Advanced Iris Recognition: A Deep Learning Approach to Human Identification Using Convolutional Neural Networks

Rekha Sachin Kamble[1], Varsha Ravsaheb Kamble[2], Shrenik R. Patil[3]

[1]Assistant Professor, DKTE Society's Textile & Engineering Institute (An Empowered Autonomous Institute), Ichalkaranji
[2]M. Tech Scholar, DKTE Society's Textile & Engineering Institute (An Empowered Autonomous Institute), Ichalkaranji
[31]Assistant Professor, DKTE Society's Textile & Engineering Institute (An Empowered Autonomous Institute), Ichalkaranji

---

Abstract - The component of a computer system that is in charge of user security is one of the most crucial ones. Simple logins and passwords have been shown to be vulnerable to hackers and unable to provide high levels of efficiency. The most common replacements is identity recognition using biometrics. The use of the iris as a biometric feature has gained popularity in recent years. It resulted from the exceptional efficiency and precision that this approach provided. The results of this interest may be seen in the literature. Various authors have put forward a variety of various methods. The authors of this paper describe their own method for an iris-based algorithm for recognizing human identification. Artificial neural networks and a CNN-based transfer learning model (Mobile Net) were employed in the classification process. As soon as the classification is complete, the iris section is segmented on the result of the classification. The proposed approach can produce results that are adequate, according to tests that have been run.

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

1. INTRODUCTION

The solution to this problem is quite simple, and the widely recognized answer is biometrics. Biometrics is the science that identifies or verifies individuals based on their measurable physical traits, such as fingerprints, iris patterns, retina scans, or keystroke dynamics. These characteristics are categorized into three main types: physiological (related to the body and its measurements), behavioral (traits that can be learned, like a signature), and hybrid (which combines both physiological and behavioral traits, such as voice). Essentially, with a biometric-based security system, users won't need to remember additional passwords, as their unique physical traits act as their "password."

Research and experiments have shown that one of the most reliable and accurate biometric traits is the iris. The iris contains more than 250 distinct elements, each contributing to an individual's identity through a feature vector. Studies have demonstrated that the feature vectors for the left and right irises of the same person differ significantly, and this holds true even for twins. Furthermore, iris patterns are extremely difficult to spoof, with only a few studies showing any successful attempts at iris spoofing. However, it's worth noting that these studies were based on basic iris biometrics systems that did not account for "liveness" detection, leaving them vulnerable to attacks involving printed iris images.

Another challenge with iris-based biometrics is the difficulty of obtaining high-quality iris samples. Specialized devices are often needed to capture these images, and in some cases, the help of an experienced ophthalmologist may be required. While high-end smartphones like the iPhone 12 Max or Samsung Galaxy S20+ can capture good quality iris images, this typically requires assistance from another person. Alternatively, specialized sensors are available, but these tend to be expensive and may require specific lighting conditions for optimal image quality.

A significant portion of this work focused on the testing and verification processes used to assess the quality of the biometric system. The authors applied the Scrum methodology to develop the solution iteratively, evaluating the system's accuracy at each stage to ensure continuous improvement.

Another important consideration in designing iris-based security systems is preventing spoofing attacks. A common vulnerability in biometric systems is false positives caused by printed images or other replicas of real biometric samples, a particular issue in iris recognition systems. Research has shown that using printed images of live irises, contact lenses, or a combination of both can significantly increase the chances of a false-positive identification. A novel approach to address this problem involves using deep convolutional neural networks to detect and prevent such spoofing attempts.

2. Literature overview

[1] Gupta P, Behera S, and Vatsa M, Singh R: The human iris contains detailed and distinctive texture patterns, making it a highly reliable biometric identifier. Due to its uniqueness, iris recognition is considered one of the most precise methods in biometric authentication. However, these systems are not immune to spoofing attempts, which can be used to hide or mimic an identity, leading to incorrect acceptance or rejection of users. This study revisits the issue of spoofing in iris recognition and examines how such attacks impact system performance. It particularly focuses on print-based attacks combined with the use of contact lenses as a method of deception. Findings reveal that both print attacks and contact lenses—whether used alone or together—can significantly alter the biometric data, affecting the variation within and between individuals, and thereby increasing the system's vulnerability to deception. Additionally, the paper introduces the IIITD Iris Spoofing Database, which includes more than 4,800 iris images from over 100 individuals, incorporating variations caused by sensors, lenses, and printed images. The research further suggests that affordable feature descriptor techniques could be effective in mitigating spoofing risks.

Summary: This study explores the impact of spoofing attacks—specifically print-based methods combined with contact lens use—on iris recognition accuracy. It finds that these attacks can substantially alter biometric distributions, increasing the chances of deceiving recognition systems.

[2] Rana HK, Azam MS, Akhtar MR, Qunin JMW, Moni MA: The growing need for robust security has driven significant research into automated person identification using biometrics in the past decade. Biometric systems identify individuals by analyzing unique physical or behavioral traits like irises, faces, voices, or fingerprints. The iris, with its intricate and stable structure, has become a particularly attractive biometric. This study introduces a method that uses Discrete Wavelet Transformation (DWT) to prepare iris images for Principal Component Analysis (PCA). This approach aims to extract the most effective iris features and speed up the process of matching iris templates. By using DWT to reduce the image resolution into frequency sub-bands, the subsequent PCA feature extraction is performed on a smaller dataset. Our results show that this proposed technique performs efficiently.

Summary: This research introduces a method that combines Discrete Wavelet Transformation (DWT) with Principal Component Analysis (PCA) to extract the best iris features and speed up the classification of iris templates. The underlying principle of using DWT before PCA is to lower the resolution of the iris template.

[3] Arora S, Bhatia MPS: Iris recognition is widely employed in various systems for personal identification. However, these systems are increasingly susceptible to presentation attacks, where unauthorized users attempt to mimic legitimate users. This study specifically explores print-based spoofing, where printed iris images are presented to the sensor to fool the system. The research, based on the IIIT-WVU iris dataset, demonstrates that using printed iris images, contact lenses, or a combination of both can significantly disrupt the accuracy of iris recognition systems. To address this vulnerability, the study implements deep Convolutional Neural Networks (CNNs), which prove to be highly effective in detecting such spoofing attempts, outperforming existing leading techniques.

Summary: Using the IIIT-WVU iris dataset, the study shows that spoofing through printed iris images, contact lenses, or both can compromise iris recognition systems. The proposed method, based on deep Convolutional Neural Networks, effectively detects these attacks and delivers better performance than current state-of-the-art solutions.

Investigation of current project and related work

Human Identification Using Iris by CNN is a research project focused on utilizing Convolutional Neural Networks (CNN) for iris recognition and identification. It aims to create an accurate system that can identify individuals based on their unique iris patterns, which is considered a reliable biometric identification technique.

The project leverages previous research and technologies in iris recognition. Traditional methods like Daugman's algorithm have been widely used as the foundation for iris recognition systems. CNN-based approaches have also emerged, taking advantage of deep learning techniques for feature extraction and classification.

Researchers commonly use iris databases such as the CASIA Iris Image Database and the IIT Delhi Iris Dataset to evaluate and compare the performance of iris recognition algorithms. These databases consist of diverse iris images captured under various conditions, including different devices and iris presentation attacks.

DeepIrisNet and IrisNet are examples of CNN-based iris recognition models that have demonstrated competitive performance. DeepIrisNet utilizes a deep network architecture for end-to-end iris recognition, while IrisNet incorporates attention mechanisms to improve recognition accuracy.

To enhance security and prevent presentation attacks, researchers have explored iris liveness detection techniques and multi-spectral imaging. Liveness detection helps differentiate real iris patterns from fake or spoofed samples, while multi-spectral imaging captures additional iris information for better presentation attack detection.

Ethical considerations surrounding privacy, data protection, bias, fairness, and consent are important in the development and deployment of biometric identification systems like iris recognition. Addressing these concerns ensures responsible and ethical use of the technology.

The "Human Identification Using Iris by CNN" project aims to advance iris recognition technology by building upon previous research. It strives to improve accuracy, robustness, and efficiency in iris recognition through the development of a CNN-based system. By addressing existing challenges and limitations, the project contributes to the broader field of iris recognition and its practical applications.

3. Architectural Design

The architectural design diagram for the "Human Identification Using Iris by CNN" project provides a high-level overview of the system's structure and how its components interact.

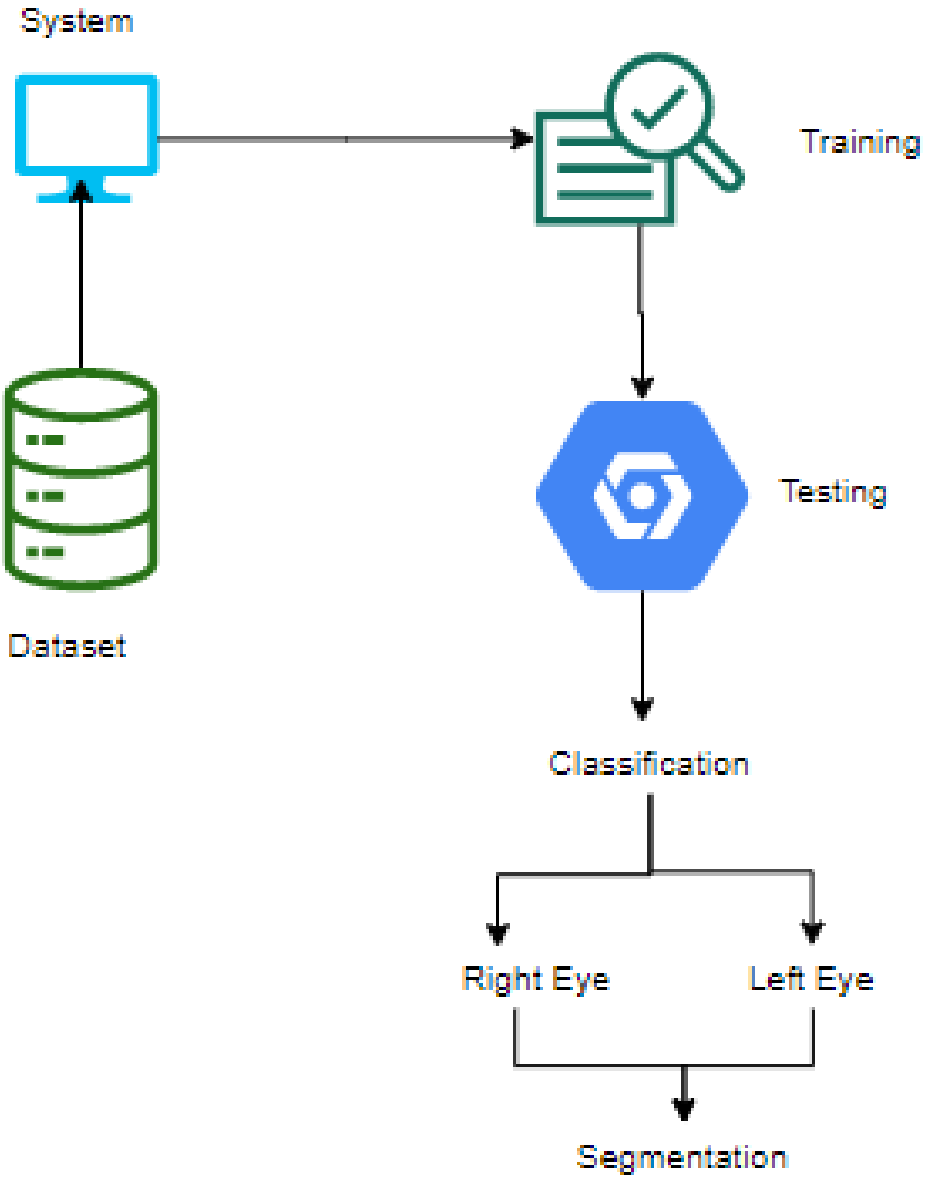


Fig 3.1 Architectural Design

. Algorithmic description of each module

4.1 Convolutional Neural Network

Step1: convolutional operation

The convolution operation forms the first crucial element of our approach. In this stage, we will examine feature detectors, essentially the filters used by the neural network. Our discussion will also include feature maps, how their parameters are learned, the mechanism of pattern detection, the hierarchy of detection layers, and the mapping of the resulting information.

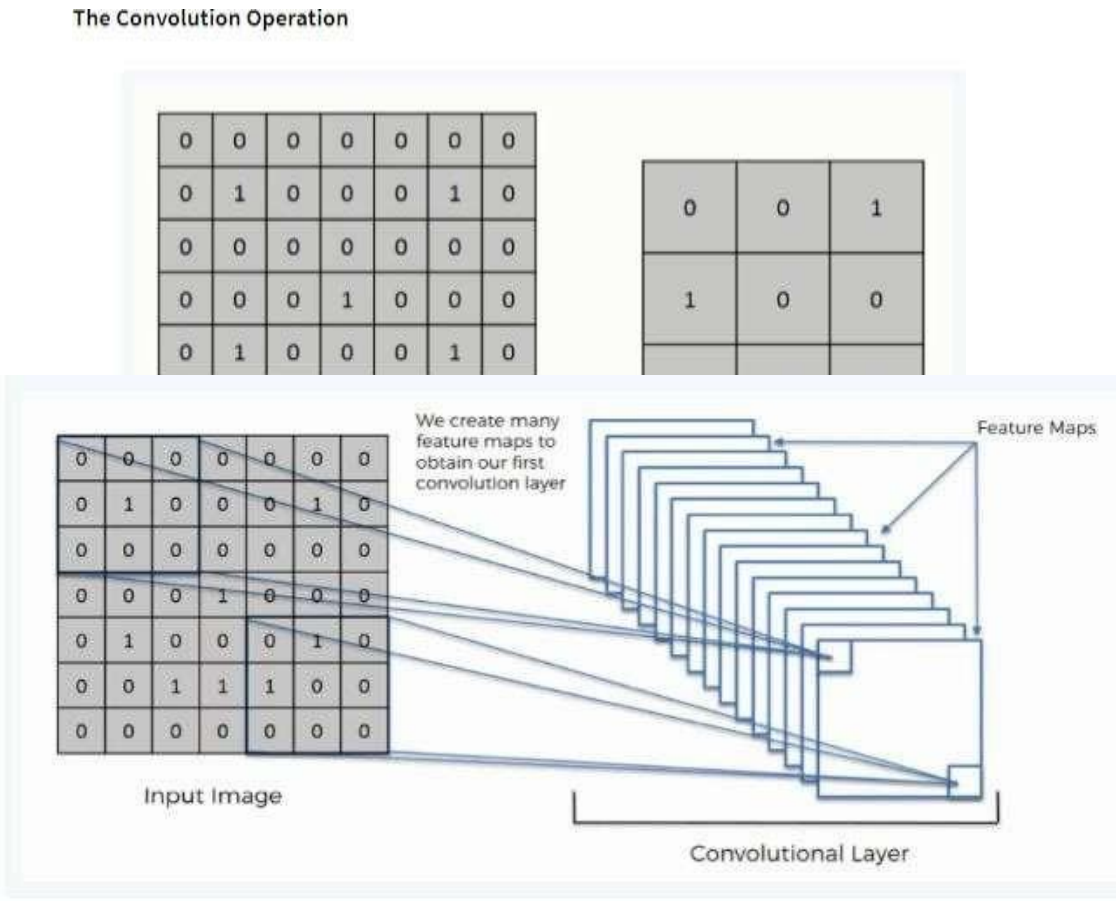


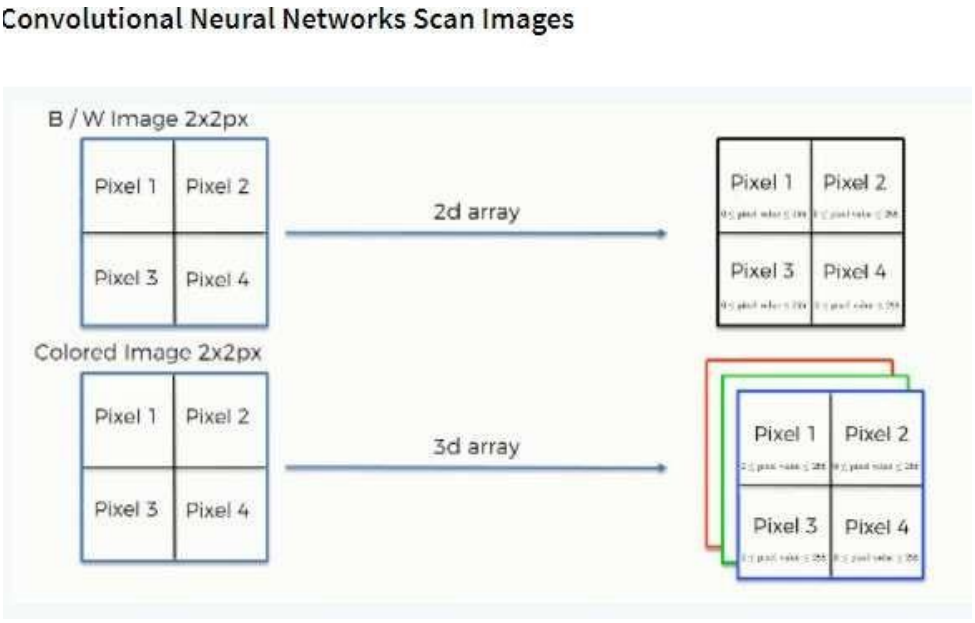
Fig 4.1 Convolution Operation

Step (1b): ReLU Layer

The subsequent part of this stage involves the Rectified Linear Unit, or ReLU. We will discuss ReLU layers and examine how linearity operates within Convolutional Neural Networks.

Not necessary for understanding CNN's, but there's no harm in a quick lesson to improve your skills.

Fig 4.2 Convolutional Neural Networks Scan Images



Step 2: Pooling Layer

In this section, we will delve into pooling, explaining its general operation. Our primary focus here will be on max pooling, though we will also touch upon other methods like mean (or sum) pooling. This part will conclude with an interactive visual demonstration to solidify your understanding of the concept.

Step 3: Flattening

This will be a brief breakdown of the flattening process and how we move from pooled to flattened layers when working with Convolutional Neural Networks.

Step 4: Full Connection

In this concluding part, we will integrate all the concepts discussed throughout this section. By understanding this synthesis, you will gain a comprehensive view of how Convolutional Neural Networks function and how the final "neurons" learn to classify images.

Summary

To conclude, we will summarize the key concepts discussed in this section. For those who would benefit from further learning (which is highly recommended), we encourage you to explore the extra tutorial covering Softmax and Cross-Entropy. While not required for this course, familiarity with these concepts will likely be advantageous when working with Convolutional Neural Networks.

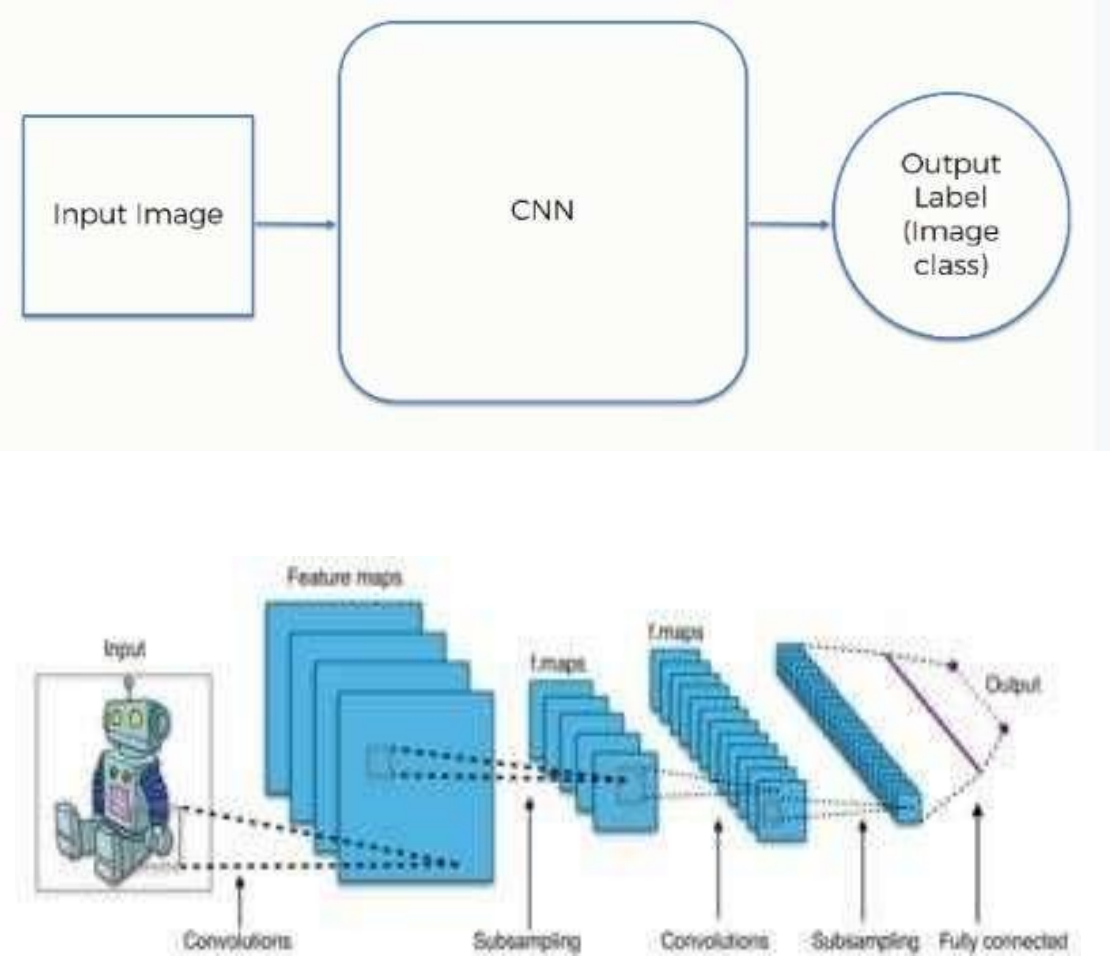


Fig 4.3 CNN Architecture

MobileNet

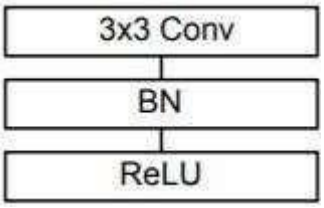
MobileNet is a resource-efficient and adaptable Convolutional Neural Network (CNN) architecture designed for real-world applications. Unlike earlier models, MobileNets primarily employ depthwise separable convolutions instead of standard convolutions to create smaller models. MobileNets also introduce two global hyperparameters – the width multiplier and the resolution multiplier – which enable developers to balance speed and size against latency and accuracy based on their specific needs.

Architecture

MobileNets are built on depth wise separable convolution layers. Each depth wise separable convolution layer consists of a depth wise convolution and a point wise convolution. Counting depth wise and point wise convolutions as separate layers, a MobileNet has 28 layers. A standard MobileNet has 4.2 million parameters which can be further reduced by tuning the width multiplier hyperparameter appropriately.

The size of the input image is 224 × 224 × 3.

A single standard convolution unit (denoted by **Conv** in the table above) looks like this:



5. Testing:

Testing of the "Human Identification Using Iris by CNN" project involves evaluating the performance and accuracy of the developed system. The testing phase typically includes the following steps:

i. Dataset Preparation:

- Collect a diverse dataset of iris images, including images from a significant number of individuals.
- Ensure that the dataset covers a wide range of variations, such as different lighting conditions, occlusions, and image qualities.
- Annotate the dataset with ground truth labels indicating the true identities of the individuals in the images.

ii. Data Split:

- Divide the dataset into training and testing subsets, typically using a predefined ratio (e.g., 80% for training and 20% for testing).
- Ensure that the data split maintains a balanced distribution of individuals across both subsets to avoid biases.

iii. Model Training:

- Design and configure a CNN architecture suitable for iris recognition.
- Initialize the CNN model with random weights and biases.
- Train the model using the training subset of the dataset:
- Input the iris images into the model.
- Compute the loss function (e.g., cross-entropy) by comparing the predicted identities with the ground truth labels.
- Use backpropagation and gradient descent to update the model's weights and biases, optimizing the loss function.
- Repeat the training process for multiple epochs until convergence or predefined stopping criteria.

iv. Model Evaluation:

- Input the iris images from the testing subset into the trained CNN model.
- Obtain the predicted identities for the iris images based on the model's outputs.

- Compare the predicted identities with the ground truth labels to evaluate the model's performance.
- Calculate various evaluation metrics, including:
  - Accuracy: The percentage of correctly identified individuals.
  - Precision: The ability to correctly identify true positives.
  - Recall: The ability to correctly detect all positive instances.
  - F1 score: The harmonic mean of precision and recall.
  - False Acceptance Rate (FAR): The percentage of falsely accepted identities.
  - False Rejection Rate (FRR): The percentage of falsely rejected identities.

v. Performance Analysis:

- Analyze the obtained results to assess the system's performance:
- Identify the accuracy of the predictions and compare it to the baseline or desired performance.
- Examine false positives (incorrectly accepted identities) and false negatives (incorrectly rejected identities) to understand the system's limitations and areas for improvement.
- Evaluate the system's robustness to variations in iris patterns, such as lighting changes or occlusions.
- Consider the computational efficiency of the system, including the processing time required for identification.

vi. Fine-tuning and Optimization:

- If the initial testing reveals performance gaps or limitations, fine-tuning and optimization can be performed:
- Modify the CNN architecture, such as adjusting the number of layers or filters, to enhance performance.
- Augment the training dataset by introducing additional variations or generating synthetic iris images.
- Tune hyperparameters, such as learning rate, batch size, or regularization techniques, to improve the model's generalization capabilities.
- Apply advanced techniques, such as transfer learning or ensemble methods, to leverage pre-trained models or combine multiple models for improved performance.

vii. Iterative Testing:

- Repeat the testing process with the refined system to validate the improvements.
- Conduct multiple iterations of fine-tuning, testing, and analysis until the desired performance is achieved.

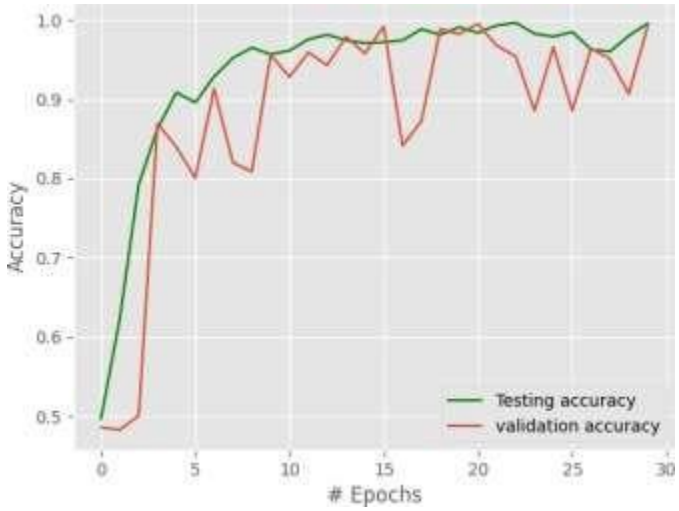


Fig 5.1 Model Accuracy

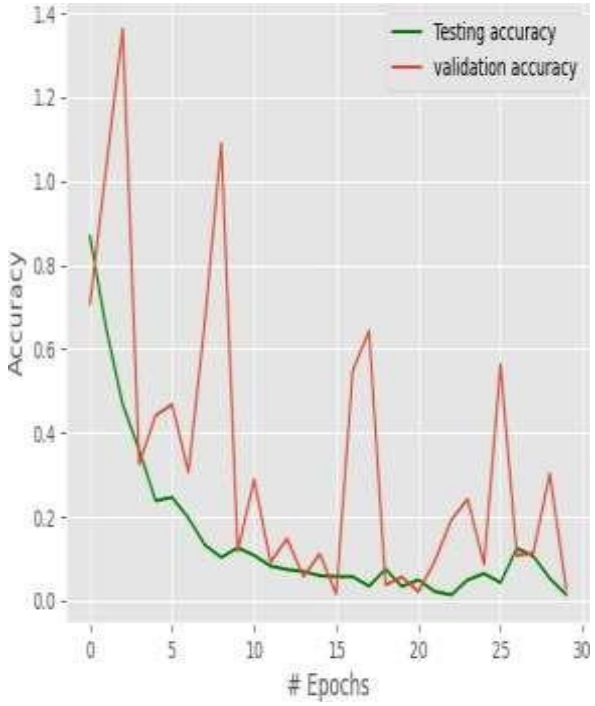


Fig 5.2 Model Loss

6. CONCLUSIONS

This study contributes to the evolving landscape of biometric technology by demonstrating that deep learning approaches can significantly enhance the accuracy, security, and practicality of iris recognition systems, bringing us closer to the goal of universal, secure, and user-friendly biometric authentication.

REFERENCES

[1] https://www.cybintsolutions.com/cyber-security-facts-stats/. Accessed 2 Jan 2021

[2] Sun H-M, Chen Y-H, Lin Y-H (2012) pass: a user authentication protocol resistant to password stealing and password reuse attacks. IEEE Trans Inf Forensics Secur 7(2):651–663

[3] Gupta P, Behera S, Vatsa M, Singh R (2014) On iris spoofing using print attack. In: IEEE 2014 22nd international conference on pattern recognition, Stockholm, Sweden, 24–28 August 2014. https://doi.org/10.1109/ICPR.2014.296

[4] Daugman J (2004) how iris recognition works. IEEE Trans Circuits Syst Video Technol 14(1):21 30

[5] Rana HK, Azam MS, Akhtar MR, Qunin JMW, Moni MA (2019) A fast iris recognition system through optimum feature extraction. PeerJ Comput Sci 5:184

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