Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 35 (2014) 832 – 841

Procedia Computer Science

18th International Conference on Knowledge Based and Intelligent Information & Engineering Systems - KES2014

Biometric identification on android smartphones

Shah Faisal Darwaish[a]*, Esmiralda Moradian[a],Tirdad Rahmani[b], Martin Knauer[b]

[a] *Department of Computer and Systems Sciences, Stockholm University, Forum 100, SE-164 40 Kista, Sweden*
[b] *SAP AG, Vincenz-Priessnitz-Strasse 1, 76131 Karlsruhe, Germany*

Abstract

Smart devices are gaining popularity and are becoming key platform for accessing business and personal information. Access to this sensitive information also requires proper authentication and identification. This paper describes a solution proposed for farmers' biometric identification in African Cashew Initiative. African cashew initiative is a project which focuses on organizing and supporting cashew producers in five African project countries. The paper presents an implementation of biometric identification in large datasets and provides results regarding the performance and accuracy of the proposed system. This work is a first approach towards offline biometric identification on smartphones providing preliminary results for deployment on large scale.

Keywords: Biometric Identification; Face Recognition; Android smartphones; LBP; OpenCV

1. Introduction

Mobile computing is rapidly gaining popularity and mobile devices are becoming the key platform for accessing business and personal information. Access to such information requires identification and authentication for secure transaction[1]. With the advancement of hardware and software resources in smartphones and with high usage of these devices for different business transactions, biometric identification is becoming a common solution for identification and authentication purposes[1]. The Identification can be done in different forms. It may be in the form of

* Corresponding author. Tel.: +(00)46 723 29 16 51.
E-mail address: shda3340@student.su.se.

doi:10.1016/j.procs.2014.08.250

authentication or recognition. Authentication involves verifying a claimed identity while recognition involves resolving identity of a person from database [3].

Anil K. Jain and Arun Ross[4] defined biometrics as "the science of establishing the identity of an individual based on the physical, chemical or behavioral attributes of the person". Among the different biometrics, iris texture pattern and finger prints are considered as some of the unique feature of every person[5], and identification/authentications systems based on these biometrics are used widely in different applications. Iris is the circular region between pupil and sclera of the eye[5]. However, considering smartphones, finger prints recognition is not very popular as it requires an external hardware for scanning the finger prints. The external attachment is also considered as a problem towards the adoption of finger prints on mobile/smartphones. Iris based recognition system also requires a very good quality image of an iris, which considering the smartphones camera capability could be a limitation.

Despite different research efforts that have been put on biometric identification in smartphones, its performance in large datasets still require exploration.

This research addresses few challenges: 1) In Africa, most of the countries have slow data network. So, the biometric data couldn't be processed online and it needs to be processed and stored on the device; 2)The project has thousands of producers and the performance of biometric identification may degrade in large datasets due to limited processing power and storage capacities of smartphones. Besides, the smartphones has limited possibilities in terms of user interaction for different biometric techniques.

Within SAP's African Cashew initiative, Smart devices are used for different transactions between the producers (farmers) and the co-operative. Currently, transaction between the producers and the co-operative take places on-field in different locations. For successful transaction, the producers need to be identified correctly. Presently, the producers are identified by matching their barcodes. Each producer has given a unique barcode. These barcodes are printed on the paper. In a normal transaction, the producers are identified by asking for the barcode. The barcode is then matched to producer's barcode in the name list and his name is verified. This process takes much time as in many cases, farmers misplaced or lost their identification paper which carries their barcode, which make it even more time consuming to search for a farmer in a list of thousands farmers. Besides, the paper printing for thousands of farmers also costs too much.

The research provides a solution that enables and handles biometric identification of the producers on smart devices offline in large datasets. Thus, the provided solution saves time and cost.

2. Related work

Biometric Identification on mobile/smartphones is one of the active research areas in secure and intelligent Information systems. Different research studies have been done on the available different biometric techniques for mobile/smartphones. These techniques include, finger prints recognition, face recognition, hand geometry, iris recognition, voice recognition, signature and keystrokes recognition etc.

M. Gargi et al.[6] proposed a method to provide security for android smartphones using iris biometric feature. The study provides promising results on an android device with 1 GHz processor and 4GB of internal memory, and with total time of 80 to 90 seconds to authenticate a single mobile user from database of 75 people containing 5 iris images of each person.

Santo Sierra et al.[7] proposed a biometric system based on hand geometry, which is oriented to mobile devices. Authors state that the system is able to provide accurate results on individual identification. The research of de Santo Sierra et al.[7] shows the implementation of hand biometrics on a PC with 2.4 GHz and android mobile platform with 1 GHz processor and 576 Mb of RAM. The result of the research showed good performance with FAR= 0.089% and FRR=5.89%. The mobile implementation took less than 3 seconds to provide identification from a database of 120 different individuals. One of the limitations of the hand geometry is that the hand geometry is not very unique and it cannot be used for identification within large population[4].

Guillaume Dave et al.[8] investigated performance of different algorithms of face recognition on smart phones. Authors[8] analyse performance of the algorithms applying those on an android phone with 600 MHz processor and 256 Mb RAM. The tests were performed with 134 face images of 10 different persons. The results indicate that it achieved 94% recognition rate with fisher-face algorithms and took no more than 1.6 seconds.

Vazquez-Fernandez et al[9] present a smart photo sharing application for mobile devices based on face recognition engine. The system is implemented on android platform and tested on two different manufacturer smartphones, HTC Desire with 1 GHz processor and 576 MB RAM and Samsung Galaxy Tab with 1 GHz processor and 512 MB RAM. The tests were performed for 50 contacts with 4 faces per contact. The results showed that the application took 0.35 sec on HTC Desire and 0.47sec on Samsung Galaxy tab to recognize face.

These studies provide implementation of different biometric identification techniques on smartphones but do not indicate their performance in large datasets.

3. Biometric system

Traditionally biometric identification tasks are considered for two purposes, such as identification and verification[2, 5, 9]. In identification systems, the identity of a person is determined from a database of known records. The person makes no claim to identity and the biometric is searched in the whole database of templates which requires one-to-many comparisons[9]. In verification systems, the person's biometric sample is matched only with a claimed identity-stored template [2]. It only requires a one-to-one comparison.

A typical biometric identification system operates into two phases, i.e. the enrollment phase and the identification phase[10]. During the enrollment phase, a digital representation of biometric is acquired by scanning the biometric characteristics by a special biometric scanner[2]. The digital representation is further processed to get an expressive representation called template. During the identification phase, the same process is repeated to generate a template and then it is compared against the templates in the database by the matcher to establish an identity. An ideal biometrics should have characteristics of universality, uniqueness, permanence, collectability and acceptability[2, 4, 5]. These characteristics are explained by[4, 10, 5] as; 1) Universality: All people should possess the biometric trait. 2) Uniqueness: The biometric trait should not be the same across individuals. 3) Permanence: The biometric trait should not change over a period of time. 4) Collectability: The trait should be possible to acquire and digitize using suitable devices. 5) Acceptability: The biometric should be acceptable to the users of authentication/identification system, as an authentication/identification method.

A generic biometric system contains four modules, such as sensors, quality assessment and feature extraction module, matching and decision making module and database module [10].

4. African cashew initiative

African Cashew Initiative (ACI) is a project that focuses on organizing and supporting cashew producers in five African project countries, namely Mozambique, Ghana, Burkina Faso, Côte d'Ivoire and Benin. The project aims to facilitate the linkages between the producers (farmers) and the processors to grow their business and to support them with IT in order to enable traceability and transparency within the business processes.

Value Chain is promoted in the project to generate greater added value in local markets and to improve the competitiveness in international markets. There are different stakeholders involved in the value chain consisting of input suppliers, cashew producers, processors, distributor, exporter and consumers.

In ACI project, during a buying transaction, there is a change of ownership between the farmers and the cooperative. The producers and staff member needs to be identified correctly in order to have a legally valid transaction. The identification of producers needs to be done on smart devices through biometrics. However, the following challenges need to be considered: 1) Biometric identification availability despite only occasionally connected devices because of no network in some places; 2) Handling Identification in huge data sets as there are thousands of farmers associated with this project. The proposed system is presented in chapters 5 and 6. Conclusions are presented in chapter 7.

5. Biometric identification on android smartphones

5.1. System requirements

The transactions between the producers and the co-operative or processors take places on-field in different locations. For successful transaction, the producers have to be identified correctly. Following high level requirements were identified from the case study:

- Biometric identification should be available offline because of no network in some places.
- Identification shall be possible to perform in huge data sets as there are thousands of farmers associated with this project.

The requirements were further refined and resulted in following categories: System and Data requirements, Biometric Technique requirements, and Usability requirements. These requirements are presented in Table 1.

Table 1.Requirements

System and Data requirements
1. The biometric data must be stored on the smartphone device.
2. The biometric data shall be stored in such a way that it can be synchronized when the data network is available.
3. The application shall be deployable on Android version 2.2 or higher.
4. The system shall allow storing multiple biometric data templates for each farmer.
5. The application shall be developed in such a way that it can be integrated with the existing application and the existing application can be installed without it.
Biometric Technique requirements
1. The end users of the project are farmers which do labor job, so in such case, For instance, the hand biometric data may not be sufficient. So, the biometric technique should consider the availability of the biometric data.
2. The biometric technique can be deployed on the smartphone without any extra hardware. Besides, the biometric data should be easily acquirable/ attainable
Usability requirements
1. The application should present the captured image to the user before it can be forwarded to the recognition/identification phase.
2. The identification process should present a list of top three results from the matches found.
3. The identification process shall first do the matching, if the match is not found it shall then show a list of existing producers, to allow the user to associate the captured biometric with producer and save it in database.

5.2. Motivation to adapt face recognition

The previous studies on biometric identification shows that the most of the biometrics like voice recognition, signature and keystroke are indistinct and they vary with different physical and behavioral conditions. Iris recognition is one of the very unique and distinctive features of human [5], but the iris biometric requires a high quality of image and highly controlled condition for capturing the iris, which considering the camera available with most smartphone, is not quite feasible. Finger prints is also the most widely used technique but it require extra hardware for scanning it. In this research, the different transactions are done on the field, and the biometric identification would also be done on the field. So, for an extra external hardware, extra power would also be needed. Besides, the project has farmers, which do labor job. They usually have bruises and damage fingers, which could be time consuming considering the collectability of biometric data, and the insufficient biometric data can also affect the performance of biometric identification. Hand recognition is also considered indistinctive and can be time consuming considering acquiring of the full hand image. Face Recognition on the other hand showed quite promising results considering the performance of biometric identification and computational requirements.

Regarding the collectability of biometric data, Face biometric can be easily acquired by embedded camera on smartphones.

5.3. System design

This phase was started by making the outline design of the biometric system. The biometric technique selected for identification is Face Recognition. The motivation to adopt face recognition is described in section 5.2. Face Identification/Recognition can be done easily on smartphone by scanning the face through the embedded camera. The standard biometric system has two main phases i.e. Enrollment and Identification/Authentication. So, each step of two phases was outlined with respect to Face recognition. The design of the system is shown in Figure 1.

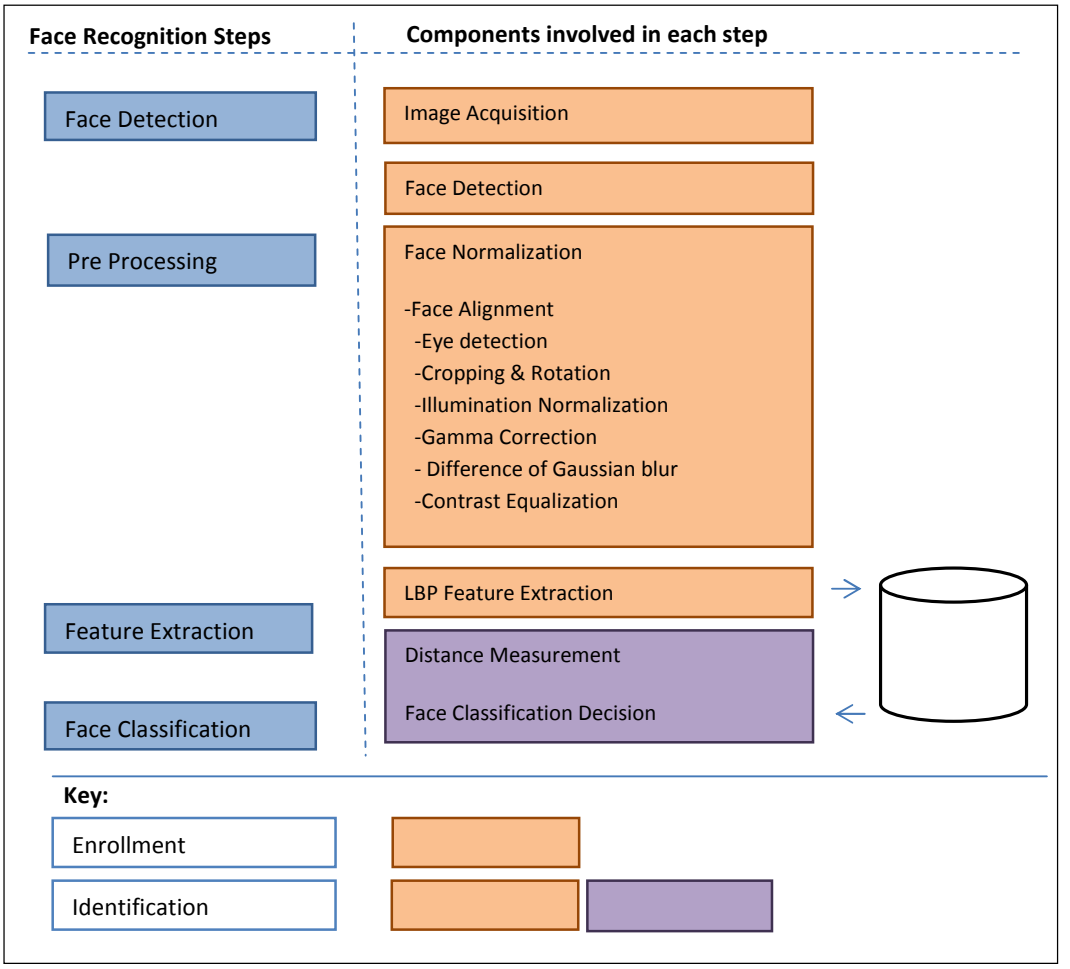

Fig. 1. System components

The available software libraries and tools for face recognition were then analysed with respect to the components, system and biometric technique related requirements defined in the previous section. The common software library available for image processing is OpenCV. The library was analysed for the face recognition technique and for android implementation. The OpenCV is still not completely migrated to android platform and some of the functions are not available in the android version. To complement that, the researcher used JavaCV. JavaCV is a java wrapper

to the OpenCV. JavaCV is licensed under the GNU General Public License version 2 (GPLv2) with Class path exception[11].

5.4. System development

The development of the system is explained according to the four components as given in the outline design in Figure 1.

5.4.1. Face detection

For face detection, OpenCV LBP face detector was utilized. OpenCV has two different methods for face detection. Viola & Jones [12] Haar based and LBP based face detector [13]. LBP has adopted for fast face detection because tests showed that LBP detector has a lower computational cost [9]. The Haar based face detector performs about 20 stages of comparison to decide a face or a non-face object [14] and differentiate the face from non-face object on the idea that the eye region should be darker from the forehead and the cheeks and the mouth should be a bit darker from the cheeks. The LBP on other hand uses pixel intensity comparison such as edges, flat region and corners in an image[14]. The LBP face detector requires an image in gray color so the image is converted into grayscale before face detection.

5.4.2. Pre processing

For improved recognition rates, the face image needs normalization. The face normalization consist of several steps consisting of face alignment, background removal and illumination normalization. The face alignment is done using the eye positions in the face. Eyes are detected using the trained Haar cascade classifier for eye detection available in OpenCV. There are exist various Haar eyes' detectors available in openCV[14]. This research uses the open eye detectors. The open eye detectors in OpenCV are given below:

a) haarcascade_mcs_lefteye.xml (and haarcascade_mcs_righteye.xml);

b). haarcascade_lefteye_2splits.xml (and haarcascade_righteye_2splits.xml).

According to Baggio D.L et.al [14], the first category in the above list i.e. haarcascade_mcs_lefteye.xml (and haarcascade_ mcs_righteye.xml) is more reliable as compared to the other one. The performance of eye detector is also evaluated on image datasets of 1081 images. From the analysis of results, haarcascade_mcs_righteye.xml performed better as compared to the others. So, haarcascade_mcs_righteye.xml was used for eye detection. The face is then aligned by first aligning the eyes in a horizontal line and then rotating the image. The image is rotated based on the angle defined by calculating the difference of the eyes x-axis and y-axis position and converting them into polar co-ordinates. An example of aligning the face and background removal is presented in Figure 2.

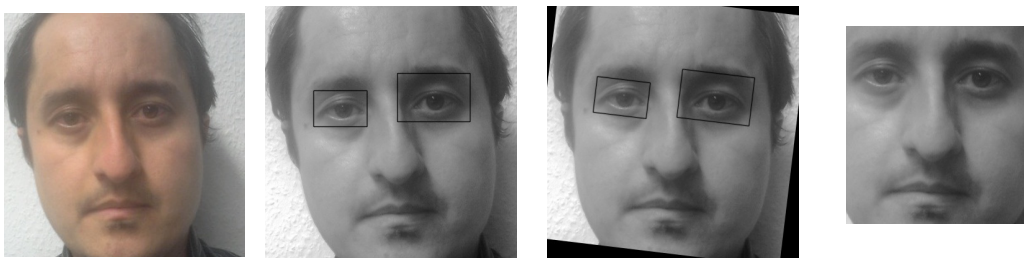

Fig 2. Face Normalization

After the face is aligned, the extra background is removed by setting width offset and height offset (in percentage) with respect to the detected eye's outer most x-axis position and total height of the face respectively. For illumination normalization, the three step function is used as suggested by Tan & Triggs[15]. The three steps

involve Gamma Correction, Difference of Gaussian blur and Contrast Equalization. Gamma Correction enhances dynamic region of the image in dark or shadowed region and compress them in bright region[15]. The Gaussian filters remove the noise and contrast equalization rescales the image intensities to overall contrast variation. The final image after applying these functions is demonstrated in Figure 3.

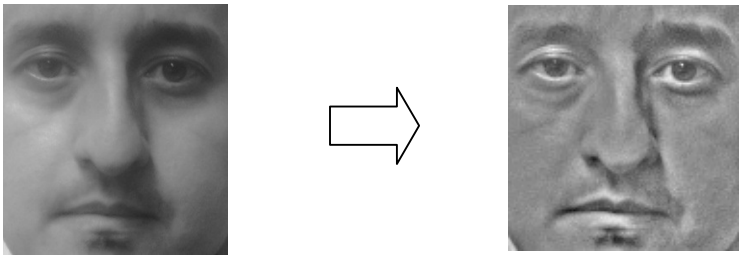

Fig. 3. Final Face Image

5.4.3. Feature extraction

The LBP features are extracted using Extended LBP or Circular LBP implementation available in OpenCV. The radius for circular region is set as 1 and the neighbor size to 8 sample points. The higher the radius and neighbor's size, the higher the computational cost. The numbers of cells in the horizontal and vertical direction are also retained to default value of 8 to keep the size of histogram lower. The LBP Histogram is created from the normalized face image. The LBP Histogram matrix is converted into Binary Large Object (BLOB) data type to store it into the database for face classification, which also complies with the requirement of saving the biometric data into a data type that can easily be stored in the database for synchronization.

5.4.4 Face classification/recognition

Face recognition is comparing the distance between the test face image and the trained images in the databases. The image with smaller distance from the database is presented to the user that can either accept the results or save the new image into database. Face recognition systems are semi-automatic and the users are accepted or rejected by the system manually. The distance is measured using the X^2 measure called Chi-square distance, as it is the most optimal distance measure for LBP histograms. The measured distances are then sorted in ascending order to get top three matches. The top three matches are then presented to the user.

5.5. System evaluation

To evaluate the system, experiments were carried out. Experiments give possibility to measure the performance and accuracy of biometric identification. The performance is measured in terms of response time of the face identification. For finding the accuracy, a performance measure of biometric system, called Matching error is used. The database for testing the accuracy rate of recognition is built from different face image databases used for face recognition. The databases were filtered for only frontal face images and a single image from each class/subject is collected. The system is aimed to perform biometric identification in large datasets, so the database of 1000 subjects/classes, containing different ethnic group is built from the following databases: 1) FEI face database[16]; 2) CIE Biometric[17]; 3) Indian Faces[18]; 4) Visual Cognition Laboratory[19]; 5) Faces 94 , faces 95, and faces 96 by Dr. Libor Spacek[20]; 6) CASIA Face Image Database[21]; 7) African Cashew Initiative.

As the stored biometric image and the test sample may have varied lightning, so an image with artificial variation in illumination is created as a second image of the same subject. The match is considered a true match, if a first image matches with the second image (with varied lightning) of the same class/subject.

To evaluate the accuracy and performance, different test cases have been developed to provide results on different scales of the biometric data. The training or creating the biometric representation of the face database images were done on the computer with 3.4 GHz core i-7 processor and 16GB of RAM.

6. Results and analysis

As discussed previously, the accuracy is measured in terms of matching errors. Matching errors are defined to avoid ambiguity with systems having multiple templates. The matching error has two types, i.e. False match rate (FMR) also referred as false positive, and false non-match rate (FNMR). False Match Rate (FMR) is the probability that a biometric sample is falsely declared to match a single non-self-template. Non-self means genetically different. False Non-Match Rate (FNMR) is the probability that sample is falsely declared not to match a template to the same user's sample[22]. For matching, the test image is compared with each trained image and the similarity distance is calculated. These distances are then sorted and a minimum distance is considered as a match. To evaluate the performance with different scales of trained images, a test case has been created in which three training sets are prepared. Three different tests were carried out to find the matching error rate for first match and top three matches. The number of trained images and test images in each test is mentioned below in the table 2.

Table 2. Test case: Find matching error rate for first match and top three matches

Test No.	Test Set (classes/subjects)	Training Set (classes/subjects)
1	250	500
2	250	750
3	250	1000

The results of the test case are described below in table 3 in terms of FMR and FNMR.

Table 3. Results of matching Error rate – Test case

Test	First Match		Top Three Matches	
No.	FMR	FNMR	FMR	FNMR
1	12,2%	0%	9,6%	0%
2	12,4%	0%	9,6%	0%
3	12,6%	0%	9,6%	0%

The results for first match indicate that, the FMR increases 0.2% each time the trained dataset size is increased by a factor of test set size, while for the top three results, it remained the same for all the tests.

For testing the performance of a system, the database of trained face images is migrated to the mobile and tests were carried out on Google LG Nexus 4 with 2GB RAM and 1.5Ghz Quad core Processor. The results of the tests are described below in table 4.

Table 4. Response time of Matching in milliseconds

Test No.	Test Set (trained Images)	Time in milliseconds
1	1000	1032990
2	500	527542

The above tests describe performance of a single test image being searched in different trained datasets. The single image is selected randomly. The results shows that it took about 1032.9 seconds to find a single face in 1000 images and 527 seconds in 500 images. The results showed quite poor performance for practical deployment. To

improve the performance, the performance of each component involved in searching was analyzed. The performance analysis of each component is given below in table 5.

Table 5.Time taken by each component of recognition

No.	Component	Time in milliseconds
1	Each Biometric template retrieval from database	12 to 17
2	Each Biometric template conversion into OpenCV matrix	600 to 1000
3	Each Biometric template Comparison	0 to 1

As it is obvious from the table, the histogram conversion into OpenCV Matrix takes the highest time. So, this component is analyzed and alternative solutions were tested. The biometric template data is serialized into binary large object data format and the performance was tested, by this conversion, the total time for biometric template conversion into OpenCV matrix is reduced to 14 to 18 milliseconds, which is almost 33 times better than the first implementation. After optimization, tests were carried out to compute time for a single test sample being searched on different scales of trained images. The results are given in table 6.

Table 6. Response time of Matching in milliseconds

Test No.	Test Set (trained Images)	Time in milliseconds
1	1000	97752
2	500	29632

The result shows improved performance for biometric matching. The match is found in less than 30 seconds being searched in 500 biometric templates, which is quite practical.

6.1. Analysis

The system was evaluated with respect to the identified requirements, such as System and Data requirements, Biometric Technique requirements, and Usability requirements.

- System and Data requirements. The system proved to comply with all the data and network related requirement. The tests provide a demonstration of storing the biometric data on smartphone. The biometric data is converted into a data type, which can be stored into the database and can be synchronized. It was also observed that the system is able to store multiple biometric templates for a single producer. The system has been tested on Android 2.2 smartphone and it worked smoothly. The system can be integrated with the existing application and the existing application can be installed without it.
- Biometric Technique requirements. The biometric technique of face recognition is used for identification of producers. The face image can be easily acquired through embedded camera in smartphone. It doesn't require any external device to capture the biometric data.
- Usability requirements. The demonstration of the system provided an evaluation of usability requirements. The developed application is able to show the captured face image to the user before it is forwarded to matching. The system first searches the image in the database and provides the closest top three matches. If the input producers is not in the match list, the user has the option to store the captured biometric and continue the transaction. The system is able to find a match with accuracy rate of 87% and response time of less than 30 seconds over 500 biometric templates/ face images. Currently, the African Cashew Initiative project has several thousand producers, but the application can be deployed in the field for scenarios with 500 or less producers.

7. Conclusion and future work

This paper proposes a solution for biometric identification on smartphones offline in large datasets. The system for biometric identification of farmers in agriculture value chain is developed. The system is able to perform the

whole biometric identification process offline on smartphone and identify the input image with the probability of over 87% in large datasets. The response time for a single biometric identification is under 30 seconds for searching a test sample in 500 biometric templates, which considering the dataset size, is quite optimal and can be deployed in the field.

The performance of the system can be improved in the future by the advancement of hardware and the underlying software. The response time can be improved by partitioning the database and search each partition until the match is found. Other face recognition algorithms than LBP can be utilized for smart phone and can be compared to the results of LBP for large datasets.

Acknowledgements

This research has been carried out with support of SAP AG. SAP AG is one of the contributing partners in the African Cashew Initiative project, co-funded by Bill & Melinda Gates Foundation, the German Federal Ministry for Economic Development and Cooperation and private sector organizations.

References

1. Trewin S, C. Swart, L. Koved, J. Martino, K. Singh,S. Ben-David. “Biometric Authentication on a Mobile Device: A Study of User Effort, Error and Task Disruption”, Proceedings of the 28th Annual Computer Security Applications Conference, 2012, pp. 159-168.
2. Mrs. Kasturika B. Ray, Mrs. RachitaMisra. “Textural Features of Palm Print”, International Journal of Computer Science and Telecommunications, Vol 3, no. 4, pp. 78-81, Apr 2012.
3. Anil Jain, Lin Hong, SharathPankanti. “Biometric Identification”, Communications of the ACM, Vol 43, no. 2, pp. 90-98, Feb 2000.
4. Anil K. Jain and Arun Ross. Handbook of Biometrics.(2008). e-ISBN-13: 978-0-387-71041-9, 2008.
5. Tikkanen P, S. Puolitaival and I. Känsälä. “Capabilities of Biometric Identification in wireless devices”, Published by Springer Berlin Heidelberg, vol 2688, pp 796-804, 2003.
6. Gargi M, J. Jasmin Sylvia Rani, Madhu Ramiah, N. T. Naresh Babu, A. Annis Fathima and V. Vaidehi. “Mobile Authentication Using Iris Biometrics”. Published by Springer Berlin Heidelberg, Networked Digital Technologies, Vol. 294. pp 332-341, 2012.
7. De Santos Sierra. A, C. Sanchez Avila, A. MendazaOrmaza, J. Guerra Casanova. Towards Hand Biometrics in Mobile devices. In Proceeding of BIOSIG, Darmstadt, ISBN: 978-3-88579-285-7, 2011.
8. Dave G, Chao, X., & Sriadibhatla, K. “Face Recognition in Mobile Phones”. Department of Electrical Engineering Stanford University, USA, 2010.
9. Vazquez-Fernandez, Esteban, et al. "Built-in face recognition for smart photo sharing in mobile devices." Multimedia and Expo (ICME), 2011 IEEE International Conference on. IEEE.
10. Kizza J.M. Ethical and Social Issues in the Information Age. 4th Ed.Springer Verlag London Limited 2010, ISBN: 978-1-84996-037-3
11. JavaCV (n.d). https://code.google.com/p/javacv/
12. Paul V and Michael J. Jones. "Robust real-time face detection." *International journal of computer vision* 57, no. 2 (2004): 137-154.
13. Marqúes I. Face Recognition Algorithm. Master Thesis.http://www.ehu.es/ccwintco/uploads/e/eb/PFC-IonMarques.pdf.
14. Baggio. D. L, S. Emami, D. M. Escrivá, K. Ievgen, N. Mahmood, J. Saragih, R. Shilkrot. *Mastering OpenCV with Practical Computer Vision Projects*. Packt Publishing Ltd.Livery Place 35 Livery Street, Birmingham B3 2PB, UK. ISBN 978-1-84951-782-9, 2012.
15. Tan, Xiaoyang, and Bill Triggs. "Enhanced local texture feature sets for face recognition under difficult lighting conditions." *Image Processing, IEEE Transactions on* 19, no. 6 (2010): 1635-1650.
16. FEI Face Database (n.d). http://fei.edu.br/~cet/facedatabase.html
17. CIE Biometrics (n.d). https://biometrics.cie.put.poznan.pl/index.php?option=com_content&view=article&id=3&Itemid=15&lang=en
18. Indian Face Database (n.d). http://vis-www.cs.umass.edu/~vidit/IndianFaceDatabase/
19. Visual Cognition Laboratory (n.d). http://viscog.hku.hk/facedb.htm
20. Dr Libor Spacek, (2008, Jun 20), Computer Vision Science Research Projects (n.d). http://cswww.essex.ac.uk/mv/otherprojects.html
21. CASIA Face Image Database Version 5.0, Biometric Ideal Test. http://www.idealtest.org/findDownloadDbByMode.do?mode=Face
22. Mansfield A.J and J.L Wayman (2002). *Best Practices in Testing and Reporting Performance of Biometric Devices*.© Crown Copyright 2002. ISSN 1471-0005, NPL Report CMSC 14/02