IJSRTM
https://www.ijsrtm.com
Vol.5 Issue 2 Jun 2025: 21-25
Published online 11 June 2025
E-ISSN: 2583-7141

International Journal of Scientific Research in Technology & Management

Biometric Iris Recognition using Sobel Edge Detection for Secured Authentication

Nisha Vishwakarma
Dept. of Computer Science and Engineering
Lakshmi Narian College of Technology & Science
Bhopal, Madhya Pradesh, India
vishwakarmanisha140@gmail.com

Vinod Patel
Dept. of Computer Science and Engineering
Lakshmi Narian College of Technology & Science
Bhopal, Madhya Pradesh, India
vinod.gwl@gmail.com

***Abstract*— Recognition of iris is basically a technique used by taking out the mathematical forms biometrically over any video-based images either of the eyes that consists of complex pattern which are exclusive and static in nature. Iris is a favoured biometric feature equated to supplementary biometrics due to its specificity and constancy characteristics. The first developed systems are often relied on bad edge recognition methods and filters. Various Recognition methods like Canny Edge Detection, Huff Transform, Gabor Filters, Dagman's Operator Iris, are often utilized in the arena. There are some confines in the form of complex computational tactics, lack of precision for the images that contains complex noise, impediment due to lens, lashes of eyes and reflection observed in pre-work. The structure proposes a recognition of an iris or a validation system utilizing the method of Sobel Age Detection for the extraction of Iris feature. The tactic also evidences that the figurative depiction efficiently handles noise and declines, considering low resolutions, specular reflections and features that creates obstacle in the eye. The proposed system delivers improved safety results with the exact feature extraction here.**

Keywords*— *Iris, Sobel Edge Detection, Image Filtration, Noise Degradation, Feature Extraction.

I. INTRODUCTION

IRIS is a biometric feature among humans that uniquely identifies them. Iris formation began from 3 months of fetal life. But the unique pattern of IRIS started after one year from birth. The unique image of the IRIS has unique features that can be used for authentication systems. Iris recognition evolves multiple phases for extracting precise precision which includes Iris image acquisition where Iris image has been captured either through camera or scanner, next phase is preprocessing where image correction or enhancement has been done for better feature extraction, then image segmentation which includes normalization, pixel intensity value alteration and many more, after segmentation feature will be extracted and stored either in the form of texture or binary codes that later matches with the input image for authentication. Various algorithms have been developed for executing all these phases for acquiring better level of accuracy in the field of Iris based authentication system.

Fig. 1. Iris Feature

II. RELATED WORKS

A. Literature Survey

Fabián Rolando Jiménez López et al. developed a system for biometric iris recognition that proceeds with segmentation and normalization. Exploitation of these methods extracts the features of an eye. Here the algorithm for segmentation took place by Gabor filters and Hough

Transform which are traditional approaches, lacking somewhere toward better precision [1]. Arezou Banitalebi Dehkordi et al. proposed a method that uses multiple thresholds for identifying eyelids, eyelashes, pupil and light reflection. System uses Daugman algorithm for implementing Iris recognition which leads to distort sensitive feature that Iris contains [2]. P.Thirumuruga et al. proposed a biometric system that uses Canny Edge detection algorithm along with Hough transform. Hough transform is a feature extraction method which has been used in digital image processing. Moreover wavelet transform is used to extract the cognitive patterns from the iris of an eye [3]. Navjot Kaur et al. represent a survey report on existing methods and their algorithms that have been used for iris based authentication system. Canny edge detection is generally used to find the edges of an iris and Hough transform is used to create the boundary of an iris [4]. Amena Khatun et al. proposed a biometric attendance system using iris recognition for identifying students. Implementation took place by capturing iris images using webcam and processed through MATLAB to extract their feature and later compare with the existing images stored in the database [5]. Mateusz Trokielewicz et al. proposed a technique through which a database for iris images can be configured that has been captured from smart phone cameras. The result has been obtained from the experiment took place using existing iris recognition methods which are : IriCore, VeriEye, OSIRIS and MIRLIN [6]. Sarika B Solanke et al. proposed a review over various techniques for Iris identification. There are lots of techniques have been developed for segmentation and feature extraction such as Cascade Classifiers, match score fusion methods and many more. This paper also represent the flaws over the existing systems [7]. Jagadeesh N. et al. proposed an algorithm for Iris image preprocessing. System uses Canny Edge Detection for feature extraction and Gaussian Filter for image enhancement or feature correction and match has been drafted with the existing data in UPOL database. Canny edge detection is poor method for recognizing complete edge of sensitive data because of broken edges [8].

III. Problem Identification

As per the survey takes place on various researches made in the field of Iris Recognition system, there are different available methods implemented by the researchers with certain modification to create an authentic recognition of iris. Most of the techniques employed basic algorithms available for the operations needs to take place for the recognition of Iris. Typical operations performed to recognize an iris are segmentation, normalization, feature extraction and matching. Canny Edge detection, Hough Transform, Gabor Filter, Daugman's operator are some frequently used technique in the systems which have been proposed. There are few limitations as complex computational approach, lack of accuracy for complex noisy image, obstructions due to lens, eye lashes and reflection examined in the prior work done. So, a system is required which can efficiently recognize the Iris with zero false rates and secure the crucial applications. Base paper developed a system which is relied on Canny Edge Detection and Gaussian Filter for the process of recognition. Though the method which has been proposed in the paper utilized the predefined algorithm which limits the practical implementation of system as slight illumination can affect the accuracy of iris scanner and appearance of iris occluded by eyelashes may block the precise extraction. Since, the implementation of Canny Edge Detection is not suitable for sensitive pattern extraction that Iris belongs.

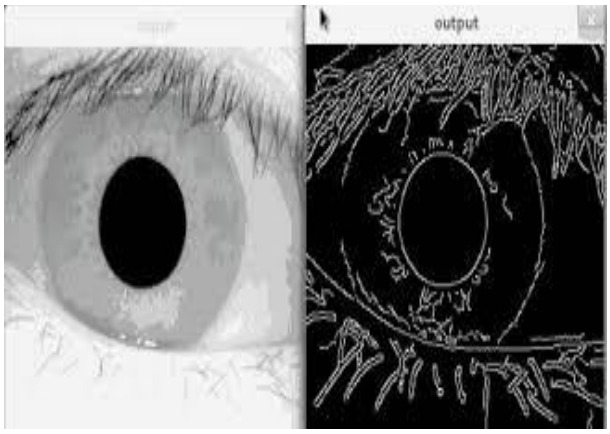

Fig. 2. Canny Edge Detection [3]

In figure 2, shows the edges of Iris image that possesses broken lines and less feature density.

IV. Proposed Work & Implementation

The proposed system is able to overcome all the flaws found in previously proposed systems. Here the system is liable to attain higher precision rate in the form of false rejection. If a true Iris get rejected for a while then no harm over authentication system but if a single false acceptance occurred then whole system will get failed in aspect of security. System uses Sobel edge detection instead of Canny edge detection that resulting better feature extraction. Sobel is a method of advanced edge detection in the field of digital image processing. User is required to process the image for feature extraction and template creation, once the template has been created, it will be stored in the database for future matching.

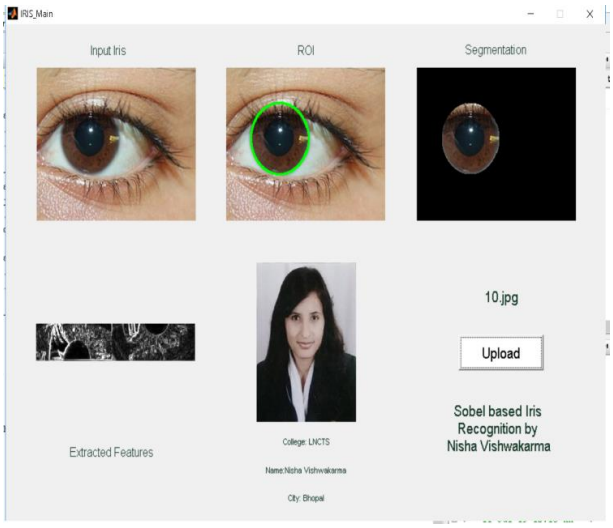

Fig. 3. Successful Authentication

If a user input an Iris image that belongs to the database, it will started capturing ROI (region of interest) and proceed for feature extraction and once the feature has been extracted it will started matching key features and if key feature is greater than the threshold value, threshold value is a value where the condition has been applied for decision

making, if it satisfies the threshold then user will be authenticated and details will become appeared accordingly. But if computed key feature is less than the threshold value then user will get denied. As per the scientific law if 20% key points get matched then it belongs to that person. So that is why the threshold value is set to 20% of key features or points found. System is capable to return true positive results with minimal false or fake results. System has been tested with many enrollments and system observed as effective biometric authentication system.

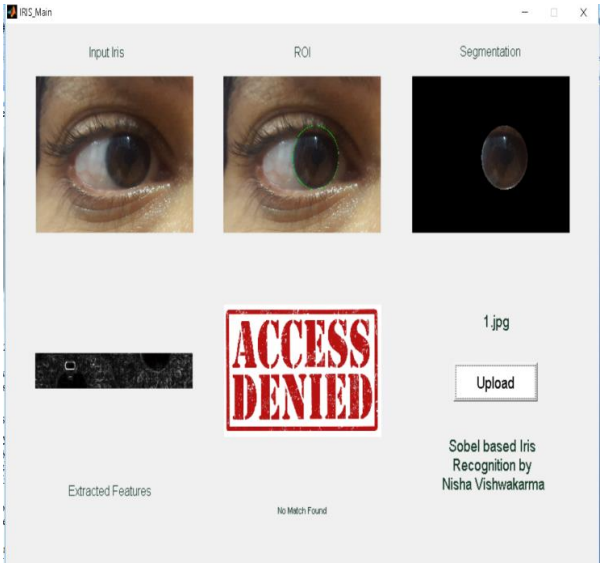

Fig. 4. Authentication Denied for Unauthorized Holder

In the training phase it is required to create feature templates of Irs images as per the authentication being tested. First of all an iris image has been acquired to obtain the edge detection by applying sobel edge detection tool. Once the edges have been extracted the feature has been declared in the form of texture, these textures later stored as template for future matching. The extraction process is similar to the training process except template matching. Once the feature has been extracted, it compared with the template that stored previously. If it is greater than the threshold data points then it will fetch the user details else it will deny the user. The Sobel operator, occasionally named as the Sobel-Feldman operator or Sobel Filter, is employed in processing of image and computer vision, particularly within the Edge Detection Algorithm where it develops prominence on the edges. The discussed technique is termed after Irwin Sobel and Gary Feldman who are co-workers of the Stanford Artificial Intelligence Laboratory (SAIL). Proposed system is able to provide better level of feature extraction and matching for secured IRIS based authentication system. IRIS is a biometric feature among human that uniquely identifies them. Iris formation started from the 3rd month of an embryonic life. But the formation of unique patterns of IRIS started after a year of life. The digital image of IRIS contains unique features that can be used for authentication system. Iris recognition technique evolves various stages to get it precisely detected, which includes image acquisition in which wavelength of light, light reflected from the base of iris and some other factors are considered. Preprocessing is the next stage of recognition in which boundaries and other parts of an eye are taken into account with enhanced image quality. Image segmentation which includes the analysis of background texture, image normalization is used to change the intensity value of pixels obtained from an image. Feature extraction is considered as a crucial stage of recognition, as it extracts the vectors of those areas of an image which is taken under consideration.

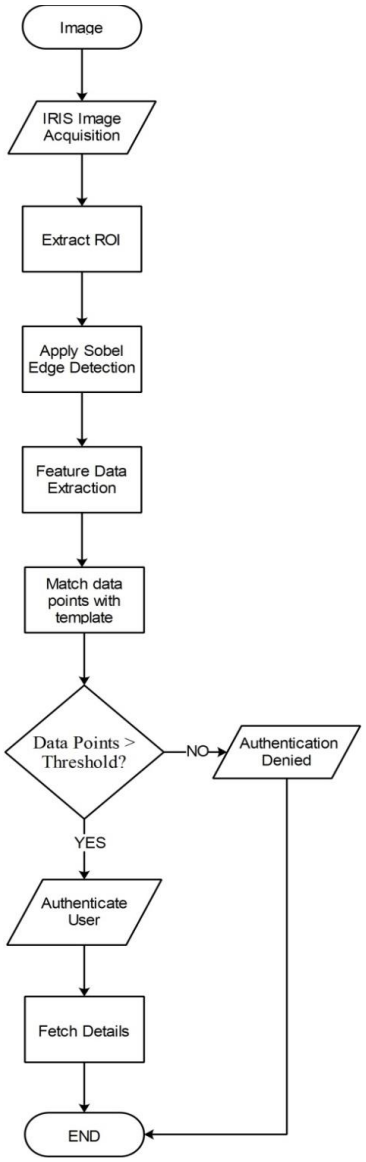

Fig. 5. Flow Chart for Feature Extraction and Matching

Final stage is matching where the acquired data in terms of coding from previous stage is compared with the existing information stored in the database to accomplish the recognition process. Various algorithms have been developed to execute those operations of localization, preprocessing, normalization, feature extraction and matching.

A. GMS (Gradient Magnitude Sobel) Algorithm:

Require: A as input image, M_x as horizontal gradient function, M_y as vertical gradient function, S_1 as gradient of horizontal edges, S_2 as gradient of vertical edges, mag as

magnitude, sqrt as square root, T as threshold, K_n as extracted key points.

Step 1: Input Iris image A as two dimensional image array
Step 2: Extract ROI
Step 3: Apply Sobel Function
function sobel(A)
M_x=[-1 0 1; -2 0 2; -1 0 1]
M_y=[-1 -2 -1; 0 0 0; 1 2 1]
rows = size(A,1)
columns = size(A,2)
mag=zeros(A)
for i=1:rows-2
for j=1:columns-2
S_1=sum(sum(M_x.*A(i:i+2,j:j+2)))
S_2=sum(sum(M_y.*A(i:i+2,j:j+2)))
mag(i+1,j+1)=sqrt(S1.^2+S2.^2)
end for
end for
end function
Step 4: Threshold (T)= 20 %
output_image = mag;
Count Key Points K_n from mag
Step 5: If (K_n > T) **then**
Authenticate Iris;
else
Deny Authentication;
end else
end if
Step 6: End

In the algorithm, first of all an IRIS image has been acquired, then system requires to extract region of interest i.e. ROI and mask the rest background. Then apply sobel function for edge detection to extract the key points. Once the key points have been extracted, it will compare with the template as per threshold validates and result accordingly.

V. Result Analysis

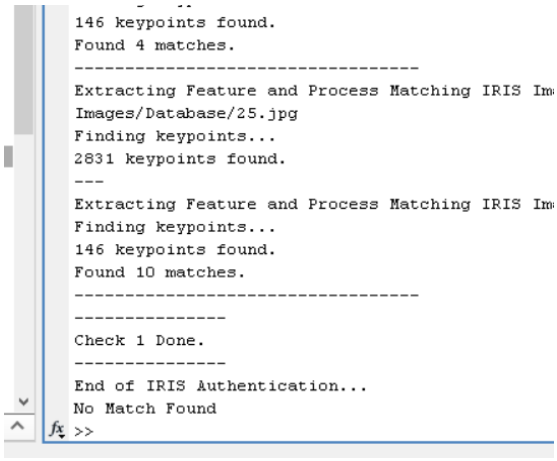

Fig. 6. Result Simulation for Key Feature Extraction & Matching

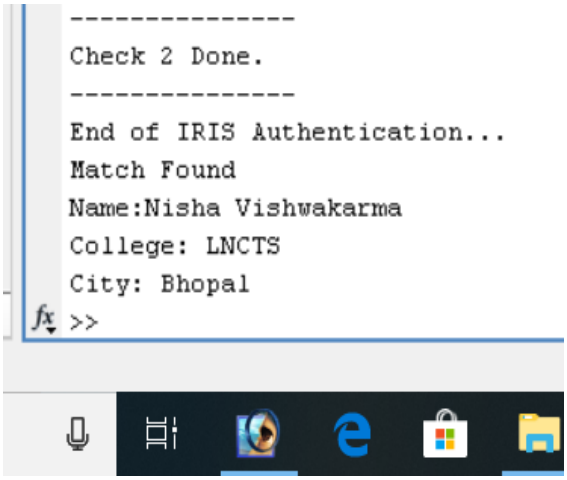

Fig. 7. Result Simulation for Authentic User Data Extraction

True Positive (TP) = 29

True Negative (TN) = 1

False Positive (FP) = 0

False Negative (FN)= 30

$$Accuracy = \frac{\text{Total testing class} - (TN + FP)}{\text{Total testing class}} * 100\%$$

$$Accuracy = 96.66\%$$

$$\text{Pr}ecision = \frac{TP}{TP + FP} * 100\%$$

$$\text{Pr}ecision = 100\%$$

$$Overall\_Accuracy = \frac{\text{Accuracy} + \text{Precision}}{2}\%$$

$$Overall\_Accuracy = 98.33\%$$

As per the feature matching only those users authenticated that satisfy the threshold value, otherwise illegitimate user will get denied every time. Fig 6 and Fig 7 show the result simulation of iris based user authentication system. Table no. I shows the key terminologies or parameters that have been used to compute the result. Here the total no. of authentic iris holder is 30 and unauthentic iris holder is also 30. The result has been computer on the basis of these key holders.

TABLE I. Result Analysis

Key Terms	Recorded
Total No. of Authentic Iris Holder	30
Total No. of Unauthentic Iris Holder	30
Total No. of Authentic User Succeeded	29
Total No. of Authentic User Denied	1
Total No. of Unauthentic User Succeeded	0
Total No. of Unauthentic User Denied	30
FRR	100 %
TRR	96.66 %
Precision	1
Recall	0.50
Overall Accuracy	98.34

Table no. II shows the result comparison where accuracy and error rate have been computed on the basis of various testing classes. The proposed system pertains bit higher accuracy as compare to the previous one. Hence the system has no false acceptance rate which shows the higher feasibility in comparison with the previously proposed systems.

TABLE II. RESULT ANALYSIS

Key Terms	Amena [5]	Proposed
Total Testing Class	-	60
Error Rate	17.8 %	1.66 %
Accuracy	82.2 %	98.34 %

VI. CONCLUSION & FUTURE SCOPE

Thus the system which has been proposed is bit capable to reject false users or pertains high false rejection rate. System uses sobel edge detection that extract features with high magnitude that possesses better precision rate. System acquired 98.34 % of accuracy which is enough higher than the previously proposed system. System does not distort the feasibility of Iris by applying various image enhancement filters. Iris can be used in future for multi-level authentication system where no illegitimate user can get access in anyhow.

REFERENCES

[1] F. R. J. López, C. E. P. Beainy and O. E. U. Mendez, "Biometric iris recognition using Hough Transform," *Symposium of Signals, Images and Artificial Vision - 2013: STSIVA - 2013*, Bogota, 2013, pp. 1-6.

[2] A. B. Dehkordi and S. A. R. Abu-Bakar, "Noise reduction in iris recognition using multiple thresholding," *2013 IEEE International Conference on Signal and Image Processing Applications*, Melaka, 2013, pp. 140-144.

[3] P.Thirumurugan et al., "Iris Recognition using Wavelet Transformation Techniques", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.1, January- 2014.

[4] N. Kaur and M. Juneja, "A review on Iris Recognition," *2014 Recent Advances in Engineering and Computational Sciences (RAECS)*, Chandigarh, 2014, pp. 1-5.

[5] A. Khatun, A. K. M. F. Haque, S. Ahmed and M. M. Rahman, "Design and implementation of iris recognition based attendance management system," *2015 International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*, Dhaka, 2015, pp. 1-6.

[6] M. Trokielewicz, "Iris recognition with a database of iris images obtained in visible light using smartphone camera," *2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*, Sendai, 2016, pp. 1-6.

[7] S. B. Solanke and R. R. Deshmukh, "“Biometrics — Iris recognition system” A study of promising approaches for secured authentication," *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2016, pp. 811-814.

[8] N. Jagadeesh and C. M. Patil, "Iris recognition system development using MATLAB," *2017 International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, 2017, pp. 348-353.

[9] Tedmontgomery, "The Iris" 2019.[Online]. Available: http://tedmontgomery.com/the_eye/iris.html, [Accessed: 11 July 2019].

[10] GitHub. "C Based Human Eye IRIS Segmentation Algorithm based on Daugman's Itegro-Differential Operator" 3 Oct 2016.[Online]. Available: https://github.com/ghazi94/IRIS-Segmentation, [Accessed: 11 July 2019].

[11] Raghavender Reddy Jillela, Arun Ross, Segmenting iris images in the visible spectrum with applications in mobile biometrics, Pattern Recognition Letters, Volume 57, 2015, Pages 4-16, ISSN 0167-8655.

[12] Mattoo, Iqra & Agarwal, Parul. (2017). Iris Biometric Modality: A Review. Oriental journal of computer science and technology. 10. 502-506.

[13] Harb, "Iris Scanning" 21 March 2015.[Online]. Available: https://habr.com/en/post/377665/, [Accessed: 11 July 2019].