VOL. 8, NO. 11, NOVEMBER 2013 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

HUMAN RECOGNITION USING BIOMETRIC AUTHENTICATION SYSTEM

M. Jasmine Pemeena Priyadarsini[1], K. Murugesan[2], Srinivasa Rao Inbathini[1] and A. Arun Kumar[1]
[1]School of Electronics Engineering, VIT University, India
[2]Sree Sastha Institute of Engineering and Technology, Chennai, India
E-Mail: jasmin@vit.ac.in

ABSTRACT

A model is designed to work for Face recognition, Finger Print recognition, and Signature recognition for recognizing the individual person test images out of training images. There are various methods for recognition and images need to have good sensor quality. A Fisher LDA approach which produces a set of Eigen faces and fisher faces to obtain projected images has been implemented. In this paper both PCA and LDA techniques have been used. Minutiae matching algorithm which after several preprocessing stages produces minutiae points on finger print has been implemented. The offline signature is taken for verification and recognition system; Global features are extracted and matched. A set of fisher images are projected and reconstructed. The test image is also projected and a minimum error reconstruction value is calculated. If error is less than a threshold value, then it recognizes the face from the database. A set of false minutia points are extracted and efficiently the minutia points are removed from the finger and made into a template and verification is done with other template for producing percentage score of the matching template. After extracting Global features from the signature, the same steps are applied for the input signature and matched with the database of signature images. Multimodal biometric authentication is applied for verification and identification of humans where same the human being database is matched with the input image.

Keywords: authentication system, LDA, PCA, minutia, eigen faces, fisher faces, global features.

INTRODUCTION

The main objective of this paper is multimodal biometric authentication. Biometric systems make use of behavioral traits for recognition. In the biometrics three different traits are used. Each has a separate method such as Face, Fingerprint, and Signature. A unimodal biometric system is easily affected by noise, error and attacks. A training set of database is taken for an identification of each biometric with the testing database. Each stage has separate algorithm for determination of input image from the database.

BIOMETRICS

Biometrics comprises methods for recognizing human depending upon physical or behavioral traits. In computer science this biometrics is used as a form of identity access management and access control. It is also used for finding an individual person under groups through surveillance [4],[11].

A biometric system is operated in these two modes:

- **Verification:** In this one to one comparison is done where stored template can be matched with database of template to verify to who it is. In this it is not be possible to match all the template at a time.
- **Identification:** Many comparisons are done by matching an input with a database a biometric in order to identify the unknown individual. Identification succeeds when the individual biometric matching with the database of biometric falls with in a previously set threshold.

Biometric authentication

Biometric authentication is the process of using individual physical or behavioral trait or a method to confirm the identity and determine the profile of a person. Biometrics has gently increased its popularity in the data collection devices. Common examples of biometric authentication include fingerprint scanning and voice activated locks.

There are two types of biometric authentication: physiological and behavioral. Physiological biometrics depends on each unique physical trait such as fingerprint, palm print, DNA, Iris, or face recognition. In this type of system, a scan of the trait is taken at a secured site and connected to profile of person. Security rights are assigned to this profile, based on the person's job or security access level. This information is stored in a secured system connected directly to the individual locks or security stations.

Behavior authentication depends on the actual behavior of the person. Some of the examples of this type of authentication include voice, gait, and speaking rhythm or diction. Where as it is easy to mimic the sound of another person's voice, the actual tone or note of their speech is harder to duplicate. This type of security is most often used to access computer files or other system maintained security.

Image acquisition is done through different types of sensor for different biometrics. The first block acquires necessary information from the sensor which acts as interface between the real world and the system. The second block is the preprocessing stage which removes the artificial noise or impulse noise from the sensor to enhance or remove background noise from the data acquired. A

template is the synthesis of characteristic features extracted from a source. Feature extraction stage correct features of an image are to be extracted in an optimal way then it is matched with the database or template for recognition of an individual. In the matching stage, the matching is performed by obtaining the template from feature vector stage and this template is matched with stored templates or database. This can be calculated by estimating the distance between them using any algorithm like hamming distance, Euclidean distance. Then matching program if the input is matched with database then it may be accepted or rejected.

Types of biometrics

Face recognition

Face recognition works by using computer for analyzing a subject's facial structure. Face recognition software takes a number of key measurements such as distance between eyes, nose and mouth, angles such as jaw and forehead, and length of various portions of face. Then by using this key measurement a template is created which is matched with enormous database of face images to identify the individual [1, 3].

Face recognition must have several problems in different techniques. This difficulty arises because face must be represented in a way that best utilizes the available face information to distinguish a particular face from all other faces. Faces pose a particularly difficult problem in this. Some faces are similar to one another in that they contain same features such as eyes, nose and mouth arranged in roughly the same manner.

Fingerprint recognition

Fingerprint is unique for each person in the world, even twins also. Fingerprint recognition software are used for desktop, laptops, cell phones instead of password which is more efficient. This type of fingerprint devices is available for vendors at low cost. Instead of password, just a touch is enough for instant access of device. Several states check fingerprints for new applicants to social service benefits to ensure recipients do not fraud under fake names. Finger prints have four types' whorl, left loop, right loop and arch. Criminals included in bank robberies, murder cases are identified with their fingerprint at crime scenes, with their past record collected from them earlier [1, 2].

Signature recognition

Each person signature is also unique from each other; this technology is dynamically used to authenticate a person. The technology is based on pressure and angle used by the person when the signature is produced. This technology is used for e-business applications and other applications where signature is used for authentication [1, 4].

Iris recognition

Recognition of iris in the eye is called iris recognition. The black dot in the middle of the eye is the pupil which is surrounded by a colored part. It does not require any physical contact with any scanning devices and any video acquisition system can be used for capturing the iris. Systems based on iris are recognition has substantially decreased in price and this is expected to continue in future. This technology works well in both verification and identification modes. Iris recognition has also demonstrated the work with various nationalities of individual [1].

Face recognition using LDA

Face recognition using LDA is used to implement the model for a particular face and recognize it from a large number of database stored faces with some real time variations as well.

LDA (Linear Discriminant Analysis) and related fisher's linear discriminant algorithm which are used for statistics and pattern recognition and to find the linear combination of features which separate two or more classes of objects or events. Then LDA technique used for data classification and PCA (Principal Component Analysis) technique for feature classification. In PCA, shape and location of the data sets change when transformed to different space where as in LDA it doesn't change the location of data set but tries to provide class severability and draws a decision region. PCA is a dimensionality reduction technique; LDA which is used for labeled information of data sets can be projected orthogonal without destroying the information of scatter matrices. In fisher face is combination of both LDA and PCA. In this projection the data is separated without clustering into each other and then separated into scatter matrices depending upon the variance between class scatter (S_b) and within class scatter (S_w). Recognition is widely under the variation of front view, where data sets consist of limited view.

Linear discriminant analysis

The famous example of dimensionality reduction is PCA technique which searches for directions in data that have highest variance is frequently project the data. Due to this some lower dimensional data are not projected. There are many difficult issues such as how many direction one has to choose is beyond the scope. PCA is unsupervised technique and does not include label information of the data [5].

When two data s1 and s2 are projected on a plane which are parallel and very close to each other, such that the variance in the data set will be in terrible projection, because all labels get mixed and the useful information will be destroyed. A useful projection is orthogonal and with least overall variance, then the data sets are perfectly separated.

In order to utilize the label information in projection Fisher LDA considers the following objective, [6].

$$J(W) = \frac{W^T S_B W}{W^T S_W W} \quad (1)$$

Where s_B is the "between classes scatter matrix" and s_w is the "within classes scatter matrix". Note that scatter matrices are proportional to the covariance matrices.

METHODOLOGY

The whole recognition process involves two:

a) Initialization process
b) Recognition process

The initialization process involves the following operations:

a) Acquire the set of face images called training set.
b) Calculate the mean adjusted image for all the samples and each class and then the scatter is calculated for between class scatter and within class scatter.
c) Then the projection of fisher criterion is satisfied then the face space value is calculated for fisher.

The recognition process involves the following operations:

a) Calculate a set of weights based on the input image and then projecting the input image in Eigen space.
b) In this face of test database is kept and matched with the input image to recognize.

Finger print recognition

Fingerprint recognition uses minutiae which are used for automated verification of matching between two human fingerprints. Through many intensive research fingerprints have been identified through their ridges and furrows which may be called as minutiae. These ridges are formed are fully developed during pregnancy and which will not change during the whole life time. A fingerprint is feature pattern of one finger and can be compared with another finger for identification and verification [7].
Minutiae are mainly classified into two types, they are

- Ridge ending - The abrupt end of a ridge.
- Ridge bifurcation - a single ridge which divides into two ridges.

Figure-1. Two minutiae features.

Figure-2. Other minutiae feature in finger.

Fingerprint based matching techniques may be classified into three types:

a) **Minutiae based matching:** This is the most frequently used algorithm which is used for recognition. Fingerprints are matched by certain alignment of minutiae points with another finger minutia and produce the matching percent of the fingerprint. This technology has widely increased various services all over the world [8].
b) **Correlation based matching:** Two fingerprints are superimposed and then correlations between the pixels are calculated as displacement and rotation angles etc.
c) **Pattern based matching:** This method is also known as image based matching. It considers the following while trying to recognize whether it is right loop, left loop, whorl, and arch. It compares the finger with the stored template of the database of candidate fingerprints. Orientation angles, type and size of the fingerprint are matched with the degree to which it matches. In this we are using minutiae matching algorithm, which is now, the backbone of the present technology products.

Signature recognition

In this, offline signature is taken for verification and recognition system; the signatures are composed of special characters and are not readable most of the time. It is varying from one person to another and it should be treated as image only not as letters and words. In many business applications signature is used for authentication and authorization in legal bank transactions and so the research signature verification has increased in recent years [9].

In this, recognition is for identifying the signature owner. Verification is to identify the signature is original or forgery. There are two types of forgeries

a) Random forgeries
b) Simple forgeries

In Random forgeries the perpetration knows the signature name and signature shape. Simple forgeries are produced without having the signer's signature. SRVS (signature Recognition and Verification system) is often

categorized in two classes: in online SRVS the data is obtained through the electronic tablets where as in offline signature the data is obtained from the signature written on paper. Offline handwriting recognition systems are more difficult than online systems as information like duration, number of strokes and direction of writing are lost. But, offline systems have an advantage because they need not require accessing the processing devices where the signature is produced. In this database of signature images are taken for verification and identification. It is tested with the forgery and random signature of each person in the database.

FACE RECOGNITION INTIALIZATION PROCESS

Let a face image be T(x,y) with two dimensional N by N matrixes of 8-bit intensity values of 256 gray levels. An image is considered as a vector of dimension N^2, so the size of image is 200x180 becomes a dimension of 36000 in dimensional space, x and y denote pair of coordinates in the image [5]. In order to determine the Eigen face of training set T_1, T_2, T_3….T_n we have to calculate the mean vector. Where M is total number of database image which we are taking. Then mean of the total M samples are

$$\psi = (1/M)\sum_{n=1}^{M} T_n \quad (2)$$

Figure-4. Mean image.

The set of deviation from mean vectors $\{ø_1ø_2ø_3….ø_n\}$ which has individual difference of each training image from a mean vector, where i=1, 2...M, the training set of images T_i is $\{T_1, T_2, T_3….T_n\}$

$$\phi_i = T_i - \psi \quad (3)$$

In order to calculate the Eigen face the principal components of the training image should be calculated this gives set of vectors then the Eigen face is obtained through the Eigen vector of the covariance matrix which is given by [5].

$$C = (1/M)\sum_{n=1}^{M} \phi_n \phi^T{}_n \quad (4)$$

Where n=1, 2…M, $A = \{\phi_1, \phi_2, \phi_3 .....\phi_n\}$

Then the covariance matrix can be written as

$$C = (1/M)AA^T \quad (5)$$

For this covariance matrix a set of $N^2 \times N^2$ dimensional matrix is obtained. Calculating Eigen vector for these dimension is impossible 40000×32400 due to less compact data point in image space (i.e., $M << N^2$), so M-1 Eigen vector are calculated. Consider the Eigen vector v_i of AA^T.

In this AA^T can write as A^TA.

$$A^T A v_i = \mu_i v_i \quad (6)$$

Where μ_i is a scalar are corresponding Eigen values of Eigen vector v_i. Then the above equation is multiplied with $\frac{1}{M}A$ on both sides of the equation.

$$\frac{1}{M}AA^T A v_i = \frac{1}{M}A\mu_i v_i \quad (7)$$

$$CAv_i = \frac{1}{M}\mu_i A v_i \quad (8)$$

C is the covariance matrix, the right hand side equation 'Av_i' is called Eigen vector of the training set of images, This Eigen vector is multiplied with individual difference from a mean vector then it is known as Eigen face of training images or projected face image.

$$x_k = Av_i * (T_i - \psi) \quad (9)$$

Let the training set of images face images be x_1, x_2, x_3….x_m be the M samples with 'c' classes which is χ_1, χ_2…. χ_c which denote the number of persons in the database is taken. Then the mean is calculated for projected Eigen face image for each person's j=1, 2….c [10].

$$\mu_j = (1/M_j)\sum_{x_k \in \chi_i} x_k \, . \quad (10)$$

Then the total average mean calculated for M projected Eigen face image is given as [6].

$$\mu = (1/M)\sum_{k=1}^{M} x_k \quad (11)$$

The mean are separated from the M samples of the projected Eigen face images the scatter matrix is given below [5].

$$S_j = \sum_{x_k \in \chi_i} (x_k - \mu_j)(x_k - \mu_j)^T \quad (12)$$

We define the scatter matrix S_j and S_w then the within class scatter can be calculated as follows:

$$S_w = S_1 + S_2 \quad (13)$$

This is formed from above equation with no of class's c where j=1, 2……c, where this is initialization of within class scatter [6].

$$S_w = \sum_{j=1}^{c} S_j \quad (14)$$

Then class scatter can be calculated with class mean and total adjusted mean which is initialization of between class scatter [6].

$$S_B = \sum_{j=1}^{c} \left|\chi_j\right| (\mu_j - \mu)(\mu_j - \mu)^T \quad (15)$$

Then the total scatter matrix can be calculated as follows

$$S_T = S_w + S_B \quad (16)$$

Then the Eigen vector value is calculated for the S_T total scatter matrix. Then the vector obtained is called as fisher projected image. Then the fisher criterion is satisfied by multiplying projected Eigen face with fisher projected image.

In LDA data dimension are much larger than No of samples N is given by d>>N. since S_w is a symmetric and positive semi definite with a non singular n>d. But for S_B it is also symmetric and positive semi definite its outer product of two vectors, with rank one and S_B is singular. This is fisher criterion function which must be satisfied [1].

$$w_k = \frac{S_B}{S_W} \quad (17)$$

Where w_k is projected fisher face image.

Recognition process

The Fisher face image obtained is subtracted with the image vector obtained from the Recognition process is an individual image compared with the total data base of training set. This vector can be compared using weighted Euclidean distance algorithm or weighted hamming distance algorithm. From that a k^{th} face class is identified. Then the face belongs to training dataset which allows to set a threshold otherwise the face will be unknown.

$$\varepsilon = \left|\Omega_p - \Omega_k\right| \quad (18)$$

Where the weights of projected fisher face image is Ω_p, Ω_k is the weight of input image vector.

FINGERPRINT RECOGNITION PREPROCESSING STAGE

The steps are image segmentation and image enhancement. In this image enhancement the main function is to improve the quality of image. So the fingerprint images obtained from various sources are contrasted and clarity must be increased. By enhancing the image the merged ridges and furrows can be clearly extracted.

Histogram equalization

Histogram equalization is performed for increasing the quality of the image. This histogram equalization is used for changing a low contrast image to a high contrast image. It occupies range from 0 to 255. By this histogram equalization the deep ridges and valley are identified easily in the finger print [8].

Figure-5. a) Fingerprint image b) histogram equalized image

Image binarization

The image binarization is done for converting 8-bit gray level image to 1-bit image where 0 for ridges and l for furrows or deep valley which are present in fingerprint. A locally adaptive binarization method is used to binarize the image. Such named method comes from the mechanism of transforming the pixel value to 1 then the value of mean intensity larger than (16×16) where the pixel belongs to.

Figure-6. a) Image after binarization b) image before binarization

Image segmentation

Generally Region of Interest (ROI) is used for recognizing each fingerprint image. The ridges and furrows unoccupied image area is first discarded it just holds background information. Then the remaining effective bounding area is confusing without spurious

minutiae that are generated out of bound ridges in the sensor. Then the processed fingerprint image is divided into16x16 non overlapping block size, followed by gradient calculation of each block. ROI is done using two morphological operations called OPEN or CLOSE. The open operation expands images and removes peaks produced by background noise. The close operation is used for shrinking the image. Then by subtracting closed region from open region the final ROI is obtained by discarding the bottom, top, right, left portion [7].

Figure-7. Region of interest.

Minutiae extraction

The processing ridge thinning is used for removing redundant pixels in the image. An iterative parallel thinning algorithm is used for scanning full fingerprint image. This algorithm marks down more redundant pixels and removes the pixels by several scanning. In Matlab Morphological operation the thinning function [11].

bwmorph (binaryimage,'thin',inf)

Then the thinned ridge map is filtered with three morphological operations using H breaks, isolated points, spikes [8].

bwmorph (binaryimage,'hbreak',inf)
bwmorph (binaryimage,'clean',inf)
bwmorph (binaryimage,'spur',inf)

Figure-8. Thinned image.

Minutiae marking

Minutiae marking are done using 3x3 window pixels. If center pixel is 1 with three values having neighbors 1 then it is ridge branch [8].

0	1	0
0	1	0
1	0	1

If center pixel is 1 and has only neighbor 1, then it is ridge ending.

0	0	0
0	1	0
0	0	1

In this case both the uppermost pixel with value 1 and rightmost pixel with value1 have another neighbor outside the 3x3 window due to some left over spikes, so then the two pixels are also matched as branches too, but only one branch is located in small region.

0	1	0
0	1	1
1	0	0

False minutiae removal

Due to insufficient amount of ink or over inking in the finger print image which may lead to ridge cross connections are formed so to keep system consistent this false minutiae should be removed. The average inter ridge refers to the average distance between two inter ridge neighbors. Sum up all pixels in the row whose value is one then divide it by row length where inter ridge distance D is obtained [8].

Now 7 false minutiae from m1, m2, m3, m4, m5, m6, m7 are removed using these steps.

d(x,y) is the distance between two minutiae points

d(bifuracation,termination)<D then 2 minutiae point in same ridge then remove (case m1)

d(bifurcation,bifurcation)<D then 2 minutiae point in same ridge then remove(case m2 and m3)

d(termination,termination)=D then their directions are coincident then remove(case m4,m5,m6)

d(termination,termination)<D then 2 minutiae point in same ridge removes (case m7).

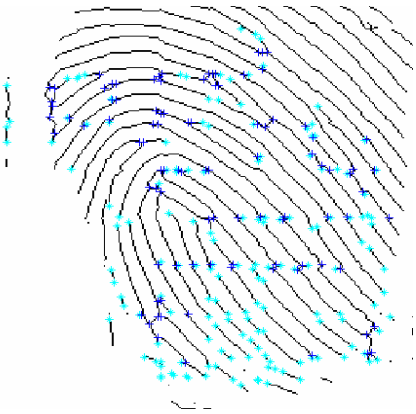


Figure-10. Minutiae along false minutiae points.

Figure-11. After removing false minutiae.

Minutiae match

Two minutia finger print images are matched through minutia matching algorithm to decide whether both finger prints are from same finger or not. If the similarity of finger is matched with larger than threshold then it is matched. It has two stages: alignment stage, match stage [8].

Alignment stage

Two finger print images are matched with alignment coordinates I_1 and I_2 where this similarity set are matched with each ridge of the reference minutia points. If they are similar and larger than threshold, then the two sets are transformed to new coordinate systems with origin as reference point and the coincident and reference point at x-axis.

The x-coordinates (x1, x2, x3...xn) are points on the ridge. A sampled point on each ridge length L starting from the minutiae point, the average inter ridge length is L. n value is set to 10 unless the total ridge length is less than 10*L [8].

So the similarity of correlating the two ridges are given below

$$S=\frac{\sum_{i=0}^{m} xi * Xi}{\sum_{i=0}^{m} xi^2 * Xi^2} \quad (19)$$

Where (x_i~x_n) and (X_i~X_N) are the set of minutiae for each fingerprint image. If the similarity score is larger than 0.25 then the finger is matched else the percentage score is zero. If the two finger print images are translated and rotated then we get a transformed set of minutia points I_1^T and I_2^T.

Match stage

In this I_1^T and I_2^T are two reference minutia matched pairs must strictly require these (x, y, θ) parameters. In this elastic matching of minutia is achieved by placing a boundary box around each finger minutiae points. If we are placing rectangle box around the minutia points of the image it reduces the discrepancy of minutia matching. Matching with very small discrepancy is two finger print images of an identical person. Finally, a matching score is generated in the range from 0 to 100 the minutia points in finger print matching produces ratio of percentage score is obtained [8].

SIGNATURE RECOGNITION PREPROCESSING STAGES

In signature recognition, both training and testing phases are taken and then they are normalized. The signature which is colored can be scanned to gray. Then the steps performed in post processing are background elimination, Noise extraction, width normalization and thinning. In the feature extracting stage the global features are extracted and then a post processing stage is performed where the input is matched with database of signature which consists of random and forgery signature.

Background elimination

Thresholding is applied for the signature to capture signature. In this signature occupied in the data area is represented by '1' and back ground area is represented by '0' [9].

Noise reduction

In noise reduction, a filter is applied for the binary image which can be used for removing single black pixels on the white background. If the number of black pixels is greater than the number of white pixels then it chooses black otherwise white.

In width normalization the signature of each person will have difference in dimension. The adjusted image value does not have any effect on height and width ratio.

Thinning

The main aim of thinning is to eliminate thickness difference of each pen should make difference during computation. So, the pen difference of signature image into one pixel thick. This operation can done using morphological operation in matlab.

Feature extraction

The training databases of inputs are taken. Global features provide information about the shape of signature and area occupied by the signature, center of signature is also calculated [9].

Signature area

The area occupied by the signature in number of pixels, which denotes the density of the signature.

Signature height to width ratio

The height of signature is divided with width of signature is also called Aspect Ratio of the signature. This aspect ratio is approximately equal for each person.

Maximum horizontal histogram and maximum vertical histogram

The histogram calculated for horizontal takes a row in that which row has the highest value is taken

horizontal histogram. The histogram calculated for vertical takes a column in that which column has the highest value is taken as vertical histogram.

Horizontal and vertical center of the signature

The center of signature is calculated for horizontal and vertical using this formula [12].

$$center_x = \frac{\sum_{x=1}^{x\max} x \sum_{y=1}^{y\max} b[x][y]}{\sum_{x=1}^{x\max}\sum_{y=1}^{y\max} b[x][y]} \quad (20)$$

$$center_y = \frac{\sum_{y=1}^{y\max} y \sum_{x=1}^{x\max} b[x][y]}{\sum_{x=1}^{x\max}\sum_{y=1}^{y\max} b[x][y]} \quad (21)$$

After all this preprocessing steps a rotation angel of the signature is known and bounding box is created for the signature to match the signature correctly. The same operation is applied for the input image which is used for verification. In this database of original signature and forgery signature are combined.

IMPLEMENTATION OF FACE RECOGNITION

The Training database obtained from 5 people's each with 12 images with different facial expressions and testing phase by taking photographs with different pose of images which are not present in the training database. The images are taken low resolution camera in this lighting, background, are the factors which are considered.

Training

1. Training images are kept in a particular folder with '.jpg' format in which the program is stored. A total of 60 images considered of person with each 12 images.
2. Then the training images are the M samples where each matrix is converted into gray levels and reshaped into size of 200x180. This is a single large dimensional matrix T.
3. Where T is a matrix of each individual training images.
4. For this mean is calculated as follows:

$$Z = mean(T) \quad (22)$$

5. Then the mean is subtracted from the individual image vectors and kept in matrix A.

$$A = T - Z \quad (23)$$

6. Calculating the Eigen face of covariance matrix is

$$C = (1/M)AA^T \quad (24)$$

7. For this covariance matrix a eigen vector is calculated as follows:

$$Eig[c] = [V\ D] \quad (25)$$

Where V is the Eigen vector and D is the Eigen value.

8. Then the Eigen vector when projected Eigen space or multiplied with individual difference from mean vector. Then the Eigen face obtained is as follows

$$X = V^T A \quad (26)$$

9. The mean is calculated for total Eigen face as follows:

$$P = mean(X) \quad (27)$$

10. Then the average mean calculated for each person is also obtained that is considered to be R.
11. A matrix q is obtained when subtracting total mean P from Eigen space X then q matrix is multiplied with transpose of q. then a scatter matrix S is calculated.
12. Then within matrix 'W' is summation of scatter matrix S.
13. The between scatter matrix 'B' is calculated by subtracting a mean R from mean P, and multiplied number of classes or number of persons.
14. The total scatter matrix 'F' is the total of within scatter and between scatter.
15. Eigen vector is calculated for total scatter matrix F is given as

$$Eig[F] = [E\ U] \quad (28)$$

'E' is the Eigen vector and U is the Eigen value.
16. The Eigen vector of the projected fisher image when multiplied with Eigen face of pca the projected fisher face Y is obtained.

$$Y = EX \quad (29)$$

Testing process

1. The test images 'T' in the Database are reshaped into 200x180. For real time applications the image may be taken from web cam also.
2. Then the image vector of test images individual difference is calculated by subtracting mean from image vector.

$$L = T - Z \quad (30)$$

3. A normalized projected image 'J' of the input image is obtained.
4. For each column matrix J we calculate the Euclidean norm difference between the projected fisher face vectors Y. Then by setting a certain threshold value for Euclidean the person with small value shows the image is identified.

Minutiae extraction includes image segmentation, image enhancement, final extraction stage; minutiae alignment and matching are done. The steps involved in

image enhancement are histogram equalization which is used for increasing the contrast of image. Image binarization is used for converting gray level image to bitmap image. In image segmentation the steps are ridge flow estimation and region of interest through Matlab's morphological operation. Then the two steps above are known as preprocessing stages. In final extraction stage the steps involved are ridge thinning, minutiae marking and false minutiae removal process.

In minutiae alignment stage the steps involved are fine reference minutiae pair, transform minutiae sets. The alignment stage is known as post processing stage.
=Signature image

The implementation of various pre processing steps in matlab through looping, the signature area, signature height to width ratio is calculated and global features are extracted the same can be applied to post processing stage and both can be matched for recognition. It shows accepted or rejected [9].

FACE RECOGNITION RESULTS

Here we are considering a total of 60 images with 5 persons with each 12 images, with varying facial expressions of each person.
The training database is shown below

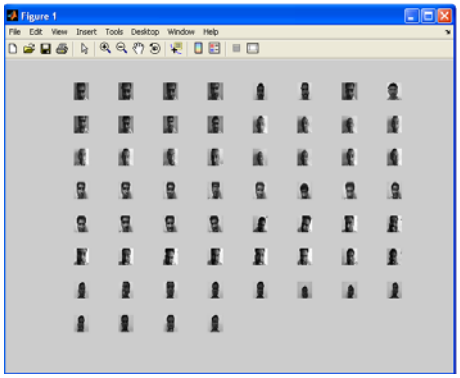


Figure-14. Database of face images.

Then the training dataset of images are acquired, mean should be calculated.

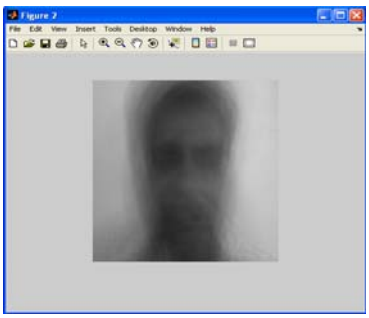
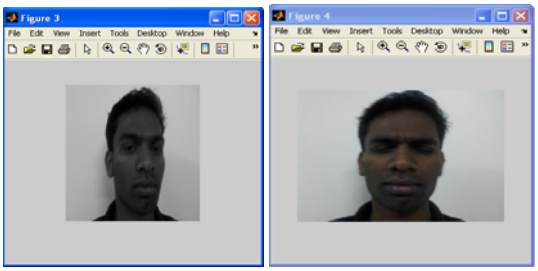


Figure-15. Mean adjusted image.

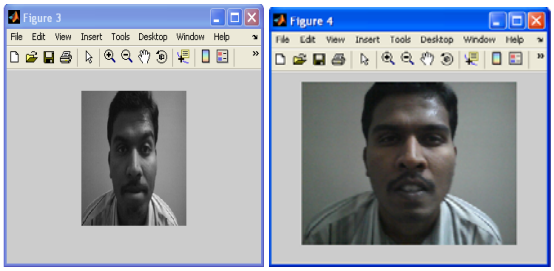
In this after normalization the Eigen face is calculated from the covariance matrix of Eigen vector. This Eigen vector is multiplied with individual difference from the mean vector where Eigen face is obtained. And this Eigen face can be multiplied with total scatter fisher face then it is fisher criterion.

This shows the following image recognized for given input.

Case-1



Case-2



Case-3

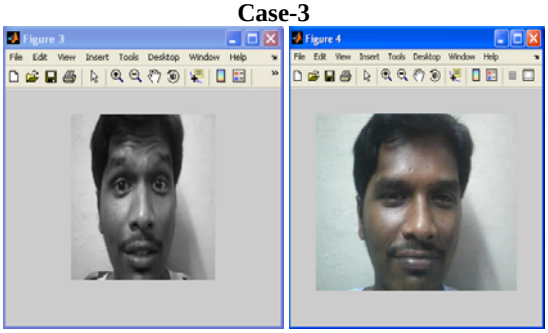


Figure-16. Output recognized from the database.

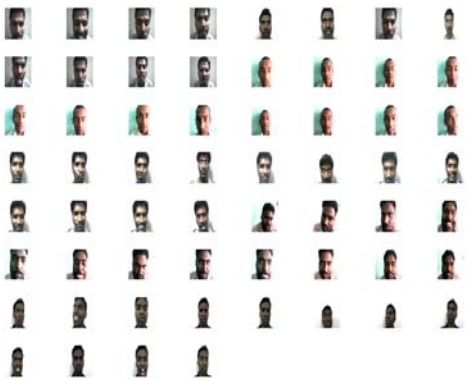


Figure-17. Database of image taken for recognition.

Table-1. Accuracy of database images.

No. of images	No of persons	accuracy
12	1	50%
36	3	69%
60	5	90%

FINGER PRINT RECOGNITION RESULTS

The finger print of 5 persons each having 4 finger prints and a total of 20 images are there this fingerprints lot more 100 to 200 images I have done just sample for recognition of fingerprint. The fingerprint images are captured by using a sensor. Then the fingerprint images may vary with quality from each image. In this each fingerprint template obtained is matched with other fingerprint matching technique. Fingerprint verification produces a percentage matching score of above 10 percent then the fingerprint image is some way matched with each other of the template. The table given below shows, the highest percentage scores of each person image taken from the database.

Figure-18. FVC-DB1 (2004) Database of fingerprint images.

Table-2. Fingerprint recognition percentage score.

Finger print image	Matched with	Highest matching percentage
Person 1 image 1	Person1finger image 3	39.8
Person2 image 2	Person2 finger image 3	31
Person3 image1	Person3 finger image 2	29
Person4 image3	Person4 finger image 1	39
Person5 image 1	Person5 finger image 3	61

Due to insufficient inking or over inking the matching percentage score is in the range of 37%.

SIGNATURE RECOGNITION RESULTS

The database signatures are taken for recognition which may not be treated as special character and it is normally taken as image. The signature taken here four of each person which may have random and simple forgeries this can be overcome by this algorithm a total of 20 signatures is available. In this cropped image or bounding box created around the signature of both post and pre processing stages are compared for verification or recognition of the signature.

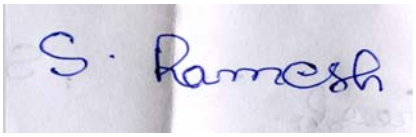


Figure-19. Color signature image.

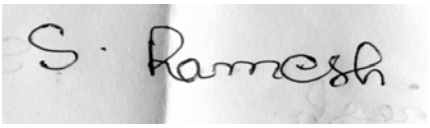


Figure-20. Gray converted signature image.

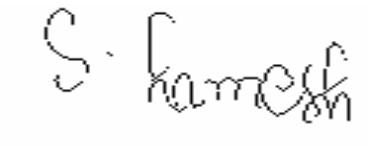


Figure-21. Thinned image.

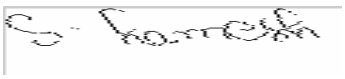


Figure-22. Moving signature to origin.

Figure-23. Boundary box created image.

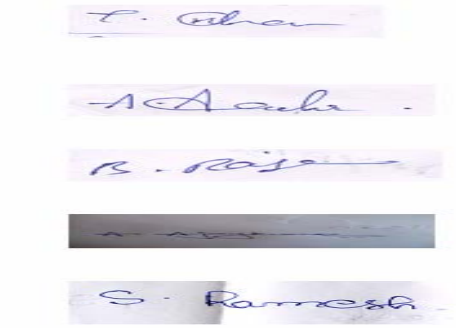


Figure-24. Database of signatures which are taken for recognition.

The same steps are also performed in post processing stages than they are matched for verification if it is matched it produces accept else rejected.

Future scope

This paper is based on recognition using certain biometric traits. In this through fusion of all these face, finger, signature algorithms at any three stages can produce better results for recognition of a person and highly efficient. In face LDA technique has been used which has more future in neural networks and can produce more accuracy. Without fixing a constant depending upon the conditions the database can be available. Finger print recognition is fundamental algorithm for recognition which has more scope in future by using various matching methods Such as correlation, pattern matching. Signature can also be done in neural networks which is treated same as image which has highest matching points is considered. All these biometric used are dependent upon the database, and database is dependent upon resolution of the sensor. The results considered can be improved highly.

CONCLUSIONS

Face, finger, signature recognition techniques available can provide better results whereas face recognition through fisher's LDA which is combination of both PCA and LDA uses both Eigen face approach and discriminant analysis for more practical results. It is fast, reliable and simple. This works in any constrained environment. And it depends on head size and background, lighting of this are necessary for this unambiguous technique. In Minutiae matching algorithm which various factors are consideration at image size, quality of image, skeletoization of image and rectangle box around the minutiae matching points then only it can produce better result. This matching of finger print produces a matching score in range of percentage from 0 to100. In signature recognition the signature image is not treated as a special character. Lot of preprocessing or normalization is done for the image. Then feature extraction can be done through these Global features of the signature has been extracted for matching with post processed signature. The signature depends on height-width ratio, area of signature, background elimination of the image.

REFERENCES

[1] A.M. patil, Satish R. Kohle and Pradeep M. Patil. Face Recognition by pca technique. 2nd international conference on emerging trends in engineering and technology, ICETET-09.

[2] Priyadarsini M.J.P., K. Murugesan, S.R. Inbathini and V. Kumar. 2012. Efficient face recognition in video by bit planes slicing. J. Comput. Sci. 8: 26-30. DOI:10.3844/jcssp.2012.26.30.

[3] H. Hassanpour and S. Asadi. 2011. Image quality Enhancement using pixel wise Gamma. Transactions B: Application. 24-(4): 301-312.

[4] H. Hassanpour and H. Yousefian. 2011. An Improved Pixon- Based approach for Image Segmentation. Transactions A: Basics, January. 24(1): 25-35.

[5] Anil K. Jain, Arun Ross and Salil prabhakar. 2004. An introduction to biometric recognition. IEEE Transactions on circuits and systems for video technology. 14(1), January, DOI 10.1.1.113.6189.

[6] Lishi zhang, Dehong wang and Shengzho gao. Application of improved fisher linear discriminant analysis approach. Appeared at IEEE @2011.

[7] H B Kekre and V A Bhadri. Finger print core point detection algorithm using orientation field based multiple features. International Journal of Computer Applications, ISSN 0975-8887, 1(15).

[8] Sangram Bana and Davinder Kaur. Finger print recognition using image segmentation. International Journal of Advanced Engineering Sciences and Technologies. 5(1): 12-23.

[9] 2005. Emre ozgunduz tulin senturk and M. Elif karsiligal. Off line signature verification and recognition by support vector machine. Yildez technical university, yildiz, Istanbul. 13th European Signal Processing Conference Antalya.

[10] Thomas Heseltine, Nick pears and Jim Austin. 2004. Combining multiple face recognition systems using fisher's linear discriminant. The Proceedings of the SPIE Defense and Security Symposium. DOI: 10.1117/12.542033.

[11] Andrew Ackerman. 2005. Finger print recognition. Professor Rafail Ostrovsky. Doi: 10.3390/ molecules16021240.

[12] Maya V. Karki, K. Indira and S. Sethu Selvi. 2007. Off-line signature recognition and verification use neural networks. International conference on computational intelligence and multimedia applications. Doi 10.1109/ICCIMA.2007.296. 307.