Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Using biometric-based identification systems in Brazil: A review on low cost fingerprint techniques on-the-go

Márjory Da Costa-Abreu [a,*], *Stephen Smith* [b]

[a] DIMAp-UFRN, Campus Universitário Lagoa Nova., CEP: 59078-970, Natal, RN, Brazil
[b] Department of Electronics, University of York, Heslington, York YO10 5DD, UK

Keywords:
Security in Brazil
Biometrics
Affordable devices
Fingerprint

ABSTRACT

Automatic authentication has become an essential service in several public areas. However, although the technology related with this kind of service has evolved, the price tag of its use is not affordable for most countries. In the so-called "under developed" counties, such as Brazil, South Africa and India, for example, registration systems are often paper-based and/or cover only a fraction of the population. Thus, the reality is that there is an increasing gap into the usage of such technologies amongst different countries and it can be a factor that makes development more difficult and, therefore, less inclusive. One of the main technologies used for automatic identity prediction is based on biometrics analysis, which can distinguish physical or behavioural features to help overcome the traditional paper-based identity systems. Despite the limitations already mentioned, Brazil is known to have introduced several different uses of biometric-based technologies for authentication. However, the use of these technologies is not always ideal and, since the population size is a key factor, it is essential to select the most affordable option which is not necessarily the most adequate for the country's needs. This paper will focus on establishing what biometric-based solutions exist in Brazil today, highlighting the main challenges, as well as briefly proposing a new prototype for mobile fingerprint acquisition.

1. Introduction

It is now well accepted that automatic identity verification is an established and reliable part of the user identification process in many countries. However, the reality in a lot of poor, or developing countries, is that there is still no reliable way to verify identification (ID), since they cannot afford the latest and more effective technology and, thus, are forced to use outdated paper-based systems. Despite the cost issues, it is now common to see governments adopting automatic data analysis for identification, such as iris, fingerprint or other biometric processing, as the basis for national ID, elections and payment of benefits (Jain and Ross, 2015).

The main difference between paper-based and automatic-based biometric systems is the theoretical guarantee of an authentication which will be reliable and can be tracked, if necessary. Another recent important player in this scenario is the popularisation of mobile devices, which has been used, more often than not, as a means of substitute paper-based systems,

[*] *Corresponding author.* DIMAp-UFRN, Campus Universitário Lagoa Nova., CEP: 59078-970, Natal, RN, Brazil.
E-mail address: marjory@dimap.ufrn.br (M. Costa-Abreu).

http://dx.doi.org/10.1016/j.clsr.2017.03.003

Please cite this article in press as: Márjory Da Costa-Abreu, Stephen Smith, Using biometric-based identification systems in Brazil: A review on low cost fingerprint techniques on-the-go, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.003

such as bank transactions and purchases in general. A downfall of this sort of technology is privacy concerns and personal data protection. Thus, combining automatic biometric-based systems with mobile usage for private and secure transactions is a very popular trend (Ibrahim and Abubakar, 2016).

Although Brazil has a growing economy and has an increasing world profile, the reality is that its continuing underinvestment in basic services (security, health, transport) still defines it as an under-developed unit in terms of its problems with access to emerging technology. Following the aforementioned trend, the 2014 FIFA World-Cup and the 2016 Olympics have generated new interest by local government in investing to develop its own solutions for identity verification and protection, aiming to take real steps towards “smart cities”.

However, this will require the development and deployment of appropriate technology-focused solutions which, in turn, means that important engineering challenges will need to be addressed and core expertise built up and nurtured within Brazil. One of the areas within which enormous opportunities are arising in this respect is that of the security of citizens. In particular, improving effective crime investigation, detection and prevention through the exploitation of technological “smart” solutions is likely to pay substantial dividends both in terms of quality of life for all citizens and economic impact. This type of scenario is promoting opportunities for more effective and efficient support for security initiatives, and is encouraging a desire for greater collaboration between academic and public service agencies.

This paper aims to consider the main challenges of employing biometric data in Brazil by highlighting several aspects of its use, as well as proposing a new and cost-effective technique for fingerprint acquisition on the go and in challenging environments, that can have a significant impact on the work of the local police for fighting crime.

Our approach is to explore the deployment of biometric technologies in a way that integrates two complementary perspectives. First, we will show how biometrics can substantially increase the security of individual citizens in their everyday lives, easily and cost-effectively, and how this is currently not being fully explored in Brazil. Secondly, we will demonstrate one way in which biometrics can support more effective crime detection and prevention.

2. Biometrics usage around the world

The increasing use of automatic biometric-based identification systems has encouraged their development, with regards to improving effectiveness, reliability, and guarantee of service, as well as helping decrease the gap between poorer countries with regards to more sophisticated identification systems. This technology can also improve the lives of minority groups because, as already mentioned previously, it provides a more robust identification system. A few examples can be seen below:

- The use of biometrics systems in the Nigerian federal pension system eliminated nearly 40% of the beneficiary roll. This not only increases efficiency and accountability, but also has the potential to improve services (assuming the funds saved are redirected accordingly) (Aranuwa and Ogunniye, 2012).
- India has introduced an ID programme that covers just over 240 million people, and has contributed to the rapidly falling costs of the new technology. However, many programmes are still in the early stages, and only a few of the 160 cases have had impact studies conducted so far (Tandon, 2005).
- South Africa has already been using this technology in electronic transfers and ATMs to distribute pensions and social grants for over 20 years (Wall et al., 2015).
- The Pakistani national identification agency has deployed a systems that reliably verifies who is entitled to the disaster relief funds resulting from the 2010 floods, through the use of Visa cards (Jacobsen, 2015).

Despite the above examples, most uses of automatic biometrics-based systems can be found in well-developed and prosperous countries, such as members of the European Union (Caldwell, 2015; Labati et al., 2015) and the USA (Farrell, 2016). This is understandable as they are mature democracies that have strong protection laws that legislate for the appropriate use of this type of data (Bustard, 2015). Relative to alternatives, biometric identification can increase inclusion, privacy and efficiency.

Biometric authentication combined with PINs or numbers conveys no significant personal information. In some cases, this can be preferable to more “human” processes, involving personal knowledge or intrusive questioning. In the absence of a functioning identification system, completing a biometric exercise to create one may be no more costly than a paper-based alternative, and may save greatly in the long run due to more automation and reduced fraud.

3. Brazil and biometrics usage

Brazil has a long history of attempting to adopt automatic means of identity verification.

There has been a plan for a Civil Identification Registry (RIC) since 1997 (with the signing of a new law) which intended to have a unique identification system for the 27 regions of the country by 2020. Despite the federal law being nearly 20 years old, there are still obstacles to its implementation. These registrations are made at city council level and the fact that the cities will “lose” that income to the federal level is the main problem this scheme faces.

In 2014, the Ministry of Justice took over the project and since then there has been a smartcard prototype launched, containing digitised face, fingerprint and iris information linked to an Automated Fingerprint Identification System (AFIS) (Lenharo, 2014). However, despite the fact that the fingerprint is considered standard practice in identity registration in Brazil, there is growing concern regarding threats to privacy, since this information would be held in a centralised database.

Once the RIC is established as the new national ID, a proposed bill under discussion would make the use of the ID-based biometrics registration mandatory, after allowing one year for issuing agencies to improve the technology, and setting a six year cut-off after which non-biometric ID cards would be rendered invalid.

Please cite this article in press as: Márjory Da Costa-Abreu, Stephen Smith, Using biometric-based identification systems in Brazil: A review on low cost fingerprint techniques on-the-go, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.003

Since there has been such a long discussion regarding a nationalised ID system, some states of Brazil have started to propose their own internal ID, based on the RIC and funded by public–private partnerships, such as the 'Sao Paulo Card' in Sao Paulo. Despite the unrealistic deadline for the implementation of the RIC, the growing trend of biometric data collection in Brazil has in no way slowed.

One good example of an automatic biometric-based system that is being implemented in Brazil at the moment is the electronic electoral system. The Superior Electoral Court launched a pilot project of biometric voting registration in 2008 which aimed to be used for the first time in the elections of 2011.

Once the Superior Electoral Tribunal's database is fully populated (which will include the selection of 100% Brazilian software for certifying and managing the election process), this will be the world's largest biometric identification system based on fingerprints. Although the numbers are very optimistic, the reality in the voting polls is that the systems still needs a long time to work properly with the sheer number of voters. The election of 2014 saw voters waiting for up to four hours to vote in polling stations because the systems did not perform as expected.

The fact that the national automated biometric-based systems are being implemented very slowly and with little success to date has not discouraged its use in several different facets of public life.

- There are plans to adopt a fingerprint-based transport card system in a few capitals.
- Facial recognition technology for surveillance on buses is already in use in a number of Brazilian cities.
- Several schools (from education to driving) have already adopted a fingerprint-based present system.
- Some banks have already started to use fingerprint recognition in ATMs for authentication instead of pin numbers.

Again, these biometric-based systems are the result of public–private partnerships, thus, there is no guarantee of privacy or even provision of government access to this data.

Brazilian legislation governing the protection of personal data is found in several statutory laws. The private lives of people is considered inviolable according to the Brazilian Civil Code and, if there is a violation, the affected person is entitled to seek punishment for any unauthorised collection or use of their personal data. The protection established by the Brazilian Regulatory Framework for the Internet takes into account private communication content, connection and Internet applications access logs; however, it does not define "personal data".

Further regulation is expected in the near future via a Presidential Decree that will detail some of the matters addressed in the law (Costa, 2012). The main rule protecting personal data is set out in the Brazilian Federal Constitution.

4. Challenges specific to Brazil

As already presented in the Section 3, the use of automated biometric-based authentication in Brazil is relatively well accepted and its use commercially is growing. This section will consider in more detail some well-known problems regarding the use of biometric data, and some fundamental problems specific to Brazil related to the unchecked usage of such data.

4.1. *Data acquisition costs*

Failures to enrol are often a serious problem when deploying biometric systems, and yet they have not received as much attention as matching failures. This problem can be caused by missing or damaged biometric characteristics, poor user training, poor devices and other issues.

Since Brazil is a continental country and the social and economical differences are large, it is a challenge in itself to collect the same quality data in the middle of the Amazon, or in the desert areas of the Northeast. Thus, it is clear that any biometric system will have to plan for participants who are not able to enrol in the system, and this may be a sizeable portion of the participants depending on the target areas. It is important to remember that a major part of the population still lives in remote and hard to access areas.

Even though prices are falling, the unit cost reported for some national ID schemes developed for prosperous countries far exceed the unit cost affordable in poor countries, which have typically been around US5 per head. Where technology is costly, the cost may be passed on to citizens and imposes barriers to access.

4.2. *Exclusion*

It not everyone that is able to provide the ideal biometric data necessary for an acceptable recognition performance, particularly fingerprints. The exclusion happens when there is a limitation of the technology that can marginalise those individuals if other options are not put in place.

It is especially hard for Brazil that has agriculture as one of its major pillars of the economy, and the challenges this presents to implementing popular biometric modalities such as face (sun-burn and early ageing), fingerprint (damage to the skin), and signature (most of this specific population is illiterate), for example. One of the most popular solutions for this specific problem is the use of multiple biometrics ("multimodal"). This approach can lower the risk, but the cost involved in adding extra modalities needs to be taken into account.

A very common Brazilian practice can be especially sensitive to this problem. It is very likely that these systems are developed within a short deadline, which normally is not enough time to deal with issues in the enrolment and otherwise eligible people may be overlooked or unable to enrol.

4.3. *Online mobile data processing*

With the increase of the mobile data, which can be collected by mobile devices, there is a significant rise in data-intensive applications, which deals with a huge amount of mobile data. Many of the applications regarding authentication are oriented towards detecting particular real-time situations, which brings them into the domain of Event Processing.

This expansion introduces new challenges for mobile computing such as how to manage real-time big data or what kind of sensor can work on several different environments in an efficient way. The globalisation process accelerated the evolution of telecommunication technologies over the past years, providing higher quality, connection speeds and stability for users.

There is a new move by the Brazilian government to bring broadband connections to most parts of the country and to provide universal access to the Internet. But, in a country where some of its population is still without running water, basic sewage system or electricity, or where mobile networks had not yet reached, it is hard to be optimistic.

4.4. *Data privacy and security*

A more complex challenge is that related to violation of individual privacy. There are a number of facets to this fear, including the need for data to be securely held and the question of whether or not taking a biometric image is inherently intrusive and an infringement of essential human rights. Biometric technology raises some special privacy issues – digital photography poses a unique challenge as facial recognition is increasingly used for remote surveillance by governments and private companies. Unlike fingerprint and iris scanners, facial recognition can be used without the knowledge or consent of the subject.

Another important issue is how long biometric data should be kept, and there is a real concern worldwide that retention of such data may far exceed the period of relevance for the particular application that motivated its collection. Perhaps, because there is currently no specific data protection law in Brazil that prohibits anyone to generate a new database unchecked, there are more complex privacy issues, which are concerned with the ability to link information from a number of databases using a common biometric identifier. The argument that this may increase efficiency can be used; however, it may also facilitate the government (or others) infringing the right to confidentiality.

Since personal data processing is more popular now, privacy concerns and protection of such data has become part of the Brazilian government agenda. This has initiated a series of changes in law and recommendations. The current Brazilian legal framework has only touched on the protection of privacy of personal data in provisions spread across the Federal Constitution, the Consumer Protection Code and a few other laws. Because there is wide fragmentation of these specific laws, the legal uncertainty is not uncommon when analysing different cases.

One considerable step in the right direction was the Civil Rights Framework for the Internet (Law 12.965, of 23 April 2014) which has established the rights regarding the use of personal data obtained electronically, as well as including the rights for owners of the data to be clearly and fully informed about the processing of their data, a requirement to obtain the consent of the data subject to such processing and a right to opt out of any processing.

The current challenge for the police is to take into account the use of biometric personal data and consider introducing some transitional measures, such as:

- being more transparent about the treatment of personal data;
- being clear how the users can check, update and delete their information; and,
- having a reliable way to guarantee security and protection of the database and its integrity, preventing partial or total unauthorised access.

5. Using fingerprint-based identification in the wild: state of the art

It is clear from the issues considered in the previous sections of this report that there is a clear and immediate need to develop an inexpensive and reliable solution for authentication and identification of individuals in the street environment using biometric data, whilst protecting the privacy of all involved, where appropriate.

In order to do this, we have developed and evaluated a fingerprint-based toolkit suitable for use in a local area to support (a) individual citizens in improving their personal security and (b) the police and other agencies to improve their crime detection and prevention capabilities, through the adoption of new technological approaches.

We have chosen fingerprints as our test modality as, in Brazilian society, it is the most widely accepted modality and been previously used in several other government initiatives, such as the voting system. This will make our prototype more likely to be adopted by the general security related community (such as police officers and the border force, for example). We propose to enhance the way in which easy-to-use, flexible and reliable technology-assisted individual identification can improve security and quality of life for citizens.

Since fingerprint-based authentication techniques are well developed and widely used in several different sectors of society, we are now interested into developing a new way of acquiring fingerprint data cost-effectively and in the street environment, which, in our case, will mean using mobile devices. Thus, this section will present the latest development towards reaching this goal.

There are several different mobile devices that now come with a fingerprint sensor; however, their price is still out of reach for ordinary people. In Derawi et al. (2012) and Lee et al. (2008), an analysis is presented of how well the camera of several different mobile devices can be used for fingerprint capture. Their main experiments are based on data collected in laboratory conditions which would be very hard to replicate in the real-life scenarios. The authors in Bisio et al. (2013) and Modi et al. (2010) analyse classification performance variations caused by the positioning of the finger against the camera during the capture stage in different smartphones. Their conclusions indicate that if the quality of the image is good enough, it is possible to use correction algorithms to achieve acceptable accuracies. Again, their experiments were performed in laboratory conditions.

In Feng et al. (2015) and Stein et al. (2013), the authors use frames from video capture by several mobile device cameras in order to detect spoofing attempts. Similarly Tiwari and Gupta (2015) proposes an authentication system using finger images from the mobile hand-held devices by using scale-invariant features and Sankaran et al. (2015) proposes the creation of a publicly available smartphone finger photo database that will address the challenges of environmental illumination and background.

In Feng et al. (2013) Piuri and Scotti (2008), and Sandoval-Orozco et al. (2015), the authors analyse the performance of fingerprints collected by external sensors attached to mobile devices. The overall results are very encouraging, but the technique implies extra technology and that will always have impact on cost.

There are several more references in the literature that explore the use of mobile devices for fingerprint processing and acquisition, but their solutions are hardly usable for the ordinary citizen or the police with budget limitations. The main aspect that needs to be highlighted here is the non-ubiquitous characteristic of all acquisition techniques presented in the papers considered here, which is a major hurdle to providing a cost effective and widely deployable identification system.

6. New fingerprint mobile acquisition technique

One of the aims of this paper is to propose a cost-effective and easy way to collect quality fingerprint data from a mobile device. This section will present on such proposed solution.

After investigating the existing solutions in the literature as well as the commercial options, it became clear that the most cost-effective and rapid solution to a deployable identification system is to develop a universal adapter that allows the reuse of existing tablet computer cameras. By designing a simple and yet carefully designed jig placed around the camera, the positioning of the finger is controlled so that a finger print image can be acquired that has minimal deformity and other visual deficiencies.

Fig. 1 shows the jig that was designed for fingerprint acquisition. The material used was VeroWhite, a rigid opaque photopolymer from a manufacturer called Stratasys and was printed on a Stratasys Objet500, Connex3 3D printer. The cost of the printed part was less than five dollars. This kit was designed to be attached to a Samsung Galaxy Note PRO 12.2-inch Tablet. This equipment has an 8MP, 3264 × 2448 pixels camera with LED flash.

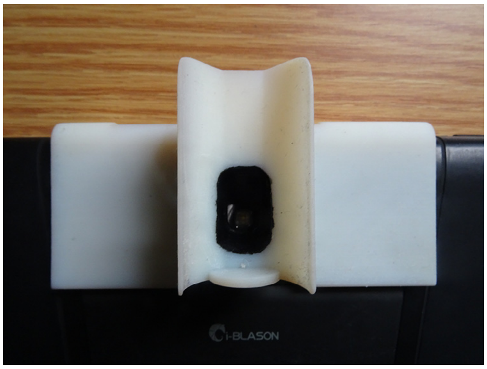

Fig. 1 – Fingerprint collection kit.

In order to identify the fingerprint minutiae which are used by the matching algorithm, a feature extraction algorithm is needed. For this study we used the MINDTCT algorithm (Watson et al., 2007). The reasons why the MINDTCT was used are: is open source; it is widely used commercially, mainly by the FBI, and is also widely used in other studies on biometrics. The IMGTOOLS are included to support the processing of fingerprint images and provide encoders and decoders for Baseline JPEG, Lossless JPEG, and the FBI's Wavelet Scalar Quantitasation (WSQ) which were used in this paper.

After the image has been encoded to the correct format using the IMGTOOLS, the following steps are applied: the fingerprint image is processed to locate all minutiae, for each specifying its location, orientation, type and quality. The MINDTCT architecture and can be divided into the following steps: (i) generation of image quality map; (ii) binarisation; (iii) minutiae detection; (iv) removing false minutiae; (v) counting of ridges between a minutia point and its nearest neighbour; and (vi) minutiae quality assessment.

Due to the variation of image quality in a captured fingerprint image, NBIS analyses the image and locates areas that are degraded. Several features are measured, including low-contrast regions, incoherent ridges flows and high curvatures. These three conditions represent unstable areas in the image where the minutiae detection is unreliable and, together, they are used to represent the levels of quality in the image. An image quality map is generated by integrating these three features. The images are divided into non-overlapping blocks, where a quality level between one and five is assigned to each block.

The minutiae detection step scans the binarised fingerprint image, identifying local pixels patterns indicating a ridge ending or a bifurcation. A set of minutiae patterns is used to detect points of candidate minutiae. Subsequently, false minutiae are removed and the remaining candidates are considered true minutiae in the image.

In the last step, a measure of confidence/quality is associated with each minutiae point detected. Even after the removal step, potential false minutiae remain in minutiae list. A robust quality measure can help get around this. Two factors are combined to produce a quality measure for each minutiae point detected. The first factor is taken directly from the minutia point location within the quality map described above. The second factor is based on a simple statistical of pixels intensity (mean and standard deviation) near the minutia point.

A very small database was collected for these experiments and, just by using the matching algorithm provided by the FBI in the toolkit, we have reached accuracies of 90% when collecting samples in different environments. This is a very encouraging result and demonstrates the potential of this solution and the possibility of wider use of inexpensive but reliable fingerprint-based recognition.

This proof of concept study has led to the adoption of this prototype in the database of the Public Security Secretary (SSP) of Rio Grande do Norte (RN), in collaboration with the Universidade Federal do Rio Grande do Norte (UFRN). Our aim is to develop practical and viable techniques to address the challenges of identification of criminals, and developing intelligence-led data repositories and analytical facilities for this purpose.

7. Final remarks

This paper presents a better understanding of how to adopt biometric technologies in order to create a smart environment to promote greater security and protection from crime for citizens and better technological support for crime investigation agencies, with an emphasis on local solutions with a high degree of ease of use and cost effectiveness.

The impact of the proposed solution will be an increased quality of life for citizens through better protection of assets and less exposure to crime, enhanced procedures and practical tools for agencies involved in crime investigation and prevention.

Although the toolkit includes a facility for identification of individuals based on fingerprint matching of biometric measures, we recognise that national programmes of long-standing exist internationally and are more likely to use the now highly sophisticated options.

It is important to stress that we do not seek to compete with other major initiatives currently being implemented in Brazil and elsewhere, but instead we focus greater attention on the provision of inexpensive, easily deployable tools, which are not widely available in routine security applications.

Acknowledgements

This research was the result of the project entitled “Security for all: Using smart technologies to promote security for citizens” supported by Newton Research Collaboration Programme of the Royal Engineering Academy (NRCP1516/1/135).

REFERENCES

Aranuwa FO, Ogunniye GB. Enhanced biometric authentication system for efficient and reliable e-payment system in Nigeria. Int J Appl Inform Syst 2012;4(2):56–61.

Bisio I, Lavagetto F, Marchese M, Sciarrone A. Performance comparison of a probabilistic fingerprint-based indoor positioning system over different smartphones. In International Symposium on Performance Evaluation of Computer and Telecommunication Systems, SPECTS, pages 161–166, July 2013.

Bustard J. The impact of EU privacy legislation on biometric system deployment: protecting citizens but constraining applications. IEEE Signal Process Mag 2015;32(5):101–8.

Caldwell T. Market report: border biometrics. Biom Technol Today 2015;2015(5):5–11.

Costa L. A brief analysis of data protection law in Brazil. Report, Federal Prosecutor in Brazil. Presented to the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 2012.

Derawi MO, Yang B, Busch C. Security and privacy in mobile information and communication systems: Third International ICST Conference, MobiSec 2011, Aalborg, Denmark, May 17–19, 2011, Revised Selected Papers, chapter Fingerprint Recognition with Embedded Cameras on Mobile Phones, pages 136–147. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

Farrell S. How airports can fly to self-service biometrics. Biom Technol Today 2016;2016(1):5–7.

Feng T, Prakash V, Shi W. Touch panel with integrated fingerprint sensors based user identity management. In IEEE International Conference on Technologies for Homeland Security, HST, pages 154–160, November 2013.

Feng T, Zhao X, DeSalvo N, Gao Z, Wang X, Shi W. Security after login: identity change detection on smartphones using sensor fusion. In IEEE International Symposium on Technologies for Homeland Security, HST, pages 1–6, April 2015.

Ibrahim IA, Abubakar Y. The importance of identity management systems in developing countries. Int J Innov Res Eng Manag 2016;3(1).

Jacobsen KL. Experimentation in humanitarian locations: UNHCR and biometric registration of afghan refugees. Secur Dialogue 2015;46(2):144–64.

Jain AK, Ross A. Bridging the gap: from biometrics to forensics. Philos T Royal Soc Lond B 2015;370(1674).

Labati RD, Genovese A, Munoz E, Piuri V, Scotti F, Sforza G. Advanced design of automated border control gates: biometric system techniques and research trends. In IEEE International Symposium on Systems Engineering, ISSE, pages 412–419, September 2015.

Lee D, Choi K, Choi H, Kim J. Recognizable-image selection for fingerprint recognition with a mobile-device camera. IEEE Trans Syst Man Cybern B Cybern 2008;38(1):233–43.

Lenharo SLR. Brazilian national biometric selection: new and legacy challenges. In Biometrics Group of the RIC (Brazilian Civil Identification Program), 2014.

Modi S, Mohan A, Senjaya B, Elliott S. Fingerprint recognition performance evaluation for mobile id applications. In IEEE International Carnahan Conference on Security Technology, ICCST, pages 243–249, October 2010.

Piuri V, Scotti F. Fingerprint biometrics via low-cost sensors and webcams. In The 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems, BTAS 2008, pages 1–6, September 2008.

Sandoval-Orozco AL, Garca-Villalba LJ, Arenas-Gonzalez DM, Rosales-Corripio J, Hernandez-Castro J, Gibson SJ. Smartphone image acquisition forensics using sensor fingerprint. IET Comput Vis 2015;9(5):723–31.

Sankaran A, Malhotra A, Mittal A, Vatsa M, Singh R. On smartphone camera based fingerphoto authentication. In The IEEE 7th International Conference on Biometrics Theory, Applications and Systems, BTAS, pages 1–7, September 2015.

Stein C, Bouatou V, Busch C. Video-based fingerphoto recognition with anti-spoofing techniques with smartphone cameras. In International Conference of the Biometrics Special Interest Group, BIOSIG, pages 1–12, September 2013.

Tandon H. e-governance: an Indian perspective. Policy Soc 2005;24(3):142–69.

Tiwari K, Gupta P. A touch-less fingerphoto recognition system for mobile hand-held devices. In International Conference on Biometrics, ICB, pages 151–156, May 2015.

Wall KM, Kilembe W, Inambao M, Chen YN, Mchoongo M, Kimaru L, et al. Implementation of an electronic fingerprint-linked data collection system: a feasibility and acceptability study among Zambian female sex workers. Global Health 2015;11(1):1–11.

Watson CI, Garris MD, Tabassi E, Wilson CL, Mccabe RM, Janet A, et al. User’s guide to NIST biometric image software (NBIS). NIST Interagency/Internal Report (NISTIR) - 7392, January 2007.

Please cite this article in press as: Márjory Da Costa-Abreu, Stephen Smith, Using biometric-based identification systems in Brazil: A review on low cost fingerprint techniques on-the-go, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.003