IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

Intelligent Laptop Lock-Unlock Security Based Application

P.S. Hanawate[1], Kalyani Kolte[2], Aishwarya Patil[3], Yashashri Kuchekar[4]

Computer Department, NBNSSOE Pune[1,2,3,4]

Abstract: "Intelligent Laptop Lock-Unlock Security Based Application" is designed for the security purpose of the laptop. The application is helpful when someone tries to unlock the laptop at the same time the application act as a trigger to the camera and camera captures the image of person which sat in front of the laptop otherwise send the default image after specific time and it also send the notification on the mobile phone with captured image. By using this application owner can take actions from mobile phone. The framework is outlined with the end goal that the runtime operations captures which performed by client and the client will be identified and afterward just he will be given a key to lock or unlock the system. The application is intended to permit the client to likewise check the status of the entryway. The cell phone requires a password to expand the security of the framework. Security is primary support toward taking care of such archived data in laptop, tablets, cell phones, PCs. We don't have that much good security with these gadgets. The security we have is making lock for system as a secret word however anybody can hack the password and mischief our information to maintain security and avoid hacking such a variety of security functions are given like thumb print, retina acknowledgment and so on. In any case, there is no security for watching that who is attempting to crack the password. That security is given in our proposed system.

Keywords: Laptop security, Embedded security, Face detection.

I. INTRODUCTION

The basic aim of project is to develop a Intelligent Laptop Lock-Unlock Security Based Application which will help user receive notification on his/her mobile if somebody unlock Laptops. Security is primary support toward dealing with such records in portable workstation cell phones PCs. We don't have that much good security with these gadgets. The security we have is making lock for framework as a secret key however anybody can hack the
password and mischief our information to maintain security and avoid hacking such a large number of security capacities are given like thumb print, retina acknowledgment and so on. In any case, there is no security for watching that who is attempting to break the secret key. That security is given in our proposed framework.

II. ARCHITECTURE

An Architecture of the system is depends on the laptop security. our system proposed the application which secure laptop by using mobile phone. There are two users one is laptop user (client) and another is mobile user (server).our system is WiFi based communication system. First mobile user has to sign up/login in the application which is handle by request decoder.

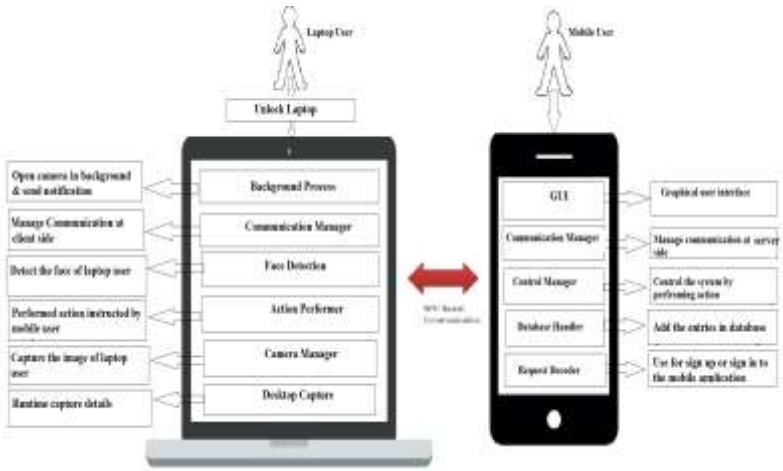

Figure 1. "System Architecture diagram"

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

When someone tries to register in the application then new entry is updated in database. Database is handling by database handler. If anybody wants to access the laptop then he/she will enter the password. Then request send to GUI handler .GUI (Graphical user interface) helps to interact with the user .There are two communication manager one at client side and another at server side which are useful for the communication. After unlock the laptop camera will open in the background and the image. Notification sends to the mobile user with the captured image. On the basis of captured image mobile user perform the authentication that is user is valid or invalid. If user is valid then mobile user gives the permission to access the laptop otherwise he can take action like lock or shutdown or restart the laptop. Also he can capture the runtime operations which performed by laptop user and also hide the important data. Control manager take actions and action performer perform those actions. Camera manager capture the images and desktop capture captures all the desktop operations and shows it on the mobile phone. In our system we used different algorithms like eigenface for face detection and REST and AES for the communication.

III.TECHNOLOGIES/ALGORITHM USED IN THE MACHINE

A. Eigen vector

- Main idea behind eigenfaces: it is algorithm for face detection and recognition.

- Suppose G is an N2x1 vector, corresponding to an NxN face image I.
- This idea represent G (F=G - mean face) into a low-dimensional space.
-Represented in equation form as given bellow

Fˆ - mean = w1u1 + w2u2 + . . . wK uK

- Calculating eigenfaces

Let face image I(x, y) 2D N by N array of 8-bit intensity values. Image is vector dimension N2 means 65535 dimensional space ensemble of image the map collection point in this space for example figure shows training set of various images of faces. Standard part analysis used to discover vectors. These vectors find face space with length N2.

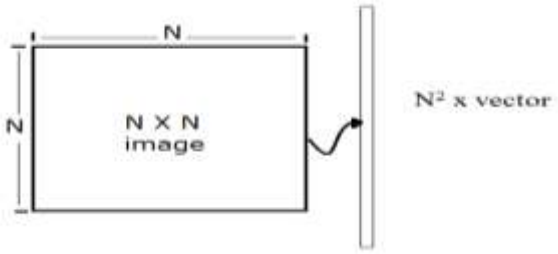

Figure 2. “Image representation in eigenfaces”

- Database

-2500 face images digitized under monitor and controlled conditions.
-16 subject with three head orientation are digitized and also with head size, scales, three lightning conditions etc.
-Gaussian pyramid of 6 level having image resolution 512x512 pixel to 16x16 pixel.

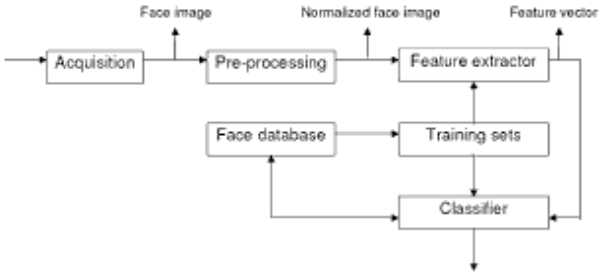

Figure 3. “Position of database in face detection”

Summary of steps for eigenfaces: Collect a set of characteristics which contain set of images.

$$\lambda_k = \frac{1}{M}\sum_{n=1}^{M}(\mathbf{u}_k^T\Phi_n)^2 \qquad (1)$$

$$\mathbf{u}_l^T\mathbf{u}_k = \delta_{lk} = \begin{cases} 1, & \text{if } l = k \\ 0, & \text{otherwise} \end{cases} \qquad (2)$$

λk and uk are eigenvectors and eigenvalues respectively which we have calculated in equation 1 & 2.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

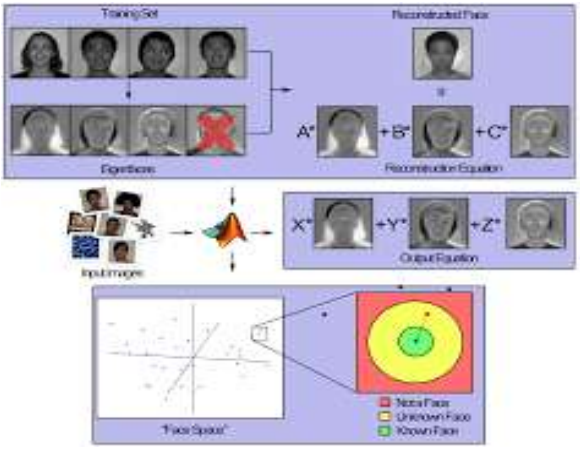

Figure 4."Face images in training set"

$$C = \frac{1}{M}\sum_{n=1}^{M}\Phi_n\Phi_n^T \qquad (3)$$
$$= AA^T$$

Equation 3 gives covariance matrix. Which calculate 40x40 matrix and find eigenvector and eigenvalues which ultimately gives average face Ψ.

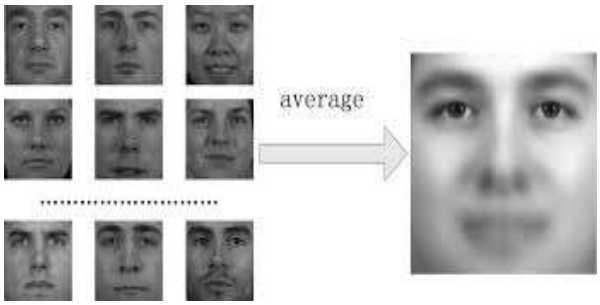

Figure 5. "Average face Ψ"

Following image shows process of face recognition. In that we have second step face detection. Which contain input images as training fringe images and unknown fringe images. In our paper only face detection is needed to capture the machine user image. Face recognition is done by machine owner itself.

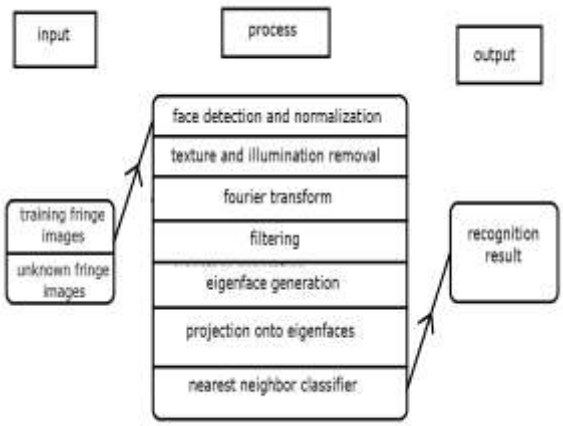

Figure 6. "Face detection in face recognition"

From input images shown seven eigenfaces calculated and from those images one average image is calculated. Combine set of normalized training set call as uk. Following equations represents this procedure.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

Figure 7. "eigenface images calculated from input images"

$$A^T A\mathbf{v}_i = \mu_i \mathbf{v}_i \qquad (4)$$

$$AA^T A\mathbf{v}_i = \mu_i A\mathbf{v}_i \qquad (5)$$

$$\mathbf{u}_l = \sum_{k=1}^{M} \mathbf{v}_{lk}\Phi_k, \qquad l = 1, \ldots, M \qquad (6)$$

This image gives variation in head size, three light conditions, and three head orientation.

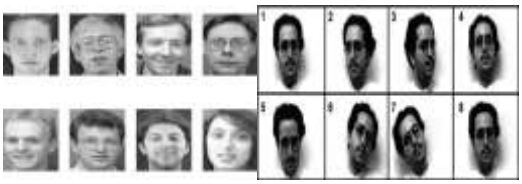

Figure 8. "Variation in head size, three light conditions, and three head orientation"

Following equation shows how to classify a face image by eigenfaces.

$$\omega_k = \mathbf{u}_k^T(\Gamma - \Psi) \qquad (7)$$

For each uk calculate class vector Ωk by taking average of Ω choose threshold maximum allowable distance Θ€. For each new face image calculate pattern vector Ω €k<Θ€ is minimum distance. €<Θ€ implies individual is from class vector Ωk €k>Θ€ but distance €k<Θ€ then image may be declared as unknown.

$$\epsilon_k^2 = \|(\Omega - \Omega_k)\|^2 \qquad (8)$$

$$\epsilon^2 = \|\Phi - \Phi_f\|^2 \qquad (9)$$

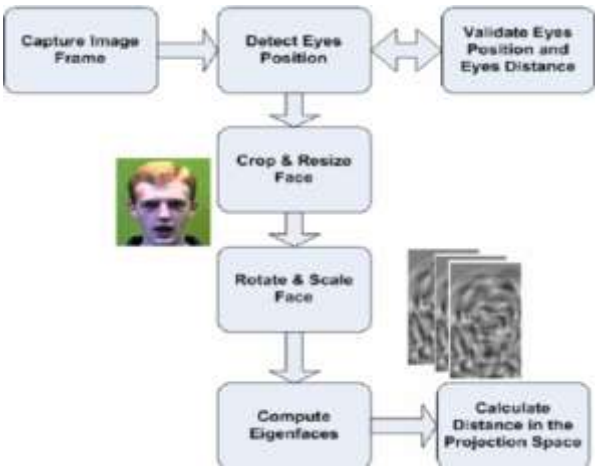

Figure 9. "Flow of eigenface algorithm"

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

If image is known then it will get added with original set of known faces.
Computation of the eigenfaces
Step 1: obtain face images I1, I2... IM (training faces)
(Very important: the face images must be centred and of the same size)
Step 2: represent every image Ii as a vector Gi
Step 3: compute the average face vector Y:
Y =1/MMi=1S Gi
Step 4: subtract the mean face:
Fi = Gi -Y
Step 5: compute the covariance matrix C:
C =1MMn=1S FnFTn= AAT (N2xN2 matrix)
Where A = [F1 F2 . . . FM] (N2xM matrix)
Step 6: compute the eigenvectors ui of AAT
The matrix AAT is very large --> not practical.
Step 6.1: consider the matrix AT A (MxM matrix)
Step 6.2: compute the eigenvectors vi of ATA
ATA vi = mi vi
What is the relationship between usi and vi?
ATA vi = mi vi => AAT Avi = m
i Avi =>CAvi = mi Avi or Cui = m
i ui where ui = Avi
Thus, AAT and ATA have the same eigenvalues
and their eigenvectorsare related as follows:
ui = Avi !!
Note 1: AAT can have up to N2 eigenvalues and eigenvectors.
Note 2: AT A can have up to M eigenvalues and
eigenvectors.
Note 3: The M eigenvalues of AT A (along with
their corresponding
eigenvectors) correspond to the M largest
eigenvalues of AAT (along
with their corresponding eigenvectors).
Step 6.3: compute the M best eigenvectors of AAT :
ui = Avi
(Important: normalize ui such that ||ui|| = 1)
Step 7: keep only K eigenvectors (corresponding to the
largest eigenvalues)

Following figure shows three layer linear networks for eigenface calculation. The symmetric weights ui are the eigen faces and the hidden units reveal the projection of the input image Φ onto the eigenfaces the output Φf is the face space projection of input image.

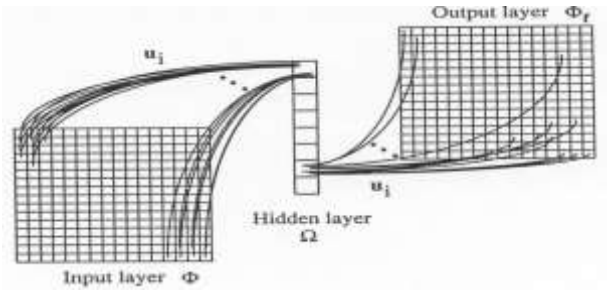

Figure 10. "3-layer linear network for eigenface calculation"

B. REST: (Representational State Transfer)

What is REST?
• REST means Representational State Transfer. (It is in some cases spelled "ReST".) It depends on a stateless, client-server, cacheable communications protocol and in virtually all cases, the HTTP protocol is utilized.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

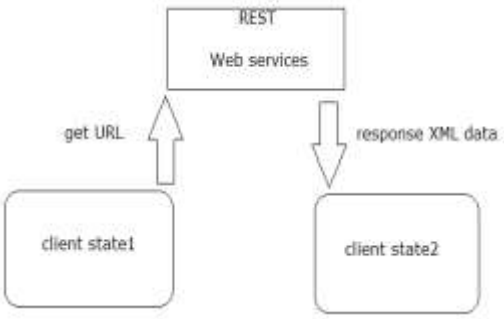

Figure 11. "REST"

- REST designed the network application on the basis of architecture style. The thought is that, as opposed to utilizing complex systems, for example, CORBA, RPC or SOAP to associate between machines, straightforward HTTP protocol is used to make communication between machines.
- In numerous ways, the World Wide Web itself, in view of HTTP, can be seen as a REST-based design.
- REST full applications utilize HTTP requests to post data(create and/or update), read data (e.g., make queries), and delete data. Along these lines, REST utilizes HTTP for every one of the four CRUD (Create/Read/Update/Delete) operations.
- REST is a lightweight other option to systems like RPC (Remote Procedure Calls) and Web Services (SOAP, WSDL, et al.). Afterward, we will perceive the amount more simple REST is.
- Despite being simple, REST is completely highlighted; there's fundamentally nothing you can do in Web Services that isn't possible with a RESTful architecture.
- REST is not a "standard". There will never be a W3C recommendation for REST, for example. And while there are REST programming frameworks, working with REST is so simple that you can often "roll your own" with standard library features in languages like Perl, Java, or C#.

IV. PROPOSED SYSTEM

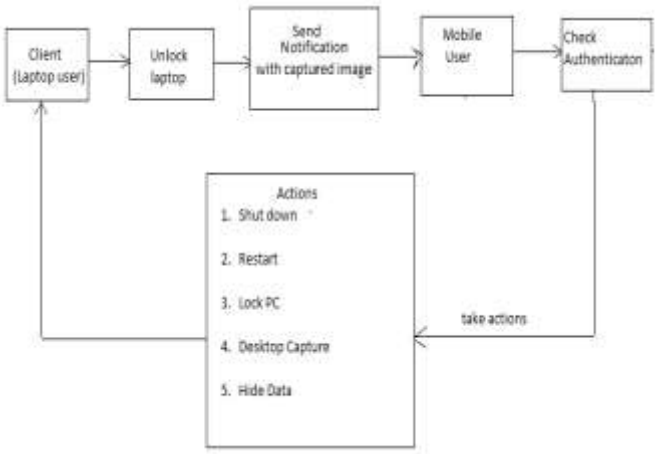

Figure 12 "proposed system block diagram"

Our proposed system is useful for the security purpose. It will work if anybody tries to unlock the laptop, it will act as a trigger to the camera and capture the image in background and send it with the notification to the mobile user. If anybody enters wrong password it also notify that someone is trying to access the laptop etc. Mobile user receives the notification and check user is valid or invalid. Take the action on the basis of authentication. Mobile user can take many actions like Shutdown, Restart, Lock PC, Desktop capture, Hide data. In desktop capture mobile user can see the runtime operations performed by desktop client. That security is given in our system.

Implementation of proposed system:

- Database Manager:

This module will help to handle all database related activity. All the SQL queries will be taken care in this module. A database connection polling system will be present to avoid repeatedly opening and closing database connection. The

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

JDBC driver manager ensures that the correct driver is used to access each data source. The driver manager is capable of supporting multiple concurrent drivers connected to multiple heterogeneous databases.

- Communication Manager:

Communication Manager will handle the client server communication part. We have used HTTP Standard communication technique for communication. It relies on a stateless, client-server, cacheable communications protocol -- and in virtually all cases, the HTTP protocol is used. The idea is that, rather than using complex mechanisms such as CORBA, RPC or SOAP to connect between machines, simple HTTP is used to make calls between machines.

- System Configuration:

The configuration manager which will be holding IP address of the entire client will be singleton in nature. The singleton pattern is a design pattern that restricts the instantiation of a class to one object. This is useful when exactly one object is needed to coordinate actions across the system.

- Socket Programming:

Sockets provide the communication mechanism between two computers using TCP. A client program creates a socket on its end of the communication and attempts to connect that socket to a server. When the connection is made, the server creates a socket object on its end of the communication. The client and the server can now communicate by writing to and reading from the socket.

V. RESULT

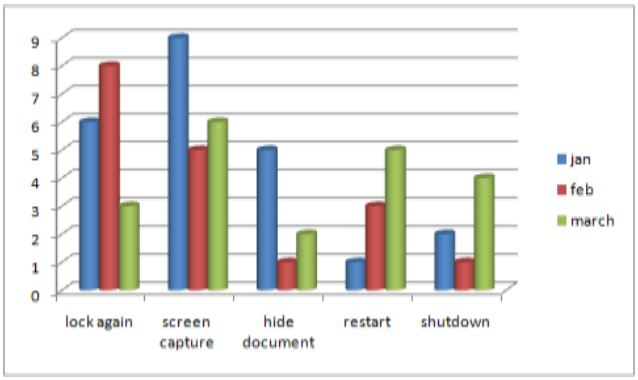

Figure 13 “count of actions taken”

We have designed an application to secure laptop. For that we have implemented operations like lock again, screen capture, and hide document, restart, and shutdown. This graph shows that how many times these actions are taken by user in which month. So suppose lock again action is taken six times in January, eight times in February, and three times in march for securing particular user laptop.

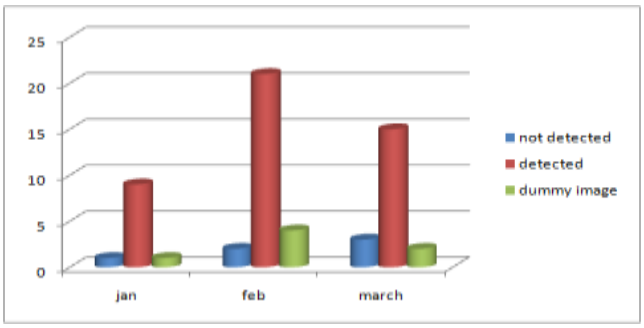

Figure 14 “face detection count”

We designed an application to secure laptop. For that we used face detection. That face detection count means how many times system is successfully able to detect face of a person in front of laptop. So in January one time the face is not detected eight times the face is detected and one time dummy image is send. So we have detected the face or action each time successfully. Because when face is not detected dummy image get send by system so the notification is sensed each and every time.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

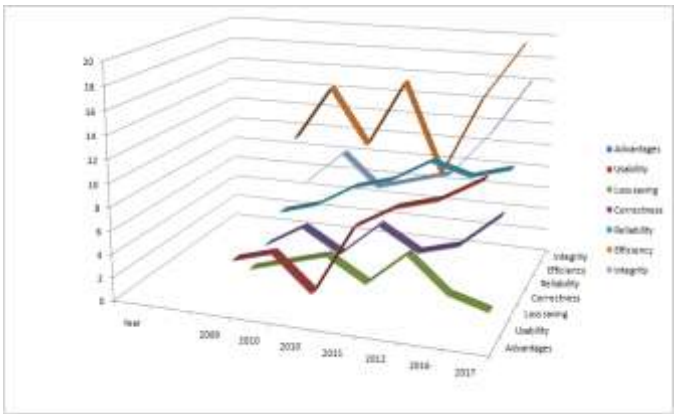

Figure 15 “comparison with old systems”

This graph shows comparison between system of year 2009, 2010, 2011, 2012, 2016, and 2017. It compares through some parameters like advantages, usability, loss saving, correctness, reliability, efficiency, and integrity.

VI. CONCLUSION

Our proposed system guarantees all the quality as for security. The framework parameters are check with feasibility. Our system provides complete security to gadget with advanced technology of face detection to lock/unlock laptop. So the laptop owner got total security to the laptop.

REFERENCES

[1] http://www.ijtra.com/view/smart-lock-a-locking-system-using- bluetooth -technology-camera-verification.pdf (2016)
[2] Potts, Josh, and SomsakSukittanon. ”Exploiting Bluetooth on Android mobile devices for home security application.” Southeastcon, 2012 Proceedings of IEEE. IEEE, 2012.
[3] Piyare, R., and M. Tazil. ”Bluetooth based home automation system using cell phone.” Consumer Electronics (ISCE), 2011 IEEE 15th International Symposium on. IEEE, 2011.
[4] Kaur, Inderpreet. ”Microcontroller based home automation system with security.” International journal of advanced computer science and applications 1.6 (2010)
[5] M. Turk and A. Pentland, "Eigenfaces for Recognition", Journal of Cognitive Neuroscience, vol.3, no. 1, pp. 71-86, 1991, hard copy
[6] http://www.face-rec.org/algorithms/PCA/jcn.pdf