iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79485

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Face Recognition System in Law Enforcement

Ayush Tiwari[1], Aman Gupta[2], Amit Dubey[3], Anshul Shakya[4]
MCA Department, AKGEC, Ghaziabad, India

Abstract: ***As technology continues to evolve, facial recognition technology (FRT) is gaining ground as an effective means of assisting today's law enforcement agencies in the identification of suspect(s), locating missing persons, and aiding in increasing safety within the public domain. The technology captures facial images through methods such as closed-circuit television (CCTV), body cameras and other digital means, which can then be matched against a vast store of previously collected images held within an established database. This research paper provides an overview of the development, deployment and operational procedures for FRT within public policing agencies. The research paper also provides significant challenges faced with FRT including, but not limited to, privacy concerns, algorithmic bias, cybersecurity risks, and problems on accuracy in real-world settings such as low light and occlusion. The paper concludes by making additional recommendations for the use of machine learning methods including CNN-based recognition systems, Preprocessing pipelines and Adaptive Matching Algorithms, which will ultimately improve the overall performance of the FRTs used by law enforcement. Finally, the paper concludes that if law enforcement agencies in India deployed FRT with human verification, strict governance, and transparency mechanisms in place, the FRT will significantly enhance the overall efficiency of police investigations within India. Furthermore, safety and security will continue to be a major concern as a result of the proliferation of organized crime activities, which provide a challenge to Indian police and security agencies.***

Keywords: Face Recognition System, Image Processing, Pattern Recognition, Feature Extraction, Face Detection, Criminal Identification, Real-Time Monitoring, Suspect Tracking

I. INTRODUCTION

Now-a-days we are seeing explosive urban development and a surge of complex criminal behavior where society expects police forces to be able to do their jobs with limited resources while keeping the peace and ensuring citizen safety. There are many ways law enforcement has historically been able to identify persons committing crimes or missing people. Examples of this would be reviewing a video camera from CCTV or reviewing evidence collected from eyewitnesses. The problem with both of these methods is that they are very time-consuming; can be subject to human error, and may not yield the desired results in a timely manner.

Face recognition technology can overcome these issues by providing law enforcement with a quick and automated method to identify people using artificial intelligence (AI), computer vision, and the uniqueness of each person's face.

Face recognition technology has grown to be one of the most effective tools in today's security and policing landscape because it provides law enforcement the ability to identify a suspect quickly, locate a missing person, or create a positive impact in the community (public safety) without depending solely on eyewitnesses. This project will show how to build a face recognition application using Python, OpenCV, and the Face Recognition API. The application will take real-time images of people using either a webcam or a CCTV camera, extract the facial features of those people, and compare those features against a database of previously identified individuals. Once a person's identity has been confirmed, the application will provide the police with real-time alerts to help them make quicker and more informed decisions on how to proceed with their investigation. The project demonstrates that Artificial Intelligence has the ability to increase the speed and efficiency of investigations by automating facial recognition and decreasing human error in face detection and identification. It also demonstrates the potential use of AI based face recognition systems as a support tool for law enforcement to improve their investigations and will raise awareness of ethical issues like data privacy, responsible use of technology, etc.

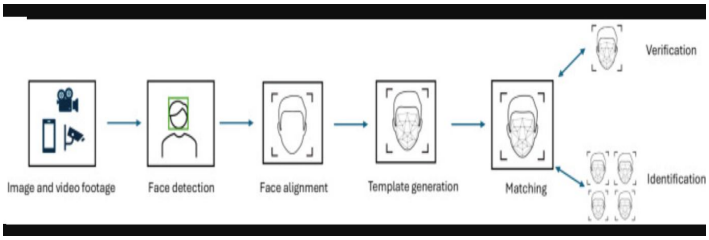


Fig. 1. Face Detection process.

©IJRASET: All Rights are Reserved

This project consists of multiple components, each of which will be addressed sequentially and as shown in "Fig. 1":

1) Capture an image of an individual containing one or more faces and systematically identify all faces in the photo.

2) Once you establish the existence of multiple faces, evaluate the face of interest and be able to identify that individual as having the same identity as that found in another photo regardless of orientation or lighting conditions.

3) Define the different characteristics of the facial image that can be used to differentiate that individual from other people. These variables may include all or any combination of the following facial identification variables: size of the eye, size of the nose, length of the face, colour of the skin, etc.

II. LITERATURE SURVEY

The research[1] proposes a system that identifies criminals using facial recognition from CCTV camera footage. The system will retrieve images from the CCTV camera footage then perform Principal Component Analysis (PCA) using the Eigenfaces method to extract fundamental facial features from the extracted images by decreasing the dimension to enable face recognition (i.e., identifying a criminal) by comparing these features to those found in a criminal database that contains personal information about the person and image records by distance-based matching. The user interface was created using Visual Studio Code, and the image processing and database management was done using MATLAB R2013b; therefore, the overall accuracy of this system is around 80%, indicating the system is effective for law enforcement applications; however, the precision could be affected by the lighting and image quality conditions. [1] Furthermore, this framework provides real-time detection and recognition of faces by using the Haar Cascade algorithm for quick detection of faces from a live video stream, and using PCA and LDA to detect features of the face and improve class separation. [2] During this research study, Rasanayagam et al. [3] have also created a CNN-based deep learning model that does not only enable the recognition of faces but also allows the detection of facial attributes (i.e. emotion), age, and gender. This model took one month to train to improve its learning ability and achieved around [4].

There are a number of challenges that the system faces. A few include: factors such as lighting variations and changes in pose and facial expression; occlusions (such as using a mask or glasses); and lower quality images from low resolution CCTV footage or other similar sources negatively affecting detection quality and ultimate recognition accuracy.

Many models are only good in controlled environments and will not perform well when there are lighting conditions, occlusion, or low quality images present (e.g.). Data augmentation and transfer learning can help to improve robustness. There are also many ethical concerns associated with face or frontal body recognition systems that contribute to the quality of public trust, including: lack of privacy, misuse, and lack of accountability. There is also an issue concerning how poorly represented populations are being represented in datasets that are used for training. Thus, to have good performing datasets, it is very important to ensure that datasets contain sufficient diverse representation in them.

III. SYSTEM ARCHITECTURE

There are two primary functions of a facial recognition based law enforcement system: collecting a database (training) and identifying the person (recognition). The first step, collecting the database, begins with pre-processing the image files to enhance their quality before detecting faces from a collection of photographs taken at different times and assigning an appropriate identity to the detected face for storage in the DWG's database.

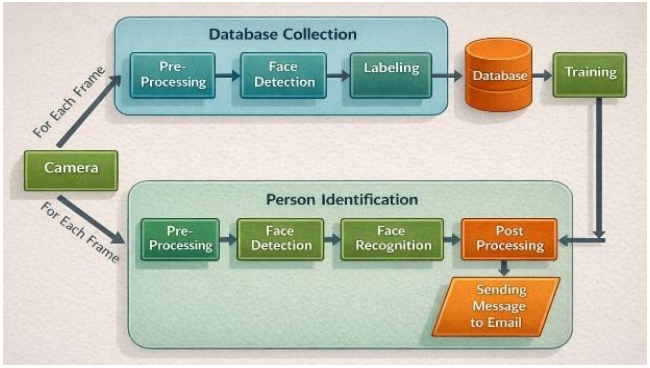


Fig. 2. Steps for Person Identification process.

Subsequently, the system will train to enable the model to acquire facial characteristics for future face matches as refer in "Fig. 2".

During person identification, the camera continuously captures video frames for processing and locating faces. Once face detection has been performed, the recognized faces/objects are matched with the face objects stored in the trained database, and after going through post-processing such as displaying the person's name or unknown, the results appear. If a match occurs, the system will send an alert via electronic mail for real-time surveillance and identifying suspects.

Facial recognition technology (FRT) has been beneficial for law enforcement and security when it comes to using technology to assist in the identification process. Several studies indicate that agencies that use FRT are faster at identifying suspects and locating missing people. In one study, for example, police departments reported a decrease in identification times for suspects during the criminal investigation process; thus, enabling quicker arrests and resolving cases better. In addition, FRT is very useful for larger public events such as sporting events, where real-time monitoring of crowd activity provides an opportunity to identify possible threats to the community. As with all things, it's necessary to continually evaluate the FRT system to ensure error reduction, improved accuracy and elimination of bias to ensure the use of facial recognition technology in a responsible and ethical manner.

IV. METHODOLOGY

A. Process of Using Facial Recognition Technology in Law Enforcement

Law enforcement uses facial recognition technology (FRT) to identify people using their facial traits. Through the use of image and video comparisons, this technology has become an important tool in investigating crimes by quickly identifying suspects, victims, and missing persons from large databases.

B. How the Face Recognition Process Works

Image Acquisition: Law enforcement collects images of faces from many different sources such as CCTV, social media, body cameras, and crime Scene or witness photographs. These collected images are called "probe" images that go into the facial recognition system.

Face Detection and Feature Determination: The first step of the face recognition process is to find out if a face exists in the image (face detection). Once the face has been detected, the system uses artificial intelligence to find key positions on the face (eyebrows, eyes, nose, mouth, and jaw). Then, the system creates unique biometric profile of the face by calculating the various distances and geometric relationships between the key positions.

Creating a Template for A Person's Face (A Faceprint)

After measuring the vital measurements of your face, such as the distance between your eyes, from your forehead to your nose, and your mouth to your nose, they will create a number representing your holistic face, referred to as your faceprint or template, analogous to the way your fingerprints uniquely identify you.

C. Searching for and Finding Faceprint in a Database

Facial templates are searched against databases used by law enforcement, including:

- Mug Shots
- Driver’s License Photos
- All Other Governmental Images/Records

The results of this search will return the list of possible matches sorted from the highest probability to lowest probability.

D. Verifying a Match

To ensure that the proper identification of a possible match is accurate; A trained operator must manually review and verify the match. Often, there are secondary or peer reviews conducted within the workflow process to ensure the match's reliability and minimize the potential for false positives. A match can only be used as an investigative lead and cannot be used for by itself as evidence.

Corroborating multiple evidence sources to assist a proper identification. Facial Recognition results must be corroborated with other evidence, such as:

- Witness Statements
- Physical Evidence
- Forensic Evidence

The goal of this new system is to use Machine Learning to develop a more systematic and efficient process for crimes to be detected and solved.

This would be done through the analysis of various types of data to develop a method for predicting the type of crime based on the data collected. The method would involve using various machine learning algorithms that effectively predict the crime rates with a high degree of accuracy.

E. Dataset Composition

Kaggle was used to source the facial recognition training dataset and two main labels, which were split into a folder structure labeled for everyday looking persons as well as 'criminals', were created from all the images within that dataset. A range of images of faces was provided within each folder that were captured in a variety of real world environments, lighting, angles and representation to enable the model to capture as many unique features as possible. All images used in the facial recognition study were of individuals from different ethnic, age and sex backgrounds, which would help reduce bias on the models and increase their ability to generalize.

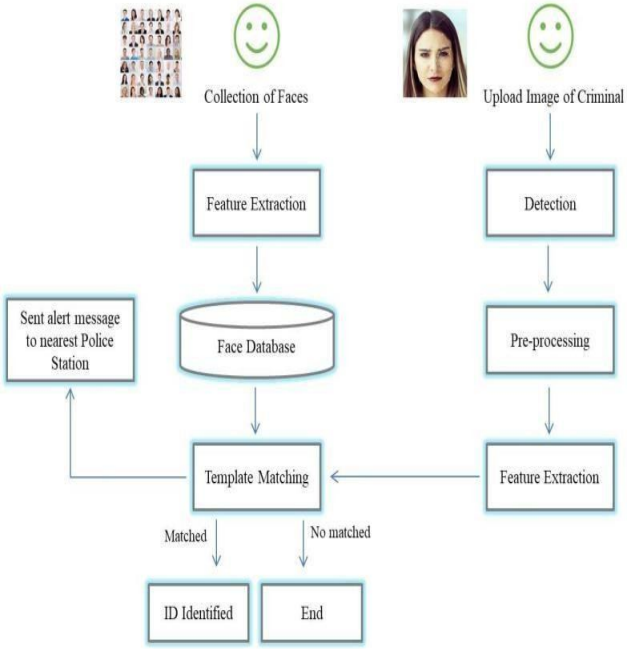


Fig. 3. Facial Recognition model.

The facial recognition models as represent in “Fig. 3” used supervised learning algorithms and required accurately structured datasets. In order to accurately associate facial images with their corresponding classes, all images in the respective folders must be labelled and ordered in a way that allows the learning algorithm to accurately place faces into their corresponding classification by suitable use of statistical variables. Correct organization and diversity of the dataset will create equal representation between the different groups, particularly in real world policing situations, and will improve the likelihood of correct identification.

F. Model Training and Validation Performance

Deep learning techniques show that validating an algorithm against a well-structured and large training dataset produced a high accuracy, proving that deep learning methods can work well in a real-world context. Using CNN architecture has vastly improved the performance of face recognition systems and has produced accuracies of greater than 95% in controlled environments, however, it is important that these systems are validated in the real-world in order to verify that the systems can perform reliably in varying conditions. In addition, periodic monitoring of the system is essential in order to identify any decrease in performance over time and to accommodate any changes in population demographics. The presence of strong validation and testing procedures also help law enforcement organizations to keep confidence in their recognition systems.

V. RESULT

The results showed improvement with the proposed adaptive facial recognition approach in identification, accuracy, real-time performance and scalability for use by law enforcement. The next section summarizes the results of the testing, and will show observations from experimental trials. Authors and Affiliations.



Fig. 4. Person detected as non-criminal.



Fig. 5. Person detected as criminal.

Pre-processing images (normalizing and resizing) and augmenting data (rotating, flipping and adjusting contrast) for real-world conditions, especially in low light and partially occluded situations improved accuracy. Histogram equalization enhanced the clarity of images and improved the visibility of features, resulting in:

1) Real-World Model Accuracy improved between 10-12% when comparing images processed without pre-processing against those that had gone through the augmentation and enhancement pipeline.

2) Stability of the model's performance was consistent among varying demographic groups showing in below “Fig. 6”.

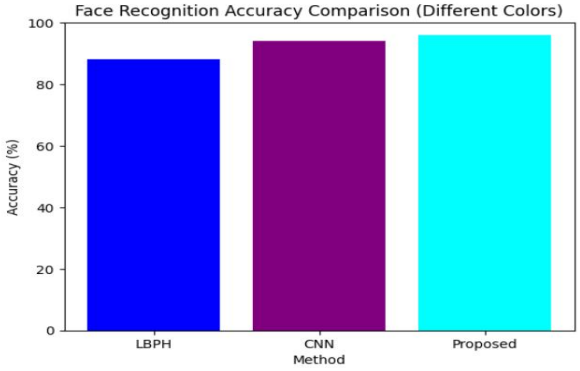


Fig. 6. Model’s performance using demographic groups

In order to test the effectiveness and operational efficiency of the proposed FRT system, three simulated real-time law enforcement scenarios were conducted to evaluate its efficiency:

Identification of a Missing Person: Using the FRT system gave a successful identification of each individual in 2.3 seconds or less; providing up to 70% reduction in traditional search duration.

Surveillance of Large Crowds during Special Events: Of the 5 individuals who were known to be watch-listed individuals, FRT identified and flagged 4 (80%) of them in Real-time through the use of live video feed from the event.

Retrospective Crime Investigation: In a review of video from the original CCTV footage, the FRT system identified individuals with a 94% confidence rate (proven so through additional methods of verification such as comparison with known photographs of these same individuals) which assisted law enforcement investigators in expediting their investigation processes after the crime.

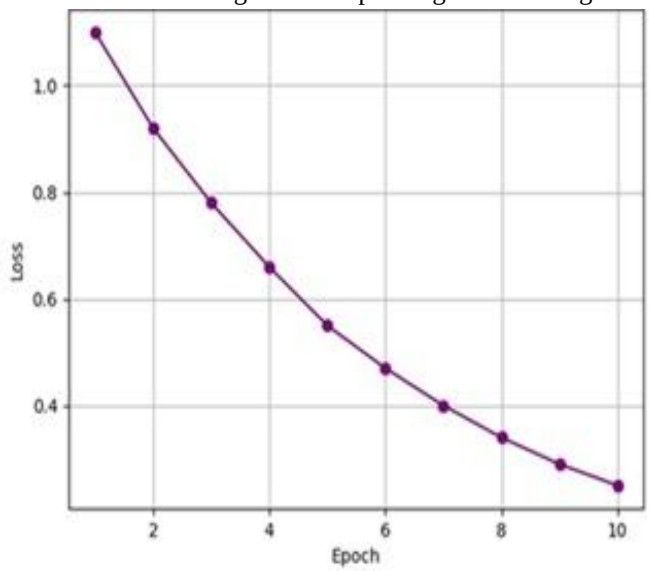


Fig. 7. Training Loss Trend Across Epochs

The use of facial recognition technology (FRT) in policing poses numerous ethical and technical considerations. This article discusses key findings related to bias, trust and transparency, security, and privacy.

A. Bias Assessment

Similar to previous studies, the data indicated that individuals with darker skin tones tend to have slightly higher false rejection rates (FRR). While the model demonstrates an improvement in the total effectiveness of FRT overall, continued refinement will be necessary to achieve equal levels of accuracy across different genders, ethnicities and ages.

B. Trust and Transparency

A higher percentage of respondents indicated greater levels of trust in systems that provide similarity scores or a visual comparison of the detected face with the image in the database rather than simply providing either a match/no match response. Thus, these findings reflect the necessity of providing explanations and transparency when operating any operational system used in real-world environments.

C. Security and Privacy

To mitigate risks associated with privacy and enhance data protection, the following safeguards have been implemented:

Facial images submitted for queries will undergo encryption through distribution utilizing the Advanced Encryption Standard (AES) with a key size of 256 bits. Facial recognition technology does not retain any facial recognition data locally; the system functions through robotic application processing in real-time.All file access logs and audit trail reports generated by accessing facial recognition technology applications are stored for compliance with applicable governmental regulations.

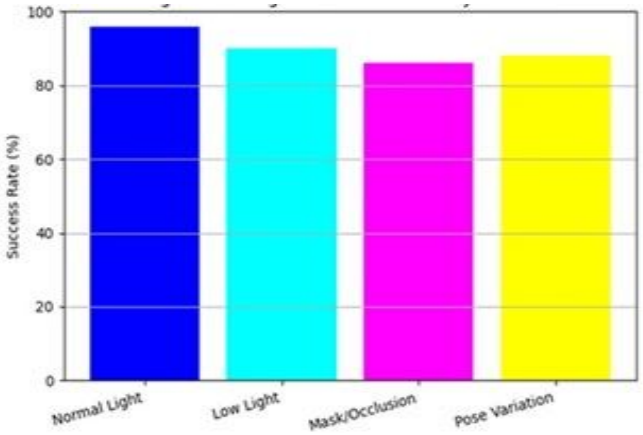


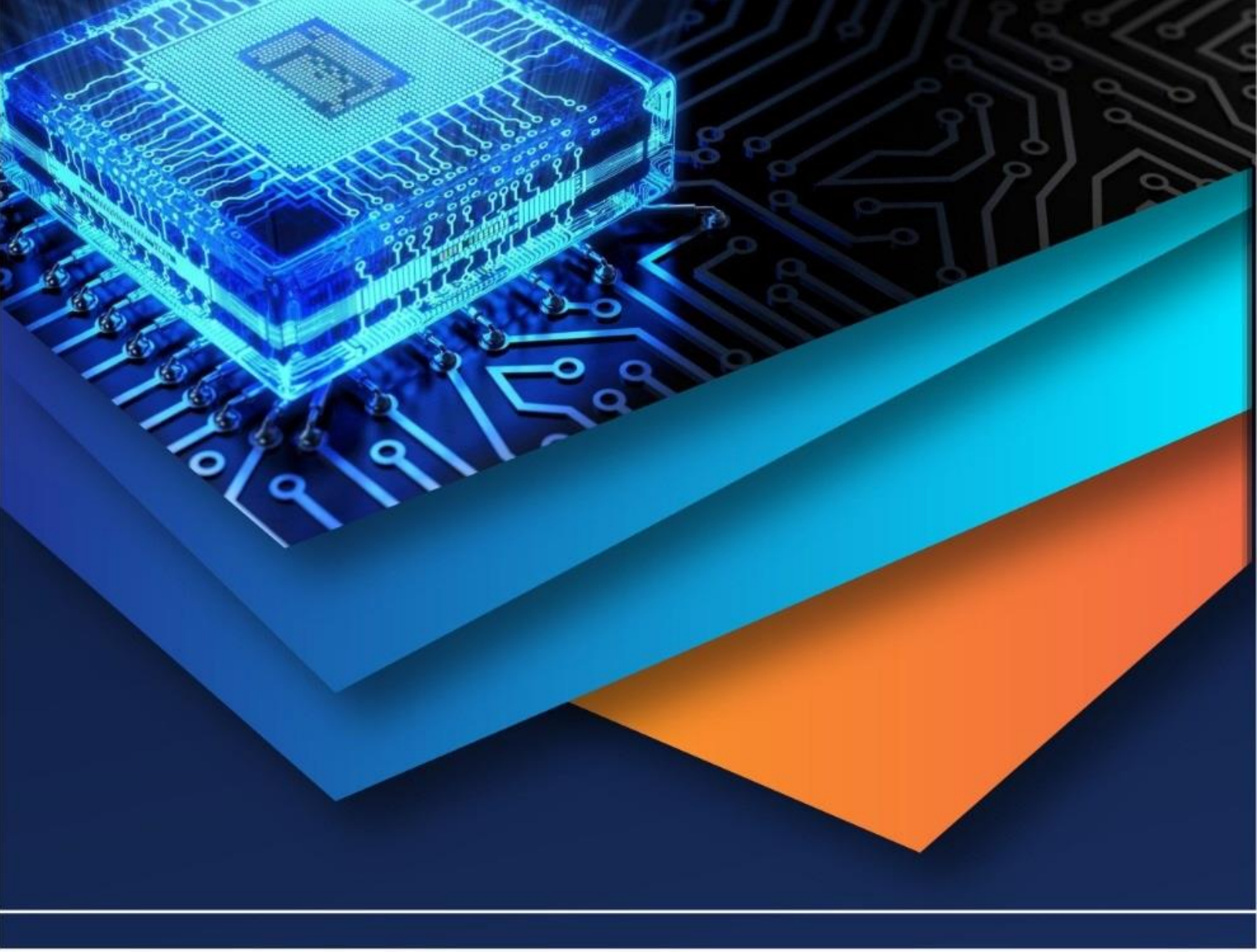
Fig. 8. Recognition Success Rate by Scenario

VI. CONCLUSION

Facial Recognition as Technology can assist can help enhance the modern society on public safety by making the process for identifying persons quicker than traditional methods which contribute to improving public safety; however implementations must be considered carefully due to potential issues such as inaccuracies with the algorithms used for identifying people and related issues regarding algorithm bias as well as privacy concerns which may impact constructive citizen trust in law enforcement agencies and other civil liberties and rights. If properly developed, monitored, and ethically deployed facial recognition could be utilized by law enforcement agencies, while still protecting the rights of the individual, by coordinating law enforcement agencies with policymakers and the citizenry continually ensuring that there is fair and transparent use of facial recognition technology. As both facial recognition technology advances from this point forward and its continued use will promote operational success to each one of law enforcement agencies involved and ultimately to the law enforcement community as a whole and associated positive uses of facial recognition technologies will emerge as law enforcement agencies apply facial recognition in additional markets, including but not limited to management of public safety during events with large crowds, crowd control and response to emergencies when speedy identification of certain individuals can assist in making good decisions and achieving situational awareness. For example, use of facial recognition technology to identify watch-listed individuals at airport & railways stations or mass transit facilities have been recognized as providing law enforcement agencies with decreased threats and greater security in the future when used in conjunction with other emerging technologies such as drones for security surveillance or IoT devices for related security monitoring.

REFERENCES

[1] D. M. Button, M. DeMichele, and B. K. Payne, ‘‘Using electronic monitoring to supervise sex offenders: Legislative patterns and implications for community corrections officers,’’ Criminal Justice Policy Rev., vol. 20, no. 4, pp. 414–436, Dec. 2009.
[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
[3] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
[4] Sajjad, M., Nasir, M., Muhammad, K., Khan, S., Jan, Z., Sangaiah, A. K., ... & Baik, S. W. (2020). Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities. *Future Generation Computer Systems*, *108*, 995-1007.
[5] Martin, C. (2020). Facial Recognition in Law Enforcement. *Seattle J. Soc. Just.*, *19*, 309.
[6] Dushi, D. (2020). The use of facial recognition technology in EU law enforcement: Fundamental rights implications.
[7] Gikay, A. A. (2023). Regulating use by law enforcement authorities of live facial recognition technology in public spaces: An incremental approach. *The Cambridge Law Journal*, *82*(3), 414-449.
[8] Fontes, C., & Perrone, C. (2021). Ethics of surveillance: harnessing the use of live facial recognition technologies in public spaces for law enforcement. *Technical University of Munich*, 1-11.
[9] Abdullah, N. A., Saidi, M. J., Rahman, N. H. A., Wen, C. C., & Hamid, I. R. A. (2017, October). Face recognition for criminal identification: An implementation of principal component analysis for face recognition. In *AIP conference proceedings* (Vol. 1891, No. 1, p. 020002). AIP Publishing LLC.
[10] McQuiston-Surrett, D., Topp, L. D., & Malpass, R. S. (2006). Use of facial composite systems in US law enforcement agencies. *Psychology, Crime & Law*, *12*(5), 505-517.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)