iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.49911

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

IRIS-Based Human Identity Recognition with Deep Learning Methods

Dr. Anithakarthi[1], Dharani M[2], Bindu Sri P[3], Monika V[4], Sailaja M[5]
[1]*Professor,* [2, 3, 4, 5]*Student, Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Chennai, Tamil Nadu, India*

Abstract: ***One of the most important computer system modules is the one in charge of user security. It has been demonstrated that simple logins and passwords cannot provide high efficiency and are simple for hackers to crack. The popular substitute is identity identification using bio-metrics. Iris as a biometric characteristic has attracted increased attention in recent years. It was brought on by the high efficiency and precision this quantifiable aspect ensured. Throughout the literature, the effects of this curiosity can be seen. Several authors have put forth a variety of various approaches. This paper describe methods for an iris-based algorithm for recognizing human identity. Artificial neural networks (ANN) and a CNN-based transfer learning model (Mobile-net) were employed in the classification process. Once the output has been categorized, the iris component is segmented using a process called segmentation. Tests that have been run have demonstrated that the suggested procedure can produce results that are adequate.***

Keywords: Iris-based human identity recognition, CNN, Transfer learning, Image segmentation, artificial neural networks

I. INTRODUCTION

The solution for security problems is really easy. The popular response is bio-metrics. The science uses quantitative characteristics to identify (or verify) humans (e.g., fingerprint, iris, retina, keystroke dynamics). These characteristics can be categorized into three primary categories: physiological (related to our bodies and appropriate measurements), behavioral (these are the attributes we can learn, like a signature), or hybrid, which includes both physiological and behavioral characteristics (e.g., voice). We can infer that each user of a computer system (with a biometric security system) won't supply any more passwords because he will serve as a real password thanks to his measurable characteristics.

An important characteristic that can provide high accuracy, efficiency, and identification rate is iris, according to a variety of experiments and study. More than 250 different elements make up this feature. Each one is employed to define human identity (in the form of feature vector). In the literature, it has also been demonstrated that these feature vectors are entirely distinct for a single person's left and right eyes, and that this is also true in the case of twins. They each have distinctive irises (feature vectors are completely different).

The fact that iris is very difficult to fake is the most significant. Only a few study publications in the literature provide sufficient proof that such spoofing procedures were successfully completed.

II. PROBLEM STATEMENT

Preventing spoofing is another factor that must be taken into account when designing iris-based security solutions. Positive recognition based on printed images rather than actual samples is the most commonly seen susceptibility in bio-metrics systems. In particular, it is linked to iris-based systems. This issue was extensively discussed. So we need to demonstrate how the use of contact lenses, print attack pictures of a live iris, and the combination of both can significantly affect the system's ability to identify false positives. With the IIIT-WVU iris data set, all trials were completed. The authors also offered a fresh method for stopping such assaults using a deep convolution neural network.

III. LITERATURE SURVEY

1) The paper revisits *"iris recognition with spoofing attacks"* and analyzes their effect on the recognition performance by Gupta P, Behera S, and Vatsa M, Singh R.Specifically, spoofing attack with contact lens variations is used as the spoofing mechanism.It has been found that contact lenses and print attacks, used separately or together, can drastically alter intra- and inter-personal distributions, increasing the likelihood that iris recognition systems would be tricked.

©IJRASET: All Rights are Reserved

2) *"A fast iris recognition system through optimum feature extraction"* by Rana HK, Azam MS, Akhtar MR, Qunin JMW, and Moni MA. This paper suggests a method for using Principal Component Analysis (PCA) based on Discrete Wavelet Transformation (DWT) to extract the best features of an iris and shorten the processing time required for classifying iris templates. Reducing the resolution of the iris template is the purpose of employing DWT in conjunction with PCA.
3) *"Presentation attack detection for iris recognition using deep learning"* by Arora S, Bhatia MPS: Studies done on the IIIT-WVU iris dataset reveal that contact lenses, print attack photos of live iris images, and a combination of both can be quite effective at fooling iris recognition systems. In contrast to current state-of-the-art methodologies, the article uses deep convolution neural networks to detect such spoofing tactics with better results.
4) By M. Jenadeleh, M. Pedersen, & D. Saupe, The paper says about *"Blind Quality Evaluation of Iris Pictures Taken in Visible Light for Biometric Recognition"*. Statistical aspects of the sign-magnitude transform are used to determine the iris picture quality.
5) *"Security evaluation of negative iris recognition"*. IEICE Trans Inf Syst by Ouda O, Chaoui S, Tsumura N .The negative iris recognition scheme that has recently been proposed to secure iris-codes utilizing the concept of negative database.

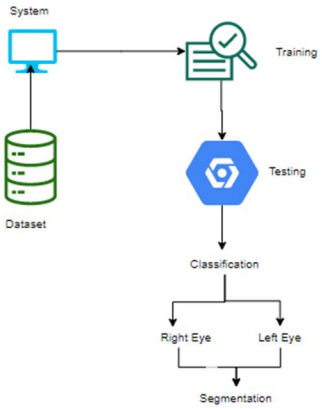
IV. PROPOSED APPROACH

In purposed method we are performing the classification of either the Iris-based Human Identity Recognition identification using Convolution Neural Network (CNN) based transfer learning (Mobile Net) of deep learning method. As image analysis-based approaches for Iris-based human identity recognition. Hence, proper classification is important for the proper nutrition that which will be possible by using our proposed method.utilizing the CNN algorithm to classify the images.The segmentation of the iris portion occurs following categorization.

A. Advantages of Proposed System:

1) Accurate up to 99.7%.
2) Less complexity.
3) Nearly 40 samples are taken.
4) Twice the performance rate of existing system.

V. SYSTEM ARCHITECTURE



VII. MODULE DESCRIPTION

A. System

1) *Create Dataset:* The dataset containing images of the left and right eyes images are considered that which are to be classified is split into training and testing dataset with the test size of 30-20%.
2) *Pre-processing:* The photos are resized and reshaped into the proper format so that our model may be trained.
3) *Training:*
4) The CNN technique is utilized to train our model using the pre- processed training dataset.

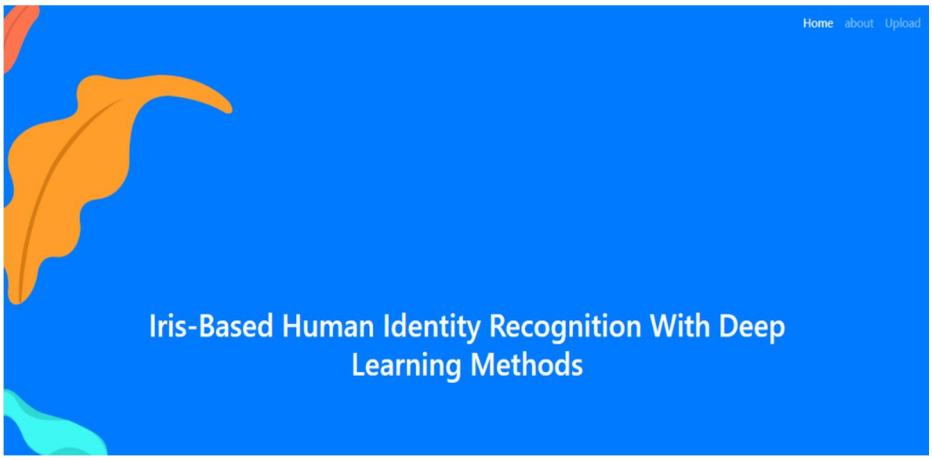
5) *Classification:* The results of our model is display of classified images either it is left or right eye.
6) *Segmentation:* Segmenting the iris begins after classification..

B. User

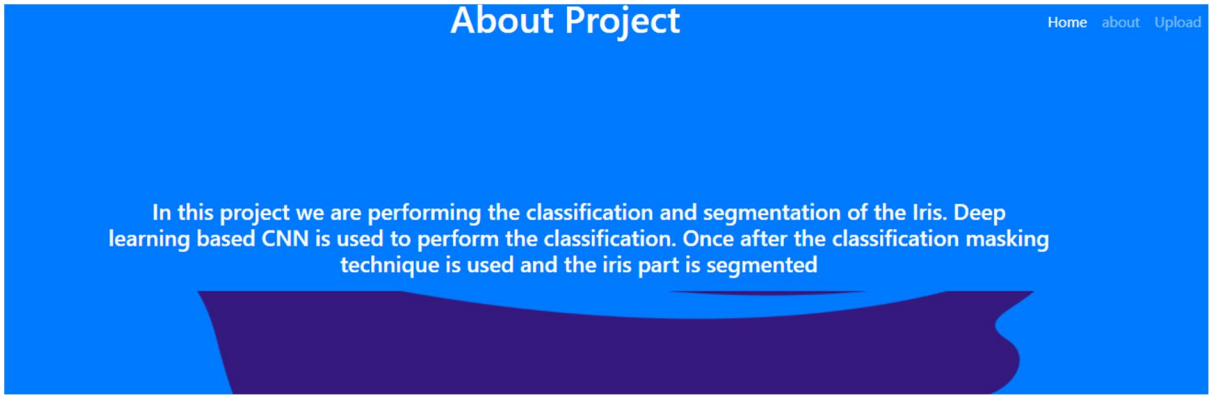
1) *View Training Accuracy:* The trained algorithm's accuracy can be verified by the user.
2) *Upload Image:* A user must upload a classification-required image.
3) *View Results:* The user can view the segmented and classified image results.

VIII. RESULT ANALYSIS

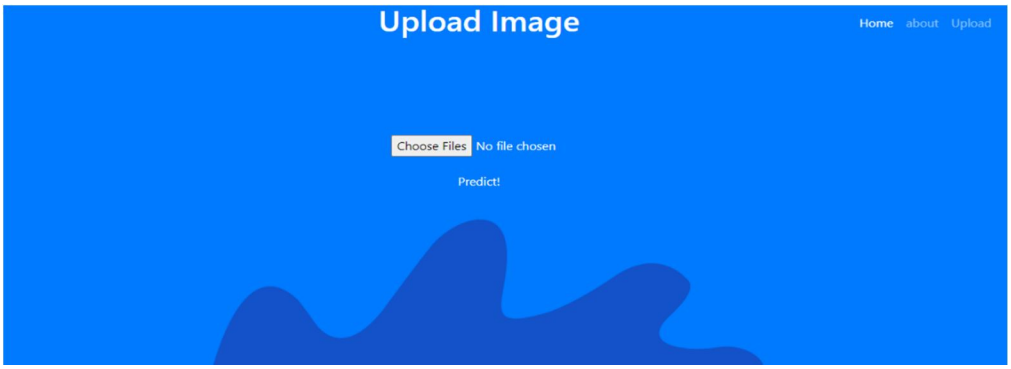
1) *Home*: In our project, we are classifying the eyes and making the segmentation of the iris.



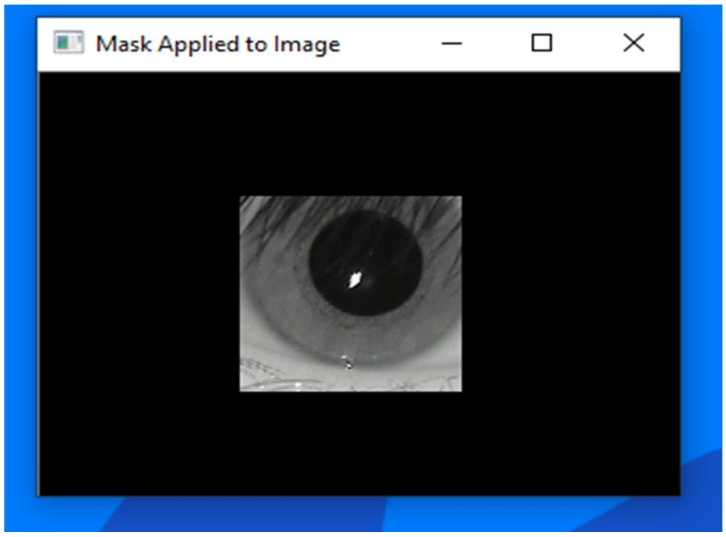
2) *About Project:* The user will learn briefly about the project here.



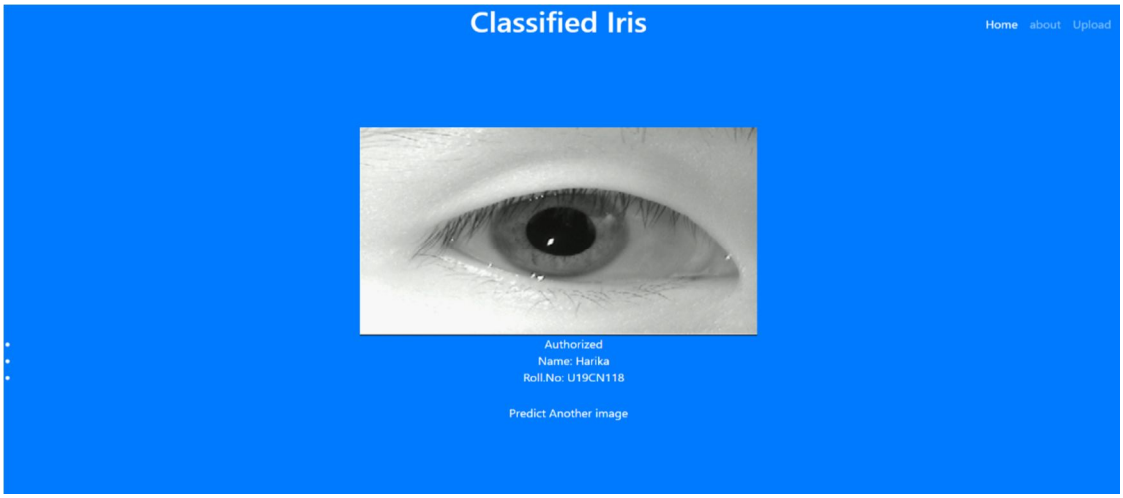
3) *Upload The Image:* the images can be uploaded those which are to be classified.



4) *Classified output:* The classified output.



5) *Segmented Output:* Iris segmented from the classified output.



IX. CONCLUSION

In this project we have successfully classified the left or right eye image using the deep learning. Here, we have considered the dataset of eye classes and trained using CNN. After the training user can test by uploading the image and can check for the classified results. Once after the classification the iris part of the classified output is segmented.

REFERENCES

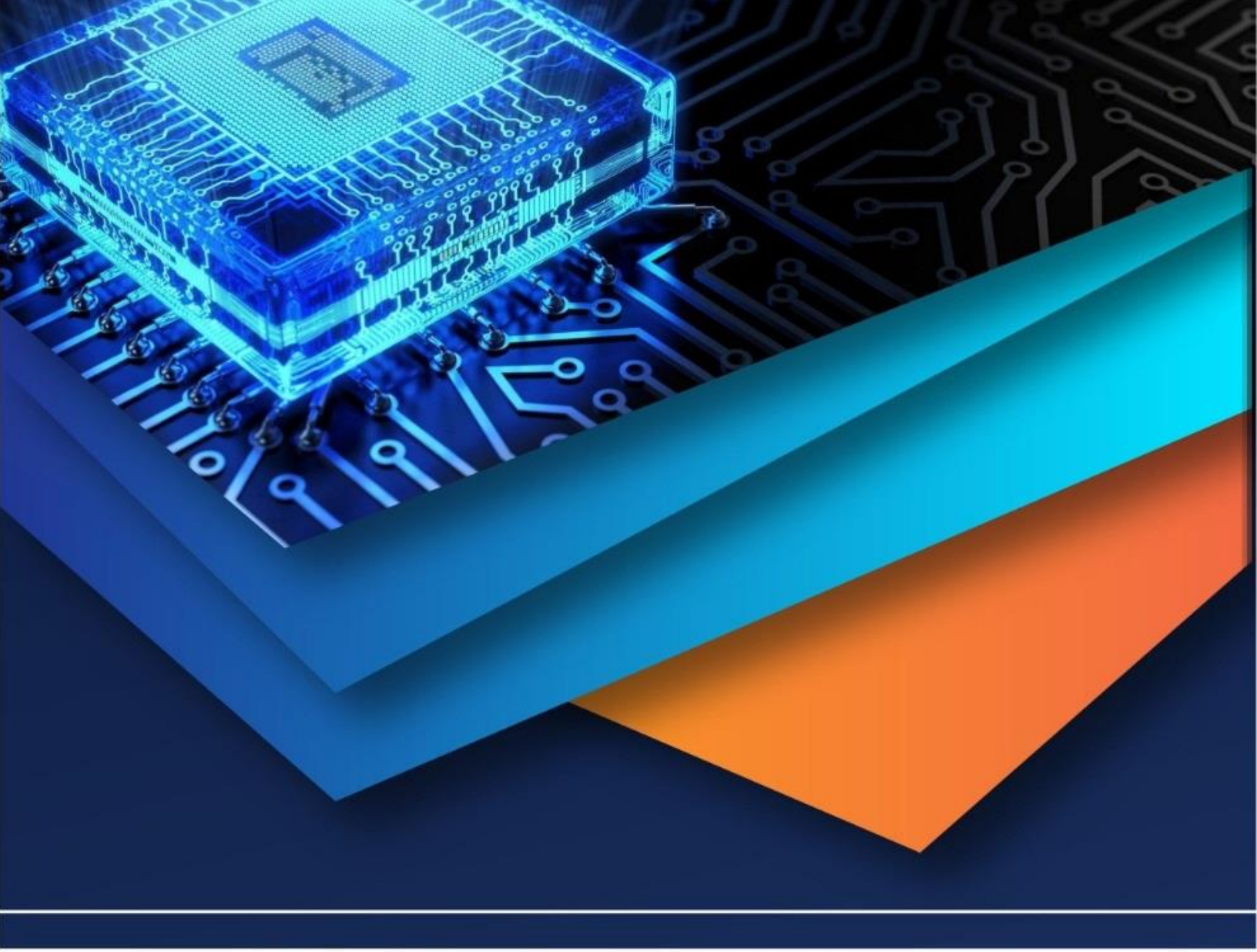
[1] Prashanth CR, Shashikumar DR, Raja KB, Venugopal KR, Patnaik LM (2009) *"High security human recognition system using iris images"*. Int J Recent Trends Eng 1(1):647–652

[2] Miyazawa K, Ito K, Aoki T, Kobayashi K, Nakajima H (2006) *"A phase-based iris recognition algorithm"*. In: Zhang D, Jain A (eds) Proceedings of advances in biometrics, international conference, ICB 2006, Hong Kong, China, January 5–7, 2006, Springer lecture notes in computer science, vol 3832, pp 356–365

[3] Mohammed NF, Ali SA, Jawad MJ (2020) *"Iris recognition system based on lifting wavelet"*. In: Mallick P, Balas V, Bhoi A, Chae GS (eds) Cognitive informatics and soft computing. Springer advances in intelligent systems and computing, vol 1040, pp. 245–254. Springer, Berlin

[4] Trokielewicz M, Czajka A, Maciejewicz P (2020) *"Post-mortem iris recognition with deep-learning-based image segmentation"*. Image Vision Compu 94:103866. https://doi.org/10.1016/j.imavis.2019.103866

[5] Jalilian E, Uhl A, Kwitt R (2017)" *Domain adaptation for CNN based iris segmentation"*. In: IEEE proceedings of 2017 IEEE international conference of the biometrics special interest group (BIOSIG), Darmstadt, Germany, September 20–22, 2017. https://doi.org/10.23919/BIOSIG.2017.8053502



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)