ENHANCING LIVENESS DETECTION METHODS IN IRIS CODES FOR IRIS RECOGNITION

J. Vijayaraj
Ph.D. Scholar, Department of
Computer Science and Engineering
Pondicherry Engineering College, Puducherry India

D. Loganathan
Professor, Department of Computer Science and Engineering
Pondicherry Engineering College, Puducherry India

***Abstract*— Iris Recognition methodology is anauthentication mechanism that combines the various methodology. It is used to increase the accuracy of the iris detection method. Iris recognition has inherent weaknesses that can potentially compromise the security of a system. Parodying attacks is one of them and enhanced iris recognition is more vulnerable to parody attack than normal iris recognition method. Parodying is giving duplicate input to the biometric sensor. Parody detection is used to check whether the given input is original or duplicate. The objective is to overcome parodying attacks in iris recognition method. The proposed methodology extracts a set of features from iris using mean, median, variance and local ternary pattern (LTP) techniques respectively and the extracted biometric features are fused and fed to a convolution neural network that employs deep learning to detect parodied features from original features. The proposed method gives better results than the existing liveness detection methods in iris recognition.**

***Index Terms*—CT Image, Image segmentation,Sequential filter, Digital Radiography, Solitary Pulmonary Nodule.**

1. INTRODUCTION

1.1 OVERVIEW

The term biometrics comes from the ancient Greek words bios means life and metrics means measure and refers to recognizing people on the basis of anatomical or behavioral characteristics. Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits.

Biometric System Modules:

A biometric system is designed using the following four main modules

Sensor module:

It captures the biometric data of an individual. An example is a fingerprint sensor that images the ridge and valley structure of a user's finger.

Feature extraction module:

Biometric data is processed to extract a set of salient or discriminatory features. For example, the position and orientation of minutiae points (local ridge and valley singularities) in a finger print image are extracted in the feature extraction module of a fingerprint-based biometric system.

Matcher module:

The features during recognition are compared against the stored templates to generate matching scores. For example, in the matching module of a fingerprint-based biometric system, the number of matching minutiae between the input and the template fingerprint images is determined and a matching score is reported. The matcher module also encapsulates a decision making module, in which a user's claimed identity is confirmed (verification) or a user's

Identity is established (identification) based on the matching score.

System database module:

The biometric system stores the biometric templates of the enrolled users. The enrollment module is responsible for enrolling individuals into the biometric system database. During the enrollment phase, the biometric characteristic of an individual is first scanned by a biometric reader to produce a digital representation (feature values) of the characteristic. The data capture during the enrollment process may or may not be supervised by a human depending on the application. A quality check is generally performed to ensure that the acquired sample can be reliably processed by successive stages. In order to facilitate matching, the input digital representation is further processed by a feature extractor to generate a compact but expressive representation, called a template. . Depending on the application, the template may be stored in the central database of the biometric system or be recorded on a smart card issued to the individual. Usually, multiple templates of an individual are stored to account for variations observed in the biometric trait and the templates in the database may be updated over time.

1.2 ATTACKS AGAINST IRIS BIOMETRIC SYSTEM

Among the potential attacks discussed in the literature Ratha et al. [1], the one with the greatest practical relevance is "spoof attack", which consists in submitting a stolen, copied or synthetically replicated biometric trait to the sensor to defeat the biometric system security in order to gain unauthorized access. Recently, it has been shown that spoof attacks can be carried against many types of biometrics, like fingerprint, face, and iris. This kind of attack is also known as "direct attack", since it is carried out directly on the biometric sensor. The feasibility of a spoof attack is much higher than other types of attacks against biometric systems, as it does not require any knowledge on the system, such as the feature extraction or matching algorithm used.

This enhancing liveness detection methods in iris codes for iris recognition can be evaded by an impostor even by spoofing the normal biometric trait.

B. 1.2 OBJECTIVE OF THE STUDY

The objective is to overcome spoofing attacks in iris recognition system .The proposed system extracts a set of features from iris using mean, median, variance technique is used respectively and classifies them as real or fake biometric using hamming distance. The proposed system detects whether biometric input given by the user at the sensor is real or fake.

C. 1.3 MOTIVATION/ NEED FOR THE STUDY

The motivation for this project comes from the literature survey it can be inferred that spoofing attacks on the iris biometric system can be done by the attacker easily without knowing the internal working of the biometric system and the available sensor is not differentiating the real and fake input. This has motivated in the implementation of an anti-spoofing mechanism for the iris biometric system.

2. LITERATURE REVIEW

D. 2.1 SURVEY OF THE RELATED WORK

J. Daugman et al. [1-3] Generally speaking, traditional feature extraction approaches and corresponding iris recognition system can be divided into five major categories roughly: phase-based approaches

Diego et al. [4] proposed Local Binary Pattern. LBP for spoof detection LBP encodes the intensity variations between a pixel and its neighboring pixels. For each pixel, the surrounding pixels and sampled. The result of LBP is a binary code.

Oleg el al. [5] proposed Liveness detection techniques in the area of eye movement biometrics. Two attack scenarios were considered, in which the imposter does and does not have direct access to the biometric database. Liveness detection was performed at the feature- and match score-levels for several existing eye movement biometric techniques. The results suggest that eye movement biometrics are highly resistant to circumvention by artificial recordings when liveness detection is performed at the feature-level.

Mohit et al. [6] proposed to spoof an iris recognition system by synthesizing a semi-transparent contact lens. The Response of Gaussian derivative filters with multiple scales and orientations at each pixel location is clustered using K-means to certain regions with different textures.

Yang Hu et al. [7] proposed to exploits the bits in different position of code by using the spatial relationship. This research attentions on a deeper insight into this binarization method to produce iris codes. The results of spatial relationship is improved binary code.

Ying chen et al. [8] proposed the process of feature extraction and representation based on scale invariant feature transformation and which are orientation probability distribution function based strategy to delete some redundant feature keypoints.
Outperform some of the existing methods interms of correct recognition rate, equal error rate, and computation complexity.

Y. Alvarez-Betancourt et al. [9] use Harris-Laplace, Hessian-Laplace, and Fast Hessian to improve a robust key points based feature extraction method for iris recognition under variable image quality conditions. Outperform recognition on highly or less textured iris images.

Table 2.1 COMPARISON OF IRIS RECOGNITION.

Title	**Author and year**	**Technique**	**Dataset**	**Performance measure**
Iris liveness detection for mobile device based on local descriptors	Diego et al., 2015	Level Feature(Minu tia count)	MobBIOfa ke, MICHE	Error Rate 4.38
Efficient iris recognition based on optimal sub feature selection and weighted sub region fusion	Y. Chen et al.,2014	scale invariant feature transformatio n (SIFT)	ATVS	Accuracy 77.5%
Sub region mosaicking applied to non-ideal iris recognition	T. Yang et al.,2014	Computation -al Intelligence	CASIA	Error Rate 22%
Attack of Mechanical Replicas: Liveness Detection With Eye Movements	Oleg el al., 2015	eye movement	EMDB	Error Rate 16%
A key points-based feature extraction method for iris recognition under variable image quality conditions	Y. AlvarezBetancourt el al., 2016	HessianLaplace, and Fast Hessian	MOBILIVE	Error Rate 11%
Iris Liveness Detection Using Segmentation	Mohit et al, 2015	Texture Segmentation	UPOL	Accuracy 87.5%

3. EXSITING SYSTEM

Iris Recognition system is an authentication mechanism that combines the various methodology. It is used to increase the accuracy of the iris detection system. Iris recognition has inherent weaknesses that can potentially compromise the security of a system. Spoofing attacks is one of them and enhanced iris recognition is more vulnerable to spoof attack than normal iris recognition system. Spoofing is giving fake input to the biometric sensor. Spoof detection is used to check whether the given input is real or fake.

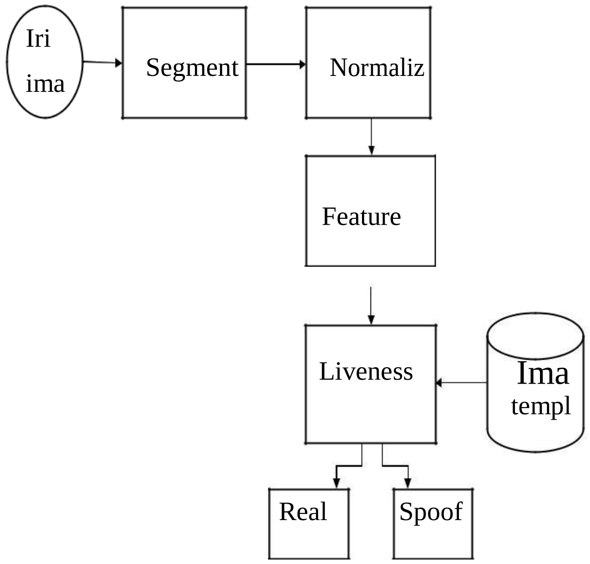


Fig. 3.1 Architecture diagram for the existing system

E. 3.2 MODULES DESCRIPTION

The modules in the existing system are listed below:

Image Acquisition module.

Image segmentation.

Image normalization.

Feature Extraction module.

Classification module.

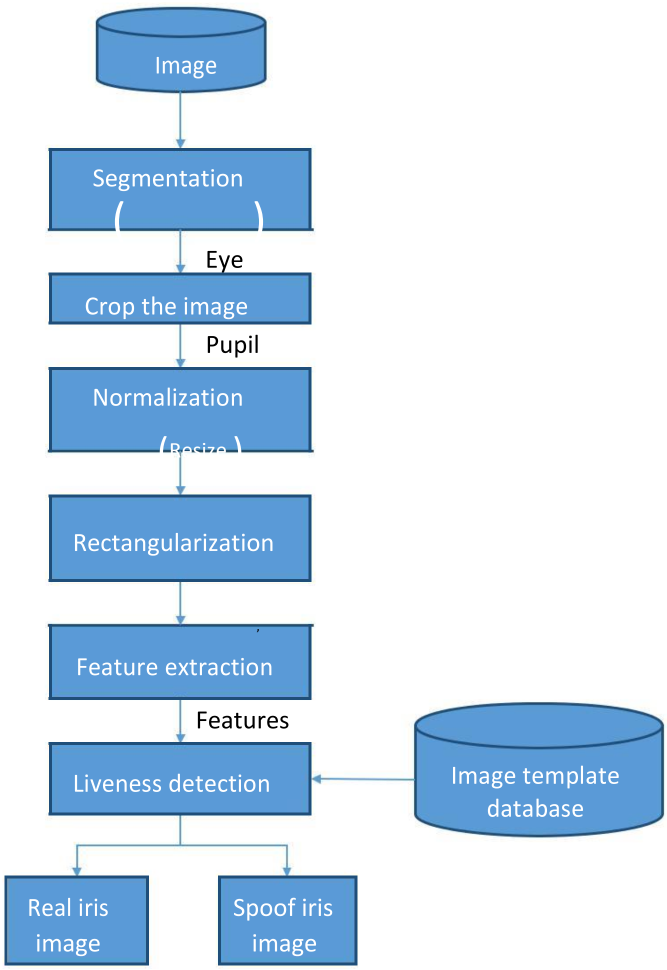


Fig. 3.2 Data flow diagram for the existing system

1) 3.2.1 IMAGE ACQUISITION MODULE

The png images of iris are obtained from user for extracting features. This subsystem comprises of suitable capture devices or sensors. A sensor is required to collect signals from a biometric trait and convert the captured signals into a biometric sample such as iris image.

2) 3.2.2 IMAGE SEGMENTATION MODULE

CANNY EDGE DETECTION

The algorithm runs in 5 separate steps:

➢ Smoothing: Blurring of the image to remove noise.

➢ Finding gradients: The edges should be marked where the gradients of the image has large magnitudes. Compute the derivatives (Dx(x, y) and Dy(x, y)) of the image in the x and y directions i.e., use central differencing.

➢ Non-maximum suppression: Only local maxima should be marked as edges. The

“non-maximal suppression”

The three pixels in a 3 × 3 around pixel (x, y) are examined:

- If Dx(x, y) = 0◦, then the pixels (x + 1, y), (x, y), and (x − 1, y) are examined.
- If Dy(x, y) = 90◦, then the pixels (x, y + 1), (x, y), and (x, y − 1) are examined.
- If Dx (x, y) = 45◦, then the pixels (x + 1, y + 1), (x, y), and (x − 1, y − 1) are examined.
- If Dy(x, y) = 135◦, then the pixels (x + 1, y − 1), (x, y), and (x − 1, y + 1) are examined.

➢ Double thresholding: Potential edges are determined by thresholding.

➢ Edge tracking by hysteresis: The Canny operator is optimum even for noisy images as the method bridge the gap between strong and weak edges of the image by connecting the weak edges in the output only if they are connected to strong edges.

CIRCULAR HOUGH TRANSFORM (CHT)

➢ Circular hough transform is used to transform a set of edge points in the image space into a set of accumulated votes in a parameter space

➢ For each edge point, votes are accumulated in an accumulator array for all parameter combinations.

➢ The array elements that contain the highest number of votes indicate the presence of the shape.

Step1: For every edge pixel (p) find the candidate centerpoint using

= - r * cos( )

= - r * sin( )

Where and is the location of edge point p

∈ [ ] and is thedetermined circle center **Step2**: For range of radius:

➢ The center point is computed.

➢ The Accumulator array is incremented by one for calculated.

Accum [, , r] = Accum [, , r]+1

➢ The point with maximum value in the accumulator is denoted as circle center with radius r

3.2.3 IRIS NORMALIZATION MODULE:

Step1: Localizing iris from an image delineates the annular portion from the rest of the image.

Step2: The annular ring is transformed to rectangular ring.

Step3: The coordinate system is changed by unwrapping the iris from Cartesian coordinate their polar equivalent.

), (,)) → (,) With,
(,) = 0( ) + * cos
(,) = 0( ) +
(,) = 0( ) +
(,) = 0( ) +

- where rp and ri are respectively the radius of pupil and the iris.
- while (xp(θ), yp(θ))and (xi(θ), yi(θ))are the coordinates of the pupillary and limbic boundaries in the direction θ. The value of θ belongs to [0;2], ρ belongs to [0;1]

3) 3.2.4 FEATURE EXTRACTION MODULE

MEAN: Average or mean value.

- S = mean(X) is the mean value of the elements in X if X is a vector.
- For matrices, S is a row vector containing the mean value of each column.

MEDIAN: (Median value)

- For vectors, median(x) is the median value of the elements in x. For matrices, median(X) is a row vector containing the median value of each column.

VARIANCE:

- For vectors, Y = var(X) returns the variance of the values in X. For matrices, Y is a row vector containing the variance of each column of X.

4) 3.2.5 CLASSIFICATION

Database template (S) is matched with the query template (T) using Hamming distance approach

$$MS_{IRIS} = \frac{1}{n * m} \sum_{\substack{i=1 \\ j=1}}^{\substack{n \\ m}} t_{i,j} \otimes s_{i,j}$$

where n X m is the size of template and ⊗ is the bitwise xor. *5) 3.2.6 LIMITATIONS OF EXISTING SYSTEM*

In the existing system the performance is not good and also the error rate is high. The Mean, Median, variance technique is used. It is sensitive to severe lighting changes, to blurred and noisy images and also the fusion stage gives the poor performance and the classification stage is ineffective in learning features.

4. PROPOSED SYSTEM

Reliable user authentication has become very important with rapid advancements in networking and mobility coupled with increased concerns about security. Biometric systems perform recognition based on specific physiological or behavioral characteristics possessed by a user. Biometric systems have now been deployed in various commercial, civilian, and forensic applications for reliable individual recognition.

Iris Recognition system is an authentication mechanism that combines the various methodology. It is used to increase the accuracy of the iris detection system. Spoofing attacks is one of them and enhanced iris recognition is more vulnerable to spoof attack than normal iris recognition system. Spoofing is giving fake input to the biometric sensor. Spoof detection is used to check whether the given input is real or fake.

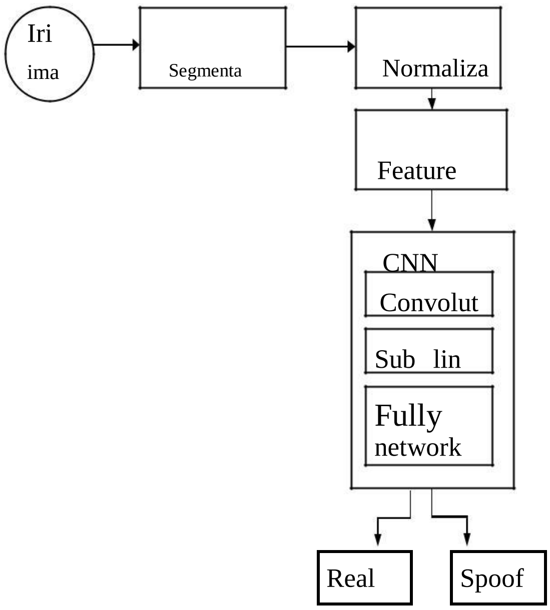


Fig. 4.1: Proposed system

F. 4.2 MODULE DESCRIPTION

The modules in the proposed system are listed below:

Image Acquisition module.

Image segmentation.

iiImage normalization.

Feature Extraction module.

Classification module.

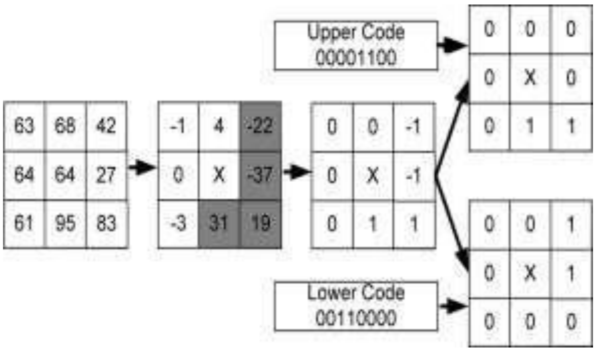
1) 4.2.1 IMAGE ACQUISITION MODULE

The png images of face, iris and fingerprint are obtained from user for extracting features. This subsystem comprises of suitable capture devices or sensors. A sensor is required to collect signals from a biometric trait and convert the captured signals into a biometric sample such as a face image, iris image or fingerprint image.

2) 4.2.2 FEATURE EXTRACTION MODULE

From the Iris image, the local ternary pattern (LTP) is calculated. In LTP the neighborhood pixel values are compared with the central pixel using a lag limit value ‘l’. Based on this comparison the neighborhood values will be assigned one of the three values +1 or 0 or -1.

3) Algorithm: Local Ternary Pattern



4) Fig 4.2: Steps to calculate local ternary pattern (LTP) Steps to calculate local ternary pattern (LTP):

1. Calculate the Local Ternary Pattern (LTP) from the iris image.
2. Compare the neighborhood pixel values with central pixel value.
3. Assign the neighborhood values based on steps 1 and 2.

5) 4.2.3 CLASSIFICATION

The Convolution neural network is used for classification. It contains sampling layer and convolution layer. The architecture of a typical CNN is composed of multiple layers where each layer performs a specific function of transforming its input into a useful representation. The Convolution layer transforms the basis of the CNN and performs the core operations of training. Convolutional layers consist of a rectangular grid of neuron. It performs the convolution operation over the input volume. The SubSampling Layer is placed after the Convolutional layer. It reduces the spatial dimensions (Width x Height) of the Input Volume for the next Convolutional Layer.

Convolutional Neural Networks (ConvNets or CNNs) are category of Neural Networks that have proven very effective in areas such as image recognition and classification.

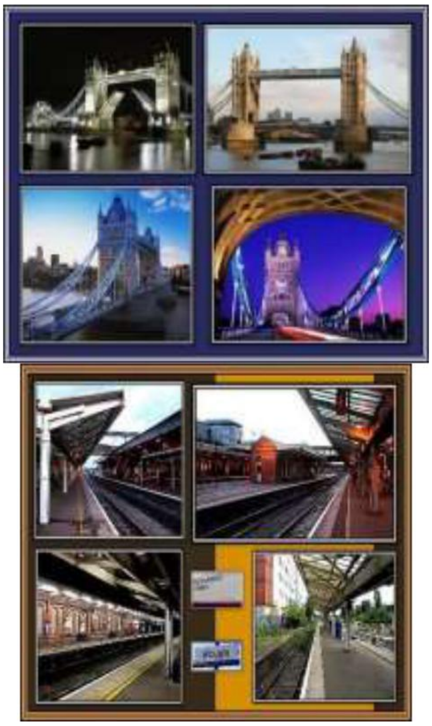


Fig 4.3 : a) bridge b) railway station c) playground

In Figure 4.6 above, a CNN is able to recognize scenes and the system is able to suggest relevant tags such as ‘bridge’, ‘railway’ and ‘playground’ while Figure 4.7 shows an example of CNN being used for recognizing eveyday objects, humans and animals. Lately, CNN have been effective in several Natural Language Processing taks as well.

Fig 4.4: CNN recognition

CNN is an important tool for most machine learning practitioners today. However, understanding CNN and learning to use them for the first time can sometimes be an intimidating experience.

5. EXPERIMENTAL RESULTS

G. 5.1 SNAPSHOTS OF EXISTING SYSTEM

These Figure shows about the experimental results and the snapshots for the implementation of the existing work.

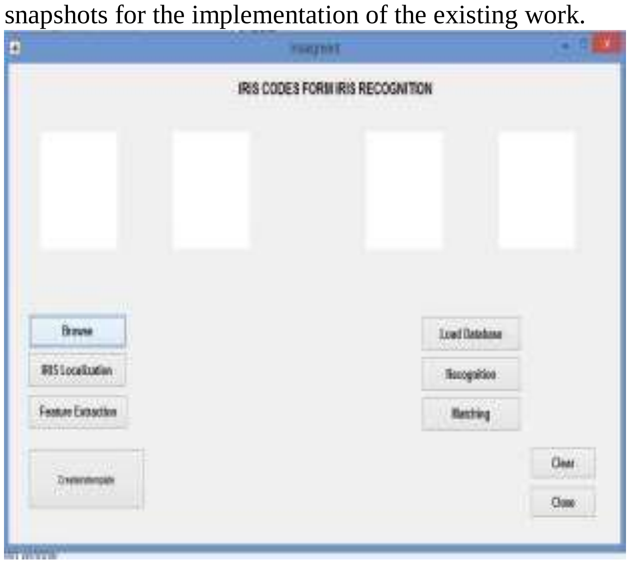


Fig 5.1: The GUI to get input

Fig 5.2: Loading real eye input

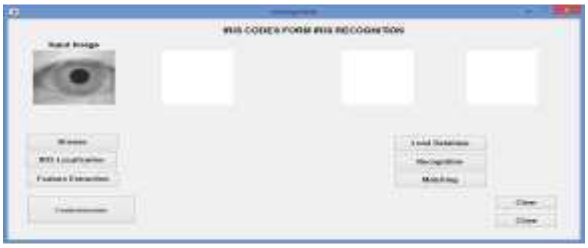


Fig 5.3: Loaded real iris input.

Fig 5.4 Localization of iris image.

Figure 5.5 shows the feature extraction of iris image.

Fig 5.5 Feature extraction of iris image.

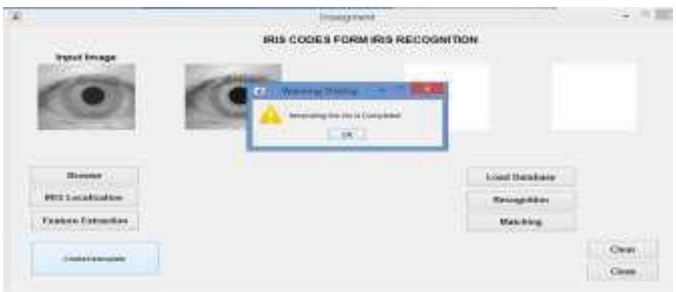


Fig 5.6 shows the localization of iris image

Fig 5.7 Loading of eye image into database.

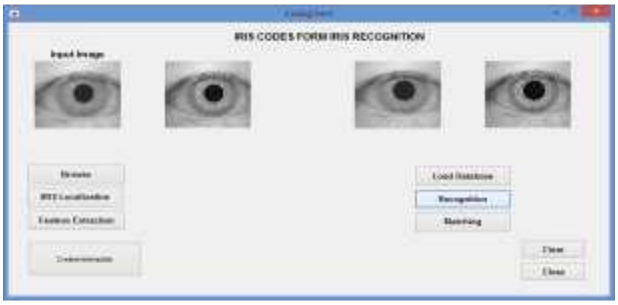


Fig 5.8 Recognition of iris image.

Fig 5.9: Displaying the result

Fig 5.10: Displaying output

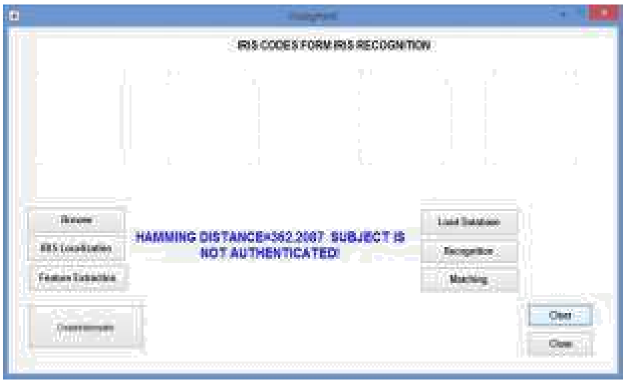


Fig 5.11: Clear the working environment.

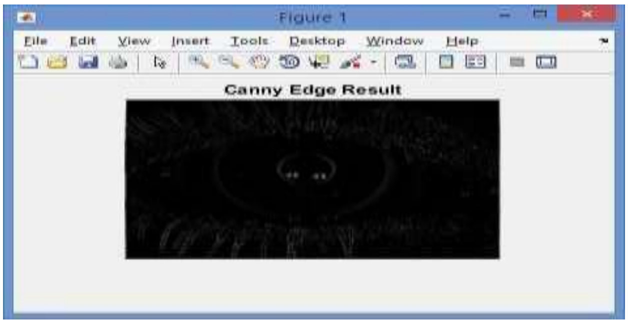


Fig 5.12 Edge detected eye image.

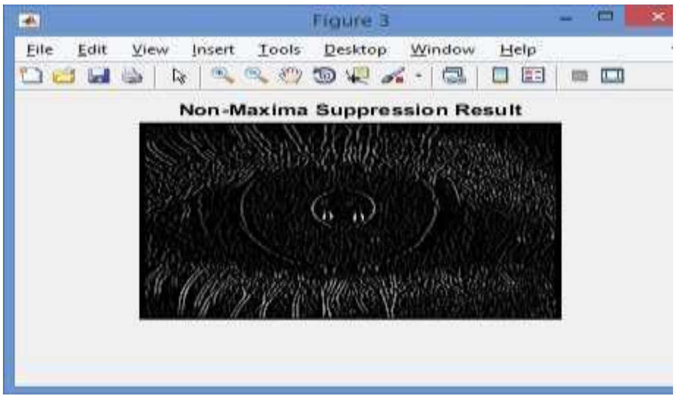


Fig 5.14 Non-Maxima detected eye image.

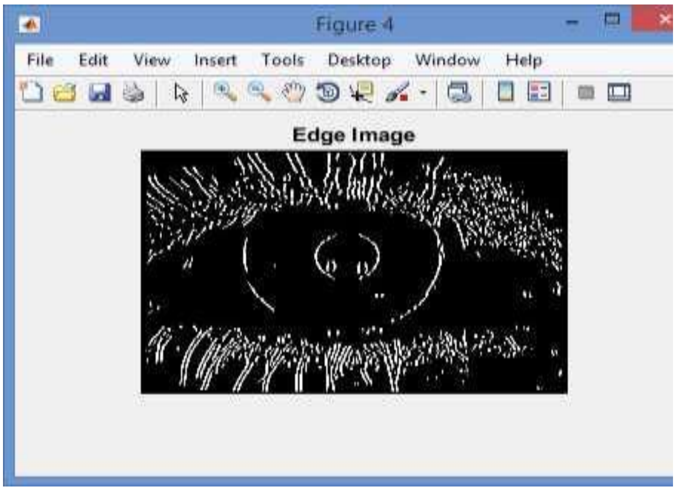


Fig 5.15 Edge detected eye image.

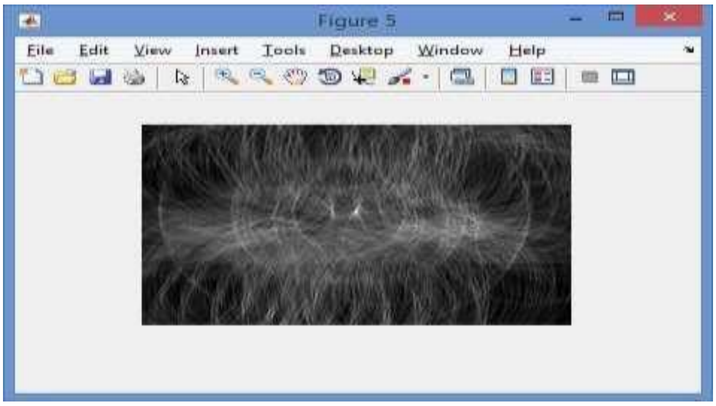


Fig 5.16 Hough circle detected eye image.

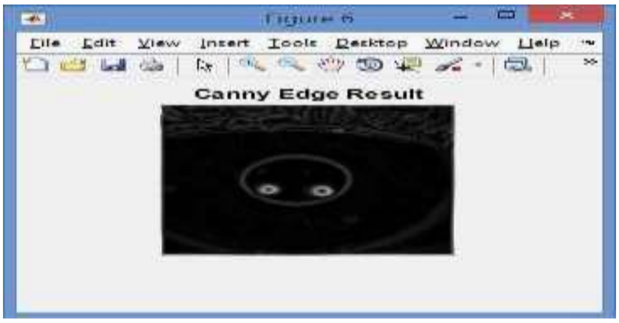


Fig 5.17 Canny Edge detected pupil image.

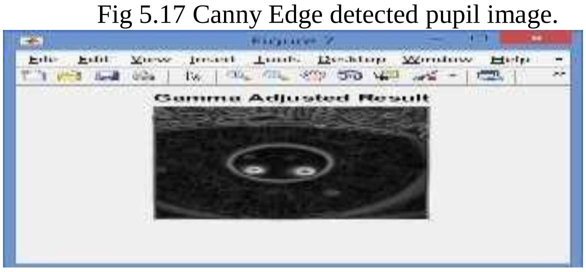


Fig 5.18 Gamma Edge detected pupil image.

Fig 5.19 Non-Maxima edge detected pupil image.

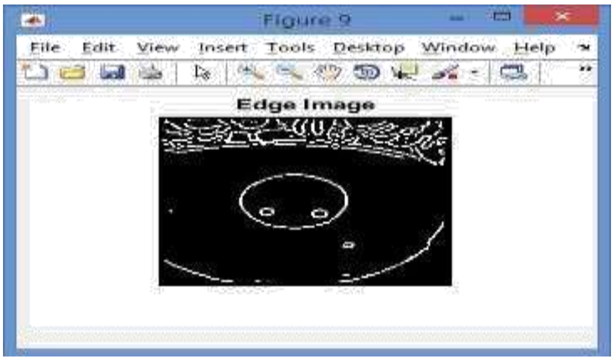


Fig 5.20 edge detected for pupil image.

Fig 5.21 Hough Circle edge detection for pupil image.

The training phase and testing methods of proposed system are shown in the figure 5.1. In the proposed system the training stage of all the biometrics are shown in the figure 5.22. All the datasets are trained by using the Neural Network Pattern Recognition tool (NPR) are shown in the figure 5.23. The experimental results and the snapshots for the implementation of the proposed work are in the figure 5.24 Loading real iris biometric as input and the image is extracted by using LTP algorithm and feature vector has been calculated are shown . Fusion process after the extraction of all the biometrics and the fused vector values are displayed. The final output of all the biometric input as real image by using convolution neural network. And the same time the final output of all the biometric input as fake image are shown in the figure 5.25.

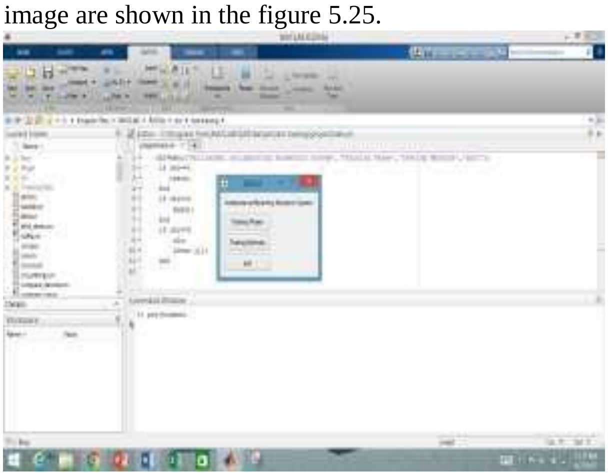


Fig 5.22 the GUI of proposed system

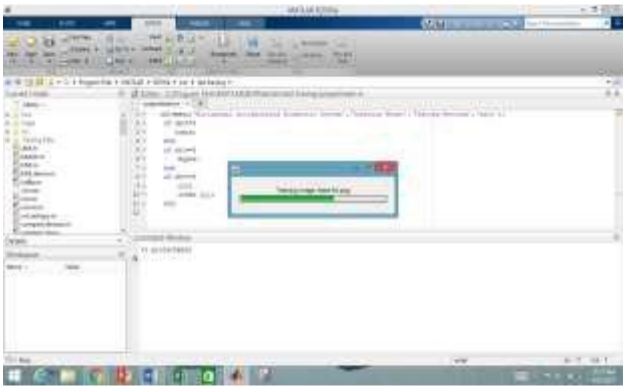


Fig 5.23 training stage of proposed system

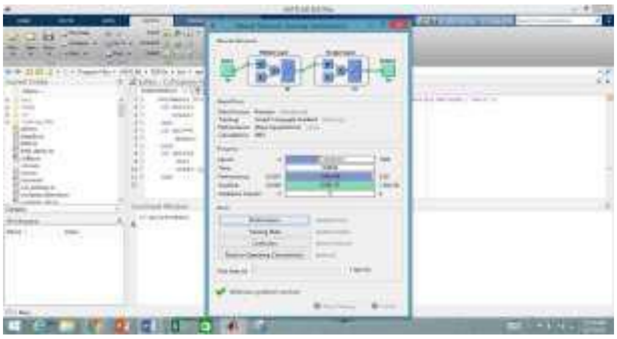


Fig 5.24 NPR training the database

Fig 5.25 Getting the LTP of an iris image

Fig 5.26 Getting the LTP of an iris image and CNN will be applied.

1) EVALUATION METRICS

False Acceptance Rate: It represents the percentage of fake images misclassified as real.

FAR = Misclassified Spoof Recordings / Total Spoof recordings.

False Rejection Rate: It represents the percentage of Real images misclassified as Fake.

FRR= Misclassified Live Recordings / Total Live recordings.

Half Total Error Rate: It denotes the average of FAR and FRR.

Half Total Error Rate= (FAR+FRR)/2

6. **CONCLUSION AND FUTURE ENHANCEMENTS**

Biometric system is used for authentication using biological and physiological traits. Iris Recognition system is an authentication mechanism that combines the various methodology. It is used to increase the accuracy of the iris detection system. Iris recognition has inherent weaknesses that can potentially compromise the security of a system. Spoofing attacks is one of them and enhanced iris recognition is more vulnerable to spoof attack than normal iris recognition system. Spoofing is giving fake input to the biometric sensor. Spoof detection is used to check whether the given input is real or fake. To overcome the disadvantages of the existing system, the iris recognition anti-spoofing biometric system is designed by combining iris biometrics. The local Ternary pattern texture feature is extracted from iris image. Convolution neural network is used for classification.

2) REFERENCES

[1] J. G. Daugman, "*High confidence visual recognition of persons by atest of statistical independence,* " IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15, no. 11, pp. 1148–1161, 1993.

[2] J. Daugman, "*New methods in iris recognition*, "IEEE Transactions on Systems, Man, and Cybernetics B, vol.37, no. 5, pp. 1167– 1175, 2007.

[3] J. Daugman, "*Statistical richness of visual phase information: updateon recognizing persons by iris patterns*," International Journal of
Computer Vision, vol. 45, no. 1, pp. 25–38, 2001.

[4] Diego Gragnaniello, Carlo Sanson, Luisa Verdolivaa, *"Iris liveness detection for mobile device based on local descriptors,"* PatternRecognition Letters, Vol. 57, pp.81–87, 2015.

[5] Oleg V. Komogortsev, Alexey Karpov and Corey D. Holland, "Attack of Mechanical Replicas: Liveness Detection with Eye Movements", *IEEE Transactions On Information Forensics And Security,* vol. 10,no. 4, April 2015.

[6] Mohit Kumar and N. B. Puhan, *"Iris Liveness Detection UsingTexture Segmentation,"* in Proc. Fifth National Conference onComputer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG), pp.1-4, 2015.

[7] Y. Hu, K. Sirlantzis, and G. Howells, *"Improving colour irissegmentation using a model selection technique,"* Pattern Recogn.Lett., vol. 57, pp. 24–32, 2015.

[8] Y. Chen, Y. Liu, X. Zhu, F. He, H. Wang, and N. Deng, *"Efficient irisrecognition based on optimal sub feature selection and weighted sub region fusion,"* Scientific World J., vol. 2014, pp. 1–19, 2014.

[9] Y. Alvarez-Betancourt and M. Garcia-Silvente, *"A key points-basedfeature extraction method for iris recognition under variable image quality conditions,"* Knowl -Based Syst. ,Elsevier Science PublishersB. V. Amsterdam ,vol. 92, pp. 169–182, 2016.

[10] T. Yang, J. Stahl, S. Schuckers, and F. Hua,*"Sub region mosaickingapplied to nonideal iris recognition,"* Int. Symp. ComputationalIntelligence in Biometrics and Identity Management, pp. 139–145, 2014.