Fingerprint Match in Box

Joshua J. Engelsma, Kai Cao, Anil K. Jain
Michigan State University
East Lansing, MI, USA
{engelsm7, kaicao, jain}@cse.msu.edu

Abstract

We open source fingerprint Match in Box, a complete end-to-end fingerprint recognition system embedded within a 4 inch cube. Match in Box stands in contrast to a typical bulky and expensive proprietary fingerprint recognition system which requires sending a fingerprint image to an external host for processing and subsequent spoof detection and matching. In particular, Match in Box is a first of a kind, portable, low-cost, and easy-to-assemble fingerprint reader with an enrollment database embedded within the reader's memory and fingerprint spoof detector, feature extractor, and matcher all running on the reader's internal vision processing unit (VPU). An onboard touch screen and rechargeable battery pack make this device extremely portable and ideal for applying both fingerprint authentication (1:1 comparison) and fingerprint identification (1:N search) to applications (vaccination tracking, food and benefit distribution programs, human trafficking prevention) in rural communities, especially in developing countries. We also show that Match in Box is suited for capturing neonate fingerprints due to its high resolution (1900 ppi) cameras.

1. Introduction

Automated fingerprint identification systems (AFIS) are now prevalent around the globe providing an accurate and widely acceptable method for authentication (1:1 match) or identification and de-duplication (1:N search) of individuals [1]. To date, fingerprint recognition systems have been successfully deployed into a plethora of applications including healthcare access, financial transactions, forensics, border crossing security, national ID systems, and mobile device access and payments [1]. Despite widespread deployment of fingerprint recognition systems in place of ID cards and passwords, they still need to overcome some hurdles before their further deployments into several niche domains, especially pertaining to applications in developing countries. These limitations include spoofing vulnerabilities, insufficient resolution for neonate fingerprinting, lack
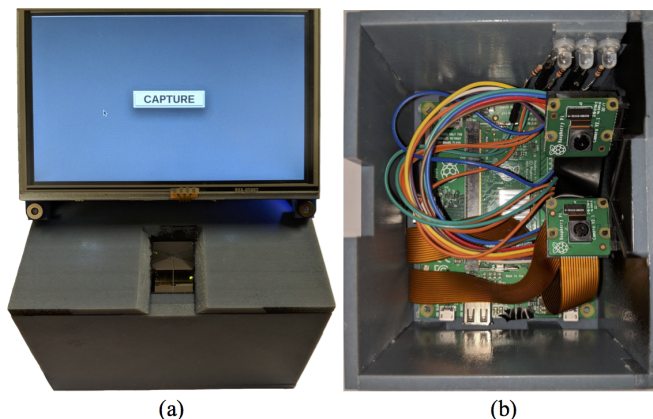

Figure 1. Match in Box. (a) A working prototype of Match in Box. Match in Box is a complete, open-source, end-to-end fingerprint recognition system (with 1900 ppi fingerprint acquisition, spoof detector, feature extractor, template storage, and 1:N search) embedded within a portable (rechargeable battery and touch screen) 4-inch cube. (b) Assembly of Match in Box requires only low-cost ($400 USD), ubiquitous, off-the-shelf components, enabling its easy build and customization for niche applications, particularly in inaccessible locations in developing countries.

of portability, difficult customization, and high cost of hardware and software.

1.1. Spoofing Vulnerability

Fingerprint recognition systems are known to be susceptible to circumvention through "*spoofing*" attacks[1]. Fingerprint spoofing is a nefarious act in which a hacker mimics the identity of an unsuspecting victim (through replicating the victim's fingerprint with materials such as silicone, gelatin, and wood glue) in order to gain access to the victim's biometric protected data [2, 3]. Any failure of a fingerprint recognition system to automatically detect and flag spoof attacks prior to authentication could result in loss of

---

[1]Fingerprint spoof attacks are a subset of "*presentation attacks*" defined in ISO standard IEC 30107-1:2016(E) as "*presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system.*"
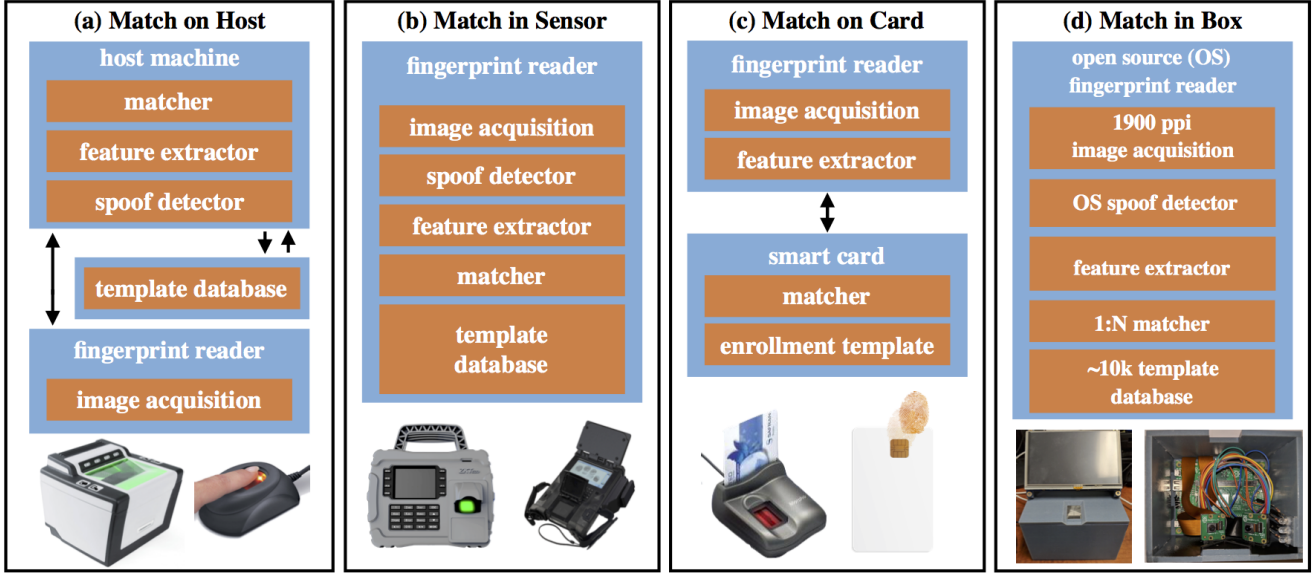
Figure 2. Schematic diagrams and example commercial fingerprint recognition system architectures. (a) Match on Host, (b) Match in Sensor, (c) Match on Card, and (d) the proposed Match in Box, the first open source implementation following the Match in Sensor architecture, allowing customization to fit application specific needs, particularly in developing countries. Figures for commercial products retrieved from [4, 5, 6, 7, 8, 9].

personal data and benefits, or prevent proper identification of a person of interest (by obfuscating a person's true identity).

Given the requirements of accurately detecting fingerprint spoof attacks in most applications, a number of techniques involving both hardware and software have been proposed [10]. In hardware based approaches, additional sensors embedded within the fingerprint readers output/provide features such as skin color, sub-dermal fingerprints, blood flow, odor, and heartbeat which can be used to distinguish live fingers from spoof fingers [10, 11, 12, 13, 14, 15, 16, 17, 18]. In contrast to hardware based solutions, software based techniques do not require special sensors or special illumination within the fingerprint reader. Instead, software based approaches operate by extracting textural [19], anatomical [20], physiological [21], or learned [22, 23] features from images being output by the reader for the purpose of fingerprint recognition (i.e. the same image is used for both spoof detection and subsequent recognition). To date, much work remains to be done in spoof detection research, especially in detecting spoofs not used during training of the spoof detectors [24, 25].

1.2. Insufficient Fingerprint Resolution

A limitation of commercial fingerprint readers is that most only produce 500 ppi fingerprint images, because of the cost and the targeted adult end users. However, as noted by Jain *et al.* in [26], higher fingerprint resolution (> 1000 ppi) is necessary to capture the minute fingerprint details of a neonate or an infant. Neonate biometric recognition, especially involving fingerprints, is an area of increasing interest by governments (e.g. Aadhaar program [27, 28]), international agencies (e.g. various UN agencies such as WFP [29], and UNCHR [30]) and NGOs (e.g. Bill and Melinda Gates Foundation [31]). While commercial 1000 ppi fingerprint reader solutions do exist [32, 33], they can cost upwards of over $1000 USD, negating the practicality of their utility in capturing neonate fingerprints, especially in the developing world.

1.3. Portability

Many fingerprint recognition systems have limited portability due to their reliance on multiple physical hardware modules. In a typical "Match in Host" (Fig. 2 (a)) [34] system, a fingerprint reader acquires the fingerprint image which is then transferred to a host to perform spoof detection, feature extraction, template storage, and matching. Although the host offers choice of processors and memory, the Match in Host design suffers from two main drawbacks: (i) sensitive biometric data needs to be transferred from the fingerprint reader to the host and (ii) the system is costly, bulky, and immobile. These limitations are especially prohibitive to field operations in developing countries (such as vaccination and health tracking of children, banking, and benefits distributions) where low cost and portability are essential given the lack of financial resources, electric power and network reliability.

To solve the limitations inherent to Match in Host architectures, two newer generations of fingerprint recognition architectures emerged. The first of these architectures has been termed "Match in Sensor" (Fig. 2 (b)) [34] or alternatively described as operating in "Embedded Mode" [6,

Table 1: Match in Box vs RaspiReader

Reader	Capture Time (seconds)	Capture Area (pixels)	Native x Resolution (ppi)	Native y Resolution (ppi)	Spoof Detector	Feature Extractor & Matcher	Portability
RaspiReader [11]	1.5	290x267	1594 - 2480	2463 - 3320	on host	on host	low
Match in Box	**0.75**	**285x357**	**1917-2962**	**2900-3768**	**embedded**	**embedded**	**high**

7, 35]. Match in Sensor operates entirely (fingerprint acquisition, feature extraction, template storage, matching, spoof detection) within the processor and memory, embedded within the fingerprint reader. The advantages of this newer paradigm are; (i) higher security, since fingerprint data does not need to be transmitted and (ii) greater portability.

Another fingerprint recognition architecture, known as "Match on Card" (Fig. 2 (c)) [36, 37], has now been gaining traction. There are two instances of the Match on Card paradigm (dependent on whether the fingerprint reader is on the card or not). If the fingerprint reader is *not* on the card, a user simply inserts a card into a specialized fingerprint reader which (i) acquires the user's fingerprint, (ii) extracts a template from the fingerprint image, and (iii) securely transmits the template to the card where the template can be securely stored as an enrollment template or used for matching (authentication) directly on the smart card. If the fingerprint reader is already on the card, then fingerprint image acquisition, feature extraction and matching can all be performed directly on the card.

Both the Match in Sensor and the Match on Card paradigms solve *some* of the limitations inherent to Match in Host. However, the commercial products available for Match in Sensor and Match on Card still have several limitations of their own, especially as it pertains to applications in developing countries involving identification of tens of thousands of individuals. These limitations include: inability to customize the black box systems, high-cost, insufficient resolution for neonate fingerprints, and spoofing vulnerabilities.

In summary, the advances in spoof detection research, fingerprint readers, and system mobility have come a long ways, however, gaps still exist, especially with respect to utilizing fingerprint recognition technologies in many emerging and critical applications in the developing world, including: delivering nutrition to undernourished children [44], improving child vaccination coverage [45], and government distribution programs [28, 46]. Given these limitations of available commercial fingerprint recognition systems in many applications specifically relevant to developing countries, we open source fingerprint Match in Box, a cost-effective, customizable, mobile, spoof resistant, and 1900 ppi end-to-end fingerprint recognition system aimed at filling these voids. Match in Box makes several major customizations and improvements to the open source

RaspiReader [11] (Table 1). More concisely, the main contributions of this research are as follows:

- The first open source, portable, end-to-end fingerprint recognition system with image acquisition, spoof detection, feature extraction, matching, and enrollment database all embedded within a single 4 inch cube. Unlike black-box commercial systems, Match in Box is completely customizable and low-cost.

- Complete mobility and portability through the addition of a touch screen, intuitive GUI, and rechargeable battery pack. The touch screen and GUI allow for easy enrollment, authentication and metadata access of enrolled subjects.

- State of the art in high-resolution, *neonate* fingerprint image acquisition using the 1900 ppi Match in Box. Initial experiments demonstrate significant improvement in capturing level-3 features from neonate fingerprint images with Match in Box in comparison to the proprietary 1270 ppi, high-resolution reader used by Jain *et al.* in [26].
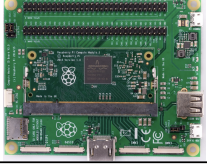
2. Match in Box Hardware

In assembling Match in Box, the following hardware design choices (including image acquisition hardware, processor and memory requirements for Match in Sensor capabilities, and peripherals for portability) are made to best meet our objective of prototyping an open source, spoof resistant, high-resolution, portable, customizable, low-cost, end-to-end fingerprint recognition system. Table 2 lists all the hardware components that were used to assemble Match in Box. Except for the casing that was custom fabricated using a Stratasys Objet350 Connex [47] 3D printer, all other components to construct the reader are available off-the-shelf.

2.1. Image Acquisition Hardware

To make Match in Box spoof resistant, we follow the success of RaspiReader in using two cameras for fingerprint image acquisition. In particular, one camera captures a colorful, *direct image* of the finger in contact with the glass platen (useful for spoof detection) while the second camera captures a high contrast, *frustrated total internal reflection image* (useful for both spoof detection and subsequent fingerprint matching) (Figs. 3, 4). Unlike RaspiReader, Match in Box uses the Raspberry Pi Compute Module 3

Table 2: Primary Components Used to Construct Match in Box. Total cost is $400 USD (as of April 1, 2018)

Component Image	Name and Description	Quantity	Cost (USD)
	Raspberry Pi Compute Module 3 Lite [38]: A single board computer (SBC) with 1.2 GHz 64-bit quad-core CPU, 1 GB RAM, MicroSDHC storage, and Broadcom VideoCore IV Graphic card	1	$29.95
	Raspberry Pi Compute I/O Board [39]: Compute Module breakout board	1	$114.95
	Pi Camera v2 [40]: 8 Megapixel, 30 frames per second	2	$29.95
	Intel Neural Compute Stick [41]: Intel Movidius VPU processor	1	$80.43
	Touch Screen [42]: 5-inch TFT touch screen	1	$74.95
	Rechargeable Battery [43]: 10,000 mAh lithium ion battery	1	$39.95

Lite (CM3L) to capture two still-images or video streams simultaneously.

The CM3L Raspberry Pi is a single board computer (SBC) which, when used in conjunction with the Raspberry Pi Compute Module I/O board and two 8 MP Raspberry Pi v2.0 cameras, is capable of capturing two still-images or video streams simultaneously in 0.75 seconds. Furthermore, the 8 MP cameras increase the fingerprint pixel resolution of Match in Box to 1917 ppi - 2962 ppi in the x-axis and 2900 ppi - 3768 ppi in the y-axis. This extremely high native resolution makes this affordable fingerprint recognition system extremely well suited for neonate fingerprint recognition.

2.2. Processors and Memory

An extremely vital and useful feature of Match in Box is its capability to perform fingerprint spoof detection and authentication (1:1 comparison) or identification (1:N search) directly on-board the fingerprint reader. To enable this functionality, Match in Box is equipped with a 32 Gigabyte SD card for storing approximately 10,000 fingerprint templates and associated user meta-data on device. Additionally, the processing speed of Match in Box is accelerated through the addition of the Intel Movidius Neural Compute Stick (NCS). The NCS is a low-power vision processing unit (VPU) designed with 12 specialized vector processing units, called SHAVES, for accelerating deep learning on the edge. The NCS is compatible with popular deep learning libraries Tensorflow and Caffe and is connected to USB. As such, the NCS is also compatible with the CM3L Raspberry Pi hardware and our Convolutional Neural Network (CNN) based spoof detection and fingerprint feature extraction software modules (both implemented in Tensorflow). While, one CNN inference of our "light-weight" spoof detection model (MobileNet) takes 475 milliseconds to run on the Match in Box CPU, an inference on the Match in Box VPU (NCS) takes a mere 58 milliseconds, an almost ten-fold speedup.

2.3. Portability Peripherals

Finally, in order to make Match in Box a completely portable and standalone system, we add a rechargeable battery pack (with the capability of powering a Raspberry Pi for up to 15 hours) and a 5-inch, 800x480 thin film transistor (TFT) touch screen.

All of these primary components are assembled together in accordance with the schematic diagram shown in Figure 3. Given a basic knowledge of circuits and programming, the entire device can be fabricated in under one hour. Upon completion of assembly, Match in Box is ready for fingerprint image acquisition, spoof detection, feature extraction, and matching in any location.

3. Match in Box Software

The Match in Box software is comprised of four main modules: fingerprint image acquisition, fingerprint spoof detection, fingerprint feature extraction and matching (1:1 verification and 1:N search), and a Graphical User Interface (GUI) for enrolling users and subsequently displaying user meta-data. Each of these modules are further explained in the following subsections.

3.1. Fingerprint Acquisition

The primary software involved in fingerprint image acquisition is the calibration of a raw FTIR image (e.g. Fig. 4b) into a processed, grayscale FTIR image which can be used for fingerprint matching. Following the same steps as reported in [11], a raw FTIR fingerprint image is converted into a grayscale matching image by (i) RGB to grayscale conversion, (ii) contrast enhancement via histogram equalization, (iii) perspective transformation, and (iv) scaling to
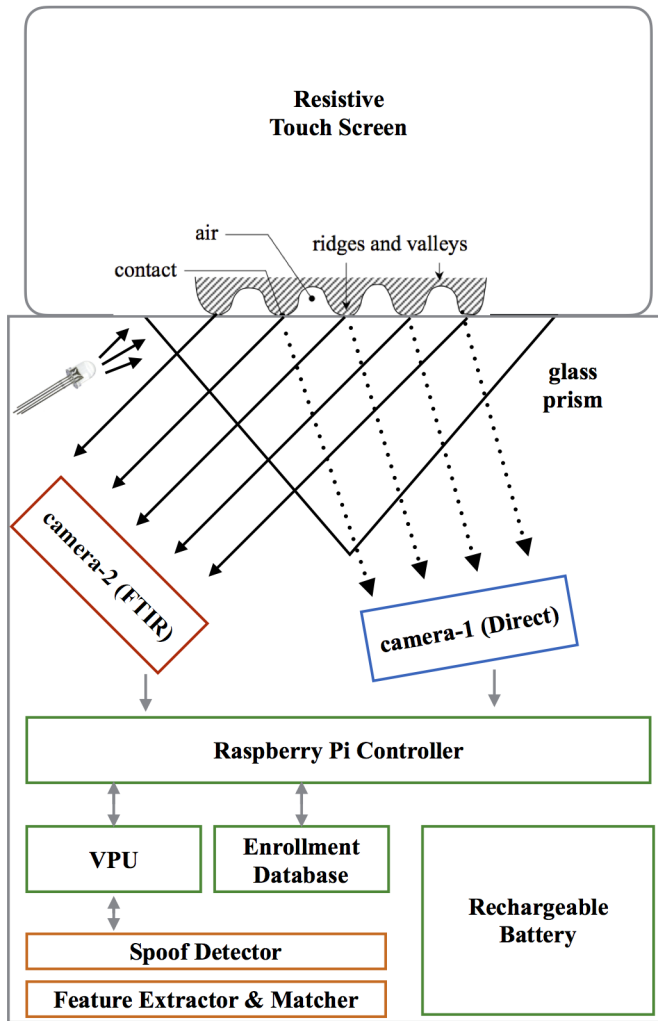

Figure 3. Schematic diagram of Match in Box.

the required fingerprint resolution (500 ppi for adults or 1900 ppi for neonates). As in [11], the perspective transformation and scaling parameters are obtained using a 2D printed checkerboard pattern to estimate the source and destination coordinate pairs needed to estimate the transformation parameters.
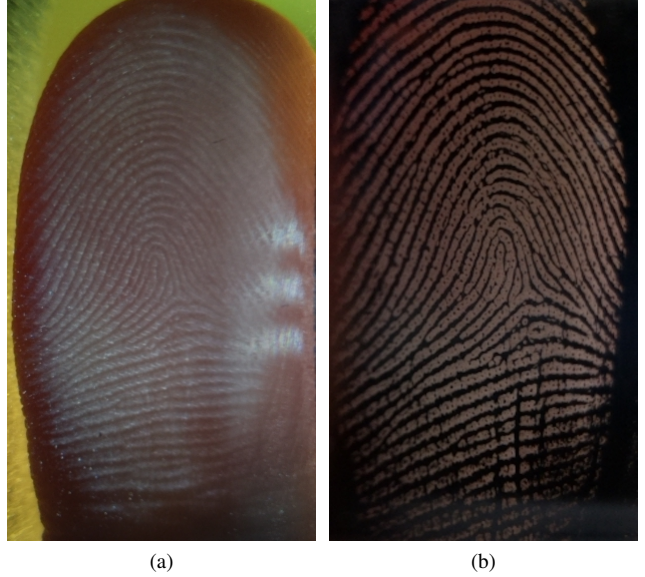

(a) (b)

Figure 4. Match in Box captures two fingerprint images of a user's finger from two different cameras. (a) Direct image of the finger for spoof detection; (b) high-contrast FTIR image for both spoof detection and matching.

3.2. Spoof Detector

The Match in Box spoof detector employs two MobileNet CNNs [48] to classify an input fingerprint image as live or spoof. Following the success of RasiReader [11], one MobileNet CNN is trained to make a binary classification (live or spoof) given an input image from the direct view camera (Fig. 4a) of Match in Box, and a second MobileNet CNN is trained to make a binary classification (live or spoof) given an input image from the FTIR view camera (Fig. 4b) of Match in Box. Finally, the scores generated by each of these respective CNN models are fused using the max rule [49].

3.3. Feature Extractor and Matcher

Upon completion of fingerprint spoof detection, fingerprint images which are determined to be "live" are passed to the Match in Box feature extractor. The embedded Match in Box feature extractor operates in two main steps. First, a Convolutional AutoEncoder (CAE) is utilized to locate the (x, y) locations and orientations of the input fingerprint's minutiae points. Then, in a manner similar to [50], a 96x96 patch is cropped around each located minutiae point and passed to a MobileNet CNN to extract a minutiae descrip-
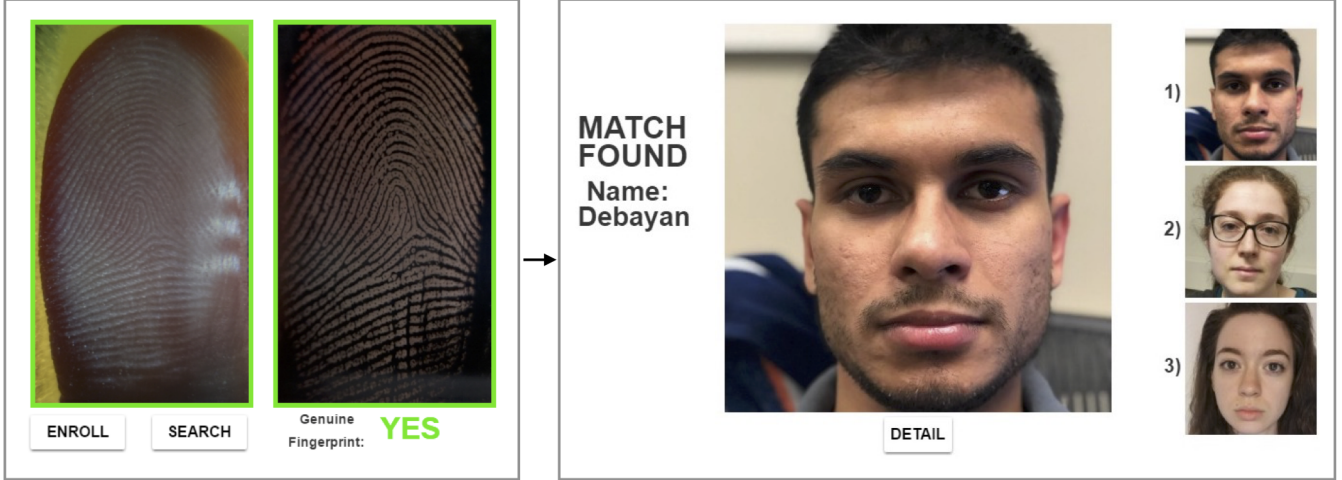
Figure 5. The Match in Box GUI is displayed on a 5-inch, 800x480 touch screen.

tor. The collection of all extracted minutiae descriptors comprise the template used by the Match in Box embedded matcher.

To match two templates in Match in Box, pairwise cosine similarity scores are first computed between the sets of minutiae descriptors comprising each template. Using these similarity scores, the top 120 minutiae descriptor pairs are selected and further filtered into a final set S using a graph matching algorithm. Finally, a match score is produced by summing the cosine similarity scores between all pairwise minutiae descriptors in S.

3.4. GUI

The Match in Box GUI was developed using the popular Electron framework. Electron enables building custom desktop applications using a combination of Javascript, HTML, and CSS. Due to the simplicity, cross-platform deployment capabilities, and modern UI/UX of the framework, it has been extensively used [51]. For Match in Box, we specifically develop a light-weight GUI allowing (i) subject enrollment, (ii) verification or search, and (iii) retrieval and display of subject meta-data (Fig. 5).

4. Experimental Analysis

With the Match in Box fully assembled and operational, we conduct several experiments demonstrating its (i) spoof resistance, (ii) matching performance, and (iii) neonate fingerprint acquisition capability. These experimental results and analyses are further enumerated in the following sections.

4.1. Spoof Detection

To demonstrate the spoof detection capability of Match in Box, we first constructed a dataset of both live and spoof finger impressions (Tables 3, 4) (Fig. 6). In particular, we

Table 3: Summary of Spoof Dataset

Material	# Training Impressions	# Testing Impressions
Clear Ecoflex	603	151
Pigmented Ecoflex	832	208
2D Paper	333	84
Total	1,768	443

Table 4: Summary of Live Dataset

Subjects	# Training Impressions	# Testing Impressions
56[†]	2,240	560

[†] For each subject, 5 impressions were captured from all 10 fingers.

fabricated nearly 1,800 spoofs from three different materials (clear ecoflex, flesh-pigmented ecoflex, and 2D printed paper), and we collected live finger impressions from 56 human subjects. The live finger impressions and spoof finger impressions were split into 5 training (80% of impressions) and testing (20% of impressions) splits. Using these training and testing splits in conjunction with the Match in Box spoof detector, we demonstrate the robust spoof detection capability of Match in Box by computing a mean True Accept Rate (TAR) of **98.46%** over the 5-folds at a False Accept Rate (FAR) of **0.2%** (standard deviation is **2.5%**). Note, the time to perform spoof detection on Match in Box is approximately 120 milliseconds due to the fast inference time available through the on-board VPU.

4.2. Matching

Both authentication (1:1 comparison) and identification (1:N search) performances are reported for Match in Box. As a baseline, we also report the authentication and identi-
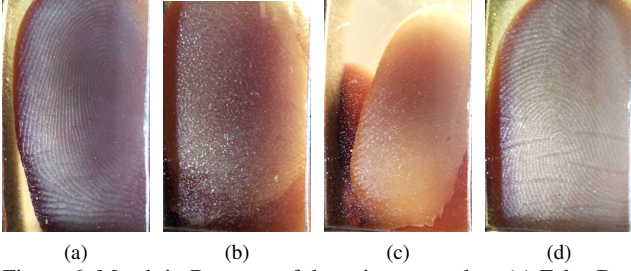
(a)   (b)   (c)   (d)

Figure 6. Match in Box: spoof detection examples. (a) False Detect (live misclassified as spoof) due to the excessively pink color of the subject's finger. (b) False Reject (spoof misclassified as live) due to the close approximation in color of the spoof to human skin. (c, d) True Detect (spoof classified as spoof) and True Reject (live classified as live) examples, respectively.
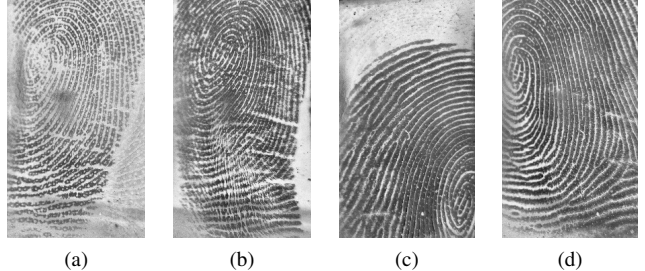
(a)   (b)   (c)   (d)

Figure 7. Match in Box: failure matching cases. (a, b) Fingerprint image pair resulting in a False Accept, due to close similarity between the imposter fingerprints. (c, d) Fingerprint image pair resulting in a False Reject due to capturing different portions of the fingerprints in consecutive captures.

fication performance when using the Match in Box fingerprint images in conjunction with the well-known and popular COTS Innovatrics SDK [52].

Using the fingerprint impressions enumerated in Table 4, we compute the ROC for authentication and the CMC for identification from 5,600 genuine scores and 156,520 imposter scores. From the ROC, we extract True Accept Rates of **98.0%** and **98.57%** at a FAR of 0.01%, using Match in Box and Innovatrics, respectively (Table 5). From the CMC, we extract rank one identification rates of **99.1%** and **98.9%**, using Match in Box and Innovatrics, respectively (Table 6). Both of these results, while reported on a small database, demonstrate the ability of Match in Box to perform state-of-the-art fingerprint authentication and identification. Note, time to perform authentication on Match in Box is approximately 600 milliseconds and time to perform identification from a gallery of 10,000 subjects is less than 2 minutes.

Table 5: Verification Performance

Matcher	False Accept Rate	True Accept Rate
Innovatrics	0.1%	99.0%
Innovatrics	0.01%	98.6%
Match in Box	0.1%	98.6%
Match in Box	0.01%	98.0%

Table 6: Identification Performance

Matcher	Rank-1 Identification Rate	Rank-5 Identification Rate
Innovatrics	98.9%	99.5%
Match in Box	99.1%	99.5%

4.3. Neonate Fingerprints

We demonstrate the utility of Match in Box for collecting high quality neonate fingerprints due to its 1900 ppi cameras. To conduct this experiment, we capture the right
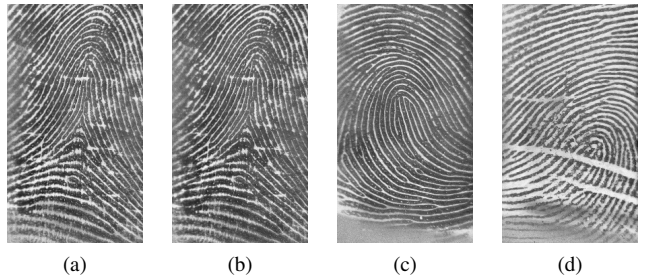

(a)   (b)   (c)   (d)

Figure 8. Match in Box: successful matching cases. (a, b) Fingerprint image pair resulting in a True Accept. (c, d) Fingerprint image pair resulting in a True Reject.

thumb print of a 3-month old infant on (i) the 500 ppi Digital Persona U.are.U 4500 HD, (ii) a custom 1270 ppi fingerprint reader designed by NEC [32] for neonate fingerprint acquisition [26], and (iii) our proposed 1900 ppi Match in Box. As is shown in (Fig. 9 (i)), the 500 ppi Digital Persona is not able to capture all the minute details of the infant's fingerprints. The 1270 ppi, custom NEC reader performs well in capturing a high quality fingerprint image, however, closer inspection reveals lack of separation between the ridges and valleys around the peripheral of the fingerprint (Fig. 9 (ii)). In contrast, the 1900 ppi Match in Box (Fig. 9 (iii)) is able to capture the entire infant fingerprint, with clean separation between the ridges and valleys throughout the fingerprint image. Furthermore, Match in Box is able to capture more pore information than the NEC reader.

Finally, we generate match scores between multiple impressions of the infant's fingerprint as captured by Match in Box and the custom NEC reader (Figs. 10, 11). Using Verifinger 6.3, match scores of 161 and 107 are computed for the fingerprint image pairs acquired by Match in Box and the NEC reader, respectively (score threshold of Verifinger at 0.01% FAR is 33). The annotated minutiae points in Figures 10 and 11 indicate that the high resolution Match in Box fingerprints are less susceptible to spurious minutiae than the NEC reader fingerprints.

While our initial experiments are qualitative, we posit

(i) Digital Persona U.are.U 4500 HD (500 ppi)   **(ii) Custom NEC Reader [26] (1270 ppi)**   **(iii) Match in Box (1900 ppi)**
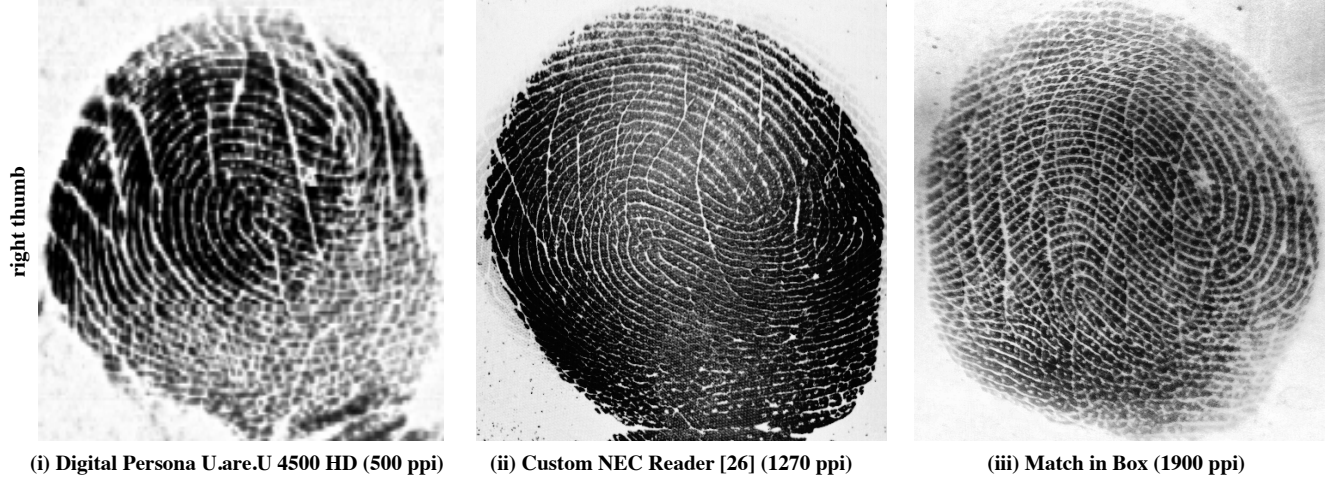
Figure 9. Fingerprint images of the right thumb of a 3 month old infant captured with (i) the 500 ppi Digital Persona U.are.U 4500 HD, (ii) a custom, NEC designed, 1270 ppi fingerprint reader for neonate fingerprint acquisition [26] and (iii) our 1900 ppi Match in Box.
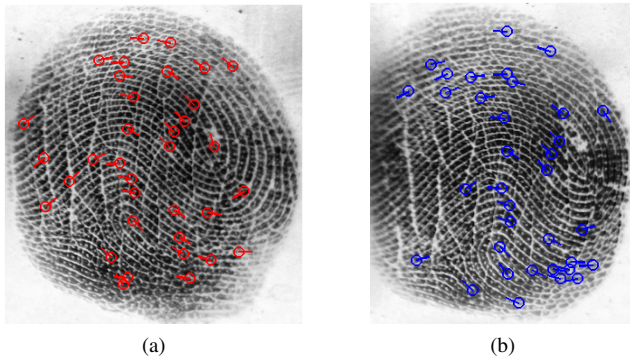

(a)   (b)

Figure 10. Fingerprint images of the right thumb of a 3 month old infant captured by Match in Box (a, b). Verifinger 6.3 was used to generate a match score of 161 between (a) and (b). The score threshold of Verifinger at 0.01% FAR is 33.
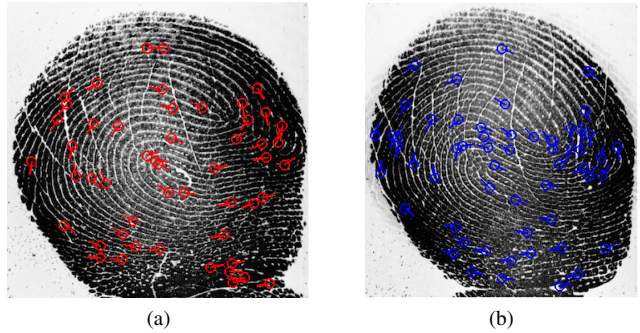

(a)   (b)

Figure 11. (a, b) Fingerprint images of the right thumb of a 3 month old infant captured by NEC [32] (a, b). Verifinger 6.3 was used to generate a match score of 107 between (a) and (b). The score threshold of Verifinger at 0.01% FAR is 33.

that our early findings show tremendous promise for utilizing Match in Box for state-of-the-art neonate fingerprint recognition, an area of increasing interest around the world by governments, international agencies, and NGOs alike.

5. Conclusion

We have designed and prototyped a complete, spoof resistant, 1900 ppi, fingerprint recognition system, called Match in Box, embedded within a portable form factor. Match in Box is easy and cost-effective to reproduce given the open source software and off-the-shelf components used to construct the device. Our experimental results demonstrate that Match in Box is able to achieve fast, state-of-the-art fingerprint spoof detection, authentication, and identification on device. We have also shown the utility of Match in Box for neonate fingerprint recognition. In the future, we will field test Match in Box at a site in India, where we will

specifically target capturing neonate fingerprints of a large number of subjects in a longitudinal study. In doing so, we hope Match in Box will push the boundaries of state-of-the-art neonate fingerprint recognition. We also plan to add a face camera and face matcher to Match in Box, enabling multi-modal biometric fusion and recognition.

6. Acknowledgement

References

[1] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Springer Science & Business Media, 2009.

[2] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial" gummy" fingers on fingerprint systems," in *Optical Security and Counterfeit Deterrence Techniques IV*, vol. 4677, pp. 275–290, 2002.

[3] T. Van der Putte and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned," in *Smart Card Research and Advanced Applications*, pp. 289–303, Springer, 2000.

[4] "Guardian USB." http://info.crossmatch.com/hubfs/datasheet/guardian-usb.pdf.

[5] "Morpho BTO 500." https://www.morpho.com/sites/morpho/files/bto_500_en-2_0.pdf.

[6] "ZKTeco US922." http://www.zktechnology.com/zk/upload/file/fronts/2017/20171121/201711211446567326.pdf.

[7] "CrossMatch SEEK Avenger." http://info.crossmatch.com/hubfs/datasheet/seek-avenger.pdf.

[8] "Morphosmart 1300 Series." https://www.morpho.com/sites/morpho/files/morphosmart-1300-series-0517-en.pdf.

[9] "Precise Match on Card." https://precisebiometrics.com/case/match-on-card-portugal/.

[10] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Computing Surveys*, vol. 47, no. 2, p. 28, 2015.

[11] J. J. Engelsma, K. Cao, and A. K. Jain, "Raspireader: Open source fingerprint reader," *arXiv preprint arXiv:1712.09392*, 2017.

[12] K. A. Nixon, V. Aimale, and R. K. Rowe, "Spoof detection schemes," in *Handbook of Biometrics*, pp. 403–423, Springer, 2008.

[13] "Morpho Fake Finger Detection." https://www.morpho.com/en/media/morpho-worlds-first-company-receive-common-criteria-certification-fake-finger-detection-20130702.

[14] "Goodix Live Finger Detection." https://findbiometrics.com/goodix-zte-biometric-sensor-3103187/.

[15] D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake fingerprint detection by odor analysis," in *International Conference on Biometrics*, pp. 265–272, Springer, 2006.

[16] P. D. Lapsley, J. A. Lee, D. F. Pare Jr, and N. Hoffman, "Anti-fraud biometric scanner that accurately detects blood flow," Apr. 7 1998. US Patent 5,737,439.

[17] R. K. Rowe, "Multispectral imaging biometrics," Dec. 2 2008. US Patent 7,460,696.

[18] A. Shiratsuki, E. Sano, M. Shikai, T. Nakashima, T. Takashima, M. Ohmi, and M. Haruna, "Novel optical fingerprint sensor utilizing optical characteristics of skin tissue under fingerprints," in *Biomedical Optics*, pp. 80–87, 2005.

[19] S. B. Nikam and S. Agarwal, "Local binary pattern and wavelet based spoof fingerprint detection," *Int. J. Biometrics*, vol. 1, pp. 141–159, Aug. 2008.

[20] L. Ghiani, P. Denti, and G. L. Marcialis, "Experimental results on fingerprint liveness detection," in *7th International Conference on Articulated Motion and Deformable Objects*, pp. 210–218, Springer-Verlag, 2012.

[21] A. Abhyankar and S. Schuckers, "Integrating a wavelet based perspiration liveness check with fingerprint recognition," *Pattern Recogn.*, vol. 42, pp. 452–464, Mar. 2009.

[22] T. Chugh, K. Cao, and A. K. Jain, "Fingerprint spoof buster: Use of minutiae-centered patches," *IEEE Trans. Information Forensics and Security*, 2018.

[23] R. Nogueira, R. Lotufo, and R. Machado, "Fingerprint liveness detection using convolutional neural networks," *IEEE Trans. Information Forensics and Security*, vol. 11, no. 6, pp. 1206–1213, 2016.

[24] E. Marasco and C. Sansone, "On the robustness of fingerprint liveness detection algorithms against new materials used for spoofing," in *Proc. Int. Conf. Bio-Inspired Syst. Signal Process.*, pp. 553–558, 2011.

[25] B. Tan, A. Lewicke, D. Yambay, and S. Schuckers, "The effect of environmental conditions and novel spoofing methods on fingerprint anti-spoofing algorithms," *IEEE Workshop on Information Forensics and Security*, 2010.

[26] A. K. Jain, S. S. Arora, K. Cao, L. Best-Rowden, and A. Bhatnagar, "Fingerprint recognition of young children," *IEEE Trans. Information Forensics and Security*, vol. 12, no. 7, pp. 1501–1514, 2017.

[27] "Unique Identification Authority of India." https://uidai.gov.in/.

[28] "Unique Identification Authority of India, dashboard summary." https://portal.uidai.gov.in/uidwebportal/dashboard.do.

[29] "World Food Programme." http://www1.wfp.org/.

[30] "The UN Refugee Agency." http://www.unhcr.org/en-us/.

[31] "Bill and Melinda Gates Foundation." https://www.gatesfoundation.org/.

[32] Y. Koda, T. Higuchi, and A. K. Jain, "Advances in capturing child fingerprints: A high resolution cmos image sensor with sldr method," in *Biometrics Special Interest Group (BIOSIG), 2016 International Conference of the*, pp. 1–4, IEEE, 2016.

[33] "Crossmatch L Scan 500/1000." https://a3fcb69dc7037ab91b58f8ba-qnewmedia.netdna-ssl.com/wp-content/uploads/2017/05/20160726-DS-En-L-Scan-500-1000.pdf.

[34] "Fingerprint Sensing: The Next Generation." https://www.synaptics.com/sites/default/files/fingerprint-sensing-biometric-security.pdf.

[35] "Lumidigm M-series fingerprint sensors." https://www.hidglobal.com/sites/default/files/resource_files/hid-lumidigm-m-series-sensors-ds-en.pdf.

[36] "Tech 101: Match on Card Biometrics." https://www.secureidnews.com/news-item/tech-101-match-on-card-biometrics/.

[37] "Gemalto IDPrime .NET Bio Solution." https://www.gemalto.com/brochures-site/download-site/Documents/dotnet_bio.pdf.

[38] "Compute Module 3 Lite." https://www.raspberrypi.org/products/compute-module-3-lite/.

[39] "Compute Module IO." https://www.raspberrypi.org/products/compute-module-io-board-v3/.

[40] "Camera Module V2." https://www.raspberrypi.org/products/camera-module-v2/.

[41] "Intel Neural Compute Stick." https://developer.movidius.com/.

[42] "HDMI Resistive Touchscreen." https://www.adafruit.com/product/2260.

[43] "USB Battery Pack." https://www.adafruit.com/product/1566.

[44] "Improving Maternal and Child Nutrition." https://www.wfp.org/sites/default/files/IMCN%20factsheet.pdf.

[45] "Immunization Coverage." http://www.who.int/mediacentre/factsheets/fs378/en/.

[46] "Social Protection for a Changing India : Executive summary." http://documents.worldbank.org/curated/en/971181468044348789/Executive-summary.

[47] "Connex 350." http://global72.stratasys.com/~/media/Main/Files/Machine_Spec_Sheets/PSS_PJ_Connex3.ashx.

[48] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, and H. Adam, "Mobilenets: Efficient convolutional neural networks for mobile vision applications," *arXiv preprint arXiv:1704.04861*, 2017.

[49] A. A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics*. Springer, 2006.

[50] K. Cao and A. K. Jain, "Automated latent fingerprint recognition," *IEEE Trans. Pattern Analysis and Machine Intelligence*, 2018.

[51] "Electron." https://electronjs.org/.

[52] "Fingerprint Matching Software." https://www.innovatrics.com/idkit-fingerprint-sdk/.