IET Biometrics

Special Issue: Mobile Biometrics

Small fingerprint scanners used in mobile devices: the impact on biometric performance

ISSN 2047-4938
Received on 14th April 2015
Revised on 18th December 2015
Accepted on 18th December 2015
doi: 10.1049/iet-bmt.2015.0018
www.ietdl.org

Belen Fernandez-Saavedra[1] ✉, *Raul Sanchez-Reillo*[2], *Rodrigo Ros-Gomez*[2], *Judith Liu-Jimenez*[2]

[1]IDTestingLab – Scientific Park, Carlos III University of Madrid, Avda. Gregorio Peces Barba, 1, 28918 Leganes, Madrid, Spain
[2]University Group for Identification Technologies – Electronic Technology Department, Carlos III University of Madrid, Avda. Universidad, 30, 28911 Leganes, Madrid, Spain
✉ *E-mail: mbfernan@ing.uc3m.es*

Abstract: Biometrics has burst into mobile technology. Fingerprint scanners are being embedded in smartphones and tablets supplying these devices with the security and usability provided by biometric authentication mechanisms. However, performance results obtained by biometric systems cannot be extrapolated to mobile devices. The conditions change, especially at capture process, due to the reduced sensing area of the scanners used. The impact of small fingerprint scanners on the quality and biometric performance of the system is studied. A database using three different fingerprint scanners has been collected and reduced-size images (i.e. 12 × 12 mm^2, 10 × 10 mm^2 and 8 × 8 mm^2) have been modelled by cropping the original ones. Performance testing has been conducted using one public and one commercial algorithm, and considering two application scenarios. One scenario in which enrolment and authentication are executed using the same small sensor included in the mobile device (i.e. cropped image against cropped image) and a second scenario in which enrolment is executed using an external larger sensor and authentication is done using the mobile device sensor (i.e. full image against cropped image). Results show the gradual worsening of quality and error rates as the size of the fingerprint scanner is reduced revealing a significant difference between the application scenarios analysed.

1 Introduction

In a short period of time some mobile devices have been equipped with biometrics offering new authentication mechanisms [1–3]. Currently, this new functionality is not only used for unlocking the device but also for other kind of applications that require a higher level of security such as online payments [4, 5], password management [6], mobile security services [7] and so on.

Nevertheless, the use of biometrics in mobile devices and especially, fingerprint authentication systems, cannot be compared with traditional biometric systems [8]. Mobile devices can be used in different situations which entails several positions (e.g. the user could be holding the device while sitting, or with the device on a table, or standing, or even walking or driving) and diverse ambient conditions. This fact modifies the user interaction significantly, altering the quality of the captured samples and diminishing the performance of the complete authentication process. This is also noticeable when using other modalities [9]. This effect can be even worse, considering the reduced sensing area of the fingerprint scanners that have been embedded in the current mobile devices. In 2005, Watson and Wilson [10] studied the effect of image size and compressions factors on biometric performance concluding that image sizes less than 320 × 320 pixels degrade matching performance. Considering a resolution of 500ppi, the recommended image size has to be higher than 0.64"× 0.64" (16.25 × 16.25 mm^2). In addition, more recent works [11] recommend that a fingerprint image captured by a mobile device shall have been at least 0.5" × 0.65" (12.7 × 16.50 mm^2). The fingerprint scanner Touch ID embedded in Apple devices has an area of 6.35 × 6.35 mm^2 [12].

Considering these circumstances, authors wanted to analyse the impact of using small fingerprint scanners in the whole authentication process. There are previous works that have already analysed this influence [12–14], but the cropping method used in these studies does not reproduce correctly the user interaction process. In those studies, images were cropped based on the centre of the fingerprint images or using the delta and core points; however, in most cases, images captured by small scanners do not include the core and delta of the fingerprints. When the area is too small, users have difficulties to place the centre of the fingerprint in the centre of the active area of the sensor.

Therefore, authors have examined the user's interaction process for a set of 589 subjects collecting a database of more than 180,000 fingerprint images using three different commercial fingerprint scanners. Based on those results, a cropping method has been designed obtaining three cropped databases: 12 × 12 mm^2, 10 × 10 mm^2 and 8 × 8 mm^2. To obtain performance results, these databases have been processed using two algorithms to observe any effects they could cause and to achieve more comprehensive outcomes. It is important to note that both the databases collection and the performance analysis have been conducted in accordance to the ISO/IEC 19795 'Biometric performance testing and reporting' series of standards [15].

In addition, in [14] the influence of the size of the template in performance rates is analysed. Likewise, authors also wanted to study this effect emulating the potential application scenarios that may happen using mobile technology. As a consequence, performance testing has been conducted analysing two relevant scenarios. The first one is a scenario (SC1) in which everything is executed in the mobile device, both enrolment and verification, by using the fingerprint scanner embedded in the device. Therefore, the authentication for this scenario is executed comparing cropped images of the same size. The second scenario (SC2) simulates when the user is enrolled externally to the mobile device (e.g. in an enrolment office). Such external fingerprint scanner is usually larger (e.g. conformant to the federal information processing standards [16]), and in SC2 the authentication is conducted using the smaller sensor embedded in the mobile device. Therefore, comparisons involve full-size images against cropped images.

To address the aforementioned work, this paper first describes sensors and algorithms used in the study and the database

Table 1 Fingerprint sensors characteristics

	Sensor D1	Sensor D2	Sensor D3
based technology	active thermal	active capacitive	active capacitive
active area size, mm^2	11.9 × 16.9	10.6 × 14	12.8 × 18
resolution, ppi	385	363	508
captured image size, pixels	180 × 256	152 × 200	192 × 270

collection procedures of the full-size images. Commercial sensors and algorithms have been anonymised to preserve their confidentiality, although for scientific reasons, the main features are provided as to be able to identify the technology behind them. Then, we explain the cropping method in Section 3. This is the method applied for obtaining images that model the use of small sensors. After that, Section 4 describes the full-size database collected and the cropped size generated and Sections 5 and 6 present results of the quality and the performance tests, respectively. The paper finishes by providing a comparison of the results with previous works and the conclusions are obtained.

2 Sensors, algorithms and data collection procedures

This section describes the tools and procedures for obtaining the full-size database that is needed for the study.

2.1 Fingerprint sensors

The fingerprint scanners selected for this study are three fingerprint scanners with the characteristics shown in Table 1.

2.2 Processing algorithms

For this work two algorithms have been used: one is the public distribution of the National Institute of Standards and Technology (NIST) fingerprint algorithm included in NIST Biometric Image Software [17]. This algorithm is referred as A1. The other is a commercial algorithm. This algorithm has been called A2. None of the algorithms was adjusted to the characteristics of the images needed for this study.

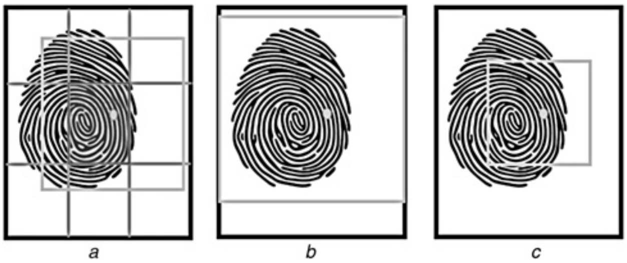


Fig. 2 *Cropping method applied*

a 10 × 10 mm^2 size, random position of the centre for cropping is selected based on this size
b 12 × 12 mm^2 size
c 8 × 8 mm^2 size

2.3 Database collection

As it was mentioned, the data collection process has been done according to the ISO/IEC 19795 standard [15]. Major details about this process are explained in the following paragraphs.

The database collection is carried out in indoor conditions, at a testing laboratory, where test subjects had to come twice with a separation of a minimum of 15 days. During the first day, test subjects had to conduct enrolment and acquisition processes. Throughout this visit, all the collection procedures were explained and, specifically, how to interact with fingerprint scanners correctly. Also, they were requested to provide personal data that may be significant for the fingerprint modality as well as to sign the acceptance forms according to data protection regulations. During the second visit, test subjects only had to carry out the acquisition process, with no further information from the operator.

For conducting all these steps, a capture application was developed. This application selects, for each visit and subject, the order of the fingerprint scanners and the fingers randomly, avoiding the influence of habituation and tiredness on the results. An operator who controlled the collection procedures at all times managed this application. The specific enrolment and acquisition processes are described below.

2.3.1 Enrolment: Enrolment is the process in which six fingers of one test subject are collected (i.e. thumb, index and middle fingers of both hands) to generate users' biometric references. To consider that a finger had been successfully enrolled, one image of the finger had to be correctly acquired and then, a second image of the same finger, also correctly acquired, was compared with the first image as to validate the enrolment.

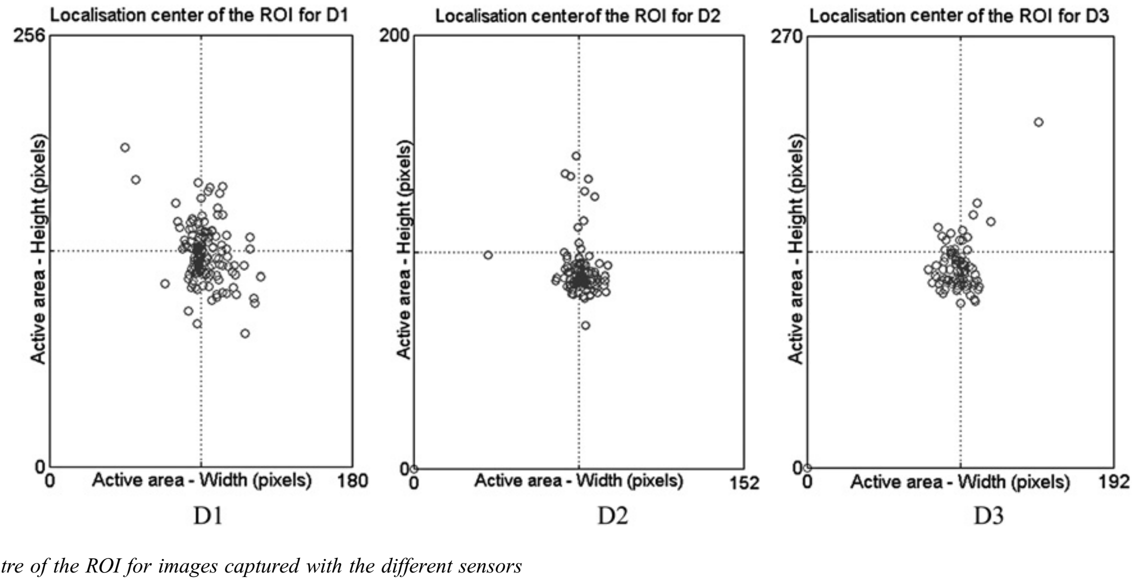


Fig. 1 *Centre of the ROI for images captured with the different sensors*

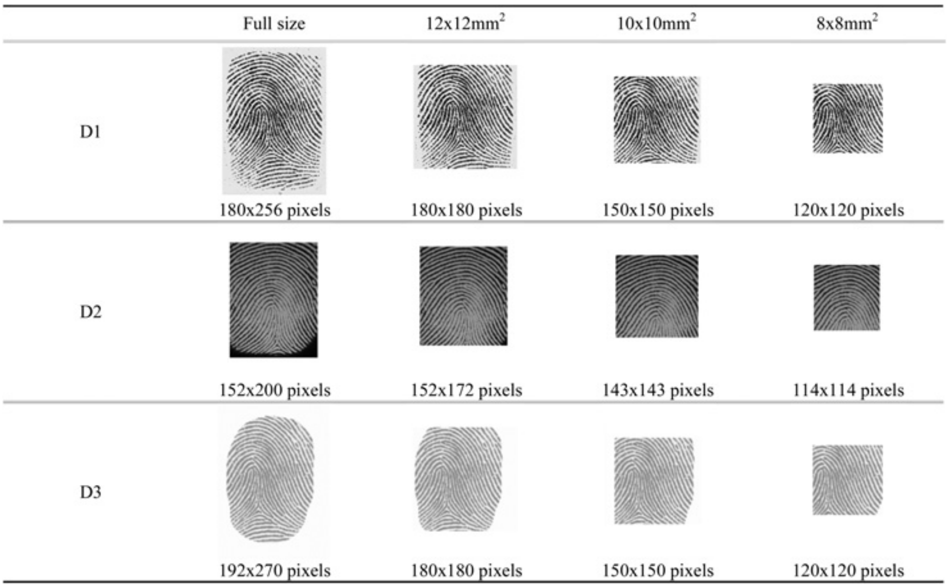


Fig. 3 *Examples of cropped database*

For the enrolment of each finger, test subjects had two transactions composed by three attempts. If after this number of attempts, the test subject did not successfully accomplish the aforementioned process, a failure to enrol (FTE) was claimed for that finger on that sensor.

It is important to emphasise that an image was correctly acquired if the quality score NFIQ [18] was equal or below 3 (NFIQ = 1 means that the quality of the image is very good, whereas NFIQ = 5 means that the quality of the image is very bad) and the operator considered that the fingerprint image contained an appropriate fingerprint image. Test subjects had a total of 30 s to provide an image. If not, a timeout error was reported and, a new attempt is started if more attempts are left. If the NFIQ was above 3, the image was discarded automatically by the application and a new attempt was required. If not, the operator had the possibility to discard it. If everything was correct, a second image was required. For this second image the operator did not have the possibility to discard it. If the NFIQ was equal or below 3, the image was directly compared with the previous image. If the result of the comparison was successful, that finger was enrolled and a new enrolment of another finger or in another sensor was required. If the comparison failed, the operator had the opportunity to check what happened and decide to re-start the attempt or discard the enrolment for that finger and that sensor.

The sequence of enrolment began with one finger of one hand. When that finger was enrolled using all the scanners, a new finger of the same hand was required. When all the fingers (i.e. thumb, index and middle fingers) of that hand were enrolled, the fingers of the other hand were requested.

2.3.2 Acquisition: Acquisition is the process in which six images of the different fingers are collected. To consider that the image of one finger had been successfully collected, the image of that finger had to be successfully compared with the biometric reference obtained at the enrolment process for the same finger. For doing it, test subjects had one transaction composed by three attempts. If after these attempts the test subject did not successfully accomplish the process, a failure to acquire (FTA) error was claimed for the corresponding finger in that sensor. In this case, an image was considered correctly acquired if the quality score NFIQ of the image was equal or below 4. During the acquisition the operator did not have the chance to discard any image. Again, if after 30 s the user did not provide an image, a timeout error was informed.

The sequence of acquisition began by one finger of one hand. Again, the finger and sensor orders were selected randomly. The selected finger was acquired in all sensors. When that finger was acquired in all sensors six times (or attempted to be acquired but a FTA error happened), then a new finger of this hand was required. When all the fingers of one hand were acquired, then the fingers of the other hand were required.

3 Cropping methodology

Once the full-size database was obtained, an approach for cropping the images was designed. One of the most important aspects of this work is to reproduce the user interaction when users have to present their fingerprint to the small fingerprint scanner embedded in a mobile device. Several approaches can be applied to obtain the cropped image depending on the selection of the centre:

(i) Select the centre as the centre of the captured fingerprint.
(ii) Select the centre based on delta and core points.
(iii) Select the centre as the centre of the sensing area.
(iv) Select a random centre considering a limited area.

The first and third methods reduce the size of the images but it is based on the idea that a user always places the finger in the same position of the sensing area. This is not realistic, especially for small sensors, for which it is difficult to place the centre of the fingerprint on the centre of the active area. Analysing the database of the full images for the three fingerprint sensors included in the study, the location of the centre of the captured fingerprint varies, as it can be seen in Fig. 1.

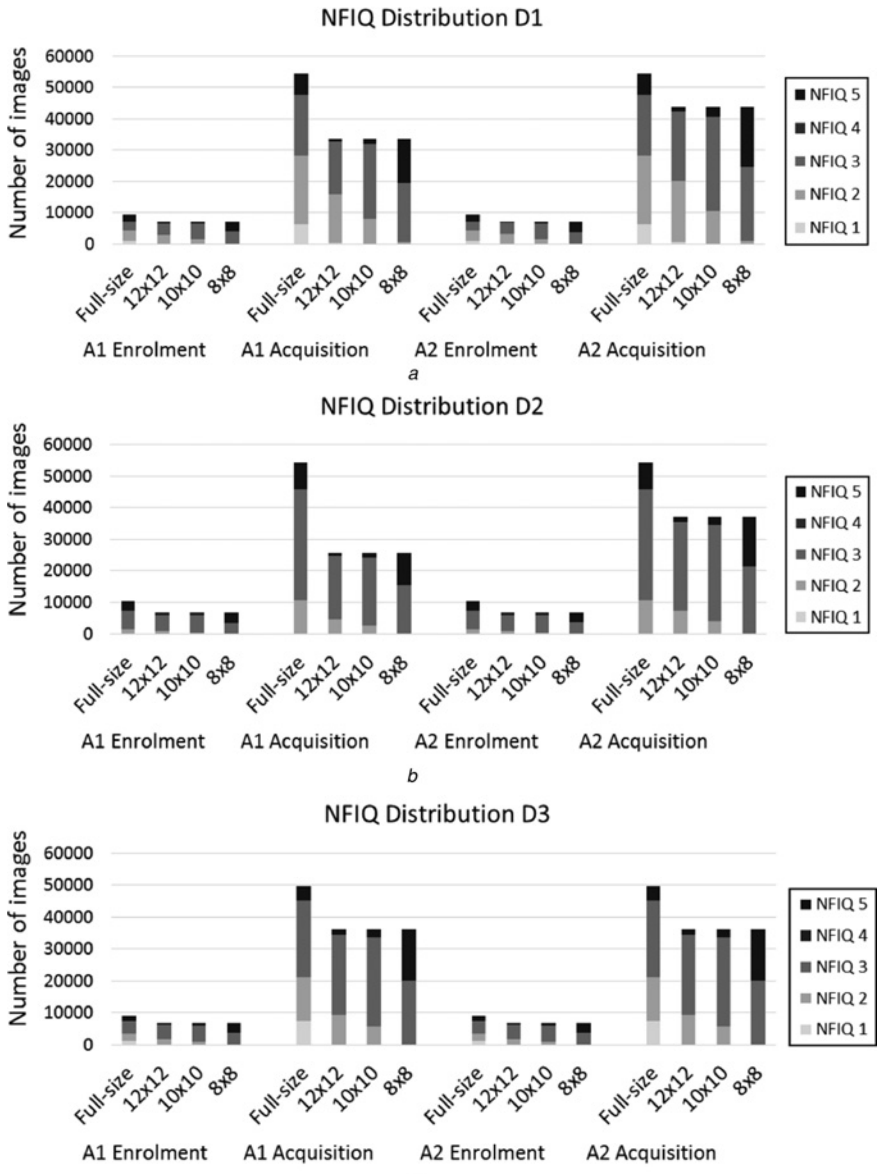
The second method is difficult to apply because many of the original images do not include either delta or core points of the fingerprint, as it was mentioned in the introduction.

Finally, the fourth method is the more realistic method because it is based on the idea that a user tries to place the fingerprint on the centre of the sensing area but there is a variability due to the difficulty to find it in small sensors as it can be seen in Fig. 1. Therefore, this is the method that has been used for cropping the images.

In particular, this method consists of selecting the centre of the cropped image considering a random position in a limited area. That limited area has been chosen based on the 10×10 mm^2 size

Table 2 Composition of the different databases: number of images

Images	D1	D2	D3	Total
original database	63 493	64 613	58 487	186 593
cropped database A1	40 466	32 133	42 871	115 470
cropped database A2	50 587	43 638	42 871	137 096



a

b

c

Fig. 4 *NFIQ distributions for D1 fingerprint scanner*

a NFIQ distribution for D1
b NFIQ distribution for D2
c NFIQ distribution for D3

and the possible variations across these dimensions. The possibilities considering the 12 × 12 mm^2 size entail a low variability of the user's placement of the finger and considering the 8 × 8 mm^2 size entail a high variability of the user's placement of the finger.

Once the centre has been randomly selected in the full-size image, then this image is cut according to the different sizes. The results of the cropping method are illustrated in Fig. 2. The blue region shows the area in which the centre of the cropped images can be placed and the yellow square provides the resulting areas of the cropping methods.

In addition, examples for the different fingerprint scanners can be seen in Fig. 3. It is important to note that for the D2 scanner, the 12 × 12 size has been cropped to 10.2 × 12 mm^2 due to the width of the original image being already smaller than 12 mm.

4 Composition of the full-size and cropped databases

On the basis of the collection procedures and the approach to crop the original images, four databases were generated. This section provides details about the test crew characteristics and the fingerprint images that compose each database.

4.1 Test crew

The database is formed by fingerprints from 589 subjects. Regarding the characteristics of this group, 57.05% are males and 42.95% are females being 84.21% below 30 years old, 10.02% between 31 and 50 years old and 5.77% older than 50 years old. Moreover, the percentage of subjects that have knowledge of IT products was 95.59%, and 34.64% of subjects are habituated to biometric products.

4.2 Fingerprint images

The number of fingerprint images that have been collected and used for generating the different databases is given in Table 2. Databases of cropped images were obtained from the full-size database after applying the cropping method to those images of which the enrolment and acquisition requirements are mentioned in Section 2.3. That is the reason why the cropped databases have less

Table 3 Acquisition errors for images acquired using A1

Capture device	Image size	A1		A2	
		FTE, %	FTA, %	FTE, %	FTA, %
D1	full size	8.97	12.18	8.60	4.14
	12 × 12	27.61	14.86	17.77	7.40
	10 × 10	74.13	17.12	46.46	11.02
	8 × 8	98.24	54.16	87.97	47.96
D2	full size	20.03	15.21	17.85	15.21
	12 × 12	68.33	18.30	17.63	19.09
	10 × 10	66.64	20.35	22.61	21.91
	8 × 8	94.59	54.82	30.81	57.19
D3	full size	11.82	8.83	11.40	8.83
	12 × 12	33.95	13.84	20.91	13.84
	10 × 10	75.89	16.42	26.62	16.47
	8 × 8	98.41	53.64	88.92	53.64

images than the original database and the number of images is different for each algorithm.

5 Quality analysis

The first test executed was a quality analysis of the images in the databases. This study has been focused on the distribution of the NFIQ score obtained, noting that the values given are integers between 1 and 5. Due to the different quality requirements specified for each process (i.e. NFIQ ≤3 for enrolment and NFIQ ≤4 for acquisition), results have been reflected separately.

Results are given in Fig. 4. It can be seen how the quality of the images gets worse as the size of the image is reduced, in spite some original images have been removed (as mentioned in Section 4.2) before obtaining the cropped databases. Most of the full-size images have an NFIQ of 3 or less, whereas the smaller images (8 × 8 mm^2 size) report an majority of NFIQ = 3 or higher. This is because the small images could be made from a low-quality area of the original image. A similar behaviour has been obtained for the image captured with the other sensors, being worse for D2. The active area of this sensor is smaller than the other sensors and the full-size images have already a larger number of images with an NFIQ of 3 or higher than the other sensors. These conclusions are equivalent for the cropped sets obtained for both algorithms.

From these results, it is possible to predict that performance error rates will be degraded as well, as the size of the images is decreased. However, there are other performance aspects that shall be analysed. All of them are explained in the next section.

6 Performance analysis

Performance evaluations entail the calculation of two kinds of parameters: error rates and throughput rates. Both types of rates have been obtained for both algorithms, the three fingerprint sensors and for all the databases in each scenario.

First, FTE and FTA error rates have been shown. These rates provide information about the enrolment and acquisition processes. These errors are common to both application scenarios because the comparison process has not been executed yet. After that, comparison results are given by means of the most typical biometric curves (i.e. ROC and DET). These curves have been generated using the BioSecure tool [19]. For a correct interpretation of results, the number of comparisons executed is provided in each case. At the end, throughput rates are presented using time measurements.

6.1 Results for the enrolment and acquisition processes

Table 3 shows error rates related to enrolment and acquisition processes. These rates increase as the image size is reduced. In particular, error rates for the smaller size (8 × 8 mm^2) rise drastically. This effect is analogous for all the sensors and for both algorithms.

Regarding comparisons, Table 4 gives the number of authentication attempts that have been conducted. The amount of comparisons is smaller as the size of the image is reduced due to the number of failures obtained during the enrolment and acquisition processes.

Moreover, Figs. 5 and 6 present the curves that reflect the obtained false match (FMR) and false non-match (FNMR) rates for A1 and A2 algorithms, respectively.

Observing the set of curves for A1, the degradation of error measurements when smaller scanners are used can be seen. There is a difference between application scenarios, as this degradation is lower when the cropped images are compared with the full-size images. For example, equal error rates (EER) for SC1 analysing the test case of 8 × 8 mm^2 are: 47.2% for D1, 27.8% for D2 and 47.9% for D3. Nevertheless, these rates for SC2 are reduced to 36.5% for D1, 22.7% for D2 and 34.5% for D3. This fact can also be observed analysing D2 results. For this scanner, the difference between full-size images and cropped images is smaller in comparison to the other scanners, especially considering the 12 × 12 mm^2 size. Therefore, the degradation obtained for this sensor is the lowest comparing SC1 to SC2 error rates (e.g. EER of 12 × 12 mm^2 is 7.8% in SC1 and 4.7% in SC2).

Regarding the error rate curves for A2, the tendency according to the different image sizes and the studied application scenarios is equivalent to A1, although absolute values provide better results for A2 (e.g. EER of full-size curves for A1 are higher than 0.5%, whereas for A2 they are lower than 0.1%).

Finally, Table 5 shows time measurements considering just genuine attempts. As opposed to error rates, the system throughput is improved as smaller is the size. This effect is similar for impostor attempts. Also, there is no significant difference for the two application scenarios that have been studied. However, there is

Table 4 Number of comparisons executed

Capture device	Image size	A1				A2			
		Genuine		Impostor		Genuine		Impostor	
		SC1	SC2	SC1	SC2	SC1	SC2	SC1	SC2
D1	full size	34.3 K	34.2 K	110.1 M	110.1 M	43.3 K	43.2 K	139.7 M	139.7 M
	12 × 12	27.1 K	33.5 K	69.2 M	107.7 M	36.1 K	39.3 K	104.9 M	127 M
	10 × 10	9.7 K	33.5 K	8.9 M	107.7 M	19.8 K	30.1 K	37.5 M	97.1 M
	8 × 8	655	33.5 K	40.0 K	107.7 M	2.7 K	11.6 K	1.1 M	37.6 M
D2	full size	26.3 K	26.3 K	74.4 M	74.4 M	37.1 K	37.1 K	107.7 M	107.7 M
	12 × 12	22.4 K	25.5 K	54.1 M	72.1 M	36.5 K	36.7 K	106.3 M	107.4 M
	10 × 10	11.4 K	25.5 K	13.4 M	72.1 M	34.7 K	36.7 K	94.9 M	107.0 M
	8 × 8	1.9 K	25.5 K	368.6 K	72.1 M	15.9 K	36.7 K	19.9 M	107.4 M
D3	full size	34.0 K	34.0 K	105.9 M	105.9 M	40.0 K	42.4 K	125.1 M	138.8 M
	12 × 12	25.6 K	33.7 K	59.8 M	102.8 M	29.1 K	41.2 K	81.3 M	134.9 M
	10 × 10	9.5 K	33.7 K	8.1 M	102.8 M	28.3 K	41.0 K	73.2 M	134.3 M
	8 × 8	632	33.7 K	34.8 K	102.7 M	2.2 K	38.5 K	865.9 M	126.17 M

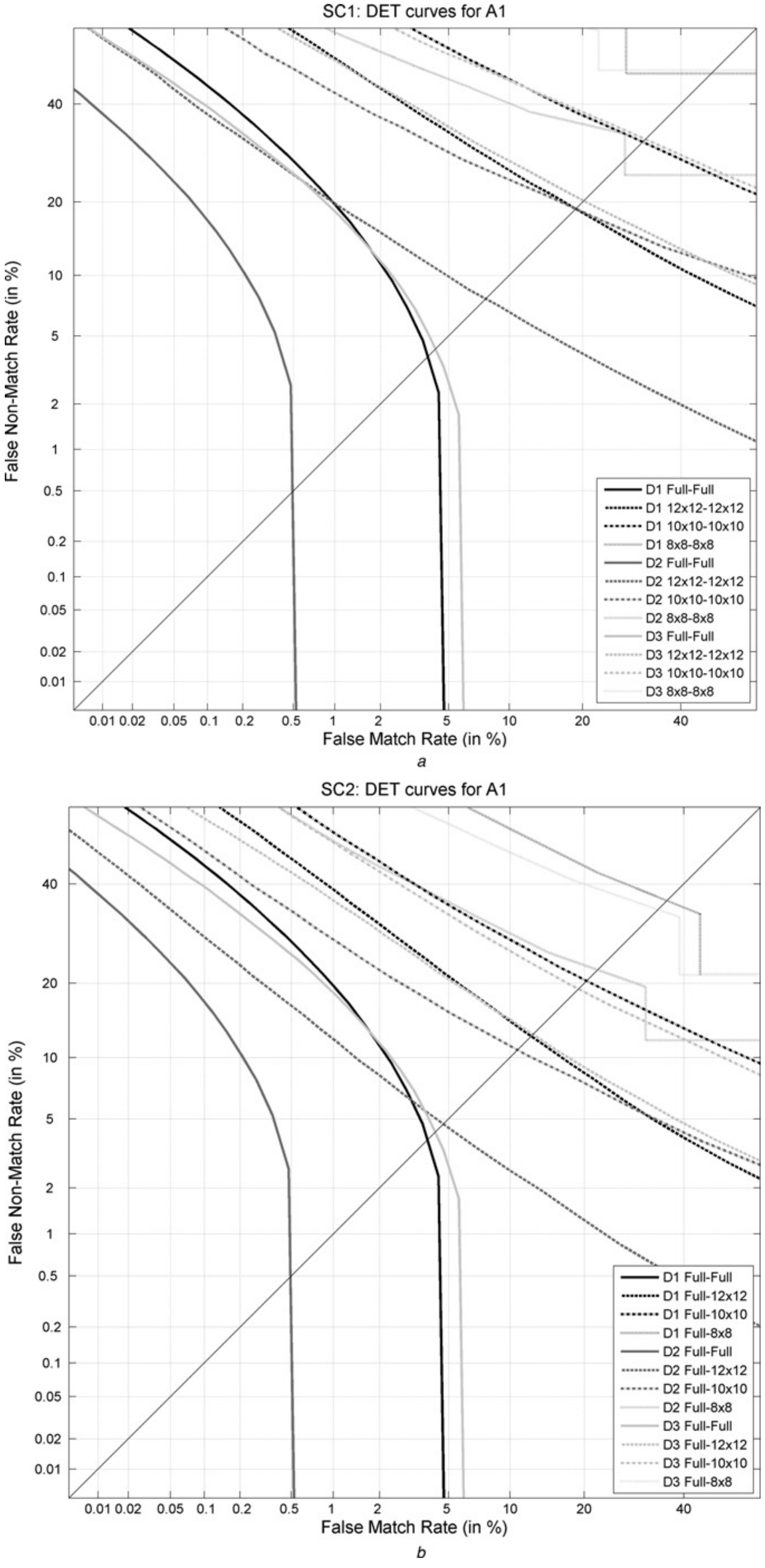
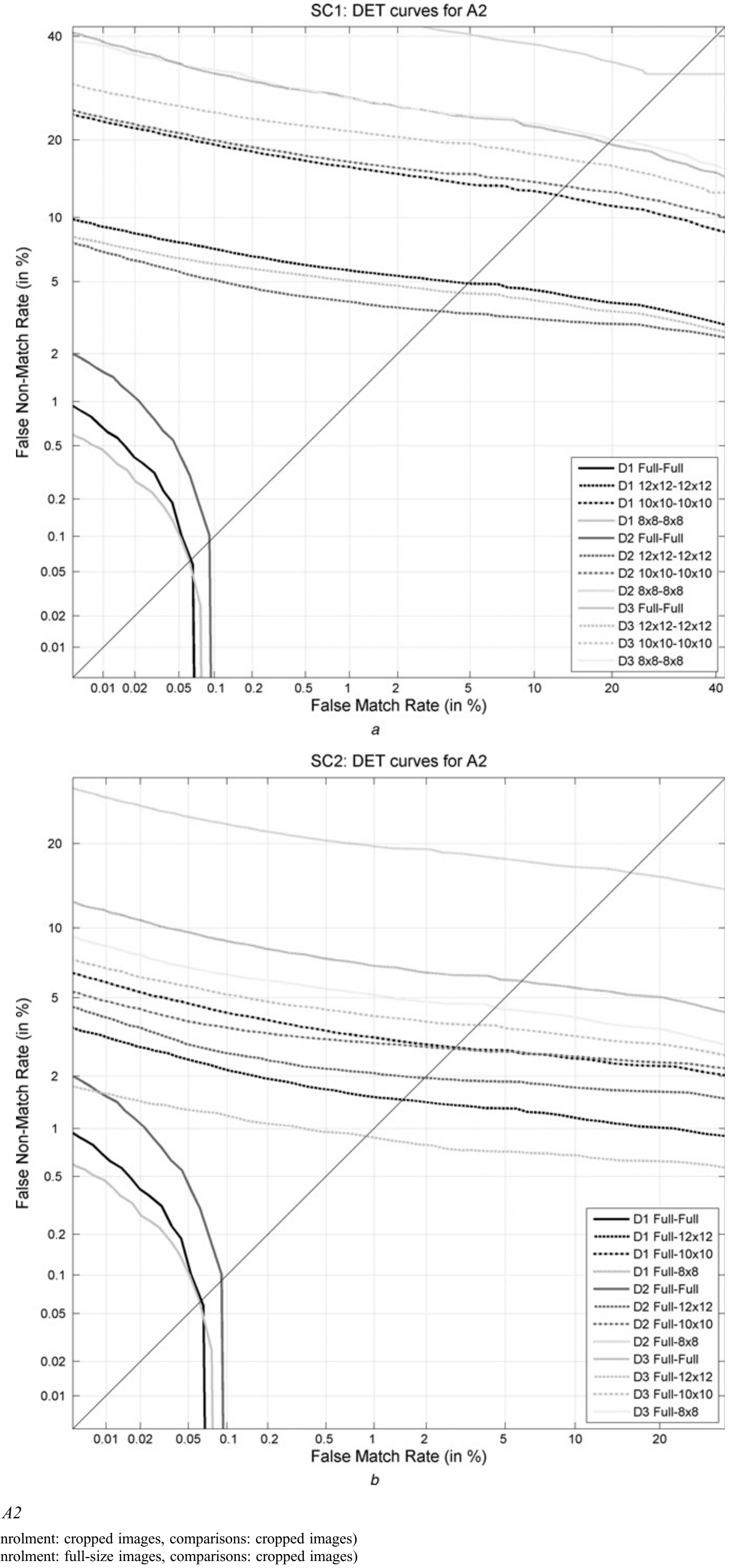


Fig. 5 *Error rates using A1*

a DET graph for scenario 1 (enrolment: cropped images, comparisons: cropped images)
b DET graph for scenario 2 (enrolment: full-size images, comparisons: cropped images)



a

b

Fig. 6 *Error rates using A2*

a DET graph for scenario 1 (enrolment: cropped images, comparisons: cropped images)
b DET graph for scenario 2 (enrolment: full-size images, comparisons: cropped images)

Table 5 Time measurements

Capture device	Image size	A1 Genuine		A2 Genuine	
		SC1, ms	SC2, ms	SC1, ms	SC2, ms
D1	full size	33.7 ± 48.1	33.7 ± 48.1	2.2 ± 1.8	2.2 ± 1.8
	12 × 12	21.6 ± 40.1	27.6 ± 49.6	1.0 ± 0.5	1.4 ± 0.8
	10 × 10	3.3 ± 13.4	3.6 ± 13.8	0.3 ± 0.5	1.0 ± 4.1
	8 × 8	0.1 ± 1.7	0.42 ± 2.9	0.0 ± 0.0	0.1 ± 0.3
D2	full size	11.7 ± 26.3	11.7 ± 26.3	1.1 ± 1.1	1.1 ± 1.2
	12 × 12	7.0 ± 20.5	8.3 ± 22.1	0.6 ± 2.6	0.1 ± 1.1
	10 × 10	1.9 ± 9.9	2.4 ± 10.9	0.4 ± 2.6	0.8 ± 0.7
	8 × 8	0.2 ± 1.8	0.2 ± 1.6	0.1 ± 2.0	0.2 ± 4.1
D3	full size	31.7 ± 48.9	31.7 ± 48.9	1.6 ± 0.2	2 ± 1.7
	12 × 12	22.2 ± 45.4	18.47 ± 37.6	0.2 ± 0.4	0.4 ± 0.5
	10 × 10	3.4 ± 17.0	2.5 ± 10.7	0.0 ± 0.9	0.9 ± 1.5
	8 × 8	0.1 ± 1.2	0.2 ± 1.8	0.6 ± 2.0	0.9 ± 0.5

a variation between algorithms: A2 has better throughput rates than A1.

7 Comparison with previous works

Once the analysis has been conducted, results show that biometric performance is degraded as the size of the captured image become smaller. It is difficult to compare these results to other published previous works because in those, testing conditions which may influence performance are different to the conditions considered in our work: algorithms are not specified (in [12]) or are not the same (in [13] the commercial algorithm used is Ultra-Scan's Modell 811 and in [14] the VeriFinger Matcher algorithm is used); the sizes of the images that have been analysed in those works are similar but not equal to the one used in this research (i.e. previous works study sizes between 20.32 × 25.4 mm^2 in [12] and 2.5 × 3.2 mm^2 in [14]); the sensors used to capture the original images have different characteristics (e.g. the size of the original images are 40.64 × 48.10 mm^2 in [12], 19.5 × 29.3 mm^2 in [13] and 14.6 × 15.69 mm^2 in [14]); databases have been collected from different fingers; error rates have been calculated based on different comparison processes (i.e. in [12] identification rates are computed, whereas in the other works [13, 14] verification rates are obtained), and so on.

Nevertheless, Fig. 7*a* provides the tendency of EER measured in this study for A2 (the commercial algorithm) and the EER calculated in [13] which is the work that presents the most similar testing characteristics (i.e. error rates have been analysed as in SC1 for analogous image sizes). As it can be observed, curves show a similar tendency. Performance rates got reduced for small image sizes. The difference between error rates could be due to the processing algorithm or due to the cropping method which in our study considers the influence of the user's placement variation. Results for our analysis are worse than those obtained in [13].

On the other hand, Fig. 7*b* shows the tendency of FNMR at FMR = 0.1% measured in the current study for A2 (the commercial algorithm) and the same rates calculated in [14], which is the work that analyses the two application scenarios SC1 and SC2. Analysing curves, it can be seen that results of [14] are opposite to the results obtained here, in which comparing small fingerprints to the original references gets better performance rates. This opposite effect could be due to the cropping method used in [14]. In [14], images are cropped using the fingerprint core. That means that the cropped images do not include minutia at the border, which are usually the minutia that have less quality. Hence, when comparing small size images to references of the same size, better error rates are obtained. However, the variation of FNMR in [14] is minimal (i.e. 1.7% in SC1 and 2.6% in SC2). Hence, it seems that the impact of small sensors in performance rates depends not only on the image size, but also on the user interaction with this kind of sensors. When these two effects are considered together, as it is done in this work, performance rates get less degraded if small images are compared with full-size references.

8 Conclusions

This paper has analysed the impact of using small fingerprint sensors in mobile devices. To conduct this analysis, a database of 589 users using three types of fingerprint scanners was collected including more than 180,000 images. Based on the observations when users interact with fingerprint scanners and analysing the captured images, a cropping method was designed to generate cropped images databases that model the images obtained by small sensors.

Then, these databases were processed using one public and one commercial algorithm considering two application scenarios in the analysis. The first one is when the same scanner (i.e. included in the mobile device) is used for enrolment and authentication. For simulating this situation, cropped images captured during enrolment were compared with cropped images captured during acquisition. The second one models the case of a different scanner being used for enrolment than for authentication. In this case, the original full-size enrolment images were compared with cropped images obtained during acquisition.

Considering these experiments, authors carried out quality and performance testing in accordance to the ISO/IEC 19795 [15] standard, achieving the following conclusions. The quality of the cropped images gets worse as the image size is reduced. Error rates during enrolment and acquisition suffer similar effects. It can be seen that FTE and FTA rates increase for smaller image sizes. This fact also happens because most of the errors in these processes are due to the non-compliance of quality requirements.

Regarding FMR and FNMR, two general tendencies have been observed. First, error rates get worse when the size of images is

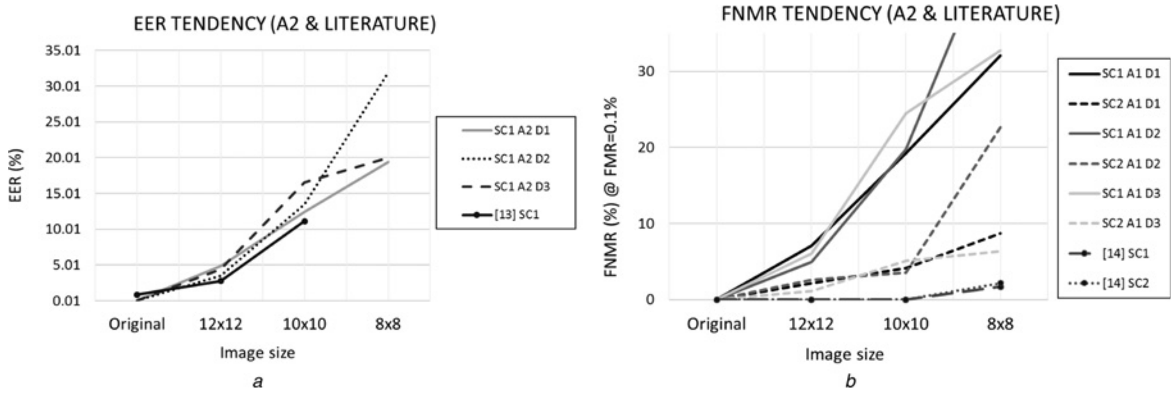


Fig. 7 *Comparison of A2 results to literature*

a EER tendency
b FNMR tendency

reduced. Second, this effect is compensated for the second application scenario. These results mean that the impact of small sensors embedded on mobile devices can be reduced if the enrolment is carried out externally to the mobile device, using a larger scanner. This kind of comparisons can be executed without affecting throughput rates as time measurements remaining equivalent in spite images were compared with the full-size references instead of the cropped size references.

Finally, it is important to note that the type of scanner and algorithms used for the authentication process may also impact the performance results obtained. As it can be seen, the commercial algorithm A2 gets better performance rates than the public algorithm A1.

9 References

1 'Apple – iphone 6 – Touch ID'. Available at https://www.apple.com/iphone-6/touch-id/, accessed 30 March 2015

2 'Samsung – Your finger is your key'. Available at http://www.samsung.com/global/microsite/galaxys5/features.html, accessed 30 March 2015

3 'htc – one – max, super simple accesibility'. Available at http://www.htc.com/us/smartphones/htc-one-max/#/, accessed 30 March 2015

4 'Paypal – Samsumg Pay simply and more securely'. Available at https://www.paypal-pages.com/samsunggalaxys5/us/index.html, accessed 30 March 2015

5 'Use Touch ID on iPhone and iPad – Apple Support'. Available at https://support.apple.com/en-is/HT201371, accessed 30 March 2015

6 'LassPass Password Manager Premium'. Available at http://www.androidcentral.com/app/lastpass-password-manager-premium, accessed 30 March 2015

7 'Samsumg Knox 2.0'. Available at http://www.samsung.com/global/business/mobile/platform/mobile-platform/knox/, accessed 30 March 2015

8 Sanchez-Reillo, R., Sierra-Ramos, D., Estrada-Casarrubios, R., *et al.*: 'Strengths, weaknesses and recommendations in implementing biometrics in mobile devices'. Proc. of Int. Carnahan Conf. on Security Technology (ICCST), Rome, Italy, 13–16 October 2014, pp. 39–44

9 Blanco-Gonzalo, R., Sanchez-Reillo, R., Miguel-Hurtado, O., *et al.*: 'Performance evaluation of handwritten signature recognition in mobile environments', *IET Biometrics*, 2014, **3**, (3), pp. 139–146

10 Watson, C., Wilson, C.: 'Effect of image size and compression on one-to-one fingerprint matching'. National Institute of Standards and Technology (NIST), NISTIR 7201, 2005

11 Orandi, S., McCabe, R.M.: 'Mobile ID device best practice recommendation varsion 1.0'. National Institute of Standards and Technology (NIST), NIST Special Publication 500–280, 2009

12 Orandi, S., Ko, K., Wood, S., *et al.*: 'Examination of the impact of fingerprint spatial area loss on matcher performance in varios mobile identification scenarios'. National Institute of Standards and Technology (NIST), NISTIR 7950, 2014

13 Schneider, J., Richardson, C.E., Kiefer, F.W., *et al.*: 'On the correlation of image size to system accuracy in automatic fingerprint identification systems'. Audio-and Video-Based Biometrie Person Authentication, Guildford, UK, 2003 (*LNCS*, 2688), pp. 895–902

14 Modi, S., Mohan, A., Senjaya, B., *et al.*: 'Fingerprint recognition performance evaluation for mobile ID applications'. Proc. of Int. Carnahan Conf. on Security Technology (ICCST), San Jose, California, USA, 5–8 October 2010, pp. 243–249

15 International Organization for Standardization: 'ISO/IEC 19795-1, information technology – biometric performance testing and reporting – part 1: principles and framework', ISO/IEC 19795-1:2006

16 FIPS Publication 202, personal identity verification (PIV) of federal employees and contractors, National Institute of Standards and Technology (NIST), August, 2013

17 Watson, C.I., Garris, M., Tabassi, E., *et al.*: 'User's guide to NIST biometric image software (NBIS),'. National Institute of Standards and Technology (NIST), NIST IR 7392, January 2007, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=51097, accessed 30 March 2015

18 Tabassi, E., Wilson, C.L., Watson, C.I.: 'Fingerprint image quality'. National Institute of Standards and Technology (NIST), NIST IR 7152, 2004

19 The BioSecure Reference and Evaluation Framework, biosecure tool, performance evaluation of a biometric verification system. Available at http://svnext.it-sudparis.eu/svnview2-eph/ref_syst//Tools/PerformanceEvaluation/, accessed 30 March 2015