	8	
	1	19	up to 6	110	8	
FVC2002 [8]	1	30	4	110	8	Available publicly
	1	30	4	110	8	
	1	30	4	110	8	
FVC2004 [9]	1	30	4	110	8	Available publicly
	1	30	4	110	8	
	1	30	4	110	8	
FVC2006 [10]	1	—	—	150	12	Available publicly
	1	—	—	150	12	
	1	—	—	150	12	
FVC-onGoing [11]						Web-based automated evaluation system for fingerprint recognition algorithms, sequestered database
BioSec [12]	3	200	4	800	24	Available publicly from mid-2006
MCYT [13]	2	330	all 10	3300	24	Publicly available
GUC100 (this paper)	6	100	all 10	1000	72	Available for in-house (semi-public) testing

Institute of Standards and Technology) which consists of thousands of fingerprint images, for example, SD29 [4], SD4 [5], and SD14 [6]. However, these images are rolled ones that is, scanned from inked tenprint paper card. Such type of images is quite different from electronically captured ones and is not suited well for evaluation of algorithms that should be operated in an "on-line" application. In spite of this, the NIST fingerprint databases are still being used in research community and are available for purchase [4–6]. In addition, in the context of the MINEX project NIST composed a large-scale fingerprint data set for in-house testing of algorithms [14]. The database series FVC200x [7–10] were designed for the Fingerprint Verification Competition (FVC) where several competing algorithms were tested on them. Every FVC200x database consists of 4 disjoint data sets. Out of the four, in three data sets, images were captured electronically by some commercially available fingerprint scanners. The fourth database consisted of synthetically generated fingerprint images (therefore not listed in the Table 1). In fact in databases FVC2000, 2002, and 2004, the *#UF* and *#NF* were 120 and 12, respectively, but only 110 and 8 were used. There are also multimodal databases, where the fingerprint is collected as one of the modalities [12, 13, 15].

This paper describes a multi-scanner fingerprint database, which has been created for independent and in-house performance and interoperability testing. In the rest of the paper, we will refer to this database as GUC100 (GUC stands for Gjøvik University College.)

The rest of the paper is organized as follows. Section 2 describes objectives, targeted application scenarios, and availability of the GUC100 database. Section 3 details more on the data collection process, subject demographics population, fingerprint scanners, and so on. Section 4 presents an overview of interoperability testing on the GUC100 database as well as some factors that can be considered while conducting a test on the GUC100 database. Section 5 provides performance of two publicly available fingerprint verification software on GUC100 database. Section 6 points out to some possible biases in the database which are needed to be taken into account when interpreting results of evaluation on GUC100. Section 7 summarizes the paper.

2. Objectives, Scenarios, and Availability of the Database

The primary objective of the GUC100 database is to enable performance evaluation of fingerprint algorithms in cross-scanner (interoperability) scenarios where enrolment and verification scanners are different. The targeted performance accuracy with this database is aimed at FRR 1% (or lower) at FAR 0.1%.

Although evaluation of products from a single biometric supplier is essential from the supplier's perspective, testing of scenarios, where products (e.g., sensor, minutia extractor, minutia comparator) are provided by different suppliers, is very important for both integrators and operators to proof the interoperability prior to component integration and/or system roll-out. This refers to the settings where, for example, the enrolment and verification fingerprint images

Table 2: Some characteristics of fingerprint scanners.

Scanner	Area [mm]	Temperature range [Celsius]	Technology
TST BiRD3	19 × 16	5–50	Optical
L-1 DFR2100	32 × 28	0–40	TIR (Total Internal Reflection)
Cross Match LSCAN100	31 × 31	10–40	TIR (Total Internal Reflection)
Precise 250MC	18 × 12.8	0–50	Capacitive
Lumidigm V100	27.94 × 17.78	0–40	MSI (MultiSpectral Images)
Sagem MorphoSmart	21 × 21	0–40	TIR (Total Internal Reflection)

are acquired by different capture devices. For instance, in a biometric passport case, the document issued by a country where the enrolment image is captured by one scanner shall be able to be verified by another country where the probe image is very likely to be acquired by a different scanner. The GUC100 fingerprint database provides 15 and 30 cross-scanner combinations for a symmetric and an asymmetric comparators, respectively.

The GUC100 database is intended for technology testing which is an offline evaluation of biometric components using a pre-existing corpus [16]. In creating the GUC100, we aimed at increasing several dimensions of the database as the numbers in Table 1 (last row) indicate. The database aims to simulate an indoor, covert (i.e., supervised), and verification (i.e., one to one) application environments. It is useful for performance evaluation not only at the traditional minutiae level but also at the pseudonymous identifier level which is more privacy protective compared to conventional minutiae templates [17, 18].

In exploitation of this database we follow—due to privacy regulations in Norway—the principal of "*If the data cannot travel to the algorithm, then the algorithm shall travel to the data*". This means that copies of GUC100 database cannot be distributed to other parties outside of GUC campus. However, algorithm developers are free to visit GUC and perform testing of their algorithm in its premises or submit their (binary code) fingerprint recognition algorithm to GUC team for testing. The interested party can contact authors of this paper or visit the GUC100 webpage for any updates on the database at http://www.nislab.no/guc100. The minimum specification for a fingerprint encoder is that it should be able to produce a template from fingerprint image in PNG format, and a fingerprint comparator should be able to compare two templates and produce a comparison score. If there are any specific requirements then they will be posted in aforementioned GUC100 webpage. It is also possible to send requests or inquires about database to the E-mail address: turbines@hig.no. It is worth mentioning that the database is available for algorithm evaluation until 2021. After that the database will be destroyed due to the agreement with Norwegian Data Privacy Authority (NSD) [19].

3. GUC100 Fingerprint Database

The GUC100 database was collected at GUC (Gjøvik University College) in Norway during February 2008–January 2009. Before starting the data collection, we obtained permission from the Norwegian Data Privacy Authority (NSD) [19]. In addition, all volunteers signed a consent form. Although due to Norwegian regulations the database cannot be sent over to other parties, but it is freely accessible and available for testing within GUC's campus to external parties.

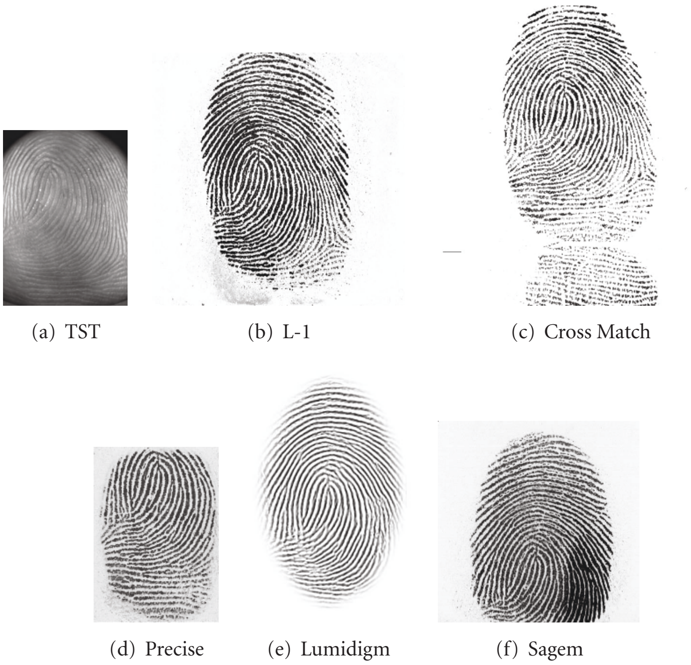
3.1. Population. The number of subjects who participated in the data collection was 100: 80 males and 20 females. The average ages of male and female groups were about 30.5 (±12.3) and 28.3 (±8) years old, respectively. Participants were mostly students and staff at GUC.

3.2. Fingerprint Scanners. The GUC100 database was collected by using six fingerprint scanners from different suppliers. The scanners were TST BiRD3, L-1 DFR2100, Cross Match LSCAN100, Precise 250MC, Lumidigm V100, and Sagem MorphoSmart. All these scanners, except TST BiRD3, were based on touching interaction. The TST scanner was based on touchless interaction. The resolution of all scanners was 500 dpi. Photos of the fingerprint scanners are given in Figure 2, and some of their properties are presented in Table 2(In this table, the order of scanners does not indicate any preference, it merely follows the order in Figure 2.) In this table, the columns *Area*, *Temperature range*, and *Technology* represent acquisition area, operating temperature range and sensor technology of the scanners, respectively.

The lack of the swipe sensor in GUC100 database can be justified by the fact that database is intended to simulate and predict performance for public, commercial, and governmental applications but not for access to personal devices, where swipe sensors are in common use. Furthermore, the main purpose of the database is not comparing performance of various scanner technology but rather benchmarking different algorithms and investigating cross-scanner interoperability.

Example images of the same finger in one session for each scanner are shown in Figure 1. As it can be seen from the figure, due to the scanner principle, the nature of fingerprint images from the TST scanner is rather different compared to the images from the other scanners.

3.3. Data Collection. The data collection was conducted in an indoor environment. Each subject attended 12 sessions during a period of several months. The average time interval



(a) TST (b) L-1 (c) Cross Match

(d) Precise (e) Lumidigm (f) Sagem

Figure 1: Images of the same finger in one session on all scanners.

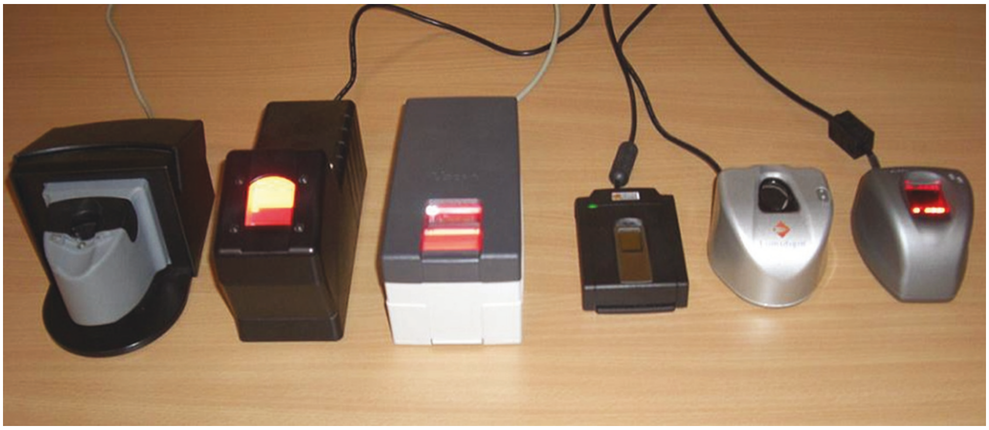


Figure 2: Fingerprint scanners (from left to right): TST, L-1, Cross Match, Precise, Lumidigm, and Sagem.

between each session was about one week. A restriction was applied such that the participant was not allowed to attend more than one session per day. We believe that introducing such long time delays (i.e., in terms of days and weeks) between acquisition sessions allows natural variations of the fingerprint skin to occur and thus to cover more realistic scenarios. All sessions were carried out under supervision of a human operator, so that no extreme rotations of the fingerprints are included in the database. During the capture process no objective quality measurements were taken, and the quality of the images was determined visually (i.e., subjectively) by the human operator.

For each person, the first 3 sessions were *uncontrolled* and the other 9 sessions were *controlled* (the term controlled refers to signal quality control by means of adjustment of the environmental factors that was conducted by an operator.) The reason for introducing such controlled session was that when the data collection was started in February 2008, it was not straightforward to capture good quality fingerprint image (visual jugement) without some extra action. Thus, in the controlled sessions, some actions were undertaken to improve image quality for example, subjects could wet/clean their fingers (by touching wet sponge) before touching scanners platens, or sometimes they were instructed to apply more finger pressure on scanners. This was mostly required on cold days with outside temperature below zero and mainly for L-1 and Cross Match scanners. In uncontrolled sessions, no extra actions were undertaken to get better images. Figure 3 presents an example of images of a single finger over all 12 sessions. In addition, over most sessions of

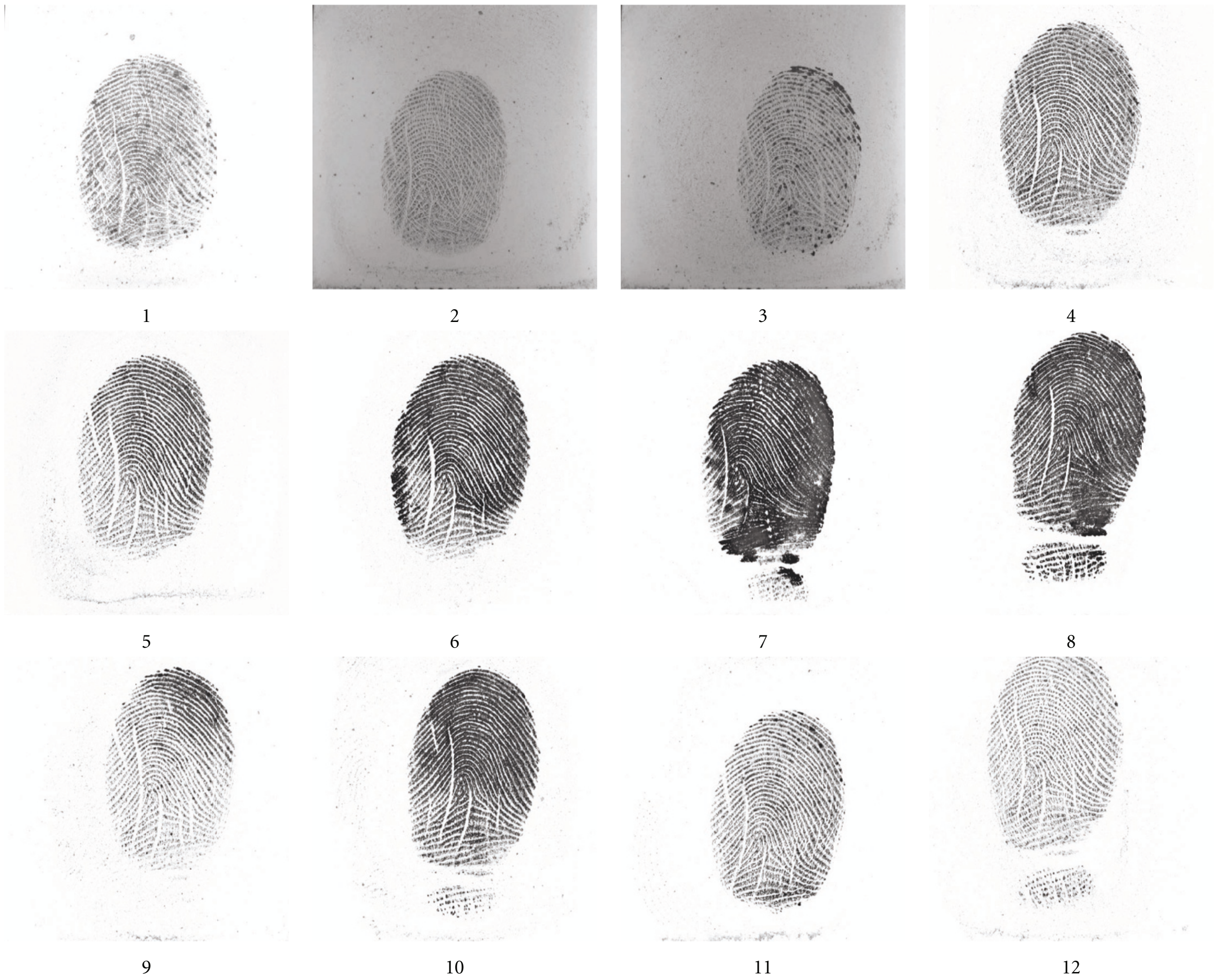


Figure 3: Images of the same finger in 12 sessions over several months on one scanner (left to right, top to down).

the data collection, the environmental conditions were also recorded on line (i.e., during data capture of the subject), which include inside and outside temperatures as well as the humidity of the room.

In each session (both in controlled and uncontrolled ones), subjects provided all 10 fingers on each of the 6 scanners. Participants presented their fingers in the following order: left small finger, . . ., left thumb, right thumb, . . ., right ring and right small finger. The order of visiting scanners was as follow: first they presented all 10 fingers (in the above mentioned order) in TST scanner, then in L-1, Cross Match, Precise, Lumidigm, and finally in Sagem scanner. In every session, 60, fingerprint images per person were obtained. In total, GUC100 database contains 71934 (= 100 × 10 × 6 × 12 − 66) fingerprint images. Few images were discarded due to the duplication or mislabeling.

In order to speed up data collection time and reduce human errors, we also developed a graphical user interface integrating all scanners. The program integrates image capturing functions from all scanners into a common interface and automatically saves the captured fingerprints according to the filename convention. The visual interface of this software is shown in Figure 4. This program made the data collection process easier and faster, and every session took about 5–7 minutes per subject.

In addition, two separate smaller fingerprint databases are also available that can be used for algorithm development [20]. They consist of fingerprint images from 45 and 40 subjects (these are different subjects from GUC100 database), respectively.

3.4. Fingerprint Image Quality. We applied NIST Fingerprint Image Quality (NFIQ) algorithm [21] to have an overview of image qualities in GUC100 database. For each fingerprint image, the NFIQ algorithm returns number 1 (best quality), 2, 3, 4, or 5 (worst quality). The aim of the this work is not comparing performances of individual scanners; therefore, here the NFIQ scores are not provided separately for each scanner. Figure 5 shows distribution of NIFIQ scores over all scanners (except TST). The NFIQ scores for TST images are not included due to the nature of images. The ordinate of the figure is given in percentage (%). It is worth noting that quality score may be affected by the order the subject uses the scanners, and other image quality algorithms can also be applied on the database.

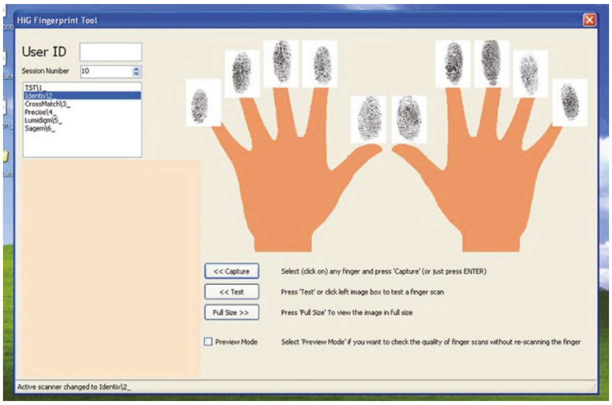
4. Interoperability and Parameters

4.1. Interoperability Performance and Matrices. From a customer perspective, performance interoperability of biometric components is very important. Performance interoperability is an essential measure to ensure that biometric subsystems from different suppliers are capable of generating and comparing samples and to meet at the same time an absolute level of performance within some margin [22]. Interoperability performance results of biometric components/systems provide a better choice on selecting products and thus reduce dependency on a single supplier. The GUC100 fingerprint database enables performance evaluation of not only components from a single supplier but also components from different suppliers in intra- and intersensor settings. Such interoperability can be viewed at two different processing levels which are image and minutiae template levels.

Figure 6 depicts interoperability perspective at the image level according to ISO interoperability schema [22]. In this figure, the blue octagons, blue ellipses, and green round rectangle represent fingerprint scanners (S), fingerprint images (FP) and IMage-based Comparators (IMC), respectively. In this figure (also in Figure 7), the subscripts denote product supplier's id. In Figures 6, 7, and 8, the TST, IDT, CMT, PBA, LUM, and SAG stand for TST, L-1 (Identix), Cross Match, Precise, Lumidigm, and Sagem, respectively. The A and B indicate some arbitrary suppliers. In addition, in this figure (also in Figure 7), the left part of comparators (i.e., IMC and MTC) represents enrolment and the right part represents verification. In Figure 6, the dimension of interoperability is 3. In first dimension there are 6 scanners (enrolment mode), in second dimension there are 2 IMC, in third dimension there are 6 scanners (verification mode).

Figure 7 depicts interoperability picture at the minutia level according to ISO interoperability schema [22]. In this figure, the blue octagons, blue circles, yellow round rectangles, yellow circles, and green round rectangle represent fingerprint scanners (S), fingerprint images (FP), Minutia Template Encoder (MTE), minutiae template (T), and Minutia Template Comparator (MTC), respectively. In addition, the superscripts (s) and (p) denote whether MTE/MTC produces/processes proprietary or standard data formats (e.g., ISO standard on finger minutiae [23]), respectively. In Figure 7, the dimension of interoperability is 5. In first dimension there are 6 scanners (enrolment mode), in second dimension there are 4 MTE (enrolment mode), in third dimension there are 4 MTC, in fourth dimension there are 4 MTE (verification mode), and in fifth dimension there are 6 scanners (verification mode).

4.2. Evaluation Parameters. The GUC100 database enables evaluation of various configurations of native and interoperability performances by focusing on some influencing factors. Such factors can be the following.



Select (click on) any finger and press 'Capture' (or just press ENTER)

Press 'Test' or click left image box to test a finger scan

Press 'Full Size' To view the image in full size

Select 'Preview Mode' if you want to check the quality of finger scans without re-scanning the finger

Active scanner changed to Identix\2_

Figure 4: Visual interface of the software tool.

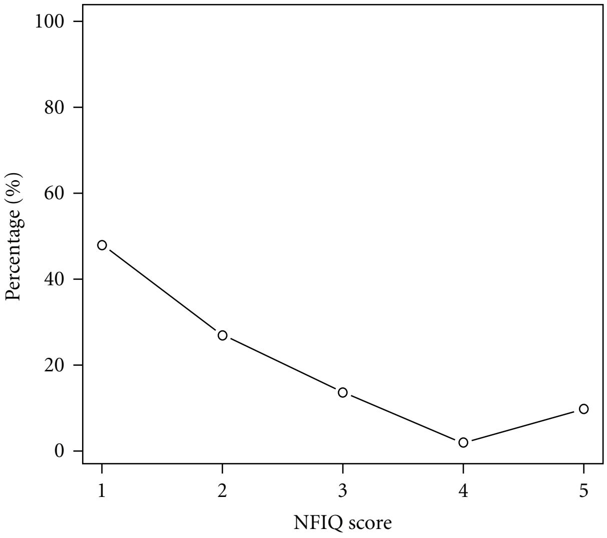


Figure 5: NFIQ distribution.

(i) *Fingerprint Scanner.* Scanner interoperability is an important issue, although not very much investigated. It has been shown that when enrolment and verification images are acquired by different scanners, the performance deteriorates significantly [24]. Recently, some methods have been proposed to address this problem [25, 26]. At the same time, interestingly, experimental evaluation indicates that fusing scores from different scanners results in better performance compared to fusing different instances of the same sensor [27, 28]. In addition to disparate fingerprint scanners, if MTE and MTC are also provided by different suppliers, then the interoperability schema gets more complex, for example, as the red path in Figure 7 highlights. The GUC100 database provides 6 intrascanner and 15 inter-scanner combinations for the specified pair of MTC and MTE.

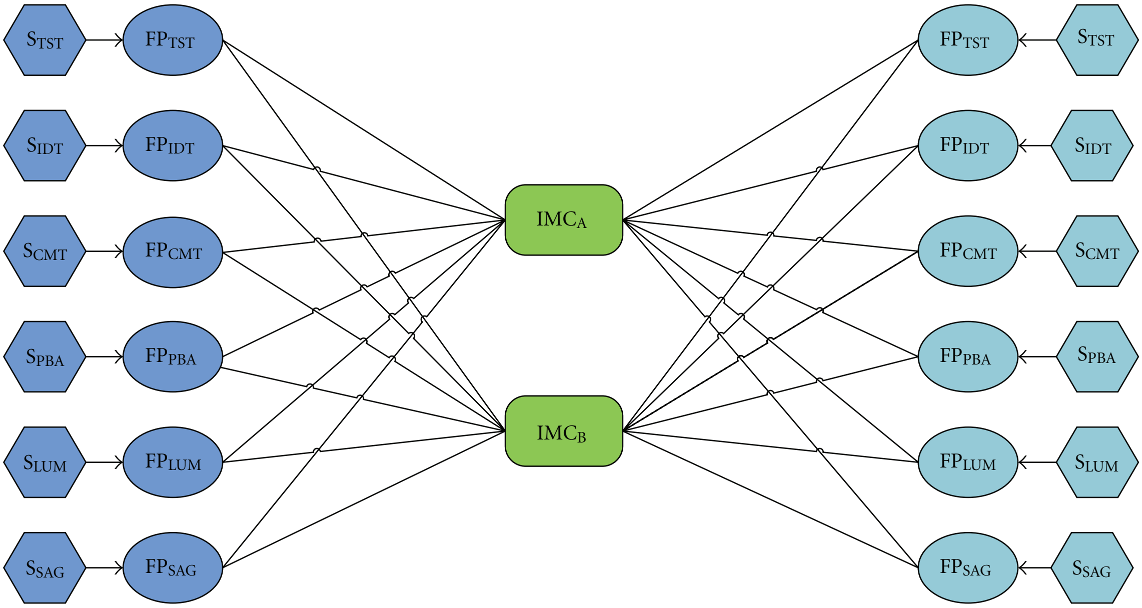


Figure 6: Interoperability picture at the image level.

(ii) *Image Quality*. Image quality is a very important factor that influences performance [29]. As mentioned earlier, each fingerprint image is associated with the NFIQ score that indicates its quality. Depending on application, one can test performance on various configurations in the context of image quality, for example, use only good quality images for the enrolment and then medium to low quality images for the verification; use only good quality images both for the enrolment and verification, and so forth.

(iii) *Session Type*. Usually in biometric system the enrolment phase is conducted in a controlled way where the image quality, finger positioning, and so forth. are controlled or instructed to some extent. On the other hand, the verification phase can be performed in a more relaxed environment where no feedbacks to the user are expected. Therefore, one may use images from controlled sessions only for enrolment while images from uncontrolled sessions only for verification. It is worth noting that the image quality and session type parameters might be somewhat correlated because in controlled session image qualities were usually (not necessarily always) better compared to in uncontrolled sessions.

In addition to aforementioned factors, the GUC100 database may enable performance evaluations in the context of some other parameters such as temperature, humidity, and finger type (e.g., thumb finger, small finger).

5. Experimental Results

We have applied a public and a commercial fingerprint verification software for validating the value of the database. The publicly available fingerprint verification software was NIST's MINDTCT and BOZORTH3 [30]. The second software was Neurotechnology VeriFinger which is commercially available [31]. In this work, we use images from all ten fingers for genuine comparisons, but due to the large number of comparisons (and consequently long time), we use images from only one finger (left index) for impostor comparisons. In addition, we use only one finger for estimating impostor scores and also compare only the same session samples. Thus by denoting $n = 100$ number of subjects, $k = 10$ number of fingers per subject, and $m = 12$ number of images per finger and also by assuming asymmetric template comparator, we can have about $132000 = n \cdot k \cdot m \cdot (m - 1)$ genuine comparisons (scores) and $118800 = m \cdot n \cdot (n - 1)$ impostor comparisons (scores). Performance metric curves in terms of FAR/FRR plots for each scanner are presented in Figure 8. Plots are given both when enrolment and verification scanners are the same and when they are different. The EERs of the curves are also shown in the legends of the plots.

As can be observed from the figures in general, when enrolment and verification scanners are different, EERs are higher compared to when they are the same. Tables 3 and 4 provide summarizing statistics (median and mean) of cross-scanner comparisons (interoperability) in terms of EER for Neurotechnology and NIST algorithms, respectively. In these tables, the last two columns indicate average performance degradation with respect to same scanner comparison which are computed according to the following:

$$\text{Degradation} = \frac{(\text{EER}_2 - \text{EER}_1)}{\text{EER}_1} \cdot 100\%, \qquad (1)$$

where EER_1 is the EER of same scanner comparison (i.e., no interoperability—second column) and EER_2 is the average (median or mean) EER of cross scanner comparison (i.e., interoperability—columns three and four in the tables).

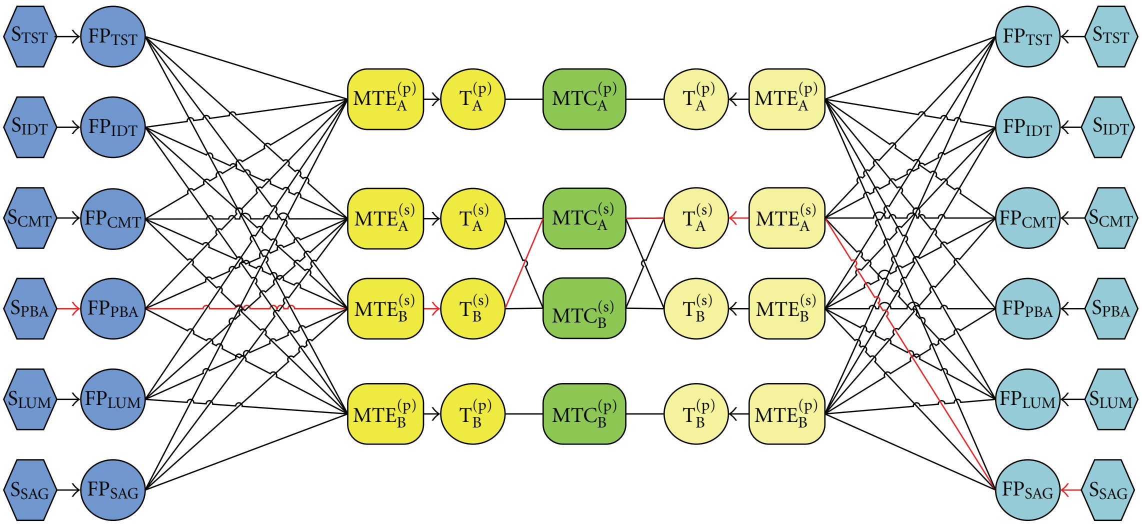


Figure 7: Interoperability picture at the minutia level.

Table 3: Neurotechnology: median, mean, and degradation in cross-scanner comparison (interop) in terms of EER.

Scanner	EER (no interop.), %	Median EER (interop.), %	Mean EER (interop.), %	Median degradation, %	Mean degradation, %
S1	1.56	2.88	4.196	84.62	168.97
S2	3.73	3.53	5.83	−5.36	56.3
S3	1.93	2.94	4.158	52.33	115.44
S4	1.89	4.04	5.17	113.76	173.54
S5	4.3	9.86	11.382	129.3	164.7
S6	3.19	3.54	5.212	10.97	63.39

Table 4: NIST: median, mean, and degradation in cross-scanner comparison (interop) in terms of EER.

Scanner	EER (no interop.), %	Median EER (interop.), %	Mean EER (interop.), %	Median degradation, %	Mean degradation, %
S1	4.94	7.85	11.578	58.91	134.37
S2	9.25	9.66	13.51	4.43	46.05
S3	4.95	7.46	11.866	50.71	139.72
S4	4.72	8	12.38	69.49	162.29
S5	26.3	29.88	29.828	13.61	13.41
S6	6	7.97	11.952	32.83	99.2

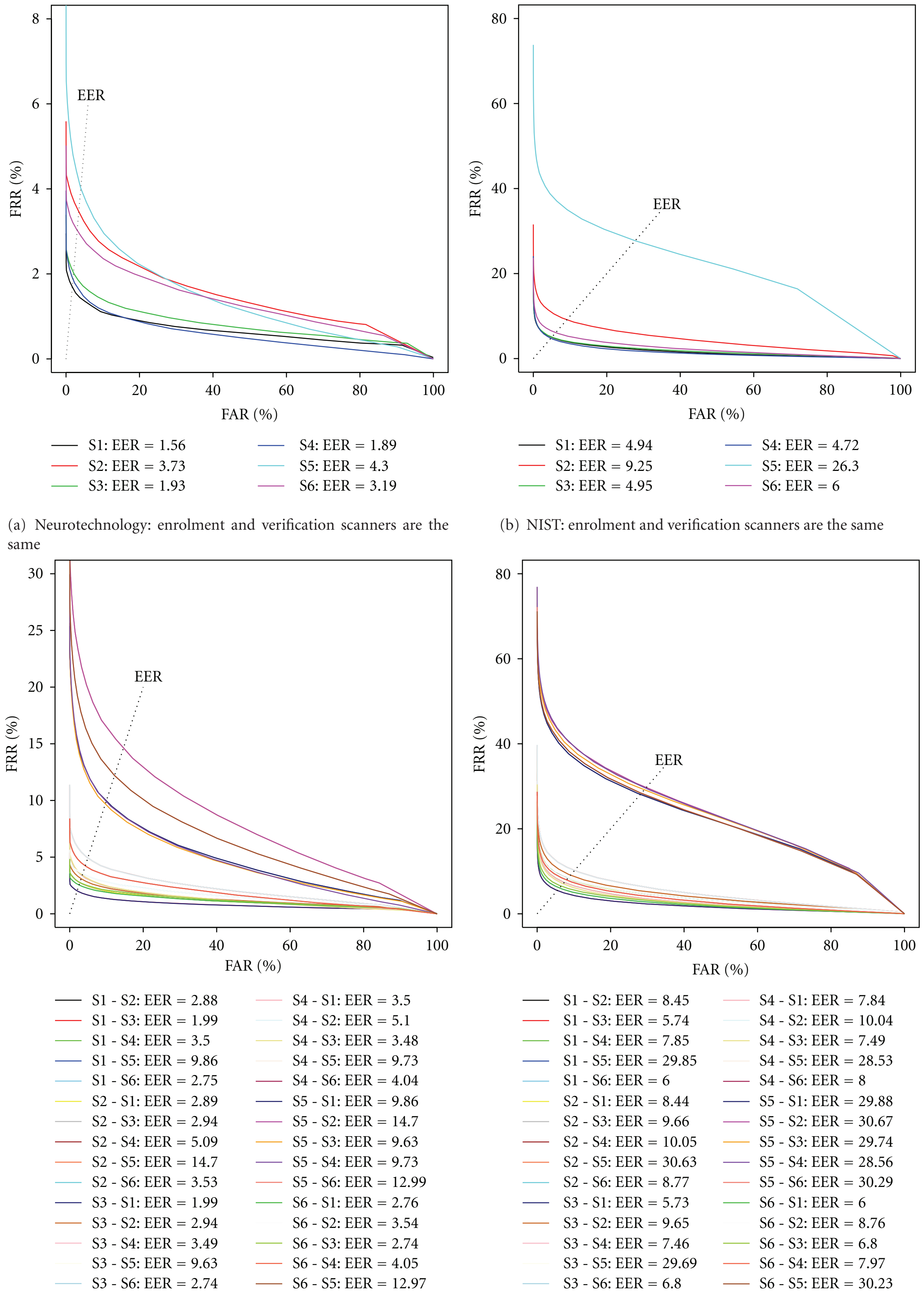
6. Limitations of the Database

There are few factors that may introduce bias, and one needs to take them into account when interpreting performance reports which are produced using GUC100 database. Since it is not always easy to recruit representative persons for experiments, the demographics of the subjects in GUC100 database in terms of gender (mostly men) and age (mostly adults) are not ideally balanced. Therefore, caution must be taken when analysing results in the context of the gender or when generalizing results to the other population of users like for instance, children or old people.

The order of finger presentation and order of scanner selection are fixed and not randomized. Although not investigated or proved yet, this may introduce bias when comparing performance of scanners (e.g., due to habituation). Thus, the main purposes of the GUC100 database are interoperability and benchmarking different algorithms but not comparing performance of different scanner technologies. In addition, interoperability results are primarily related to the scanner set used in GUC100, for other types of fingerprint scanners, the performance results might not be adequately generalized.

7. Summary

In this paper, we presented a GUC100 fingerprint database which was created for *in-house* performance and



(a) Neurotechnology: enrolment and verification scanners are the same

(b) NIST: enrolment and verification scanners are the same

(c) Neurotechnology: enrolment and verification scanners are different

(d) NIST: enrolment and verification scanners are different

Figure 8: Performance of public and commercial algorithms on GUC100.

interoperability evaluation of fingerprint recognition algorithms in technology testing. The GUC100 database consists of 71934 fingerprint images of all 10 fingers from 100 subjects which were acquired by using 6 different scanners. The data collection was carried out during February 2008–January 2009 at the campus of the Gjøvik University College (GUC) in Norway. The GUC100 database is referred as "in-house" (semi-public) which means that the database is freely available for researchers and practitioners provided that all testing shall be conducted in the premises of GUC. Thus, the interested parties (i.e., industry, research institution, independent developers, etc.) can visit GUC premises and perform training and testing by themselves or alternatively submit their (binary) algorithms to be tested by researchers at GUC.

Acknowledgment

This work is supported by funding under the Seventh Research Framework Programme of the European Union, Project TURBINE (ICT-2007-216339). This document has been created in the context of the TURBINE project. All information is provided *as is* and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. The European Commission has no liability in respect of this document, which is merely representing the authors' view.

References

[1] International Biometric Group, "Biometrics market and industry report 2009–2014," 2008,http://www.biometricgroup.com/reports/public/market report.php.

[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, New York, NY, USA, 2003.

[3] M. Arnold, C. Busch, and H. Ihmor, "Investigating performance and impacts on fingerprint recognition systems," in *Proceedings of the 6th Annual IEEE System, Man and Cybernetics Information Assurance Workshop (SMC '05)*, pp. 1–7, West Point, NY, USA, June 2005.

[4] "NIST special database 29," 2008, http://www.nist.gov/srd/nistsd29.cfm.

[5] "NIST special database 4," 2008, http://www.nist.gov/srd/nistsd4.cfm.

[6] "NIST special database 14," 2008, http://www.nist.gov/srd/nistsd14.cfm.

[7] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2000: fingerprint verification competition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 3, pp. 402–412, 2002.

[8] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: second fingerprint verification competition," in *Proceedings of the 16th International Conference on Pattern Recognition*, pp. 811–814, 2002.

[9] R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "Performance evaluation of fingerprint verification systems," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 1, pp. 3–17, 2006.

[10] "FVC2006: fingerprint verification competition," 2006.

[11] "FVC-onGoing: web-based automated evaluation system for fingerprint recognition algorithms," https://biolab.csr.unibo.it/fvcongoing/UI/Form/Home.aspx.

[12] J. Fierrez, J. Ortega-Garcia, D. Torre Toledano, and J. Gonzalez-Rodriguez, "Biosec baseline corpus: a multimodal biometric database," *Pattern Recognition*, vol. 40, no. 4, pp. 1389–1392, 2007.

[13] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon et al., "MCYT baseline corpus: a bimodal biometric database," *IEE Proceedings: Vision, Image and Signal Processing*, vol. 150, no. 6, pp. 395–401, 2003.

[14] P. Grother, W. Salamon, C. Watson, M. Indovina, and P. Flanagan, "Performance of fingerprint match-on-card algorithms, phase ii report," 2008, http://fingerprint.nist.gov/minexII/.

[15] S. Garcia-Salicetti, C. Beumier, G. Chollet et al., "BIOMET: a multimodal person authentication database including face, voice, fingerprint, hand and signature modalities," in *Proceedings of International Conference on Audio- and Video-Based Biometric Person Authentication*, vol. 2688 of *Lecture Notes in Computer Science*, pp. 845–853, 2003.

[16] ISO/IEC 19795-2:2007, "Information technology—biometric performance testing and reporting—part 2: testing methodologies for technology and scenario evaluation," 2007.

[17] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, Article ID 579416, 17 pages, 2008, special issue on Advanced Signal Processing and Pattern Recognition Methods for Biometrics.

[18] D. Gafurov, B. Yang, P. Bours, and C. Busch, "Independent performance evaluation of fingerprint verification at the minutiae and pseudonymous identifier levels," in *Proceedings of IEEE International Conference on Systems, Man, and Cybernetics*, 2010.

[19] Norwegian data privacy authority, http://www.datatilsynet.no/.

[20] "GUC100 multi-scanner fingerprint database for in-house (semi-public) performance and interoperability evaluation," http://www.nislab.no/guc100.

[21] M. D. Garris, E. Tabassi, and C. L. Wilson, "NIST fingerprint evaluations and developments," *Proceedings of the IEEE*, vol. 94, no. 11, pp. 1915–1925, 2006.

[22] ISO/IEC 19795-4, "Information technology—biometric performance testing and reporting—part 4: interoperability performance testing," 2007.

[23] ISO/IEC 19794-2:2005, "Information technology—biometric data interchange formats—part 2: finger minutiae data," 2005.

[24] A. Ross and A. Jain, "Biometric sensor interoperability: a case study in fingerprints," in *Proceedings of the International Biometric Authentication, the 8th European Conference on Computer Vision (ECCV '04)*, vol. 3087 of *Lecture Notes in Computer Science*, pp. 134–145, 2004.

[25] Y. Han, J. Nam, N. Park, and H. Kim, "Resolution and distortion compensation based on sensor evaluation for interoperable fingerprint recognition," in *Proceedings of International Joint Conference on Neural Networks (IJCNN '06)*, pp. 692–698, Vancouver, Canada, July 2006.

[26] A. Ross and R. Nadgir, "A thin-plate spline calibration model for fingerprint sensor interoperability," *IEEE Transactions on Knowledge and Data Engineering*, vol. 20, no. 8, Article ID 4358973, pp. 1097–1110, 2008.

[27] F. Alonso-Fernandez, R. N. J. Veldhuis, A. M. Bazen, J. Fierrez-Aguilar, and J. Ortega-Garcia, "Sensor interoperability and fusion in fingerprint verification: a case study using minutiae-and ridge-based matchers," in *Proceedings of the 9th International Conference on Control, Automation, Robotics and Vision (ICARCV '06)*, Singapore, December 2006.

[28] G. L. Marcialis and F. Roli, "Fingerprint verification by fusion of optical and capacitive sensors," *Pattern Recognition Letters*, vol. 25, no. 11, pp. 1315–1322, 2004.

[29] F. Alonso-Fernandez, J. Fierrez, J. Qrtega-Garcia et al., "A comparative study of fingerprint image-quality estimation methods," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 734–743, 2007.

[30] "NIST's Fingerprint verification software," 2009, http://fingerprint.nist.gov/NBIS/nbis_non_export_control.pdf.

[31] "Neurotechnology's VeriFinger 6.0.," 2009, http://www.neurotechnology.com/.