Advanced International Journal of Multidisciplinary Research

E-ISSN: 2584-0487
editor@aijmr.com

Volume 4, Issue 2, March-April 2026

CrossRef DOI: 10.62127/aijmr.2026.v04i02.1275

DEVELOPMENT AND IMPLEMENTATION OF FACE RECOGNITION TECHNOLOGY FOR CRIMINAL IDENTIFICATION AND PUBLIC SAFETY

Dr. M. Vishnu Vardhana Roa[1], K. Lohitha[2], J. Akhila[3], K. Sathwika[4]

[1]Associate Professor, CSE(AI&ML), Vignan's Institute of Management and Technology for Women, HYD, India.
[2,3,4]BTech 4th year Student, CSE(AI&ML), Vignan's Institute of Management and Technology for Women, Hyderabad, India.

Abstract:
Criminal identification in rapidly growing urban environments continues to rely heavily on traditional methods such as manual CCTV monitoring, eyewitness testimonies, and time-consuming verification processes, which often lead to delays, inaccuracies, and reduced situational awareness. These limitations have become more evident with increasing urbanization, population density, and the growing sophistication of criminal behavior. The core problem stems from fragmented criminal databases, lack of real-time coordination among agencies, and minimal public participation in reporting mechanisms, creating a substantial gap in proactive crime prevention. To overcome these challenges, this research develops *CrimeVision*, an AI-powered facial recognition and public safety platform designed to transform static surveillance into an intelligent, automated, and community-inclusive safety system. The proposed system integrates DeepFace with ArcFace facial embeddings, multi-backend detectors such as RetinaFace and MTCNN, and OpenCV preprocessing to ensure high-accuracy face matching from both uploaded images and live camera feeds. Additionally, the system incorporates GPS-based geolocation, interactive map visualization, role-based dashboards, OTP-secured authentication, multilingual interfaces, and real-time alert mechanisms for efficient monitoring. Public users can report suspicious activities with images and location details, while police personnel can manage criminal records, validate reports, track incidents on a map, and receive instant detection alerts. By combining AI-driven recognition, geospatial intelligence, and public engagement within a secure and scalable web architecture, CrimeVision significantly enhances identification speed, reduces manual investigation workload, strengthens community–police collaboration, and supports timely law enforcement response. Ultimately, this system offers a cost-effective, accessible, and technologically advanced framework for improving public safety and enabling smarter, data-driven urban policing.

Keywords: Facial Recognition, Crime Detection, Deep Learning, Computer Vision, Public Safety

I. INTRODUCTION:

Crime prevention and effective criminal identification are essential for ensuring public safety, social stability, and efficient law enforcement, particularly in rapidly growing urban environments. While smart cities increasingly deploy AI-powered surveillance and automated monitoring systems, many regions still

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1275

rely heavily on conventional methods such as manual CCTV observation, eyewitness reports, and fragmented criminal databases. These traditional approaches provide reactive rather than proactive intelligence, often resulting in delayed identification and reduced situational awareness. Furthermore, fully automated surveillance infrastructures may require high-cost hardware and large-scale integration, limiting their accessibility and scalability. To address this gap, this paper proposes CrimeVision: An AI-Driven Face Recognition Framework for Criminal Identification and Public Safety, which transforms static surveillance and reporting mechanisms into real-time predictive and identification intelligence using Artificial Intelligence.

Deep learning–based facial recognition models have demonstrated strong capability in extracting discriminative facial embeddings for automated identification tasks [1], while integration of face recognition with smart surveillance infrastructure has improved real-time monitoring efficiency [2]. Advanced architectures and optimization strategies such as DenseNet-based feature extraction [3], YOLO-based real-time detection pipelines [4], and transfer learning models like VGG16 for CCTV environments [5] have further enhanced recognition accuracy. However, concerns regarding algorithmic bias, fairness in low-quality police images [6], image enhancement techniques for improved facial clarity [7], and regulatory challenges in law enforcement applications [8][9] highlight the need for responsible, secure, and well-integrated systems.
The proposed CrimeVision framework incorporates multi-backend face detection, deep learning–based facial embedding extraction, structured criminal database management, and GPS-integrated alert visualization to strengthen situational awareness. By eliminating excessive hardware dependency and enabling role-based dashboards, multilingual accessibility, and community-based reporting, the system offers a scalable and cost-effective approach to intelligent crime monitoring. This integrated solution enhances identification speed, supports data-driven policing, and promotes collaborative public safety management in modern urban environments.

II. RELATED WORK:

Recent research Several studies have explored the use of artificial intelligence and facial recognition to enhance criminal identification and public safety. Early research in automated inference of criminality from facial images used deep convolutional neural networks to analyze facial attributes, but raised ethical concerns due to dataset limitations and algorithmic bias [1]. Work on smart city surveillance demonstrated the feasibility of integrating AI-based face recognition with CCTV infrastructure to improve real-time monitoring, although scalability and privacy challenges remained significant barriers [2]. Advanced image-processing approaches combining Principal Component Analysis (PCA), DenseNet architectures, and optimization techniques such as Ant Colony Optimization (ACO) were proposed to strengthen feature extraction and classification accuracy; however, their applicability was limited due to controlled datasets and lack of field validation [3]. Real-time facial recognition systems using YOLO-based detection pipelines and web-based dashboards have shown promising results for continuous monitoring, but performance is often dependent on hardware capacity and video quality [4]. Similarly, CCTV-based recognition using transfer learning models like VGG16 improved identification accuracy in structured environments but faced difficulties in low-light and crowded settings [5]. Collectively, these studies highlight the growing potential of AI-driven face recognition while emphasizing the need for integrated, secure, and community-inclusive systems for practical criminal identification and public safety management.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1275

III. PROPOSED SYSTEM:

A. Overview of Proposed System:

The proposed CrimeVision system is an AI-driven face recognition platform designed to improve criminal identification and overall public safety. It employs deep learning and computer vision to accurately match faces with a centralized criminal database. The platform supports role-based access, enabling police to manage records, view alerts, and monitor surveillance, while citizens can report suspicious activities and upload images. Features such as real-time face matching, GPS-based location tagging, interactive dashboards, and automated notifications ensure rapid response. With strong data privacy controls and multilingual accessibility, CrimeVision strengthens coordination between the public and law enforcement.

B. System Architecture:

The architecture consists of six core modules:

- User Management & Authentication
- Face Recognition System
- Criminal Database Management
- Public Reporting & Image Upload
- Real-Time Alerts & Notifications
- Maps & Location Tracking

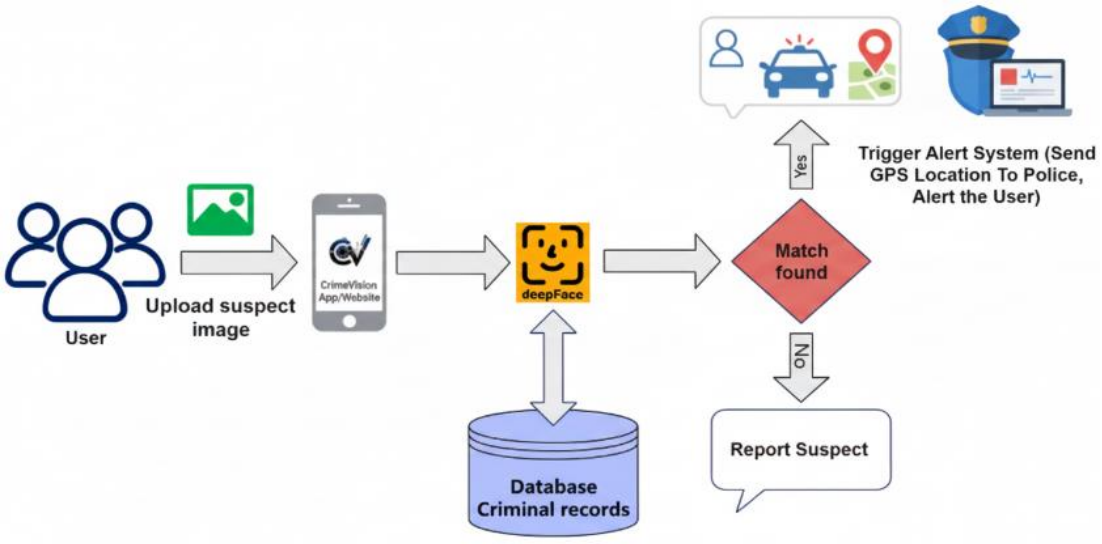


Fig 1: System Architecture

1. User Management & Authentication

This module acts as a secure entry point, ensuring only authorized users—administrators, police, and the public—access the system. It uses encrypted credentials, token-based authentication, email verification, password recovery, and multilingual support for enhanced security and accessibility.

2. Face Recognition System

The face recognition module performs automatic detection and identification using deep learning and multi-model algorithms. It includes preprocessing steps like alignment and normalization, and matches facial features through threshold-based confidence scoring to ensure accurate, reliable results.

3. Criminal Database Management

This module stores structured criminal records, including images, personal details, crime history, and

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1275

threat levels. Multiple images per individual are supported, and facial features are generated dynamically. Access is restricted to authorized law enforcement personnel.

4. Public Reporting & Image Upload

Citizens can report incidents and upload images, which are analyzed by the recognition engine. The system captures geographic coordinates and stores reports securely, while map visualization helps identify crime patterns and support investigations.

5. Real-Time Alerts & Notifications

Instant notifications are generated when a match or critical report occurs. Alerts include identity, location, and threat level, and are prioritized based on severity for fast response.

6. Maps & Location Tracking

Interactive mapping displays real-time incidents, alerts, and reports using GPS coordinates, enabling hotspot detection and strategic planning.

IV. IMPLEMENTATION:

A. Development Environment

CrimeVision is implemented as a full-stack web application. The frontend is built with React.js, Vite, and Tailwind CSS, with multilingual support through i18n language detection and local storage caching. The backend is developed using Python Flask and exposes REST APIs for authentication, scanning, reporting, and alerts. SQLite is used for operational data such as users, scans, reports, and alerts. Face recognition is implemented using DeepFace with ArcFace, and mapping/visualization uses Leaflet-based components in the frontend. The architecture is modular, separating authentication, scanning, reporting, and alert modules.

B. User Authentication and Role Management

Authentication is JWT-based. Users are primarily handled as PUBLIC and POLICE roles, with approval control for police accounts (including main-admin style privilege checks in approval paths). Passwords are securely hashed before storage. Police users must be approved before login access is granted. OTP functionality exists for password reset in backend models, and registration-time email OTP verification is handled in the frontend using EmailJS integration.

C. Image Acquisition and Preprocessing

Facial images are accepted through two API paths: multipart image upload and base64 camera capture. Inputs are validated (file/data presence and readability), then stored temporarily for processing. The recognition flow relies on DeepFace extraction and alignment rather than a custom OpenCV preprocessing pipeline with explicit grayscale or noise-reduction stages. Temporary scan files are removed after processing.

D. Face Detection and Recognition Implementation

Face detection and recognition are implemented using DeepFace with ArcFace configuration. Detection uses fallback backends (configured backend, RetinaFace, MTCNN, OpenCV) to improve robustness. For each detected face, the system performs DeepFace.find against the criminal dataset, selects the best candidate based on minimum distance, applies ambiguity checks, and uses a two-stage acceptance strategy. Strong-distance thresholding is applied for high-confidence matches, while DeepFace.verify is used for additional validation in weaker cases. Final outputs include match status, confidence score, and associated criminal metadata.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1275

E. Criminal Database Management
Criminal face references are maintained as image datasets in the filesystem, organized for DeepFace matching. Criminal profile details such as name, crime type, and risk level are retrieved from structured application data mappings. SQLite is used for storing user, report, scan, and alert records, while facial images are not stored as database BLOB embeddings in the current implementation.

F. Real-Time Alerts and Notification System
When a criminal match is detected, the backend generates alert records for the scanning user and creates scan-alert entries for police dashboards and map views when location data is available. Alerts include details such as number of faces detected, match status, and identified criminal information. EmailJS is used for OTP and transactional communication, while detection alerts are primarily delivered through dashboard and API-based alert feeds. Nearby-user proximity notifications are not currently implemented.

G. Public Reporting and Location Integration
Users can submit incident reports including images, descriptions, and geographic coordinates. Reports may be linked to authenticated users or stored as anonymous submissions. Each report follows a workflow status including PENDING, REVIEWED, VERIFIED, or REJECTED for police evaluation. Location data is visualized using Leaflet-based maps integrated with backend APIs.

H. Visualization and Dashboard System
Role-based dashboards are implemented for both public users and police/admin users. Public users can view scan history and personal alerts, while police and administrators can monitor scan alerts, review reports, access global alert feeds, and analyze system data. News updates are integrated using external APIs such as NewsData.io and TheNewsAPI within the frontend interface.

I. Data Storage and Security
SQLite is used to store core system data including user accounts, scan history, reports, alerts, news entries, and OTP records. Security mechanisms include password hashing, JWT-based authentication, protected API endpoints, and role-based authorization. Persistent logging of scans, reports, and alerts enables monitoring, auditing, and future system improvements.

V. ALGORITHM:

INPUT:
User registration/login data
Facial image (upload or live capture)
Criminal image dataset
Optional scan location (latitude, longitude)
Report data (photo, description, location)

OUTPUT:
Match result per detected face (criminal or no match)
User alert and police map alert (when match found)
Scan/report history and alert feeds

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1275

```
BEGIN

INITIALIZE Flask application, database models, JWT authentication, and DeepFace configuration (ArcFace model, RetinaFace with fallback backends)

IF user registration request THEN
   VALIDATE required fields
   STORE user with hashed password, role, and location fields

   IF role == POLICE THEN
      SET approval_status ← PENDING
   ELSE
      SET approval_status ← APPROVED
   END IF

ELSE IF user login request THEN
   VERIFY email and password

   IF role == POLICE AND approval_status ≠ APPROVED THEN
      DENY login
   ELSE
      GENERATE JWT token
      RETURN user profile and role
   END IF
END IF

ACCEPT scan image (multipart upload or base64 capture)

SAVE image temporarily

CHECK image validity

DETECT faces using DeepFace.extract_faces with backend fallback (retinaface, mtcnn, opencv)

IF no face detected THEN
   RETURN "NO_FACE_DETECTED"
END IF

FOR each detected face DO
   ALIGN and CROP face

   embedding ← GENERATE using DeepFace (ArcFace)

   matches ← DeepFace.find (embedding, criminal dataset)
```

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1275

```
best_match ← SELECT minimum distance

   IF distance ≤ strong_threshold THEN
      identified_person ← MATCHED_CRIMINAL
   ELSE
      RUN DeepFace.verify (top 5 candidates)
      IF verification passes THEN
         identified_person ← MATCHED_CRIMINAL
      ELSE
         identified_person ← NO_MATCH
      END IF
   END IF

   STORE result for each face
END FOR

ENRICH matched results with criminal details

RETURN faces_detected, matches_found, match_details

DELETE temporary image

STORE scan data in scan_history:
user_id, faces_detected, matches_found, status, match_details, location

IF match found THEN
   CREATE user alert (CRIMINAL_DETECTED)

   IF location available THEN
      CREATE scan_alert for police dashboard/map
   END IF
END IF

IF report submitted THEN
   VALIDATE description, type, location, and photo
   SAVE report image
   STORE report with status ← PENDING

   IF authenticated user THEN
      ATTACH user_id
   ELSE
      STORE as anonymous report
   END IF
END IF
```

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1275

```
FOR each report reviewed by police DO
   UPDATE status (REVIEWED / VERIFIED / REJECTED)

   IF applicable THEN
      CREATE user alert
   END IF
END FOR

GENERATE user alert feed, police scan alerts, and global alerts aggregation

DISPLAY alerts on dashboard and map interface

END
```

VI. RESULTS:

The CrimeVision system demonstrated efficient and accurate facial recognition across varied lighting conditions and image qualities. The platform successfully matched faces with the criminal database using high-confidence thresholds, generating timely alerts for law enforcement. Public reports were correctly geo-tagged and visualized on the interactive map, improving situational awareness. Role-based dashboards functioned smoothly, providing clear access to records, alerts, and reports. Overall, the system delivered reliable performance, faster identification, and improved coordination between citizens and police.

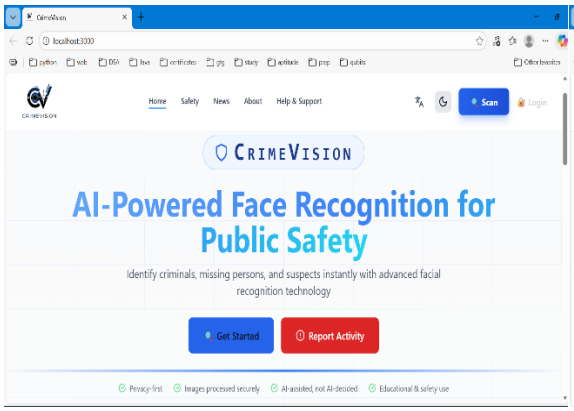


Fig 2: Home Page Interface (Light Mode)

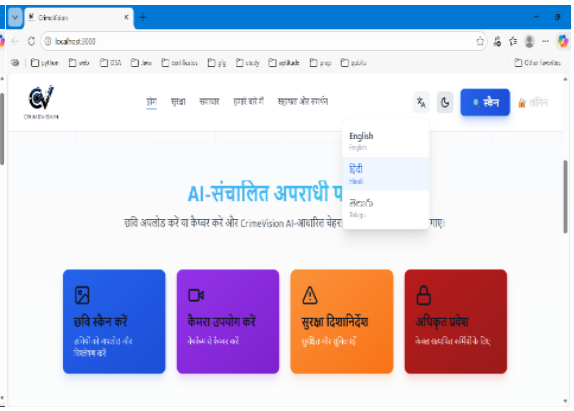


Fig 3: Home Page (Hindi Interface)

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1275

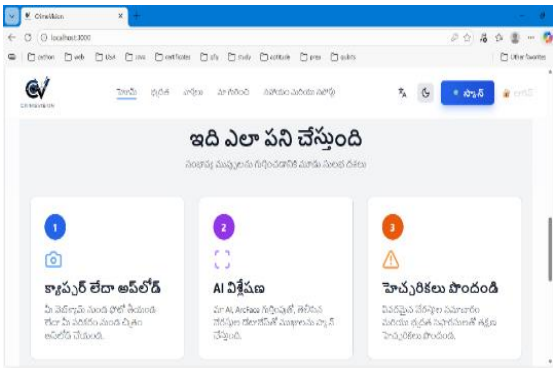


Fig 4: Home Page (Telugu Interface)

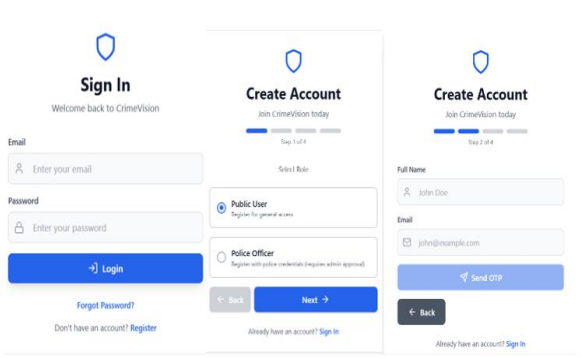


Fig 5: Sign-in and Registration Screen (Mobile View)

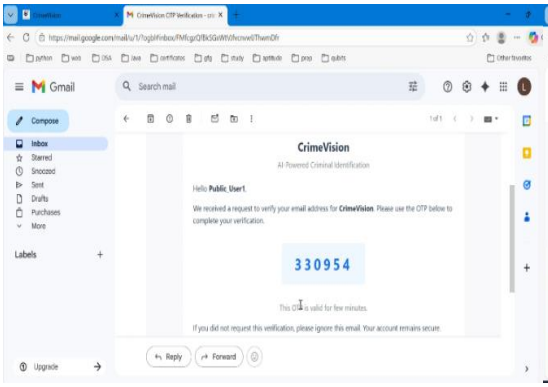


Fig 6: OTP Verification Email Template

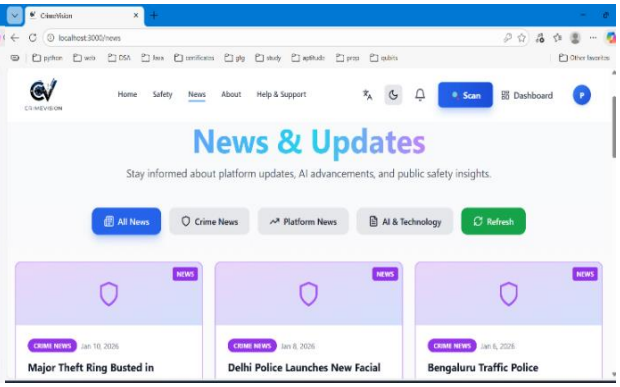


Fig 7: News and Update Section

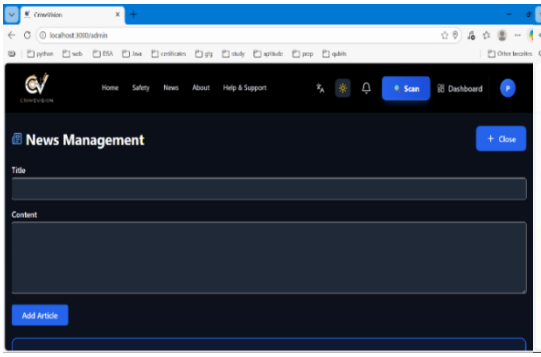


Fig 8: News Management Panel

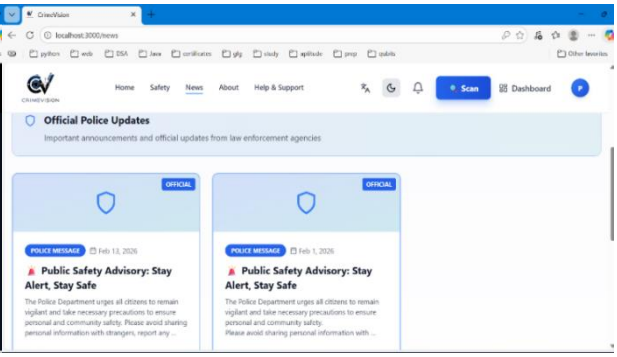
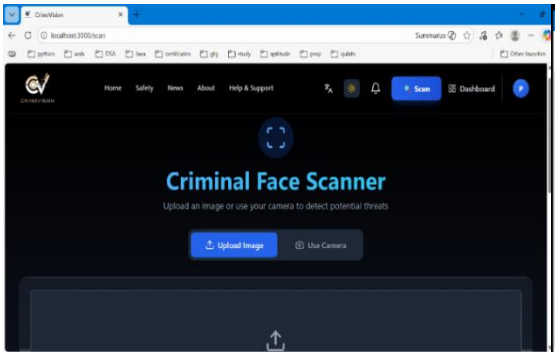
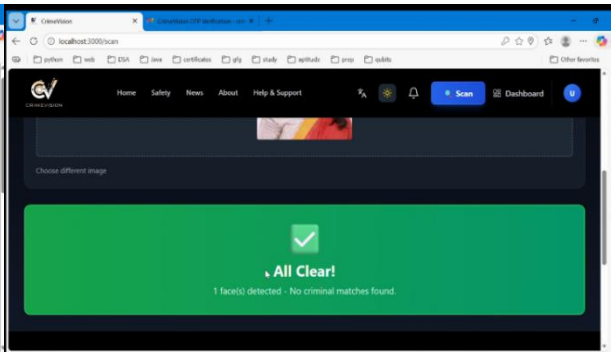


Fig 9: News Page Displaying Official Police Messages





Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1275

Fig 10: Face Scan and Image Upload Interface

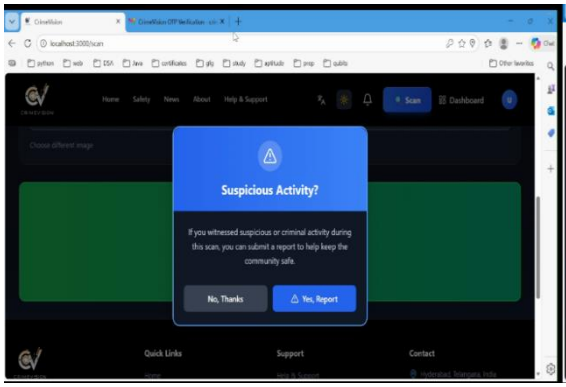


Fig 11: Face Recognition Result (Clean Record)

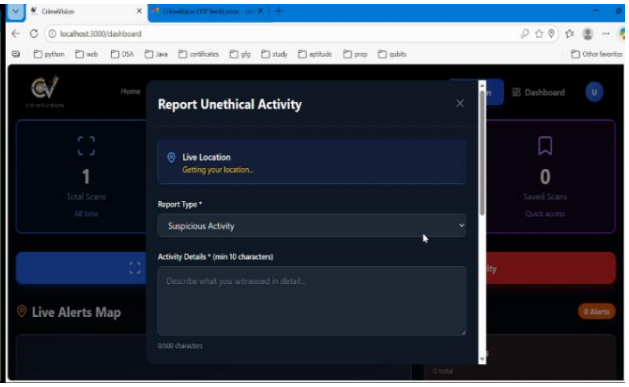
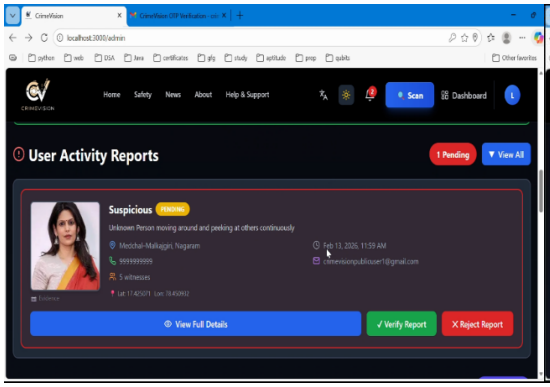


Fig 12: Criminal Reporting Form

Fig 13: Report Submission Confirmation



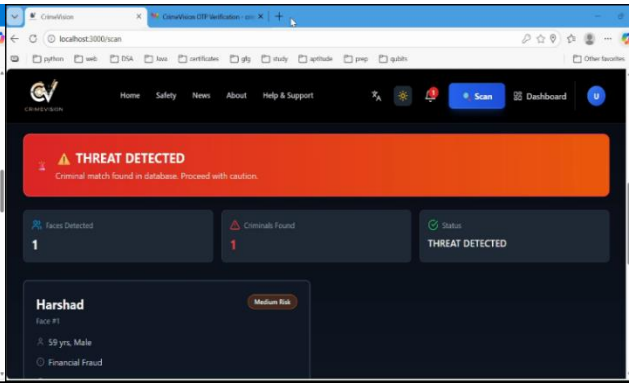
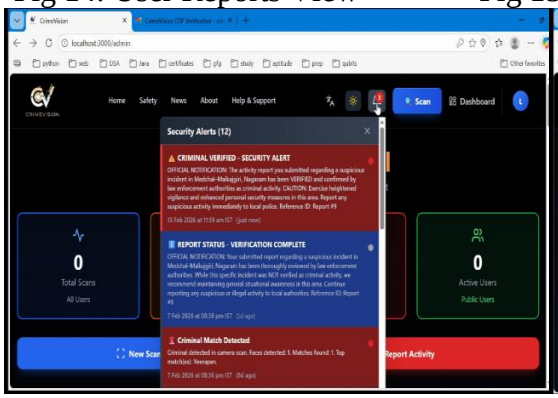


Fig 14: User Reports View

Fig 15: Face Recognition Result (Criminal Identified)



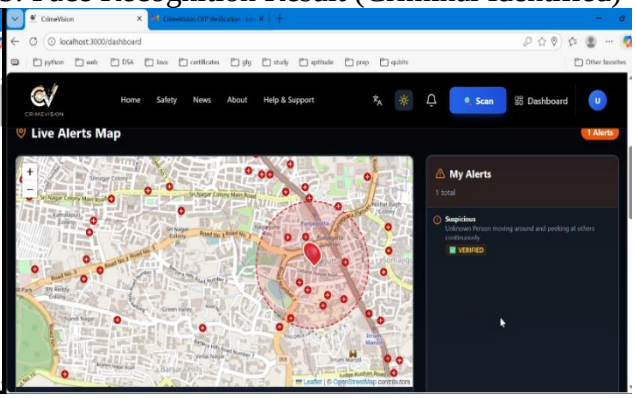


Fig 16: System Alerts Interface

Fig 17: Live Alerts Interactive Map

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1275

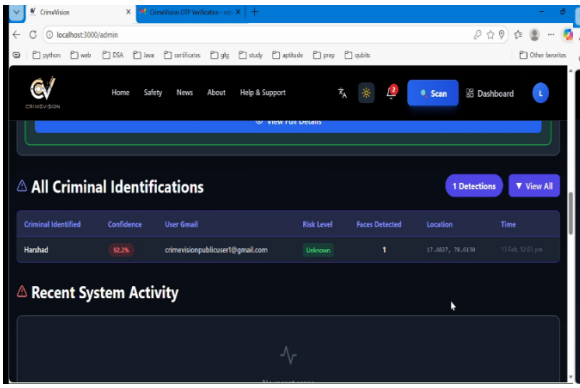


Fig 18: Identified Criminal Details

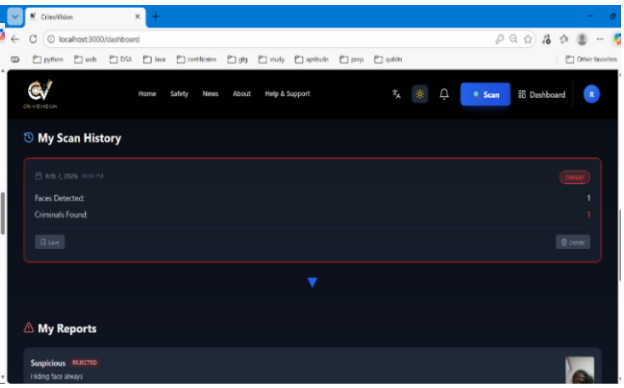


Fig 19: Scan and Reports History(User Dashboard)

VII.CONCLUSION:

The development of CrimeVision represents a notable step forward in applying artificial intelligence, facial recognition, and data analytics to improve criminal identification and public safety. The system uses deep learning–based face recognition combined with computer vision techniques to accurately match uploaded images or live camera captures with a structured criminal database in a short time. By reducing dependence on manual processes and minimizing human error, it provides a faster and more reliable identification approach. Additional features such as multi-model face detection, GPS-based geo-tagging, interactive map visualization, and instant alert notifications enhance situational awareness for law enforcement agencies. Furthermore, the platform supports collaboration between authorities and citizens through role-based access, secure authentication, multilingual support, and real-time reporting, creating an efficient and technology-driven framework for modern crime prevention technology.

REFERENCES:

[1] Wu, X., & Zhang, X. (2016). Automated inference on criminality using face images. arXiv preprint arXiv:1611.04135, 4.

[2] Balamurugan, A. & Gowtham, N. & Atchara, U. & Kannan, M. & Prasad, R.. (2020). Surveillance using Face Recognition in Smart Cities. International Journal of Innovative Technology and Exploring Engineering. 9. 2042-2047. 10.35940/ijitee.F3582.049620.

[3] Sivanagireddy, K., Jagadeesh, S., & Narmada, A. (2024). Identification of criminal & non-criminal faces using deep learning and optimization of image processing. Multimedia Tools and Applications, 83(16), 47373-47395.

[4] Divya, S., Jeevika, T., & Geo, A. A. (2025, January). Innovative Approaches to Criminal Identification Using Real Time Facial Recognition. In 2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI) (pp. 1694-1700). IEEE.

[5] Rani, R., Napte, K., Kumar, S., Pippal, S. K., & Dalsaniya, M. (2025). Face Recognition System for Criminal Identification in CCTV Footage Using Keras and OpenCV. Ingénierie des Systèmes d'Information, 30(3).

[6] Cuellar, M., Kiu, H., & Mehrotra, A. (2025). Accuracy and Fairness of Facial Recognition Technology in Low-Quality Police Images: An Experiment With Synthetic Faces. arXiv preprint arXiv:2505.14320.

[7] Beulah Benslet, S. S., & Parameswari, P. (2024). Enhancement of Criminal Facial Image Using Multistage Progressive V-Net for Facial Recognition by Pixel Restoration. EAI Endorsed Transactions on Scalable Information Systems, 11(3).

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1275

[8] Simmler, M., & Canova, G. (2025). Facial recognition technology in law enforcement: Regulating data analysis of another kind. Computer Law & Security Review, 56, 106092.
[9] Robles, P., Mallinson, D. J., Best, E., Devaney, C., & Azevedo, L. (2025). Global perspectives on regulating facial recognition technology utilization for criminal justice arrests.