Contactless Finger and Face Capturing on a Secure Handheld Embedded Device

Axel Weissenfeld, Bernhard Strobl, Franz Daubner
Austrian Institute of Technology
Donau-City-Straße 1, 1220 Vienna, Austria
{firstname.lastname}@ait.ac.at

***Abstract*— Traveler flows and crossings at the external borders of the EU are increasing and are expected to increase even more in the future; trends which encompass great challenges for travelers, border guards and the border infrastructure. In this paper, we present a new handheld device that enables border control authorities to check European, visa-holding and frequent third country travelers in a comfortable, fast and secure way. The mobile solution incorporates new multimodal biometric capturing and matching units for face and 4-finger authentication. Thereby, the focus is on the capturing unit and fingerprint verification, which is evaluated in detail. The use in border control requires high security measurements and trustworthy use of credentials, which are also presented. Tests of the handheld device at a land border indicate great acceptance by travelers and border guards.**

Keywords*— heterogeneous computing platform, biometrics on the move, secure embedded hardware

I. Introduction

International movement is on the rise and, consequently, so are the numbers of border crossings each year. The total number of border crossings significantly increases from 700 million in 2011 to 887 million in 2025 [15]. Hence, border crossings and identity checks by law enforcement agencies (LEAs) should be made as smooth and rapid as possible without compromising security. At the same time it might become necessary to establish ad-hoc checkpoints, which require mobile authentication devices. The recent refugee crisis is an example but so are security measures surrounding large events like G20 or football cups.

Within the scope of the MobilePass project [10] a technologically advanced mobile equipment (denoted as MobilePass device) was developed, which will allow border control authorities to carry out identity checks in a comfortable, fast and secure way. The mobile equipment needs to bridge facilitation and usability with security requirements.

Current commercial products have not satisfactorily solved these requirements yet. For instance, many devices do not provide a face scan; e.g. SPC MDR-1[23]. Many devices integrate a traditional touch-based sensor for fingerprint recognition; e.g. SEEK Avenger [24]. Hence, we try to enhance current solutions by incorporating new advanced features as displayed in Fig. 1. For instance, the embedded device incorporates reading the eMRTD [8] (including MRZ and chip), facial image and contactless fingerprint capturing as well as matching against the passport stored chip image, cross- and validity checks and background systems (or hitlist) information display, all on a secure and trusted platform.

Advances in digital chips and vision sensors with associated image analysis are now likewise paving the way for new applications. Embedded vision opportunities in mobile electronics devices for border control include functions such as passport scanning and capturing of biometric traits for identity checks. We use a single visual sensor for passport scanning as well as face and fingerprint capturing. A biometric passport and visa contain picture and user information areas for visual inspection (specified in the standard ICAO 9303). The machine-readable zone (MRZ) can be optically captured and processed using optical character recognition (OCR) methods [16]. To cope with various illumination conditions as occurring in mobile applications is still a challenge for MRZ scanning. The MobilePass device cannot validate a passport yet, because many security features (e.g. microprinting or security inks) can only be checked with specialized equipment like an ultraviolet lamp or a magnified glass [17].

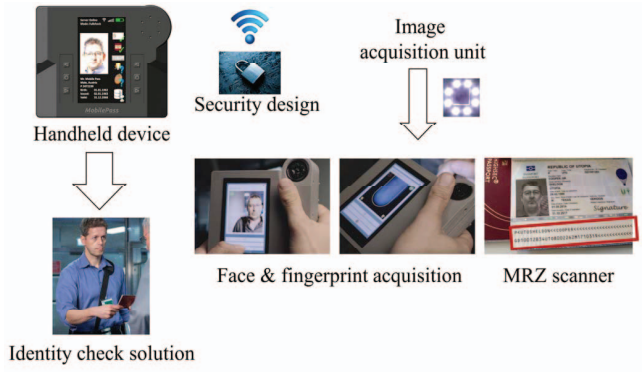


Fig. 1: System overview of the developed secure handheld device for identity checks. Vision sensors are used to scan passport data (MRZ) and biometric traits (face and fingerprints).

The fingerprint authentication is based on a fingerphoto captured with a visual sensor instead of integrating an additional touch-based fingerprint sensor. Users prefer touchless acquisition systems to classical touch-based solutions according to [18]. Fingerphoto authentication systems are based on smart phones [20], webcams [22] and digital cameras [21] as well as dedicated sensing devices. Originally, the

contactless fingerprint recognition of the index finger of Jonietz et al. [19] was part of the developed device. We have been extending their work to capture 4-fingerprints at once. Our approach is based on the project results of [25], which was initially developed for smart phones.

This paper is organized as follows: Section 2 describes the handheld device with a focus on usability and security aspects. Section 3 presents the image acquisition system and processing of the captured fingerphotos. Section 4 presents results of contactless fingerprint recognition and the survey results of the handheld device at a border control scenario. Section 5 concludes the paper and discusses future work.

II. Handheld Device

The design goal of the MobilePass device was to have a versatile, high performance adaptable platform for image processing which also can be used in a mobile way. The hardware is a trusted platform enabling high secure applications. Embedded hardware was designed with respect to typical industrial requirements such as components with long availability, scalability in terms of processing power, secure boot capabilities and extended temperature range. A plugin FPGA module enables high-performance computing for complex real-time applications. The developed MobilePass device incorporates functionalities like contactless fingerprint scanning, MRZ reading with a camera and facial verification (Fig. 2). It has a specialized hardware and ergonomics design optimally suited for Border guards' use. It can be operated attached to the wrist, leaving both hands free for passport handling and also with one hand for biometric operations. The hardware includes a high-resolution camera, a quad core CPU and an accelerator FPGA. A large and sunlight readable display with touch support and a colored multi wheel makes it very comfortable for one handed operations. The operating system is a special adapted Linux version with a system boot time of less than 15 seconds. High connectivity features like BT LE, Wi-Fi and 4G help to integrate it with other IT systems.

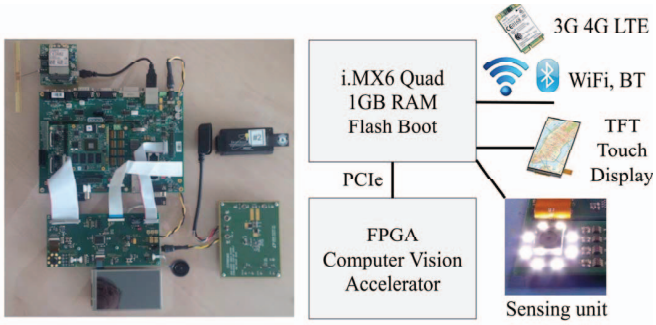


Fig. 2: Components assembly and block diagram of MobilePass device, which is based on a heterogeneous computing platform.

A. Functionality

The device includes among others the following functionalities:

The built-in camera is capable of scanning the MRZ from a machine readable travel document (MRTD) in a very fast and convenient way. It also verifies if checksums are correct. The software scans type 1, 2 and 3 MRZ documents.

For facial verification (e.g. facial image read from electronic passports) the image is compared to the live image from the built in camera. The result of the verification process is immediately shown on the display. For easier use an indicator turns green if the match quality is high enough. The capturing and verification process work in parallel.

The device demonstrates a new possibility to scan fingerprints very fast in a contactless way. In the typical border control use-case, the fingerprint information from the passport is verified against the passport holders fingerprints and – according to the national rules - access is granted or denied. The capturing process and the verification works in parallel, the human operator immediately observes the results of verification on the device´s screen. This new method allows the biometric verification of a traveler in a less intrusive way.

The embedded device connects to the workflow system of the border control unit (base station), which provides information about the certificates store and the background databases such as SIS-II, VIS, Interpol and national ones. Moreover, the border control procedure is monitored and stored.

B. Security Aspects

Security is a very important area in any system where personal data are processed [26]. Hence, it is an essential requirement for embedded devices designed for border control applications. For example, with respect to the embedded design – a trusted platform [6][7] doing a secure boot [8][9] protects against infiltration. During the boot process the loaded firmware can be measured in the TPM to ensure that the firmware has not been tampered with. To reach this state a mechanism called "secure boot" is used. The boot loader (which cannot be changed in such a system because it is stored in ROM) starts the primary operating system hosting the applications. The ROM-boot loader has a cryptographic key to verify the digital signature of the following software part (e.g. the operating system in a 2-stage system). This enables the system to boot only when the signature of the complete operating system is authenticated, every change or patching is detected.

The embedded device needs to exchange data with the workflow system of the border control unit, which is connected to databases and certificate stores. The certificates store provides and checks electronically signed certificates, which is needed for validating documents or accessing sensitive data stored inside document's RFID chip. For this, the "Extended Access Control" (EAC) is provided, which consists of multiple protocols such as "Chip Authentication" (CA) and "Terminal Authentication" (TA), both protocols are executed along with "Basic Access Control" (BAC), respectively "Password Authenticated Connection Establishment" (PACE) and "Passive Authentication" (PA) [27].

Since the MobilePass device itself is a trusted platform module (TPM), certificates stored on the device cannot be readout. Typically EAC certificates for biometric elements like

iris or fingerprints must be specially secured. For example, if a device is stolen, an attacker would not be able to readout the Flash PROM where certificates are stored, because the OS as well as certificates are encrypted by the manufacturer or the trusted company bringing those devices into operation (e.g. LEAs). The second security measure is the hashing of the operating system and the application code. Only the CPU at boot time knows the correct hash, so any change in the OS, application or certificates store is immediately detected. In this case the CPU refuses to operate. Hash values and decryption keys for OS and application cannot be readout by the operator after programming. Access mechanisms to this data are destroyed physically inside the CPU processor by overloading electric capacities. This technique is called eFUSE programming [28] and is only provided by some chipsets providers. In general, consumer products such as smartphones do not use these specific chipsets.

The traveler's ID is checked against different databases during the border control procedure. For these background checks the system connects to international databases e.g. VIS (Visa Information System) or SIS (Schengen Information System) and alerts the border control guard in case of an issue. For this procedure the developed device acquires sensitive data from documents, processes them and sends them to external databases. The last stage of this process - wireless transmission - is especially vulnerable to attackers. That is why the communication between the handheld device and database servers has to be protected with additional measures. Such solutions include e.g. firewall, Intrusion Detection System (IDS), Intrusion Prevention System (IPS) and point-to-point transmission with end-to-end secured tunnel.

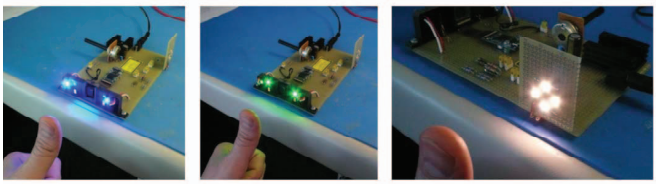
III. Image Acquisition and Proccessing Unit

A sophisticated capturing unit is essential for performing demanding vision tasks. It is challenging to scan MRZ and capture typical biometric traits (finger and face) with a single sensor in a mobile device. Hence, one of the main challenges was the development of a robust sensing unit. In addition, the fingerphoto processing steps are outlined.

A. Sensing Unit

The capturing of high quality images is crucial because they enable the extraction of high quality biometric features to accurately authenticate a person. The requirements are challenging as the camera needs to capture face and 4-fingerprint images with sufficient resolution to extract high quality features. Furthermore, it needs to reliably work in semi-constrained environments. Under semi-constrained environments we understand that the device shall e.g. operate in outdoor scenarios but that e.g. direct sunlight is avoided.

Bright-field illumination is a very suitable approach to illuminate fingerprints [19]. In order to achieve this kind of illumination, the LEDs are closely arranged around the optical axis of the camera (Fig. 3). We selected the camera block FCB MA130 from Sony [2] equipped with a 5.3mm focal length (31mm full frame equivalent), which delivers HD images (1920x1080 pixel) with a frame rate of 30 frames per second. The choice of the lens is related to the working distance (between the face, finger and sensor). If fingers are captured at a distance of 10cm, then the resulting pixel density is around 580DPI (dots per inch), which is sufficient for fingerprint recognition.



(a) (b) (c)

Fig. 3: Fingerprint capture setup: Testing multiple wavelengths and arranging LEDs in various positions. (a) Testing LEDs emitting mainly blue light. (b) Testing LEDs emitting mainly blue light. (c) Testing LEDs emitting white light. Four LEDs are arranged around camera to produce a bright-field illumination.

The camera needs to capture both face and fingerprints modalities with high quality. Hence, an automatic backlight compensation is necessary to enable the usage of the device in various environments. While the image acquisition of faces of cooperative subjects is a simple task, fingerprints are challenging because of their fine structure. In the following the capturing set-up improving fingerprint acquisition is described in more detail.

In the targeted environments, controlling fingerprint capture and illumination is extremely important because sharp, high-contrast images simplify the fingerprint recognition task. In order to guarantee this quality, the following parameters are taken into account: exposure time, signal amplification, automatic brightness control, focus finder and an external control to manage lighting. For capturing the face the camera rapidly sweeps the focal plane through the scene to find the best auto-focus setting, while for fingerprint capturing a macro focus is used. The arrangement of the light emitting elements should ensure a uniform illumination. To increase the contrast and thus to enhance the segmentation between fingers and background, powerful white LED's are arranged around the optical axis of the camera.

Although the subject's fingers as well as the imaging device are moving, the goal is to capture very sharp images consisting of the detailed topology of the fingers. For this, we configured the camera in fast exposure modes with low apertures (e.g. f 2.8). The low aperture has the additional benefit that the depth of focus is small and only the surface of the fingers are in focus. The additional illumination also supports a short exposure time. The LED arrangement is done in pairs, so 4x2 pairs can be controlled independently by I2C commands. The electric power is provided by pulse width modulated (PWM) mechanisms with a frequency of 10 kHz. The main advantage of PWM is the low power loss. The high frequency ensures that the modulation is not visible in the images.

B. Fingerphoto Processing

The device captures not a single but multiple fingerphotos of the subject to ensure the required quality, which results in a

reliable authentication. For this, the proposed approach consists of the following steps: (1) fingerphoto segmentation and enhancement based on [25], (2) quality assurance and (3) re-scaling fingerprints. For the feature extraction and matching a commercial algorithm [3] is used, which is out of the scope of this work.

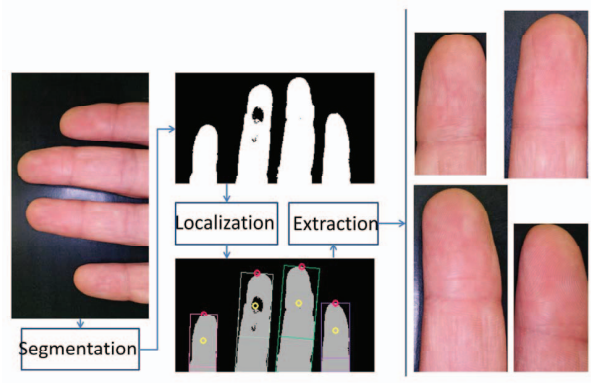


Fig. 4: Fingerphoto processing consists among others of segmentation, localization and extraction of 4-fingerprints.

Due to the small depth of focus of the sensing unit and the unconstrained capture setting (hand-held device, unsupported subject), it is quite challenging to capture a high-quality fingerphoto. Our approach is to capture a series of images, while the operator of the mobile device slightly varies the distance to the subject. From this series of images a best-shot selection is performed, evaluating sharpness based on edge pixels [29] and selecting the overall sharpest image.

A key feature of our method is the fast image segmentation that extracts up to four finger images from an input image. At first, the high-resolution input image is greatly reduced in size, which speeds up the segmentation procedure tremendously. The segmentation itself is based on a pixel-based skin tone detection, using combined masks in the HLS and RGB color spaces. Touching fingers are separated by using the dark finger borders that are obscured by shadows. In order to be able to separate fingers from the possible visible palm of the hand, an outline tracing separates significant peaks (fingers) from the torso (palm of the hand). A rectangle bounding box encloses each finger by optimally fitting it to the detected contours of the fingertips. The segmentation results are then used to cut out the individual finger images from the full resolution input image (Fig. 4).

The goal of enhancing the fingerphotos is to increase the contrast between ridges and valleys, and to mimic the appearance of classic fingerprint images. The enhancement itself is essentially noise reduction and contrast enhancement using histogram equalization and normalized box-filters. Afterwards the background pixels are removed, avoiding sharp edges on the border of the fingerprint, and the image is mirrored, like classic fingerprint images (Fig. 5).

To assess the quality of the captured fingerprints, we use the publicly available software provided by National Institute of Standards and Technology, denoted as NFIQ which is part of NBIS package [11], and considered as a "de facto" standard approach for fingerprint quality estimation. The NFIQ algorithm has several shortcomings as discussed in [12][13], so that recently NFIQ-2 was released. We plan to use this method in the near future.

Fig. 5: Captured fingerphoto (left image) is segmented and enhanced in order to extract fingerprint (right image).

In a final step, we need to scale the previously determined fingerprints, since many fingerprint matching algorithms are actually not invariant to scaling [14]. Due to our capturing process, using a fixed focus with shallow depth of field, and by selecting the sharpest image from a series of images, we can safely assume that the distance of the fingers to the camera at the time of capture corresponds to the focus distance. Using this information we can scale the fingerprints to 500 DPI, so that we are compliant to FBI-standards [13].

IV. Evaluation

A. Fingerprint Evaluation

The evaluation of the fingerprints was carried out by capturing the fingerphotos on two mobile phones (Huawei P9 and LG G5 850) so far. We expect to obtain much better results on dedicated hardware with a sophisticated image acquisition unit.

Experiments were conducted under lab conditions (controlled illumination and distance between hands and sensor) to investigate the performance of the touchless 4-fingerprint recognition, which is evaluated using 1920 fingerprint images of 12 different persons.

The captured images are processed and re-scaled to 500DPI as previously described. Afterwards those templates are transferred to the PC for feature (minutiae) extraction and verification. For this, we use the commercial fingerprint matching software IDKit Fingerprint SDK from Innovatrics [3]; a state-of-the-art feature extractor and matcher.

The achieved results using a single fingerprint are displayed in Fig. 6. The corresponding EER (Equal Error Rate) is roughly 1.0%. The FRR (False Reject Rate) is 1.2% at a given FAR (False Acceptance Rate) of 0.01%. Hence, every 120th person is wrongly rejected while every 10000th person is wrongly accepted. The reliability of authentication significantly increases if 4 fingerprints instead of a single fingerprint are taken into account. Based on our database the FRR rate significantly decreases at a given FAR. But these promising results are based on a small dataset under lab

conditions, so we need to carry out additional evaluations to precisely measure the FRR and FAR rates in border control scenarios.

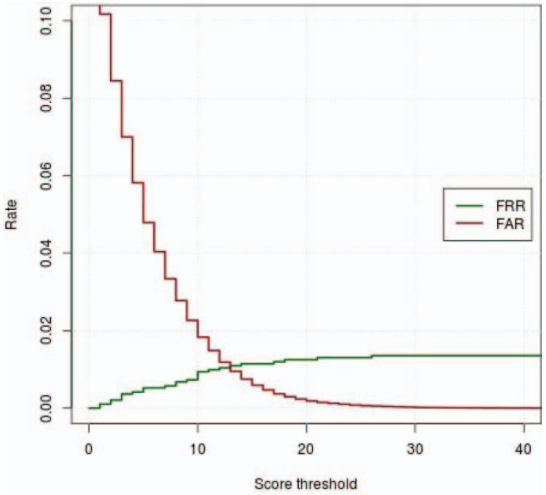


Fig. 6: As the score threshold increases, fewer impostor attempts will falsely be considered matches, but at the same time more genuine attempts will falsely be classified as non-matches. The FAR (False Acceptance Rate) and FRR (False Rejection Rate) curves are displayed.

B. Handheld Device

In order to test the designed equipment under an operational environment, a usability evaluation following ISO 9241-11:1998 standard [1] was carried out at the border between Romania and Moldavia. The equipment was used under different conditions in real scenarios for two consecutive days. A total of 93 participants took part in the border checking through our handheld device and subsequently completed a questionnaire.

The following border control procedure was conducted during the test: 1. Read MRZ and access chip of passport. 2. Display traveler's data, including chip face on display. 3. Proceed to facial verification (compare live-face with chip face). 4. Proceed to fingerprint capturing (capture left and right index finger). 5. Ask traveler/ border guard about experience.

The usability [5] of the handheld device with respect to effectiveness (defined in terms of accuracy and completeness), efficiency (duration of entire identity check), and satisfaction (user experience with new device/ procedure) was evaluated.

The efficiency is determined by measuring the duration of travelers at the border control procedure. The average duration was 38s with a standard deviation of 19s. The minimum and maximum durations were 17s and 118s, respectively. On average the control procedure was longer at outdoor scenarios.

The device and border procedure is very effective. There were 94 users in the evaluation, performing 184 interactions in total. There were only 11 wrong interactions (6%). 10 during the face recognition and 1 during the fingerprint acquisition process. These problems occurred because of varying environmental illuminations, so that the capturing process took a longer.

Satisfaction is determined by analyzing the completed surveys of travelers and border guards. Fig. 7 shows the travelers' feedback, which was overall very good. A total of 7 border guards participated in the experiment and completed the questionnaire. They were very satisfied with the new device and procedure. Their feedback also pointed to open issues. For instance, border guards noted a difference in the performance of capturing biometrics depending on the environmental conditions. In general, the time for capturing increased in outdoor scenarios.

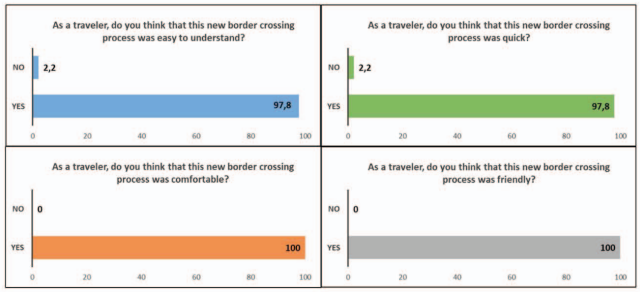


Fig. 7: The following questions were answered: As a traveler, do you think that this new border crossing process was (a) easy to understand? (b) quick? (c) comfortable? (d) friendly?

V. Conclusions

In this paper a novel handheld device for border control was presented. The developed solution considers usability as well as security issues, which are relevant for a device intended to be used in the context of identity checks at borders. A prototype camera system with bright-field illumination has been presented, which is suitable for MRZ scanning as well as capturing the face and fingerprint for authentication.

Extending the algorithm from a single to a 4-fingerprint authentication method significantly improves the performance. These tests were currently carried out on mobile phones but will be ported to the MobilePass device in the near future. The evaluation demonstrates the suitability of the MobilePass device for border control. Travelers and border guards were very satisfied with the new device.

References

[1] ISO 9241-11:1998 - Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 11: Guidance on usability. (n.d.). Retrieved from http://www.iso.org/iso/catalogue_detail.htm?csnumber=16883.

[2] Sony. (4.10.2015) Retrieved from https://pro.sony.com/bbsc/ssr/cat-camerasindustrial/cat-cimicrofcb.

[3] Innovatrics (16.11.2017). Retrieved from https://www.innovatrics.com/idkit-fingerprint-sdk/.

[4] ICAO 9303 Machine Readable Travel Documents, Part 1- Machine Readable Passports. Volume 2 - Specifications for Electronically Enabled Passports with Biometric Identification Capability, 6th edition, 2006.

[5] Bevan, Nigel, James Carter, and Susan Harker. "ISO 9241-11 revised: What have we learnt about usability since 1998?." International Conference on Human-Computer Interaction. Springer, Cham, 2015.

[6] Trusted Computing Group (TCG), Konsortium, Beaverton (Oregon), USA, Trusted Platform Module (TPM) Specifications. www.trustedcomputinggroup.org.

[7] Trusted computing architectures for a mobile IT infrastructure, Vijay Anand, Jafar Saniie, Erdal Oruklu, Southeast Missouri State University and Illinois Institute of Technology, Cape Girardeau, MO, USA.

[8] Roots of Trust in Mobile Devices, ISPAB, February 2012, Andrew Regenscheid, NIST – National Institute of Standards and Technology.

[9] Securing the core root of trust (malware, counterfeiting and IP theft in hardware), Ramesh Karri, ECE Department, NYU – New York University.

[10] AIT Austrian Institute of Technology GmbH, MobilePass, MobilePass is a FP7 research project, accessed 21 November 2017, http://mobilepass-project.eu/

[11] National Institute of Standards and Technology. Nist biometric image software. http://www.nist.gov/itl/iad/ig/nbis. Cfm , June 2012.

[12] M. Olsen and C. Busch. Deficiencies in nist fingerprint image quality algorithm. Proceedings 12. Deutscher IT-Sicherheitskongress, BSI , May 2011.

[13] Johannes Merkle, Michael Schwaiger, and Marco Breitenstein. Towards improving the nist fingerprint image quality (nfiq) al- gorithm. In Arslan Brömme and Christoph Busch, editors, BIOSIG, volume 164 of LNI, pages 29–44. GI, 2010. Criminal Justice Information Services: Electronic Fingerprint Transmission Specification. Int. Report. CJIS-RS-0010 (V7), (1999), available at: http://www.fbi.gov/hq/cjisd/iafis/efts70/cover.htm

[14] Piuri, Vincenzo, and Fabio Scotti. "Fingerprint biometrics via low-cost sensors and webcams." Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on. IEEE, 2008.

[15] PwC Technical Study on Smart Borders. (04.10.2017). Retrieved from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_executive_summary_en.pdf

[16] Najera, Pablo, Francisco Moyano, and Javier Lopez. "Security Mechanisms and Access Control Infrastructure for e-Passports and General Purpose e-Documents." J. UCS 15.5 (2009): 970-991.

[17] Berenguel, Albert, et al. "e-Counterfeit: a mobile-server platform for document counterfeit detection." arXiv preprint arXiv:1708.06126 (2017).

[18] C. Lee, S. Lee, J. Kim, and S.-J. Kim. Preprocessing of a Fingerprint Image Captured with a Mobile Camera, pages 348–355. 2005.

[19] C. Jonietz, E. Monari, H. Widak, and C. Qu. Towards mobile and touchless fingerprint verification. In Proc. Int'l Conf. on Advanced Video and Signal Based Surveillance (AVSS), pages 1–6, Aug 2015.

[20] M. Derawi, B. Yang, and C. Busch. Fingerprint Recognition with Embedded Cameras on Mobile Phones, pages 136–147. 2012.

[21] B. Hiew, A. B. Teoh, and D. C. Ngo. Preprocessing of fingerprint images captured with a digital camera. In Proc. Int'l Conf. on Control, Automation, Robotics and Vision, pages 1–6, Dec 2006.

[22] H. Ravi and S. K. Sivanath. A novel method for touch-less fingerprint authentication. In Proc. Int'l Conf. on Technologies for Homeland Security (HST), pages 147–153, Nov 2013.

[23] Security Printing Consulting AG, eDocument Reader, accessed 21 November 2017, https://www.sp-consulting.ch/p.reader_mdr1.html.

[24] CrossMatch, Seek Avenger, accessed 21 November 2017, https://www.crossmatch.com/.

[25] Federal Ministry for Transport, Innovation and Technology (BMVIT), Modentity, KIRAS, accessed 21 November 2017, http://www.kiras.at/en/projects/detail/d/modentity/

[26] Kc, Gaurav S., and Paul A. Karger. "Security and privacy issues in machine readable travel documents (MRTDs)." (2005).

[27] BSI, BSI TR-03110 Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, Publications, accessed 21 November 2017, https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03110/BSITR03110.html

[28] Sanders, Lester. "Secure boot of zynq-7000 all programmable SoC." Application note XAPP1175 (v1.0), Xilinx (2013).

[29] Caviedes, Jorge, and Sabri Gurbuz. "No-reference sharpness metric based on local edge kurtosis." Image Processing. 2002. Proceedings. 2002 International Conference on. Vol. 3. IEEE, 2002.