MEDINFO 2017: Precision Healthcare through Informatics
A.V. Gundlapalli et al. (Eds.)

doi:10.3233/978-1-61499-830-3-1053

Comparative Performance Analysis of Different Fingerprint Biometric Scanners for Patient Matching

Noah Kasiiti[a], Judy Wawira[b], Saptarshi Purkayastha[c], Martin C. Were[a,d,e]

[a] *Institute of Biomedical Informatics, Moi University, Eldoret, Kenya*
[b] *Department of Radiology, Indiana University, Indianapolis, IN, USA*
[c] *School of Informatics, Indiana University-Purdue University Indianapolis, Indianapolis, IN, USA*
[d] *Department of Biomedical Informatics & Medicine, Vanderbilt University, Nashville, TN, USA*
[e] *Vanderbilt Institute of Global Health, Vanderbilt University, Nashville, TN, USA*

Abstract

Unique patient identification within health services is an operational challenge in healthcare settings. Use of key identifiers, such as patient names, hospital identification numbers, national ID, and birth date are often inadequate for ensuring unique patient identification. In addition, approximate string comparator algorithms, such as distance-based algorithms, have proven suboptimal for improving patient matching, especially in low-resource settings. Biometric approaches may improve unique patient identification. However, before implementing the technology in a given setting, such as health care, the right scanners should be rigorously tested to identify an optimal package for the implementation. This study aimed to investigate the effects of factors such as resolution, template size, and scan capture area on the matching performance of different fingerprint scanners for use within health care settings. Performance analysis of eight different scanners was tested using the demo application distributed as part of the Neurotech Verifinger SDK 6.0.

Keywords:

Biometry; Patient Identification Systems; Health Information Systems

Introduction

A critical component of health care delivery is the ability to correctly identify the individual receiving care and access their medical record. Failure to correctly match patients is a major contributor to inefficiencies in care delivery and medical errors [1]. For example, in the United States, about 195,000 deaths occur each year because of medical errors, with 10 of 17 being the result of identity errors [2]. The problem is even worse in low and middle income countries (LMICs) where very few accurate and comprehensive person identification procedures guaranteeing the unambiguous identification of their citizens from the day they are born, have been implemented [3]. Poor national person identification systems, inefficient identification procedures, and the use of weak search criteria further aggrevate the problem.

In the western world, researchers and hospital administrators largely rely on deterministic or probabilistic algorithms and other statistical matching procedures for patient identity management [4]. Deterministic matching algorithms use an exact match or rely on comparisons between two fields [5]. As an example, deterministic matching can be used to compare unique identifiers, such as national IDs, to determine a match. Probabilistic matching, which is by far the most widely implemented technique for record matching, does not depend on unique identifiers. For probabilistic matching, the values between two records are compared across several fields and weights are assigned based on how close the values in the corresponding fields are. The sum of these weights indicate the closeness of the match for the compared records [4-6]. In the case of patient identification, probabilistic matching would compare closeness using key patient identifiers such as name, address, national IDs, and date of birth.

The application of these statistical matching approaches is limited, especially in developing countries. Deterministic matching in these settings is limited when no single field can provide a reliable match between two records. In many cases, the order that a patient's first, middle, and last name are recorded differs between visits, addresses are unreliable, dates of birth are often estimated, and patients can have multiple clinic identifiers that are not common within or across facilities [7]. These countries often do not have a single national identifier for all individuals, with national IDs given to those above a particular age and often not given to foreigners residing in the country [8]. Another challenge of using deterministic algorithms for patient matching is that they lack scalability, requiring expensive customization and business rule revisions as databases grow [5].

Probabilistic algorithms do not perform very well in many low-resource health care settings. In our institutional experience, the evaluation of various four-string manipulation strategies to improve the performance of probabilistic models, based on Kenyan names, revealed a suboptimal specificity and a positive predictive value of less than 50% [9]. While probabilistic algorithms are superior to deterministic algorithms, not all probabilistic algorithms applied to the same set of circumstances yield results with the same degree of accuracy [5]. This is because probabilistic algorithms typically sample the dataset and do not scan all possible values, thus matching functions become more complex and time consuming, increasing the number of false positive matches [10]. Current statistical matching models cause many challenges to unique patient identification in health care settings, and often tend to be difficult and expensive to implement. Thus, there is a critical need to evaluate relatively cheap, feasible, and effective solutions to tackle the patient matching problem in all health care settings, including LMICs and industrialized nations.

Biometric approaches offer a potential solution to the challenges of current patient matching algorithms. The basic principle of biometric authentication is that everyone is unique

and can be identified by his/her intrinsic physical or behavioral traits [11]. Among the available biometric technologies, fingerprint technology offers a potentially promising solution; fingerprint scanners are readily available, the technology is relatively, easy to use, has minimal database memory requirements, and there exist several demonstrated instances of their large-scale use in other sectors, such as banking and immigration departments.

Biometric technology is not without its challenges, among them being the need to invest in specialized technology and equipment required to capture many of the needed biometric measurements. Due to the poor performance of statistical patient matching models within our LMICs setting, we explored the potential of using fingerprinting biometric technology as additional metadata for patient matching. A fingerprint consists of a pattern of ridges and valleys in the surface of the fingertips and forming during early fetal months [12]. Apart from the algorithm, the performance of this technology is affected by factors such as image quality, composition of target user population, resolution, template size, and scanner type or model.

To determine the right device and approach for implementing biometrics, we conducted a systematic assessment of the technical performance of various fingerprinting devices available on the market that could be used within most care settings. The goal was to explore the selection of the right biometric device for countries aiming to develop systems for unique patient identification.

Methods

The envisioned workflow of the biometric technology at our institution, as in most clinical settings, will be as follows. When the patient first arrives at the facility, they will be asked to scan their left index finger through the fingerprint biometric scanner. Based on the scan, the fingerprint image will be converted to a template locally and this template will be sent over the network to the fingerprint matching service. The matching service will match the template against a database of existing fingerprints and will return NULL, if there is no match found or will return the patient id if a match is found. When NULL is returned, the patient registration page is opened and a new fingerprint image is used to create a fingerprint template for future matching. A matched fingerprint returns a patient id, allowing the patient's record to be directly accessed during the clinical encounter.

The current evaluation focused on identifying the technology that provides the best fingerprint match. To evaluate the technical performance of various scanners available in the market, we leveraged an application that worked with over 180 fingerprinting devices. This application, the Neurotech Verifinger Software Development Kit (SDK) 6.0, provides a wrapper of common Application Programming Interface (API) that makes it easy for use with different devices [13]. The goal of using this SDK was to showcase a methodology that other implementers could use when evaluating various scanners for their setting.

Fingerprint templates are mathematical representations of the most useful points of interest (minutiae) in fingerprint images [14]. Using fingerprint images of different fingers (not just the index finger), downloaded from various sources, including NIST SD4 [15], NIST SD9 [15], FVC2002 [16], FVC2004 [17], as well as randomly replicated of images, a large dataset of 50,000 images was generated. Using the SDK template API, we generated templates for these 50,000 images in the default format. This large number of images was adequate to stress test performance, as most care settings would have less than this number of patients. Although the SDK supports ISO/IEC 19794-2:2005, ANSI/INCITS 378-2004, and ANSI/NIST-ITL 1-2007 standards, we chose to use the default one to avoid any bias between fingerprint readers. The test template dataset used one fingerprint image per template.

For generating the evaluation template, we used two images of the left index finger and then compared the performance and accuracy against the test dataset. There is good evidence that the index finger is used the least and hence has the least normal wear and tear, making it well-suited for fingerprint scanning [18]. Since we used the SDK to translate the minutiae to a template, all templates for both the test dataset and evaluation template used the same feature set and algorithm.

Each fingerprint scanner was used in the same surrounding lighting area to ensure the quality of the image capture was not affected. The devices were connected to an Ubuntu 16.04 x64 platform and tested using the C++ application. We used the standalone application instead of the web application that is based on an ActiveX component or Java applet, because both of these technologies have been deprecated by the browser manufacturers. The C++ application was also more robust in communication with the fingerprint scanners and responded more quickly to images from the fingerprint scanner. Live finger detection was also supported by the Futronic scanners only using the C++ application.

Eight Fingerprint devices (U.are.U 4500, U.are.U 4500 UID Edition, U.are.U 5160, Futronic'FS80, Futronic FS88H, Hamster Plus (HSDU03P™), Biomini, and UPEK Eikon) were selected based on current community member usage and what was affordable and easily available for purchase. Key dimensions for the devices that were analyzed included: resolution, scan capture area, performance, template size, template format, compatible operating system, and supported standards.

Resolution

The number of pixels per inch (dpi) describing the acquired images. High scanner resolution allows for extraction of finer details from a fingerprint image, making it very important when identifying infants and elderly patients. A 500 dpi resolution is required by FBI-compliant systems [19].

Scan Capture Area

Determines the size of the fingerprint portion which can be acquired by the scanner. This parameter usually lies in the range 1.0"x1.0" square inches of some professional models to about 0.38"x0.38" of some low profile models. It is worth noting that the captured portion of the latter is about 7 times smaller than the former. A wide sensing area is important because the size of an average fingerprint is about 0.5"x0.7" (smaller for children and females and larger for adult males) and therefore the acquisition of a fingerprint with a sensing area smaller than 0.5"x0.7" produces a partial fingerprint [20].

Performance Matching

The speed and accuracy of identification and other derivatives that arise from accuracy. In our evaluation, performance was determined by the speed in milliseconds of correctly identifying a person from the test dataset of 50,000 fingerprint images. Matching speed impacts patient workflow and should be minimized to reduce patient waiting time during registration.

Template Size

Describes a stored file in a fingerprint scanning system and is normally stored as binary file. When a fingerprint is entered into the system, only a "template" of the fingerprint is stored, rather than the fingerprint image. A fingerprint template is

smaller than the actual fingerprint image and using the template instead of an image reduces processing time. Search speed is said to be directly related to template size; the smaller the template, the faster the search speed [21].

Template Format (Gray Scale Levels)

Of a fingerprint sensor is the number of gray shades produced for every pixel. 256 levels of gray is the standard format supported by most available fingerprint sensors today and results in using one-byte per pixel [22].

Compatible Operating System

Is highly dependant on the manufacturer of the scanner. Most scanners support Windows, Linux, iOS, and Android.

Supported Standards

This is similar to operating system compatibility and is largely determined by the manufacturer.

Results

Among the seven basic criteria for biometric security systems, performance or accuracy is a prerequisite (Table 1) [23]. The average perfomance time for the tested scanners was 1984.3 milliseconds, with wide variability across the different scanners. The best performance matching was achieved with the U.are.U 4500 UID edition, with a matching time of 600 milliseconds in a ratio of 1:50000 templates. The scanner resolution was 500 dpi, within the recommended range. The U.are.U 4500 scanner had a resolution higher than the U.are.U 4500 UID edition (512 dpi). This scanner will definitely produce a finer and more detailed extract from a fingerprint image, however its performance matching was 4-times higher than that of U.are.U 4500 UID edition. As performance is the most crirtical dimension for analysis, a scanner with the fastest performace matching speed and mimimun resolution requirement (i.e., 500 dpi) is prefered.

We observed that search speed when using fingerprint biometric devices was directly related to template size (i.e., the smaller the template, the faster the search speed) [19]. There appeared to be a trade-off among the template size, scan capture area, and performance matching. This is because the fastest scanner (U.are.U 4500 UID edition) did not have the smallest template (72 mm x 39 mm x 21.7). This particular device also did not have a large scan capture area (12.8 mm x 16.5 mm). While this was desirable, manufacturing large and pure silicon chips is difficult and rather expensive; therefore, the scanners currently available on the market are categorized by a small area scan capture area.

On average, it would cost about $107.60 to acquire a scanner (the cost of different fingerprint scanners has been provided in Table 1), though cost is crucial while acquiring these gadgets, we can not compromise performance for cost. That is why an inexpensive scanner with a good resolution, but poor performance matching, may not be a better choice.

Discussion

Biometrics offers an alternative method to collect additional metadata for statistical patient matching models, with good performance characteristics. When determining what scanner to buy, organizations should consider scanners with short turnaround time. We demonstrate the need to critically evaluate multiple dimensions of available scanners prior to purchase. Further, issues around what SDK to use, and how to integrate scanning within the clinical workflow is important and could be a limiting factor for scanner adoption.

Our results demonstrate that the scan area has an impact on performance speed. Optimizing scan area can be improved by training and providing ambient conditions to capture fingerprint images. The technique of capturing the fingerprint may necessitate a large scan area (e.g., in cases where you want to simultaneously capture multiple fingerprints). When speed is optimized, template size can be tweaked to reduce memory and storage requirements. This is particularly useful for mobile health where there are database capacity and infrastructure limitations.

Privacy and security implications surrounding the use of biometrics is extremely important, but was beyond the scope of the current study. Given that a number of large-scale collections of fingerprints is already underway (e.g., passports and social security in both high-income and low-income countries), debates are largely dependent on the reason for capturing biometric information. Identity theft, no means to revoke leaked biometrics, health equity, denying services to individuals, and many other ethical issues are some of the factors affecting the success of biometric implementations.

There are limitations to the current study. Only a few devices were evaluated; we did not separate groups of patients (e.g., neonates and elderly), who may skew the analysis and variation of performance between these groups; and we did not evaluate performance of various fingers (e.g., index versus middle finger for a specific patient). The evaluation was also conducted using a single test set; findings would likely be different based on the population being evaluated.

Numerous costs impact the implementation of biometric systems and vary by the size of the organization, choice of system adopted (open source or commercial), and the personnel to manage the infrastructure. Pre-scan enhancer pads, which cost roughly $47, may also be needed. Fingerprint SDK, Neurotechnology SDK costs about $422 for VeriFinger 9.0 Standard SDK. Commercial SDKs are usually restricted to specific scanners however, open source SDKs are also available and are not scanner-specific. Note, that even commercial SDKs require personnel for set-up and maintenance services. Personnel costs (i.e., both training and hire) are highly dependent on the complexity of the system being deployed. Finally, on the back end, most biometric applications are hosted on a server and accessed via client machines; machines should be purchased with a strong firewall to ensure protection from hackers.

Conclusion

Biometric fingerprint scanners offer one potential technology for improving patient matching and unique patient identification in diverse health care settings. Special attention is needed when selecting these technologies to ensure good performance at a reasonable cost. Additionally, it is important that the technology can be implemented within existing workflows and with consideration to existing patient care setting infrastructure constraints. This is especially challenging in clinical settings with complex health care workflows. While this paper is geared towards LMICs, these results and findings are equally applicable to care settings in industrialized nations.

Acknowledgements

This work was supported in part by the NORHED program (Norad: Project #QZA-0484, HI-TRAIN Project), Grand Challenges Canada Stars in Global Health - Round 5 Phase I (S5 0416-01). The content is solely the responsibility of the

authors and does not necessarily represent the official views of the Norwegian Agency for Development Cooperation.

References

[1] Safety and Quality Improvement Guide Standard 5: Patient Identification and Procedure Matching (October 2012), in, Australian Commission on Safety and Quality in Health Care, Sydney, 2012.
[2] B.H. Just, D. Marc, M. Munns, and R. Sandefer, Why Patient Matching Is a Challenge: Research on Master Patient Index (MPI) Data Discrepancies in Key Identifying Fields, *Perspectives in Health Information Management* **13** (2016).
[3] F. Verbeke, S.V. Bastelaere, and M. Nyssen, Patient Identification And Hospital Information Management Systems In Sub-Saharan Africa: A Prospective Study In Rwanda And Burundi., *Rwanda Health Communication Center - Rwanda Biomedical Center (RHCC - RBC)* **69** (2013), 7-12.
[4] L.M. Gliklich and R.E. Dreyer, Registries for Evaluating Patient Outcomes: A User's Guide [Internet], in, 2014.
[5] S. Schumacher (2007) *Probabilistic versus deterministic data matching: making an accurate decision, DM Direct,*
[6] Deterministic and Probabilistic Data Matching (Master Index Match Engine Reference). Retrieved from https://docs.oracle.com/cd/E19182-01/821-0919/ref_sme-deter-probl_c/index.html.
[7] Oracle (2010) *Deterministic and Probabilistic Data Matching (Master Index Match Engine Reference).* Retrieved from https://docs.oracle.com/cd/E19182-01/821-0919/ref_sme-deter-probl_c/index.html.
[8] theBeehive (2001) *How to get a National Identity Card | The Beehive - Kenya*. Retrieved from http://kenya.thebeehive.org/en/content/640/1757.
[9] P. Sonak, W. Martin, and G.J. Wawira, Improving registration to improve retention and linkage of patients for rural healthcare delivery in Western Kenya, in, 2014.
[10] K. Perspectives (2016) *Deterministic versus Probabilistic Matching in Big Data - Knowledgent Perspectives*. Retrieved from https://blog.knowledgent.com/deterministic-versus-probabilistic-matching-big-data/.
[11] M. Cobb. *What is biometrics?* Retrieved from http://searchsecurity.techtarget.com/definition/biometrics.
[12] H. Jhaveri, H. Jhaveri, and D. Sanghavi, Biometric Security System And Its Applications in Healthcare, *International Journal of Technical Research and Applications* **2** (2014), 15-20.
[13] VeriFinger fingerprint recognition technology, algorithm and SDK for PC, smartphones and Web. Retrieved from http://www.neurotechnology.com/verifinger.html.
[14] X. Jiang and Y. Wei-Yun, Fingerprint minutiae matching based on the local and global structures, in: *International Conference on Pattern Recognition*, IEEE, 2000, pp. 1038-1041.
[15] NIST. *NIST Special Database 4 | NIST*. Retrieved from https://www.nist.gov/srd/nist-special-database-4.
[16] FVC2002 - Second International Fingerprint Verification Competition. Retrieved from http://bias.csr.unibo.it/fvc2002/download.asp.
[17] FVC2004 - Third International Fingerprint Verification Competition. Retrieved from http://bias.csr.unibo.it/fvc2004/download.asp.
[18] Desert Hand Therapy. 18 Amazing Facts About Human Hands | Desert Hand Therapy, in, 2016.
[19] M. Sandstrom, C. Fredrik, and V. Fak, Liveness Detection in Fingerprint Recognition Systems, (2004).
[20] Biometrika srl (2015) *Biometrika - Basics of fingerprint recognition technology and biometric systems.* Retrieved from http://www.biometrika.it/eng/wp_scfing.html.
[21] F.W.S. Bhd (2009) FingerTec. *Fingerprint Technology White Paper*. Retrieved from http://www.fingertec.com/academia/download/whitepaper-01.pdf.
[22] Next Biometrics Group Asa, *Resolution & Gray Scale Levels - NEXT Biometrics*. Retrieved from http://nextbiometrics.com/security/resolution___gray_scale_levels/.
[23] R. Jain, Abstract : Keyword : Table of Contents : 2-Application Fields for Biometrics Technology, (2004), 1-10.

Address for correspondence

Noah J. Kasiiti

College of Health Sciences, Institute of Biomedical Informatics, Moi University, Eldoret, Kenya, P.O Box 3900-30100
Email:kasiitinoah@gmail.com,
Tel1:+25479016388,Tel2:+2567537641022

Table 1: Performance analysis of various fingerprint scanners

Brands	Resolution (dpi)	Template Format (bit grayscale (256 gray levels))	Template Size (mm)	Scan Capture Area (mm)	Supported Standards	Performance (ms, Matching 1:50,000)	Operating System Compatibility	Cost (USD)
U.are.U 4500	512	8	65 x 36 x 15.6	14.6 x 18.1	FCC Class B, CE, ICES, BSMI, MIC, USB, WHQL	2420	Microsoft Windows, Linux	$75.00
U.are.U 4500 UID Edition	500	8	72 x 39 x 21.7	12.8 x 16.5	FIPS 201 PIV, STQC	600	Microsoft Windows, Linux	$60-70
U.are.U 5160	500	8	72 x 39.5 x 21.7	15 x 18	FIPS 201 PIV, RoHS, WEEE UL, USB, WHQL	1388	Windows Linux Android	$183.81
Futronic' FS80	500	8	45 x 63 x 26	16 x 24	USB 2.0 compatible interface, plug and play device	1450	Windows, Linux, MAC OS , Android	$65.99
Futronic FS88H	500	8	59 x 60 x 20	16.3 x 24.4	FIPS 201/PIV, FAP20, Microsoft WHQL, FCC and CE, RoHS	1280	Windows, Linux, MAC OS , Android	$233.92
Hamster Plus (HSDU03P™)	500	8	53 x 73 x 84	13.2 x 15.2	FCC, CE, KCC, RoHS	900	Windows, Windows Server, Android, Java, Linux	$76.99
Biomini	500	8	66 x 90 x 58	16 x 18	CE, FCC, KC, WHQL	3800	Windows, Linux, Android	$115.00
UPEK Eikon	508	8	84 x 34 x 14	25 x 10	• ISO/IEC 1 9794-2 (minutiae) and ISO/IEC 1 9794-4 (image) • ANSI INCITS 378 (minutiae) and ANSI INCITS 381 (image), • WSQ 3.1	2952	Windows, Linux, MAC OS , Android	$ 39.95