International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Iris Based Human Identity Recognition with Deep Learning Methods

[1]T. Manjula, [2]J. Vasantha,[3]S. Yuva Tejeswari [4]R. Someswari, [5]Dr. Y. Subba Reddy
[1,2,3,4]UG Students, Department of Computer Science and Engineering, Sai Rajeswari Institute of Technology, Proddatur, Andhra Pradesh-516360
[5]Professor, Department of Computer Science and Engineering, Sai Rajeswari Institute of Technology, Proddatur, Andhra Pradesh-516360
Email: manjulathalari3014@gmail.com, vasanthajinka42@gmail.com, tejeswaripandu@gmail.com, revuru3@gmail.com, y.subbareddy@gmail.com

Abstract:
One of the most important modules of computer systems is the one that is responsible for user safety. It was proven that simple passwords and logins cannot guarantee high efficiency and are easy to obtain by hackers. The well-known alternative is identity recognition based on biometrics. In recent years, more interest was observed in iris as a biometrics trait. It was caused due to high efficiency and accuracy guaranteed by this measurable feature. The consequences of such interest are observable in the literature. There are multiple, diversified approaches proposed by different authors. In this work, we present our own approach to iris-based human identity recognition algorithm. For classification, the algorithm was used CNN (Convolutional neural network) based transfer learning model (Mobile Net) and artificial neural networks.Once after the classification, the segmentation is performed on the classified output and iris part is segmented. Performed tests have shown that satisfactory results can be obtained with the proposed method.

Keywords ---Iris based human identity recognition, CNN

1.Introduction
Biometrics presents a straightforward solution to authentication challenges by relying on measurable human traits like fingerprints, iris scans, or even unique behavioral patterns such as keystroke dynamics. These characteristics fall into three main categories: physiological (related to the body), behavioral (learned traits like signatures), and hybrid (traits combining both physiological and behavioral aspects, such as voice recognition). Employing biometric security means users won't need additional passwords since their unique traits serve as their authentic identifiers. This approach enhances security by leveraging traits that are difficult to replicate, providing a robust authentication method. However, it's crucial to address potential concerns such as privacy issues and the risk of spoofing to ensure the effectiveness and integrity of biometric systems.
Diversified experiments and research are showing that one of the most important traits that can guarantee high accuracy, efficiency and recognition rate is iris. This feature consists of more than 250 unique elements. Each of them is used to describe human identity (in the form of feature vector). In the literature, it was also proven that such feature vectors are completely different for both eyes of one person (left and right), and moreover it is true, even in the case of twins. Each of them has different irises (feature vectors are completely different). The most important is that iris is really hard to spoof. In the literature, we can find only a couple of research papers that provide some vital evidence that such spoofing procedure was finished with the success.

BACKGROUND AND RELATED WORKS
Numerous studies have been conducted on this subject: In this work, [1] a discrete wavelet transformation-based approach for merging principal component analysis (PCA) (DWT) is provided. DWT is used in front of PCA to reduce the iris template's resolution. This study proposes [2] IrisParseNet, an iris segmentation technique based on deep learning that is incredibly effective. It differs from a few previous CNN-based iris segmentation methods, we only cared to follow a

general semantic segmentation framework in order to predict iris masks with accuracy. As per the revolutionary research of John Daugman [3], this study does not include Gabor wavelets and other filter banks that are commonly utilized in iris identification systems. Rather, they employed machine learning methods that classify biometric templates as numerical characteristics. [4] This research uses three state-of-the-art pretrained models for iris detection: VGG16, InceptionV3, and ResNet50. It also uses a deep learning approach based on the capsule network architecture. The contents of the other paper are [5] In this investigation, connected generative adversarial networks (cpGAN) and conditional generative adversarial networks (cGAN) were used.

[1] Gupta P, Behera S, and Vatsa M, Singh R:

This paper revisits iris recognition with spoofing attacks and analyzes their effect on the recognition performance. Specifically, print attack with contact lens variations is used as the spoofing mechanism. It is observed that print attack and contact lens, individually and in conjunction, can significantly change the inter-personal and intra-personal distributions and thereby increase the possibility to deceive the iris recognition systems.

[2] Rana HK, Azam MS, Akhtar MR, Qunin JMW, Moni MA:

In this study, a technique is proposed for incorporating Principal Component Analysis (PCA) based on Discrete Wavelet Transformation (DWT) for the extraction of the optimum features of an iris and reducing the runtime needed for iris templates classification. The idea of using DWT behind PCA is to reduce the resolution of the iris template.

[3] Arora S, Bhatia MPS:

Experiments conducted on the IIIT-WVU (Indian Institute of Information Technology-West Verginia University) iris dataset show that print attack images of live iris images, use of contact lenses and conjunction of both can play a significant role in deceiving the iris recognition systems. The paper makes use of deep Convolutional Neural Networks to detect such spoofing techniques with superior results as compared to the existing state-of-theart techniques.

[4] Aravind Krishnaswamy Rangarajan, Raja Purushothaman*, Anirudh Ramesh:

In this cognitive radio spectrum sensing, the speed of operation of the network is one of the important factors for efficient data handling and transmission process. Cyclostationary feature detection is one of the efficient methods for Cognitive Radio spectrum sensing applications. The speed and power of the cyclostationary feature detection-based spectrum sensing architecture in cognitive radio networks can be improved by implementing advanced multiplication techniques like Vedic multipliers for test statistic computing modules deployed in the architecture

SYSTEM ANALYSIS & FEASIBILITY STUDY

1. Existing System

In the earlier works, machine learning was essential. Then, machine learning models were used to finish much of the work. However, a few deep learning algorithms are currently in high demand because of their accuracy. The models that highlight the deep learning methods that are now in use are GANs, ResNet51, IrisParseNet, VGG16, and InceptionV3.

Consequences

- Limited feature compatibility
- Reduced complexity
- Poor performance

2.Proposed System

We are approaching our job with a deep learning mindset. We execute image classification and iris based human detection using a convolutional neural network. The suggested approach makes accurate classification practicable, which is essential for the best possible nutrition. The classification leads to the division of the iris component.

Benefits include:

- High performance
- Less complexity
- High accuracy

Methodology:

Required Technologies and Techniques:

Software

- **Frontend:**
  1. HTML
  2. CSS 3. JavaScript
- **Backend:**
  1. Python
  2. Flask

Modules:

System

1.Establish a dataset with pictures of the left and right eyes. For classification, this dataset will be split into training and testing datasets.

2.Pre-processing: Modify the image's size and shape to make them suitable for model training.

3.Training: Using the previously processed training dataset, train the CNN algorithm model.

4.Classification: Our model's output is categorized and presented.

5. Segmentation: Iris data is segmented following categorization.

User

1. View training accuracy: The user can examine the model's correctness.

2. Upload Image: In order to be recognized, the user must upload the image.

3. View Results: The user can ascertain whether the iris data is authorized or unauthorized.

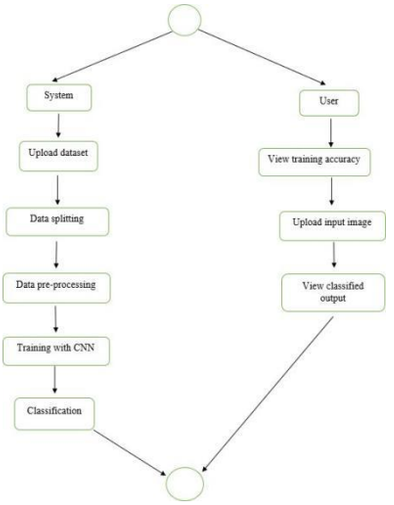
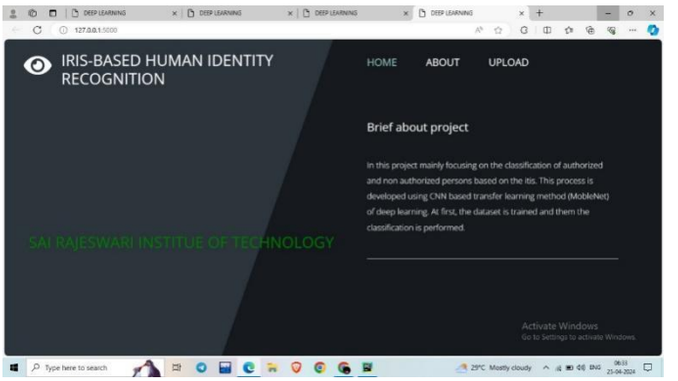


Fig 1. Software Design

ARCHITECTURE

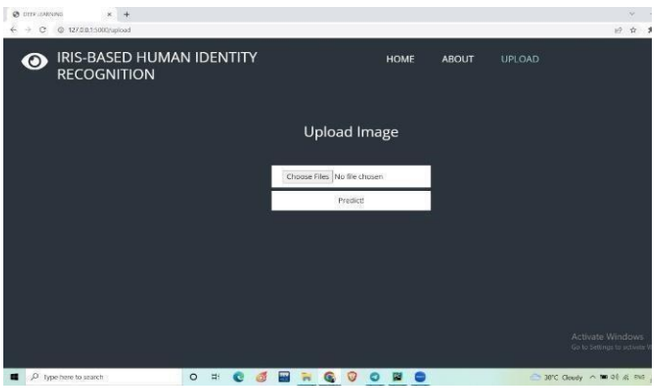
The steps 1 through 7 are listed below:

1. The user must access the main page.
   - o A web link is formed when the user executes the code.
   - o The home page appeared when the user clicks on the weblink.
   - o There are three options on the main page: -upload, about, and home.



2. User needs to upload Iris image

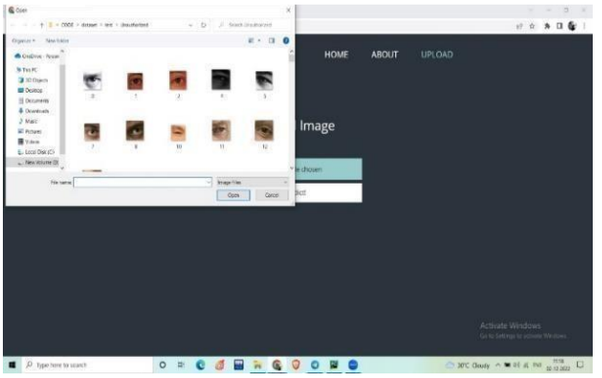
   - o From the home page, user needs to click on upload option. o Choose image dialogue box appears.



3.The user will select the picture

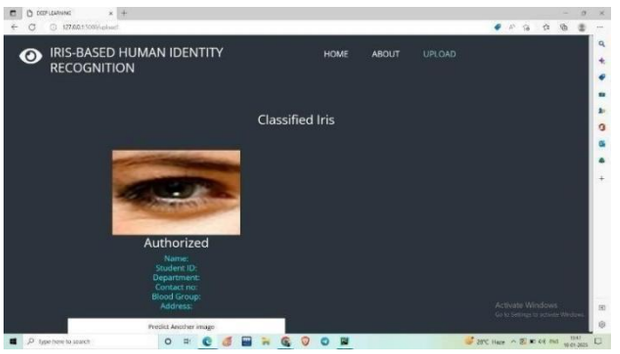
   - o In order to forecast the result, the user must now choose an iris image.

4. The model will forecast the iris image o Following the selection of a certain iris image, our model forecasts the image's authorization status.



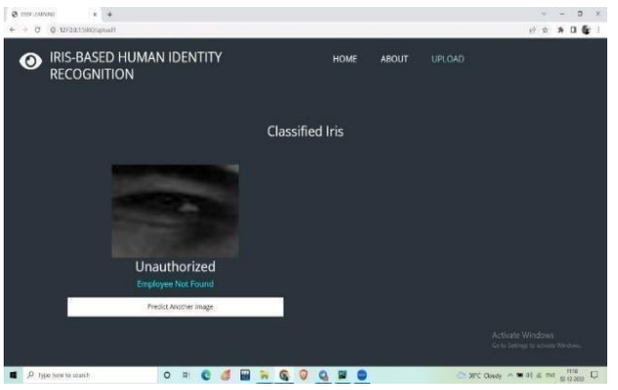
5. Verified identity

o If the human iris matches, our model indicates that an authorized employee has been located.



6. Unauthorized identity

o Our model indicates "unauthorized- employee not found" if the human iris does not match



7. Iris Classification

o After the prediction the user simply gets out of the web

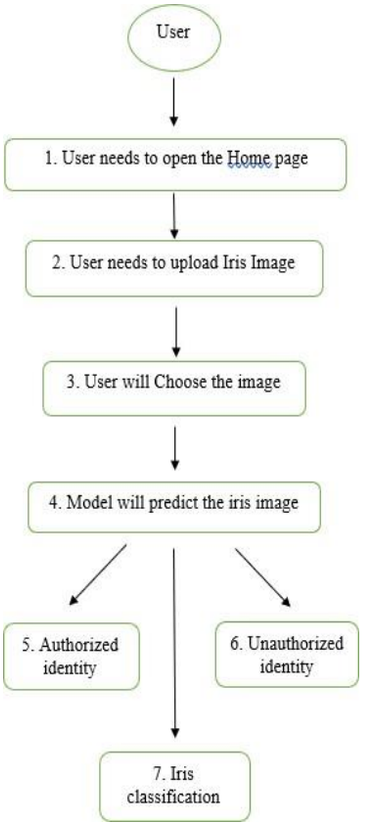


Fig. 2: Architecture

Algorithms:

Convolutional Neural Network

Convolutional neural networks, a type of deep learning technique, are used for object or image identification and grouping. The fundamental reasoning is that images high dimensionality is reduced without losing information because to the integrated convolutional layer. Padding and stride are important concepts in convolutional neural network understanding. The number of steps we take during a convolutional revolution is measured by our stride. One is the default value. It is clear that the output's size is smaller than the input's. To maintain

the same dimensions in the output and the input, we use padding. Symmetrically adding zeros to the input matrix is the padding approach. It is used to equalize the size of the input and output.

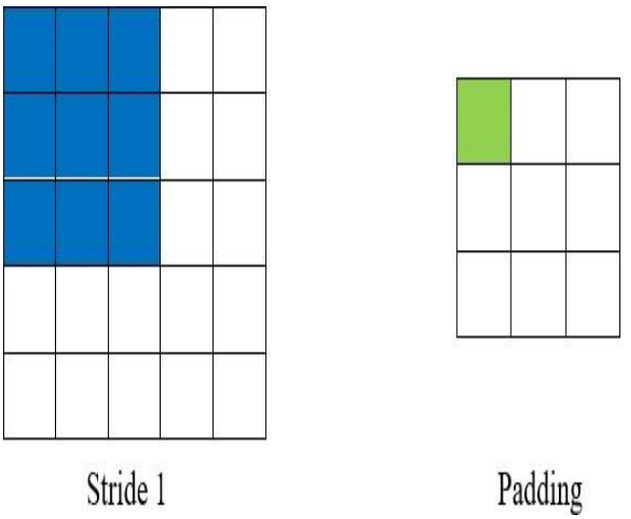


Fig 3. Strides and Padding

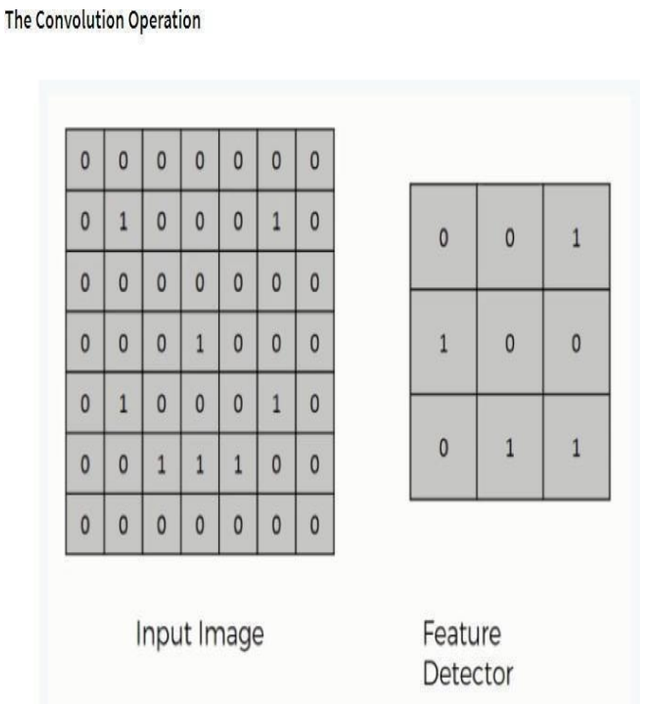


Fig 4. Convolution operation

Layers in CNN

- Input layer
- (FC) layer
- SoftMax or logistic layer
- Output
- Convo layer (Convo + ReLU)
- Pooling layer
- Fully connected layer

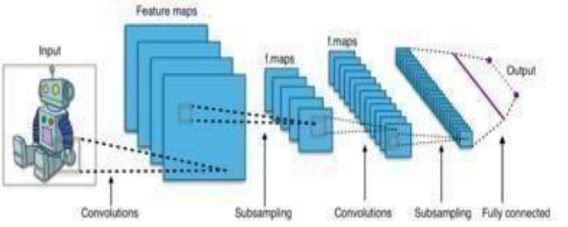


Fig 5. CNN Architecture

CNN Architecture

Image classification using convolutional neural network

Step 1: First, Select the Datasets.
Step 2: Get Training Datasets Ready
Step 3: Produce Training Data
Step 4: Combining Datasets
Step 5: Give Features and Labels
Step 6: Convert Labels to Categorical Data and Normalize X
Step 7: Divide Y and X
Step 8: Define, Compile, and Train a CNN Model
Step 9: Model Accuracy and Evaluation

CONCLUSION

For this experiment, we were able to successfully identify an iris image with the aid of deep learning. Here, we analysed the dataset of iris pictures using CNN training. The user can upload an image and review the categorization results after training. After categorization, the iris part of the output is segmented.

Future Scope

This process might be extended to incorporate biometrics in the future. Biometrics that primarily use the iris area will be more beneficial for this type of task.

References

[1]. Rana HK, Azam MS, Akhtar MR, Qunin JMW, Moni MA (2019) A fast iris recognition system through optimum feature extraction. PeerJ Comput Sci.

[2]. Daugman J. (2004) Iris recognition implementation. 14(1):21-30The IEEE Transactions on Circuits, Systems, and Video Technology.

[3]. A quick iris is expected to register via optimised feature extraction. Rana HK, Azam MS, Akhtar MR, Qunin JMW, and Moni MA (2019). PeerJ Comput Sci., 184.

[4].Sun H-M, Chen Y-H, and Lin Y-H (2012) established Pass, a user authentication system that seems to be immune to hacking attempts that also steal or reuse passwords. 7(2):651-663 IEEE Transactions on Inf Forensics and Security.

[5].On iris spoofing employing a print attack, Gupta P, Behera S, Vatsa M, and Singh R (2014). Within the IEEE 2014.

[6]. Security evaluation of negative iris recognition, Ouda O, Chaoui S, and Tsumura N (2020). IEICE Trans Inf Syst, 103(5):1144-1152.

[7]. Arora S., Bhatia MPS (2020): Deep learning-based presentation attack detection for iris recognition. Int. J. Syst. Assur. Eng. Manag., https://doi.org/10.1007/s13198-020-00948-1.

[8].Mohammed NF, Ali SA, and Jawad MJ (2020): Lifting the curled iris recognition system Cognitive informatics and soft computing, published by Mallick P, Balas V, Bhoi A, and Chae GS Articles 245-254 in Springer Advances in Intelligent Systems and Computing, vol. 1040 Berlin-based Springer

[9]. Blind quality evaluation of iris pictures taken in visible light for biometric recognition Jenadeleh M, Pedersen M, and Saupe D (2020). 20(5):1308 Sensors

[10]. Post-mortem iris recognition utilising deep learning-based photo segmentation Trokielewicz M, Czajka A, and Maciejewicz P (2020). computer vision image