VOL. 11, NO. 23, DECEMBER 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

A MULTIMODAL BIOMETRIC RECOGNITION SYSTEM BASED ON DECISION LEVEL FUSION FOR USER AUTHENTICATION

Vijayalakshmi G. V. and Mohana C.
Department of Electronics and Communication Engineering, Dr.T. Thimmaiah Institute of Technology, Oorgaum, Kolar Gold Fields, Karnataka, India
E-Mail: vijugv@gmail.com

ABSTRACT

In the traditional authentication methods like passwords, smart cards etc., there is lack of security, hence to overcome this biometrics is used. In case of single modal biometric there is a chance of misuse and the accuracy is also less, hence to achieve good authentication accuracy and to improve security multimodal biometrics is used. The project work on 'A Multimodal Biometric Recognition System Based on Decision Level Fusion for User Authentication' was carried out using face, iris and fingerprint Databases. The features such as Gabor filter, GLCM (Gray Level Co-Occurrence Matrix), Affine Moment and LBP (Local Binary Patterns) were extracted from the face, iris and fingerprint respectively. The classification of face and iris images was performed using LDA (Linear Discriminant Analysis) and that of fingerprint images was performed using *k*-NN (*k*-Nearest Neighbor) from the features extracted. The performance of the classifier was evaluated using confusion matrix. From the evaluation the authentication accuracy of 97.5%, 98% and 99.3% were obtained for iris, fingerprint and face respectively. Also, the single biometrics were fused using decision level fusion based on majority logic function to achieve highest accuracy and an authentication accuracy of 99.6% was obtained after fusion.

Keywords: authentication, decision level fusion, gray level co-occurrence matrix, fusion, multimodal biometric recognition.

1. INTRODUCTION

In present years, authentication based on biometric has been significant improvement in providing accuracy and reliability by offering good performance [1]. With a view to increase individual security, the government of India has introduced Adhaar which gives unique identity to each individual by using biometrics such as iris, face and fingerprint [2]. In current year's biometric techniques plays a very important role in identifying the individuals. Using passwords, Personal Identification Numbers (PIN), smart cards etc. there is a chance of forgetting the passwords, stealing of smart cards and hacking of sensitive records by the malicious users hence to overcome this biometrics helps to identify the correct person, since the biometrics characteristics cannot be stolen, misplaced or changed [3]. Biometrics with single modal has constraints like high error rate, noise; non-universality and uniqueness, hence by using multimodal biometric accuracy can be increased, while vulnerability to spoofing can be reduced. The important part in multimodal biometrics is the fusion of various biometrics. Image Fusion is the method of combining significant information from two or more images into a single image, the resultant image will be more informative than any of the input images.

2. RELATED WORK

In today's world authentication plays a very important role in identifying the individual, hence biometrics plays a very important role in providing the security against malicious user who try to steal individual personal details. In this section the research carried out by various authors is reviewed for understanding the concepts of fusion techniques for providing authentication accuracy.

The authors in [4, 5] proposed a fusion technique; since the single modal biometric possesses many problems to overcome this multimodal biometric is used. The two single modal biometric traits iris and fingerprint are taken. The use of multi-modal biometrics produces higher performance then the single modal biometrics. The accuracy of iris is 97.5% and that of fingerprint is 96%. Fusion is carried out using fuzzy logic at decision level, the iris is weighted with 80% and fingerprint is weighted with 20%. The accuracy of the fused multimodal biometrics is 98.3%. Hence, the use of multimodal biometrics gives better results. The authors in [6] proposed a facial feature extraction method based on FPD (Face Part Detection) and (GLCM) Gray Level Co-Occurrence Matrix. GLCM is used to extract texture features and FPD is based on bounding box method. The performance factors such as accuracy and execution time was measured. On comparison of the outcomes of the two algorithms it was observed that extracting the features using GLCM involved minimum execution time and it resulted in good performance accuracy when compared to the FPD.

The author in [7] proposed a feature level fusion for face and fingerprint. The features are first extracted from the individual biometrics. The feature from the face is extracted using scale invariant transform (SIFT) and the feature from the fingerprint is extracted is minutiae matching. The features are matched based on point pattern matching or Delaunay triangulation. The accuracy obtained with face feature extraction is 93.95% and that of fingerprint is 92.64%. The accuracy obtained after fusion is 98.51%.

3. METHODOLOGY

This section describes the methodology of the proposed system. In the case of traditional authentication methods such as passwords, PIN (Personal Identification Number) and smart cards there is a chance of misuse by the fraudulent user and hence to provide security against the unauthorized user Biometrics plays a very important role in identifying the individual. Biometrics provides authentication by using the physiological characteristics and behavioural traits. In case of behavioural traits there is a chance of replicating the individual and the authentication accuracy is also less, hence to overcome this physiological characteristic is used. Physiological characteristics provides authentication by considering the physical characteristics of the individual. Even in the case of physiological characteristics there is a chance of misusing the data by using the fake fingerprints and photo of a face which reduces the authentication accuracy and hence to overcome this multimodal biometrics is used. The block diagram of the proposed system is shown in Figure-1.

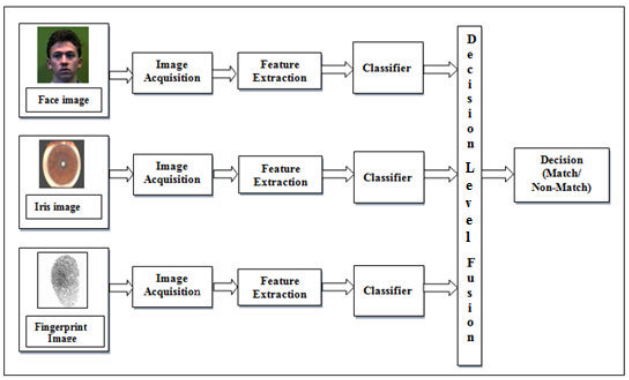

Figure-1. Block diagram of the proposed system.

3.1 Image acquisition

Image acquisition is defined as the action of retrieving an image from the source. The biometric template can be present in Biometric device which is usually in the case of small or closed systems, database on central computer, plastic card or token (barcode, stripe, optical, smart card). The proposed system uses three biometrics i.e. face, iris and fingerprint multimodal biometrics was considered in order to increase the authentication accuracy, since the three biometrics were not available from the same database, hence it was acquired from different databases which is explained below:

a) Face images are collected from the Faces94 database [8], the database contains images of 40 individuals (20 male subjects and 20 female subjects), out of which 20 individuals (10 male subjects and 10 female subjects) with 6 images from each individual was selected; hence a total of 120 images was selected.
b) Iris images are collected from the UPOL database [9], the database contains images of 56 individuals with 6 images of each individual (3 images of left iris and 3 images of right iris), out of which 20 individuals with 6 images per individual was selected; hence a total of 120 images was selected.
c) Fingerprint images are collected from FVC2002 (Fingerprint Verification Competition 2002) database [10], the database contains images of 40 individuals with 10 images of each individual from which 20 individual with 6 images per individual was selected, hence a total of 120 images.

From the selected 120 images, 67% of images (80images) is taken in training database and 33 % of images (40 images) is taken in the testing database, that is out of 6 images, 4 images is taken in the training database and 2 images is taken in the testing database.

3.2 Feature extraction

Feature extraction is the process of transforming the large set of data to a reduced set, feature extraction specifies the reduction in the dimensionality. The feature that is extracted from the data contains specific information from the input data [11].

3.2.1 Feature extraction using GLCM

Statistical texture analysis deals with calculation of texture features from the statistical distribution of intensity that is specified at positions relative to the image. The texture features from the second order statistics is extracted using GLCM (Gray Level Co-occurrence Matrix) [12]. GLCM is a N×N matrix that represents the relationship between two adjacent pixels, the reference and the neighbour pixels [13]. GLCM matrix formulation is explained in the Figure-2.

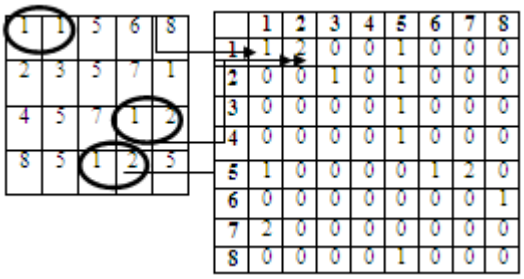

Figure-2. Formulation of GLCM matrix.

An 8×8 GLCM matrix will be created by default. The element at (1, 1) contains the value 1, because in the input matrix the values 1 (reference pixel) and 1 (neighbour pixel) appears only once in the horizontal direction. Similarly the element at (1, 2) contains the value 2, because in the input matrix the values 1 (reference pixel) and 2 (neighbour pixel) appear twice. Similarly the matrix is updated with the same procedure.

The important features that is calculated from the GLCM matrix are described below:

A. Energy/ Uniformity/Angular second moment: "Energy is defined as the sum of the square of the values in the GLCM". If the energy is high or if the

pixels are similar then the image has good homogeneity. The energy is calculated using the equation (1).

$$E = \sum_x \sum_y p(x,y)^2 \quad (1)$$

where x, y are the spatial coordinates of the function p (x, y).

B. Correlation: "Correlation measures the linear dependency of grey levels of neighbouring pixels". Correlation is calculated by using the equation (2).

$$C = \sum_x \sum_y \frac{(x,y)p(x,y)-\mu_x\mu_y}{\sigma_x\sigma_y} \quad (2)$$

whereμ_x and $\mu_y$is the mean and σ_x and σ_y is the variance

C. Contrast: "Contrast is the measure of intensity of the pixel and its neighbour". The contrast is calculated using the equation (3)

$$S = -\sum_x \sum_y p(x,y) * \log p(x,y) \quad (3)$$

D. Homogeneity: "Homogeneity measures the closeness of the distribution of elements in the GLCM to the GLCM diagonal" and it is calculated using the equation (4).

$$H = \sum_x \sum_y \frac{1}{1+(x-y)^2} p(x,y) \quad (4)$$

3.2.2. Affine moments

Moment functions for an image are used as shape descriptors. The first moment invariant was introduced by Hu [14], which is based on algebraic invariants. The Hu moments are invariant to rotation, scale and translation but not to affine transformation, hence to overcome this affine moment is introduced [14]. Affine moment finds its application in computer vision [15] and pattern recognition [15]. The geometric transforms is decomposed from affine transform. Since affine moments are invariant to linear transformations they are very useful in extracting features from an image. [15]. In order to compute affine moments, geometric moment and centroid of the images have to be computed which is explained in the following section.

A. Computation of geometric moments

Geometric moments for image intensity function f(x,y)of order (p+q) is given by equation (5).

$$m_{pq} = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} x^p y^q f(x,y) dxdy \quad (5)$$

with p,q≥0 .

B. Centroid and central moment of an image

Moment invariant doesn't change under the group of transformations. The effect of elimination of transformation is known as image normalization. Normalization to translation can be achieved by shifting the image centroid $(\hat{x},\hat{y})$ coincides with the origin of the coordinate system [15]. The centroid of the image is given by equation (6) and equation (7),

$$\hat{x} = \frac{m_{10}}{m_{00}} \quad (6)$$

$$\hat{y} = \frac{m_{01}}{m_{00}} \quad (7)$$

The central moments of the image is given by equation (8),

$$\mu_{pq} = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} (x-\hat{x})^p (y-\hat{y})^q f(x,y) dxdy \quad (8)$$

The affine moments invariants are computed using the Table-1.

Table-1. Affine moments invariants.

I_1	$\frac{1}{\mu_{00}^4}(\mu_{20}\mu_{02} - \mu_{11}^2)$
I_2	$\frac{1}{\mu_{00}^{10}}(\mu_{30}^2\mu_{03}^2 - 6\mu_{30}\mu_{21}\mu_{12}\mu_{03} + 4\mu_{30}\mu_{12}^3 + 4\mu_{03}\mu_{21}^3 - 3\mu_{21}^2\mu_{12}^2)$
I_3	$\frac{1}{\mu_{00}^{10}}\left(\mu_{20}(\mu_{21}\mu_{03} - \mu_{12}^2)\right) - \mu_{11}(\mu_{30}\mu_{03} - \mu_{21}\mu_{12}) + \mu_{02}(\mu_{30}\mu_{12} - \mu_{21}^2))$
I_4	$\frac{1}{\mu_{00}^{11}}(\mu_{20}^3\mu_{03}^2 - 6\mu_{20}^2\mu_{11}\mu_{12}\mu_{03} - 6\mu_{20}^2\mu_{21}\mu_{02}\mu_{03} + 9\mu_{20}^2\mu_{02}\mu_{12}^2 + 12\mu_{20}\mu_{11}^2\mu_{03}\mu_{21} + 6\mu_{20}\mu_{11}\mu_{02}\mu_{30}\mu_{03} - 18\mu_{20}\mu_{11}\mu_{02}\mu_{21}\mu_{12} - 8\mu_{11}^3\mu_0^3\mu_{30}6\mu_{20}\mu_{02}^2\mu_{30}\mu_{12} + 9\mu_{20}\mu_{02}^2\mu_{21}^2 + 12\mu_{11}^2\mu_{02}\mu_{30}\mu_{12} - 6\mu_{11}^2\mu_{02}^2\mu_{30}\mu_{21} + \mu_{02}^2\mu_{30}^2)$
I_5	$\frac{1}{\mu_{00}^6}(\mu_{40}\mu_{04} - 4\mu_{31}\mu_{13} + 3\mu_{22}^2)$
I_6	$\frac{1}{\mu_{00}^9}(\mu_{40}\mu_{04}\mu_{22} + 2\mu_{31}\mu_{22}\mu_{13} - \mu_{40}\mu_{13}^2 - \mu_{04}\mu_{31}^2 - \mu_{22}^3)$
I_7	$\frac{1}{\mu_{00}^7}(\mu_{20}^2\mu_{04}^4\mu_{20}\mu_{11}\mu_{13} + 2\mu_{20}\mu_{02}\mu_{22} + 4\mu_{11}^2\mu_{22}^4\mu_{11}\mu_{02}\mu_{31} + \mu_{02}^2\mu_{40})$

3.2.3 Gabor filter

Gabor filter is used to extract the texture features from an image [16]. A Gabor filter is obtained by modulating a sinusoid with a Gaussian. In case of one dimensional signal, a 1D sinusoid is modulated with a Gaussian. In the case of two dimensional signals such as images, a 2D sinusoid is modulated with a Gaussian [16]. 2-D Gabor filter in the spatial domain is given by the equation (9)

$$G(x, y, \theta, u, \sigma) = \frac{1}{2\Pi\sigma^2}\exp\left\{-\frac{x^2 + y^2}{2\sigma^2}\right\}\exp\{2\Pi i(uxcos\theta + uysin\theta)\} \quad (9)$$

Where θ the orientation function, σ is the standard deviation

The features can be extracted using a set of Gabor filters [16]. The 2-D Gabor in the discrete domain is given by equations (10) and (11).

$$G_c[i, j] = Be^{\frac{-(i^2+j^2)}{2\sigma^2}}\cos\big(2\Pi f(icos\theta + jsin\theta)\big) \quad (10)$$

$$G_s[i, j] = Ce^{\frac{-(i^2+j^2)}{2\sigma^2}}\sin\big(2\Pi f(icos\theta + jsin\theta)\big) \quad (11)$$

where B and C are normalizing factor, f specifies the frequency

3.2.4. LBP features

Local Binary Pattern (LBP) is a type of visual descriptor that is used for classification in computer vision. It is a dominant feature for texture classification [17]. LBP thresholds the 3×3-neighborhood and labels the pixels of an image with its center values [17] and the result is converted and represented into binary number which is represented by equation (12).

$$LBP_{p,r} = \sum_{n=0}^{p-1} s\big(x_{r,n} - x_{0,0}\big)2^n,\ s(x) = \begin{cases}1, x \geq 0\\ 0, x < 0\end{cases} \quad (12)$$

LBP operator has two extensions. First is that LBP with different size of neighbourhood, in this it is able to operate on texture with different scales. The second is uniform patterns, if there is a one 0-1 and one 1-0 transitions then the LBP is uniform, when (8, 1) neighbourhood is used, it accounts for 90% bit less and about 70% in the case of (16, 2) neighbourhood. Interpolation is used when the gray values are not present in the pixel position [18]. For an image I of size N×M, the histogram h of length for a texture image is given by equation (13).

$$h(k) = \sum_{i=1}^{N}\sum_{j=1}^{M}\delta(LBP_{p,r}(i, j) - k) \quad (13)$$

where LBPp,r(i,j) identified pattern of each pixel (i,j)
$0 \leq k \leq K-1$ and $K=2^P$ is the number of LBP codes.

3.3 Classifier

Classifier maps the feature space to a label, classifier plots the training data in the multidimensional space and then it plots the testing data into the same and performs comparison of the data points between testing and training to determine the correct class for each individual [18]. Accuracy of the classifier is calculated by determining its performance on a known set of objects [19].In this section K-NN and LDA classifier is explained.

3.3.1 *k*-Nearest neighbour

k-NN classifier is a non-parametric discrimination technique [20]. Classification is done by defining the comparison by finding the distance between the objects in the training data, *k*-NN algorithm finds the *k*-nearest neighbours of the test sample in the training data. [21] The important learning task performed by *k*-NN is to determine the two factors: they are the number of neighbours denoted as '*k*' and the distance metric denoted as 'd'. Appropriate value of *k* can be selected by changing different values and loading the results in a separate test set. When the value of *k* is fixed, then there is variation of size of neighbourhood. If the value of *k* is small, then the variation in the neighbourhood size is small and hence the classification is done using few data points, hence in the classifier in unbalanced. If the value of the *k* is very large then there is deviation of neighbourhood and the real class [20]. Let T be the training sample, then the test sample will be assigned to the majority class of *k*-samples which is given by the equation (14).

$$T = \{(x_i, c_j; i = 1, \ldots\ldots, N)\} \quad (14)$$

where c_j represents the label of the class.

k-NN algorithm determines the distance between the test sample (x) and the elements in the training set and determines the *k*-nearest neighbour which is given by the equation (15).

$$d(x, x_k) = \min(d(x, x_i)) \quad (15)$$

The predicted class $\hat{c} = c_k$ represents the majority class identified by the *k*-nearest neighbor. The decision rule of the classifier is to assign the label to the test sample given by the equation (16).

$$\hat{c} = \arg\max_c \sum_j I(V = class((c_j)) \quad (16)$$

3.3.2 Linear Discriminant Analysis (LDA)

Classification is used to place an object into one class based on its characteristics. If the data in the test set is properly classified then the classifier has high accuracy [21]. If the data in the test set is misclassified then the classifier is not a correct model [21]. LDA is a supervised technique which is used for classification and dimensionality reduction. In LDA the implementation requires all the samples to be available in advance [22]. LDA involves the following mathematical steps,

a) The data sets and the test sets are formulated, which is calculated in the original space. The data sets is represented by a matrix consisting of features which is given by the equation (17)

$$\text{set } 1 = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ \cdots & \cdots \\ \cdots & \cdots \\ a_{m1} & a_{m2} \end{bmatrix} \&\text{set } 2 = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & a_{22} \\ \cdots & \cdots \\ \cdots & \cdots \\ b_{m1} & b_{m2} \end{bmatrix} \quad (17)$$

b) Let $\mu_1 \text{and} \mu_2$ be the mean of set 1 and set 2 respectively and μ_3 represent the mean of the entire data, then the mean of the entire data is given by equation (18)

$$\mu_3 = p_1\mu_1 + p_2\mu_2 \quad (18)$$

where p_1 and p_2 are the probabilities of the classes.

c) After the calculation of mean of the entire data, scatter matrix is computed by using the equation (19)

$$S_w = \sum_j p_j(\text{cov}_j) \quad (19)$$

d) The covariance matrix is computed using the equation (20)

$$\text{cov}_j = (x_j - \mu_j)(x_j - \mu_j)^T \quad (20)$$

e) The between class scatter is computed using equation (21)

$$S_b = \sum_j(\mu_j - \mu_3) \times (\mu_j - \mu_3)^T \quad (21)$$

f) The optimizing factor for class dependent type is calculated by using equation (22)

$$\text{crirerion}_j = \text{inv}(\text{cov}_j) \times S_b \quad (22)$$

g) The optimizing factor for class independent type is calculated by using equation (23)

$$\text{criterion} = \text{inv}(S_w) \times S_b \quad (23)$$

3.4. Confusion matrix

Confusion matrix is a table layout, which visualizes the performance of an algorithm. In the confusion matrix the column specifies predicted classes and the row specifies the actual classes, this matrix is used to determine how one class is confused with the other classes [23]. It is also known contingency table [24]. It is the standard representation of output in the classification [25]. It is an N×N matrix where N specifies the number of labels (classes), the performance of the matrix is evaluated by using the data in the matrix. If the diagonal entries are correctly classified then the accuracy is 100%. Table 2 specifies the confusion matrix for a two class classifier.

Table-2. Confusion matrix for a two-class classifier.

	Predicted class	
Actual Class	a	b
	c	d

a) a is the correct predictions that the instance is negative.
b) b is the incorrect predictions that the instance is positive.
c) c is the incorrect predictions that the instance is negative.
d) d is the correct predictions that an instance is positive.

The terms defined for a performance evaluation of a 2 class matrix are as follows [24]:

A) Accuracy (AC): Accuracy is the ratio that the number of predictions is correct accuracy is given by the equation (24).

$$\text{AC} = \frac{a+d}{a+b+c+d} \quad (24)$$

B) True positive rate or Recall (TP): Recall is the ratio of positive cases that were correctly identified; true positive is calculated using the equation (25).

$$TP = \frac{d}{c+d} \quad (25)$$

C) False Positive Rate (FP): False positive rate is the ratio of negative cases that were incorrectly classified as positive; it is calculated using the equation (26).

$$FP = \frac{b}{a+b} \quad (26)$$

D) True negative rate (TN): True negative is ratio of negative cases that were correctly classified; true negative is calculated using the equation (27).

$$TN = \frac{a}{a+b} \quad (27)$$

E) False Negative Rate (FP): False negative rate is the ratio of negative cases that were incorrectly classified as negative; it is calculated using the equation (28).

$$FN = \frac{c}{c+d} \quad (28)$$

3.5 Decision level fusion

Image Fusion is the method of combining significant information from two or more images into a single image, the resultant image is more informative than the input images. Decision level fusion is performed at decision level when the decisions are available by the individual matcher [26]. Decision level is based on binary hypothesis, it is based on the threshold i.e. the decision is

considering the presence or absence of the individual which is denoted as 1 and 0 respectively [27]. The biometric verification has two problems they are, firstly hypotheses are H0: Score(s) indicates an authorization, secondly H1: Score(s) indicates an un-authorized user.

Decision level fusion can be implemented by using the rules like "AND" or "OR", majority logic function. The rules provide the information regarding whether the user is authenticated or unauthenticated. The authors in [28] proposed majority logic function rule. The author in [29] proposed AND/ OR rules for deciding the decision. Majority logic is the frequently used approach, the input sample is given the identity in which majority of the matchers are approved. AND & OR rules are used infrequently, because as they combine two different matchers, and also these two methods degrades the performance. The major advantage of the majority logic method is that neither it requires previous information about the matcher nor the training is required for final decision making. In the proposed method three biometrics are used and hence to fuse the biometrics in the decision level, Majority logic is used, truth table of majority logic is shown in Table-3.

Table-3. Truth table of majority logic.

x	y	z	F(x,y,z)
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

4. RESULTS AND DISCUSSIONS

The proposed work uses three biometrics i.e., face fingerprint and iris, to overcome the limitation of single modal biometric. In this work multimodal biometrics are considered, hence fusion is accomplished in order to increase the authentication accuracy. The features are extracted for each individual biometric and accuracy is calculated for each individual. Later in order to increase the authentication accuracy, fusion is performed at decision level using majority logic. The experiment was carried out using MATLAB version R2013a.

Fingerprint images are acquired from the FVC2002 database. The database contained images of 40 individual with 8 images per each individual. Among the 40 individuals, 20 individual was selected with 6 images per each individual, from the selected 120 images a matrix of 1×120 is created by labelling the 20 individuals such that the first 6 images represents the fingerprints of first individual and the next 6 images represent the fingerprint of the second individual etc. the similar labelling method was done for 20 individuals and a new database for fingerprint images was created. Training and testing database was created by taking the first 4 images in the training database and the next 2 images in the testing database, hence a training database with 80 images (4 images of 20 individuals) and a testing database with 40 images (2 images of 20 individuals) was created.

After the training and testing database creation, feature extraction was performed. The features for the images in the training database was extracted using LBP (Local Binary Patterns) which extracts the texture features from the fingerprint images and after the feature extraction the feature vector is stored, similar approach is carried out for the images in the testing database. After the feature extraction classification is performed. The features extracted from the training database are used to train the classifier and the features extracted from the testing database are used to test the classifier. The classification is performed using *k*-NN (*k*-Nearest Neighbour). The values of *k* was varied to get the highest accuracy and at *k* =4 maximum accuracy was obtained. The output obtained using *k* -NN classifier is shown in Figure-3.

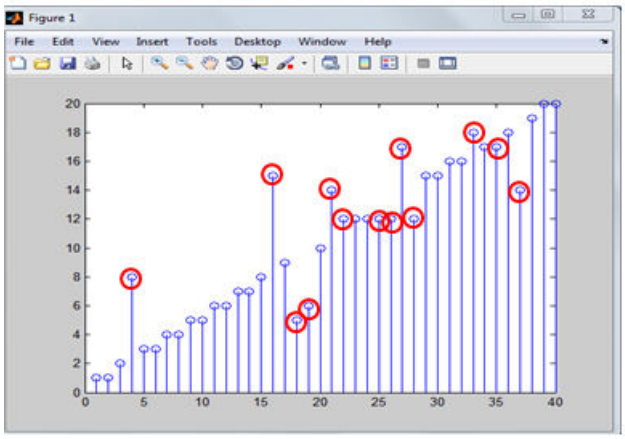

Figure-3. Classification of fingerprint images using *k*-NN classifier.

The Figure shows the classification of 20 individual with 2 images per each individual in the testing database. From the Figure it is observed that 13 individuals are misclassified belonging to other class which is highlighted as shown in the Figure. Hence, the authentication accuracy is calculated by using confusion matrix as shown in Figure-4.

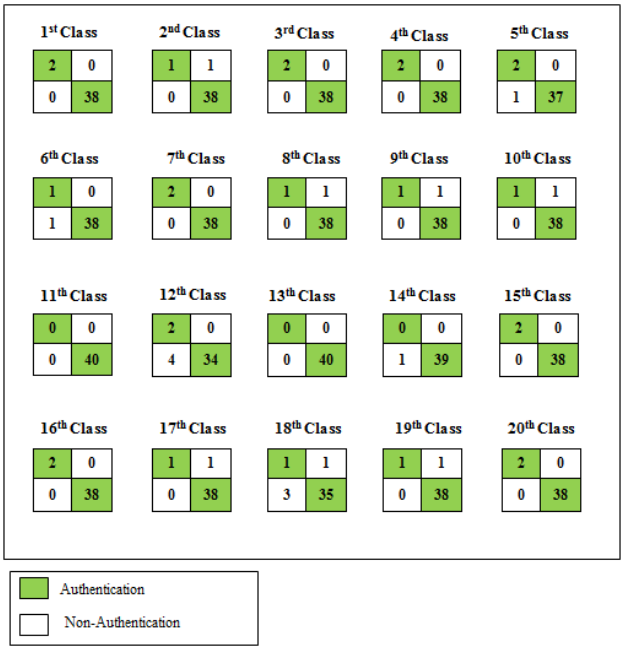

Figure-4. Confusion matrix for calculating the authentication accuracy of fingerprint.

The diagonal values specify that the classes are correctly classified, the value other than diagonal specifies the misclassification, and the accuracy is calculated, which is the ratio of sum of diagonal elements to the total number of individuals, accuracy for fingerprint images is given by equation (29).

$$\text{Accuracy} = \frac{784}{800} = 98\% \quad (29)$$

Face images are acquired from the Faces94 database. The database contains images of 40 individual with 20 images per each individual. From the 40 individuals available in the database, 20 individual was selected with 6 images per each individual. Creation of training and testing database is similar to that was followed for the fingerprint images. After the creation of training and testing database, feature extraction was performed. The features for the images in the training database are extracted using Gabor filter which extracts the texture features from the face images and after the feature extraction the feature vector is stored, similar approach is carried out for the images in the testing database. After the feature extraction classification is performed. The features extracted from the training database are used to train the classifier and the features extracted from the testing database are used to test the classifier. LDA is used for classification; the classifier classifies the images in the testing database to one of the classes in the training database. Similarly the authentication accuracy is calculated using the confusion matrix which is given by the equation (30).

$$\text{Accuracy} = \frac{795}{800} = 99.3\% \quad (30)$$

Iris images are acquired from the UPOL database. The database contains images of 56 individual with 6 images per each individual. From the 56 individuals available in the database, 20 individual with 6 images per individual was selected. Training and testing database was created in a similar way which was done for fingerprint. The features for the images in the training database are extracted using GLCM and affine moments that is used to extract the texture and shape features from the iris images and after the feature extraction the feature vector is stored, similar approach is carried out for the images in the testing database. After the feature extraction, classification is performed. The features extracted from the training database are used to train the classifier and the features extracted from the testing database are used to test the classifier. LDA is used for classification; the classifier classifies the images in the testing database to one of the classes in the training database. Similarly the authentication accuracy is calculated using the confusion matrix as it was done for fingerprint, which is given by equation (31).

$$\text{Accuracy} = \frac{780}{800} = 97.5\% \quad (31)$$

Table-4. Specify the performance evaluation of individual biometrics which is calculated using the values in the confusion matrix.

Table-4. Performance evaluation of biometrics.

Terms for performance evaluation	Face	Fingerprint	Iris
Accuracy(%)	99.3%	98 %	97.5%
True positive rate	1	0.80	0.75
False positive rate	0.065	0.0130	0.0143
True negative rate	0.99	0.94	0.99
False negative rate	0	0.21	0.25

Figure-5. Shows the plot of true positive rate of each individual biometric, if the value of true positive is closer to one it specifies the better performance.

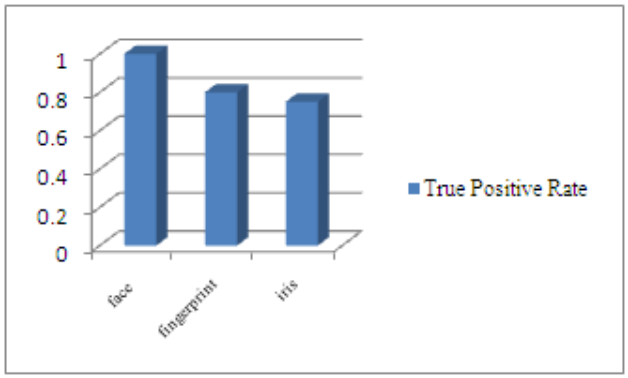

Figure-5. True positive rate for single modal biometrics.

Figure-6 shows the plot of false positive rate of each individual biometric, if the value of false positive is closer to zero it specifies the better performance.

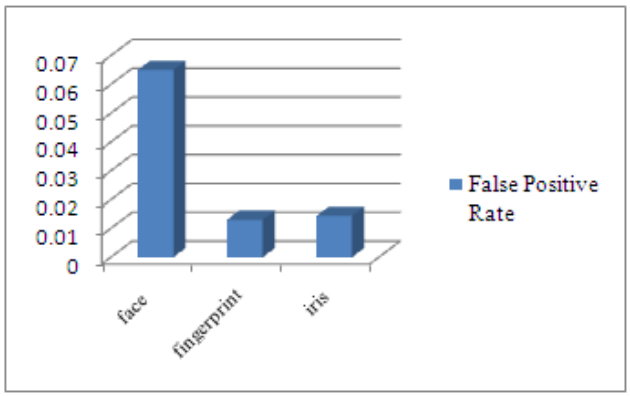

Figure-6. False positive rate for single modal biometrics.

Figure-7 shows the plot of true negative rate of each individual biometric, if the value of true negative is closer to one it specifies the better performance.

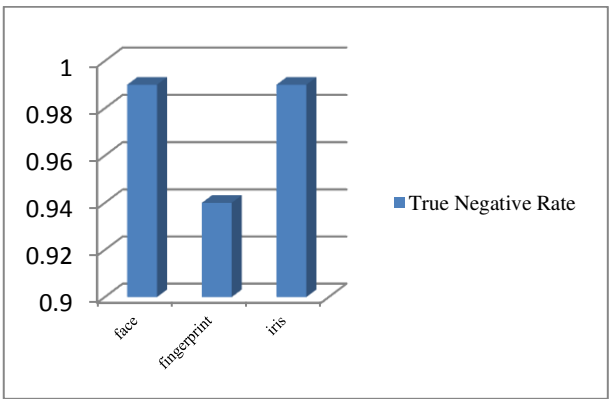

Figure-7. True negative rate for single modal biometrics.

Figure-8 shows the plot of false negative rate of each individual biometric, if the value of false positive is closer to zero it specifies the better performance.

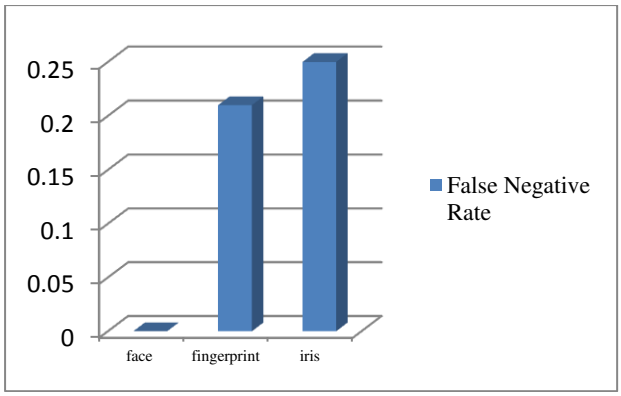

Figure-8. False negative rate for single modal biometrics.

The feature from each biometric is extracted and individual authentication accuracy is calculated. Decision level fusion is done using majority logic, since three single modal biometrics (Face, Fingerprint and Iris) are considered; fusion is performed using majority logic. If the person is correctly classified then the decision is represented by logic-1 else logic-0, the Decision Level Fusion using Majority Logic Function is given in Table-5.

Table-5. Decision level fusion using majority logic function.

S. No.	Face	Iris	Finger print	Majority logic
1	0	0	0	0
2	0	0	1	0
3	0	1	0	0
4	0	1	1	1
5	1	0	0	0
6	1	0	1	1
7	1	1	0	1
8	1	1	1	1

Based on the values specified in the table, the individual is identified as authenticated and unauthenticated. The decision of 40 images taken in the testing database falls within any one of the combination specified in the table, since for 3 biometrics the number of combination is 2^3. Figure-9 shows the comparison of accuracy of individual biometrics and fusion using majority logic function. From the Figure it is clear that the authentication accuracy has been increased by using decision level fusion which resulted in an accuracy of 99.6% which is obtained by using the confusion matrix. Hence by using fusion authentication accuracy can be increased.

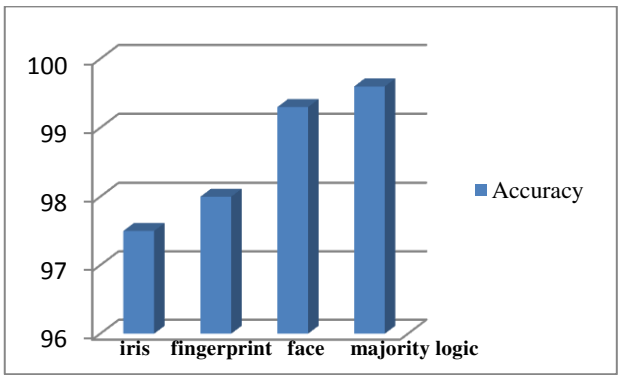

Figure-9. Comparison of accuracy of each biometric and the fusion using majority logic.

5. CONCLUSIONS

In order to overcome the limitations of single modal biometric, multimodal biometric is used. In the proposed work face, iris and fingerprint images were considered. The feature from each individual was extracted, the features from face, iris and fingerprint were extracted using Gabor filter, GLCM and affine moments and LBP features extraction algorithm respectively. The authentication accuracy obtained is 97.5%, 97.8%, and 99.3% for iris, fingerprint and face respectively. Fusion was done at decision level; majority logic was used since three biometric was considered. The main advantage of the proposed work is that the accuracy obtained after fusion is 99.6% which is high when compared to the accuracy that was obtained by the other researches which was reviewed in the literature and also three biometrics was used in the proposed work where others have carried out using two biometrics. The main application of the proposed work is that it is used in Adhaar authentication.

REFERENCES

[1] Rattani A, Kisku D R, Bicego M, Tistarelli M. 2007. Feature Level Fusion of Face and Fingerprint Biometrics. IEEE. pp. 1-6.

[2] Uniqeidentieication authority of India, www.uidai.gov.in.22/04/ 2012.

[3] Vijayalakshmi G V, Raj A N J., Varma A. 2014. S V S K3 Optimum selection of features for 2D (color) and 3D (depth) Face Recognition using modified PCA (2D) International Conference on Smart Structures and Systems (ICSSS-2014), Chennai, INDIAB. 2(11): 1-5.

[4] Abdolahi M, Mohamadi M, Jafari M. 2013. Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic. International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307. 2(6): 1-7.

[5] Haghighat M B A, Aghagolzadeh A, Seyedarabi H. 2011. Multi-focus image fusion for visual sensor networks in DCT domain. Computers and Electrical Engineering. 37(5): 789-97.

[6] Vijayarani S, Priyatharsini S. 2015. Facial Feature Extraction Based On FPD and GLCM Algorithms. International Journal of Innovative Research in Computer and Communication Engineering. 3(3): 1-8.

[7] RattaniA, Kisku D R, Bicegon M, Tistarelli M. 2007. Feature Level Fusion of Face and Fingerprint Biometrics. pp. 1-7.

[8] FacialImages: Faces94, http://cmp.felk.cvut.cz/~spacelib/faces/faces94.html, Date accessed: 03/03/2016.

[9] UPOLdatabase, http://drive.google.com/folderview?id=0B41boLTX7jcbNWJh Date accessed: 03/03/2016.

[10] Welcome to FVC2002 web site, http://bias.csr.unibo.it/fvc2002/,Date accessed: 03/03/2016.

[11] Pawar V, Londhe R. 2012. Facial Expression Recognition based on Affine Moment Invariants., IJCSI International Journal of Computer Science Issues. 9(6): 600-604

[12] Mohanaiah P, Sathyanarayana P, Guru Kumar L. 2013. Image texture feature extraction using GLCM approach. International Journal of Scientific and Research Publications. 3(5): 291.

[13] Heikkinen K, Vuorimaa P. 1999. Computation of Two Texture Features in Hardware. Proceedings of the 10th International Conference on Image Analysis and Processing, Venice, Italy. pp. 125-29.

[14] Mashor M Y, Arshad M R, Osman M K. 2008. 3D Object Recognition Using Multiple Views, Affine Moment Invariants and Multilayered Perceptron Network. Research gate. pp. 264-76.

[15] Khalid M, Hosny H. 2008. On the computational aspects of affine moment invariants for gray-scale images, Applied Mathematics and Computation. 195(2): 762-71.

[16] Kong W K, Zhang D, Li W. 2003. Palmprint Feature Extraction Using 2-D Gabor Filters. 36(10): 2339-47.

[17] Rahim M A, Hossain M N, Wahid T, Azam M. 2013. Face Recognition using Local Binary Patterns (LBP). Global Journal of Computer Science and Technology Graphics and Vision. 13(4): 1-9.

[18] Kim J, Kim B, Savarese S. 2012. Comparing Image Classification Methods: k-Nearest-Neighbor and Support-Vector-Machines. Applied Mathematics in Electrical and Computer Engineering. pp. 6-8.

[19] Kenneth R, Castleman C. 1992. Digital Image Processing. 1st Edition. p. 554.

[20] Nait-Ali A, Fournier R. 2012. Signal and Image Processing for Biometrics. p. 336.

[21] Hamalainen W, Vinni M. 2010. Classifiers for educational data mining.

[22] Ghassabeh Y A, Rudzicz F, Moghaddam H A. 2014. Fast Incremental LDA feature extraction. Pattern Recognition, Elsevier. 48(6): 1999-2012.

[23] Divyakant T, Meva C K, Kumbharana K. 2013. Comparative Study of Different Fusion Techniques in Multimodal Biometric Authentication. International Journal of Computer Applications. 66(19): 1-1.

[24] Veeramachaneni K, Osadciw L, Ross A, Srinivas N. 2008. Decision-level Fusion Strategies for Correlated Biometric Classifiers. Proc. of IEEE Computer Society Workshop on Biometrics at the Computer Vision and Pattern Recogniton (CVPR) conference, (Anchorage, USA). pp. 1-6.

[25] Lam L, Suen C Y. 1995. Optimal Combination of Pattern Classifiers. Pattern Recognition Letters. 16(9): 945-54.

[26] Handbook of Multibiometric. http://www.cl.cam.ac.uk/users/jgdlOOO/combine/combine. html. Date accessed: 12/04/2016.

[27] Santra A K, Christy C J. 2012. Genetic Algorithm and Confusion Matrix for Document Clustering, IJCSI International Journal of Computer Science. 9(1-2): 1-7.

[28] Godbole S. 2002. Exploiting confusion matrices for automatic generation of topic hierarchies and scaling up multi-way classifiers. Indian Institute of Technology - Bombay Annual Progress Report.

[29] Gupta A. 2008. Learning Apache Mahout Classification, PACKT publishing, open source community experience distilled Proc. of IEEE Computer Society Workshop on Biometrics at the Computer Vision and Pattern Recogniton (CVPR) conference, (Anchorage, USA). p. 130.