

The Implementation of Face Security for Authentication Implemented on Mobile Phone

Emir Kremić*, Abdulhamit Subaşi*

*Faculty of Engineering and Information Technology, International Burch University, Francuske revolucije bb., 71210 Ilidža, Bosnia and Herzegovina
k.emir@acm.org, asubasi@ibu.edu.ba

Abstract: *In this paper we are presenting the face recognition security for mobile phones. The model which has been applied for face recognition is Eigenface. The implementation consists from two parts: MATLAB and Droid Emulator for ANDROID mobile phones. The proposed implementation model has come as an idea, since today's mobile phones are computers in medium. We run our e-mails, agendas, storing data, using it for financial applications for viewing stock markets etc., and we would like to provide the approach of security model which will be based on face recognition as a biometric approach for authentication on mobile phones. Due the PIN vulnerability, as the most used mobile phone authentication mechanism we are presenting the approach which will enable a new level of mobile phone user's security. This has been tested with the database which consists from many images of facial expression. The algorithm which was implemented for mobile face recognition on MATLAB side is PCA. Limited with hardware capabilities we made of substitution between accuracy and computation complexity on the application. Proliferation of application and data has aim to increase the user need to protect the data which exist in mobile devices.*

Keywords: *Face Recognition, PCA, MATLAB, Droid, Authentication*

Received July 29, 2011; accepted September 15, 2011

1. Introduction

Nowadays mobile phones has become very powerful medium size running machines, where on application level there are many application which are running and many data that is stored. Due to the problem with the privacy the new paths of security has started to implement. Mobile phones enable us to connect with our e-mails, bank account, order money transfer, etc. the Personal Identification Number (PIN) which consist out of four digits, cannot be considered as very secure method. Therefore, in this paper here we aim to discuss and presents the results of face recognition method which is implemented for mobile phone authentication security. The main idea of this paper is to present the model of face recognition being implemented for android mobile phones. This has been achieved through MATLAB and DROID emulator. This has been implemented for user authorization, authentication on phone. The algorithm which has been implemented on MATLAB side is PCA. This algorithm has been tested on the IBU database. The IBU (International Burch University) database has been created for this research on the University campus indented to acquire the accuracy results which were retrieved from testing. Since there are existing many different approaches for face recognition and

detection for this implementation we have been working on the implementation for DROID with PCA therefore it is the most common used method. The aspiration of this project is to combine the methods of human faces recognition and to develop a model which will perform high performance. This tested example is mobile to server face recognition model. Where on mobile phone application is running and server side is MATLAB and where the part of recognition method is accomplished. Detection and recognition are the most difficult problems which appear in computer vision, pattern recognition. First approach on face recognition is face detection. Consequently by applying PCA instead of face detection for recognition will be used eigenface methods. Specifically in this work and applications operate on mobile phone or the client and on a server. In brief, images (inputs) are provided from mobile phone and sent over the server to be processed and recognized. This has been implemented for ANDROID open source system and has been tested on mobile phone Samsung Galaxy S. Endeavour is to put forward mobile technology and application to become more beneficial to sociality.

Today's world security issues are the most important segment among all. Therefore, segment

of authentication plays a major role. When a person or a system checks the person's identity against another person then we are in process of authentication. That means the one who is authenticated can confirm that he/she is the person compares to. There are two essential type of authentication:

• **Verification:**

This is a process of confirming identity of any person by comparing the input data with ones existing in database. This is 1:1 authentication method

• **Identification:**

In this case we are matching the input data with all samples in the database with a view to retrieving the data related for the person. This system represents the 1:N authentication model

1.1. Cutting Edge Mobile Authentication

Since mobile phones are becoming a computer in medium, security issues have arisen due to the many applications which run on the phones,[1]. Therefore, the focus will be on resolving the security issue with previously – proposed models which can be integrated to upgrade new approaches. With the introduction of 3G, mobile phones changed significantly. Proliferation of application and data has increased the user need to protect the data which exist in mobile devices. The current approach is to protect with PIN. Such an approach could be used both on Subscriber Identity Module, PDA and smart-phone devices; are password based. Both PIN and password have been established many years ago. Even though they have been applied by different coding and encryptions of digital PINs and password, they remain weak.

The most frequent weakness of breaking the password or PIN by third party is based on assumption. The survey presented in the paper *Beyond the PIN: Enhancing user authentication for mobile devices* in [5], has found that 34% of 297 respondents did not use the PIN. Authors have also presented the results for security research: where 70% were interested in security and 69% were willing to pay for the security. Since the mobile evolution has gained momentum, the demand for an advanced model of security is becoming more apparent. Observing new approaches of the security, we will propose the face – recognition model of security for mobile authentication.

2. Background

For many years, there has been different research related to the subject. Due to the incensement of technology, strategy and approaches were changed. In this paper, we aim to provide an brief overview of discuss papers related to the subject, examine different approaches and present the model which has been implemented for this project. In the section that follows, we will present the model and its implementation.

Many papers related to the subject of implementation based in the mobile phone face recognition approach were published in 2010 and 2011. Different research related to it was started is in the process of testing in implementation. Different approaches were implemented and described in papers which were researching a face recognition approaches for mobile phones in [4]. The most used are PCA, color segmentation, KPCA and SVM, etc. The area of face detection and recognition are very complex subject in the field of computer vision [4]. In any paper that deals with this subject, the very first steps considered are those related to face detection. In [4] the authors were working with color segmentation and eigenfaces and fisherface schemes. It is very challenging to work on face detections, since faces are characterized by a variety of poses, shapes, sizes and textures. In [4], they have listed the following problems:

- *Pose* – a face can vary depending on the position of the camera while the image is captured.
- *Presence of structural components* – There may be an additional component on the face such as spectacles, moustache or beard with different type, shape, colors and textures.
- *Facial expression* – The facial expression worn directly on the person's face.
- *Occlusion* – A face may be partially obstructed by someone else or something when the image is captured among crowds.
- *Image orientation* – It involves the variation in rotation of the camera's optical axis.
- *Image condition* – The condition of an image depends on the lighting and camera characteristics.

3. The Algorithm and System Architecture

3.1. Face Recognition System and PCA

The *Principle Component Analysis* (“PCA”) is the common and successful techniques which have been used in image recognition and compression. It is a statistical method among many different factors which are applied in analysis. The main goal of PCA is to reduce the large dimensionality of data, to the smaller dimensionality of feature space, and this needed to describe data economically. This happens when there is a strong correlation between observed variables.

The PCA enable us to do:

- prediction
- redundancy removal
- feature extraction
- data compression

Application of face recognition may be applied in many different areas:

- face identification
- face classification
- sex determination
- Biometric security

The idea of implementing and using PCA for face recognition is to express images in 1–D vector of pixels constructed from 2–D facial image into the compact principle components of the feature space. Automatic face recognition system tries to find the identity of a given face image according to their memory. The memory is simulated by a training set. Our training set consists of the features extracted from known face images of different persons. The task is to find the most similar feature vector among the training set to the feature vectors as a given test images. The feature extraction algorithm which we have used is PCA. In Figure 1., is shown the diagram for face recognition and the same has been implemented in the application.

3.2. The Model Architecture

In Figure 2, is shown an authentication model which is used in this paper. As it is shown we have: *Cellular Phone Side* and *Matlab Side*. The connector between these two is Tomcat Server. On the Cellular Phone Side is Java Application. On the Server side is Matlab consisting of:

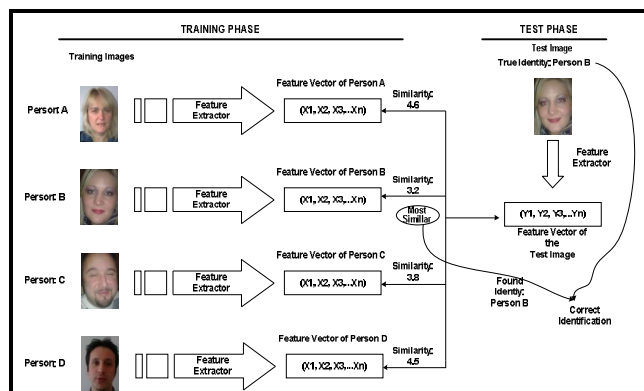


Figure 1: Schematic diagram of a face recognizer

user database, authentication engine, biometric profile and authentication manager. Authentication manager has overall control of the authentication system, deterring both when authentication should take place and what is the current state of security. Authentication engine, authenticates users, a Biometric Profile generate and train the relevant biometric template. Database contains information about users, compatibility, information about which mobile devices are configured to work with the architecture, along with a list of supported biometric system, in our case it is PCA. Mobile phone is via wireless and HTTP connected with a server side and it communicate to standard protocols.

3.3. Euclidean Distance

Face detection is based on distance measure, between two vectors (points), [3]. The idea of finding the distance between two or more vectors is defined as

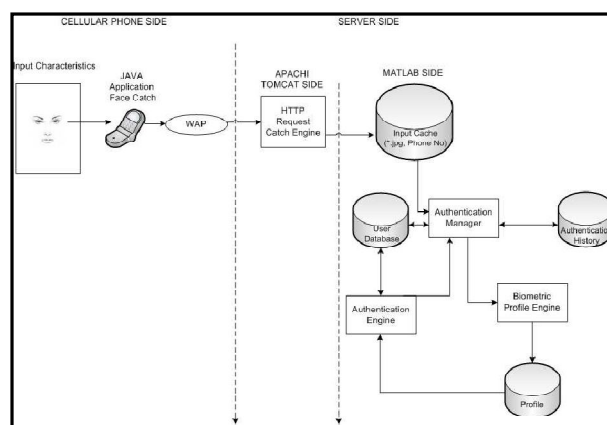


Figure 2: System Architecture

Euclidian distance. Euclidian distance is based on *Pythagorean Theorem*. It is a classical distance between two vectors, for example, distance between vectors in two – dimensional array we calculate as [3]:

$$D = \sqrt{(xa^2 - xb)^2 + (ya^2 - yb)^2} \quad 1.1$$

where from Eq. 1.1, x and y are coordinates in two dimension space. In three – dimensional space following formulas is known to us:

$$D = \sqrt{(xa - xb)^2 + (ya - yb)^2 + (za - zb)^2} \quad 1.2.$$

When calculating feature vectors well have result with a larger space dimensions. Therefore, we define vector over detected face as:

$$P = (p_1, p_2, \dots, p_n) \quad 1.3.$$

and we define vector of values over the detected face as:

$$Q = (q_1, q_2, \dots, q_n) \quad 1.4.$$

Defining values as shown in Eq. 3.3 and 3.4 will enable us to calculate the distance between vectors as:

$$D = \sqrt{(p^2 - q_1)^2 + (p_2 - q_1)^2 + \dots + (p_n - q_n)^2}$$

4. Application and Implementation

Increased processing power, storage capacity of mobile phone devices in real-time face recognition for mobile phones are no longer unattainable, [2]. There are many popular with high performance mobile phones as: *Apple's, iPhone, Google's Android and RIM's Blackberry*. This paper is developed and tested on Android Samsung Galaxy S. The application built is identity authentication for access control and prevention of unauthorized mobile phone usages. When eigenfaces are computed, different types could be made, depending on the application. Face recognition is a broad term and we could define it as:

- *Identification*: labels of individual must be obtain
- *Recognition*: must be decided if individual has already been seen
- *Categorization*: face must be assigned to a certain class

In here we will consider face identification only. Each face in the training set is transformed into the face space and its components are stored in

memory. An input (face image) is given to the system, and then is projected onto the space. The system computes its distance from all the stored faces.

4.1. Development Environment

System consists of two different parts, the server part and the face recognition part as follows:

- *Mobile Platform* – System is embedded into Samsung Galaxy S model of mobile phone and supports Java technology and is integrated with Java.
- *Android Mobile Technology* – Java SDK and Android technology, with DROID emulator
- *Hosting Web Server* – A server is required to host the application. This application will transmit and receive data over the Internet. Tomcat Apache HTTP Server is used as the web server.
- *Database* – Small database is developed for testing and evaluation. Database consists of face images.
- *Face Recognition Method* – Face Recognition part is developed using Matlab. It is integrated with the server.

4.2. Image Training and Test Set

We have prepared personal database called IBU Face Database (IBU = International Burch University Database) Figure 3. Face database contains 40 persons, and each person contains 20 different images. We have prepared five cases. This is implemented and tested in MATLAB. Training and test images are under *train image - directory*, and *test image* directory. A sample of MATLAB. For some subjects images are taken from different prospective, varying the lighting, facial expressions as: open/closed eyes, smiling/not smiling; facial details: glasses / no glasses. All of the images are taken against a dark homogeneous background with the subject in an upright frontal position with a tolerance for some side movements.

We have calculated the Euclidean distance between test images and training image and have found the closest Euclidian distance. A threshold is set such that if the closest distance above the threshold, the test face is considered unrecognized, and if below, is associated with the identity of the

closest face. With implementing PCA we have achieved on average accuracy of 88.88%.



Figure 3: Sample of training database

Table 1: Testing Results

Case No:	Description	Accuracy	Euclid Distance
Case 1	Lightning variation	82.35%	10E + 16
Case 2	Face Variation	85,29%	10E + 16
Case 3	Only males	100%	10E + 16
Case 4	Light hair females	81,81%	10E + 16
Case 5	Dark hair females	88,88%	10E + 16

In test case 1 was chosen 35 subjects (persons) and for each person were in test folder randomly chosen three images, where in total was 102 images. Selected images were tested in Matlab. After, testing and running as it is described above in Table 1 for test case one we have got results 82,35%. During this testing phases six face recognition occurred wrongly.

In the test 2 case was chosen 33 subjects and for each person were in test folder were three images with looks from different angles, where in total was 102 images.

Selected images from were tested in Matlab. After, testing and running as it is described above in Table1. Are shown results, where on different face variation from different angles accuracy is achieved 85,29%.

During this testing phases six face recognition occurred wrongly to be matched. In the test case 3 were consider only males and in testing phase were 9 people and in test database were 27 images. The accuracy achieved is 100 %. In test case 4 and 5 were women. Test case 4 was light hair woman's and test case 5 with dark hair woman. The accuracy achieved in test case 4 is 81,81% and case 5 is 88,88%. In the case 4 we have got a lower result, due, we have few blonds looking similar between others. In Figure 4 is a sample of image

data with consists of train and tested. The images circle with red are the ones which were matched wrongly in the database.

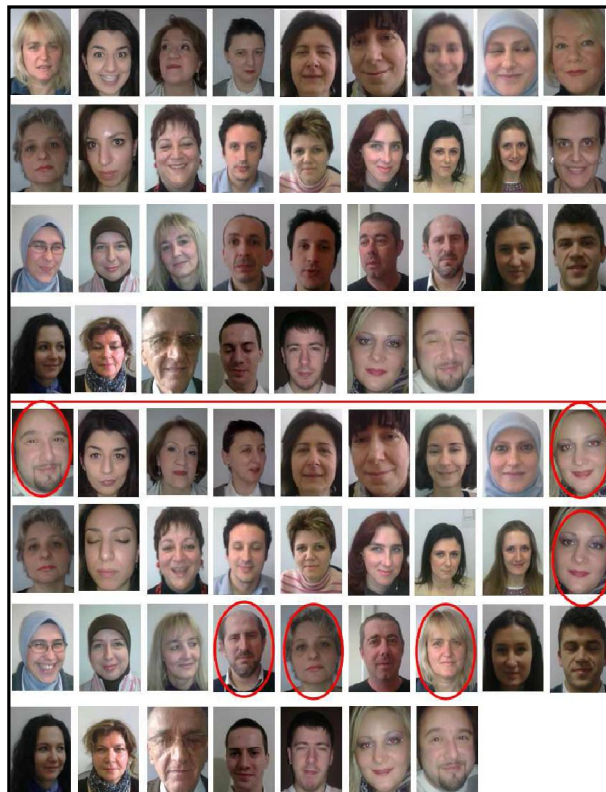


Figure 4: Comparison between tested and matched images

5. Conclusion

In this thesis, we have examined how can we improve the security of a mobile phone, authentication and implemented it. We have done extensive and exhaustive work in implementing face recognition with mobile phone authentication and making it work in real time on Android Samsung Galaxy S. For the accuracy of the experiments, the training set should not overlap the test set. This thesis is a prototype developed to test face recognition on mobile phone. Here, we have implemented PCA algorithm for face recognition on Matlab side, and have developed the JAVA authentication methods for Android. There are some limitations in our face detection algorithm. By implementing this on mobile system we have achieved 88% accuracy. Even though we have done significant research, there is still open room for continuing working on this subject. With mobile phones usage, traditional method of user authentication changes and raises important security issues. Still used PIN techniques will be under – utilized and will be replaces. Adding the level of intelligent authentication will not be a problem to pass or fail but to confirm the identity of the user. An open

question to future work stays in video and speech recognition in mobile phone security as part of mobile authentication.

References

- [1] Clark N., Furnell S., “Advanced user authentication for mobile devices,” *Elsevier Computer and Security*, vol. 26, pp. 109-119, 2007.
- [2] Choi K., Toh K.A., Byun H., “Realtime training on mobile devices for face recognition application,” *Elsevier Pattern Recognition*, vol. 44, pp. 412-320, 2011.
- [3] Sharma M., Singh S., “Practical implementation of matlab based approach for face detection using feed forward network”, *Journal of Computer Science and Information Security*, vol. 9, pp. 284-290, 2011.
- [4] Sabri M., Nurulhuda I., “Mobile to server face recognition: A System overview,” *World Academy of Science, Engineering and Technology*, vol. 69, pp. 767-771, 2010.
- [5] Clark N., Furnell S., Karatzouni S., “Beyond the pin: Enhancing user authentication for mobile devices,” *Center for Information Security and Network Research, University of Plymouth, UK*, pp. 12 – 27, 2008.