International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 2, March - April 2026||

DOI:10.15662/IJRPETM.2026.0902006

Face Recognition using Criminal Identification System

Valepu Nandu Reddy[1], Padala Hema Sunder Rao[2], Nenavath Satnam Singh[3], Vemula Sai Sravanth Kumar[4], Yenumula Bharath Reddy[5], Dr. Prasad Dharnasi[6]

UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science, Telangana, India[1]

UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science, Telangana, India[2]

UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science, Telangana, India[3]

UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science, Telangana, India[4]

UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science, Telangana, India[5]

Professor, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science, Telangana, India[6]

Publication History: Received: 25.02.2026; Revised: 05.03.2026; Accepted: 09.03. 2026; Published: 13.03.2026.

ABSTRACT: India is a populous country, and high crime rates are also increasing because of the population it is difficult to identify the criminals; there are traditional methods to identify the criminals, but those methods are time-consuming and have human error to overcome these problems, the project proposes we use Face Recognition using the Criminals Identification System that detect and identify the criminals without any physical contact

This identification Framework uses upload image or live camera capture to get a face image, then it analyses the face features with the data set and detects the criminals and shows the results. This identification Framework uses OpenCv and a Convolutional Neural Network for facial features to detect and identify the criminals. Tensor Flow uses to build and run machine learning models in the backend, and a Flask web page interface that helps in uploading images and live camera and it helps in showing the results. This identification framework is mainly to overcome human error and speed up investing to maintain law and order

KEYWORDS: Face Recognition, Deep Learning, Convolutional Neural Network CNN), OpenCV, TensorFlow, Computer Vision, Feature Extraction, Image Processing, Haar Cascade Classifier, Flask

I. INTRODUCTION

In today's digital era, we use technology in improving polices and safety. Population became a major problem as the population is increasing, identifying criminals is becoming hard, and maintaining law enforcement is becoming difficult. There are various methods for detecting criminals, but among them face recognition system has become popular because of its fast identification and the ability to operate without physical contact.

In the past, criminal identification relied on eyewitnesses, fingerprints, and some manual checking. These are effective, but it consumed so much time and are prone to human error, like eyewitnesses can forget the face or a fingerprint can be changed or manipulated. Unlike the traditional methods, this face recognition eliminates human error and manual work.

A face recognition system uses face extraction, image processing, and a machine learning algorithm to analyse the data of humans. Every human has different facial features like eyes, nose, lips, and jawline. By extracting these features, it compares with the data set to detect and identify the criminals by using Deep Learning and Convolutional Neural Network for accurate recognition.

Unlike the traditional methods, the system mainly eliminates human error. It can handle large data sets and perform comparisons quickly, then it produces results without error and good accuracy. This uses OpenCV and analyses them through deep learning models built on TensorFlow. The flask-based web application allows seamless interaction and database management, which makes it totally digital.

This face identification system technology is used to maintain law enforcement and detect criminals. Preventing the crime from happening and ensuring the safety of the public, offenders can detect the criminals through cameras in public, and it also speeds up the investigation. This face recognition is considered one of the best approaches to maintaining law and order in society.

II. LITERATURE REVIEW

Turk and Pentland [1] have developed a method called Eigenfaces, which uses Principal Component Analysis (PCA) to simplify face recognition. This method helps compress and simplify high-dimensional facial image data to a low-dimensional space, which is referred to as Eigenfaces. Every face image is boiled down to a linear combination of the Eigenfaces, and recognition happens as a function of the distance between feature vectors. Relevance: This method has become a hallmark of face recognition systems. It is important to note, however, that the Eigenfaces method has low tolerance to the challenges of variability in illumination, pose, and expressions of the face. This is a significant shortcoming when the method is considered for the recognition of criminals in real life situations.

Viola and Jones [2] proposed the Haar Cascade classifier, which is used in real-time face detection. It uses Haar-like features and a cascade of classifiers trained with AdaBoost to detect faces. Relevance: Because of its quick processing, Haar Cascade is one of the most frequently used classifiers in face detection. Relevance: This method is used for face detection before we use deep learning-based recognition. However, it is important to note that this method has a high probability of failing in situations of low illumination and performs poorly in profiles.

With the development of deep learning, Taigman atal. [3] proposed the DeepFace that uses a Convolutional Neural Network (CNN) to identify the face at the human level. This shows deep learning effectively in facial recognition

Schroff et al. [4] introduced FaceNet, which is a deep CNN model that uses triplet loss to learn a mapping of facial images into a compact embedding space. With this embedding space, face verification and identification can be performed. Accurate results can be achieved with the use of distance metrics, such as cosine distance. Relevance: For our project, we will be using FaceNet with the Deep Face framework to create embeddings and compare faces for the identification of criminals. FaceNet is known for its reliability and accuracy.

Parkhi et al. [5] presented VGG Face, which is a deep CNN architecture that has been trained on a very large dataset, built for the purpose of face recognition. With this deep CNN architecture, face recognition becomes much more accurate because now it is able to extract more discriminative features. Relevance: Here, this framework serves to show the way in which deep CNN architectures enhance the results of facial recognition, thereby justifying the use of CNN in our project.

Zhang et al. [6] proposed for the first time Multi-task Cascaded Convolutional Networks (MTCNN) for the purpose of face detection and face alignment. Her approach improves detection accuracy, as detection and alignment are achieved simultaneously. Relevance: MTCNN improves face detection, producing better results than before. It generates better input for the recognition systems.

Deng et al. [7] Proposed Arc Face, a deep learning-based face recognition model that uses additive angular margin loss for better discriminatory ability. Relevance: Arc Face has better recognition accuracy, and it shows the necessity for an advanced CNN architecture in facial recognition.

Insight Face [8] proposed Retina Face, a deep learning-based face detection model that can detect faces accurately in difficult situations such as blur and low resolution. Relevance: Retina Face increases detection performance in real life situations like CCTV surveillance, which matters for a crime detection system.

III. RESEARCH METHODOLOGY

The Criminal Face Identification System runs on a deep learning Convolutional Neural Network (CNN) and connects everything through a web app.

A. Dataset Collection

First, you need a good set of facial images. Each person gets their own folder, so the model knows whose face is whose. The dataset has all sorts of images-different expressions, lighting, angles. This helps the system handle real-world situations and makes it more reliable.

B. Input Image Acquisition

There are two ways to get images into the system:

1. **Image Upload:** In this we can upload image in frontend then it detect weather the person is criminal or not
2. **Live Camera Capture:** In this identification system the live camera uses the camera to detect and identify the human face by using CNN and deep leaning

C. Image Preprocessing

Before the CNN sees anything, the system cleans up the image:

1. **Face Detection:**
OpenCV's Haar Cascade Classifier finds where the face is.
2. **Face Cropping:**
It crops out extra background, keeping only the face.
3. **Image Resizing:**
Then, it resizes the image to fit the CNN's requirements.
4. **Normalization:**
Finally, it normalizes pixel values. This step boosts both accuracy and speed.

D. CNN Feature Extraction

The system uses a CNN-based FaceNet model. It pulls out the important stuff—like eyes, nose, mouth, and overall facial shape. Then it turns the face into a series of numbers called an embedding. This embedding is unique for each person.

E. Face Matching and Identification

The Identification system compares the face with the dataset and identifies weather the person is a criminal or not, then it generates the results

F. Result Display

Once it matches the face, it shows results

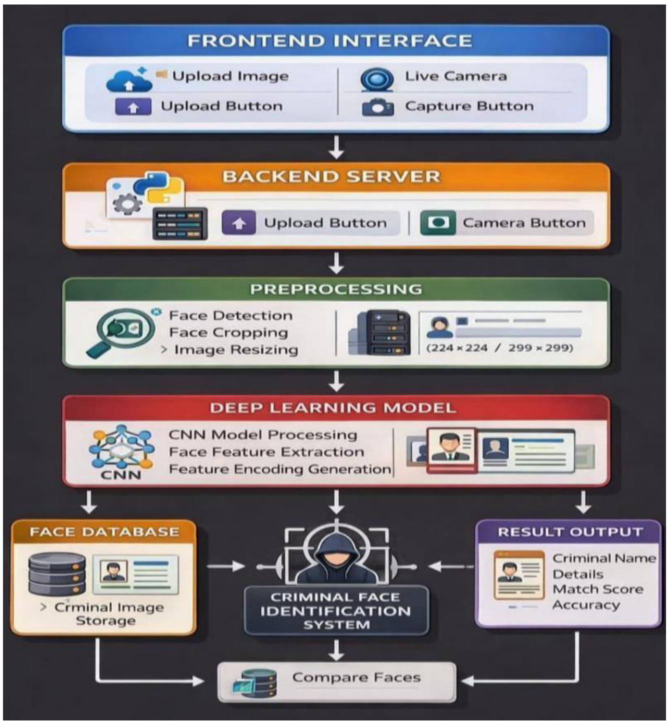
- Name
- Age
- Crime
- Location
- Match score

G. Web Application Implementation

Frontend: In this frontend user can upload the image or capture the image, and also in this frontend, it shows the results
Backend: In this backend, the image sent from the frontend is handled, processed, and predicted with the CNN

H. System Workflow

In this Face Recognition Identification System, we can upload image or use live camera to detect face then it crops the face, preprocess the image, extract features with the CNN, march the face and show the results



IV. KEY FINDINGS

1. Accurate Criminal Face Identification:
This Identification system identifies the criminal's face in both uploads images and live camera. The deep learning and CNN models extract face features and compare them with the data set, and provide results.

2. Real-Time Detection Capability:
This Face Recognition Identification System is capable of identifying criminals in the real world to maintain law and order.

3. CNN Feature Extraction:
This Convolutional Neural Network uses data set to learn the features of a human face. Every individual has different feature this CNN learns feature and uses them to detect and identify the criminals.

4. Frontened and Backend:
It has a Frontend that contains an image upload and live camera, and a Backend that has deep learning models that process the data to identify the criminals. It shows the criminal’s details as results.

5. Security Application:

- It can be used police investigation
- Airport security
- Crime prevention
- Surveillance system

V. WORKFLOW

1. Input Image:
It has a home, then click on the detection. The Identification first captures the images of a human in the uploaded image or live camera. Then it is sent to the backend to process.

2. Face Detection:
This identification system uses OpenCV to detect a human face. It mainly focuses on the structure region, it removes unnecessary background, and starts to detect.

3. Image Processing:
After detecting, the image processing is performed to identify the criminals. This process has face cropping, which extracts the face region, then Image Resizer for resizing the image to standard, and at last Normalization, which scales the pixel value to be between 0 and 1.

4. Feature Extraction:
To identify, then given to a Convolutional Neural Network (CNN), which performs automatic feature extraction, identifies the facial features, and generates the face feature vectors.

5. Face Matching:
These extracted features are compared with the data set to identify the criminals. It calculates the similarity features, detects and identifies the match, and determines whether the person is a criminal or not.

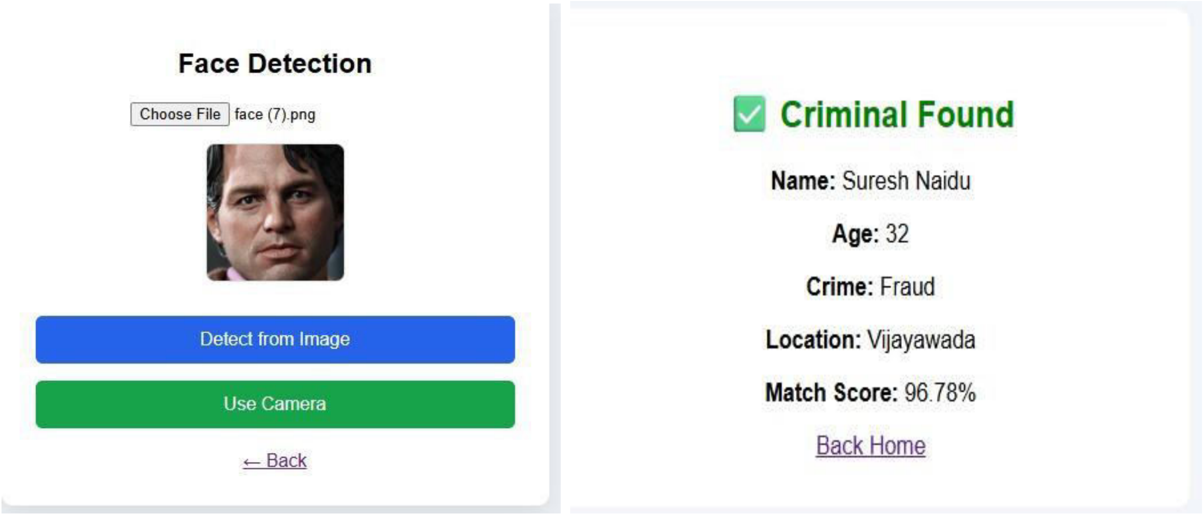
6. Results Generation and Results Display:
After detecting the criminal, it generates the results to show in the frontend.

- Name
- Age
- Crime
- Location
- Match score

VI. RESULTS AND DISCUSSION

This Face Recognition Identification System is detecting and identifying the criminal by using deep learning and a Convolutional Neural Network (CNN). This identification system is capable of detecting the criminal in both Image upload and Live camera. This system detects faces using the Haar Cascade algorithm, then it extracts facial features by using a CNN model. After extracting, it compares with the data set and detect whether the person is a criminal or not. Finally, the result is displayed in the frontend.

Upload image screenshot:



✅ Criminal Found

Name: Suresh Naidu

Age: 32

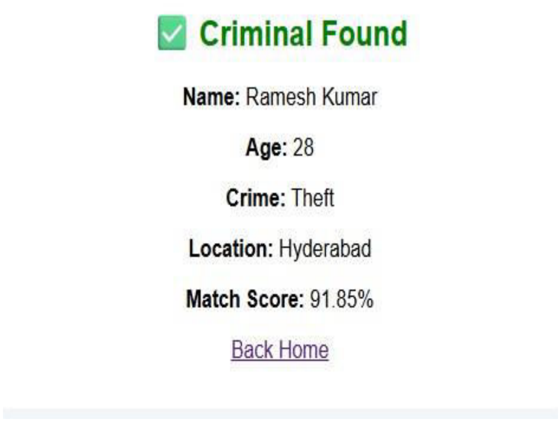
Crime: Fraud

Location: Vijayawada

Match Score: 96.78%

Back Home

Live camera:



☑ Criminal Found

Name: Ramesh Kumar

Age: 28

Crime: Theft

Location: Hyderabad

Match Score: 91.85%

This result confirms that both the upload image and live camera effectively identify criminals overall; this identification is used in real-time criminal surveillance for smart and secure.

VII. CONCLUSION

In this populated country, identifying criminals is difficult and remembering each person is also hard, so we use this framework for detecting and identifying the criminals. In this identification framework, we can upload an image or a live camera for detecting the person, which uses deep learning and CNN for identifying the person through facial features. This framework mainly reduces the manual work increase the speed of investing. This framework is implemented to ensure the safety and protect the law and order

VIII. FUTURE WORK

There are several areas where this system can be further improved

1.Real-Time CCTV Integration:

This identification system is integrated with a real-time surveillance system to monitor and detect criminals in public areas, airports, banks, and shopping malls. This will work without any manual intervention.

2. Advanced Face Recognition Models:

This identification system can be developed by using advanced deep learning models such as Arc Face, Deep Face, and improved versions of FaceNet.

3. Mobile and Edge Device Deployment:

This identification system can be deployed in mobile devices, so we can detect the criminals anywhere using technologies like TensorFlow or OpenCV.

4. Automated Alert and Notification System:

We can add an alert system where when a criminal is detected and identified. It will send a notification, then rescue can be reached fast.

REFERENCES

1. Chinthala, S., Erla, P. K., Dongari, A., Bantu, A., Chityala, S. G., & Saravanan, M. S. (2026). Food recognition and calorie estimation using machine learning. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(2), 480–488.

2. Gopinathan, V. R. (2025). Designing Cloud-Native Enterprise Systems by Modernizing Applications with Microservices and Kubernetes Platforms. International Journal of Research and Applied Innovations, 8(5), 13052-13063.

3. Nagarajan, C., Neelakrishnan, G., Janani, R., Maithili, S., & Ramya, G. (2022). Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay. Asian Journal of Electrical Sciences, 11(1), 1-8.

4. Amitha, K., Ram Manohar Reddy, M., Yashwanth, K., Shylaja, K., Rahul Reddy, M., Srinu, B., & Dharnasi, P. (2026). AI empowered security monitoring system with the help of deployed ML models. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(1), 69–73.

5. Gogada, S., Gopichand, K., Reddy, K. C., Keerthana, G., Nithish Kumar, M., Shivalingam, N., & Dharnasi, P. (2026). Cloud computing/deep learning customer churn prediction for SaaS platforms. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(1), 74–78.

6. Akula, A., Budha, G., Bingi, G., Chanda, U., Borra, A. R., Yadav, D. B., & Saravanan, M. (2026). Emotion recognition from facial expressions using CNNs. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(1), 120–125.

7. Varshini, M., Chandrapathi, M., Manirekha, G., Balaraju, M., Afraz, M., Sarvanan, M., & Dharnasi, P. (2026). ATM access using card scanner and face recognition with AIML. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(1), 113–118.

8. Feroz, A., Pranay, D., Srikar Sai Raj, B., Harsha Vardhan, C., Rohith Raja, B., Nirmala, B., & Dharnasi, P. (2026). Blockchain and machine learning combined secured voting system. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(1), 119–124.

9. Tirupalli, S. R., Munduri, S. K., Sangaraju, V., Yeruva, S. D., Saravanan, M., & Dharnasi, P. (2026). Blockchain integration with cloud storage for secure and transparent file management. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(1), 79–86.

10. Chandu, S., Goutham, T., Badrinath, P., Prashanth Reddy, V., Yadav, D. B., & Dharnas, P. (2026). Biometric authentication using IoT devices powered by deep learning and encrypted verification. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(1), 87–92.

11. Singh, K., Amrutha Varshini, G., Karthikeya, M., Manideep, G., Sarvanan, M., & Dharnasi, P. (2026). Automatic brand logo detection using deep learning. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(1), 126–130.

12. Keerthana, L. M., Mounika, G., Abhinaya, K., Zakeer, M., Chowdary, K. M., Bhagyaraj, K., & Prasad, D. (2026). Floods and landslide prediction using machine learning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(1), 125–129.

13. Dadigari, M., Appikatla, S., Gandhala, Y., Bollu, S., Macha, K., & Saravanan, M. (2026). Bitcoin price prediction with ML through blockchain technology. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(1), 130–136.

14. Chinthamalla, N., Anumula, G., Banja, N., Chelluboina, L., Dangeti, S., Jitendra, A., & Saravanan, M. (2026). IoT-based vehicle tracking with accident alert system. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 486–494.

15. Hu, C., Deng, Y., Min, G., Huang, P., & Qin, X. (2018). QoS promotion in energy-efficient datacenters through peak load scheduling. IEEE Transactions on Cloud Computing, 9(2), 777-792.

16. Nagamani, K., Laxmikala, K., Sreeram, K., Eshwar, K., Jitendra, A., & Dharnasi, P. (2026). Disaster management and earthquake prediction system using machine learning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 495–499.

17. Devarajan, R., Prabakaran, N., Vinod Kumar, D., Umasankar, P., Venkatesh, R., & Shyamalagowri, M. (2023, August). IoT Based Under Ground Cable Fault Detection with Cloud Storage. In 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1580-1583). IEEE.

18. Prasad, E. D., Sahithi, B., Jyoshnavi, C., Swathi, D., Arun Kumar, T., Dharnasi, P., & Saravanan, M. (2026). A technology driven – solution for food and hunger management. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 440–448.

19. Anitha, K., Vijayakumar, R., Jeslin, J. G., Elangovan, K., Jagadeeswaran, M., & Srinivasan, C. (2024, March). Marine Propulsion Health Monitoring: Integrating Neural Networks and IoT Sensor Fusion in Predictive Maintenance. In 2024 2nd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT) (pp. 1-6). IEEE.

20. Rakesh, V., Vinay Kumar, M., Bharath Patel, P., Varun Raj, B., Saravanan, M., & Dharnasi, P. (2026). IoT-based gas leakage detector with SMS alert. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 449–456.

21. S. Vishwarup et al., "Automatic Person Count Indication System using IoT in a Hotel Infrastructure," 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2020, pp. 1-4, doi: 10.1109/ICCCI48352.2020.9104195

22. Chanamalla, B., Murali, V. N., Suresh, B., Deepak, M. S., Zakriya, M., Yadav, D. B., & Saravanan, M. (2026). AI-driven multi-agent shopping system through e-commerce system. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 463–470.

23. Nandhini, T., Babu, M. R., Natarajan, B., Subramaniam, K., & Prasanna, D. (2024). A NOVEL HYBRID ALGORITHM COMBINING NEURAL NETWORKS AND GENETIC PROGRAMMING FOR CLOUD RESOURCE MANAGEMENT. Frontiers in Health Informatics, 13(8).

24. Bhagyasri, Y., Bhargavi, P., Akshaya, T., Pavansai, S., Dharnasi, P., & Jitendra, A. (2026). IoT based security & smart home intrusion prevention system. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 457–462.

25. Ananth, S., & Saranya, A. (2016, January). Reliability enhancement for cloud services-a survey. In 2016 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-7). IEEE.

26. Thotla, S. B., Vyshnavi, S., Anusha, P., Vinisha, R., Mahesh, S., Yadav, D. B., & Dharnasi, P. (2026). Traffic congestion prediction using real time data by using deep learning techniques. , 8(2), 489–494.

27. Poornima, G., & Anand, L. (2024, April). Effective strategies and techniques used for pulmonary carcinoma survival analysis. In 2024 1st International Conference on Trends in Engineering Systems and Technologies (ICTEST) (pp. 1-6). IEEE.

28. S. Roy and S. Saravana Kumar, "Feature Construction Through Inductive Transfer Learning in Computer Vision," in Cybernetics, Cognition and Machine Learning Applications: Proceedings of ICCCMLA 2020, Springer, 2021, pp. 95–107.

29. Rupika, M., Nandini, G., Mythri, M., Vasu, K., Abhiram, M., Shivalingam, N., & Dharnasi, P. (2026). Electronic gadget addiction prediction using machine learning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 500–505.

30. Vimal Raja, G. (2025). Context-Aware Demand Forecasting in Grocery Retail Using Generative AI: A Multivariate Approach Incorporating Weather, Local Events, and Consumer Behaviour. International Journal of Innovative Research in Science Engineering and Technology (Ijirset), 14(1), 743-746.

31. Akshaya, N., Balaji, Y., Chennarao, J., Sathwik, P., & Dharnasi, P. (2026). Diabetic retinopathy diagnosis with deep learning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 506–512.