A Vary Approach to Face Recognition Veritable Mechanisms for Android Mobile against Spoofing

V.Ravibabu
PG Scholar, Centre for Information Technology and Engineering
Manonmaniam Sundaranar University
Tirunelveli, India
v_ravibabu@yahoo.com

Dr.N.Krishnan
Professor, Centre for Information Technology and Engineering
Manonmaniam Sundaranar University
Tirunelveli, India
krishnan@computer.org

***Abstract*—Authentication is the process of identifying and verifying someone, who it claims to be known as user. The increasing popularity of smart mobile phones provides user to store personal data and user information. It is necessary to ensure the confidential access of the mobile phone to its user. Currently, Face Unlock is the biometric user authenticating system widely available in mobile phone. However, user's face image for authentication could not be considered as a secure. Since we faced the problem of 2D face spoofing attacks by displaying user photo in front of the camera. In this paper, we analyze on current methods of face recognition for authentication on mobile phone and present a novel approach for Face Recognition system to be more secure and convenient use. We perform by acquiring with various angular of face information from user and analyze the liveness detection of user by comparing with biometric template of data acquired in a database. The results to the user face recognition are promising in liveness detection and reliable against spoofing.**

Keywords—face recognition; android mobile; user authentication; spoof attack; liveness detection; opencv; javacv;

I. Introduction

Authentication is a vital security measure for mobile device protection. Unlocking a mobile phone is to authenticate the user with unique identity such as PIN, Password, and Pattern to access mobile device. The current mechanisms towards unlocking mobile are quite reliable but much less secure and threat to use in real world. The Face Unlock is a biometric system that available with support from current mobile platforms and that uses face recognition to unlock phone. Although it's an alternative, is now becoming an attractive for authenticating its user. Because user doesn't need to remember PIN, Password or Gesture Pattern rather only frontal face information is necessary and easy to unlock mobile. Despite the current liveness detection feature, it has vulnerable problem for spoofing attacks [2].

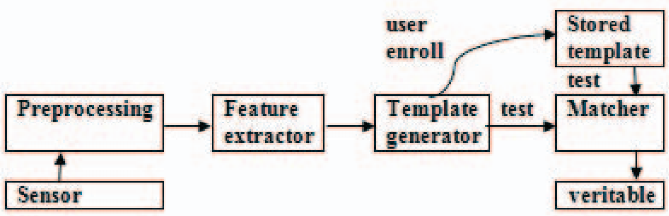

Fig.1. Biometric System for User Authentication

However, numerous algorithms have been proposed for liveness detection in face recognition for various applications such as video surveillance, security, identity verification, forensics, etc. The security and usability in mobile phone application remains an open research topic.

Intel released Open Source Computer Vision (OpenCV) in 1999 [1], [15]; an open- source computer vision library provides interfaces for the C, C++, Java and Python programming languages. It encourages the capability of face detection, face tracking, face recognition, and several image processing and artificial methods. It supports major desktop and mobile operating systems including Windows, Mac OS, Linux, Android, and iOS via its lower level APIs. JNI wrapper (JavaCV) provides wrappers to commonly used library in OpenCV. Dalvik Java Virtual Machine used on Android Operating Systems supports library and its functionality of OpenCV and JavaCV.

A. Spoof Attacks – its types

In general, the face recognition has three way spoof attacks using Frontal face photo of a user, Frontal face video of a user and 3D face model of user. Photo attack is the easiest approach in spoofing 2D face recognition system, since user's photo is available in their social network profiles or captured unknowingly using spy camera. The photo can be showed before the camera to fool the authentication system [3].

Video spoofing attack is similar to photo attack where user's face can be shot unknowingly with spy camera. Advantageous in video spoof; it captures the head movement, facial expression, and blinking features. Further, a frontal face video of user could be replayed on a digital screen of mobile phone either hand-held or fixed 3D model provides static 3D information of user's face. However, it lacks on facial expressions of the user. It is very difficult to make a realistic 3D model and deserves cost [2].

II. Literature Review on Anti-spoof

A. Face Detection

Face detection was initially proposed by Turn and Pentland [13] uses Principal Component Analysis (PCA) and Eigenface subspace. Rowley et.al[5] use neural networks for face detection by build up an input image pyramid by scaling the input image to multiple sizes, then perform sliding window

978-1-4799-3975-6/14/$31.00 ©2014 IEEE

based face detection. Papageorgiou et.al. uses Haar-like features based on wavelet representations of object in an image. Lienhart and Maydt extended the approach proposed by Viola and Jones with rotating features to defacto standard. A view-base model clusters that distinguish between 'face' and 'non face' by evaluating the frontal face images incorporates a Mahalanobis distance measurement.

B. Face Recognition

In mobile domain, we can easily find research papers showing results of face recognition accuracy rate above 95 percent. But testing those algorithms in real time, you may often find the accuracy rate is lower than 50 percent. Because the current face recognition techniques are very sensitive to real world environments such as lighting, shadows, and orientation. The data set needs more training images with all environments [3].

Face recognition was initially proposed by Turk and Pentland [13] is known for successful face recognition and work is based on the usage of Eigenfaces for face representation previously published by Sirovich and Kirby [11]. The change in illumination was the major problem identified. Belhumeur et.al.[7] overcomes those using FisherFaces for facial recognition. They evaluate their approach in direct comparison to the baseline Eigen for recognition. Significant increase in 2D and 3D face recognition approaches and algorithms have been proposed. Riaz[14] directly compares different implementations of Principal Component Analysis (PCA), Independent Component Analysis (ICA), Hidden Markov Models (HMM), and NeuralNetwork (NN). Venkataramani et.al [6] compares correlation filter, individual PCA and Fisher Faces as approaches to face recognition in mobile domain.

Gang Pan Et.al proposed [3] blinking based on liveness detection. They approached a quick and accurate recognition of blink behavior using adaptive boosting algorithm. This liveness detection approach may have possible spoof attack through same trick that done for liveness detection for Google API. Gao and Leung [4] proposed a side view face recognition by matching profile line segments and hausdorff distance to measure similarity. Pinar Santemiz Et.al. [8] improved a side view method by implementing Local Binary Pattern (LBP). This approach may cause trouble for user to authenticate in mobile at real time environment due to false detection of side view.

Rainhard and Rene [10] proposed an approach on acquiring a panshot of frontal face image around 180° and uses gyroscope sensor in mobile phone to calculate the movement of mobile. This method uses Viola and Jones algorithm and the real time approach seems to be difficult to use crowded environment. There is chance of producing blurred image by mobile camera due to capturing picture while rotating mobile about 180°.

III. PROPOSED FRAMEWORK

A. Pattern Acquisition

The proposed approach requires a front side camera enabled android mobile phone. The least API Level is 14; Android 4.0 is a major platform which supports high resolution photos for storage. For our current implementation, we use a Xolo Q500 device currently running on 4.1.2 Jelly Bean arrives 1.2 GHz Qualcomm Quad Core Processor, VGA Front Camera, 1 GB Ram, and 4GB built in memory.

In our prototypical implementation we require the user to perform following steps to acquire facial image for training.

1. The user holds his/her mobile phone facing straight to his/her face. The arm holding the phone should be stretched and user turns his/her face up to 30° (T = 30°) left side and start to capture his/her first image.
2. The user turns his/her face towards right and keeps face straight towards mobile phone, in our approach frontal face assumed to be 0° (T = 0°) and captures his/her second image.
3. The user turns his/her face towards right up to 45° (T = 45°) and captures his/her third image.

B. Dataset

We have created a preliminary heuristic face database at outdoor environment and indoor environment. The proposed template consists of three frontal face image of the user captured with various face angles such as -30°, 0°, and +45° used for training. The dataset prepared with facial image photos of user in various environment shown in Fig.2. includes cropped face image after face detection.

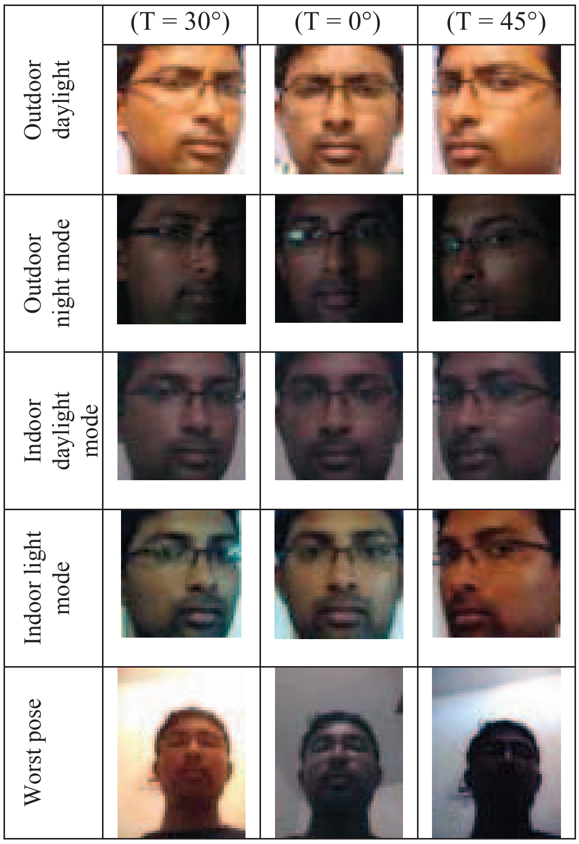

Fig.2. Training and Testing Images

The preliminary database contains images each with 480 x 640 pixels. It contains user face image captured from indoor and outdoor with various lighting environments. Assuming that preprocessing more images for face recognition would consumes time in mobile domain. We store three set of face image of user. For testing purpose we have used various kind of test image of same user.

IV. Experimental Analysis

We implemented Local Binary Pattern (LBP), and two baseline algorithms for face recognition algorithms, Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA). The PCA uses Eigenface approach is an unsupervised method that reduces the dimensionality of the feature space. LDA uses Fisherface approach is an extension of the Eigenface approach; is a supervised method used for dimensionality reduction and classification. The experiment was done with the help of preliminary database contains 15 images of user with 5 data set under various lighting condition. The figure (a) is used as training image from our database with each face detected image being cropped and resized to 128 x 128 pixels for the face recognition shown.

A. *Template Matching*

The Face Recognition in android application available either in training mode or in classifier mode. Both modes take the cropped image of three frontal face information of a user image dataset. The detected face images are assigned and the identity of the person is processed manually in each classifier mode. The classifier detects user face at angle of -30° and the classifier process for its identity. Every time after successful identification, the next process for classification mode to recognize the identity of the user will be expanded. Otherwise there is no provision for classifier expansion.

Additionally image matcher has been used to compare the difference between user's first image and third image. This can be done by inverting first image horizontally and the template matches both face images detected at -30° and +45°. The authentication is accepted only if both images don't match. Otherwise, assumed both are same image.

B. *Image Matcher*

The image matcher requires OpenCV library to manipulate images. It uses Oriented FAST and Rotated BRIEF (ORB) feature detector with Binary Robust Independent Elementary Features (BRIEF) descriptor extractors and BRUTEFORCE_HAMMING methods to match the descriptors [15]. This finds the closest descriptor in the second image and supports masking permissible matches between descriptor sets. To create efficiency matching between two images, distance metric is used.

In our approach we have used Image flipping (also called Mirroring Image) is preprocess for matching template where the user images captured at angles of -30° and +45° are used. The both images where flipped vertically and matched to each other individually to make an assumption on liveness detection. The separate components of face recognition and image matcher worked successfully independently; since there were difficulties while implementing on android device.

C. *Threshold Selection*

Threshold selection decides whether the incoming image belongs to the person in the training set or not. Therefore, even if the probe image is not in the database, the image will still be recognized as the training image with which its matching score is the lowest, which we know is incorrect. Hence, a threshold is required. Threshold value is chosen arbitrarily in general. There is no predefined formula for calculating the threshold value. Its value is either chosen arbitrarily or taken as some factor of maximum value of minimum Euclidian distances of each image from other images [12].

Here we used threshold value directly proportional to the rate of identification of face recognition. Therefore three threshold value such as 50, 75 and 100 is set as the recognition rate. More than average threshold is calculated for the recognition calculation.

V. Results

The preliminary face database was used as input for training images. Our heuristic approach is taken with OpenCV library in android which integrated with native code. The recognizer was trained with different number of training images for Eigenface, Fisherface and Local Binary Pattern approaches. The application has been tested in real time scenario with various lighting conditions and environments with three different values of the number of training images used for training recognizer. After training the recognizer with different images of the same person, recognition performance was tested with preliminary database.

A. *Results of Eigenface, Fisherface and LBP Approach*

The results with real time images and static images are shown by representing table and graphical format.

TABLE I. Results of Eigenface, Fisherface and LBP Approach

	Environment	**T = -30° RR**	**T = 0° RR**	**T= +45° RR**	**Average RR**
Eigenface	outdoor with daylight	100	100	100	100
	outdoor night mode	0	50	0	0
	indoor daylight	50	75	50	50
	indoor night mode	50	75	50	50
	worst pose images	0	0	0	0
Fisherface	outdoor with daylight	100	100	100	100
	outdoor night mode	50	50	0	0
	indoor daylight	75	75	50	75
	indoor night mode	50	75	0	50
	worst pose images	0	0	0	0
LBP	outdoor with daylight	100	100	100	100
	outdoor night mode	75	75	50	75
	indoor daylight	100	100	75	100
	indoor night mode	75	75	50	75
	worst pose images	0	0	0	0

RR – Recognition Rate

B. Image Matching

The result of image matching is used from images that are inverted with same angle of left side and right side frontal images from preliminary dataset and secondary dataset. The variation value in images that below the threshold value is assumed as different image, otherwise our approach assumes it as the same image. The results of variations in graphical representation were shown in Fig. 3

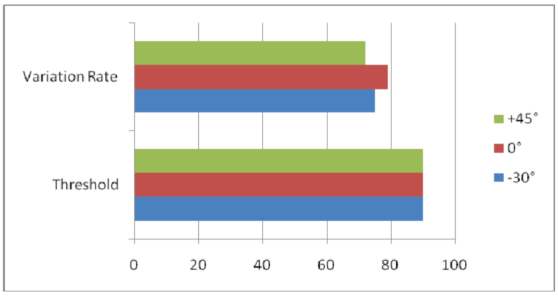

Fig.3. Image Matching Variation Rate

C. Analysis

From results, it shows that Local Binary Pattern approach is performing better than Eigenface and Fisherface approach for night mode images. With lighting illumination in indoor or outdoor, the Local Binary Pattern and Fisherface perform better than Eigenface approach and minute variations in various angles of frontal images.

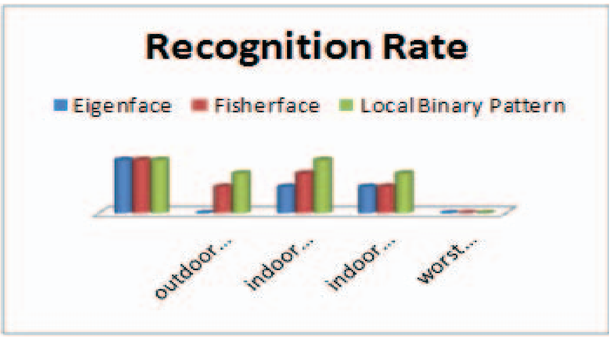

Fig.4. Average Rate Comparison of Each Approach

Analyzing with results from given tables, it shows that LBP is less sensitive against illumination variation and pose. Also, LBP is not affected by local changes and produces better confidentially result than PCA and LDA algorithms

VI. CONCLUSIONS

LBP algorithm provides better result in recognizing the face in all angles with various illuminations than PCA and LDA. The preliminary dataset applied with current approaches and initial results promising the better rate of face recognition in all three facial angles. The training set needs to perform once with three face samples of a user, but it requires training decent set of images that implicit good illumination to face. The face detection seems to be reliable, where recognition lacks due to changing illumination. The false positive results were detected in night mode which affects due to low illumination to face. Our current approach has very less chance in capturing blurred image and assures rapid performance with positive results.

In future, we aim to implement face tracking algorithm to track the user face automatically to improve liveness detection. This helps to possible face recognition with various pose and expressions, in order to obtain more robust recognition approach. With this integration, a stand-alone application that can perform facial recognition can be created along with face tracking algorithm to make better recognition rate in liveness detection.

REFERENCES

[1] Daniel Lelis Baggio, Mastering OpenCV with Practical Computer Vision Projects, 2012.

[2] R. D. Findling and R. Mayrhofer. Towards face unlock: on the difficulty of reliably detecting faces on mobile phones. In *International Conference on Advances in Mobile Computing & Multimedia*, pages 275–280, 2012.

[3] Gang Pan, Zhaohui Wu and Lin Sun, Liveness Detection for Face Recognition. Recent Advances in Face Recognition, ISBN 978-953-7619-34-3, pp.236, Dec 2008.

[4] Y.Gao, and M. Leung, “Line segment Hausdorff distance on face matching,”Pattern Recognition, vol.35, pp.361–371, 2002.

[5] Henry A. Rowley, Shumeet Baluja, and Takeo Kanade. “Neural Network-Based Face Detection”. In: *IEEE Transactions On Pattern Analysis and Machine intelligence* 20.1 (1998), pp. 23–38.

[6] Krithika Venkataramani, S. Qidwai, and B. Vijayakumar. “Face authentication from cell phone camera images with illumination and temporal variations”. In: *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on* 35.3 (2005), pp. 411–418.

[7] Peter N. Belhumeur, João P. Hespanha, and David J. Kriegman. “Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection”. In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 19.7 (July 1997), pp. 711–720.

[8] Pinar Santemiz, Luuk J.Spreeuwers, and Raymond N.J. Veldhuis.”Side-View Face Recognition”.

[9] Rene Maryhofer, Thomas Kaiser. ”Towards usable authentication on mobile phones: An evaluation of speaker and face recognition on off-the-shelf handsets”,2008.

[10] Rainhard D. Findling, Rene Maryhofer. “Towards Face Unlock: On the Difficulty of Reliably Detecting Faces on Mobile Phones”. MoMM2012, 3-5 December, 2012.

[11] L. Sirovich and M. Kirby. “Low-Dimensional Procedure for the Characterization of Human Faces”. In: *Journal of the Optical Society of America A* 4.3 (1987), pp. 519–524.

[12] Sheifali Gupta, OP Sahoo, Ajay Goel, and Rupesh Gupta. A new optimized approach to face recognition using eigenfaces. Global Journal of Computer Science and Technology, 10(1), 2010.

[13] M. Turk and A. Pentland. Eigenfaces for recognition. Cognitive Neuroscience, 3(1):71-86, Jan. 1991.

[14] Z. Riaz, A. Gilgiti, and S.M. Mirza. “Face recognition: a review and comparison of HMM, PCA, ICA and neural networks”. In: *E-Tech 2004*. July 2004, pp. 41 –46.

[15] http://docs.opencv.org/trunk/modules/contrib/doc/facerec/