

# Face Detection and Recognition For Criminal Identification

<sup>1</sup>N.Anithaa, <sup>2</sup>Puchakayala Srikanth, <sup>3</sup>puppala Nithin, <sup>4</sup>Pinreddy Tharun Reddy, <sup>5</sup>pulagam Akshaya sai

Department of Computer Science and Engineering,  
Bharat Institute of Higher Education and research  
Chennai, India.

**Abstract-** The security of India is increasingly crucial in the contemporary world. There is a growing concern about organized crime activities that pose a potential threat to law enforcement and defense agencies. In this context, the utilization of technology becomes paramount. Video analytics is a significant aspect of technology implementation in law enforcement, comprising various components. One key component involves identifying patterns across different videos. The specific task at hand is the analysis of a 30-second to 1-minute video, focusing on capturing facial images of individuals present. Subsequently, another video is analyzed to determine how many individuals from the initial video reappear, along with the corresponding timestamps. Implementing such technology on a larger scale, involving thousands of videos sourced from diverse intelligence channels and conducting cross-checks, holds the potential to extract substantial information regarding patterns in organized crime. This innovative approach to video analytics provides a systematic and efficient means of identifying recurring individuals across various video sources, offering valuable insights for law enforcement and defense agencies in combating organized crime effectively.

**Keywords:** crime, threat, analytics, Manual Identification System.

## I. INTRODUCTION

Criminal identification stands as a paramount task

for law enforcement agencies, necessitating a thorough and time-consuming search for criminals, particularly in densely populated urban areas. In recent years, computer vision has become an essential tool for enhancing safety and protection, with facial recognition emerging as a promising application. Despite human proficiency in recognizing various faces, technological advancements aim to develop systems comparable to human perception. Various algorithms and approaches have been developed to identify faces, focusing on tracing facial contours and isolating features like eyes, nose, and mouth. However, challenges persist, encompassing intrinsic factors such as age and expressions, and extrinsic factors like lighting and poses.

When it comes to identifying and verifying criminals, facial recognition technology is crucial in combating the alarming rise in crime rates. The criminal recognition system operates by automatically locating faces in images or videos, utilizing a criminal database to match faces and authenticate individuals. The process involves two stages: face detection and face recognition. Face detection compares input images to face templates, while face recognition identifies faces by comparing them to stored facial templates in the database.

The goal of this technique is to identify offenders in moving images, storing information in a criminal database alongside personal details. The facial recognition system processes uploaded images, matches features, and presents relevant information if a match is detected. The paper outlines face detection methods (HAAR cascade classifier, HOG) and face recognition methods (LB pattern histograms, SVM, CNN), concluding with discussions on potential future enhancements.

The system's significance lies in its ability to assist law enforcement in identifying and apprehending criminals in public places. A comparison is drawn between Manual Identification System (MIS), where officers manually search public places, and Automated Identification System (AIS), which eliminates the need for human observation in public spaces, offering efficiency and accuracy. Motivation behind the project stems from the desire to provide police personnel with a time and cost-effective tool for criminal identification. The application aids in maintaining criminal records, offering a comprehensive solution to law enforcement challenges.

## II. LITERATURE SURVEY

The first research conducted by Nurul Azma Abdullah, Md. Jamri Saidi, Nurul Hidayah Ab Rahman, Chuah Chai Wen, and Isredza, Rahmi A. Hamid [1] focuses on utilizing CCTV footage for criminal identification. The authors employ Principal Component Analysis (PCA) to detect similar features between images from the footage and a criminal database. The system uses facial recognition dependent on a database containing personal information. The user interface is developed using Visual Studio Code, and MATLAB R2013b is used for coding and database management, achieving an 80% accuracy rate.

In the study by Shalinda Adikari, Kaumalee Bogahawatte [2], clustering techniques are applied to group crime data, followed by Naive Bayesian classification to identify likely suspects. JSF (Java Server Faces) and PrimeFaces are employed for User Interface implementation. Oracle Database 10g Express Edition is used for database management.

Apoorva P., Impana H.C., Siri S.L., Varshitha M.R., and Ramesh B. [3] propose a robust real-time face detection methodology based on Haar Cascade for face recognition. The system achieves over 90% accuracy using multiple algorithms, including PCA with LinearDiscriminant Analysis.

Shiva Tamrkar, Ayush Gupta [5] propose a criminal identification methodology in India using face recognition, presenting feature-based, holistic, and hybrid approaches. The authors achieve a 96.2% accuracy rate with their proposed model.

Mr. R. Prashanth Kumar, Abdul Majeed, Farhan Pasha, A Sujith [6] introduce a real-time criminal identification system using face recognition with Haar feature-based cascade classifiers and OpenCV LBPH algorithms, reporting a 95% accuracy rate.

Using deep learning-based CNN techniques, Kavushica Rasanayagam, Kumarasiri S.D.D.C., Tharuka W.A.D.D., Samaranyake N.T., Dr. Pradeepa Samarasinghe, and Samantha E.R. Siriwardana [7] investigate face, emotion, age, and gender identification. After a month of training, the system reaches an accuracy of 80%. In an effort to increase accuracy, Alireza Chevelwalla, Ajay Gurav, Sachin Desai, and Prof. Sumitra Sadhukhan [8] assess and compare different face detection and recognition techniques for image-based face detection.

Shadman Shahriar et al. [9] propose a facial recognition project to identify fugitive criminals using facial recognition technology. The system creates distinct templates for each face and achieves multiple face recognition efficiently.

S. T. Bharathi, Dr. B. Indrani, Dr. M. Amutha Prabakar [10] suggest a supervised approach to identify suspects using a similarity measure and the K-Medoids clustering algorithm. The proposed system demonstrates high accuracy after implementation and analysis.

All the referenced studies contribute diverse methodologies and technologies to enhance criminal identification and improve security measures.

## III. RELATED WORKS

As the crime rate and the number of criminals continue to rise, the management, identification, and tracking of these individuals pose significant challenges for law enforcement. While existing applications assist police departments in storing criminal records, they fall short in actively locating criminals. Traditionally, criminal details were stored in record books or as software records, with photographs serving little purpose. The current methods focus on record management rather than real-time tracking, leading to several disadvantages.

### Disadvantages of the Existing System:

- Inability to detect criminals from any location.
- Existing methods only provide data storage and security but lack live tracking capabilities. There is no application for finding criminals from CCTV footage.
- Manual storage of criminal details requires substantial work.
- Information in records is prone to loss or manipulation.
- Previous applications are not 100 percent accurate, leading to unreliable criminal information.

**Proposed System:**

The proposed project aims to address these shortcomings by developing a Real-Time Criminal Identification System based on face recognition. This application enables the real-time detection and recognition of criminals in images and video streams obtained from cameras. Haar feature-based cascade classifiers in OpenCV are employed for face detection, utilizing a machine learning-based approach. LBPH are employed for face recognition. This system allows police personnel to register criminals, track them using CCTV footage or manual image inputs, and manage data through a dataset.

**Advantages of the Proposed System:**

- Enables police personnel to track and find criminals easily.
- Requires minimal manpower, reducing operational costs.
- Information cannot be manipulated or lost, ensuring data safety.
- Applicable for police and investigation departments to recognize criminals from facial features.
- The application stands out for its 95 percent accuracy, speed, robustness, reliability, and user-friendly interface.

**IV. METHODOLOGY**

The proposed system aims to enhance crime detection and resolution through the application of machine learning strategies. Utilizing data collected from various sources, the program predicts crime types based on patterns, employing high-precision machine learning algorithms for accurate crime rate prediction.

**Data Uploading and Feature Understanding:**

The data sourced from Kaggle undergoes preprocessing to extract essential natural features for crime forecasting. Factors such as specific streets, date and time, and locations with higher crime rates are considered incentives for predicting and resolving crimes swiftly. Key factors in crime rate detection include Number\_Case, Day\_of\_the\_Crime, Type\_First, Case\_Description, Location\_Description, Imprisonment, Home\_Affairs, and Ward.

**Reliable Flexible Ratings:**

Identifying reliable predictive variables is crucial for determining the most influential factors in crime-related variability. Variables like the Criminal Code (iucr) are excluded, focusing on those most impactful on crime forecasting. Visualizing analyzed data allows for the creation of a vector, enabling the use of algorithms to yield accurate results.

**Statistics and Built-in Prediction Model:**

Data analysis evaluation involves summarizing features to predict and prevent various crimes based on diverse circumstances. The system creates a predictive model using a random forest process, an ensemble learning method that combines decision trees. Variables are strategically chosen to predict key criteria for crime prevention.

**Application Design:**

The user interface of the crime rate detection app begins with a login screen. Users upload resumes to the system, and the interface offers a user-friendly look and feel. Key tasks in the project include data uploading, feature understanding, dependent variable analysis, and building a prediction model for essential crime aspects.

**Implementation:**

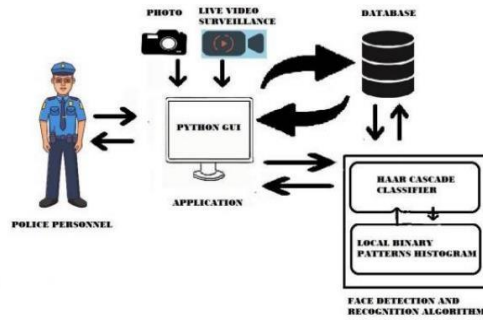
Data collection involves gathering information from various online sources to form a comprehensive dataset. Feature selection is performed using methods like `.dropna()`, `.sum()`, `.unique()`, `.info()`, and `.read_csv()`. Training involves dividing the dataset into training and test data, fitting the training data to algorithms for learning. Prediction methods are employed to predict target values based on input data.

**Data Collection and Preprocessing:**

The collected crime prediction dataset is divided into training and test sets. Data preprocessing involves removing zero or infinite values that may affect accuracy. Steps such as formatting, cleaning, and importing are executed to enhance data quality. Python is used for preprocessing, and the test result indicates the accuracy of predictions.

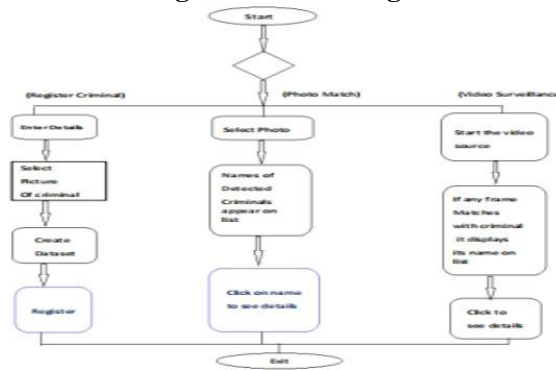
In conclusion, the proposed system combines machine learning algorithms with robust data analysis to predict crime rates accurately. The application design prioritizes user-friendly interfaces, and the implementation process includes comprehensive data collection, feature selection, and preprocessing to achieve reliable crime predictions.

**Fig.1 Architecture diagram**



Three modules make up our project: face detection, fire detection, and gun/knife detection. The primary purpose of this project is criminal detection. First, a webcam or other IP camera will be used to take the image. Certain photos will be kept in the database. The webcam's image will be compared to the image saved in the database; if a match is discovered, a screenshot will be sent along with the database user's name. The administrator receives a screenshot of the image if the person's information is not kept in the database. Processing is done using image processing mechanisms. It can identify people in the video as well. The movie will be divided into many images, with each image matching a different one. Finally, send an alarm to the administrator.

**Fig.2 Data flow diagram**



**V. RESULTS AND DISCUSSIONS**

The output screenshots of the face recognition-based Real-Time Criminal Identification System are shown below. This is how this application appears on the surface. The first window that appears when the user opens the application is this one.



**Fig.3 Message Box Showing Successful Registration of Criminal**



**Fig.4 When User Selects Detect Criminal Option**



**Fig.5 Criminal meeting**



**Fig.6 Criminal Recognition Using LiveSurveillance**

## VI. CONCLUSION

The Safety Management Centre faces the challenge of an overwhelming number of surveillance cameras that exceed the capacity of staff to visually monitor effectively. This results in crimes going unidentified, and a significant portion of recorded footage remains unused. It is difficult to determine a direct preventative effect from surveillance cameras, according to studies, even though their presence may lead to an increase in impulsive criminal action. Furthermore, artificial intelligence restrictions impede post-mortem examinations and real-time image recognition.

This research presents a novel surveillance video data analysis method that uses installed cameras to identify high-risk individuals in real time. One component of the system is an app that may quickly relay personal information to agencies concerned with public safety, enabling instantaneous identity verification. In order to avoid the requirement to retain video, the suggested system analyzes video in real-time using an iterative technique that provides instantaneous face detection and identification in every frame.

The system presents a face recognition technique that uses down-sampling to locate face positions in the source image in order to improve face detection and identification performance. Real-time detection on the same hardware is ensured by this method. By saving the location of faces identified and their identifying details, the system helps with accurate object tracking. The face tracking ID unit minimizes prediction flips and congested embedding concerns by addressing face recognition constraints inside video data.

The threshold value for the identification score accumulation approach was determined through experiments. Practical users can apply multiple models for different domains given the suggested system's compatibility with widely used face detection and identification technologies. Results from the experiments show better F-1 scores and accuracy, especially in migration experiments based on identification techniques.

The suggested method uses real-time video processing from security cameras to effectively identify particular groups of people. The technology efficiently fills in blind spots in the current system by utilizing deep learning, which makes it possible to identify and promptly identify offenders in high-crime regions. The system performs remarkably well, demonstrating increased efficiency on the same hardware by downsampling videos for processing in real time. Achieving high identification and recognition rates is made possible by the face tracking ID unit and identification score accumulation technique.

The anticipated benefits of the suggested method include enhancing blind areas in current systems and enabling quick reactions for incident and accident avoidance. The suggested system has tremendous potential to aid national programs such as criminal identification, location searches for missing persons, and facility protection.

## REFERENCES:

1. V. Tsakanikas and T. Dagiuklas, "Video surveillance systems-current status and future trends," *Comput. Electr. Eng.*, vol. 70, pp. 736–753, Aug. 2018.

2. 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.
3. B. C. Welsh and D. P. Farrington, "Public area CCTV and crime prevention: An updated systematic review and meta-analysis," *Justice Quart.*, vol. 26, no.4, pp. 716–745, Dec. 2009.
4. M. C. Hoffman, "Smart cities: A review of the most recent literature," *Informatization Policy*, vol. 27, no. 1, pp. 3–35, 2020.
5. E. L. Piza, B. C. Welsh, D. P. Farrington, and A. L. Thomas, "CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis," *Criminol. Public Policy*, vol. 18, no. 1, pp. 135–159, Feb. 2019.
6. E. L. Piza, "The crime prevention effect of CCTV in public places: A propensity score analysis," *J. Crime Justice*, vol. 41, no. 1, pp. 14–30, Jan. 2018.
7. G. Alexandrie, "Surveillance cameras and crime: A review of randomized and natural experiments," *J. Scand. Stud. Criminology Crime Prevention*, vol. 18, no. 2, pp. 210–222, Jul. 2017.
8. R. V. Clarke, "Situational crime prevention," *Crime Justice*, vol. 19, pp. 91–150, 1995.
9. J. Ratcliffe, *Video Surveillance of Public Places*. Washington, DC, USA: U.S. Department of Justice, Office of Community Oriented Policing Services, 2006.
10. J.-H. Jeon and S.-R. Jeong, "Designing a crime-prevention system by converging big data and IoT," *J. Internet Comput. Services*, vol. 17, no. 3, pp. 115–128, Jun. 2016.
11. P. Chen, H. Yuan, and X. Shu, "Forecasting crime using the ARIMA model," in *Proc. 5th Int. Conf. Fuzzy Syst. Knowl. Discovery*, Oct. 2008, pp. 627–630, doi: 10.1109/FSKD.2008.222.
12. Lubna, N. Mufti, and S. A. A. Shah, "Automatic number plate recognition: A detailed survey of relevant algorithms," *Sensors*, vol. 21, no. 9, p. 3028, Apr. 2021.
13. K. B. Kwan-Loo, J. C. Ortíz-Bayliss, S. E. Conant-Pablos, H. Terashima-Marín, and P. Rad, "Detection of violent behavior using neural networks and pose estimation," *IEEE Access*, vol. 10, pp. 86339–86352, 2022.
14. N. A. Abdullah, M. J. Saidi, N. H. A. Rahman, C.
15. C. Wen, and I. R. A. Hamid, "Face recognition for criminal identification: An implementation of principal component analysis for face recognition," in *Proc. AIPConf.*, 2017, Art. no. 020002.
16. Y. Kortli, M. Jridi, A. Al Falou, and M. Atri, "Face recognition systems: A survey," *Sensors*, vol. 20, no. 2, p. 342, Jan. 2020.
17. N. Dagnes, E. Vezzetti, F. Marcolin, and S. Tornincasa, "Occlusion detection and restoration techniques for 3D face recognition: A literature review," *Mach. Vis. Appl.*, vol. 29, no. 5, pp. 789–813, Jul. 2018.
18. M. Adil, S. Mamoon, A. Zakir, M. A. Manzoor, and Z. Lian, "Multi scale adaptive super-resolution person re-identification using GAN," *IEEE Access*, vol. 8, pp. 177351–177362, 2020.
19. I. Masi, Y. Wu, T. Hassner, and P. Natarajan, "Deep face recognition: A survey," in *Proc. 31st SIBGRAPI Conf. Graph., Patterns Images (SIBGRAPI)*, Oct. 2018, pp. 471–478, doi: 10.1109/SIBGRAPI.2018.00067.
20. X. An, X. Zhu, Y. Gao, Y. Xiao, Y. Zhao, Z. Feng,
21. L. Wu, B. Qin, M. Zhang, D. Zhang, and Y. Fu, "Partial FC: Training 10 million identities on a single machine," in *Proc. IEEE/CVF Int. Conf. Comput. Vis. Workshops (ICCVW)*, Oct. 2021, pp. 1445–1449.
22. Y. Zhu, H. Cai, S. Zhang, C. Wang, and Y. Xiong, "TinaFace: Strong but simple baseline for face detection," 2020, arXiv:2011.13183.
23. P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. (CVPR)*, 2001, pp. 1–11.
24. J. Yang, D. Zhang, A. F. Frangi, and J.-Y. Yang, "Two-dimensional PCA: A new approach to appearance-based face representation and recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 26, no. 1, pp. 131–137, Jan. 2004.
25. L.-F. Chen, H.-Y.-M. Liao, M.-T. Ko, J.-C. Lin, and G.-J. Yu, "A new LDA-based face recognition system which can solve the small sample size problem," *Pattern Recognit.*, vol. 33, no. 10, pp. 1713–1726, Oct. 2000.
26. E. Ben-Baruch, M. Karklinsky, Y. Biton, A. Ben-Cohen, H. Lawen, and N. Zamir, "It's all in the head: Representation knowledge distillation through classifier sharing," 2022, arXiv:2201.06945.
27. M. Alansari, O. A. Hay, S. Javed, A. Shoufan, Y. Zweiri, and N. Werghi, "GhostFaceNets: Lightweight face recognition model from cheap operations," *IEEE Access*, vol. 11, pp. 35429–35446, 2023, doi: 10.1109/ACCESS.2023.3266068.
28. Y. Zheng, J. Chang, Z. Zheng, and Z. Wang, "3D face reconstruction from stereo: A model based approach," in *Proc. IEEE Int. Conf. Image Process.*, 2007.
29. Y. Feng, F. Wu, X. Shao, Y. Wang, and X. Zhou, "Joint 3D face reconstruction and dense alignment with position map regression network," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, 2018, pp. 534–551.
30. Y. Wen, K. Zhang, Z. Li, and Y. Qiao, "A discriminative feature learning approach for deep face recognition," in *Proc. Eur. Conf. Comput. Vis. Cham, Switzerland: Springer*, 2016, pp. 499–515.