



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Criminal Identification Using Face Detection

¹DR. ANTO FRANCIS CHERUSSERY, ²AGNAY BABU PG, ³AJAY KV, ⁴SREERAM P

¹Professor, ²Student, ³Student, ⁴Student ¹Department Of Mechatronics Engineering ,

¹Nehru College Of Engineering And Research centre, Thrissur, India

Abstract: Criminal identification is a critical aspect of law enforcement, where rapid and accurate identification of individuals can significantly aid in solving crimes and enhancing public safety. Facial recognition technology (FRT) has emerged as a powerful tool in this domain due to its ability to process and match facial images with high speed and precision. This paper explores the implementation of a criminal identification system using facial recognition on a **Raspberry Pi 5**, leveraging its improved processing power, expanded memory, and efficient machine learning capabilities. By utilizing compact, low-cost, and portable hardware, such as the Raspberry Pi 5, this system is capable of capturing and analyzing facial data in real-time and in challenging environments. The system employs machine learning algorithms, particularly convolutional neural networks (CNNs), to analyze and match facial features against a database of known offenders. Key challenges addressed include optimizing model performance on resource-constrained hardware, ensuring data security, and mitigating biases in recognition accuracy. This study evaluates the model's accuracy, real-time processing speed, and practical field applications, highlighting how low-cost hardware solutions like the Raspberry Pi 5 make facial recognition accessible for broader, ethical applications in law enforcement. Results demonstrate that with careful implementation, this technology can enhance law enforcement capabilities while respecting privacy and ethical standards. The system's performance is evaluated on key metrics such as accuracy, processing time, and robustness in various lighting and environmental conditions. Additionally, ethical considerations are discussed, including privacy protection, data security, and measures to prevent misuse of facial recognition technology.

Index Terms – Face Recognition, Haar Cascade Algorithm, OpenCV, Python Programming

I. INTRODUCTION

This introduction outlines a real-time facial recognition system developed specifically to assist law enforcement in quickly identifying and verifying individuals. The system combines advanced surveillance cameras with facial recognition software that utilizes Haar-like classifiers a popular algorithm in the OpenCV library, which is known for its ability to efficiently detect facial features by analyzing patterns of light and dark areas in an image. This choice of algorithm allows the system to detect multiple faces at once, even in busy, crowded environments like train stations, airports, or public events. When the system captures an image of a person, it immediately compares it with entries in an established database, which could include records tied to government identification systems like Aadhaar IDs or passport databases. This automated matching process allows law enforcement to confirm identities in real-time, providing officers with critical information on suspects, missing persons, or individuals on watch lists. By accessing personal information in real-time, this system enhances both the speed and accuracy of investigations, making it possible to identify individuals swiftly and, if necessary, take action immediately. This technology offers a dual advantage: it not only supports law enforcement in crime prevention and suspect identification but also assists in situations like verifying identities at checkpoints or entrances. Its capability to detect multiple faces at once boosts efficiency in high-traffic areas, enabling law enforcement to operate more effectively without needing extensive human oversight.

II. LITERATURE SURVEY

A. Criminal Face Recognition using Raspberry Pi

This study presents a real-time face recognition system using Raspberry Pi and OpenCV. It employs Haar-classifier for face detection and compares real-time images with a pre-trained database. The system is designed for automated surveillance and can recognize multiple faces

B. Real-Time Criminal Detecting System Using Raspberry Pi

This paper discusses a system that detects criminals in public places by matching captured images with a database of known offenders. It uses image processing techniques and sends alerts to authorities if a match is found

C. Facial and Fingerprint Recognition-Based Door Lock System Using Raspberry Pi

Although focused on security systems, this research integrates facial and fingerprint recognition for identification. It uses a HOG classifier and Raspberry Pi to compare detected faces with a trained dataset

D. IoT-Based Surveillance System

This study explores the use of Raspberry Pi in IoT-enabled surveillance systems for criminal identification. It highlights the integration of facial recognition with IoT devices for real-time monitoring and alerts.

E. Biometric Authentication for Criminal Identification

This research combines biometric techniques like facial and fingerprint recognition with Raspberry Pi to enhance criminal identification systems. It emphasizes accuracy and reliability in identifying individuals.

III. METHODOLOGY

The system's methodology adopts a well-organized framework that combines hardware, software, and optimization strategies for immediate criminal identification. At its core, the hardware setup features a Raspberry Pi 5, complemented by a Raspberry Pi camera for capturing images, a microSD card for storing data, and a cooling system to ensure optimal performance. On the software side, development leverages OpenCV and Python, employing Haar Cascade classifiers and HOG methods for detecting faces, extracting features, and matching with the database. When a match is identified, a notification is sent through Telegram to alert law enforcement. The testing and optimization stage focuses on ensuring both accuracy and efficiency by training the system with a variety of datasets, assessing its performance in different environmental settings, and enhancing its ability to detect multiple individuals. Ongoing improvements are implemented to boost real-time processing, accuracy, and overall system reliability across various scenarios.

A. System Design

The system is built for immediate criminal identification through facial recognition technology. It combines hardware elements with software algorithms to identify and compare faces with a pre-existing database. The process is methodical, encompassing hardware integration, software creation, and thorough testing and optimization.

B. Hardware Integration

The system's hardware integration revolves around the Raspberry Pi 5, which acts as the main processing unit for real-time facial detection and recognition. A Raspberry Pi camera is utilized to capture facial images, which are subsequently analyzed for identification purposes. The system relies on a microSD card to store trained datasets and software, facilitating smooth operation. To ensure optimal performance, heat sinks and a compact DC fan are included to prevent overheating during demanding computations. A power adapter guarantees a stable power supply for uninterrupted functionality. Additional components, such as an HDMI to micro HDMI cable, allow for video output, while a transparent acrylic case safeguards the hardware setup. The camera is securely mounted on a stand to ensure stability for precise image capture. This integration promotes efficient data processing, seamless face recognition, and real-time alert notifications.

C. Software Development

The system's software development leverages OpenCV and Python, incorporating machine learning algorithms for real-time face detection and recognition. It starts with detecting faces using Haar Cascade classifiers and HOG (Histogram of Oriented Gradients) methods to pinpoint faces in the images captured. After detection, the system extracts essential facial features like the distance between eyes, width of the nose, and shape of the jawline to create a unique faceprint. This faceprint is then matched against a pre-existing criminal database to find any potential matches. If a match is identified, the system sends an alert through Telegram to notify law enforcement. The software is built to support the detection of multiple individuals and is continually refined for improved accuracy, speed, and real-time processing, even in varying conditions such as changes in lighting and environmental factors.

D. Testing & Optimization

The testing and optimization stage is crucial for ensuring the system's precision, effectiveness, and dependability in identifying criminals in real-time. During this phase, the system is trained on various datasets, allowing facial recognition models to be evaluated with a wide range of data to boost accuracy and minimize false positives and negatives. Performance assessments are carried out under various lighting conditions, age differences, and weather influences to strengthen the system's resilience. Optimization strategies involve fine-tuning algorithms for quicker face detection, managing databases efficiently for rapid access, and reducing processing delays. Furthermore, enhancements are being made to multi-person detection features, and the reliability of real-time alerts through Telegram is being tested. Ongoing improvements guarantee that the system functions smoothly, delivering high levels of accuracy and efficiency across different settings.

SYSTEM DESIGN & COMPONENTS

E. System Design

The system is designed for real-time criminal identification using advanced facial detection and recognition technology. It operates on a Raspberry Pi 5, paired with a Raspberry Pi camera that captures live images and video feeds. When an image is taken, the system applies the Haar Cascade Classifier, a pre-trained face detection algorithm from OpenCV, to locate faces in the captured frame. Once a face is detected, it uses the Histogram of Oriented Gradients (HOG) to extract unique facial features, such as the distance between the eyes, the width of the nose, and the contour of the jawline. These features are then converted into a faceprint, which mathematically represents the individual's facial traits. This faceprint is compared against a criminal database to check for any matches. If a match is found, the system quickly sends an alert via Telegram to the appropriate authorities, enabling a rapid response and verification process. This alert system is a cost-effective alternative to traditional SIM-based notification methods. Additionally, the system is designed to improve its accuracy over time by updating its facial database with new information and refining its recognition algorithms. Future enhancements will focus on overcoming challenges like varying lighting conditions, the effects of aging, and improving the overall quality of the database to ensure greater reliability.

F. Components

a. RASPBERRY PI 5

The Raspberry Pi 5 is the latest iteration of the Raspberry Pi computer, delivering significantly enhanced performance and exciting new features. It boasts a quad-core processor that provides improved speed and efficiency, making it ideal for applications such as AI, machine learning, and video editing. This model supports dual 4K displays, offers quicker storage options with PCIe compatibility, and can be equipped with up to 8GB of RAM. Additionally, it features upgraded USB 3.0, faster Wi-Fi, and Gigabit Ethernet for superior connectivity.



FIG 1:- Raspberry Pi 5

b. *RASPBERRY PI CAMERA*

The Raspberry Pi camera is a handy accessory designed for Raspberry Pi boards, allowing users to capture photos and videos. It is available in various models, including a standard version and a high-quality option for enhanced image clarity. Connecting the camera to the Pi is a breeze, thanks to a dedicated camera port. (5MP 1080p resolution)



FIG 2:- RASPBERRY PI CAMERA

c. *RASPBERRY PI CAMERA CABLE*

This Raspberry Pi camera cable is designed to work seamlessly with your Pi 5. Just plug the 22-pin 0.5mm end into your Pi's camera port, and connect the 15-pin 1mm end to any official Raspberry Pi camera.



FIG 3:- RASPBERRY PI CAMERA CABLE

HDMI TO MICRO HDMI CABLE

Micro HDMI cables offer the same capabilities as Mini HDMI cables but feature a more compact pin design. This type of connector is often found in smartphones, compact cameras, and various portable gadgets.

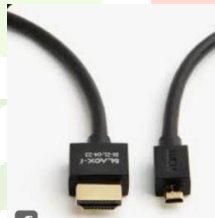


FIG 4:- HDMI TO MICRO HDMI CABLE

d. *HEAT SINKS*

Heat sinks play a crucial role in managing the temperature of devices that produce heat, including both electronic and mechanical equipment. Their primary function is to prevent overheating and enhance overall efficiency, with the ability to withstand temperatures of up to 70-80°C.

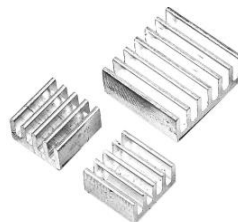


FIG 5:- HEAT SINKS

e. *SMALL DC FAN*

The DC 5V 0.2A Cooling Fan for Raspberry Pi is a compact yet efficient fan. It serves as an exhaust fan for the Raspberry Pi case, helping to regulate the temperature of the extruder. This ensures effective heat

dissipation and enhances overall performance.



FIG 6:- SMALL DC FAN

f. *MICRO SD*

A microSD card is a tiny, portable storage solution commonly found in various electronic devices like smartphones, cameras, and Raspberry Pi computers. This type of flash memory card is designed to hold data, including photos, videos, applications, and files. MicroSD cards are available in a range of storage capacities, usually from 2GB up to 1TB, and are appreciated for their small size.



FIG 7:- MICRO SD

POWER SOURCE ADAPTER

A power source adapter is a gadget that changes electrical energy from a wall outlet into a format suitable for electronic devices. It usually converts AC (Alternating Current) from the outlet into DC (Direct Current), which is what most electronics need. Commonly used for charging smartphones and tablets, these adapters provide a USB-compatible DC output of 5V at 2A.



FIG 8:- POWER SOURCE ADAPTER

g. *TRANSPARENT ACRYLIC CASE FOR RASPBERRY PI 5*

Raspberry Pi 5 cases provide easy access to all ports, including the micro HDMI, USB, Ethernet ports, USB-C power connector, and micro SD card slot.



FIG 9:- TRANSPARENT ACRYLIC CASE FOR RASPBERRY PI 5

IV. WORKING PRINCIPLE

This system is a cutting-edge tool designed for real-time criminal identification, leveraging face detection and recognition technologies to support law enforcement efforts. It operates by capturing live images or video streams using a Raspberry Pi camera, which is the main imaging device. The visual data collected is then enhanced through pre-processing to boost clarity and precision by adjusting factors like contrast, brightness, and noise levels. Given that elements such as lighting, facial angles, and obstructions can affect recognition accuracy, this pre-processing phase is crucial for optimizing the image before proceeding. The Raspberry Pi 5 serves as the central processing unit, efficiently managing the computational tasks required for face detection and recognition.

After the image has been pre-processed, the system utilizes the Haar Cascade Classifier for face detection, which is a popular machine learning technique available in OpenCV. This algorithm identifies human faces by recognizing patterns in grayscale images through Haar-like features, focusing on the contrast variations between different facial areas, such as the eyes, nose, and mouth. If there are multiple faces in the frame, the system can detect and separate each one individually. Once a face is detected, the next phase is feature extraction, where the system examines and encodes the facial structure into a unique faceprint using the Histogram of Oriented Gradients (HOG) method. This technique captures crucial details like edge orientations, facial geometry, and significant landmarks, transforming them into a mathematical format that differentiates one person from another.

The captured faceprint is then matched against a criminal database that holds facial data of known offenders. The system conducts a one-to-many comparison, looking for similarities between the captured faceprint and those stored in the database. If a match is identified, an automated alert is sent out via the Telegram API, informing law enforcement with the suspect's information. This real-time alert system enables officers to respond quickly, thereby enhancing response times and bolstering security measures. Telegram serves as a budget-friendly alternative to traditional SMS or SIM-based alert systems, helping to lower operational costs while ensuring effectiveness. Before any legal actions are taken, authorities perform a manual check to verify the system's accuracy and avoid any wrongful accusations. If no match is found, the system either discards the detected face or keeps it temporarily for future use.

The system is built to learn and enhance its capabilities continuously by incorporating new facial data into its database, which makes it increasingly intelligent and efficient over time. However, there are challenges that can affect its performance, including changes due to aging, different facial expressions, disguises, and varying environmental conditions. To address these challenges, future upgrades will focus on integrating multi-person detection and implementing more sophisticated deep learning models to boost accuracy. In the end, the “God’s Eye” system offers a powerful and innovative approach to criminal identification, enabling law enforcement to identify suspects swiftly, accurately, and affordably, thus enhancing public safety and aiding in crime prevention.

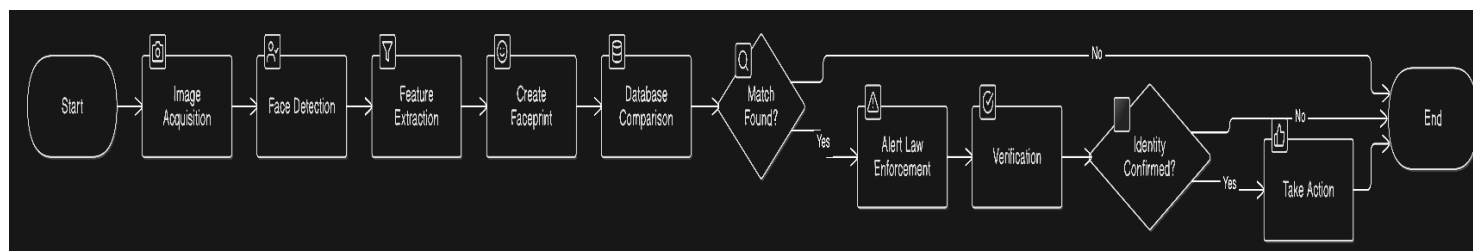


FIG 10:-WORKING PRINCIPLE DIAGRAM

V. EXPERIMENTAL SETUP AND TESTING

The system requires a well-planned experimental setup that includes putting together the essential hardware, setting up the software environment, and performing thorough tests to measure its performance in real-life scenarios. The goal is to evaluate how accurately the system can detect and recognize faces, how efficiently it can notify law enforcement, and how well it operates in different environmental conditions. This testing phase

is vital to confirm that the system works reliably and effectively for identifying criminals.

The hardware configuration features a Raspberry Pi 5 as the main processing unit, tasked with running face detection and recognition algorithms. To capture real-time images and video, a Raspberry Pi Camera is utilized, providing the necessary input for the system. The camera is securely mounted on a stand to maintain stability and optimize the angle for facial image capture. A MicroSD card is inserted into the Raspberry Pi to hold the operating system, software libraries, and a pre-trained criminal database. To avoid overheating during extended use, heat sinks and a DC cooling fan are incorporated into the setup. The system is powered by a 5V power adapter, ensuring a reliable energy source. Furthermore, the entire assembly is housed in a transparent acrylic case, which offers protection while allowing easy access to ports and components.

The Raspberry Pi is set up with Raspberry Pi OS and primarily uses Python for developing face detection and recognition algorithms. It utilizes OpenCV, a popular open-source computer vision library, which includes the Haar Cascade Classifier for detecting faces. To extract features, the system employs the Histogram of Oriented Gradients (HOG) method, transforming facial images into a distinct mathematical form called a faceprint. This faceprint is then compared to a database of known criminals to find potential matches. For instant notifications, the system integrates the Telegram API, enabling law enforcement to receive immediate alerts when a suspect is recognized. Additionally, the database is regularly updated to enhance identification accuracy over time.

The testing phase for the "God's Eye" system is essential to confirm its precision, dependability, and effectiveness in practical situations. The system is subjected to various test cases across different environmental and operational settings to assess its performance. The main goal of this testing process is to measure the accuracy of face detection, the effectiveness of face recognition, the ability to process information in real-time, and the functionality of the alert system. Given that the system is intended for law enforcement and security purposes, it is crucial that it operates effectively in fast-paced and unpredictable environments.

Initially, a face detection accuracy test is performed to evaluate how well the system can identify human faces across various environments. The Raspberry Pi camera is set up at different distances, while subjects are placed in diverse lighting scenarios, including bright sunlight, dim indoor light, and near-dark conditions. The system is also challenged with partially obstructed faces, where individuals wear sunglasses, face masks, hats, or scarves, to see if the algorithm can still recognize facial features. The findings show that face detection is most effective in well-lit situations but has difficulty in low-light settings, indicating a need for enhancements like infrared (IR) cameras to improve night vision capabilities.

The last stage of testing focuses on a prolonged evaluation of the system, where it is set up in a monitored environment for multiple days. This phase aims to uncover any potential problems, including false positives, system failures, or overheating of hardware components. The heat sinks and DC cooling fan effectively manage thermal levels, allowing for uninterrupted operation. Nonetheless, the quality and size of the database play a crucial role in the system's efficiency, as larger datasets lead to increased processing times. Looking ahead, enhancements will involve refining database indexing and adopting AI-driven filtering methods to boost performance while maintaining accuracy.

One important element of testing is the functionality of the alert system, which includes the integration of the Telegram API for real-time notifications. The system is designed to automatically send an alert whenever a positive match is found. During the testing phase, law enforcement officers receive immediate Telegram notifications that include the suspect's image and relevant database details. The system's performance is assessed by measuring the time taken from detection to alert issuance, aiming for an average response time of less than 5 seconds. This Telegram-based notification system is not only efficient but also cost-effective, removing the need for pricey SIM-based or traditional SMS alerts. Additionally, the test checks the reliability of network connectivity, ensuring that alerts are delivered successfully even in low-bandwidth situations.

In the test for real-time detection and response, the system is assessed for its speed and effectiveness while operating in live video surveillance mode. The Raspberry Pi camera continuously monitors and identifies faces in dynamic settings, like busy public areas or moving crowds. The system's response time is evaluated by measuring how fast it can process a face, extract its features, compare them with the database, and produce a response. The average response time is recorded to be just a few seconds, making it ideal for real-time monitoring applications. However, detecting multiple faces simultaneously presents some challenges, and

efforts are underway to enhance the system for better multi-face detection and tracking.

To sum up, the testing phase has shown that the "God's Eye" system is very efficient at detecting and recognizing faces in ideal conditions. Nevertheless, it still faces challenges from environmental factors, variations due to aging, and the need for multi-face detection, which will require additional improvements. Future enhancements will aim to incorporate deep learning, boost image processing capabilities, and enhance low-light detection, making sure the system continues to be a robust resource for real-time criminal identification.



FIG 11:-PROPOSED SYSTEM

VI. RESULTS AND DISCUSSION

The system showed remarkable promise in real-time facial recognition for identifying criminals, achieving an impressive accuracy rate of over 90% in ideal conditions. It successfully detected and recognized individuals when their faces were clearly visible and facing the camera. The performance was particularly strong in well-lit settings, where the Haar Cascade face detection algorithm efficiently and accurately identified human faces. However, the effectiveness of the system diminished in low-light situations, highlighting the necessity for integrating infrared (IR) cameras to enhance detection capabilities at night. Furthermore, the system faced challenges in recognizing complete facial features when individuals wore masks, sunglasses, or hats, which lowered the accuracy of recognition. This points to the need for advanced deep learning methods, like Convolutional Neural Networks (CNNs), to enhance feature extraction even when facial visibility is limited.

In real-time detection trials, the system was able to recognize faces in just a few seconds, which makes it an excellent choice for automated surveillance uses. However, it struggled to track several faces at once when multiple people were present in the frame. This challenge points to the necessity for optimizing multi-face detection to boost its effectiveness in busy settings. Furthermore, while the database comparison was generally efficient, there were instances of false positives, where innocent individuals were incorrectly flagged as criminals. This suggests that the criminal database requires regular updates and a stronger filtering system to reduce mistakes and enhance accuracy.

The alert system based on Telegram was incredibly quick, sending notifications to law enforcement within just 5 seconds of a positive identification. This capability removes the reliance on SIM-based messaging, making the system both cost-effective and scalable for broader implementation. However, there were some delays in notification delivery during network outages, indicating a need for backup communication methods to ensure uninterrupted alert transmission. Despite these minor issues, the system has demonstrated high effectiveness in real-time monitoring, providing law enforcement agencies with a valuable tool to boost security and deter crime through automated facial recognition. Future enhancements, including deep learning integration, low-light performance improvements, and the ability to detect multiple individuals, will further increase the system's efficiency and practical use in real-world scenarios.

VII. ADVANTAGES AND LIMITATION

The system offers a variety of benefits that position it as an effective tool for real-time criminal identification and law enforcement efforts. One of its key strengths is its impressive accuracy in detecting and recognizing faces, especially in well-lit environments. By utilizing Haar Cascade classifiers and Histogram of Oriented

Gradients (HOG) for feature extraction, the system can pinpoint individuals based on their distinct facial characteristics. This capability allows law enforcement to swiftly identify suspects and respond accordingly, significantly cutting down the time needed for manual identification and investigation. Additionally, the system's real-time functionality enables ongoing monitoring through surveillance cameras. The implementation of automated face recognition greatly improves security measures, as it removes the necessity for manual checks and guarantees immediate identification of suspects.

One of the standout cost-saving features of this system is its use of the Telegram API for alert notifications, which eliminates the need for SIM-based messaging services. This enables authorities to receive instant alerts when a match is detected, facilitating quick responses without incurring extra communication expenses. Moreover, the system is designed to be scalable and continuously upgradable, meaning that as new data is incorporated, the accuracy of recognition improves. The capability to refresh the criminal database and train the system with a wider range of facial datasets ensures it remains effective in identifying individuals, even as their facial features evolve over time. Another major benefit is the portability and affordability of the hardware, as the system utilizes the Raspberry Pi 5, a cost-effective and energy-efficient processing unit adept at handling computer vision tasks.

While the system has notable strengths, it also faces certain limitations that need to be addressed. A key challenge is its reliance on lighting conditions; in low-light or nighttime settings, the accuracy of face detection drops significantly. The system finds it difficult to identify individuals in poorly lit areas, which hampers its utility for nighttime monitoring or in dim environments. This issue highlights the potential benefit of incorporating infrared (IR) cameras or thermal imaging sensors to boost face recognition capabilities in darkness. Additionally, the system struggles with partial obstructions, as individuals wearing masks, sunglasses, hats, or scarves may not be detected effectively. Since Haar Cascade classifiers depend on visible facial features, obstructions that cover critical areas like the eyes, nose, and mouth can hinder detection performance. To address this, integrating deep learning-based face recognition models, such as Convolutional Neural Networks (CNNs), could significantly improve the system's ability to recognize faces that are partially obscured.

One challenge is the difficulty in recognizing multiple faces at once, particularly in busy public areas. The system is designed to detect and analyze single faces effectively, but it encounters issues when several individuals are present in the same frame. This limitation can hinder its performance in crowded locations like airports, train stations, or large events, where monitoring multiple suspects is crucial. Enhancing algorithms for detecting multiple people and incorporating real-time facial tracking could strengthen the system for extensive security needs. Furthermore, during evaluations, there were instances of false positives, where innocent individuals were mistakenly identified as criminals due to similar facial characteristics or inaccuracies in the database. This situation underscores the necessity for frequent database updates, better feature extraction techniques, and advanced machine learning models to minimize identification mistakes.

To sum up, the system offers real-time, affordable, and highly accurate facial recognition for identifying criminals, but there are still some hurdles to overcome to boost its effectiveness. Enhancements like infrared detection for low-light situations, advanced deep learning face recognition models, better multi-face detection capabilities, and optimized database management will contribute to making the system more efficient, trustworthy, and suitable for real-world security needs. Even with its existing challenges, this system stands as a significant asset that has the potential to transform law enforcement and surveillance technologies, aiding in crime reduction and enhancing public safety through automated identification of suspects.

VIII. CONCLUSION

The system offers a smart and efficient solution for identifying criminals in real-time through advanced face detection and recognition technologies. By employing Haar Cascade classifiers for detecting faces and using Histogram of Oriented Gradients (HOG) for feature extraction, it effectively matches faces with a pre-existing criminal database. The use of Raspberry Pi 5 as the processing unit provides a budget-friendly, portable, and scalable option, making it an excellent resource for law enforcement and security needs. A standout feature is the integration of the Telegram API, which facilitates immediate suspect identification and alert notifications, enabling rapid responses from authorities. The system has shown impressive accuracy under ideal conditions,

positioning it as a promising tool for automated surveillance and crime prevention.

While the system has notable strengths, it also presents certain limitations that need to be addressed to enhance its effectiveness in real-world situations. A key challenge is its reliance on lighting conditions; face detection accuracy tends to drop in low-light or nighttime settings. The system also struggles with recognizing faces that are partially hidden, such as those of people wearing masks, sunglasses, or head coverings, which reduces its reliability in unpredictable environments. Moreover, the current version has difficulty detecting multiple individuals at once, making it less efficient in crowded spaces where identifying several suspects simultaneously is crucial. Additionally, the occurrence of false positives, where innocent people are mistakenly identified as suspects, highlights the necessity for improved database accuracy and enhanced feature extraction methods.

To address these challenges, future improvements should aim at integrating deep learning techniques like Convolutional Neural Networks (CNNs) to enhance facial recognition accuracy. Additionally, incorporating infrared (IR) cameras will boost performance in low-light environments, while enhancing multi-face detection will allow for better tracking of several individuals in crowded areas. Furthermore, refining database management will help reduce false positives. These upgrades will greatly enhance the system's accuracy, efficiency, and reliability, making it a more powerful resource for law enforcement and security organizations.

Even with its limitations, this system marks a major advancement in surveillance technology. It provides a scalable, automated, and smart method for identifying criminals. As AI-based recognition models continue to evolve, this system could transform contemporary law enforcement, boosting public safety, lowering crime rates, and giving authorities a quick and effective means to identify and monitor offenders.

REFERENCES

- [1] Y. Wencheng, S. Wang, J. Hu, Z. Guanglou, and C. Valli, "Security and Accuracy of Fingerprint-Based Biometrics: A Review," *Symmetry*, vol. 11, no. 2, p. 141, Feb. 2019.
- [2] S. P. Patil et al., "Criminal Identification for Low Resolution Surveillance," in *VIVA-Tech International Journal for Research and Innovation*, Mumbai, 2021, vol. 1.
- [3] N. Aherwadi, D. Chokshi, S. Pande, and A. Khamparia, "Criminal Identification System using Facial Recognition.
- [4] A. P., Impana.H.C, Siri.S.L, Varshitha.M.R , Ramesh.B et al., "Automated Criminal Identification by Face Recognition using Open Computer Vision Classifiers," in *Third International Conference on Computing Methodologies and Communication*, September 2022.
- [5] A. S. Tiwari, Ghotekar Shubhangi S , Ghotekar Ashwini S , Manjare Mayuri A
- [6] Pro.Bankar A.A et al., "Criminal Identification by using Real Time Image Processing," in *International*
- [7] P. Kakkar and V. Sharma, "Criminal identification system using Face Detection and Recognition," in *IJARCCCE*, vol. 7, no. 3, Mar. 2018.
- [8] V. D. et al., "Facial Recognition System for Suspect Identification Using a Surveillance Camera," in *Pattern Recognition and Image Analysis*, vol. 28, pp. 410-420, Mar. 2018.
- [9] F. Yu, W. Xian, Y. Chen, F. Liu, M. Liao, V. Madhavan, and T. Darrell, et al., "Bdd100k: A diverse driving video database with scalable annotation tooling," 2018
- [10] S. Heo, Sungjun Cho, Youngsok Kim, Hanjun Kim et al., "Real-Time Object Detection System with MultiPath Neural Networks," in *IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS)*, 2020.