FAMC: Face Authentication for Mobile Concurrence

Veena V. Salunkhe, Mrs. M.P. Deshmukh, Prabodhi A. Pimplekar, Nikita S. Bhosale, Amruta G. Bendre
Department of Information Technology
JSPM's Rajarshi Shahu College of Engineering
veenasalunkhe6@gmail.com

***Abstract*—** It has been observed in the last decades that face recognition has acquired a large amount of attention and curiosity. Benefits of this have been seen in quite a few applications. An architecture which has been implemented earlier addresses the face analysis domain. As compared to other biometrics, face recognition is more advantageous but it is particularly subject to spoofing. The whole cost of the system increases since the accuracy of this technique involves the estimation of the three dimensionality of faces. An effective and efficient solution for face spoofing has been proposed in the paper. The growing use of mobile devices has been a growing concern due to their ability to store and exchange sensitive data. Thus this has given encouragement to the interest of people, to exploit their abilities, from one side, and to protect users from malicious data, on the other side. It is important to develop and deliver secure access in this scenario and identification protocols on mobile platforms are another upcoming aspect that also requires attention to deal on the commercial and social use of identity management system. After all these conclusions, the earlier architecture proposes biometrics as the choice for technology which has been also implemented and described in the earlier architecture. The earlier architecture is designed for mobile devices. This architecture thus acts as an embedded application that provides both verification and identification functionality. It includes identity management to support social activities. Examples of identity management system are finding doubles in a social network. Privacy has been provided by these functionalities which help to overcome the security concern. The architecture of FAMC: Face Authentication for Mobile Concurrence is modular. Functionalities like image acquisition, anti-spoofing, face detection, face segmentation; feature extraction and face matching have been provided by its implementation. The behavior of FAMC allows for recognition and best biometrics sample selection.

***Index Terms*—** *Biometrics, face recognition, three dimensionality, face spoofing, anti-spoofing, detection, extraction, android, mobile encounter, face authentication, identity management system, malicious data, verification, identification, image acquisition, face segmentation*

*****

I. INTRODUCTION

Face Recognition systems operate on 2D images. They use infrared light or visible light. The degree of their sensitiveness can vary indefinitely. The system can be cheated by simply showing a photo of a registered user when a poor degree of spoofing detection can be present. The movement detection of the face or other parts like smile, eye blinking can avoid this. But however by a video clip of the registered user this can also be cheated. The anti-spoofing techniques focus at verifying the 3-dimensionality of the face in the front of the capturing device which can help us to address this issue. But by introducing 3D models of face even this can be cheated. It is difficult, time consuming and expensive to make 3D verification spoofed by a 3D mask. To address mask problems few techniques are been used.

Verifying captured face three dimensionality should not be the only purpose of the anti-spoofing technique, but also should not rely on the user interaction with the system. Thus the involvement of the implementation of challenge-response protocol in turn upgrades the quality of service of the system. The specific action called as the challenge is given by the user which is required by the system. Smiling or eye blinking, or pronunciation of a specific sentence are the different challenges given by the user; then the system analyses the change and checks that the user actually carries it out defined as responses. The gesture/expression to detect is system triggered. Specific time elapse is required for its occurrence. Additional equipment/software may be required.

Instead for a demand for specific motion type the challenge based on the time requested motion has been used to avoid spoofing via pre-recorded video may be included. An extra-hardware support might require for the recognition process for detecting users' image liveliness. However, without assuring optimal performance this increases the cost of the system. User does not require staying always in a perfect frontal pose and looking towards capture device as often it is in the case of eye blink-based techniques is the further advantage of this system. Sufficient tolerance to user's position has been derived from earlier illustrations. Spoofing detection algorithm is able to detect spoofing attacks which is both quick and accurate has been proven by the results of the experiments.

In today's world secure access from security point of view is very significant issue. Technology has addressed this issue more efficiently and helped to develop complex techniques for the same which has been seen to be developed in the last decade. Attempts done towards face biometry implementation but not on a large scale which nowadays has been used to develop secure applications. The technology for face biometry has not yet been matured is the reason for it.

The light and pose variations are the major factors that determine the accuracy of image retrieval for face biometry. The solutions to such applications are applications like Polar Rose, iPhoto and Google Picasa. Social networking sites like Facebook and Flikr works with the help of Polar Rose application. Reconstruction of 3D face model, initiating from two dimensional images are the core functionality of this software. But, a semi-automatic training procedure has been performed by Picasa and iPhoto which are more towards managing and organizing photo album, where the user executes the query and redefines its result by providing a relevant feedback, i.e. by discriminating the images into interesting and uninteresting ones. Image datasets from Facebook has been introduced by the earlier architecture. No algorithm is mature for the real applications to provide satisfying performances is the conclusion on which they aroused.

Automatic classification and extraction of images by their analysis has been proposed by the framework of earlier implementation. For comparing face with other algorithms tests were performed. Datasets including 1500 photos of celebrities downloaded are included in the databases of tests. 11% increment in accuracy was granted from the results derived from the test. Further advantage of not necessarily retraining after adding new photos is given as facial image does not require any kind of training phase. Need required to re-tagging it is eliminated by an ability to tag such photos. There are almost 24 billion devices connected to internet in today's world, which include smart phones or tablets and desktop computers.

From the economic point of view a market of about 1.2 trillion dollars in 2020, with significant implications for both economic and social aspects. Support of personalization of services and contents as well as the creation of new patterns of social interactions has been provided by the technological advances. Stand alone PC's and laptops are involved in hacking data theft and spoofing. The extreme ability to store and exchange sensitive data and continuous use of mobile devices has encouraged the interest in exploiting their current abilities. As a result, to protect the user from malwares and the essentiality to develop and deliver secure access and identification protocols on mobile platforms has increased tremendously.

The social use of identity management system is also other aspect that also needs to be focused. The systematic organization of huge amount of contents available on media that the user can access, maintain and use properly systems are some of the services provided by these systems. Such dual requirements have been defined by a technology characteristic of biometrics. Rather than something that is known, with advantages not only in respective to security but also in terms of comfort and usability, biometrics is capable to bind the identity of an individual.

Dual usage functionality have been deployed by biometrics system that include one-to-one matching called as verification and one-to-many matching called as identification. The verification is particularly used for task where it is necessary to ensure legal and secure access to resources and privileges and certifies the identity claimed by a specific user. The identification is well applicable to facilitate and support social activities that aim at retrieving the identity of an individual in a set/group of potential identities, more or less limited in size.

Mobile platforms have been used to design earlier implementation. Providing security and user support in the use of mobile services based on facial biometrics is its main objective. This choice is due to two reasons: a)Face biometrics is largely been accepted and b) requirements of face biometrics are better applicable to the hardware resources made available by mobile devices. It consists of entire chain of operation: Face localization spoofing detection, correction of samples feature extraction and face matching that relies on mobile biometrics system. A verification team has been implemented to provide secure use of the mobile device and of online transactions. An identification scheme for the organization of media content and social activity has also been provided. Android platform has been used to design which acts as an operating system for mobile devices. For mobile application it also provides an open source development platform. Multiple testing sessions have to be undergone, in order to evaluate its performance based on the accuracy, functionality and acceptability, usability. Different types of user perform tests.

Face recognition systems based for Smartphone has limitations that derive limited computing power and also suffers from some problems of computer based system has the drawbacks of illumination and pose variations. In some earlier systems and via wireless network the processing tasks are performed on a server; only to sense video mobile devices are used. Trend towards the most recent works are shown towards all the computations in the mobile device. Robust and efficient face recognition algorithm in mobile devices has been implemented in the works earlier. The earlier works are based on the Local Binary Patterns (LBP) [10] features. These features have proven to be powerful and computationally efficient for feature extraction. As discussed in earlier architectures the algorithm consists of an engine of a new face recognition based photo sharing application.

II. LITERATURE SURVEY

The earlier works have designed an algorithmic approach which would improve the accuracy and performances compared with the earlier models for face analysis and face matching. Spoofing is considered as a weak point which is often not addressed in face authentication. There are many solutions presented but yet not free from limitations. By some

of the techniques only very simple attacks are detected. The approach discussed above can verify the true three dimensionality with low computational cost.

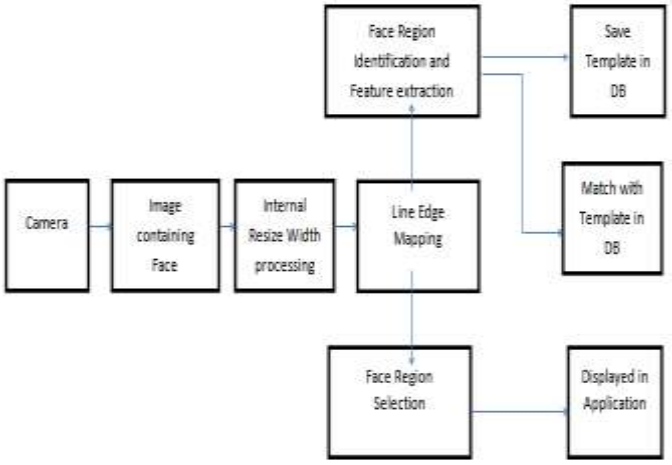
The architecture of earlier design is modular. The functionalities of image acquisition, anti-spoofing, face detection, face segmentation, feature extraction and face matching are been provided by the individual modules. Continuous recognition and best biometrics sample selection is the behavior of provided by earlier architecture. Both varying pose and illumination accommodation has been provided by this. Low demanding and computation light algorithms provided by all processors are designed for mobile use.

The scope and range of earlier implementation is on a wide scale. Many diverse applications can use the facial biometric authentication eg. Remote medicine to access physiological condition, online education to access student attention and understanding and alter state of drivers for safety purpose.

.

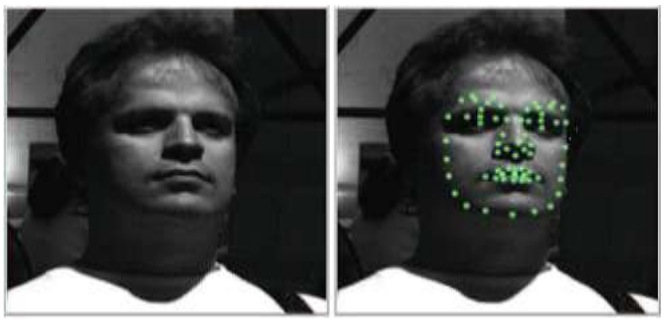
III. PROPOSED SYSTEM

The figure shows architecture of the proposed system that is Face Authentication for Mobile concurrence (FAMC). This system is the mobile application which works on Android 4.4.2 operating system and higher versions as well. This application accepts the non-distorted as well as distorted face and recognizes the face. With this application we can capture the image easily, crop the image, save the cropped image and implement the same algorithm for locking and unlocking the screen. Thus the components are as follows:
1) Face Detection and Normalization
2) Pose and Illumination Correction
3) Face Matching



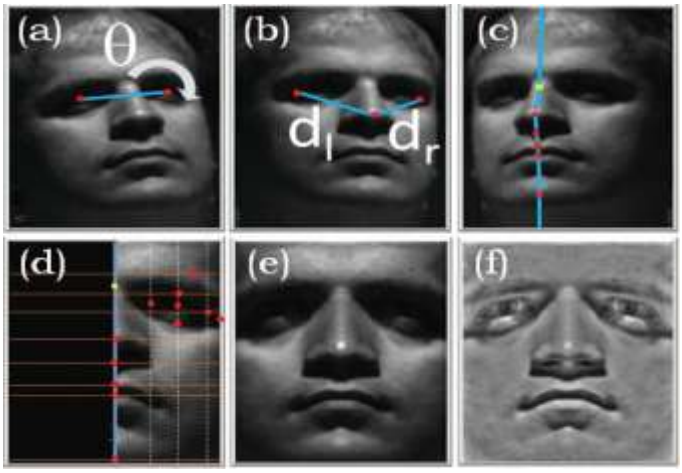
A. *Face detection and normalization*

First step of face recognition process is to detect the number of face in image. For detecting the face the face Active Shape Model(ASM) algorithm is used which aims to match the model to new image .This algorithm is used to search and mark the relevant landmarks of face. The algorithm marks 68 points on face as landmark point. These landmarks are used for normalization, taking facial image to conical pose and illumination. Landmarks show the boundary of object. Extended ASM (STASM) submit image to global face detector to extract image including face.



B. *Pose and Illumination Correction*

Out of 68 points STASM use only 14 points for detection of face. Centre of eyes is used to correct head rolling (fig a). As shown in fib.b the external angle between right eye (d_r) and left eye(d_l) is calculated with tip of the nose as centre. If the calculation shows result as ($d_r \geq d_l$) then the face is reverted towards left side otherwise face is reverted towards right side which shows result as ($d_r \leq d_l$) with respect to vertical axis. Fig.c shows exact face profile i.e divide the face in two half. Here yellow point is the median point of link between its immediate neighbor. Half of the facial image is divided in horizontal and vertical line which passes from interest points (fig.d). Stretching is performed on the row of right region of face to find some constant length. These lines are resized to get pre-determined position from the interest points. Other half face (left region) is reconstructed by reflecting the right half of face(fig e). Illumination correction is performed with Self Quotient Image (SQI) algorithm on the final image(fig f).



C. *Face Matching*

Most of the face characterization techniques are still sensible for image distortion and are gainfully to be used in application. Spatial correlation index is used to match the face. Here A and B are two given images and r_A and r_B are sub regions respectively. For each sub region r_A, we search limited window

around the same position in region r_B. This maximizes the correlation $S(r_A,r_B)$. S(A,B) is obtained as a sum of local maxima.

i. Algorithms

The Face Detection algorithm provided by the opencv platform are as follows:

- Haar-based face detector
- LBP based face detector

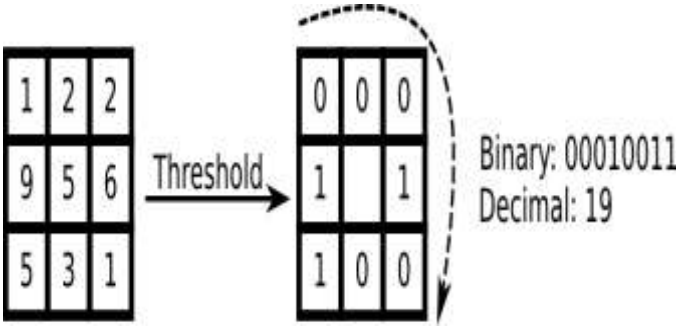
The Face Recognition algorithm provided by the opencv platform are as follows:

- FaceRecognizer.Eigenfaces
- FaceRecognizer.Fisherfaces
- FaceRecognizer.LBPH

We have used LBP for face detection and LBPH for face recognition.

ii. Local Binary Patterns Histogram

To get good recognition rates you'll need at least 8(+-1) images for each person and the Fisherfaces method doesn't really help here. Some research has been concentrated on extracting local features from images. The idea is to not look at the whole image as a high-dimensional vector, but describe only local features of an object. The features you extract this way will have a low-dimensionality implicitly. A fine idea! But you'll soon observe the image representation we are given doesn't only suffer from illumination variations. Think of things like scale, translation or rotation in images - your local description has to be at least a bit robust against those things. The Local Binary Patterns methodology has its roots in 2D texture analysis. The basic idea of Local Binary Patterns is to summarize the local structure in an image by comparing each pixel with its neighborhood. Take a pixel as center and threshold its neighbors against. If the intensity of the center pixel is greater-equal its neighbor, then denote it with 1 and 0 if not. You'll end up with a binary number for each pixel, just like 11001111. So with 8 surrounding pixels you'll end up with 2^8 possible combinations, called *Local Binary Patterns* or sometimes referred to as *LBP codes*. The first LBP operator described in literature actually used a fixed 3 x 3 neighborhood just like this:



iii. Algorithmic Description

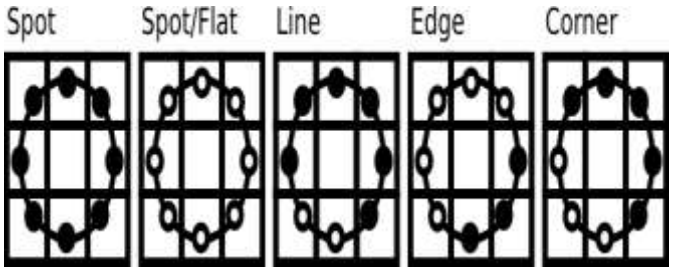
A more formal description of the LBP operator can be given as:

$$LBP(x_c,y_c)=\sum_{p=0}^{p-1}2^p s(i_p-i_c)$$

with (x_c,y_c) as central pixel with intensity i_c; and i_p being the intensity of the neighbor pixel. **S** is the sign function defined as:

$$s(x)=\begin{cases}1 & if\ x\geq 0\\ 0 & else\end{cases}$$

This description enables you to capture very fine grained details in images. In fact the authors were able to compete with state of the art results for texture classification. Soon after the operator was published it was noted, that a fixed neighborhood fails to encode details differing in scale. So the operator was extended to use a variable neighborhood. The idea is to align an arbitrary number of neighbors on a circle with a variable radius, which enables to capture the following neighborhoods:



For a given point (x_c,y_c) the position of the neighbor $(x_p,y_p), p\in P$ can be calculated by:

$$x_p=x_c+R\cos\frac{2\pi p}{P}$$

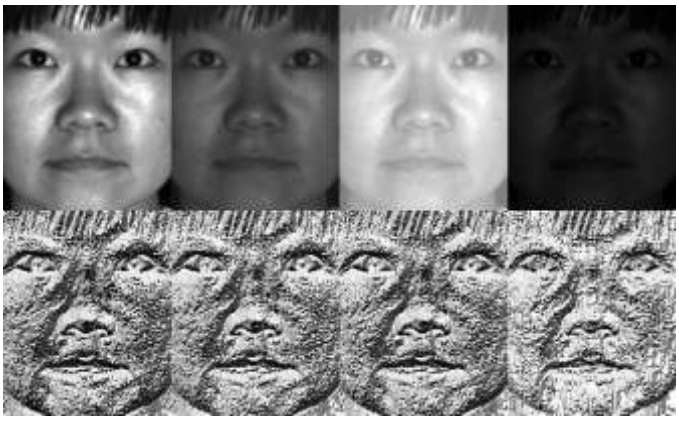
$$y_p=y_c-R\sin\frac{2\pi p}{P}$$

Where R is the radius of the circle and P is the number of sample points.

The operator is an extension to the original LBP codes, so it's sometimes called *Extended LBP* (also referred to as *Circular LBP*) . If a points coordinate on the circle doesn't correspond to image coordinates, the point get's interpolated. Computer science has a bunch of clever interpolation schemes, the OpenCV implementation does a bilinear interpolation:

$$f(x,y)\approx[1-x\ x]\begin{bmatrix}f(0,0) & f(0,1)\\ f(1,0) & f(1,1)\end{bmatrix}\begin{bmatrix}1-y\\ y\end{bmatrix}$$

By definition the LBP operator is robust against monotonic gray scale transformations. We can easily verify this by looking at the LBP image of an artificially modified image (so you see what an LBP image looks like!):



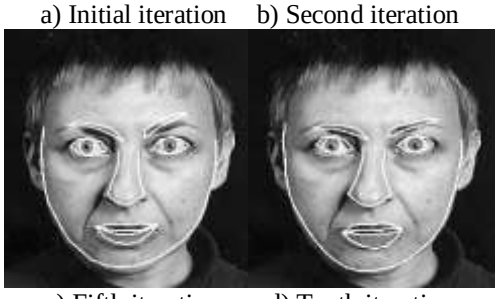
IV. EXPERIMENTS, RESULTS AND DISCUSSIONS

To perform the proposed system we are using external storage to store the images. Internal storage works as the database of this application. This application perform operations such as train recognizer, face recognizer and edit database.

A. Train Recognizer

Train recognizer is performing the task of capturing the image. While capturing the image some iterations are been calculated. In this system we are considering total 10 iterations. So at the 10^{th} iteration the face shape is in proper state. After each iteration some changes are done in the shape of the face.

a) Initial iteration b) Second iteration



c) Fifth iteration d) Tenth iteration

Above figure represents the state of image and shape at the time of iteration. For preparing the proper shape of each face, landmarks and interest points are used. ASM algorithm helps to find the shape of facial image. All these points are joining together and form a shape. At each iteration, points of shape are compared and are tried to be matched with landmark point of original image.

B. Face Recognizer

As name suggests face recognizer performs the task of recognizing the face. For recognizing the particular face or to detect the face from group image face matching algorithm is performed. This algorithm performs the following steps:

- Examine the region of the image around each point Xi to find the best nearby match for the point X'i.
- Update the parameters (Xt, Yt, s, Θ, b) to best fit the new found point X. Here,
  - X- Model point
  - B- Shape parameter
  - Θ- orientation
  - s- Scale
- Apply constraint to the parameters, b, to ensure plausible shape.
- Repeat until convergence.

Step 1- The algorithm examines all the regions of the captured image. Select each interest point Xi for different regions of the captured image. Then search for same or nearby match X'i for which point on the saved image is compared with the captured image.
Step 2- As the particular match for point Xi is found, it updates all the parameters like model point(X), shape parameter(B), orientation(Θ) and scale(S) which are best fit with X.
Step 3- For making reasonable shapes apply limitations to all parameters.
Step 4- Repeat these steps till get the match of face.

Iteration help to search the nearby or same interest point of compared image to the ASM algorithm. This iteration tries to match the landmark point of face with landmark point of shape of face. Once the image has been recognized it is further used for locking and unlocking the screen of the mobile. This helps to provide security with the usage of algorithm with a real time based environment.

C. Edit Database

As name represents edit database is used for editing the facial image database. It performs the task such as store information related to the image, save that image, deleting, editing and updating information about image. When new image is captured by camera it asks for the information related to that image. If the information already exists in the database, then it pops up that information at the recognition time.

We have used SDK as external storage for database. This database contains the information of each face. Information may contain (name,address) etc. When face is recognized it displays the recognized button and the details of the face detected are popped up.

V. Conclusion and Future Work

Thus we have implemented a system which captures the image and after performing the transformation stores the image on the internal SD card. The face thus captured is compared with the one saved and the detection and recognition phase is been performed. This detected facial image is then used for unlocking the screen. But the major concern of this implementation is that it cannot detect spoofing via 3D moving facial mask rather it detects spoofing via non 3D images. The future implementation will help to overcome it which may include fusion of eye blink or skin reflectance analysis.

References

[1] Silvio Barra, Maria De Marison, Chiara Galdi, DaneilRiccio, Harry Wechsler, "FAME: Face Authentication for Mobile Encounter"

[2] BullGuard. "Mobile Security & Malware Protection", [Online]. Available:http://www.bullguard.com/bullguard-security center/mobilesecurity/mobile-threats/mobile-security-what-you-need-to-know.aspx(seen December 2012)

[3] M. De Marsico, M. Nappi, D. Riccio. "Face: face analysis for Commercial Entities," in *17th IEEE International Conference on Image Processing (ICIP '10),* Honk Kong, China, 2010, pp.1597-1600,.

[4] M. De Marsico, M. Nappi, D. Riccio, J-L Dugelay. "Moving face spoofing detection via 3D projective invariants", in *5th IAPR Internat ional Conference on Biometrics (ICB '12)*, New Delhi, India, 2012,vol., no., pp.73-78.

[5] M. De Marsico, M. Nappi, D. Riccio." ES-RU: an entropy based rule to select representative templates in face surveillance", *Multimedia Toolsand Applications*, Special Issue on Human Vision and Information Theory, Springer Journal, published online November 08, 2012. Available: http://link.springer.com/article/10.1007%2Fs11042-012- 1279-6?LI=true

[6] K. Etemad, R. Chellappa, "Discriminant Analysis for Recognition of Human Face Images", *Journal of the Optical Society of America A*, Vol. 14, No. 8, pp. 1724-1733, Aug. 1997,

[7] IBM X-Force." Built In. Not Bolted On: Smarter security solutions from IBM – Threat Landscape - 2011 Mid-year Trend and Risk Report",[Online]. Available:http://www03.ibm.com/security/landscape.html

[8] mobiThinking (December 2012). "Global mobile statistics 2012 Part A: Mobile subscribers; handset market share; mobile operators", [Online]. Available:http://mobithinking.com/mobile-marketing-tools/latestmobile- stats/a#subscribers

[9] F. Sideco (November 2012). "Mobile Communications Equipment Market Set for Double Digit Growth This Year", ", [Online]. Available:http://www.isuppli.com/Mobile-and-Wireless- Communications/News/Pages/Mobile-Communications-Equipment-Market-Set-for-Double-Digit-Growth-This-Year.aspx

[10] E. Vazquez-Fernandez, H. Garcia-Pardo, D. Gonzalez-Jimenez, L. Perez-Freire. " Built-in face recognition for smart photo sharing in mobile devices", in *IEEE International Conference on Multimedia and Expo (ICME '11)*, Barcelona, Spain, 2011 , vol., no., pp.1-4

[11] H. Wang; S. Z. Li, Y. Wang, and J. Zhang, "Self quotient image for face recognition", in *International Conference on Image Processing (ICIP '04)*, Singapore, 2004, pp. 1397-1400.

First Author – Veena V. Salunkhe, Student, JSPM's Rajarshi Shahu College of Engineering Pune, India, Department Of Information Technology, veenasalunkhe6@gmail.com

Second Author – Mrs. M.P. Deshmukh, Lecturer, JSPM's Rajarshi Shahu College of Engineering Pune, India, Department Of Information Technology, deshmukmonali@hotmail.com

Third Author – Prabodhi A. Pimplekar, Student, JSPM's Rajarshi Shahu College of Engineering Pune, India, Department Of Information Technology, prabodhi20@gmail.com

Fourth Author – Nikita S. Bhosale, Student, JSPM's Rajarshi Shahu College of Engineering Pune, India, Department Of Information Technology, bhosalenikita68@gmail.com

Fifth Author – Amruta G. Bendre, Student, JSPM's Rajarshi Shahu College of Engineering Pune, India, Department Of Information Technology, amrutabendre1992@gmail.com