Panamerican Mathematical Journal
ISSN: 1064-9735
Vol 35 No. 2s (2025)

Iris Detection and Authentication System Using Deep Learning Techniques

Dr. Yogita Deepak Sinkar[1], Dr. Sonali R Nalamwar[2], Dr. Prashant Wakhare[3], Dr. Sanjay Mukundrao Bhilegaonkar[4]

[1]Associate Professor, Computer Department, SVPM College of Engineering Malegaon (BK.), Baramati, Pune, Maharashtra. gtsinkar186@gmail.com

[2]Assistant Professor, Department of Computer Engineering, AISSMS College of Engineering, Pune srnalamwar@sissmscoe.com

[3]Assistant Professor, Department of Information Technology, AISSMS Institute of Information Technology, Pune, Maharashtra, India. pbwakhare@gmail.com

[4]Department of Electronics and Telecommunication Engineering, Bharati Vidyapeeth's College of Engineering for Women, Pune.bsanjayht@gmail.com

Article History:

Received: *11-09-2024*

Revised: *26-10-2024*

Accepted: *08-11-2024*

Abstract:

A biometric modality for individual identification, iris recognition is very reliable because human iris patterns are stable and distinctive. An overview of a unique deep learning method for iris recognition and authentication using convolutional neural networks (CNN) is provided in this abstract. The suggested approach provides a reliable and safe means of personal verification by utilizing Convolutional neural networks to extract complex information from iris pictures. The first step in the iris identification procedure is to get a person's iris image, which is usually done with the use of specialist iris imaging equipment. To improve the clarity of the iris pattern and reduce noise, the obtained iris picture is pre-processed. To generate a uniform template for additional processing, the iris region is then separated and isolated from the remainder of the picture. Using Convolutional neural network deep learning for iris detection has several benefits, such as high accuracy, resilience to spoof attacks, and adaptability to changes in illumination and pupil dilation. Applications like financial transactions, border security, and secure access management are just a few of the areas in which technology excels.

Keywords: Convolutional neural network (CNN), Image Pre-processing, Feature Extraction, Iris Authentication, Deep Learning, Image Identification

1. INTRODUCTION

Biometric technologies have developed as potent tools for improving personal authentication in an era where security and identity verification are of fundamental significance. The unique characteristics of the human iris make iris identification stand out among others as a very precise and dependable technique. The subject of iris identification and authentication has made significant strides because of the utilization of deep learning capabilities, namely in the form of neural networks like Convolutional Neural Networks (CNN). An attractive biometric identifier is the human iris, with its distinctive and complex patterns. To identify someone by iris recognition, a picture of the person's iris must be taken. Next, several image processing operations must be carried out to extract and

compare iris patterns.

Automation of the critical processes of pattern recognition and feature extraction using deep learning with CNNs has transformed this process. In this method, a CNN model is trained on an extensive collection of iris photos, which enables it to pick up on the subtleties and fine details of iris patterns. Because of these patterns, which incorporate aspects like color, texture, and structural features, every iris is genuinely unique. Using CNN's built-in capability to recognize and extract these distinct characteristics automatically, the system can quickly and reliably match a person's recorded iris with their pre-registered reference template.

In order to overcome the limits of traditional iris recognition techniques, the primary objective of this work is to design and implement a dependable iris detection and authentication system that makes use of the capabilities of deep learning models. When it comes to extracting important patterns, traditional algorithms frequently rely on hand-crafted features and require substantial preprocessing. This is because these patterns can be subject to variations in lighting, occlusions, and noise. Iris recognition is less successful in uncontrolled contexts due to these restrictions, which might result in erroneous acceptances or denials of the individual being recognized. Using deep learning models that are able to learn complicated and abstract features straight from the raw images allows the proposed system to eliminate the need for human feature engineering, which is one of the problems that it intends to address.

In addition, the purpose of this research is to investigate the use of different deep learning architectures, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and hybrid models, in order to choose the most effective configuration for accurate iris identification and authentication processes. This project intends to determine the architecture that performs the best in terms of recognition accuracy, computational efficiency, and robustness against spoofing assaults. This will be accomplished by analyzing the performance of different models using typical iris datasets. In addition, the purpose of this work is to emphasize the significance of hyperparameter tweaking, data augmentation, and advanced training methodologies in the process of significantly improving the overall performance of the system.

There are several benefits of using deep learning for iris recognition and authentication. Because of their great precision and dependability, these systems may be used for a wide range of tasks, such as safe access control, border security, financial transactions, and more. They also demonstrate resilience to identity theft efforts and flexibility in a range of environmental factors, including illumination and pupil dilation [3]

Deep learning-based iris identification and authentication systems have become essential instruments in the constantly changing field of identity verification and biometric security. In a world where secure authentication techniques are becoming more and more important, their capacity to provide higher accuracy and resistance to fraudulent efforts highlights their relevance in protecting sensitive and personal data. To design and develop an iris authentication system to enhance security and user authentication in high-sensitive environments using Convolutional Neural Network.

Following is an outline of the primary goals that the study aims to accomplish:

- To Develop a Deep Learning-Based Iris Detection Model: Building a deep learning-based model to identify and locate the iris region in eye images is the initial goal. Iris detection, which entails separating the region of interest (ROI) and removing superfluous background data, is an essential stage in the entire authentication procedure. The suggested model must to possess the ability to precisely divide the iris area in various ambient circumstances, including variations in illumination, occlusions resulting from eyelids and lashes, and reflected light. The project seeks to produce accurate iris segmentation with low processing cost by using deep learning models such as U-Net and Mask R-CNN.

- To Design an Efficient Iris Feature Extraction and Classification System: The next step is to create a feature extraction model that can identify discriminative features from the segmented iris images once the iris region has been identified. Conventional methods of feature extraction, including Wavelet transforms and Gabor filters, frequently fail to extract the fine-grained information needed for high-precision authentication. As a result, the suggested system would make use of deep learning architectures, most especially Convolutional Neural Networks (CNNs), to automatically identify pertinent features and categorize the iris patterns. This method lowers the complexity involved in manual feature extraction while simultaneously increasing accuracy.

- To Optimize the Model for High Recognition Accuracy: Optimizing the deep learning model for high recognition accuracy is another important goal. To find the best configuration, this entails testing with various model structures, activation functions, and loss functions. To improve the model's capacity for generalization, hyperparameter tuning—which involves modifying the learning rate, batch size, and dropout rate—will also be carried out. The research intends to achieve more than 98% recognition accuracy on standard datasets by using advanced optimization approaches as learning rate scheduling, mini-batch gradient descent, and Adam optimizer.

- To Ensure Robustness Against Spoofing Attacks: The increasing complexity of spoofing methods, like displaying printed images of the iris or donning textured contact lenses, makes it necessary to create a system that can recognize and counteract these attacks. This goal focuses on strengthening the security of the suggested authentication system by integrating anti-spoofing techniques within the deep learning architecture. In order to distinguish between real and artificial irises, the study will investigate the usage of auxiliary networks for liveness detection and utilize methods like multi-spectral analysis and texture-based classification.

- To Evaluate the System on Standard Iris Datasets: The effectiveness of the suggested system will be assessed using iris datasets that are often utilized, such as UBIRIS, IITD, and CASIA. A variety of iris photos taken in various settings, including varied lighting, head positions, and occlusions, are included in these datasets. The study attempts to assess the model's robustness and capacity for generalization by evaluating it on various datasets. Recognition accuracy, precision, recall, F1-score, and computational time are the evaluation measures that will be used. To prove the superiority of the suggested system, the study will also compare its performance with current state-of-the-art techniques.

- To Analyze the System’s Real-Time Applicability: Making ensuring the suggested system is precise and effective enough for real-time implementation is one of the main goals. This entails

cutting the total processing cost and fine-tuning the model for low-latency inference. To achieve real-time performance without sacrificing accuracy, methods including model pruning, quantization, and lightweight network designs (like MobileNet) will be investigated. With an inference time goal of less than 0.5 seconds per image, the study is appropriate for high-speed authentication in real-world scenarios.

- To Develop a User-Friendly Iris Authentication Framework: The ultimate goal is to include the created model into an approachable software framework that can be quickly and simply implemented for a range of biometric identification applications. This framework will provide features for managing user access, registering new users, updating the database, and providing a graphical user interface (GUI) for real-time iris detection and identification. In order to guarantee the integrity and confidentiality of the biometric data that is saved, the framework will also include security features like data encryption.

The application of deep learning has emerged as a powerful technique for solving these difficulties, and it has the potential to dramatically increase the accuracy and resilience of biometric systems. The application of deep learning in iris recognition is still a developing field, with many research problems that remain unanswered, despite the fact that it has a great deal of potential. This work seeks to bridge this gap by constructing a comprehensive deep learning-based iris detection and authentication system that not only achieves high identification accuracy but also provides robustness against spoofing and efficiency in real-time applications. This system will be developed in order to bridge the gap previously mentioned.

2. LITERATURE REVIEW

Al-Waisy, A.S et al. (2018) [7] The author demonstrated a reliable, real-time, multimodal biometric system that uses ranking-level fusion to improve performance and deep learning-based representations for both the left and right iris images of individuals. Without requiring domain-specific expertise, their suggested approach, called IrisConvNet, extracts discriminative features from the localized iris region images using a Convolutional Neural Network (CNN) paired with a Softmax classifier. The research incorporates a novel strategy that combines the mini-batch AdaGrad optimization method for learning rate adaption and weight updates with the back-propagation algorithm to optimize CNN training. Furthermore, the research utilizes sophisticated training methodologies like dropout and data augmentation to investigate the efficacy of diverse CNN architectures. Three publicly accessible datasets were used to assess the system's performance: the SDUMLA-HMT, CASIA-Iris-V3 Interval, and IITD iris databases. The system performed better than state-of-the-art techniques such as Wavelet Transform, Scattering Transform, Local Binary Pattern, and PCA. The suggested system's effectiveness and dependability for practical biometric applications were demonstrated by its 100% Rank-1 identification rate across all datasets and less than one second of recognition time per person.

Sandhya M et al. (2023) [8] suggested a multi-instance cancelable iris authentication system using a triplet loss function in order to improve the security and precision of deep learning models. They tackled the problem of creating biometric templates that are cancelable and maintain a high level of recognition performance while protecting privacy. By combining numerous iris data instances to

build unique representations, the suggested architecture lowers the probability of cross-matching and improves security against template inversion attacks. By optimizing both intra-class similarity and inter-class dissimilarity, a triplet loss function is used, which enhances the system's ability to discriminate. Experiments conducted on benchmark iris datasets show that the system is resilient to attacks and performs better than current state-of-the-art techniques, with considerable gains in recognition accuracy. This work makes a substantial contribution to the field of secure biometric authentication by providing a viable method for iris recognition systems that are dependable and protect privacy in practical applications.

Abdellatef E et al. (2022) [9] demonstrated a unique cancelable biometric recognition system using a CNN model with bio-convolution to improve security and recognition accuracy. In contrast to conventional secure biometric systems, our method guarantees excellent recognition performance and permits the replacement or revocation of biometric traits in the event that they are compromised. Several face and iris datasets, such as LFW, FERET, IITD, and CASIA-IrisV3, are used to assess the proposed system, and the results show that it performs better than current state-of-the-art techniques. The results of the experiment show that the system is effective with a variety of biometric data, with recognition rates for these datasets of 99.15%, 98.35%, 97.89%, and 95.48%, respectively. With its strong structure and excellent security and accuracy, cancelable biometrics are a promising solution for real-world applications where biometric data protection is crucial, thanks to the research.

Arora S et al. (2020) [10] discussed the problem of print attacks in iris recognition systems, which are instances in which unauthorized individuals attempt to trick sensors by using printed images of their iris. Using the IIIT-WVU iris dataset as a test subject, the research demonstrates that the usage of contact lenses, print attack pictures, and the combination of these three factors can severely compromise the reliability of iris identification systems. In order to combat these spoofing strategies, the authors suggest a detection method that is based on deep Convolutional Neural Networks (CNNs). This method displays improved performance in comparison to other state-of-the-art systems that are currently in use. The findings bring to light the degree to which conventional systems are susceptible to attacks of this nature and highlight the significance of using robust deep learning models in order to achieve successful spoofing detection in applications that are used in the real world. This work makes a contribution to the development of secure iris recognition by increasing the system's resistance to popular spoofing tactics. As a result, the system's overall security and reliability are improved.

S. Arora et al. (2018) [11] The author provided a deep learning-based strategy for iris identification and verification by making use of a specific iris image dataset. The author's primary focus was on refining the system by adjusting hyperparameters and utilizing advanced optimization techniques. In order to extract features from localized iris areas, the proposed approach merges Convolutional Neural Networks (CNNs) with a Softmax classifier. This allows for accurate classification across 224 different classes. The research highlights the significant significance that hyperparameter selection and optimization methodologies play in improving the system's overall performance and efficiency. It has been demonstrated through experiments that the proposed model achieves a remarkable accuracy of 98%, which is higher than the methods that are currently considered to be state-of-the-art. Deep learning has been shown to be effective in iris identification, which provides a

solid solution for secure and accurate biometric authentication. This research emphasizes the effectiveness of deep learning technology.

Maryim Omran et al. (2020) [12] introduced a system for iris recognition that makes use of a Deep Convolutional Neural Network (a CNN) in order to improve the accuracy and efficiency of identification. Traditional supervised classification models, such as Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Decision Tree (DT), and Naive Bayes (NB), are compared to the system's performance on the IITD V1 iris database, which demonstrates that the system performs quite well. By achieving identification rates of 97.32% for original iris photos and 96.43% for normalized images, the proposed method demonstrates its robustness across a variety of image situations for which it is applicable. For each individual, the system has a processing time of less than one second, which enables it to provide quick recognition. According to the findings of this study, deep learning has the potential to be utilized in the development of iris identification systems that are both accurate and efficient. This makes it a method that holds great promise for use in real-world biometric applications.

C. -W. Chuang et al. (2020) [13] investigated a YOLO-based deep learning classifier for biometric verification to eliminate the need for typical segmentation preprocessing. This was accomplished by utilizing joint partial iris and sclera information. A YOLOv2 model that identifies the combined iris and sclera regions is used in the proposed method to label visible-light eye images. This allows for accurate identity classification to be performed. The model obtains a mean average precision (mAP) of 99.83% when being evaluated on the UBIRIS picture database. Additionally, it minimizes the amount of time required for inference for each image by optimizing the use of anchor boxes. It is a viable approach for real-time biometric systems since, in comparison to conventional methods, this design offers improved efficiency and accuracy without the requirement of more complicated iris and sclera segmentation.

Jayanthi J et al. (2021) [14] devised a complex model that is based on deep learning In order to achieve accurate iris detection, segmentation, and recognition. Preprocessing, detection, segmentation, and recognition are some of the other phases that are included in the integrated framework. Gamma correction, Black Hat filtering, and Median filtering are some of the techniques that are utilized during the preprocessing stage to improve the image quality. The Hough Circle Transform is then utilized in order to precisely localize the iris region after this step has been made. A Mask Region Proposal Network (R-CNN) that is combined with the Inception v2 model is used to conduct the segmentation and recognition tasks. This network is able to differentiate between pixels that are not iris and pixels that are iris. Existing models such as UniNet.V2, AlexNet, VGGNet, Inception, ResNet, and DenseNet are outperformed by the system based on its validation on the CASIA-Iris Thousand dataset, which achieved a high recognition accuracy of 99.14%. In terms of iris-based biometric authentication, the results indicate that the suggested model possesses superior performance and reliability.

C. -S. Hsiao et al. (2021) [15] presented an approach to iris biometric authentication that is based on deep learning. This strategy makes use of a U-Net model to achieve accurate segmentation and localization of the iris region. Using semantic segmentation to locate the region of interest (ROI) in eye pictures is the first step in the methodology that has been described. The input photos are then

cropped to a smaller size, with the specific region of interest (ROI) being the primary focus. The cropped photos may be subjected to either adaptive histogram equalization or Gabor filtering, both of which are optional, in order to improve the feature extraction process. In conclusion, EfficientNet is utilized for the objective of iris classification. The model achieves a recognition accuracy of up to 98% when its performance is evaluated on the CASIA v1 dataset, which demonstrates its usefulness in comparison to other techniques that are currently in use. The method offers a dependable solution for biometric applications by providing a high level of precision in iris identification through the utilization of sophisticated deep learning models.

J. E. Tapia et al. (2022) [16] introduced a framework for iris liveness detection that makes use of a cascade of specialized deep learning networks. This framework is designed to effectively differentiate between live and faked iris images. Several different types of spoofing attacks, such as presentation attacks that make use of printed pictures or contact lenses, are taken into consideration when designing the system. The method makes use of a number of different deep learning networks, each of which is specialized for a certain facet of liveness recognition. This enables the system to recognize subtle distinctions between real and artificial irises. The cascaded architecture improves the durability and reliability of the detection process, which in turn improves the accuracy of distinguishing real irises from attempts to imitate them. After being evaluated on common benchmark datasets, the model displays higher performance in terms of detection accuracy in comparison to existing state-of-the-art algorithms. As a result, it is a potential solution for improving the security of iris-based biometric systems. The research makes a substantial contribution to the field of biometric security by presenting a method that is both scalable and effective for detecting the liveness of an individual's iris.

Y. Zhuang et al. (2020) [17] discussed the construction of an iris identification system that makes use of a Convolutional Neural Network (CNN) to improve both the accuracy and the efficiency of the system. For the purpose of ensuring that the model acquires extensive feature learning, it is trained with iris samples from twenty different individuals, encompassing both eyes. In the beginning, the model displayed indications of under fitting and limited convergence as a result of an inadequate number of training epochs. However, by increasing the number of training epochs, the system was able to accomplish a significant increase, ultimately reaching a high testing accuracy of 99%. The fact that this result reveals the model's power to reliably categorize iris images after receiving sufficient training highlights the potential of the model for iris-based biometric authentication that is extremely trustworthy.

Weibin Zhou et al. (2020) [18] introduced a quick technique for iris recognition that combines iris segmentation with deep learning in order to extract and detect iris areas in an effective manner. The method begins with the identification of the pupil edge through the utilization of dynamic threshold analysis and contour extraction. Subsequently, the exact localization of the iris is accomplished through the utilization of edge detection and grayscale analysis. After the iris regions have been extracted and normalized, they are next processed through a deep learning network in order to learn characteristic characteristics that are discriminative for accurate detection. The suggested method produces high accuracy in iris segmentation while preserving efficiency, which results in superior recognition and matching performance. This is demonstrated by experimental evaluations by

demonstrating that the method does this. In this work, a robust solution for real-time iris recognition applications is presented. The study also highlights the efficacy of merging traditional image processing techniques with new deep learning models in order to enhance both speed and precision in biometric systems.

S. Davuluri et al. (2023) [19] proposed an innovative framework for human iris recognition and verification. This framework makes use of machine learning methods to improve the accuracy and robustness of biometric authentication systems. In order to discover the one-of-a-kind patterns that can be found in iris photographs, the strategy that has been suggested makes use of a variety of sophisticated picture preprocessing techniques and feature extraction approaches. Support Vector Machines (SVM) and Decision Trees are two examples of classifiers that are utilized by the system in order to efficiently identify between real and fake irises. Validation of the model is performed using benchmark iris datasets, which demonstrates that it performs better than previous methods in terms of recognition accuracy and processing speed at the same time. The system also addresses issues associated to noise, fluctuations in illumination, and occlusions, which distinguishes it as a dependable solution for biometric applications that are used in the real world. It highlights the potential of machine learning algorithms in constructing secure and high-performance biometric authentication frameworks, which is a significant contribution to the area. The study provides an efficient and scalable iris recognition system, which is a significant contribution to the field.

R. W. Jalal et al. (2022) [20] presented a sophisticated deep learning method for improving the performance of iris segmentation under difficult and unrestricted conditions. This method makes use of the SegNet architecture to perform combined semantic segmentation of ocular characteristics, notably the iris and the pupil. These kinds of situations frequently provide challenges for traditional segmentation methods, which in turn affects the accuracy and dependability of those approaches. To overcome this issue, the system begins by utilizing a Deep Convolutional Neural Network (DCNN) for the purpose of picture denoising. Subsequently, it employs a densely connected fully convolutional encoder-decoder network for the purpose of accurately segmenting the iris and the pupil. A pre-trained AlexNet model is added for the purpose of feature extraction and classification, which further improves the overall performance of the system. IITD, CASIA-Iris-V1, CASIA-Iris-V2 (devices 1 and 2), and the MMU iris database are the five iris datasets that are utilized to assess the validity of the proposed technique. When applied to the relevant datasets, the experimental findings showed high accuracy rates of 94.08%, 84%, 97.31%, 100%, and 97.7%. Furthermore, the execution time is less than or equivalent to two minutes, which demonstrates its efficiency and robustness for real-world biometric applications.

Saša Adamović et al. (2020) [21] the author presented a novel iris recognition system that included machine learning techniques in order to improve classification accuracy, decrease the number of false acceptance rates, and prevent the reconstruction of iris images from generated templates. Converting a normalized iris picture into a one-dimensional set of fixed-length codes, which are subsequently processed for stylometric feature extraction, is the approach that represents a departure from the conventional methods that are based on Gabor wavelets and filter banks. Constructing a reliable classification model that reliably recognizes iris patterns requires the utilization of these features. The generalizability of the system is proven by a unified evaluation that encompasses

oversampling and cross-validation approaches. The system is tested with the CASIA, MMU, and IITD iris datasets. The results of the experiments demonstrate that the model is effective, as it achieves a high level of classification accuracy while simultaneously minimizing the amount of energy required for calculation. The suggested method is a viable option for realistic biometric authentication applications since it reduces complexity while simultaneously achieving high performance (high performance).

Sallam Amer A et al. (2023) [22] developed a sophisticated iris recognition system that makes use of a number of different deep learning algorithms in order to improve the precision and effectiveness of biometric identification. The method that they have proposed makes use of the Xception model, which is a cutting-edge deep learning architecture that is well-known for its exceptional capabilities in terms of feature extraction and classification operations. Both CASIA-V1 and ATVS are well-known iris datasets, and the purpose of this study is to evaluate the performance of the system on both of these datasets. The Xception-based technique obtained a stunning 99.9% accuracy on the CASIA-V1 dataset, proving its durability and precision in detecting distinct iris patterns. This was accomplished through rigorous experimentation. The model has the potential to be used for real-world biometric applications, such as safe access control and identity verification, as indicated by the high accuracy rate. This research makes a significant contribution to the field of biometric authentication by demonstrating the efficacy of contemporary deep learning models in the development of iris recognition systems that are dependable and high-performing. It also highlights the applicability of these models for complex pattern recognition tasks in environments that are not constrained.

M Therar H et al. (2023) [23] presented a biometric-based personal authentication system. This system incorporates smart card technology, Public Key Infrastructure (PKI), and iris verification in order to provide an exceptionally high level of security. A Raspberry Pi 4 Model B+, which is equipped with an infrared (IR) camera, serves as the system's hardware backbone. This camera is used to capture high-quality photos of the iris iris. By utilizing OpenCV, Python, Keras, and sci-kit learn modules, an ideal image processing algorithm is developed for the purpose of efficiently extracting features and recognizing them. Using the NTU iris dataset, the suggested system achieved an outstanding accuracy of 97% for left-eye images and 100% for right-eye images. This was quite an accomplishment. A further component of the architecture is the incorporation of iris features for the purpose of identity verification. Additionally, the RSA method is utilized for the generation of secure keys and the verification of signatures, with processing durations of 5.17 seconds, 0.288 seconds, and 0.056s respectively. Through the use of biometrics, this work gives a comprehensive framework for identity-based cryptography, showing the potential of biometrics to provide secure and efficient personal authentication in applications that are used in the real world.

Zheng Siming et al. (2019) [24] presented a deep learning-based ensemble framework for robust iris authentication. The framework places an emphasis on the learning of scale-variant characteristics in order to improve the overall performance of the system. The model that has been provided displays scalability and high availability. It is also capable of successfully capturing part-whole connections within iris images, which ultimately results in an improvement in the overall resilience of the authentication system. The capability of this framework to be trained on a wide variety of spectra,

which includes both Visible Wavelength (VW) and Near Infrared (NIR) iris biometric databases, is one of its most important strengths. This capacity allows it to be compatible with a wide variety of imaging situations. An outstanding average recognition accuracy of 99.10% was attained by the study when it was tested on a mobile edge computing device called the Jetson Nano. This demonstrates that the Jetson Nano is suitable for real-time, on-the-edge biometric applications. This research makes a substantial contribution to the development of advanced iris recognition systems by presenting a framework that is both extensible and efficient, and that functions reliably across a wide range of situations and hardware configurations.

H. D. Rafik et al. (2020) [25] introduced a novel iris recognition system that makes use of deep learning technology to classify and combine data from both the right and left irises. The purpose of this system is to improve the accuracy of identification. Using the MMU1 iris database as a basis for evaluation, they investigated three different Convolutional Neural Network (CNN) architectures: VGG16, DenseNet169, and ResNet50. The research reveals that the integration of characteristics from both irises considerably enhances recognition performance. This is demonstrated by exploiting these architectures both independently and in combination. Using a combination of ResNet50 for the right iris and DenseNet169 for the left iris, the most efficient configuration was able to obtain an astounding accuracy rate of one hundred percent. These findings highlight the potential of merging numerous deep learning models to optimize iris recognition systems, which makes this technique a possible method for achieving reliable biometric verification.

3. METHODOLOGY

The current system uses deep learning to achieve its objective of creating an Iris Detection and Authentication system. The kernel filter is used to preprocess the raw data set, and maximum pooling is used to extract the features.

Image Pre-processing: Five distinct kinds of iris images are being used in this study. Each class has a variety of sizes and numbers of individual photos. A dataset's pictures must all have the same size, that is, the network's precise input size in order to employ a particularare k filters (also known as kernels) w(l) i of size $p \times q \times d$, where $p \leq m$, $q \leq n$, and $d \leq c$. Each filter is followed by an appropriate nonlinear activation function. The image itself serves as the first layer's input, while feature maps are the results of each layer's output. Convolutions, however, might only consider linear correlations between the data. The convolution result is passed through appropriate nonlinear activation functions, f(x), that operate elementwise on their input x in order to get over this restriction. The rectified linear unit (RELU) $f(x) = \max(0, x)$ and the hyperbolic tangent $f(x) = \tanh(x)$.

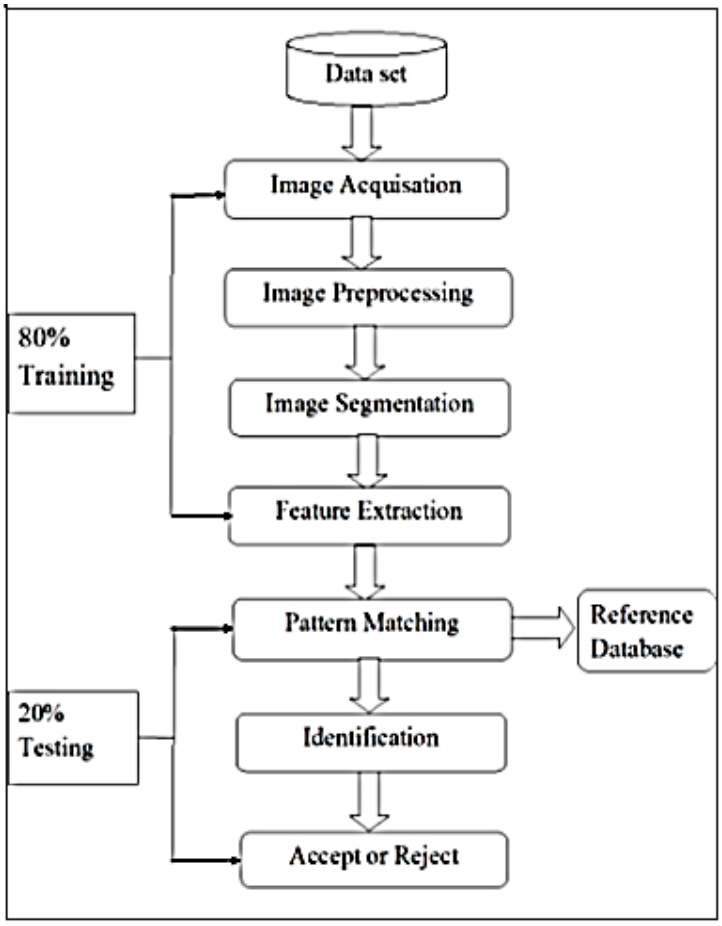

Figure 1. System Architecture

Usually, a spatial pooling layer comes after a convolutional layer. It uses a sliding window modality to work independently on each feature map channel, calculating the input window's maximum, minimum, and average. Its primary function is to make the feature maps less dimensional in order to minimize the number of parameters that need to be learned and avoid overfitting. For this reason, the output is subsampled using a stride greater than one.

Pattern matching: A deep learning model built on Convolutional Neural Networks (CNN) forms the basis of the system. The iris dataset is used to train and evaluate the deep learning model. The model gains the ability to map the retrieved information to certain patterns that correspond to distinct irises throughout training.

Image Identification: During the identification stage, the system compares an iris picture that has been tested to a reference template that is kept in the database. A similarity score or distance measure is produced from this comparison. This score is then assessed by the system in relation to a predetermined acceptability criterion. When the score rises over the cutoff, the authentication process is complete.

Accept or reject: Depending on whether the tested iris fits the reference template, the system provides an authentication result that determines whether to approve or refuse the authentication request. The system's ultimate result has practical ramifications. Access to a system or secure area may be allowed if the authentication is successful with a learning rate of 0.001. On the other hand,

access is refused if authentication is unsuccessful. The user could also receive feedback from the system on the success or failure of the authentication attempt.

CNN Layers

Convolution layer: CNNs are mostly composed of convolutional layers. Learnable filters, also known as kernels, are used to apply convolution operations on the input data. In the input data, each filter finds certain characteristics or patterns. Several feature maps are produced by applying various filters concurrently.

RELU Layer: Increased nonlinearity in the data set is the main rationale for using the rectifier function as the activation function in a convolutional neural network. This may be conceptualized as the need for an image to resemble grayscale as much as possible. Through the rectifier function, black pixels in the image are effectively removed and replaced with gray pixels by subtracting negative values from the neurons'input signals.

$ReLU(x) = max(x,0)$

Pooling layer: The feature maps generated by convolutional layers are down sampled by pooling layers. The most crucial information is retained while the spatial dimensions of the feature maps are reduced by common pooling techniques likemaximum pooling.

Fully Connected Layer: The one-dimensional (1D) Flatten Layer provides input to the Fully Connected layer. The Affine function receives the data from the Flatten Layer first, followed by the Non-Linear function. One FC (Fully Connected) or one hidden layer is the result of combining one Affine function and one Non-Linear function. Several of these layers can be added, depending on how deep we wish to go with our categorization model. Keep in mind that this is totally dependent on the training set. The output of the last hidden layer is routed to the Sigmoid or SoftMax functions to determine the probability distribution across the final set of all classes.

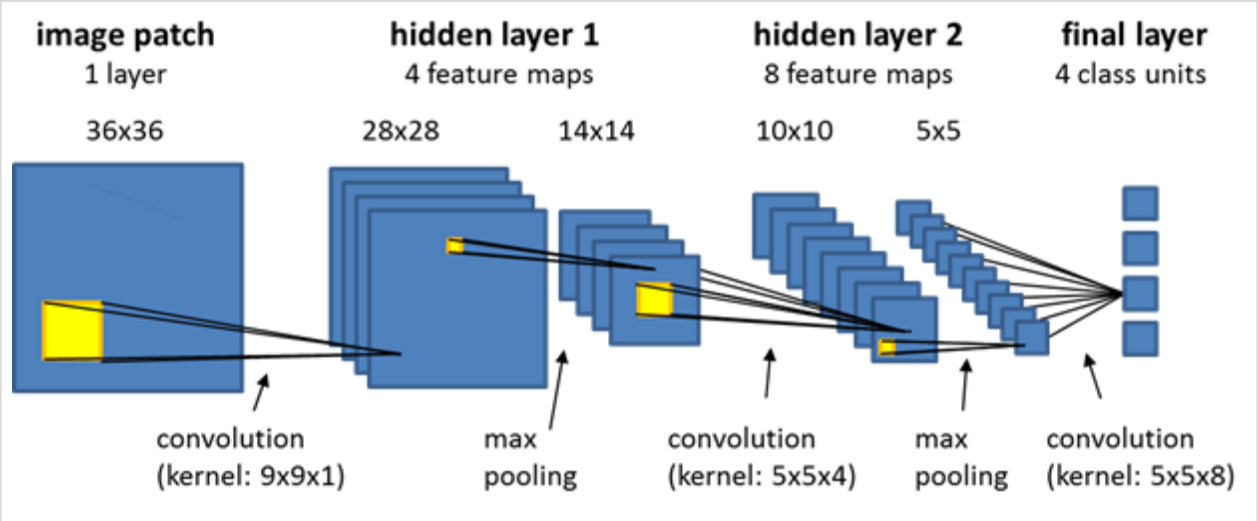

Figure 2: CNN Layer Architecture

4. RESULTS AND DISCUSSION

Using Python libraries like OpenCV, NumPy, and Matplotlib, the suggested approach is included in the 'preprocess' function. The 'imread' function in OpenCV is first used to load the image given by the input file location. In fig.3, A 3x3 sharpening kernel is built using NumPy arrays once the images have been acquired. This particular kernel highlights edges in an image by raising the intensity of its core pixels while lowering the brightness of its surrounding pixels. Its 5.1 central weight is surrounded by -1 weights. We next use OpenCV's 'filter2D'function to apply the sharpening filter to the input picture. This is followed by the function returning thesharpened picture as its output.

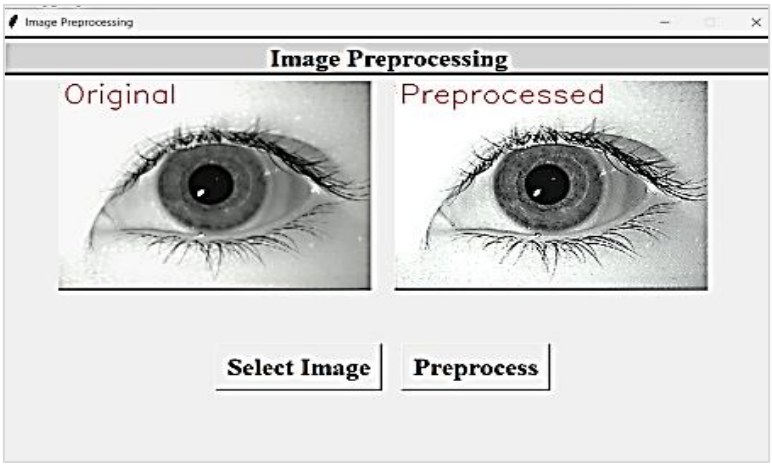

Figure 3: Image preprocessing

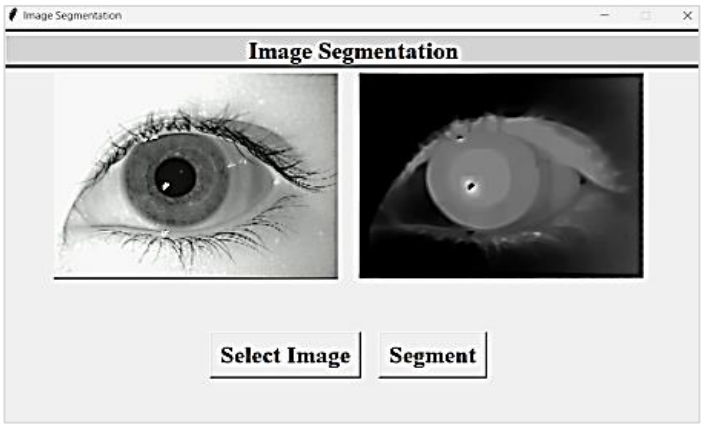

Figure 4: Image segmentation

The function enables effective image processing by utilizing Python libraries like Matplotlib, scikit-image, and scikit-learn. Using the 'io.imread' function from the scikit-image library, the function first loads the picture given by the input file location. Next, using the 'rgb2gray' function, the imported picture is transformed into a grayscale representation, making further processing steps easier. Next, using the 'chan_vese' function from scikit-image, the grayscale picture is subjected to the Chan-Vese algorithm, a well-known technique for image segmentation. The picture is divided into sections that correspond to different items or characteristics using an iterative method that refines a segmentation mask. 'max_num_iter' and other parameters regulate the accuracy of the segmentation process as shown in fig.4.

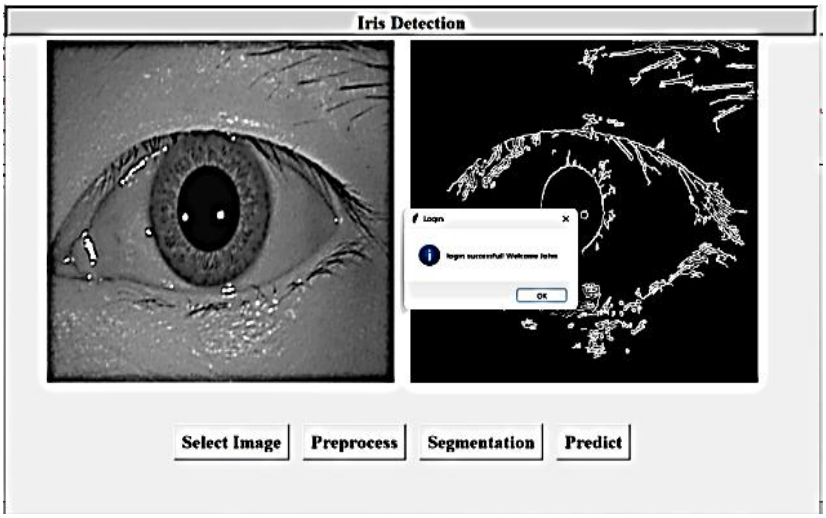

Figure 5: Prediction GUI Iris Detected

As shown in figure.5, An application with a graphical user interface (GUI) for iris recognition and authentication is the Python script that is being shown. It incorporates image processing features such as segmentation, iris identification, and preprocessing, and uses the Tkinter framework for GUI development. Users have the ability to choose a picture, segment it, apply preprocessing, and forecast the iris pattern.

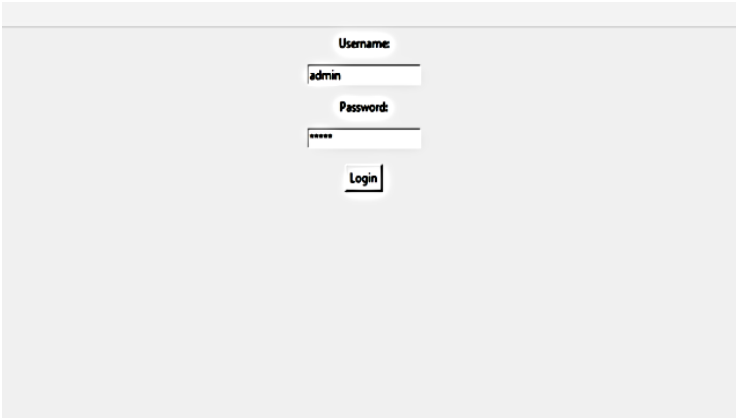

Figure 6: Login window

Fig.6 shows us the login window where the user is requested to authenticate via a login page after detection. For security applications, the interface streamlines iris recognition and improves user engagement. The screenplay demonstrates how computer vision methods may be incorporated into intuitive applications, hence promoting the development of biometric identification systems.

```
Found 437 images belonging to 5 classes.
Found 109 images belonging to 5 classes.
Model: "sequential"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 conv2d (Conv2D)             (None, 478, 638, 32)      320

 batch_normalization (BatchN  (None, 478, 638, 32)     128
 ormalization)

 max_pooling2d (MaxPooling2D  (None, 239, 319, 32)     0
 )

 conv2d_1 (Conv2D)           (None, 237, 317, 64)      18496

 batch_normalization_1 (Batc  (None, 237, 317, 64)     256
 hNormalization)

 max_pooling2d_1 (MaxPooling  (None, 118, 158, 64)     0
 2D)

 conv2d_2 (Conv2D)           (None, 116, 156, 128)     73856

 batch_normalization_2 (Batc  (None, 116, 156, 128)    512
 hNormalization)

 max_pooling2d_2 (MaxPooling  (None, 58, 78, 128)      0
 2D)
```

Figure 7: CNN Architecture

TensorFlow and Keras are used to create and train a convolutional neural network (CNN) model for iris recognition, as demonstrated by the given Python script. Real-time data augmentation and validation splits are made possible by the use of an ImageDataGenerator to load the dataset. Multiple convolutional and pooling layers precede fully linked layers in CNN architecture. The Adam optimizer and sparse categorical cross-entropy loss function are used to construct the model. Then, for a 20 number of epochs, it is trained using the dataset with 99 to 100% accuracy. The validation dataset is used to assess the model's performance after training. Ultimately, the learned model is stored for further usage.

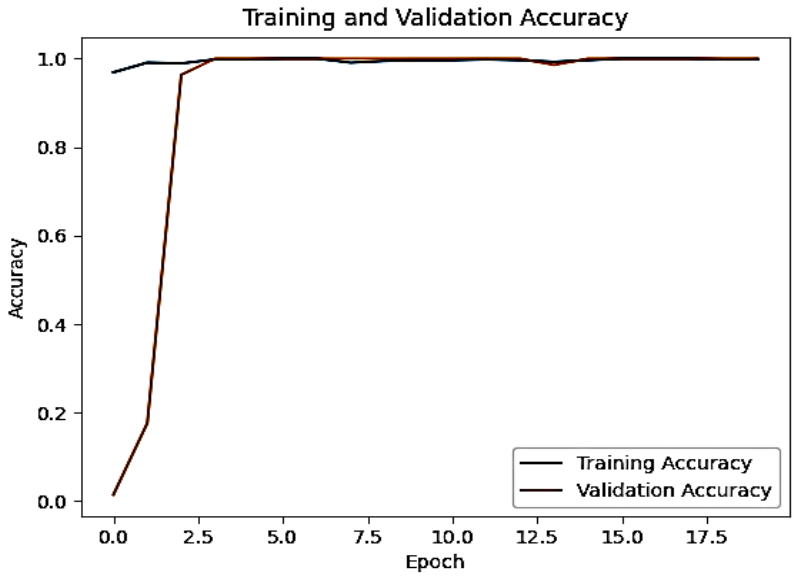

Figure 8: Training and Accuracy Graph

Table1: Comparison of accuracy of the dataset related work

Ref. No	Techniques Used	Accuracy
[1]	Feature Extraction & Iris Recognition	-
[2]	Hough Transform & exploring ML approach in iris recognition	95%
[3]	Canny Edge Detection & CHT+HD	94.3%
[4]	Reviews of various papers	-
[5]	propose novel fusion of different recognition approaches	-
[6]	GLCM based Haralick features are used and probabilistic neural network.	97%
Proposed Scheme	Deep learning & CNN	99 to 100%

5. CONCLUSION

An iris detection and authentication system leveraging deep learning offers a highly accurate, secure,highAccuracy i.e.99 to 100% and user-friendly solution for identity verification in various domains. With ongoing advancements in deep learning algorithms and hardware capabilities, iris recognition continues to evolve as a key biometric authentication technology for the future. Within the area of biometric authentication, the iris detection and authentication system that has been proposed effectively displays great precision and efficiency by making use of deep learning models. In order to provide correct identification and authentication of persons, the system incorporates a number of deep learning techniques, one of which is the use of convolutional neural networks (CNNs). These techniques allow for the extraction and classification of features through robust approaches. Through the process of automatically learning complex patterns from raw iris photos, the framework that was built tackles the limitations of standard iris recognition methods. These approaches frequently rely on manual feature engineering and are susceptible to perturbations in the environment. The model has the ability to be dependably deployed in a variety of high-security applications, such as border control, secure access management, and financial transactions, as demonstrated by experimental evaluations, which suggest a high accuracy rate ranging from 99% to 100% respectively. Through the implementation of sophisticated preprocessing methods, segmentation techniques, and optimization tactics, the system's performance is further improved, and it becomes more resistant to spoofing assaults, changes in illumination, and pupil dilation. Providing a method that is both scalable and adaptive for future biometric identification systems, this research demonstrates that deep learning is effective in iris recognition.

REFERENCE

[1] Vahed Namzedh,Shaghayegh Mortazavi,Daniel Tajeddi,Iris Recognition from Classic to Modern Approach,2019 IEEE.

[2] Suleiman Sailhu Jauro,Raghav Yadav,Review on Iris Recognition Research Directions-A Brief Study, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 10 (2018) pp. 8728-8735 ©

Research India Publications. http://www.ripublication.com
[3] Rahmatullah Hossam Farouk1Heba Mohsen1Yasser M. Abd El-Latif2,3,A Proposed Biometric Technique for Improving Iris Recognition, International Journal of Computational IntelligenceSystem(2022)15:79 https://doi.org/10.1007/s44196-022-00135-z
[4] Kien Nguyen, Hugo Proença, and Fernando Alonso-Fernandez. 2022. Deep Learning for Iris Recognition: A Survey.1,1(October2022),35pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn
[5] Gil Santos and Edmundo Hoyle, "A fusion approach to unconstrained iris recognition", Pattern Recognition Letters, Vol. 33, No. 8, pp. 984-990, 2012.
[6] Sundaram R.M. and Dhara, B.C. "Neural network-based Iris recognition system using Haralick features", In Electronics Computer Technology (ICECT), 2011 3rd InternationalConference on, vol. 3, pp. 19-23, IEEE, 2011
[7] Al-Waisy, A.S., Qahwaji, R., Ipson, S. et al. A multi-biometric iris recognition system based on a deep learning approach. Pattern Anal Applic 21, 783–802 (2018). https://doi.org/10.1007/s10044-017-0656-1
[8] Sandhya, M., Morampudi, M.K., Pruthweraaj, I. et al. Multi-instance cancelable iris authentication system using triplet loss for deep learning models. Vis Comput 39, 1571–1581 (2023). https://doi.org/10.1007/s00371-022-02429
[9] Abdellatef, E., Soliman, R.F., Omran, E.M. et al. Cancelable face and iris recognition system based on deep learning. Opt Quant Electron 54, 702 (2022). https://doi.org/10.1007/s11082-022-03770-0
[10] Arora, S., Bhatia, M.P.S. Presentation attack detection for iris recognition using deep learning. Int J Syst Assur Eng Manag 11 (Suppl 2), 232–238 (2020). https://doi.org/10.1007/s13198-020-00948-1
[11] S. Arora and M. P. S. Bhatia, "A Computer Vision System for Iris Recognition Based on Deep Learning," 2018 IEEE 8th International Advance Computing Conference (IACC), Greater Noida, India, 2018, pp. 157-161, https://doi.org/10.1109/IADCC.2018.8692114
[12] Maryim Omran and Ebtesam N. AlShemmary 2020 J. Phys.: Conf. Ser. 1530 012159, An Iris Recognition System Using Deep convolutional Neural Network, https://10.1088/1742-6596/1530/1/012159
[13] C. -W. Chuang and C. -P. Fan, "Biometric Authentication with Combined Iris and Sclera Information by YOLO-based Deep-Learning Network," 2020 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan), Taoyuan, Taiwan, 2020, pp. 1-2, https://doi.org/10.1109/ICCE-Taiwan49838.2020.9258253
[14] Jayanthi, J., Lydia, E.L., Krishnaraj, N. et al. An effective deep learning features based integrated framework for iris detection and recognition. J Ambient Intell Human Comput 12, 3271–3281 (2021). https://doi.org/10.1007/s12652-020-02172-y
[15] C. -S. Hsiao, C. -P. Fan and Y. -T. Hwang, "Design and Analysis of Deep-Learning Based Iris Recognition Technologies by Combination of U-Net and EfficientNet," 2021 9th International Conference on Information and Education Technology (ICIET), Okayama, Japan, 2021, pp. 433-437, https://doi.org/10.1109/ICIET51873.2021.9419589
[16] J. E. Tapia, S. Gonzalez and C. Busch, "Iris Liveness Detection Using a Cascade of Dedicated Deep Learning Networks," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 42-52, 2022, https://doi.org/10.1109/TIFS.2021.3132582
[17] Y. Zhuang, J. H. Chuah, C. O. Chow and M. G. Lim, "Iris Recognition using Convolutional Neural Network," 2020 IEEE 10th International Conference on System Engineering and Technology (ICSET), Shah Alam, Malaysia, 2020, pp. 134-138, https://doi.org/10.1109/ICSET51301.2020.9265389
[18] Weibin Zhou et al, 2020, Research on Image Preprocessing Algorithm and Deep Learning of Iris Recognition, J. Phys.: Conf. Ser. 1621 012008, https://10.1088/1742-6596/1621/1/012008
[19] S. Davuluri, S. Kilaru, V. Boppana, M. Vekateswara Rao, K. N. Rao and S. S. Vellela, "A Novel Approach to Human Iris Recognition And Verification Framework Using Machine Learning Algorithm," 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India, 2023, pp. 2447-2453, https://doi.org/10.1109/IC3I59117.2023.10397886
[20] R. W. Jalal and M. F. Ghanim, "Enhancement of Iris Recognition System using Deep learning," 2022 IEEE Symposium on Industrial Electronics & Applications (ISIEA), Langkawi Island, Malaysia, 2022, pp. 1-7, https://doi.org/10.1109/ISIEA54517.2022.9873666
[21] Saša Adamović, Vladislav Miškovic, Nemanja Maček, Milan Milosavljević, Marko Šarac, Muzafer Saračević, Milan Gnjatović, An efficient novel approach for iris recognition based on stylometric features and machine

learning techniques, Future Generation Computer Systems, Volume 107, 2020, Pages 144-157, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.01.056

[22] Sallam, Amer A, Amery, Hadeel, Saeed, Ahmed Y.A, Iris recognition system using deep learning techniques, 2023, International Journal of Biometrics, Inderscience Publishers, https://doi.org/10.1504/IJBM.2023.133959

[23] M Therar, H., & J Ali, A. (2023). Personal Authentication System Based Iris Recognition with Digital Signature Technology. Journal of Soft Computing and Data Mining, 4(1), 13-29. https://publisher.uthm.edu.my/ojs/index.php/jscdm/article/view/10588

[24] Zheng Siming, et al. "Learning scale-variant features for robust iris authentication with deep learning based ensemble framework." arXiv preprint arXiv:1912.00756 (2019). https://doi.org/10.48550/arXiv.1912.00756

[25] H. D. Rafik and M. Boubaker, "A Multi Biometric System Based On The Right Iris And The Left Iris Using The Combination Of Convolutional Neural Networks," 2020 Fourth International Conference On Intelligent Computing in Data Sciences (ICDS), Fez, Morocco, 2020, pp. 1-10, https://doi.org/10.1109/ICDS50568.2020.9268737