Matching Fingerphotos to Slap Fingerprint Images∗

Debayan Deb1, Tarang Chugh1, Joshua Engelsma1, Kai Cao1, Neeta Nain2, Jake Kendall3, and Anil K. Jain1

1Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824
2Malaviya National Institute of Technology, Jaipur, India
3Digital Financial Services Lab, Caribou Digital, UK

E-mail: 1{debdebay, chughtar, engelsm7, kaicao, jain}@cse.msu.edu, 2nnain.cse@mnit.ac.in, 3jake@cariboudigital.net

Abstract

We address the problem of comparing fingerphotos, fingerprint images from a commodity smartphone camera, with the corresponding legacy slap contact-based fingerprint images. Development of robust versions of these technologies would enable the use of the billions of standard Android phones as biometric readers through a simple software download, dramatically lowering the cost and complexity of deployment relative to using a separate fingerprint reader. Two fingerphoto apps running on Android phones and an optical slap reader were utilized for fingerprint collection of 309 subjects who primarily work as construction workers, farmers, and domestic helpers. Experimental results show that a True Accept Rate (TAR) of 95.79 at a False Accept Rate (FAR) of 0.1% can be achieved in matching fingerphotos to slaps (two thumbs and two index fingers) using a COTS fingerprint matcher. By comparison, a baseline TAR of 98.55% at 0.1% FAR is achieved when matching fingerprint images from two different contact-based optical readers. We also report the usability of the two smartphone apps, in terms of failure to acquire rate and fingerprint acquisition time. Our results show that fingerphotos are promising to authenticate individuals (against a national ID database) for banking, welfare distribution, and healthcare applications in developing countries.

1. Introduction

A large proportion of individuals, especially economically disadvantaged, in developing countries around the world often lack any type of identification documents making it difficult for them to access government benefits, healthcare, and financial services. To address this critical need, efforts are being made to build large-scale national biometric databases to efficiently and effectively authenticate individuals at the point of service. The world’s largest biometric-based national ID program is the India’s Aadhaar [1]. It has already enrolled face, fingerprints, and irides of over 1.2 billion residents1. See Fig. 1. Given the suc-

∗This research is supported by caribou Digital who are funded by the Bill and Melinda Gates Foundation.

1https://uidai.gov.in/aadhaar_dashboard/india.php Accessed: Apr 2, 2018
cess of national ID programs, such as India’s Aadhaar, Pakistan’s NADRA\(^2\), and other programs, new opportunities to leverage fingerprint authentication for day-to-day transactions are rapidly becoming commonplace\(^3\).

In a National ID system, such as Aadhaar, a user provides their unique 12-digit Aadhaar number along with their fingerprint (Fig. 2 (a)). Next, an encrypted template of the fingerprint image is relayed to the Aadhaar server for authentication. If authenticated, the user is eligible to receive benefits or services (Fig. 2 (b)).

Given the scale at which National ID programs function, fingerprint recognition systems need to deliver higher authentication accuracy, usability, and low-cost authentication solutions. This requires: low-cost biometric readers, fast fingerprint acquisition, integration of widely available commodity smartphones in the sensing and authentication process, and ability to process noisy fingerprints for persons engaged in manual work [9].

TouchID by Apple in 2013 [10] dramatically changed the way we unlock our phones and use smartphones for mobile payment using our fingerprints. Since then mobile phones have also been introduced with iris and face recognition capabilities\(^4\). Still, for smartphone unlock and mobile payments, fingerprints appear to be by far the most popular. However, in the case of fingerprints, smartphones must be fitted with embedded capacitive fingerprint sensors which implies only new phones can be used in this way and restricts usage of the billions of existing smartphones. Additionally, embedded capacitive sensors typically feature a small sensing area (~ 90 × 90 pixels) that can capture only partial fingerprints which are not appropriate for matching with legacy slap fingerprints in the national ID databases.

Table 1. Related work on smartphone camera based fingerprint authentication.

| Study                  | Fingerprint Capture                  | Objective                                                                 | Database | Comments                                                                 |
|------------------------|--------------------------------------|---------------------------------------------------------------------------|----------|--------------------------------------------------------------------------|
| Derawi et al., 2011    | Smartphone Camera, 2 different models | Fingerphoto-to-fingerprint matching; No preprocessing                     | 22 subjects; 1,320 images | Neurotechnology VeriFinger 6.0 SDK \([3]\) used with RGB images; EER = 4.5% |
| Stein et al., 2012     | Smartphone Camera, 2 different models | Automatic fingerprint segmentation and on-device matching                  | 41 subjects; 656 images | Controlled capture set-up with smartphone held on a stand; EER = 19.1%  |
| Stein et al., 2013     | Smartphone Camera Video Sequences, 2 different models | Finger video sequences for fingerprint-to-fingerprint matching; anti-spoofing techniques | 37 subjects; 66 finger videos; 2,100 images | Constrained background and illumination; EER = 3.0% |
| Li et al., 2013        | Smartphone Camera, 3 different models | Fingerphoto quality estimation; quality assessment using matching performance | 25 subjects; 2,100 images | Manual segmentation of finger ROI; EER ranges between 2.7% and 35.3% based on estimated quality levels |
| Sankaran et al., 2015  | Smartphone Camera; Optical Reader    | Scattering Network based feature representation                            | 64 subjects; 5,120 images | Limited subject diversity; EER = 3.65%                                   |
| This study             | Smartphone Camera, 2 different apps; Optical Readers, 2 different models | In-situ evaluation of fingerprint-to-slap-fingerprint matching; database of 309 subjects with different occupations in India | 309 subjects; 7,976 images | Innovatrics IDKit SDK \([8]\); TAR = 98.01% @ FAR = 1.0%; baseline performance in matching fingerprint images from two different contact-based optical readers of TAR = 98.55% @ FAR = 1.0% |

\(^2\)https://www.nadra.gov.pk/
\(^3\)https://aadharpaymentapp.org/
\(^4\)https://spectrum.ieee.org/tech-talk/consumer-electronics/gadgets/new-samsung-galaxy-s8-unlocks-with-facial-recognition-iris-scanning

Figure 3. Fingerprint images (500 ppi) of the same finger captured using a (a) capacitive sensor embedded in a smartphone* (96 × 96 pixels), (b) smartphone camera (fingerphoto captured by App2) (380 × 540 pixels), and (c) optical slap fingerprint reader (Cross-Match) (330 × 512 pixels).

*Courtesy: Shenzhen Goodix http://www.goodix.com/
Figure 4. Demographics of 309 subjects who provided their fingerprints in our study. (a) Age (in yrs.), and (b) occupation. 57% of the subjects were males and the remaining 43% were females.

Figure 5. Process flow for the data collection process.

Our objective is to determine whether fingerphotos of sufficiently high resolution and fidelity\(^5\) can be used to authenticate individuals who were enrolled using optical slap fingerprint readers.

In literature, both fingerphoto-to-fingerphoto and fingerphoto-to-fingerprint matching protocols have been suggested. Derawi et al. [2] utilized two smartphones, Nokia N95 and HTC Desire, to capture 1,320 fingerphotos of 22 subjects. A commercial fingerprint feature extractor and matcher was employed for user authentication. Some studies have proposed pre-processing algorithms to enhance the performance of fingerphoto-to-fingerphoto matching [4], [5], [7]. Stein et al. proposed fingerphoto matching using video sequences, instead of static RGB fingerprint images, with uniform background and illumination [5]. Sankaran et al. [7] and Gupta et al. [11] utilized Scattering Network and Gabor Filters, respectively, for feature representations in the fingerphoto-to-fingerprint matching scenario. Stein et al. [5] and Taneja et al. [12] have explored the fingerprint anti-spoofing techniques for smartphone based authentication. However, these prior studies on fingerphoto based authentication are limited in scope due to (i) data collection in constrained settings, (ii) lack of representative subject demographics, and (iii) small number of subjects. Table 1 summarizes and compares these studies with our study. There also has been some prior work on smartphone camera based palmprint recognition [13, 14, 15].

\(^5\)Jan Krissler, a German hacker known as StarBug, used high resolution images captured by a digital single-lens reflex (DSLR) camera, from a distance of 3 meters to recreate the fingerprint ridge structure of German Defense Minister, Ursula von der Leyen. https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands
User authentication in large national ID programs, such as India’s Aadhaar and Pakistan’s NADRA, requires (i) high accuracy (e.g., FAR = 0.1% @ FRR = 2.0%), (ii) high usability, (iii) high throughput, (iv) low cost, and (v) low failure to acquire rate. Amid the growing concerns on user privacy, one of the major issues facing these national ID programs is the exclusion of people from receiving their benefits for individuals with poor quality fingerprints. According to NY Times, one recent study found that “20 percent of the households in Jharkand state had failed to get their food rations under Aadhaar-based (fingerprint) verification”. Another study found that 50,151 out of 85,589 surveyed welfare beneficiaries failed to access daily rations from 125 stores due to high false reject rates by fingerprints [16]. This is true in many rural areas of India, where most of the population is involved in manual work and have worn-out or damaged fingers. We believe, a fingerphoto based authentication is a plausible solution to authenticate individuals with different occupations in a developing country setting. With this objective, we evaluate two fingerphoto solutions developed in the form of two Android apps which we call as App1 and App2. Each App has been developed by a different commercial biometrics technology company.

2. Data Collection

A total of 309 subjects, above the age of 18 years, were enlisted for data collection in our study. Among these, 57% of the subjects were males and the remaining 43% were females. Fig. 4 shows the age and occupation distributions of the subjects. The data collection was conducted in India at two different locations: (i) an indoor lecture theater of MNIT, Jaipur, India, with typical indoor illumination (200 subjects), and (ii) an outdoor courtyard covered with a canopy in the village of Jhunjhunu, India, with natural lighting (109 subjects). In order to complete all the data collection in 5 working days, the enrollment and verification data was collected in the same session but at different stations. See Figs. 5, 6 and 7 for an illustration of process flow and data capture environments.

Fingerprint images of the two thumbs and two index fingers were first enrolled using an optical slap reader, CrossMatch Guardian 200 [17] (see Fig. 8) for a total of 2,472 enrollment images (309 subjects × 4 fingers × 2 impressions/finger). For verification, the two smartphone based contact-based optical fingerprint readers (500ppi) for enrollment. (a) CrossMatch Guardian 200 slap reader for enrollment [17]; (b) SilkID (SLK20R) fingerprint reader for establishing the baseline [18].

Figure 6. Data collection at MNIT, Jaipur, India, inside a lecture theatre with typical indoor illumination conditions.

Figure 7. Outdoors data collection environment in a courtyard covered with a canopy in the village of Jhunjhunu, Rajasthan, India.

Figure 8. Contact-based optical fingerprint readers (500ppi) for enrollment. (a) CrossMatch Guardian 200 slap reader for enrollment [17]; (b) SilkID (SLK20R) fingerprint reader for establishing the baseline [18].

Figure 9. Xiaomi Redmi Note 4 smartphone, which costs less than $150, was utilized for fingerphoto collection. [19].

6https://www.nytimes.com/2018/04/07/technology/india-id-aadhaar.html  
7These applications were developed by two vendors funded by Caribou Digital via their grant from the Bill and Melinda Gates Foundation.
Android apps were used to capture two impressions of the four enrolled fingers (two thumbs and two index fingers) from the same set of 309 subjects. Both the apps were installed on the same smartphone device, Xiaomi Redmi Note 4 (32GB model) [19] that costs less than $150. See Fig. 9. This smartphone model was selected as it provided the best specifications at an affordable price and is one of the best-selling devices on a popular e-commerce site in India. Other Android smartphones such as Lenovo K8 Plus [9] or Micromax Canvas Infinity [10] that cost less than $150 can also be utilized [11]. The two apps output both raw RGB fingerphoto and the corresponding processed grayscale fingerprint image. Figure 10 presents fingerprint images from contact-based fingerprint readers (CrossMatch and SilkID) and the corresponding fingerphotos from App1 and App2.

**App Design:** A user-friendly app design that allows high throughput and prevents human error was provided to the two vendors for designing their solutions. The proposed design enabled the apps to (i) initiate a new data capture transaction that links all collected fingerphotos to unique IDs, (ii) track and streamline the data capture process, (iii) recapture any required fingerphotos, and (iv) restart an ongoing transaction that safely deletes all images associated with the current transaction avoiding orphan images in storage. Fig. 11 demonstrates the flow of the fingerprint capture process on Android apps, and presents a sample pair of raw and the corresponding processed fingerphoto images captured by one of the apps. A common specification was chosen so that differences in the user interface specification would not confound the performance tests.

Given the fingerprint or fingerphoto, ISO (ISO/IEC19794-2:2011) [20] templates are extracted from them. Comparison scores (between slap fingerprints and fingerphotos) were generated using a COTS software [12]. To obtain a baseline performance, we also acquired two impressions of the two thumbs and two index fingers for 70 subjects, for a total of 560 fingerprint images, using SilkID (SLK20R) optical fingerprint reader [18].

In addition to fingerprint matching performance, the following metrics were also logged from the two apps: (i) acquisition time per fingerphoto, and (ii) failure to acquire. These metrics are related to the usability and throughput of each app.

### 3. Experimental Results

Verification performance [13] (1:1 comparison) is reported for (i) individual fingers, *i.e.* each of the two thumbs and two index fingers, (ii) fusion of two fingers from the same hand, *i.e.* right thumb fused with right index finger, and left thumb fused with left index finger, (iii) fusion of two fingers from different hands, *i.e.* two thumbs, and two index fingers, and (iv) fusion of all four fingers, *i.e.* two thumbs and two index fingers. In all of the fusion scenarios, score level fusion with simple sum rule was utilized. No score normalization was needed since the same COTS outputs all the scores in the range [0, 800]. Under verification scenario, we report True Accept Rate (TAR) @ False Accept Rate (FAR) of 0.1%.

Fingerphotos collected by each of the two apps are compared with enrollment images from the slap scanner. In all of the matching experiments, 4,944 genuine scores (309 subjects × 4 fingers × 2 enrollment impressions × 2 verification impressions) and 95,172 impostor scores (309 fingers × 308 fingers) are computed. In order to compare the performance of the two apps, we consider the following four scenarios:

- [9]https://www.amazon.in/Lenovo-k8-LENOVO-Venom-Black/dp/B075HJD15N
- [10]https://www.amazon.in/Micromax-Canvas-Infinity-Black-18/dp/B0725RBY9X
- [11]The two apps require a minimum camera resolution of 5 Megapixels.
Table 2. TAR @ FAR = 0.1% for the two fingerprint photo Apps and SilkID reader for matching with enrollment fingerprint images from CrossMatch reader.

| Verification experiment | TAR (%) @ FAR = 0.1% |
|-------------------------|----------------------|
|                        | App1 | App2 | SilkID |
| Right Thumb             | 37.07| 74.14| 97.83  |
| Left Thumb              | 46.35| 76.63| 94.20  |
| Right Index             | 21.17| 67.96| 97.46  |
| Left Index              | 18.97| 70.79| 92.39  |
| Two Thumbs              | 58.05| 89.86| 98.55  |
| Two Index fingers       | 27.97| 83.76| 98.19  |
| Right Thumb and Index   | 43.68| 86.43| 98.55  |
| Left Thumb and Index    | 47.51| 88.14| 94.20  |
| Fusion of all 4 fingers | 54.98| 95.79| 98.55  |

1. **Individual fingers**: Scores are computed separately for individual fingers (i.e., right thumb finger photos are only compared to right thumb fingerprints and right index finger photos are only compared to right index fingerprints). See Table 2 and Figure 12.

2. **Fusion of two thumb (index fingers) scores**: Scores from the two thumbs (index fingers) are fused using the sum rule (i.e., right thumb score is fused with left thumb score; right index finger score is fused with left index finger score). See Table 2.

3. **Fusion of right hand (left hand) thumb and index finger**: Scores from the right thumb and right index (or left thumb and left index) are fused by adding both scores together. See Table 2.

4. **Fusion of scores from all four fingers (two thumbs and two index fingers)**: Scores from all fingers (two thumbs and two indexes) are fused by adding all four scores together (i.e., right thumb, right index, left thumb and left index scores). See Table 2 and Figure 12.

We also report the **FAR @ FRR = 2.0%** for both apps under the four finger fusion scenario in Table 3. This metric of fixing the False Reject Rate (FRR) to 2% was suggested by Caribou Digital (the sponsors for app development and evaluation) based on conversations with government officials who suggested this would be a basic hurdle rate for devices to be used in some large government systems. This metric is important since one of the major problems identified in Aadhaar program is the “exclusion” of individuals with poor quality fingerprints from receiving their benefits. Limiting the false reject rate ensures that no deserving beneficiary is denied the due benefits. Hence low false rejects are often of higher priority than low false accepts.
Figure 12. ROC curves for Individual Fingers for (a) App1 and (b) App2.

Table 3. FAR (%) @ FRR=2.0% reported under the four finger fusion scenario.

|          | App1 | App2 | SilkID |
|----------|------|------|--------|
| FAR (%)  | 56.20| 0.86 | 0.00   |

The low observed performance of App1 is most likely because App1 does not wait sufficiently long for the smartphone camera to focus the fingerprint in the field of view before capturing its image, resulting in relatively poor quality fingerprint images. See also false reject and false accept cases for the two Apps in Figs. 13 and 14, and the failure to acquire rates in Table 5.

3.1. Fingerphoto-to-Fingerphoto Matching

In addition to fingerphoto-to-legacy-fingerprint matching, we also report the performance on matching fingerphoto-to-fingerphoto captured by the same App. Although, the two fingerphotos of the same finger are captured consecutively within a maximum time gap of 30 sec-
Table 4. TAR @ FAR = 0.1% for the fingerphoto-to-fingerphoto matching for the apps: App1 and App2. Here, RT, LT, RI, LI, and FF refers to Right Thumb, Left Thumb, Right Index, Left Index, and Four Finger Fusion, respectively.

|       | RT    | LT    | RI    | LI    | FF    |
|-------|-------|-------|-------|-------|-------|
| App1  | 46.95 | 50.76 | 27.48 | 22.15 | 72.14 |
| App2  | 80.82 | 82.88 | 83.56 | 85.62 | 99.66 |

onds, contact-less capture environment and hand movement induce large variations in the two fingerphotos. Table 4 presents the TAR @ FAR = 0.1% for matching fingerphoto-to-fingerphoto of individual fingers and four finger fusion for the two Apps.

3.2. Baseline Performance

In order to establish a baseline verification performance, we compute comparison scores between CrossMatch enrollment images and SilkID verification images. We then plot the ROC curve for the baseline as shown in Figure 12.

3.3. Failure Cases

In order to gain a deeper insight into the verification performances for the two apps, we observe example images where (i) the genuine comparison scores between the enrollment images and the images from the app are very low (false reject), and (ii) the impostor scores between the legacy enrollment images and the images from the app are relatively high (false accept). See Fig. 13. In addition, Table 5 shows the failure to acquire rates (%) for the two apps and the two optical sensors.

Table 5. Failure to Acquire Rates (%) for App1, App2, Crossmatch slap scanner, and SilkID fingerprint reader. The total number of acquisitions is 2,472 each for CrossMatch slap scanner, App1, and App2, and 560 for SilkID reader.

|       | App1  | App2  | CrossMatch | SilkID |
|-------|-------|-------|------------|--------|
| FTA (%)| 28.5  | 13.0  | 0.1        | 4.0    |

3.4. Fingerprint Image Quality

We also compute the fingerprint image quality based on NIST Fingerprint Image Quality (NFIQ) [21]. We present histograms for the apps based on two different covariates: (i) NFIQ values in the range [1,2,3] which are images considered to be of “good” quality, and (ii) NFIQ values in the range [4,5] which comprise of “poor” quality fingerprint images (see Figure 15).

4. Conclusions

This study presents data collection protocol and analysis of an in-situ evaluation of matching fingerprint to slap fingerprint images. A total of 309 subjects, employed in different occupations, such as construction, gardening, etc. were enrolled using a contact-based slap reader, and verified using fingerprint captured by two contact-less Android apps installed on a commodity smartphone. A baseline performance in matching accuracy was established based on fingerprint images from a different contact-based optical reader. Experimental results show that score fusion of four fingers using sum rule is able to achieve a TAR of 95.79% at FAR of 0.1% for one of the apps, compared to the baseline performance of TAR = 98.55% at FAR = 0.1%. However, the best performance of individual fingers in matching fingerprint photos to slap fingerprints is only 76.63% TAR @ FAR = 0.1%. This is significantly less than the acceptable requirements. Nevertheless, the accuracy of fingerprint matching to slap images for a fusion of four fingers gives us encouragement for further developing the fingerprint technology and both companies are currently engaged in R&D to significantly improve performance and refine liveness detection. Future work would include (i) robustness to fingerprint acquisition challenges (as shown in Fig. 16), (ii) high throughput, and (iii) improved quality of captured fingerprint photos.
References

[1] Aadhaar, Unique Identification Authority of India (UIDAI), Govt. of India. https://uidai.gov.in, 2018.

[2] Mohammad Omar Derawi, Bian Yang, and Christoph Busch. Fingerprint recognition with embedded cameras on mobile phones. In International Conference on Security and Privacy in Mobile Information and Communication Systems, pages 136–147. Springer, 2011.

[3] Neurotechnology VeriFinger Fingerprint SDK. http://www.neurotechnology.com/verifinger.html. Accessed: 2018-03-28.

[4] Chris Stein, Claudia Nickel, and Christoph Busch. Fingerprint recognition with smartphone cameras. In Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), pages 1–12, 2012.

[5] Chris Stein, Vincent Bouatou, and Christoph Busch. Video-based fingerprint photo recognition with anti-spoofing techniques with smartphone cameras. In International Conference of the Biometrics Special Interest Group (BIOSIG), pages 1–12, 2013.

[6] Guoqiang Li, Bian Yang, Martin Aastrup Olsen, and Christoph Busch. Quality assessment for fingerprints collected by smartphone cameras. In IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pages 146–153, 2013.

[7] Anush Sankaran, Aakarsh Malhotra, Apoorva Mittal, Mayank Vatsa, and Richa Singh. On smartphone camera based fingerprint authentication. In IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), pages 1–7, 2015.

[8] Innovatrics IDKit Fingerprint SDK. https://www.innovatrics.com/idkit-fingerprint-sdk/. Accessed: 2018-03-28.

[9] Davide Maltoni, Dario Maio, Anil K Jain, and Salil Prabhakar. Handbook of Fingerprint Recognition. Springer Science &amp; Business Media, 2009.

[10] Apple announces iphone 5s—the most forward-thinking smartphone in the world. https://www.apple.com/newsroom/2013/09/10Apple-Announces-iPhone-5s-The-Most-Forward-Thinking-Smartphone-in-the-World/, 2013.

[11] Saksham Gupta, Sukhad Anand, and Atul Rai. Fingerprint extraction using smartphone camera. arXiv preprint arXiv:1708.00884, 2017.

[12] Archit Taneja, Aakriti Tayal, Aakarsh Malhotta, Anush Sankaran, Mayank Vatsa, and Richa Singh. Fingerphoto spoofing in mobile devices: A preliminary study. In IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), pages 1–7, 2016.

[13] Shoichiro Aoyama, Koichi Ito, Takafumi Aoki, and Haruki Ota. A contactless palmprint recognition algorithm for mobile phones. In International Workshop on Advanced Image Technology, pages 409–413, 2013.

[14] Nuno Freire Moco, Paulo Lobato Correia, and Luis Ducla Soares. Smartphone-based palmprint recognition system. In IEEE 21st International Conference on Telecommunications (ICT), pages 457–461, 2014.

[15] Chhaya Methani. Camera based palmprint recognition. Master of Science (Research) in Computer Science, IIT Hyderabad, 2010.

[16] Hindustan Times. Aadhaar-based projects failing the poor, says Andhra govt study. https://www.hindustantimes.com/india/aadhaar-based-projects-failing-the-poor-says-andhra-govt-study/story-7MFBCeJcf185Lc5z8tON6L.html, 2015.

[17] Crossmatch. Crossmatch Guardian 200. https://www.crossmatch.com/wp-content/uploads/2017/05/20160726-DS-En-Guardian-200.pdf. Accessed: 2018-03-28.

[18] SilkID SLK20R Fingerprint Reader. http://www.silkid.com/wp-content/uploads/2017/02/Silk20-Reader-Brochure-v0.7.pdf. Accessed: 2018-03-28.

[19] Amazon. Xiaomi Redmi Note 4. https://www.amazon.com/Xiaomi-5-5-Inch-Unlocked-Smartphone-Warranty/dp/B06Y1KYR6R. Accessed: 2018-03-28.

[20] ISO/IEC 19794-2:2011, Biometric Data Interchange Formats. https://www.iso.org/standard/50864.html, 2011.

[21] E. Tabassi, C. Wilson, and C. Watson. Fingerprint Image Quality, NFIQ. NIST Internal Report 7151, NIST, 2004.