Published by :
http://www.ijert.org

Detecting of Criminals using Facial Recognition

Ananthi B
Assistant Professor ,Vivekanandha College of Engineering for Women,Tiruchengode,Tamilnadu (India),

Priyanga K, Sasmitha S, Sowmiya S,Dhanya V
UG Student Of Vivekanandha College of Engineering for Women,Tiruchengode,Tamilnadu (India),

***Abstract*— An advanced facial recognition system designed to enhance law enforcement capabilities in criminal identification and management. By integrating cutting-edge computer vision algorithms and real-time image processing, the system automates the identification of suspects through a seamless workflow that includes face detection, feature encoding, and database interaction. With the vast amounts of visual data generated by surveillance cameras, this technology addresses the challenge of manual data analysis, offering rapid and accurate matching of faces with known criminal records. Beyond criminal identification, the system supports border security, access control, and forensic investigations. The paper also examines ethical considerations, including privacy and potential biases, advocating for responsible use within legal frameworks. This system represents a significant leap forward in policing technology, promising to improve public safety, streamline investigative processes, and act as a deterrent to criminal activities.**

***Keywords*— Facial Recognition Technology, Computer Vision Algorithms, Real-Time Image Processing, Face Detection, Facial Feature Encoding, Database Management, Surveillance Data Analysis, Deep Learning, Neural Networks, Biometric Identification, Criminal Face Recognition, Face Matching Algorithms, Privacy Safeguards, Ethical Considerations, Bias Mitigation**

I. INDRODUCTION

Facial recognition technology has become a transformative asset in modern law enforcement, providing unprecedented capabilities for identifying and tracking individuals. The rapid evolution of computer vision algorithms and hardware has significantly enhanced the accuracy, reliability, and scalability of facial recognition systems, revolutionizing law enforcement practices.

This paper introduces an advanced facial recognition system designed to improve criminal identification and management. Utilizing cutting-edge facial recognition algorithms, real-time image processing, and robust database management, the system aims to streamline the capturing, encoding, recognition, and storage of facial data for known criminals. The proliferation of surveillance cameras in public and private spaces has generated extensive visual data, which, if managed manually, can be time-consuming and labor-intensive. Facial recognition technology addresses this challenge by automating the identification process, enabling law enforcement agencies to efficiently and accurately match faces from surveillance footage with known criminal databases.

The system comprises several interconnected modules, including face detection, facial feature encoding, facial recognition, database interaction, and user interface components. By integrating these modules into a cohesive architecture, the system enhances investigative capabilities and public safety. Beyond criminal identification, the system has practical applications in border security, access control, and forensic investigations, demonstrating its versatility and scalability for diverse law enforcement scenarios.

In addition to its technical capabilities, this paper explores the ethical considerations of deploying facial recognition technology. Issues such as privacy rights and potential biases are examined, with a focus on responsible use within legal frameworks. The facial recognition system represents a significant advancement in law enforcement technology, offering a powerful tool to improve public safety, streamline investigative processes, and act as a deterrent to criminal activity. As technology evolves, the integration of facial recognition will continue to shape the future of policing and security .

II. LITERATURE REVIEW

Criminal Identification for Low Resolution Surveillance

S. P. Patil's model utilizes the Tiny Face Detector for real-time face recognition in surveillance, efficiently creating 128-dimensional embeddings from detected faces and landmarks. Trained on diverse criminal datasets, it processes video frames, compares extracted features to stored data, and saves matches as PNGs. A Django-based portal assists administrators in reviewing results. The literature survey focuses on techniques for low-resolution criminal identification, including image enhancement, feature extraction, and deep learning methods like CNNs to address challenges with blurry images.

Criminal identification system using deep learning
D. Nagamallika's criminal face identification system uses MTCNN, FaceNet, and OpenCV to detect and process facial data. It registers new criminals, preprocesses images, extracts features, and matches them to identify suspects, sending SMS notifications to authorities upon a positive match. The literature survey highlights deep learning techniques, including CNNs and RNNs, and discusses advancements in preprocessing, feature extraction, and model optimization to tackle challenges such as resolution, noise, and occlusion in surveillance systems.

Criminal identification system using real-time image processing
A. S. Tiwari, Ghotekar Shubhangi S, Ghotekar Ashwini S, Manjare Mayuri A et.al. Facial recognition system for surveillance preprocesses images to eliminate noise and uses Haar cascades for feature extraction. It compares these features against databases, including citizen records and watch lists, to identify potential criminals, deeming unmatched individuals as innocent. However, these systems raise privacy and ethical concerns regarding misuse and threats to personal freedoms.

A Machine Learning and Computer Vision Approach to Crime Prediction and Prevention

Pro.Banker A et.al. The paper propose integrating technologies like Sting Ray, body cams, and facial recognition with neural and Bayesian networks to create a universal police officer. This system autonomously detects threats such as burglary and terrorism to enhance urban security. The literature survey examines machine learning and computer vision for crime prediction, focusing on algorithms for analyzing surveillance footage and addressing efficacy, challenges, and ethical concerns.

Criminal recognition system using facial detection and recognition
N. Shah, Nandish Bhagat, Manan Sha et.al. The literature review discusses a real-time facial recognition system for identifying criminals from video streams. It integrates citizen databases and watch lists, employing image preprocessing, Haar cascades for feature extraction, and the LBPH recognizer. This enhances video surveillance and public safety, with features for cropping faces, searching databases, and sending SMS alerts to improve response times.

Security and Accuracy of Fingerprint-Based Biometrics
The paper analyzes 42 research articles on the security and accuracy of fingerprint-based biometric systems, addressing vulnerabilities and proposing countermeasures. Despite advancements, recognition accuracy under challenging conditions is still an issue. Future research aims to integrate deep learning for improved accuracy and develop lightweight algorithms for mobile biometrics. The survey evaluates fingerprint recognition methods, authentication techniques, anti-spoofing advancements, and applications in law enforcement and identity verification.

Real-Time Object Detection System with Multi-Path Neural Networks
Heo, Sungjun Cho, Youngsok Kim et.al. The paper presents a real-time object detection method using Deep Neural Networks (DNN), showcasing superior accuracy compared to traditional algorithms. While achieving high accuracy in detecting object locations and types, the system also meets real-time requirements. This advancement is vital for dynamic environments like autonomous driving, surveillance, and robotics, where timely object detection enhances decision-making and safety.

Joint Face Alignment and 3D Face Reconstruction with Application to Face Recognition
F Liu, Q Zhao, X Liu and D Zeng , et.al. The paper presents a novel method for joint face alignment and 3D face reconstruction, focusing on separating identity and expression components. Their process includes landmark updating, shape refinement, and visibility estimation, demonstrating superior accuracy and efficiency on benchmark datasets. The survey also explores how integrating facial landmark detection with 3D modeling enhances recognition accuracy and robustness using deep learning and geometric constraints.

Facial Expression Recognition in the Wild Using Multi-level Features
Y. Li, G. Lu, J. Li, Z. Zhang and D. Zhang et.al The paper present the SPWFASE model for facial expression recognition, utilizing SPA Net for patch-level features and WFA Net for global features. These are combined into an extended vector and processed for expression prediction using focal loss to handle imbalanced data. The paper details the model architecture and techniques, enhancing recognition accuracy.

Face Manipulation Detection Through Ensemble of CNN
N. Bonettini , Cannas, Edoardo & Mandelli, Sara & Bondi, Luca& Bestagini, Paolo & Tubaro, Stefano et.al The paper proposes a method for detecting video face manipulation using an ensemble of CNNs, specifically focusing on differentiating genuine and fake faces in video frames. It utilizes EfficientNet models, known for their accuracy and efficiency, and incorporates attention mechanisms and siamese training strategies to improve feature extraction. The architecture centers on the EfficientNetB4 model with attention, and the paper discusses various training strategies. Comparative analyses with other state-of-the-art methods demonstrate the effectiveness of this approach, contributing significantly to the field of video face manipulation detection.

III. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

Existing criminal face recognition systems utilize deep learning algorithms and facial recognition technology to identify suspects by analyzing unique facial features such as eye spacing, nose shape, and jawline. These systems are typically trained on extensive databases of facial images collected from sources like surveillance footage, mugshots, and social media. Advanced algorithms handle variations in lighting, expression, and pose to enhance accuracy. Some systems integrate additional data, including criminal records and fingerprints, to improve identification precision. Real-time monitoring capabilities alert authorities when known criminals are detected, aiding in proactive law enforcement. Despite these advancements, concerns about privacy, algorithmic bias, and false positives highlight ongoing ethical and legal debates. Continuous research is crucial to address these issues and improve system reliability and fairness.

3.2 DISADVANTAGES

Facial recognition technology raises significant concerns, including biases that disproportionately affect minorities and women, leading to wrongful arrests and systemic discrimination in the criminal justice system. It also poses privacy risks, enabling tracking of individuals without consent and fostering mass surveillance that undermines personal freedoms. Furthermore, the potential for misuse by governments, particularly authoritarian regimes, threatens citizens' rights to free speech and assembly. Security vulnerabilities, such as susceptibility to hacking and spoofing, add another layer of risk, while complex legal and ethical questions surrounding consent, data protection, and individual rights highlight the inadequacies of current regulations in addressing these challenges.

3.3 PROPOSED SYSTEM

Our proposed face recognition system represents a cutting-edge advancement in biometric technology, designed to meet diverse industry needs with high accuracy from facial images or video streams. It integrates sophisticated algorithms for facial feature extraction, pattern recognition, and machine learning, while prioritizing privacy with robust encryption and access control. The system's versatility makes it suitable for security enforcement, access management, and personalized services, promising significant impacts for businesses and individuals. The literature survey complements this by exploring real-time object detection through multi-path neural networks, focusing on enhancements in detection speed and accuracy via feature fusion, attention mechanisms, and efficient network designs. This survey discusses benchmark datasets, evaluation metrics, and future directions, while the proposed facial recognition system incorporates advanced computer vision and deep learning techniques, including real-time monitoring, database integration, and ethical considerations like privacy protection and transparency for responsible law enforcement use.

3.4 ADVANTAGES

Our facial recognition system combines state-of-the-art algorithms and deep learning to deliver high accuracy and real-time identification while minimizing false positives and negatives. It is highly scalable, adaptable for various applications such as security and access control, and offers customizable features to meet specific needs. Robust security measures, including encryption and data anonymization, ensure user privacy and compliance with regulations. The system is cost-effective, leveraging open-source technologies to provide advanced performance at competitive prices. Additionally, it is continuously updated to remain relevant to emerging technologies and supports remote access for law enforcement, enhancing investigations and border security while identifying repeat offenders.

IV. SOFTWARE DESCRIPTION

4.1 FRONT END:

HTML (Hypertext Markup Language) is the foundational language for structuring content on the web, using tags to define elements like headings, paragraphs, and multimedia. It allows for the integration of graphics through the <img> tag, enhancing visual appeal and user engagement. HTML documents consist of a head section for metadata and a body section for content, making it essential for web development.

CSS (Cascading Style Sheets) complements HTML by controlling the visual presentation and layout of web pages. It separates content from design, allowing developers to define styling aspects such as color, font, and spacing through a set of rules. CSS enables responsive designs using techniques like flexbox and grid, and supports media queries for adapting styles based on device type. Together, HTML and CSS create visually cohesive, engaging web interfaces, improving the overall user experience and usability of websites and applications.

4.2 ALGORITHM:

Our face recognition system employs a set of advanced algorithms to ensure precise and reliable identification of individuals from facial images or video streams. These algorithms are integral to various stages of the face recognition pipeline, including detection, feature extraction, encoding, clustering, and classification. Here’s an overview of the key algorithms utilized:

LBPH (Local Binary Patterns Histograms): LBP generates binary codes for each pixel by comparing it with neighboring pixels' intensities, creating histograms that capture the distribution of these patterns. These histograms serve as feature vectors representing unique facial characteristics. For recognition, LBPH compares these vectors with a database to identify and classify faces.

Haar Cascade Classifier: Haar features use rectangular filters to analyze pixel intensity variations for face detection.

The classifier is trained on images of faces and non-faces, learning to differentiate between them. It employs a cascade of classifiers to efficiently filter out non-face regions, scanning images at various scales and positions to identify potential face areas.

DBSCAN (Density-Based Spatial Clustering of Applications with Noise): DBSCAN groups data points based on density, identifying clusters as high-density areas separated by lower-density regions. It defines core points using parameters like epsilon (ε) and minPts, expanding clusters from these points by adding neighboring points within the ε-radius. Points not in dense regions are classified as noise, making the algorithm robust against outliers.

V. PROJECT DESCRIPTION

5.1 PROBLEM DEFINITION:

Current facial recognition systems face significant limitations due to their reliance on traditional methodologies, resulting in reduced accuracy and efficiency, particularly in real-time surveillance and crowded environments. Basic algorithms struggle to perform effectively, leading to constrained capabilities. Additionally, the collection and analysis of biometric data raise privacy and data security concerns, potentially infringing on personal freedoms and exposing vulnerabilities. This underscores the need for more advanced and secure solutions in facial recognition technology.

5.2 Module Description:

Our face recognition system comprises several key modules, each with specific functions. The 'main.py' file launches the Flask web server defined in 'server.py', which manages HTTP requests and renders HTML templates. 'home.py' handles the user interface and interactions. For facial detection and recognition, 'facedetection.py' utilizes OpenCV methods, such as Haar cascades. 'register.py' captures images for new registrations, while 'handler.py' and 'dbhandler.py' manage database interactions for data insertion and retrieval. 'encoding.py' encodes facial features into numerical representations using libraries like 'face_recognition' or OpenCV. Finally, 'finalencoding.py' clusters these encodings to group similar faces, enhancing identification. Each module plays a crucial role in the face recognition pipeline, ensuring high accuracy and efficiency.

5.2 Input Design:

The input design for your system involves various Python files, each contributing to different aspects of face registration, recognition, and data handling. These files include modules for registering criminals by capturing their images, detecting faces, and saving relevant information. Additionally, there are components for training face recognition models, encoding facial features, and performing clustering on facial encodings.

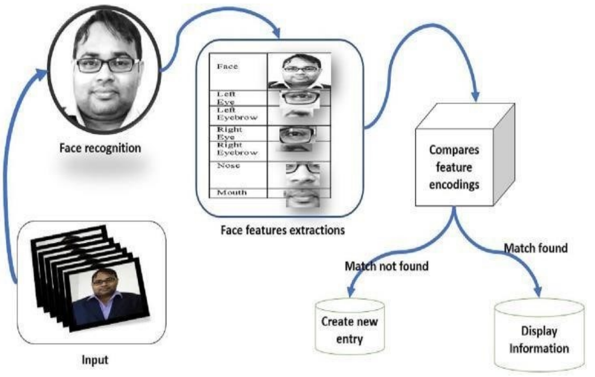
Data insertion into a database is facilitated by one module, while another focuses on preprocessing images or video streams before further processing. Utility functions are provided in a separate file to aid in common tasks across multiple modules.

5.4Output Design:

The output design of the facial recognition system includes visual representations of recognized faces, such as image montages, allowing users to validate results visually. It features structured storage for face encodings and metadata, ensuring organized and accessible information. User feedback mechanisms, like console messages and graphical interfaces, keep users informed about the recognition process, errors, and necessary actions, contributing to an intuitive experience.

For a system aimed at detecting criminals, key considerations include compliance with privacy laws and obtaining consent during data acquisition. Robust algorithms must accurately identify individuals under various conditions, and integration with criminal record databases is essential for verification. The system should incorporate machine learning to enhance recognition capabilities and prioritize transparency through audit trails. Ethical considerations, including preventing misuse and bias, are critical, necessitating regular evaluations and bias assessments to mitigate potential harm.

5.5 System Diagram:



The first step is to locate and isolate faces in an image or video frame using advanced algorithms that analyze visual data based on characteristics like color, texture, and shape. Once detected, distinguishing features such as eye size and shape, distance between facial landmarks, and overall structure are extracted and converted into mathematical representations known as face embeddings. These features are then compared against a database of known faces, which may include previously captured images, with the algorithm calculating similarity between the facial features.

VI. SYSTEM TESTING AND IMPLEMENTATION

6.1 System Testing:

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies, and/or a finished product. It is the requirement.

6.1.1 Unit Testing:

Unit testing involves designing test cases to validate that program logic functions correctly and that inputs produce valid outputs. It assesses all decision branches and internal code flow to ensure the software meets requirements and user expectations without failures. Each test type addresses specific applications and is conducted after completing an individual unit, before integration. As a form of structural testing, unit tests rely on knowledge of the code's construction and are invasive. They perform basic tests at the component level, ensuring that each unique path of a business process aligns with documented specifications, with clearly defined inputs and expected results

6.1.2 Integration Testing:

Integration tests evaluate whether integrated software components function together as a single program. These tests are event-driven and focus on the outcomes of screens or fields. They demonstrate that, while individual components may pass unit tests, their combination is correct and consistent. Integration testing specifically aims to expose issues that arise from the interaction of components.

6.1.3 Functional Testing:

Functional tests systematically demonstrate that functions meet specified business and technical requirements, system documentation, and user manuals. They focus on organizing tests around key functions, business process flows, data fields, and predefined processes.

System testing ensures the entire integrated software system meets requirements, testing configurations for known and predictable results. It emphasizes process descriptions and integration points.

White Box Testing involves testing with knowledge of the software's inner workings, allowing access to areas not reachable through black box testing. In contrast, Black Box Testing treats the software as a "black box," where tests are conducted without knowledge of its internal structure, using definitive documents like specifications for guidance.

Unit testing is typically part of the code and unit test phase of the software lifecycle, though it can also be conducted as a distinct phase.

6.2. System Implementation:

To implement a facial recognition system for detecting criminals, several key steps are involved:

Data Collection: Gather a diverse dataset of facial images, including both criminal and non-criminal individuals, to avoid bias.

Preprocessing: Clean and preprocess the images by resizing, normalizing, and aligning them for consistency.

Feature Extraction: Use techniques like Convolutional Neural Networks (CNNs) to extract discriminative features from the facial images.

Training: Train the model with preprocessed images, adjusting parameters to minimize the difference between predicted and actual labels (criminal/non-criminal).

Testing and Evaluation: Assess the model's performance using a separate test dataset, measuring accuracy, precision, recall, and F1-score.

Additionally, store high-quality images of known criminals in a database. Position surveillance cameras in key locations to capture faces as individuals pass by. The software compares these faces against the database, generating alerts if a match is found, notifying authorities of potential wanted individuals.

VII. CONCLUSION AND FUTURE WORK

7.1 CONCLUSION:

In conclusion, facial recognition technology holds promise in aiding law enforcement agencies in detecting and identifying criminals. By analyzing facial features and comparing them to existing databases, authorities can potentially track down suspects more efficiently. However, it's crucial to address concerns regarding accuracy, privacy, and potential biases to ensure fair and just outcomes. Continued research and development in this field are essential to harnessing the full potential of facial recognition while mitigating its drawbacks.

7.2 FUTURE WORK:

Current facial recognition systems face limitations due to their reliance on traditional methodologies, often lacking accuracy and efficiency, particularly in real-time surveillance. Future efforts in this project will focus on enhancing facial recognition capabilities to include features beyond identifying criminal names, such as recognizing and classifying attributes like age, gender, emotions, and behavioral patterns. We aim to implement advanced machine learning and deep learning algorithms for improved accuracy and robustness in facial analysis. Additionally, we plan to integrate real-time surveillance capabilities and develop a user-friendly interface for seamless interaction. Scalability and compatibility will also be prioritized to ensure the system adapts to diverse environments and requirements.

7.3 Outputs:

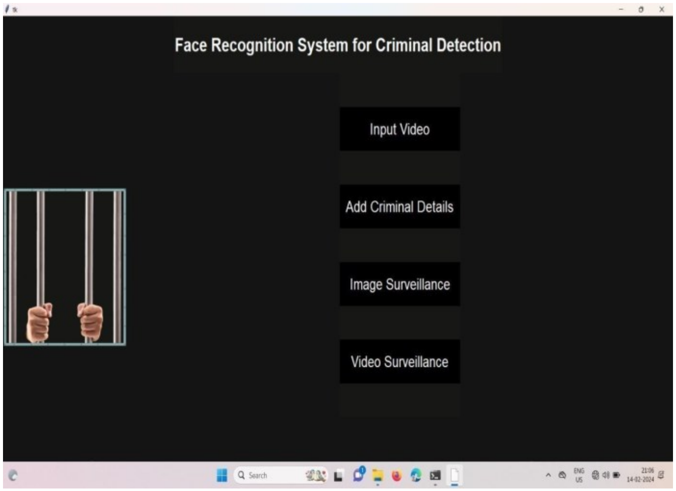


FIG 7.3.1 Face recognition system for criminal detection

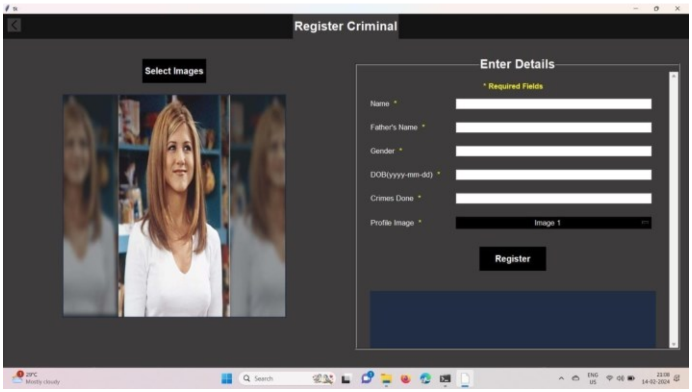


FIG 7.3.2 Register criminal

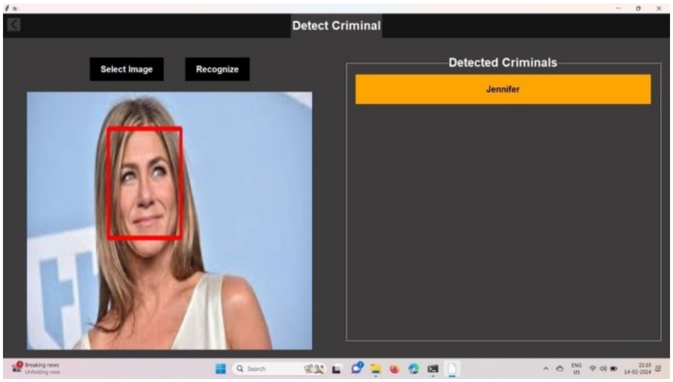


FIG 7.3.3 Detected criminal

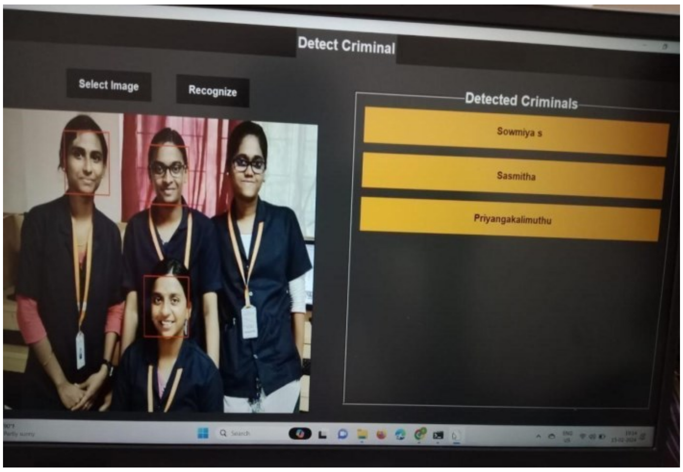


FIG 7.3.4 Detected criminal in real time

REFERENCES

[1] 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.

[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] 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,’’ *Criminal. Public Policy*, vol. 18, no. 1, pp. 135–159, Feb. 2019.

[4] 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,’’ *Criminal. Public Policy*, vol. 18, no. 1, pp. 135–159, Feb. 2019.

[5] Hyun-bin Kim, Nakhoon Choi, Hye-jeong Kwon, and Heeyoul K, “Surveillance System For Real Time High Precision Recognition Of Criminal Faces From Wild Videos,” 2 June 2023.

[6] J. T. Pickett, C. Mancini, and D. P. Mears, ‘‘Vulnerable victims, monstrous offenders, and unmanageable risk: Explaining public opinion on the social control of sex crime,’’ *Criminology*, vol. 51, no. 3, pp. 729–759, Aug. 2013.

[7] 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. 2022.

[8] 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.

[9] M. Zebrowitz LA, Montepare JM. Social psychological face perception: why appearance matters. *Soc Personal Psychol Compass*. 2008;2(3):1497–517.

[10] N. Tamilarasi, P., and R. Uma Rani, “Diagnosis of Crime Rate against Women using k-fold Cross Validation through Machine Learning,” 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC). IEEE, 2020.

[11] P. Kim, Suhong, et al. “Crime analysis through machine learning,” 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, 2018.

[12] R. Chackravarthy, Sharmila, Steven Schmitt, and Li Yang. “Intelligent crime anomaly detection in smart cities using deep learning,” 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC). IEEE, 2018.

[13] S. Viola and M. Jones, “Robust Real-time Object Detection,” *International Journal of Computer Vision*, vol. 57, no. 2, pp. 137–154, 2002.

[14] T. Apoorva, Ramesh B, and Varshitha M. R, “Automated criminal identification by face recognition using open computer vision classifiers,” Third International Conference on Computing Methodologies and Communication (ICCMC 2019).

[15] Z. Nurul Azma Abdullah, Md. Jamri Saidi, and Nurul Hidayah Ab Rahman, “Face recognition for criminal identification: An implementation of principal component analysis for face recognition,” The 2nd International Conference on Applied Science and Technology 2017 (ICAST’17).