

Reinforced Voting Security Through Iris Recognition and Deep Learning Models

Dr. N. Madhusudhana Reddy¹; Shaik Rafi²

¹Professor, ²M. Tech Student

^{1,2} Department of Computer Science Engineering, Rajeev Gandhi Memorial College of Engineering & Technology, Andhra Pradesh, India

Publication Date: 2025/06/20

Abstract: Voting has traditionally been conducted using a project ballot, an electronic voting machine (evm) based on direct response electronic (dre), or identical ballot boxes. To address the limitations of the existing voting system, this study proposes a digital voting method that utilizes a deep learning algorithm with iris recognition technology. The iris recognition-based voting system is a program that employs an individual's eye iris pattern to verify their identity. An automated biometric identification system known as iris recognition analyses video footage of an individual's iris to identify unique patterns that are distinct, consistent, and easily visible from a distance. The proposed technology ensures that voters can only submit one ballot, and it has the capability to detect and prevent multiple entries by the same individual. Additionally, since the Aadhaar is linked to the voter ID, this approach eliminates the need for the user to carry a voter ID that contains the required information. This enhances digitization by digitally verifying the biometric and iris pattern on each user's aadhaar card, allowing the voter's iris to be captured and used as an identity verification method at the polling station through a simple iris scan. The four processes involved in the iris recognition process are image capture, iris segmentation, feature extraction, and pattern matching. Due to its exceptional accuracy, iris recognition is considered one of the most dependable biometric modalities. As a result of incorporating the latest advancements, this system enhances digital voting and eliminates the primary drawbacks associated with traditional voting methods.

Keywords: Deep Learning, Iris Recognition, Image Segmentation, Databases.

How to Cite: Dr. N. Madhusudhana Reddy; Shaik Rafi (2025). Reinforced Voting Security Through Iris Recognition and Deep Learning Models. *International Journal of Innovative Science and Research Technology*, 10(6), 1206-1213. <https://doi.org/10.38124/ijisrt/25jun1032>

I. INTRODUCTION

The main purpose of the biometric process has been to recognize unique physical traits and qualities. A wide range of recognition technologies, such as voice, iris, and fingerprint recognition, have been created for this purpose, typically. The primary focus of biometrics is on the technical and technological domains related to body controls and body measurements. The appropriate biometric security system, on which the authentication system is constructed, has gained importance across all nations. The system has been given the appropriate, legitimate, and outstanding performance based on all of these steps and factors. The fingerprint is the sole method available for this purpose that provides the necessary security measures to ensure the system's overall uniqueness and robust privacy features. The automated methods and procedures used to ensure fingerprint similarity between two individuals have been the primary focus of exceptional fingerprint verification or the correct type of fingerprint authentication. The main objective of the basic research, which is guided by the research objectives and relevant research questions, has been consistently discussed throughout the entire chapter. The

comprehensive research framework for the entire study has been incorporated into this chapter. Every aspect that plays a role in this recognition process has been thoroughly explained by the fundamental study.

The different types of integro differential operators have been primarily employed in this recognition system to identify the inner and outer boundaries of the iris area. The proper categorization and recommended recognition system serve as the basis for the biometric system's and the biometric process's genuine success. The strength and efficiency of the "feature extraction and classification stages" are vital for the entire process to be successful. In this particular case, the majority of fingerprint game-planning image options have been proposed for the four different types of group fingerprints, which are divided into four to five classes. Among these four components, the overview is the initial and most crucial step. The unique certified cations are utilized by the particular biometric process types to gather valuable information from the numerous estimations. In various circumstances, individual priorities are crucial, and data plays a vital role in providing the necessary information. It remains crucial and significant

for this recognition system. The field of biometrics for human identification has been established to encompass the iris recognition technology, which has reached its full potential in terms of enthusiasm for the suitable "Bayesian graphical models" are used to match the corresponding images of these tests when talking about the whole recognition system. "Convolution neural networks" are often regarded as the most dependable and straightforward approach to overcome all of the system's difficulties among all the classifiers. It has been suggested that this extensive research project be named the "integrated approach to the proper iris recognition validation system" for the retention procedure of a human fingerprint. The main concerns and significant issues that the biometric security system has faced are numerous and varied. The main issue is the biometric authentication process, and technologies have mostly been discussed in connection with various privacy and security concerns (Hamd & Ahmed, 2018). While the biometric data is being processed, there is no alternative method to undo the damage or retrieve the pertinent data. Anyone can change the compromised passwords by using picture effects of fingerprints, iris, and ears. For all of these reasons, biometrics' fundamental functionality is still vulnerable to security and privacy risks. Several iris recognition system presentations have shown problems with the sensor module, preprocessing module, and feature extraction method, to name just a few the proper resources and state-of-the-art techniques can successfully address all of these privacy and security issues. To further secure the security process, a robust system method and a strong password should be employed.

Many publications have focused on neural networks, like multilayer perceptions (MLP), and its remarkable dependability and high accuracy states. This is mostly provided in the current era between patterned recognition and accurate classifier applications. The main machine learning technique employed in this research study was the "convolution neural network (CNN)" in order to enhance the privacy security process within the validation system. Herbadji et al. (2020) state that the input image is primarily necessary to achieve suitable working performance and to minimize the amount of processed data. In a variety of image processing states, such as factor extraction, picture enlargement, and image partitioning, the appropriate working performance has been executed. The complete research report's main objective is to start addressing the specific gaps in the current study notes on the various types of validation systems. Additionally, this part presents the greatest summary of the complete validation method, which relies solely on the iris fingerprint approach. The method is also used for properly enhancing the better approach for overly proactive security and privacy system scenarios, like fingerprints. The research topic makes it evident that the validation system in this case is totally dependent on "fingerprint iris recognition" methods and procedures. Most of the time, the appropriate number of research objectives has been proposed in accordance to the specified study purposes. All of these research objectives have mostly been presented as the best way to summarize the main investigation. All of the research objectives are listed in the following.

- To demonstrate the appropriate improvement of the validation system as a whole in relation to the relevant security tools.
- To describe the "iris biometric validation system" that is primarily used for human ID verification, including its true uniqueness, high reliability, and adequate validity.
- To reinforce the system's private networks and improve the various procedures with additional security features.
- To examine every kind of security process validation from the different study notes and identify the most important and adequate categories.

The proper validation system for iris fingerprint identification processes, according to the greatest understanding of the research. The "convolution neural network (CNN)" has served as the foundation for all machine learning methods. A suitable set of research questions has been developed in accordance with the suggested study objectives in order to ensure a thorough comprehension of the entire subject.

II. LITERATURE SURVEY

Primarily, the literature review chapter provides a comprehensive explanation of the unique problems and identifying elements that have been linked to the entire research study topic. Numerous types of study note from different writers and experts have been employed to support the fundamental research. The concise summaries of the research from the many online publications, journals, and websites also function as an assessment of the process as a whole. A fundamental inquiry has been conducted about the validation-based recognition system's whole thorough assessment technique. Together with all of these, this chapter has provided examples of the particular models and theories of the proposed topic for evaluating the description process overall. This section also discusses the gaps in the literature that are usually not included in the writers' current research notes. A biometric system is one of the safest methods to interact with the digital world, claims author Alrahawe (2018). Biometrics like fingerprint, face, and iris recognition are safer than other methods for protecting private information since they are unique to each individual (Alrahawe, 2018). Nevertheless, there was a lack of technology in the past, and any private information was not as well protected. Nowadays, biometric security is an essential part of every system because of new technology. The newest systems are using this strategy since, according to the author, these digitalization security protocols are now error-free (Singh & Kant, 2021). This is reasonably reliable for security reasons due to minor system errors. The biometric system has used a variety of recognition techniques, including the finger-knuckle recognition system.

For human identification procedures and verification phases, iris recognition has been considered one of the most popular biometric methods (Garg & Gupta, 2017). In order to show how different each person is from the others in terms of security, this particular strategy is mostly employed to highlight the unique characteristics, attributes, and elements. For the personal iris identification approach, the entire study has recommended multi-algorithmic features for the right

types of extraction methods. The technologies of segmentation and final localization are applied in tandem with the cyclical transformation process. To separate the iris from the rest of the body, the process might be used to identify a particular noise. The study method should be completed promptly in order to take into account the several kinds of components, including the customer's mental viewpoints, ergonomic features, and specific angles. Everything has been improved for the best impression of the client's specific impression based on the appropriate convenience phases of the specific biometrics. The optimum efficacy on the concentration method and the appropriate sufficiency level have been compromised with these particular circumstances. In terms of availability and cost, the ergonomic components have mostly considered the physical and psychological traits of the customers. According to Kim et al. (2019), the conduct period of the basic study is when the main opportunities for the best occurrence of the many ethical concerns are demonstrated. Overall, the process has necessitated the adoption of several facial recognition technologies that facilitate the identification of each individual in the organization. Regarding the unequal values, all of the many ethical issues have been easily managed to conduct the fundamental research in an appropriate way (Kim et al., 2019). For the sake of appropriateness and out-of-line tendencies, facial recognition is the main administrative technique that should be consistently pursued. The cutting-edge monitoring initiatives that make it very challenging to ascertain the precise quantity of the better propensity that actually exists in the face of silence are all too often avoided by technology-based businesses. Elhoseny (2018) asserts that a unimodal approach was taken in the identification and verification processes. Nevertheless, the accuracy was not fully maintained since the unimodal system failed to meet the proper decision-making demands. There was a considerable decrease in accuracy when using the unimodal technique for verification (Elhoseny, 2018). Thus, the multimodal system came into being. This overall verification accuracy was achieved because the multimodal system uses fusion technology. Among all the modalities, the fingerprint and iris always have the highest degree of permanence and distinctiveness, they are also reasonably quicker and less expensive than other modalities. They are also reasonably quicker and less expensive than other modalities. The multimodal system manages four different tasks: acquisition, feature extraction from the modalities, matching with the real one, and ultimately providing the information. In contrast, the unimodal system was not fully integrated into the decision-making concept. verdicts (La, 2021). In many cases, unimodal systems are also used when lower security can be beneficial. However, high security and sectors managing significant amounts of sensitive data require multimodal solutions. In certain technical and technological domains and departments, the biometric system has been utilized to regulate the entire body dimensioning procedure, according to Adamu (2019). According to some, the process includes a number of metrics that are directly related to the right human characteristics (Adamu, 2019). In order to achieve complete control over the human body and human processes, biometric verification has primarily proposed a variety of processor types. The system has mostly focused on accurately identifying and evaluating each person's method for correctly

classifying the various strategies under sufficient scrutiny, according to Rouid et al. (2019). The most unique approach is biometrics, which has functional traits and components to describe each thing. Some types of big data infringement processes mainly deal with higher quality business instances, and this particular technology is a superb complement to the best innovation. Biometric recognition is a valid and reliable method of verifying a live individual's actual personality, which is only dependent on their social and physiological traits (Naika, 2018). Essentially, all of these assumptions are stress-free, irreversible processes that don't change (academia.edu, 2019).

III. METHODOLOGY

➤ Proposed Work

Elections in India, the world's largest democracy, are still conducted via secret ballot voting or electronic voting machines, both of which are costly, time-consuming, and inefficient. Therefore, in order to make the system efficient and prevent undesired voting methods, it must be optimized. Inappropriate confirmation regarding the vote-casting arrangement, duplicate votes, or unlawful vote-casting are the most common problems the election commission encounters.

In an attempt to address the drawbacks of conventional voting methods, this paper investigates the idea of an iris recognition-based voting system. This approach uses iris recognition's high accuracy and dependability to address concerns with voter verification, security, and accessibility. This cutting-edge voting system is being unveiled at a pivotal moment when safe and inclusive election processes are more crucial than ever. In recent years, electronic voting machines have gained popularity as a more efficient alternative to paper ballots. Electronic voting machines (EVMs) are available for use by voters, and the machine will tabulate the results automatically. By streamlining the voting procedure and speeding up the vote count, the election results can be announced more quickly.

However, due to their widespread use, concerns have been raised regarding the security and reliability of EVMs. Critics claim that EVMs are vulnerable to hacking and tampering, endangering the integrity of the democratic process and undermining public trust in the election's outcome. Moreover, both paper-based ballots and electronic voting machines employ conventional voting methods for authentication, such as presenting identification documents or verifying voter registration information. Even while these procedures are meant to prevent fraud and ensure that only valid voter ballots are cast, they are not perfect and can be manipulated or abused. This study explores the concept of an iris recognition-based voting system to alleviate the shortcomings of traditional voting systems. By using the high precision and reliability of iris recognition, this approach aims to address concerns with voter verification, security, and accessibility. This novel voting technique is being implemented at a pivotal moment when safe and inclusive election processes are more crucial than ever. In recent years, electronic voting machines have gained popularity as a more efficient alternative to paper ballots. Electronic voting

machines (EVMs) are available for use by voters, and the machine will tabulate the results automatically. By streamlining the voting procedure and speeding up the vote count, the election results can be announced more quickly. By streamlining the voting procedure and speeding up the vote count, the election results can be announced more quickly. However, due to their widespread use, concerns have been raised regarding the security and reliability of EVMs. Critics claim that EVMs are vulnerable to hacking and tampering, endangering the integrity of the democratic process and undermining public trust in election outcomes. Additionally, both paper-based ballots and electronic voting machines employ conventional voter verification methods, such as presenting identification documents or verifying voter registration information. Even though the purpose of these processes is to prevent fraud and ensure that only eligible voters cast ballots, they are not perfect and can be manipulated or abused.

This study explores the concept of an iris recognition-based voting system to alleviate the shortcomings of traditional voting systems. By using the high precision and reliability of iris recognition, this approach aims to address concerns with voter verification, security, and accessibility. This novel voting technique is being implemented at a pivotal moment when safe and inclusive election processes are more crucial than ever. In recent years, electronic voting machines have gained popularity as a more efficient alternative to paper ballots. Electronic voting machines (EVMs) are available for use by voters, and the machine will tabulate the results automatically. By streamlining the voting procedure and speeding up the vote count, the election results can be announced more quickly. However, due to their widespread use, concerns have been raised regarding the security and reliability of EVMs. Critics claim that EVMs are vulnerable to hacking and tampering, endangering the integrity of the democratic process and undermining public trust in election outcomes. Additionally, both paper-based ballots and electronic voting machines employ conventional voter verification methods, such as presenting identification documents or verifying voter registration information. Even though the purpose of these processes is to prevent fraud and ensure that only eligible voters cast ballots, they are not perfect and can be manipulated or abused.

➤ *Proposed System;*

The "convolution neural network (CNN)" iris recognition system is highly genuine and was typically created in accordance with the business process to lessen the constraints that were in place. In order to assess the whole suitability criteria of the iris recognition system, seven steps are required, which are explained below.

- *Uniqueness:*

The specific iris system pattern varies greatly and is distinct for every element. Because of embryonic gestation, all of the symbols are extremely effective.

- *University:*

The "FER (Failure to Enrol Rate)" is extremely low. The technique is highly genuine for biometric procedures in this regard.

- *Collectability:*

The iris recognition system pattern's true shape is highly authentic, offering a wide range of solutions. The face recognition system is incredibly predictable.

- *Permanence:*

For internal use, the iris recognition technology offers numerous benefits. However, the entire mechanism is visible from the outside. For lifetime success, the one-time enrolment approach works incredibly well.

- *Acceptability:*

The primary procedure for the opposite of the specific retina is the ability to quickly scan all papers pertaining to the iris system against the fingerprint-based system.

- *Performance:*

Compared to other procedures, the identification and recognition process in this instance is incredibly efficient and authentic. Due to the extremely low acceptance rates, the "iris code matching algorithm" has been widely deployed.

- *Circumvention:*

The liveliness detection for finishing the full biometric system is a regular problem. The detection of liveliness, or the accurate confirmation of the low-intensity variation, has very limited possibilities.

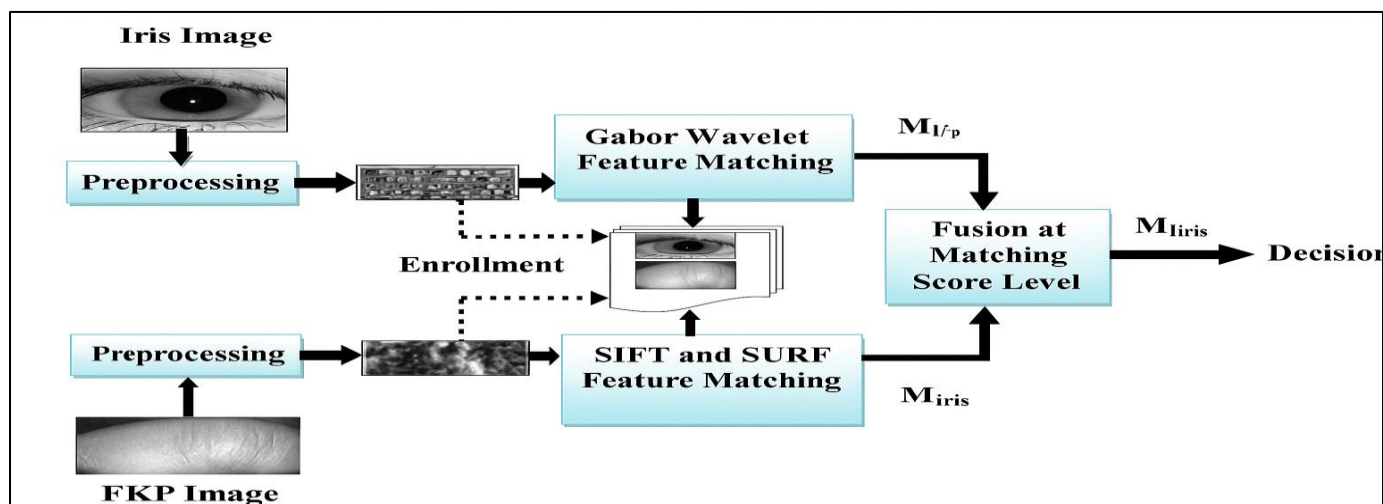


Fig 1 Architecture for Iris Image Recognition Method

IV. MODULES

Include the Iris dataset. The program will incorporate the Iris dataset during this stage.

Getting the Information Ready This module pre-processes a dataset so that it is ready for further analysis. The objective Features Extraction

This stage divides the information into two categories: training data and test data. For instance, data could be split into 30% "test" sets and 70% "training" sets. Synthesis of Models The language used to implement the idea would be Python. TensorFlow, PyTorch, and Keras are excellent Python tools for any given deep learning model. Nevertheless, leveraging these inputs to indirectly construct a model is challenging. We utilize Keras and TensorFlow as our backend libraries to create the most accurate model possible. We refer to the components of Keras sequential model as CNN layers. To improve model accuracy, these layers analyse the data in-depth by looking at various patterns that show up in the dataset. Subsequently, the data is fed into the selected model at training. Convolutional Neural Network Model Construction.

A CNN model can be constructed using this component for testing and training. Precision and Inaccuracy Chart. Using feature extraction algorithms, this enables us to visually assess the efficacy of different deep learning approaches. Uploading an Image for an Iris Recognition Test Users are able to test the software's capabilities by supplying an image for testing and then software recognition.

V. RESULT AND DISCUSSION

In this study, 108 people's photographs from the CASIA IRIS collection are utilized to identify individuals from IRIS using machine learning techniques for iris recognition. By training a CNN model on this dataset, we can utilize the CNN model to identify and predict people. We are using the Hough Circles technique, which extracts IRIS circles from eye pictures, to extract IRIS features in order to train the CNN model. The dataset with the person Identity is displayed in the screen grabs below, and it is stored in the "CASIA1" folder.

We have 200 people's IRIS images in the screen above; simply navigate to any folder to obtain that person's IRIS images, as seen in the screen below.

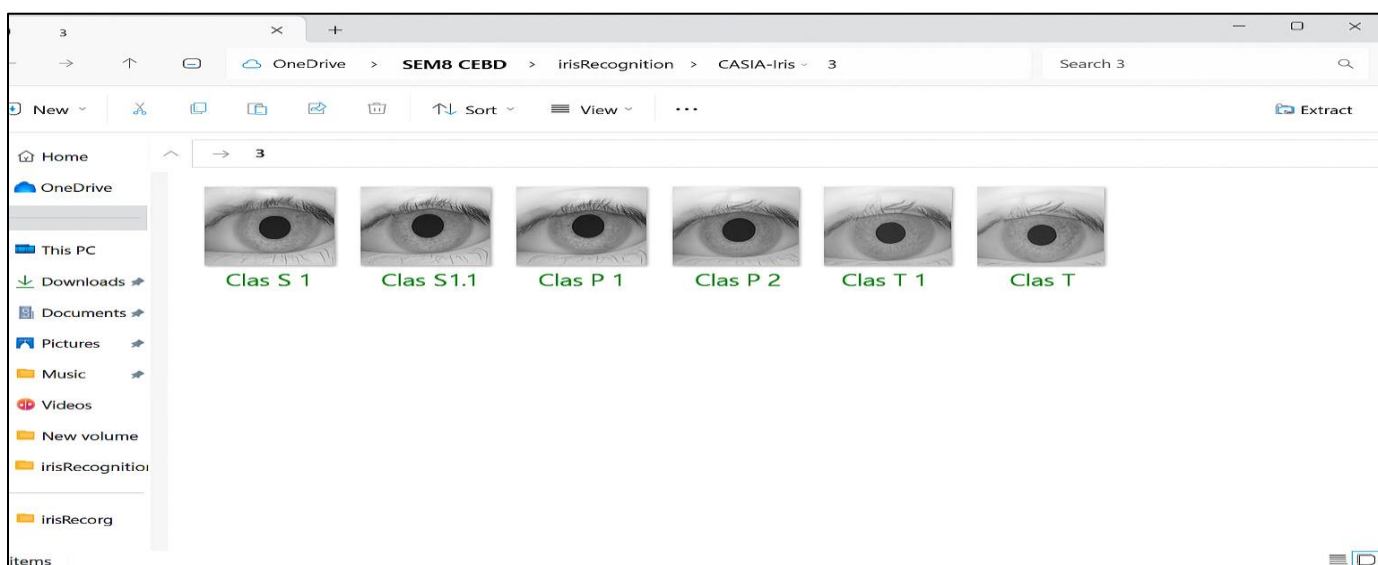


Fig 2 Iris Samples Dataset UI View

Double-clicking the "run.bat" file will launch the project and display the screen below.

Click the "Upload Iris Dataset" button in the image above, then upload the dataset folder.

After choosing and uploading a folder in the above

screen, click the "Select Folder" button to load the dataset and view the screen below.

The dataset is loaded on the screen above. To create a CNN model from the loaded dataset, click the "Generate and Load CNN Model" button.

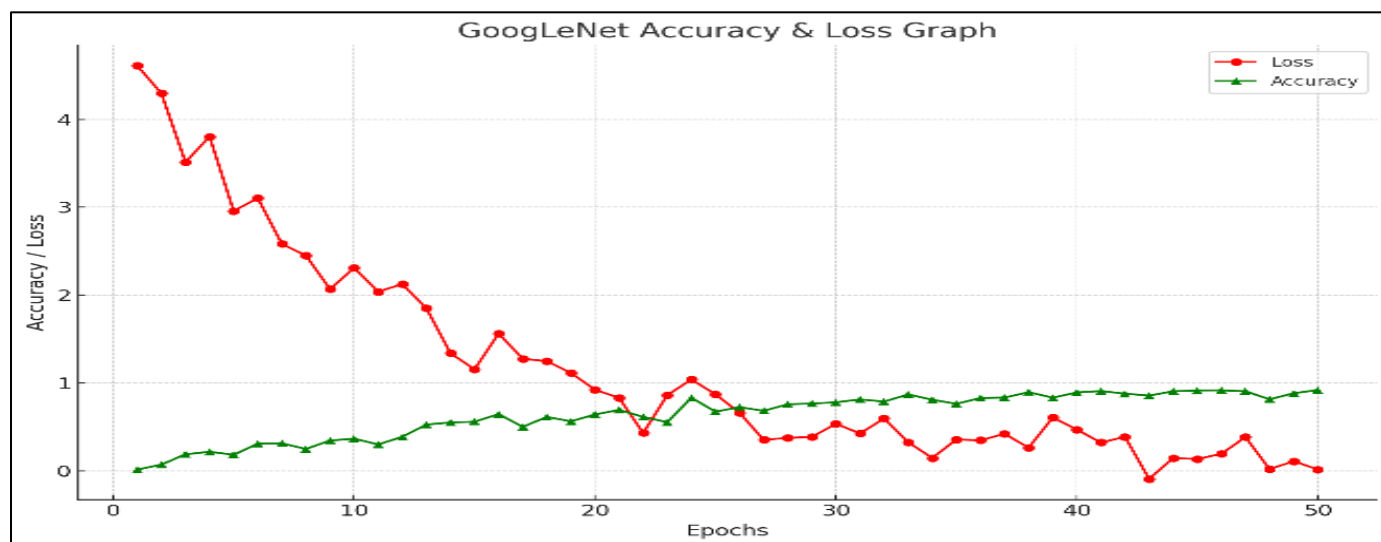


Fig 3 Google Net Accuracy & Loss Graph

The CNN model loss value, shown by the red line in the graph above, was greater than 5% at the start of the iteration and dropped to 0 as the epoch lengthened. Conversely, the green line represents accuracy, which started at 0% at the start of the iteration and rose to 100% as the number of epoch and model iterations increased. In the graph above, the x-axis stands for EPOCH, and the y-axis for accuracy and loss numbers. Click the "Upload Iris Test Image & Recognize" button now, submit any test image, and CNN will utilize the IRIS image to determine the individual's ID. If you would like to confirm that the forecast is 100% accurate, you may also

upload a test image from the folder.

To view the screen below, pick and upload the "b.jpg" file on the top screen, then click the "Open" button.

In the screen above, the uploaded image's IRIS characteristics are taken from the first image. After receiving this image, CNN makes the prediction that person Identity 25 is the owner of the IRIS. To check if CNN correctly predicts, I'll now upload one image from the CASIA folder.

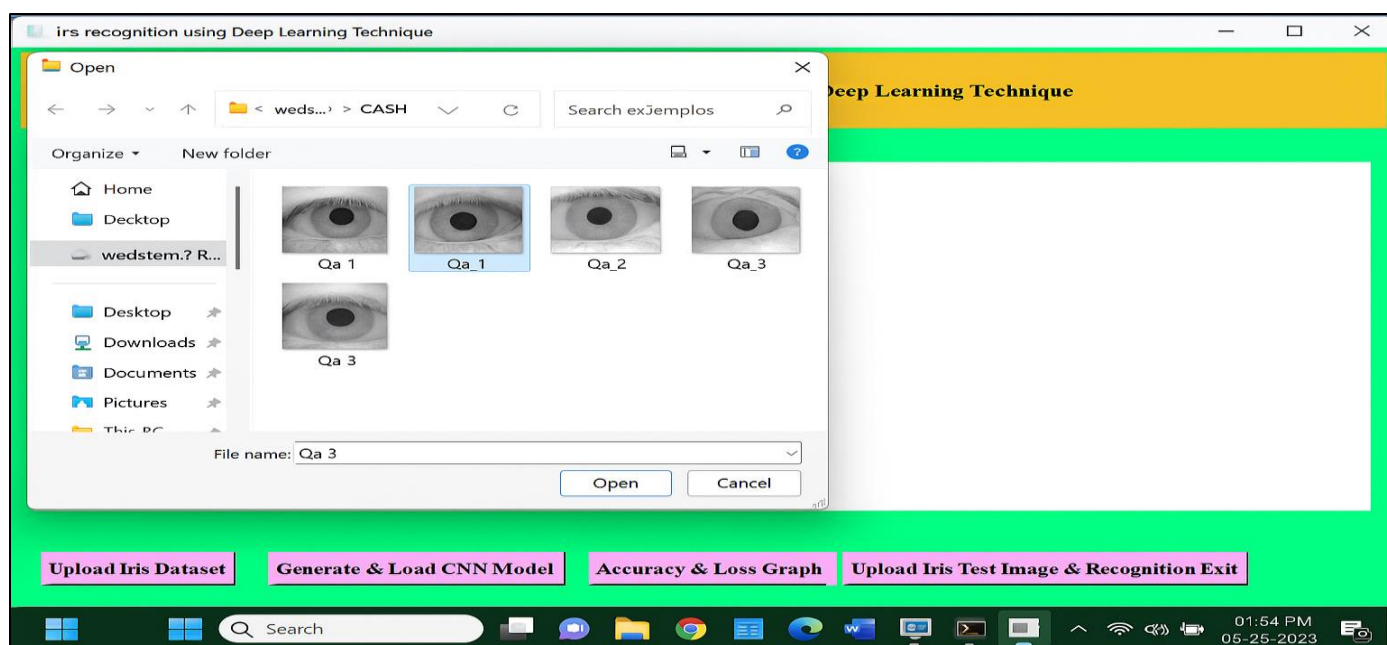


Fig 4 Deep Learning Iris GUI Dataset Selection

I've uploaded Person Identity 15's IRIS from the CASIA folder to the screen above. Click "Open" to see the results below.

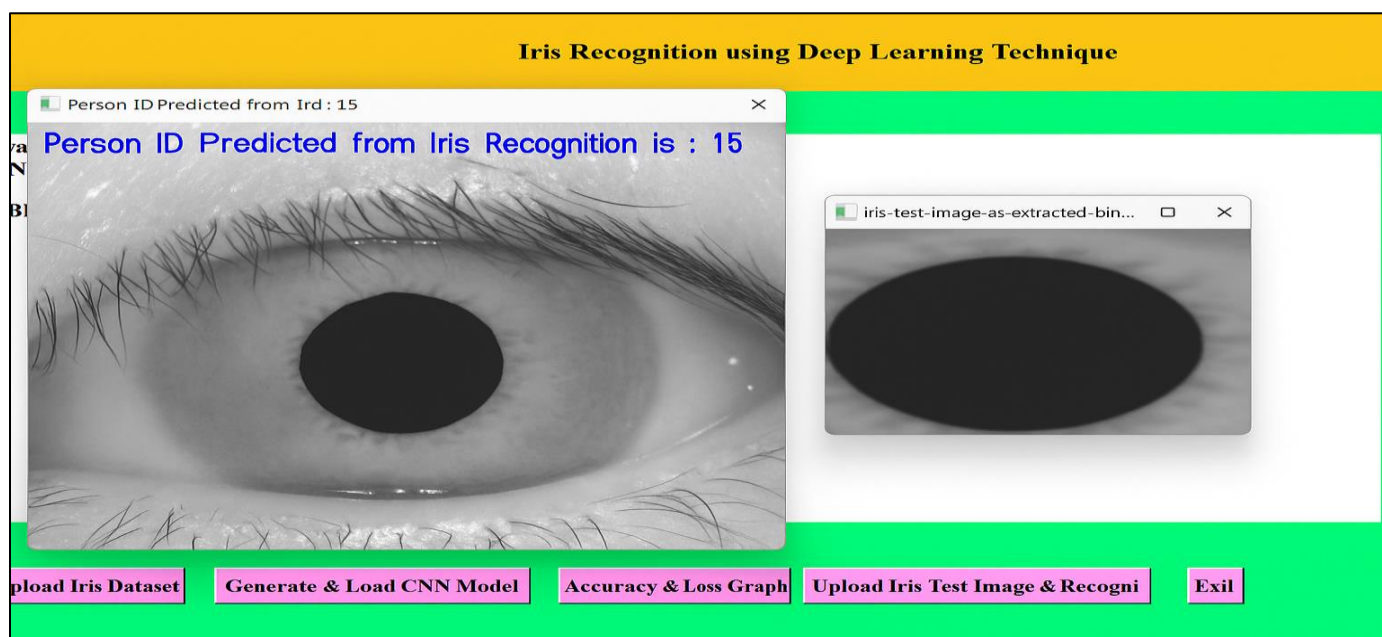


Fig 5 Iris Recognition using Deep Learning Technique

In above screen CNN predicted ID is 15 which is 100% correct.

VI. CONCLUSION

To guarantee complete validation, the iris recognition technique is suitably covered throughout the entire study paper. The most precise way to measure the various physical and automated characteristics of the entire system is through the biometric system. The most effective measurements have been conducted on the facial recognition and fingerprint-based recognition techniques out of all these features. In this instance, the artificial intelligence system and machine learning technology are far more intelligent and efficient in bringing about the real technological revolution in the relevant field. The development of the iris recognition system using the "convolution neural networking (CNN)" approach for optimal security purposes has been the primary focus of the entire project. To meet all of the needs, the technology as a whole should be more advanced for this reason. All facets of working performance have been impacted by the multimodal biometric process, which is very challenging to execute and appropriately design. With reference to the literature review, the models and theories that have been described can effectively and concisely describe all of the system's requirements and significance. The various technologies can be appropriately integrated with respect to precise software that will be really beneficial for any audience. Throughout the entire study, the right software has been employed to better understand the audience.

REFERENCES

- [1]. Mahammad, F. S., & Viswanatham, V. M. (2020). Performance Analysis of Data Compression Algorithms for Heterogeneous Architecture through Parallel Approach. *The Journal of Supercomputing*, 76(4), 2275-2288.
- [2]. Karukula, N. R., & Farooq, S. M. (2013). A Route Map for Detecting Sybil Attacks in Urban Vehicular Networks. *Journal of Information, Knowledge, and Research in Computer Engineering*, 2(2), 540-544.
- [3]. Farook, S. M., & Nageswarareddy, K. (2015). Implementation of Intrusion Detection Systems for High Performance Computing Environment Applications. *Inter National Journal Of Scientific Engineering And Technology Research*, 4(0), 41.
- [4]. Sunar, M. F., & Viswanatham, V. M. (2018). A Fast Approach To Encrypt And Decrypt Of Video Streams For Secure Channel Transmission. *World Review Of Science, Technology And Sustainable Development*, 14(1), 11-28.
- [5]. Mahammad, F. S., & Viswanatham, V. M. (2017). A Study On H. 26x Family Of Video Streaming Compression Techniques. *International Journal Of Pure And Applied Mathematics*, 117(10), 63-66.
- [6]. Devi, S. M. S., Mahammad, F. S., Bhavana, D., Sukanya, D., Thanusha, T. S., Chandrakala, M., & Swathi, P. V. (2022). "Machine Learning Based Classification and Clustering Analysis Of Efficiency Of Exercise Against Covid-19 Infection." *Journal of Algebraic Statistics*, 13(3), 112-117.
- [7]. Devi, M. M. S., & Gangadhar, M. Y. (2012). "A Comparative Study of Classification Algorithm for Printed Telugu Character Recognition." *International Journal of Electronics Communication And Computer Engineering*, 3(3), 633-641.
- [8]. Devi, M. S., Meghana, A. I., Susmitha, M., Mounika, G., Vineela, G., & Padmavathi, M. Missing Child Identification System Using Deep Learning.
- [9]. V. Lakshmi Chaitanya. "Machine Learning Based Predictive Model for Data Fusion Based Intruder Alert System." *Journal of Algebraic Statistics* 13, No. 2 (2022):

2477-2483.

- [10]. Chaitanya, V. L., & Bhaskar, G. V. (2014). Apriori Vs Genetic Algorithms For Identifying Frequent Item Sets. *International Journal of Innovative Research & Development*, 3(6), 249-254.
- [11]. Chaitanya, V. L., Sutraye, N., Praveena, A. S., Niharika, U. N., Ulfath, P., & Rani, D. P. (2023). Experimental Investigation of Machine Learning Techniques for Predicting Software Quality.
- [12]. Lakshmi, B. S., Pranavi, S., Jayalakshmi, C., Gayatri, K., Sireesha, M., & Akhila, A. Detecting Android Malware With An Enhanced Genetic Algorithm For Feature Selection And Machine Learning.
- [13]. Lakshmi, B. S., & Kumar, A. S. (2018). Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking In Public Cloud. *International Journal Of Research*, 5(22), 744-757.
- [14]. Lakshmi, B. S. (2021). Fire Detection Using Image Processing. *Asian Journal of Computer Science And Technology*, 10(2), 14-19.
- [15]. Devi, M. S., Poojitha, M., Sucharitha, R., Keerthi, K., Manideepika, P., & Vasudha, C. Extracting And Analyzing Features In Natural Language Processing For Deep Learning With English Language.
- [16]. Kumar Jds, Subramanyam Mv, Kumar Aps. Hybrid Chameleon Search And Remora Optimization Algorithm-Based Dynamic Heterogeneous Load Balancing Clustering Protocol For Extending The Lifetime Of Wireless Sensor Networks. *Int J Commun Syst*. 2023; 36(17):E5609. Doi:10.1002/Dac.5609
- [17]. David Sukeerthi Kumar, J., Subramanyam, M.V., Siva Kumar, A.P. (2023). A Hybrid Spotted Hyena and Whale Optimization Algorithm-Based Load-Balanced Clustering Technique In Wsns. In: Mahapatra, R.P., Peddoju, S.K., Roy, S., Parwekar, P. (Eds) *Proceedings Of International Conference On Recent Trends In Computing. Lecture Notes in Networks And Systems*, Vol 600. Springer, Singapore. https://doi.org/10.1007/978-981-19-8825-7_68
- [18]. Murali Kanthi, J. David Sukeerthi Kumar, K. Venkateshwara Rao, Mohmad Ahmed Ali, Sudha Pavani K, Nutanakanti Bhaskar, T. Hitendra Sarma, "A Fused 3d-2d Convolution Neural Network For Spatial-Spectral Feature Learning And Hyperspectral Image Classification," *J Theor Appl Inf Technol*, Vol. 15, No. 5, 2024, Accessed: Apr. 03, 2024. [Online]. Available: www.jatit.org
- [19]. Prediction Of Covid-19 Infection Based On Lifestyle Habits Employing Random Forest Algorithm Fs Mahammad, P Bhaskar, A Prudvi, Ny Reddy, Pj Reddy *Journal Of Algebraic Statistics* 13 (3), 40-45
- [20]. Machine Learning Based Predictive Model For Closed Loop Air Filtering System P Bhaskar, Fs Mahammad, Ah Kumar, Dr Kumar, Sma Khadar,*Journal Of Algebraic Statistics* 13 (3), 609-616