ISSN : 2454-9150 Vol-01, Issue 06, Sep 2015.

Smart Authentication System for android Smartphones

Rohit P. Narkhede[1], Prednesh N. Chaudhari[2], Dhananjay P. Ubale[3], Khushal J. Gosavi[4]
BE Student, Computer Department, Late G. N. Sakpal College of Engineering, Savitribai Phule-Pune University, Maharashtra, India[1,2,3,4]
rohitn3993@gmail.com[1], chaudharipradnesh@gmail.com[2], ubaledhanu@gmail.com[3], khushalgosavi9@gmail.com[4]

***Abstract* — Smart devices are very much popular in now a days and are becoming main platform for gain access for business and personal information or data. Personal data and business information are very sensitive information so it needs to protect from the unauthorized person. The implementation of biometric identification in large databases provides the outcomes regarding to correctness of the proposed system. In previous system passcode and voice recognition system is used to authentication and these systems are somewhat less secure. In this paper we are provide face recognition and detection for android mobile and android smartphones. We match the person face into the mobile database that is store the some Face template of the person/user. If the user face is not same or not match with original face template then user get email or location of the unauthorized user. In the mail we get the unauthorized user face snapshot or his GPS location. Also we provide the two service. In 1st service we can delete the mobile private information from the mobile. And 2nd service mobile tracker system. In mobile tracker system we can track the mobile phone i.e. if we loss our smartphones then we can track the last location of the mobile on google map and this location we are seen through website.**

***Keywords*— Biometric Identification; Android smartphones; LBP; OpenCV; Face Recognition.**

I. INTRODUCTION

Now a days smartphones are very popular and many of the smart phones uses a android operating system to manage or handle the user interface and hardware. The smart phones are main platform for storing personal data and also store the business data. For access the personal data and business data user need some authentication for security in transaction. Smart phones are rapidly use for business transaction so the biometrics identification is well known option for authentication process. There are many form of authentication such as recognition or authentication. In recognition resolving identity of user in dataset and authentication includes claimed identity.

"A recognize the user who use the system in different features automatically" is known as biometrics. Biometrics consist of any robust, measurable and distinctive personal traits to identify right person who handle or use the system. Biometric technology includes iris scan, retinal scan, voice or speaker, fingerprint, face recognition and signature verification etc. Voice recognition and Fingerprint recognition is also use for security purpose voice recognition system is based on voice that means its match the user voice with system database and In Fingerprint recognition system also match with the person fingerprint image or template and then provide access to the system.
Biometric has many technology i.e. iris scan, retinal scan voice or speaker face recognition and signature verification. Iris recognize and finger print are mostly used in many authentication system. Face recognition is other technology introduced by biometrics for authentication system in smartphones. Face recognition is older concept and it is implemented in many products in different way which is work with high performance and quality. But sill it having many challenges to farther improve the face detection of system in mobiles.

There are three steps involved in the Biometric verification of a person. In the first step, system are take the face images or template and stored in the database system. In the second step, some template are matched with database system. Third step, if template is match with database then system allow for access the system or android device and if template is not match with database then system is not allow for access the device. Here we provide authentication or more powerful security to smartphone system.

In this paper we are provide face recognition and detection for android mobile and android smartphones. We match the person face into the mobile database that is store the some Face template of the person/user. If the user face is not same or not match with original face template then user get email or location of the- unauthorized user. In the mail we get the unauthorized user face snapshot or his GPS location. Also we provide the two service. In 1st service we can delete the mobile private information from the mobile. And 2nd service mobile tracker system. In mobile tracker system we can

track the mobile phone i.e. if we loss our smartphones then we can track the last location of the mobile on Google map and this location we are seen through website.

II. RELATED WORK

Biometric identification on smartphone is ongoing research topics for securing the smartphone information and data. There are distinctive experiment are performed on currently available researches on biometric identification on smart phones. Biometric identification technology consist of iris scan, voice or speaker, retinal scan, fingerprint, signature verification and face recognition etc. Previous system introduced a method to provide security and authentication to android smartphones by using iris or eye detection biometric. The research consist of promising results on an android smartphone devices with 1 GHz processor and 4GB of internal memory of the device, and with total time of 80 to 90 sec. to authenticate a single mobile user or person from database of 70 people containing 5 iris images of each user.[1]

Biometric system is also based on hand geometry, which is depend on mobile devices. Previous system is able to provide correct results on individual identification. The research of shows the implementation of hand biometrics on a computer with 2.4 GHz and android mobile phone platform with 1 GHz processor and 576 Mb of RAM. The result of the research show good performance with FAR= 0.089% and FRR=5.89%. The mobile implementation took less than 3 sec. to provide identification from a database of 120 different pattern. Another limitation of the hand geometry is that the hand geometry is not very different and it cannot be used for identification within large population. Furthermore, commercial biometric identification systems normally have no constraints of computational cost or involved hardware but they do aim the highest correctness in personal identification. In other word we applying biometrics identification to android smartphones devices requires a reconsideration of previous constraints since a mobile device is at present far from being comparable to current available biometric systems in terms of hardware[2].

Investigated performance of different algorithms of face detection on android smartphones. The performance of the algorithms applying those on an android smartphone with 600 MHz processor and 256 Mb RAM. The test were perform with 134 face images of 10 various persons. The results indicate that it achieved 94% recognition rate with fisher-face algorithm and took no more than 1.6 sec[3].

A previous system smart image sharing application for android mobile devices based on face recognition system. The system is developed on android smartphone platform and tested on two different manufacturer smartphones 1st is HTC Desire model with 1 GHz processor and 512 MB RAM and 2nd is Samsung Galaxy Tab model with 1 GHz processor and 512 MB RAM. The tests were used for 50 contacts with 4 person face images per contact. The results show that the application took 0.35 sec on HTC Desire and 0.47 second on Samsung Galaxy tab to detect face. These research provide implementation of different biometric identification techniques on android smartphones but do not indicate their performance in large database[4].

III. ARCHITECTURE OF SYSTEM

This section was started by making the outline design or architecture of the biometric authentication system. The biometric identification technique used for identification is Face Recognition. Face Identification or Recognition can be done easily on android smartphones by scanning the face through the embedded camera. The architecture of the system is shown in Figure 1.

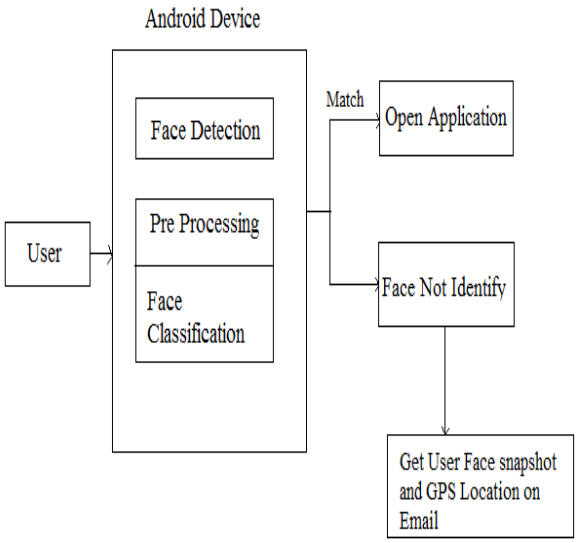

Figure 1: Architecture of smart authentication system for android smartphones.

3.1 System development

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

A) Face Detection

Face detection technic OpenCV LBP face detector was utilized. OpenCV has two different methods for face

detection. Haar and LBP based face detector in the system[5]. LBP has adopted for fast face detection because tests showed that LBP detector has a lowest computational cost[9]. The Haar based face detector implement about 20 stages of comparison to decide a face or a non-face object[6] and find out the face from non-face object on 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 otherside hand uses pixel intensity comparison as like edges, flat region and corners in an face image[6]. The LBP face detector requires an image template in gray color so the image is converted into gray scale before face detection.

B) Pre processing

Improve the recognition rates, the face images needs normalization. The face image normalization consist of some steps consisting of 1st is the face alignment,2nd is background removal and 3rd is illumination normalization. The face alignment is done using the eye positions in the face image. Eyes are detected using the Haar cascade classifier for eye detection use in OpenCV or we also use another libraries for detection. There are exist various Haar eyes detectors available in OpenCV[6]. In this paper research uses the open eye detector. The open eye detector in OpenCV are show below :

a) haarcascade_mcs_lefteye.xml (and haarcascade_mcs_righteye.xml);
b) haarcascade_lefteye_2splits.xml (and haarcascade_righteye_2splits.xml).

As per the *Baggio D.L et.al* [6], the 1st detector in the above list i.e. haarcascade_mcs_lefteye.xml (and haarcascade_ mcs_righteye.xml) is more reliable or useful as compared to the 2nd . The detection performance of eye detector is also evaluate on image datasets of 1081 images from database. The analysis of results, haarcascade_mcs_righteye.xml performed good as compared to the others detectors.So, haarcascade_mcs_righteye.xml was used for eye detection in images. The face is then aligned by 1st aligning the eyes in a horizontal line of face and then rotating the image. The face image is rotate based on angle defined by calculating the difference of the eyes x-axis and y-axis position in face image and converting them into polar co-ordinate. Below show the example of aligning the face and background removal is show in Figure 2.

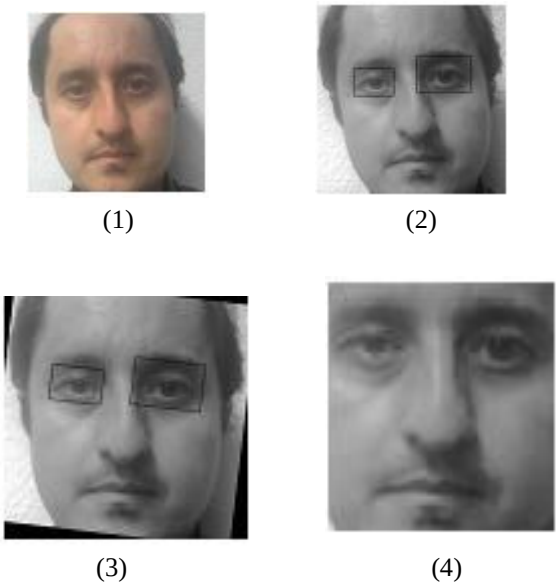

Figure. 2: Face normalization.

After the face image is aligned, then extra background of image is removed by setting width offset and height offset in percentage with respect to the detected eye's outer mostside x-axis position and total height of the face respectively. For that the illumination normalization, the three step function is used[8]. The three steps include 1st is Gamma Correction, 2nd is Difference of Gaussian blur and 3rd is Contrast Equalization. Gamma Correction uses dynamic region of the face image in dark or shadowed region and compress them into bright region[8]. The Gaussian filters is used to remove the noise and contrast equalization rescales the image intensities to overall contrast variation. The final face image after applying these functions is show in below Figure 3.

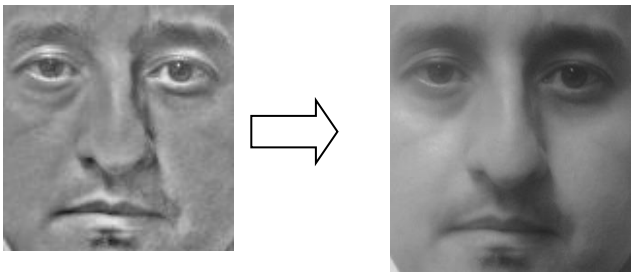

Figure 3: Final Face Image.

C) Face Classification

Face classification and recognition is comparing the distance between the test face image and the original images in the databases. The image with small distance from the database is show to the user that can either

correct the results or save the new image into database. Face image recognition systems are semi-automatic and the users are accepted or rejected by the face detection system automatically. The distance is measure by using the X^2 measure known Chi-square distance, as it is also the most optimal distance measure for LBP histograms. After the matching or checking the face image its provide the access to the user for access the android application.

As above classification system should be able to access the application and if the classification phase is fail in this case user are not allowed for access or open the android application. That time system is capture the unauthorized user face image or take snapshots and it stored in system database and also find out the unauthorized user location this both things i.e. snapshots of image and location of the user is send to the authorized user through mail.

IV. CONCLUSION

This paper proposes a solution for biometric identification for android smartphones online or offline in large datasets. The system for biometric identification is more secure for user and this system unauthenticated or any user cannot open or use our android smartphones application. This system is able to perform the whole biometric identification process offline on smartphone and identify the input face image with the probability of over 85% in large datasets. This system provide more powerful security to the android smartphones and track the smartphones on Google map.

ACKNOWLEDGMENT

The authors are thankful to Prof. N. K. Zalte, Faculty of Computer Engineering, Late G. N. Sapkal College of Engineering, Nashik, for providing the necessary facilities for this research paper preparation.

REFERENCES

[1] 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.

[2] 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.

[3] Dave G, Chao, X., & Sriadibhatla, K. "Face Recognition in Mobile Phones". Department of Electrical Engineering Stanford University, USA, 2010.

[4] 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.

[5] Marqúes I. Face Recognition Algorithm. Master Thesis.http://www.ehu.es/ccwintco/uploads/e/eb/PFC-IonMarques.pdf.

[6] 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.

[7] Dr Libor Spacek, (2008, Jun 20), Computer Vision Science Research Projects (n.d). http://cswww.essex.ac.uk/mv/otherprojects.html

[8] 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.

