International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

Two Fold Password Security Using Face Recognition and NFC

[1]Saylee Gharge, [2]Vishal Changlani, [3]Jatin Wadhwani, [4]Tarun Rohra, [5]Akshay Ghogare
[1]Associate Prof, Department of Electronics and Telecommunication Engineering, VESIT, Mumbai.
[2,3,4,5] B.E Student, Department of Electronics and Telecommunication Engineering, VESIT, Mumbai.

Abstract

Passwords are used to secure confidential information. If a password is hacked, it leads to loss of important data. Many times, it is really difficult to find the culprit. It may also happen that the password generator himself manipulates the data of importance for an organization. Password security is an important aspect to rule out any eaves dropping. Organizations like the defense units, central bank, research institutes store highly confidential data. In such cases, the responsibility of safeguarding data should be with few key persons rather than a single person safeguarding it. This require password to be split among the password holders to ensure that they all together safeguard it and absence of even any one of them rules out any access to the data. Also the presence of valid individuals should be ensured. It may happen that someone steals the password from a valid password holder and misuse it. To ensure this, biometrics like face recognition should be the first part of authentication. With this base concept down, the project aims to build a system which ensures both password division and its safety. The project is a prototype which combines two independent concepts, 'face recognition' and 'Near Field Communication (NFC)'.

Keywords-Face Recognition, Near Field Communication, Eigen Faces, Shamir's Secret sharing.

1. Introduction

Theft has always been an issue for mankind from the dawn of history. Earlier it was primarily for monetary gains i.e. theft of liquid cash, jewelry or any such personal belonging. But in today's digital world it has acquired a new dimension. It is not limited to just finance. Due to internet, almost every digital information is potentially at risk. The security measures which are implemented can range from simple password protection to sophisticated one time pad. Any security can never be fully secure. For every action which is taken by a security community there are counter – attacks by antagonist community say Hackers.

The 3 key objectives, which are the heart of information, also known as the CIA triad, are Confidentiality, Integrity and Availability. Two additional concept Authenticity & accountability provide complete picture. Cryptography is widely used, the block cipher work on principle of substitution followed by a permutation which is done iteratively. The most popular encryption standards are DES, its variants, AES to name a few. There are two types of cryptographic system: The private key (symmetric) and public key (asymmetric) systems. Private key system uses a single key for encryption & decryption and is capable for achieving data confidentiality. Public key systems on other hand use 2 keys. Public key which is known to all & private key one of the added advantages of this system is that private key of sender can serve as digit signature as receiver already has sender's public key. Thus, ensuring non-repudiation. In both systems more emphasis is on data, If the keys are found out by any means then the entire purpose gets detected[5].

To protect a confidential file one can encrypt it with an encryption key but how can one protect encryption key? Mostly by encrypting it with other encryption key. It will complicate the problem rather than solving it.

In both the cases, solutions available are too complex to implement. So there is need of simple and a robust method which can cater to such requirements. Storing confidential information is essentially storing data. Storing data is essentially protecting numeric key. It may also happen that the password generator himself manipulates the data of importance for an organization. Organizations like the defense units, central bank, research institutes store highly confidential data. In such cases, the responsibility of data is better left with few key persons rather than a single person safeguarding it. This require password to be split among the password holders to ensure that they all together safeguard it and absence of even any one of them rules out any access to the data.

To avoid security breach even in this system, biometrics can be added as authentication of persons holding the password. Biometrics is one of the most optimized techniques in the field of security. Authentication of individuals based on face recognition, fingerprint recognition, iris recognition, etc. are common techniques in biometrics. However, face recognition is most widely used techniques among all[3]. With this base concept down, the project aims to build a system which ensures both password division and its safety. Face recognition as a first factor in securing password and storing passwords electronically on ‘Near Field Communication (NFC)’ cards as second factor.

2. Proposed Model

The project is a two-fold security system. The encoding consists of two steps. The first step requires all the password holders to store their images in a computer forming an image database. This is done for identity verification. For the second step, the admin needs to enter into the system, a password which is to be shared among the participants. The controller unit of the system divides this password internally into the number of pieces equal to the number of holders. These individual pieces will be written electronically into the NFC cards of the holders by the NFC writer.

The decoding process involves all the password holders (or a minimum threshold number) to be present. The camera first captures the images of all the participants and compares them with the database formed earlier. If the identities are matched, the system prompts the password holders to generate the password. The NFC cards are read by the NFC reader one by one. The individual pieces are intercepted by the controller unit and the password is generated internally by using Shamir's secret sharing algorithm. If this password matches with the one entered by the admin the lock is opened. This verifies the validity of the NFC cards. Also, the admin cannot access the lock individually because the decoding requires individual pieces of the password and not complete password at a time, and before that image verification of all password holders is required. This system ensures the password sharing and its safety.

Encoding Process

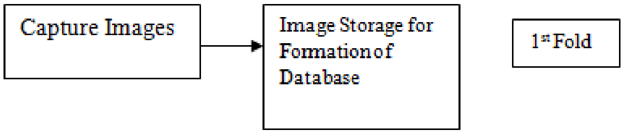


Fig.1 Formation of Image Database

Fig.1 shows the process involved in the formation of image database. Images of all password holders will be captured and stored in database for further validation.

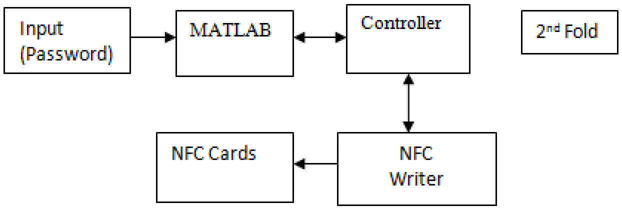


Fig.2 Password Distribution

Fig.2 indicates password distribution scheme. The password entered with keypad gets divided among all password holders and gets stored in their respective NFC cards by NFC Writer. The display device shown in Fig.2 guides the above process.

Decoding Process

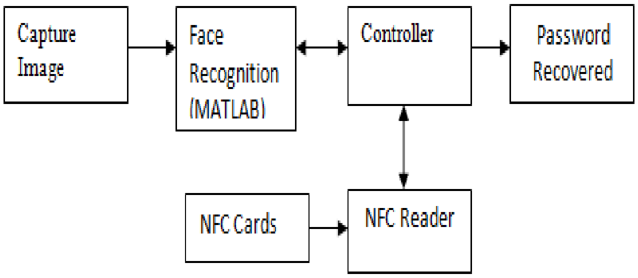


Fig.3 Block Diagram to Access the Data

Fig.3- shows the decoding process. The camera takes images of the password holders and compares it with database which was the part of encoding process. If all these images match with database then only NFC cards will be read by the NFC reader. If the password recovered by this process is valid then the important information (Virtual domain e.g. File) can be accessed through MATLAB.

3. Related Work

Passwords need to be protected from being compromised. Hence, passwords not supported by two fold security are generally considered last line of defence from prying eyes[1]. This is obviously not desirable. There is a website, 'How Secure Is My Password' which predicts how long will a computer processor take to hack a given password using brute-force attack and also give suggesstions on how to make the password more secure. The typical answer obtained is '45 thousand years'. However, there are also many password breaking tools. These tools have algorithms specifically designed to detect password. Brutus is an example of such software [2]. Two step verification is therefore an obvious choice. Hence, most popular websites use 'one time pad', meaning a numeric key is sent as an SMS to the user everytime a login is made. The user must enter this key for successful login.

The project uses face recognition as the first step in authentication. Identifying people on the basis of their facial appearance is a natural trait of humans. Face recognition started from simple comparison of 2D image matrices to involving techniques like PCA, ICA, Neural Networks and their combination to reduce the effects of illumination, pose variations, camera specifications, etc. Sophisticated techniques like 3D morphological mapping of face are incorporated in systems today. These systems estimate face characteristics in case of poor illumination, construct 3D view of facial structure based on various poses of the individual in database. These systems perform real time face tracking, its detection and its authentication. These systems are tested on standard database like Yale B database, AT&T face database, etc to obtain measure of their robustness[3].

The project uses electronic storage of passwords on NFC cards. The passwords are not visible. Also they can be interpreted by an NFC sensor only when the card is in the small range of within 10 centimeters. NFC is widely used emerging technology by credit card companies like MasterCard, VISA, etc. Google Wallet is an example of contactless paying method. NFC smartphones use NFC to initiate Bluetooth data sharing, contactless payment, etc. NFC cards, tags, stickers are interactive things used to store shortcut commands for smartphone (e.g. the phone screen brightness should dim when placed on an NFC sticker on the bedside table; this command is stored in the sticker)[4]. Thus NFC cards can be used as memory to store passwords and also secure them.

4. Face Recognition

Access to various physical or virtual domains can be provided by authenticating a person on the basis of signature, password, keys, tokens etc. These can be forged very easily. Inclusion of a biometric based technique for authentication is always advantageous and raises level of security. Biometric technologies can be based on behavioral characteristics like keystroke dynamics, signature or physiological characteristics like face, iris, fingerprint .Face recognition has certain advantage over other methods[6] .Various face recognition techniques are evaluated over past years like FERET evaluations [7,8], FRVT 2000 [9], FRVT 2002 [10] and the FAT 2004 [11].The major problems faced by any face recognition system can be categorized as illumination variation, pose variation and age variation[12].

Various steps in implementation of face recognition in MATLAB are:

4.1 Image Acquisition

The image database of 4 members consisting of 9 images of each was formed. The images were taken from webcam in YUY2_640x480 format.

4.2 Face Detection

Faces were detected using viola-jones algorithm [13,14] and were resized as 75x75.

4.3 Image Preprocessing

For improving accuracy, preprocessing like contrast enhancement and homomorphic filtering was used[17].

4.3.1 Contrast Enhancement

To enhance the contrast of a grayscale image techniques like histogram equalization(histeq), adaptive histogram equalization(adapthisteq) or imadjust can be used. The imadjust function improves contrast by saturating 1% of data at high and low intensities of input data. The histeq transforms input level so that they approximate to a default uniform distribution. The adapthisteq operates on small regions unlike histeq which operates on entire image. Better results were obtained by using imadjust[18].

4.3.2 Homomorphic Filtering

To reduce illumination related effects homomorphic filtering was used. It removes multiplicative low frequency illumination noise by converting it into additive noise using log operator and deploying high pass filter. Order 8 Butterworth filter was used with 15 as threshold.

4.4 Feature Extraction

Eigen faces technique which is based on principal component analysis (PCA) [16] was used for feature extraction. This method requires grayscale images cropped only to show faces which must be frontal with more or less uniform illumination.

4.4.1 Training Phase:

Here, image dimension = N x N = 75x75
Total Number of images = M =36

The training can be done as follows:

1. The images are loaded into an matrix (st.data)
2. The mean of input face images is calculated (avImg)
3. Mean face is subtracted from each face image to get mean shifted image (Peculiar characteristics that is st.dataAvg)

4. Every mean shifted image is converted into a column vector of size ((N x N) x 1) and a matrix A is formed which contains these mean shifted images Thus size of A is ((N x N) x M).If eigenvectors of A are to be calculated there would be N x N eigenvectors.
5. A co-variance matrix, C is calculated as A^T x A so size of C would be M x M. Eigenvectors of matrix C are calculated . As a result of covariance matrix C, dimensionality reduction is accomplished
6. The eigenvectors are projected to a higher dimension space by multiplying with matrix A to give Vlarge. Vlarge will contain M eigenvectors.
7. Each column of Vlarge is reshaped as N x N to give Eigenfaces. Only principal eigenfaces are retained which cover about 90% of variation.
8. Each of the database image is expressed as linear combination of constant weight multiplied by corresponding eigen face.

Input face1 = $w_{11}E_1 + w_{12}E_2 + w_{13}E_3 + ...+w_{1e}E_e$
Input face2 = $w_{21}E_1 + w_{22}E_2 + w_{23}E_3 + ...+w_{2e}E_e$
.
.
.
Input faceM = $w_{M1}E_1 + w_{M2}E_2 + w_{M3}E_3 + ... +w_{Me}E_e$

Here, e is the number of principal eigenfaces.

9. The weights can be calculated as
w_{11}=(Input face 1 x Eigenface 1)
.
.
.
w_{Me}= (Input face M x Eigenface e)

4.4.2 Testing Phase

1. Capture the image of person requiring access.
2. Perform same preprocessing and filtering as done for images in database.
3. Subtract the mean face.
4. Obtain weight matrix.
5. Find Euclidean distance between weight matrix and the weight matrices of individual images in database.
6. If Euclidean distance falls below a certain threshold(set heuristically), then the image will be authenticated as that of a valid user else access will be denied.[15]

5. NFC

In order to store password, we either try to memorise it in mind but there are chances of forgetting it or we scribble it down somewhere which involves a risk of eavesdropping. So wouldn't it be wonderful if password is stored such that it can't be seen e.g. in RF field and distance between reader and writer is limited to few cms.

All these are features of NFC (Near Field Communication) devices e.g. (NFC enabled smartphones, NFC Tags, NFC Cards).

Abbreviated as NFC, N*ear* F*ield* C*ommunication* is a standards-based, short-range wireless connectivity technology that enables convenient short-range communication between electronic devices. The underlying layers of NFC technology are ECMA, ISO and ETSI standards [19].

MiFare classic cards introduced in 1994 were used to store passwords.
MIFare Classic card employ a proprietary protocol ISO/IEC 14443A but is compliant to not all but some parts of it and with an NXP proprietary security protocol for authentication and ciphering [20].

It offers 1KB of data storage, splitted into 16 sectors; each sector is protected by two different keys, called KeyA and KeyB. The encryption used by the MIFARE Classic card is of 48 bit key. Each key can be programmed to allow operations such as reading, writing, etc.

6. Adafruit's PN532 Reader/Writer

The PN532 is a highly integrated transceiver module for contactless communication at 13.56 MHz based on the 80C51 microcontroller core and has antenna with 10cm (4 inch) range. It supports 6 different operating modes out of them one is ISO/IEC 14443A which is implemented by NFC cards.

The PN532 NFC chip offers three different communication interfaces to the microcontroller controlling it. It can communicate using asynchronous serial communication using a universal asynchronous receiver-transmitter (UART).
It can also use two forms of synchronous serial communication, Serial-Peripheral Interface (SPI) or Inter-Integrated Circuit communication (I2C)[22].

SPI is a point-to-point connection with data in and data out on separate lines. SPI is simple to implement, potentially very fast(10-20Mbps) whereas I2C is complex when it comes to implementing also speed obtained is upto 1Mbps for limited devices.

SPI has shortcoming that multiple devices require multiple lines while I2C requires only two lines for multiple devices.

Considering the specifications and requirement, SPI mode was chosen. This PN532 breakout board is compatible with Arduino with the help of level shifter IC [21].

7. SHAMIR'S SECRET SHARING ALGORITHM

Consider, for example, a firm that digitally signs all its cheque. If each executive is given a copy of the company's secret signature key, the system is convenient but easy to misuse. If the cooperation of all the company's executives is necessary in order to sign each cheque, the system is safe but inconvenient.

One of the solution will be that a certain minimum threshold number of users be present in order to sign a check. This is what Shamir's Secret Sharing Algorithm facilitates. This threshold value will be subjective in nature. An unfaithful executive must have at least threshold number of accomplices in order to forge the company's signature in this scheme.

Shamir's Secret Sharing algorithm generalizes the problem to one in which the secret is some data D (e.g., the safe combination) and in which non-mechanical solutions (which manipulate this data) are also allowed.

Here goal is to divide D into n pieces D_1,..... D_n in such a way that:
(1) Knowledge of any k or more D_i pieces makes D easily computable;
(2) Knowledge of any k- 1 or fewer D_i pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).
Such a scheme is called a (k, n) threshold scheme.
By using a (k, n) threshold scheme with n = 2k- 1 we get a very robust key management scheme: We can recover the original key even when n/2 = k- 1 of the n pieces are destroyed, but our opponents cannot reconstruct the key even when security breaches expose n/2 = k- 1 of the remaining k pieces.

7.1 Algorithm:

Suppose (k,n) threshold scheme is to be used to share secret S, without loss of generality assumed to be an element in a finite field F of size P where $0 < k <= n < P$; S<P and P is a prime number.

Choose at random k-1 positive integers $a_{1,}\ldots,a_{k-1}$ with a_i<P and let a_0=S.
Build the polynomial $f(x)=a_0+a_1x+a_2x^2+a_3x^3+\ldots\ldots+_{ak-1}x^{k-1}$.
Let us construct any n points out of it, for instance set i=1… n to retrieve (i,f(i)).

Every participant is given a point (an integer input to the polynomial, and the corresponding integer output).
Given any subset of k of these pairs, we can find the coefficients of the polynomial using interpolation. The secret is the constant term a_0.

Some of the useful properties of this (k, n) threshold scheme (when compared to the mechanical locks and keys solutions) are:

(1) The size of each piece does not exceed the size of the original data.
(2) When k is kept fixed, D pieces can be dynamically added or deleted (e.g., when executives join or leave the company) without affecting the other Di pieces. (A piece is deleted only when a leaving executive makes it completely inaccessible, even to himself.)
(3) It is easy to change the Di pieces without changing the original data D-all we need is a new polynomial q(x) with the same free term. A frequent change of this type can greatly enhance security since the pieces exposed by security breaches cannot be accumulated unless all of them are values of the same edition of the q(x) polynomial[23].

7.2 Shamir's Example:

Suppose secret be 1342(S=1342)
Let total number of participants be 4 (N=4)
Let the threshold value be 4 (K=3)
At random; (K-1) numbers are 166 &94.
Therefore polynomial to produce secret shares is
f(x)=1342+166x+94x2
Four points are constructed, Dx-1=(x,f(x)) from the polynomial;
D0=(1,1602); D1=(2,2050); D2=(3,2686);D3=(4, 3510);
A different single point will be given to each participant.

Reconstruction:

Since k(threshold)=3. So choose 3 points would be as follows:
$(x_0,y_0)=(2,1942);(x_1,y_1)=(4,3402);(x_2,y_2)=(5,4414)$

Reconstruction of password involves use of Lagrange Basis.

$$l_0 = \frac{x-x_1}{x_0-x_1} \times \frac{x-x_2}{x_0-x_2} = \frac{x-3}{1-4} \text{ x } \frac{x-4}{1-4} = \frac{x^2-7x+12}{6}$$
$$l_1 = \frac{x-x_0}{x_1-x_0} \times \frac{x-x_2}{x_1-x_2} = \frac{x-1}{3-1} \text{ x } \frac{x-4}{3-4} = \frac{x^2-5x+4}{-2}$$
$$l_2 = \frac{x-x_0}{x_2-x_0} \times \frac{x-x_1}{x_2-x_1} = \frac{x-1}{4-1} \text{ x } \frac{x-3}{4-3} = \frac{x^2-4x+3}{3}$$

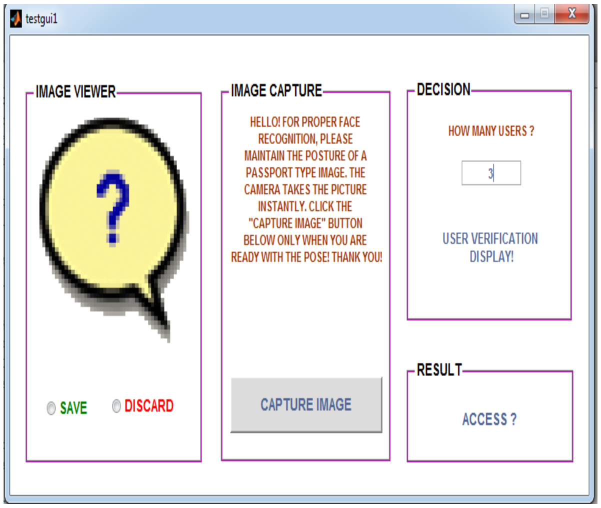
Therefore

$$f(x) = \textstyle\sum_{j=0}^{2} y_j \times l_j(\text{x})$$
$$= 1342 + 166x + 94x^2$$

Above equation are compared with equation at encoding time. If both are same then Shamir's secret sharing algorithm is properly implemented with free coefficient as secret password.

8. Implementation and Results

This GUI is invoked when the users tries to access the file.



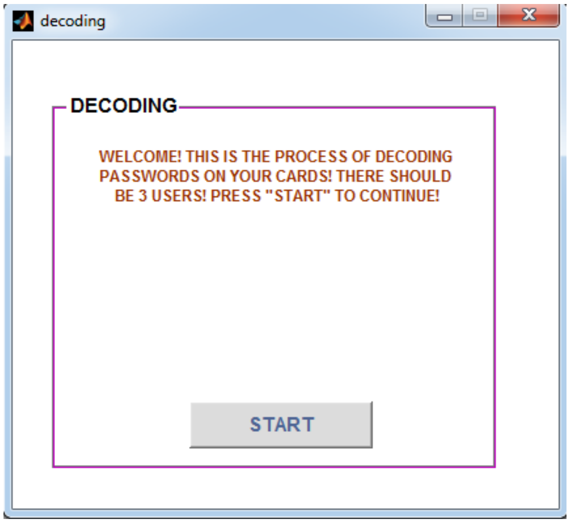
HELLO! FOR PROPER FACE RECOGNITION, PLEASE MAINTAIN THE POSTURE OF A PASSPORT TYPE IMAGE. THE CAMERA TAKES THE PICTURE INSTANTLY. CLICK THE "CAPTURE IMAGE" BUTTON BELOW ONLY WHEN YOU ARE READY WITH THE POSE! THANK YOU!

USER VERIFICATION DISPLAY!

Fig.4 Main GUI

Fig.4 shows the layout of Main GUI

This GUI shown in fig 5 is invoked when all the users are verified. The successful decoding of NFC cards will open the locked file.



WELCOME! THIS IS THE PROCESS OF DECODING PASSWORDS ON YOUR CARDS! THERE SHOULD BE 3 USERS! PRESS "START" TO CONTINUE!

Fig 5 NFC GUI

The results are obtained under following conditions:
1.The faces must be frontal with no weird expressions.
2. Illumination should be more or less uniform.

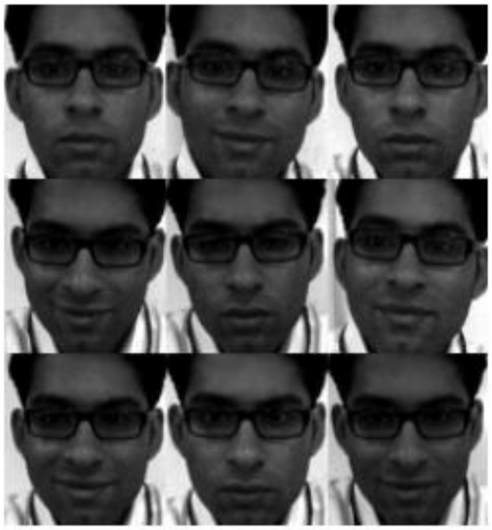


Fig.6 Contrast Enhanced Images

Fig.6 shows contrast enhanced image of one of the class of database (one among four member). The contrast enhancement is done using imadjust function.

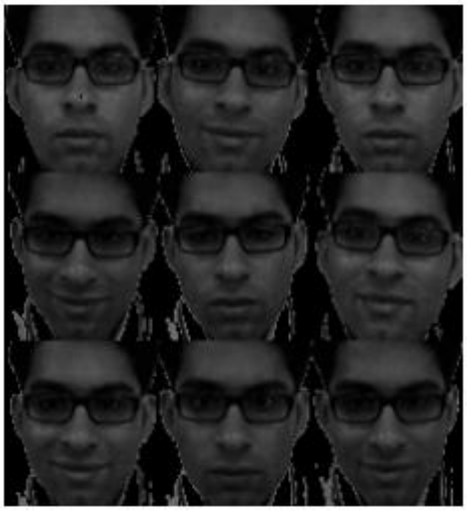


Fig.7 Filtered Images

Fig.7 shows the image of class shown in fig.4 filtered using homomorphic filter to reduce effects of non- uniform illumination.

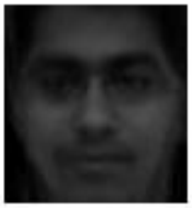


Fig.8 Mean Face

Fig.8 shows the face obtained by taking mean of all the 4 classes in the database.

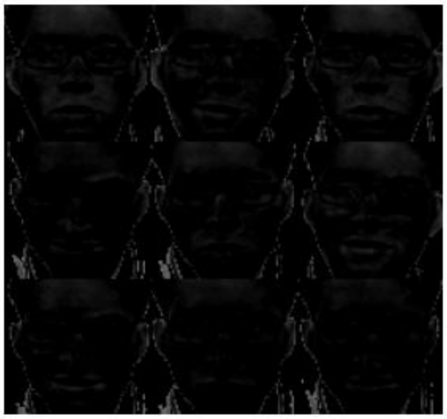


Fig.9 Mean shifted Image

Fig.9 shows faces obtained by subtracting mean from the images of class shown in fig,4 . The mean shifted image signify the peculiar characteristics of a class. The eigenvectors are calculated from mean shifted images.

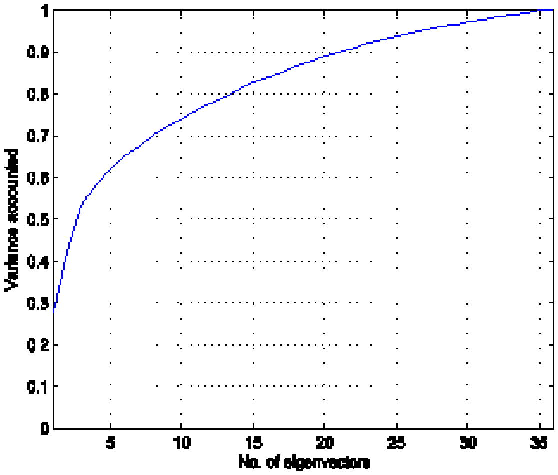


Fig.10 Optimum Number of EigenVectors

Fig.10 shows the optimum number of eigenvectors or eigenfaces that should be selected so that 90% of variance is accounted. In this case 90% variance is accounted by 21 eigenfaces.

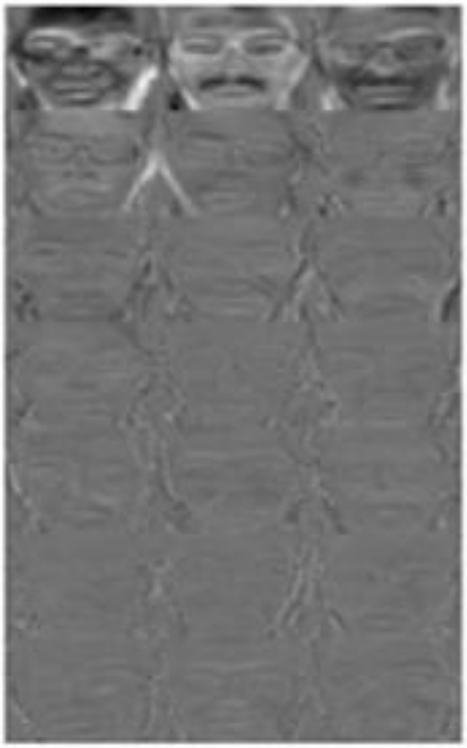
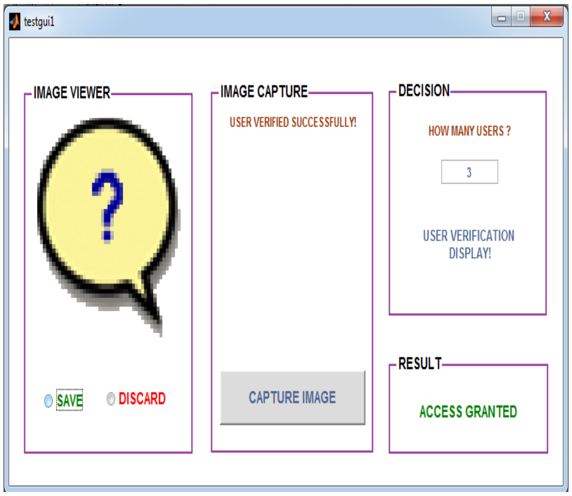


Fig.11 Principal Components

Fig.11 shows the important eigenfaces or principal components which are retained.



USER VERIFIED SUCCESSFULLY!

HOW MANY USERS ?

3

USER VERIFICATION DISPLAY!

ACCESS GRANTED

Fig.12 Successful Recognition

Fig.12 shows the snapshot of GUI in case of successful face recognition

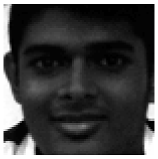


Fig.13 Test Image

Fig.13 shows an image which is not a class of database i.e an unknown person.

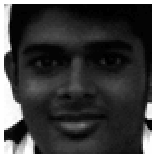


Fig.14 Contrast Enhanced Image

Fig.14 shows the contrasr enhanced image of fig.10 using imadjust function.

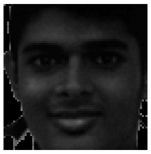


Fig.15 Filtered Image

Fig.15 shows filtered image after subjecting fig.10 image to homomorphic filter so that non-uniform illumination effects are reduced.

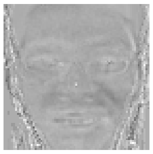


Fig.16 Reconstructed Image

Fig.16 shows reconstructed image of test face using principal components.

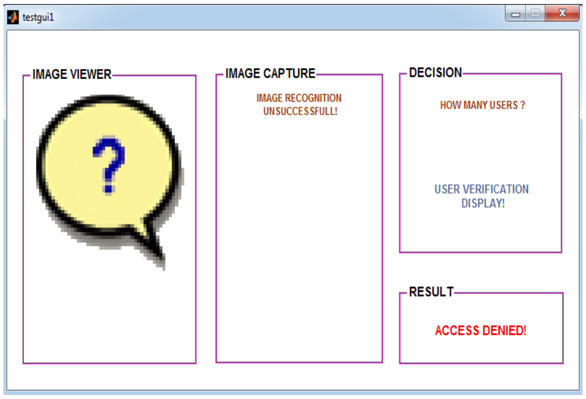


IMAGE RECOGNITION UNSUCCESSFULL!

HOW MANY USERS ?

USER VERIFICATION DISPLAY!

ACCESS DENIED!

Fig.17 Unsuccessful Recognition

Fig 17 shows the snapshot of GUI in case of unsuccessful face recognition

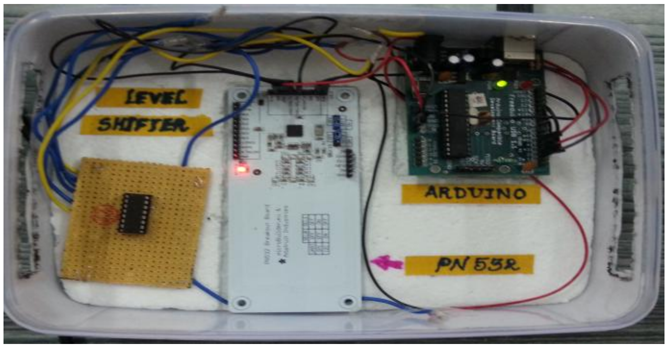


Fig.18 Circuit Diagram

Figure 18 shows the actual circuit diagram

The tests were performed on 60 images out of which 30 images were known faces and remaining 30 were unknown. Performance was evaluated on basis of following parameters-

FAR(False Acceptance Ratio)- It is the rate at which an imposter is granted access by the system.

$$FAR = \frac{\text{No of times an imposter is granted access}}{\text{Total no of unknown test faces}} * 100$$

FRR(False Rejection Ratio)- It is the rate at which an authorized person is denied access by the system.

$$FRR = \frac{\text{No of times an valid person is denied access}}{\text{Total no of known faces}} * 100$$

FMR(False Matching Ratio)-It is the rate at which an authorized person is matched to another person.

$$FMR = \frac{\text{No of improper matching}}{\text{Total no of known faces}} * 100$$

The results obtained by varying threshold are quantized in table 1

Table 1- Performance Parameters

Threshold	FAR %	FRR %	FMR %	Success Rate %
30	0	6.66	10	83.33
32	6.66	6.66	10	76.67
34	6.66	6.66	10	76.67
36	6.66	6.66	3.33	83.34
38	**6.66**	**3.33**	**3.33**	**86.67**
40	13.33	3.33	3.33	80.01

Thus, the optimum results were obtained by selecting threshold as 38.

False Acceptance Ratio (FAR) = 6.66%
False Rejection Ratio (FRR) = 3.33%
False Matching Ratio (FMR) = 3.33%
Success Rate(SR)=86.67%

For password division using Shamir secret sharing algorithm, the password set during encoding is compared with the password obtained during decoding. Both the passwords match correctly. However, the password has a limitation that it should be numeric and should be either 4 or 5 digit password.

9. Conclusion and Future Scope

For face recognition, better results can be obtained using more sophisticated methods like fisher faces, 3D morphological modeling of face, using combination of neural networks and PCA, etc. Shamir secret sharing algorithm can be made for numeric password of any length and password can be randomly generated number instead of taking from user.

10. REFERENCES

[1] http://www.cnet.com/how-to/the-guide-to-password-security-and-why-you-should-care/

[2] http://resources.infosecinstitute.com/10-popular-password-cracking-tools/

[3] Jain, Anil K., and Stan Z. Li. *Handbook of face recognition*. Vol. 1. New York: springer, 2005

[4] http://nfc-forum.org/what-is-nfc/what-it-does/

[5] William, Stallings, and William Stallings. *Cryptography and Network Security, 4/E*. Pearson Education India, 2006.

[6] Rabia Jafri and Hamid R. Arabnia,’’A Survey of Face Recognition Techniques,’’Journal of Information Processing Systems, Vol.5, No.2, June 2009

[7] P. J. Phillips, H. Moon, P. J. Rauss, and S. A. Rizvi, "The FERET Evaluation Methodology for Face Recognition Algorithms," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.22, pp.1090-1104, 2000

[8] P. J. Phillips, H. Wechsler, J.Huang, and P. J. Rauss,"The FERET database and evaluation procedure forface-recognition algorithm," Image and Vision Computing, Vol.16, pp.295-306, 1998.

[9] D. Blackburn, J. Bone, and P. J. Phillips, "Face recognition vendor test 2000," Defense Advanced Research Projects Agency, Arlington, VA, Technical report A269514, February 16, 2001.

[10] P. J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone, "Face Recognition Vendor Test (FRVT 2002)," National Institute of Standards and Technology, Evaluation report IR 6965, March, 2003.

[11] K. Messer, J. Kittler, M. Sadeghi, M. Hamouz, A. Kostin, F. Cardinaux, S. Marcel, S. Bengio, C. Sanderson, J. Czyz, L. Vandendorpe, C. McCool, S. Lowther, S. Sridharan, V. Chandran, R. P. Palacios, E. Vidal, L. Bai, L. Shen, Y. Wang, Y.-H. Chiang, H.-C. Liu, Y.-P. Hung, A. Heinrichs, M. Müller, A. Tewes, C. v. d. Malsburg, R. P. Würtz, Z. Wang, F. Xue, Y. Ma, Q. Yang, C. Fang, X. Ding, S. Lucey, R. Goss, H. Schneiderman, N. Poh, and Y. Rodriguez, "Face Authentication Test on the BANCA Database," in 17th International Conference on Pattern Recognition, Vol.4. Cambridge, UK, 2004, pp.523-532.

[12] X. Q. Ding and C. Fang, "Discussions on some problems in face recognition," in Advances In Biometric Person Authentication, Proceedings, Vol. 3338, Lecture Notes In Computer Science: Springer Berlin / Heidelberg, 2004, pp.47-56.

[13] P. Viola and M. J. Jones, Robust real-time face detection, International Journal of Computer Vision, 57 (2004), pp. 137–154 http://dx.doi.org/10.1023/B:VISI.0000013087.49260.fb

[14] http://angeljohnsy.blogspot.com/2013/07/face-detection-matlab-code.html (face detection)

[15] http://matlabsproj.blogspot.in/2012/06/face-ecognition-using-eigenfaces_11.html (face recognition)

[16] http://www.cs.otago.ac.nz/cosc453/student_tutorials/principal_components.pdf (principal component analysis, eigenvectors)

[17] http://thelearningsquare.in/ (homomorphic filter)

[18] https://homepages.cae.wisc.edu/~**ece533**/project/f06/**sc**hreiner.ppt (image processing)

[19] http://www.webopedia.com/TERM/N/Near_Field_Communication.html

[20] https://learn.adafruit.com/adafruit-pn532-rfid-fc/mifare

[21] https://learn.adafruit.com/adafruit-pn532-rfid-fc/breakout-wiring

[22] JEPSON, BRIAN, DON COLEMAN, and TOM IGOE. "Beginning NFC Near-Field Communication with Arduino, Android, and PhoneGap Jepson." (2012).

[23] Rivest, Ronald L., Adi Shamir, and Yael Tauman. "How to share a secret." *Communications of the ACM*, 1979.