Iris Recognition using Gray Level Co-occurrence Matrix and Hausdorff Dimension

Amol M. Patil
M.E (E&Tc)
S.S.V.P.S.C.O.E
North Maharashtra University

Dilip S. Patil
Asst. Professor in Electronics
S.S.V.P.S.C.O.E
North Maharashtra University

Pravin S. Patil, PhD
H.O.D (E&Tc)
S.S.V.P.S.C.O.E
North Maharashtra University

ABSTRACT
Biometrics authentication is the only accurate solution for personal identification and security problems. Password incorrect use and misapplication, intentional and inadvertent is a gaping hole in security. These results are mainly occurs due to Poor human judgment, carelessness and due to tactlessness. Biometric removes all these types of security mistakes. In iris recognition system identification and verification is one of the efficient method. The objective of this proposed system is to analyze the performance of iris. The segmentation of the iris utilizes shape, intensity, and location information for pupil or iris localization and performs normalization of the iris region by unwrapping the circular region into a rectangular region. The feature extraction of iris was done by biometrics GLCM (Gray Scale Co-occurrence Matrix) and HD (Hausdorff Dimension. The BGM (Biometric Graph Matching) algorithm is used, which is used to match the graph between the training image and test image of the iris biometric. The BGM algorithm uses graph topology to define different feature values of the iris templates. A SVM (Support Vector Machine) classifier is used to distinguish between genuine and imposter. The results give better performance and authentication than the existing method.

Keywords
SVM (Support Vector Machine), BGM (Biometric Graph Matching), Segmentation, IRIS

1. INTRODUCTION
Nowadays, the safety measures for the systems are becoming more and more important and useful. The authentication plays a major role in the line of defense, identity card and passport verification. There are three main types of authentication such as password, card or token, biometric. Biometrics is used for recognizing person physical or behavioral characteristics. There are different types of biometrics are used like finger print, retina, face recognition, voice pattern analysis etc. Among all biometrics iris is one of the best biometrics. The security is not well in many of the system such as banking, finance transaction, sales and law enforcement. So confidentiality should be provided. Iris biometrics is for personal identification before that all the characteristics are to be verified by using various techniques. Biometrics additionally gives a secure method of authentication and identification, as they are difficult to repeat and steal. Behavioral characteristics include keystroke dynamics, signature, voice pattern and physical characteristics include iris, Palm print, face recognition A biometric system process by collecting and storing the biometric information and then comparing the input biometric with what is stored in the repository. Out of all the variety of physical characteristics existing, irises are one of the more perfect and accurate physiological characteristics that can be use.

2. PRESENT STATUS
Currently in Iris recognition system moreover study and research is going on localization and authentication. Like segmentation algorithm using Daugman's Algorithm, This method was proposed in 1993 and was the first method was successfully implemented in working biometric system [5]. Yulin Si proposed various novel approaches to improve overall performance of iris recognition system. This paper uses new eyelash detection algorithm based on directional filters which achieves a low rate of eyelash misclassification. Second, a multiscale and multidirection data fusion method is introduced to reduce the edge effect of wavelet transformation produced by complex segmentation algorithms [2]. Another author Seyed Mehedi proposed automatic retina verification framework based on the biometric graph matching (BGM) algorithm [3]. The BGM algorithm, a noisy graph matching algorithm, robust to translation, non-linear distortion, and small rotations, is used to compare retinal templates. The BGM algorithm uses graph topology to define three distance measures between a pair of graphs, two of which are new. A support vector machine (SVM) classifier is used to distinguish between genuine and imposter comparisons. Using single as well as multiple graph measures, the classifier achieves complete separation on a training set of images from the VARIA database (60% of the data), equaling the state-of-the-art for retina verification. Because the available data set is small, kernel density estimation (KDE) of the genuine and imposter score distributions of the training set are used to measure performance of the BGM algorithm. An efficient indexing mechanism proposed by Somnath Dev [7] to retrieve iris biometric templates using Gabor energy features. The Gabor energy features are calculated from the preprocessed iris texture in different scales and orientations to generate a 12-dimensional index key for an iris template. An index space is created based on the values of index keys of all individuals.

3. PROPOSED SYSTEM
Biometrics refers to automatic identification of a person on a basis of his or her unique physiological or behavioral characteristics. Behavioral biometrics includes signatures, voice recognition, gait measurement, and even keystroke recognition. The four efficient methods for iris localization are present. Out of these three methods of iris localization in circular form and one method uses unwrapping the iris in to a flat bed. Experimental results are reported to demonstrate

performance evaluation of every implemented algorithms proposed by Dr. Pravin S. Patil [1]. Using this paper as a reference following proposed system is derived the physiological biometrics includes facial recognition, fingerprinting, hand profiling, iris recognition, retinal scanning, and DNA testing. Behavioral methods tend to be less reliable because they are easier to duplicate. Biometric methods based on physiological attributes are more trusted. Among that method, iris recognition is gaining much attention as an accurate and reliable one. To improve accuracy, most of the biometric authentication systems store multiple templates per user to account for variations in biometric data. Therefore, these systems suffer from storage space and computational overheads. In order to address these issues, there is need to optimize the computational and storage complexities by creating a reliable specimen iris template per user rather than maintaining multiple templates. This paper presents a new approach to enhance the performance of iris recognition systems.

3.1 IRIS Segmentation

From the eye image the iris part is separated using image segmentation. The edges of the iris inner and outer boundaries are located and detected using Canny edge detector [1], uses feature extraction and edge detection techniques. The complex iris pattern is detected using Gaussian Hermite moment. This shape information provides the discriminating features for iris recognition. But these shapes are smaller in size so it is difficult to extract the edge information out of these shapes. Therefore we found that these irregular blocks cause noticeable local intensity variations in the iris images. In canny edge detection the thresholding for the eye image is done in a vertical direction only, so that the causes due to the eyelids can be decreased. The Hough transform is used for finding out the circles in the iris image and reduces a pixel on the boundary of the circle. The location of the edge can be obtained even with the nonappearance of few pixels. It is also quicker since the boundary pixels are lesser for computation. The weak edges of below threshold are removed by the use of hysteresis thresholding. For each edge point of different radii circles is formed. From all circles the maximum sum is calculated and is used to find the circle radii and centre. The Hough transform is one more way of detecting the parameters of geometric objects. Following parameters are calculated using GLCM,

1) Homogeneity
2) Contrast

```
cmap = [f f f];
nargin < 2, m = size(colormap,1)
xmin = min(min(x))
xmax = max(max(x))
x = round(m-1)*(x-xmin)/(xmax-xmin))
f = find(diff(sort([x(:); (0:m)'])))
f = f/max(f)
```

3) Energy
4) Correlation
5) Entropy = E = -sum(p.*log2(p))
6) Solidity

3.2 IRIS Normalization

In normalization the iris region is normalized by converting circular into rectangular regions. Here, interpolation is used for unwrapping circular intensity into polar intensity. Displacement of pupil center from the iris center and radius around the iris is calculated. Hausdorff dimension of eye image is calculated using following parameters.

1) Mean = sum(x(:), [], 'double') / numel(x)
2) Standard Deviation = √(offset summation / total pixels)
3) Area = Area*10^{-3}
4) Perimeter =
5) Eccentricity
6) Major Axis length
7) Minor Axis Length
8) Solidity
9) Homogeneity

Fig 2 shows segmented image obtained after the normalization of iris image. Rings overlaying on original iris image are obtained by getting the pixel coordinates for circle around iris and pupil. An iris matching system has been presented based on the Biometric Graph Matching algorithm. The iris image was segmented. A set of images are taken and finding out the features values. Assuming, the first five values of the databases is authenticate and the next five values are assumed to be unauthenticated. Training image is compared with the test images. A spatial graph was generated from the texture, color and shape feature values and graph was plotted for the input image and a set of training image. Compare the both the graph to find out whether authorized or unauthorized person.

4. HAUSDORFF DIMENSION BY BOX COUNTING METHOD ALGORITHM

A quantitative analysis of perimeter roughness is carried out to illustrate the degree of roughness of input images. Commonly known as the Hausdorff Dimension (H.D.), the algorithm shown in figure 3 gives the aggregate perimeter roughness as a fractal dimension. The fractal dimension describes the complexity of an object; in the case of devices presented here, this algorithm gives perimeter roughness which implies parasitic emission sites for extremely rough perimeters [1]. On Hausdorff Dimension scale, a dimension of 1 equates to a smooth line, while 2 implies fractal complexity like that of a Julia set, and because the devices presented here are considered truncated fractals, the fractal dimension calculated is bound by the above limits, i.e. 1 < H.D. < 2. The algorithm to achieve this starts with an input electron micrograph image uploaded within Matlab (figure 3), then the Canny algorithm [2] is employed to find the edge within the image and superimposes a grid of N squares over the edge, while counting the occupied squares that the edge passes through (top right, N(s)). This is continued for an increasing number of squares and the fractal dimension (H.D) is given by the gradient of the logarithm of the number of squares log N, over the number of squares occupied by the

edge log N(s), as indicated by figure 3 (bottom) and equation (1)

$$H.D = \frac{\log N}{\log N(s)} \quad \ldots\ldots (1)$$

5. SUPPORT VECTOR MACHINE (SVM)

SVM is applied for classification of data members. Data members or in data points there are two things which may be genuine or imposter. The exact method is to classify the two data points is hyper planes. The margin denotes the maximum width in the hyper planes. The support vector is the data sets used to classify the vectors. To differentiate among objects of dissimilar class memberships are known as hyper planes classifiers. Support Vector Machines are specifically to perform this type of action. If the data sets are not allowed for separating the hyper planes in that case use soft margin. It means hyper planes that separate many of the data points but not all data points. To construct optimal hyper planes, SVM applies an iterative training algorithm which is used to reduce a fault acceptance. SVM supports classification, regression and also it can handle categorical variable and multiple continuous. For categorical variables multiple dummy variables are created with 0 and 1.

6. RESULTS

In this paper given input image is segmented for localization, normalization and analyzed the feature vector. Each testing iris is matched against each stored database template at each level. An genuine and imposter matching is defined as the matching between iris features of training image and iris features of test image. Here, the parameters for the iris are calculated. And getting 97.5% efficiency .Total we had used 10 persons iris image. And in this 1 to 7 is authorized person and 8 to 10 are non authorized person. For database training 30 images used means 3 images from each person 3x10=30. Final GUI of the paper is shown figure no. 7. That GUI provides all the tabs for Iris normalization, Feature extraction and localization. That provides final authorization comparing database iris images with the test image. After iris segmenation and normalization database is tarined and for that waitbar is done for processing.

7. CONCLUSIONS

The proposed method involves the biometrics details is extracted by using two technique such as GLCM (Gray Scale Co-occurrence Matrix) and Hausdorff Dimension (HD). From GLCM texture features like energy, contrast, entropy, Correlation Coefficient, homogeneity are extracted. Shape features like standard deviation, mean and shape features like area, perimeter minor axis length, major axis length, solidity, eccentricity are calculated from Hausdorff Dimension (HD). and comparing both the value in a graphical representation in BGM. Finally, Support Vector Machine (SVM) is used to classify whether the person is authorized or unauthorized. In future work this limitation can be addressed by multimodal biometrics system to combine both the biometric characteristics derived from one or modalities such as Palm print and iris which give high level of security and different secure applications. The parameters for GLCM and HD for authorized person are given in following table 1.0.

Table 1 : Parameters of GLCM and HD

SR. NO.	Parameters of GLCM and HD	
1	Homogeneity	0.0321
2	Contrast	16.9931
3	Energy	2.4160
4	Correlation	0.0051
5	Entropy	0.5782
6	Hausdorff Dimension	1.4327
7	Mean deviation	0.5344
8	Standard deviation	0.0383
9	Area	4.139
10	Perimeter	819.1269
11	Eccentricity	0.9965
12	Major Axis	269.1817
13	Minor Axis	22.4926
14	Solidity	0.8622
15	Homogeneity	0.0321

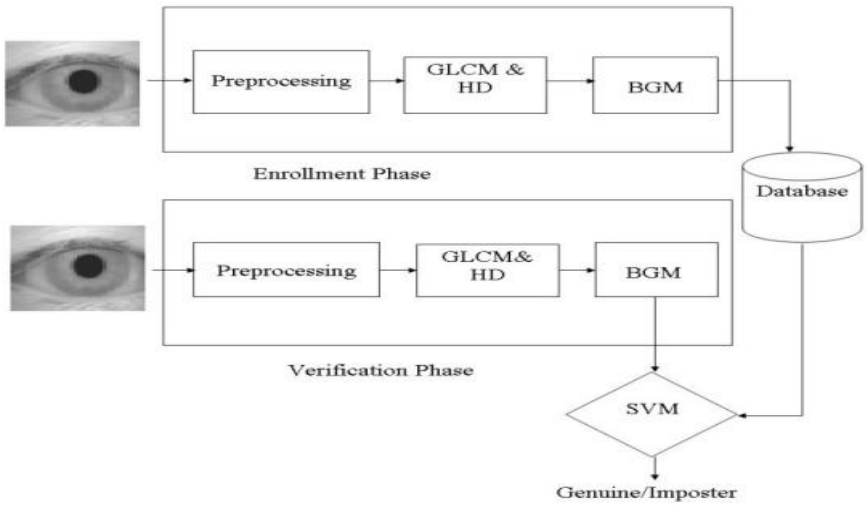

Fig. 1: Block Diagarm of proposed iris recognition system

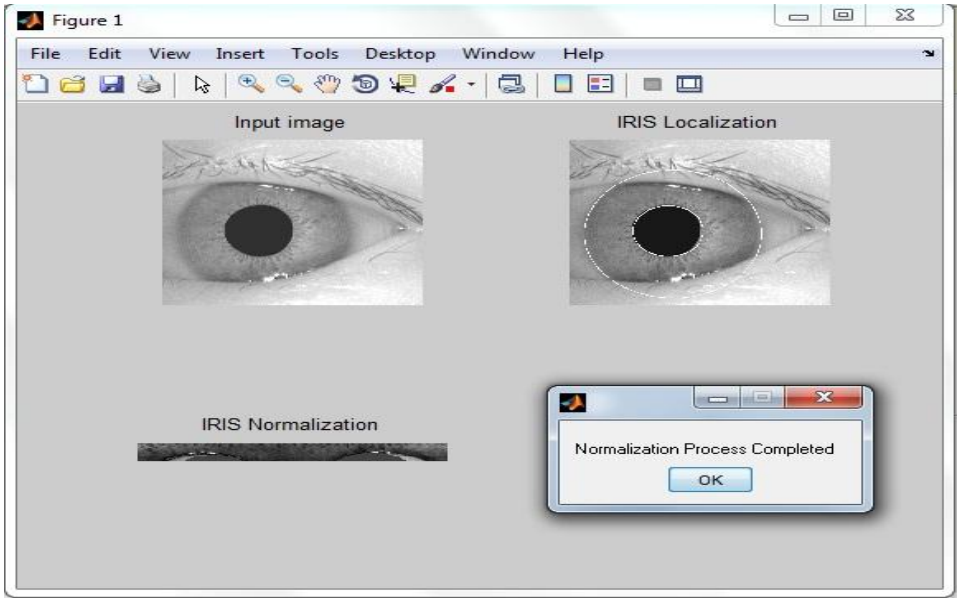

Fig. 2 : Normalized and segmented iris image

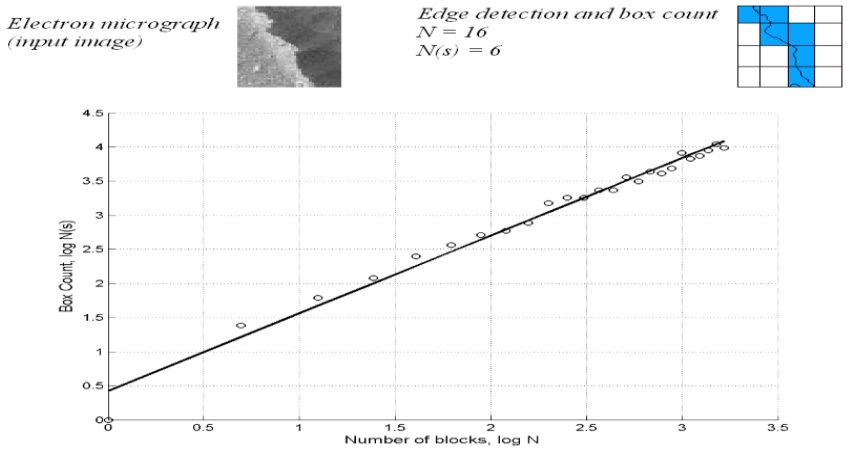

Fig. 3 : Algorithm employed to calculate the Hausdorff Dimension.

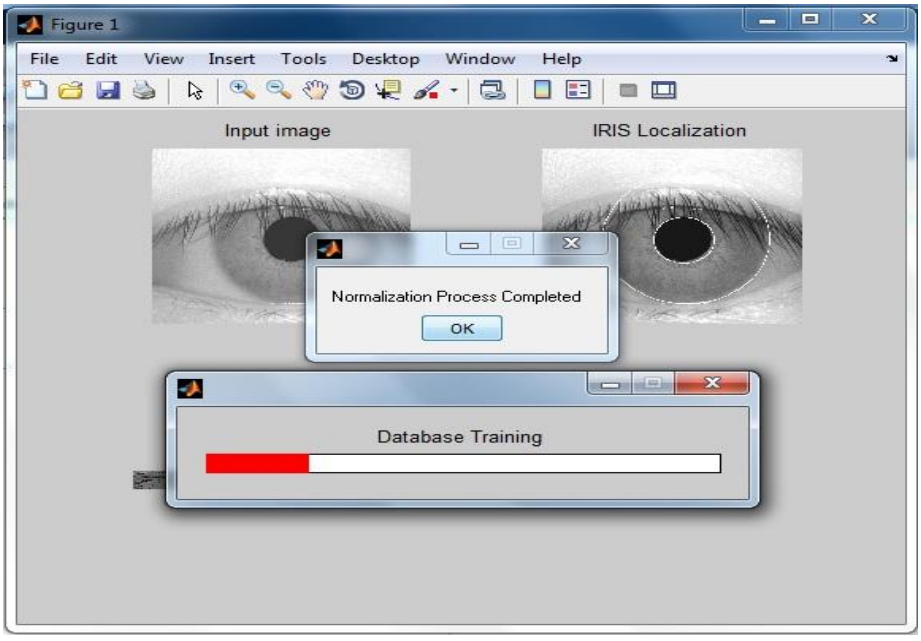

Fig.4 : Database calculations

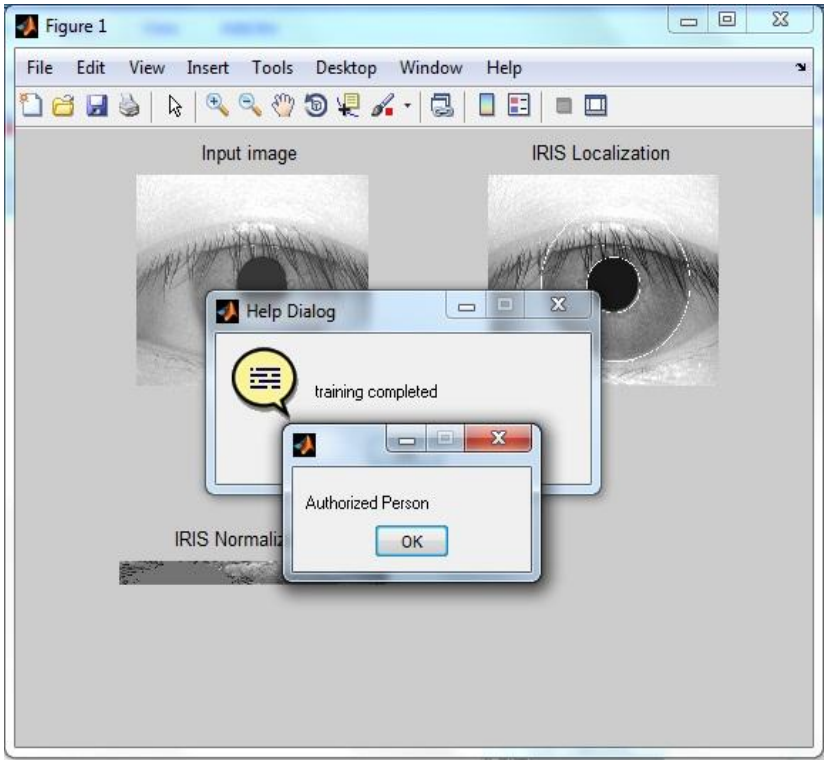

Fig. 5 : Authorized person

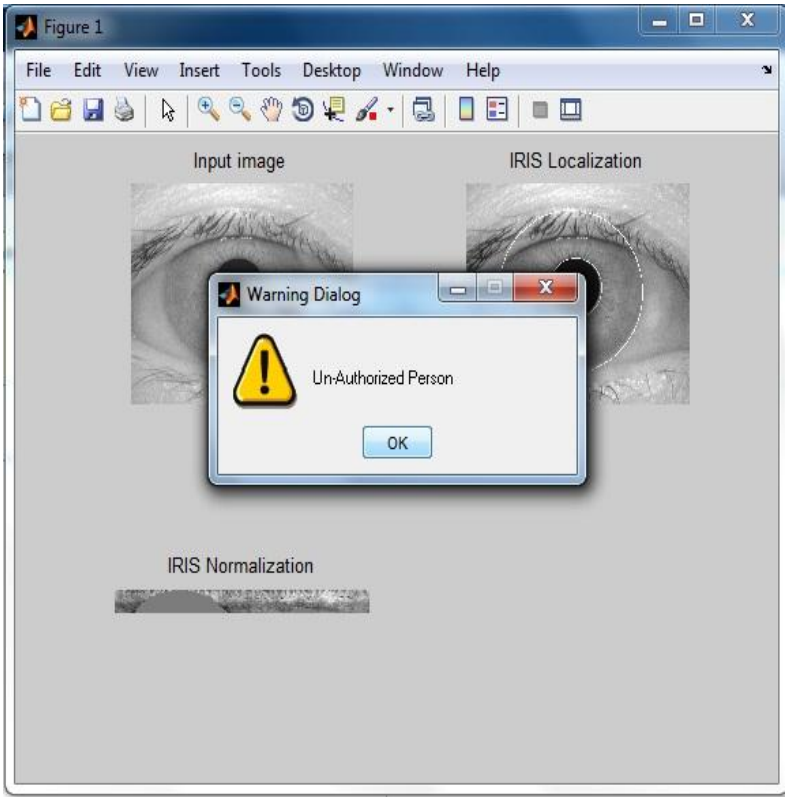

Fig.6 : Person is not authorized

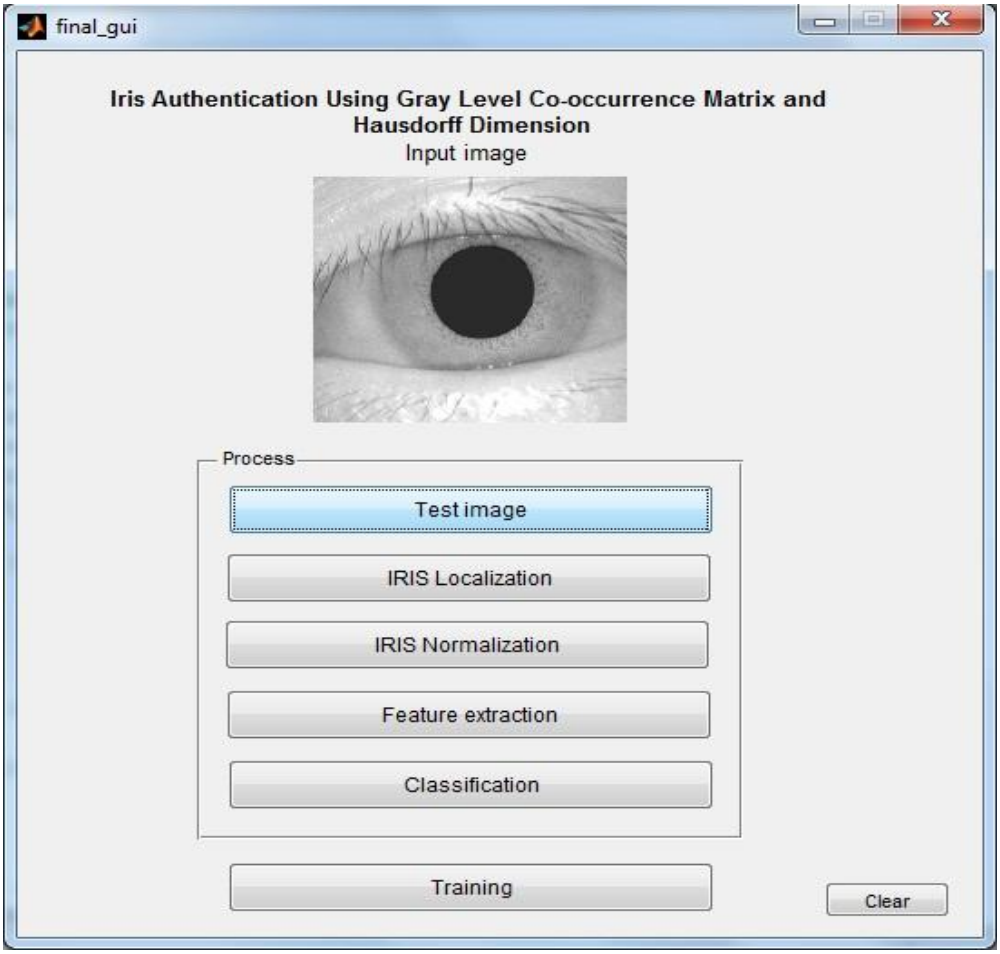

Fig. 7 : Final GUI

8. REFERENCES

[1] Pravin S.Patil "Research on Iris Region Localization Algorithms" Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 4, Issue 10 (Part - 3), October 2014, pp.111-119

[2] Yulin Si, Jiangyuan Mei, and HuijunGao, "Novel Approaches to Improve Robustness, Accuracy and Rapidity of Iris Recognition Systems" IEEE transactions on industrial informatics, vol. 8, no. 1, pp.110-117, February 2012.

[3] Seyed Mehdi Lajevardi, Arathi Arakala, Stephen A. Davis, and Kathy J. Horadam, "Retina Verification System Based on Biometric Graph Matching" IEEE Transactions on Image Processing, vol. 22, no. 9, pp.3625- 3635 September 2013.

[4] Pravin S.Patil "Iris Recognition Based On Gaussian-Hermite Moments" International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397, Vol. 4 No. 11 Nov 2012

[5] "Daughman's Algorithm method For Iris Recognition-A Biometric Approach" International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 6, June 2012)

[6] Hugo Proenca, "Toward Covert Iris Biometric Recognition: Experimental Results From the NICE Contests" IEEE Transactions On Information Forensics And Security, vol.7, no. 2, pp.798-808, April 2012.

[7] Somnath Dey, "Iris Data Indexing Method Using Gabor Energy Features" IEEE Transactions on Information Forensics and Security, vol.7, no. 4, pp.1192-1203, August 2012.