Real-Time Criminal Face Detection: The Next Era of High-Precision Surveillance

[1]Dr. A. V. Markad, [2]Mr. Sanket Dongare, [3]Mr. Prathamesh Mundada, [4]Mr. Shubham Kulange, [5]Mr. Tushar Argade, [6]Ms. Harshada Kale

Department of IT Engineering
Amrutvahini College of Engineering Sangamner
India.

Abstract-
Today, people are worried about criminals, especially those who have harmed children, committing more crimes. To prevent them from getting close to places like schools and childcare centers, governments and organizations are using cameras and extra staff for watching. But just having people look at the pictures and checking is not enough. We need a clever system that can quickly look at the pictures and decide if there are criminals in them. This paper talks about a new system that uses special technology to recognize faces. This system watches videos from cameras and can identify the faces of criminals in real-time. When it sees a criminal's face, it alerts the right people who can help. How does it work? First, the system makes the pictures a bit smaller so it can find faces faster. Then, it follows these faces over time to make sure it is really the same person. It also gives a number to show how confident it is in recognizing the person's face. This number is based on how well it has been watching the face. The final number thinks about how sure the system is and how much the face looks like other faces of known criminals. This way, even if the security people miss something, this system can catch it early, especially in places where bad things might happen. The good things about this system are that it can quickly look at camera pictures, even if they are a bit smaller. It can accurately tell who the criminals are by watching their faces closely and not making mistakes. It also solves a problem when there are many faces to look at. The system improves over time by adding up its scores for decisions. In tests, the system did well, getting things right about 90% of the time, and it was even better than other similar systems. This system could be super helpful for finding criminals and keeping important places safe, so bad things are prevented.

Keywords: **Crinal Detection, Neural network Deep learning Algorithm-task.**

Published in IJIRMPS (E-ISSN: 2349-7300), Volume 12, Issue 2, March- April 2024

I. INTRODUCTION

Wrongdoings and crimes are expanding step by step and there could be no appropriate standards to look, recognize, distinguish, and foresee these hoodlums. Regardless of different observation cameras in various regions still, wrongdoings are at a pinnacle. The police examination office can't effectively distinguish the crooks in time. In any case, in numerous nations for public and confidential security, the commencement of safety advances has been utilized for criminal recognizable proof or acknowledgment with the assistance of impression ID, finger impression ID, facial acknowledgment, or in view of other dubious action discoveries through reconnaissance cameras. Notwithstanding, there are restricted mechanized frameworks that can distinguish the hoodlums exactly and get the exact or exact closeness between the recorded film pictures with the crooks that as of now are accessible in police criminal records.

To make the police examination division more compelling, this exploration work presents the plan of a robotized criminal recognition framework for the expectation of lawbreakers. The proposed framework can

anticipate lawbreakers or potential outcomes of being criminal in view of Lombroso's Hypothesis of Criminal science about conceived crooks or the people who seem to be hoodlums.

A profound learning-based facial acknowledgment approach was utilized that can identify or foresee any individual whether he is criminal, or not and that can likewise give the chance of being criminal. For preparing, the ResNet50 model was utilized, which depends on CNN and SVM Classifiers for include extricating from the dataset. Two different marked based datasets were utilized, having various lawbreakers and non-hoodlums pictures in the data set. The proposed framework could productively help the researching officials in reducing the suspects' pool.

Wrongdoing represents a serious danger to mankind. An activity or exclusion that comprises an infraction and is endorsed by the law is alluded to as a wrongdoing. While certain wrongdoings cause the least harm, some could bring about a casualty. Wrongdoings don't have a specific spot of concern since they can happen anyplace, from modest communities to significant city. It is urgent to track down a speedier answer for this issue to safeguard our general public from all dangers. To distinguish dubious direct and shield the unprotected, the police force should continually notice individuals' activities and conduct.

Predictive analytics leverages data and machine learning algorithms to analyse past crime patterns and identify potential hotspots for future criminal activities. This proactive approach enables law enforcement to allocate resources more strategically, allowing for faster response times and a more effective crime deterrence.

Furthermore, the utilization of face recognition technology has proven invaluable in enhancing criminal identification. It can help identify suspects, track their movements, and match them to known criminal databases. By doing so, it enables law enforcement to close in on criminals more rapidly and with higher precision.

II. LITRATURE SURVAY

1. This undertaking plunges into the subject of facial acknowledgment and facial location in a computerized correspondences framework. Face acknowledgment is an innovation that is broadly utilized today which carries different advantages to society. Facial acknowledgment varies from facial discovery in the perspective that facial identification just finds and recognizes the current face/s in a picture while, in facial acknowledgment, the PC tracks down the face/s present in a subject and can recognize the face from an example of various countenances. This exploration centers around the execution of both a facial acknowledgment framework and a facial identification framework in MATLAB. This examination would utilize the different imaging tool compartments accessible in the program and would be decided on its capacity to distinguish and perceive an example in each data set precisely. Moreover, this framework ought to have the option to make and to peruse an information base of various faces.[1]

2. We understand that a person's face is a unique and essential component of their body that sets them apart. We can use it to track the personality of a criminal in this way. As a result of technological advancements, CCTV is installed in many public areas to capture criminal activity. The lawbreaker face recognition system can be used with the newly apprehended faces and criminals' photographs that are available at the police headquarters. This article presents a programmed criminal ID framework that the Police Division can use to upgrade and modernize their crook recognition process into a more effective and efficient one. Through inventiveness, this idea will complement the current framework and raise the bar for recognizing thieves. We compare the captured images of the person reaching that public location with the criminal data in our database. The framework will display the person's picture on the framework screen and indicate with their name that the crook has been located and is present in this open spot if it assumes the person's face from the public spot coordinates. This framework synchronizes more than 80% of the captured photographs with those from the data set. [2]

3. The quick financial improvement in South Korea has brought about increment of wrongdoings. Opportune identification and decrease of violations are essential focal point of cops. Web of Things (IoT) and progressively modest and wearable sensors can be utilized to work with this errand. For the most part, the use of IoT innovations to the fields of savvy urban communities, brilliant strategies and medical services should be visible more regularly. In this paper, we present the plan of IoT based brilliant wrongdoing recognition framework. The proposed framework can distinguish violations continuously by breaking down the human emotions.[3]

4. Considered as item-based picture examination (OBIA). It is a viable strategy for high spatial goal (HSR) imaging. Order by an unmistakable and instinctive specialized process. In any case, OBIA depends on manual change of the picture. Arrangement capability. This is interesting work. Profound learning (DL) The innovation consequently gains picture highlights from an enormous number of pictures, Accomplishing higher picture characterization exactness than before Procedure. The review utilizes another technique called object scale versatile convolutional brain organizations (OSA-CNN), Consolidate OBIA and CNN, suggested for HSR pictures arrangement. To begin with, OSA-CNN gathers picture masses Head pivot of the item crude taken from the picture division; the size of the previous is resolved naturally By the hub width of the last option. This step produces the info Units expected for CNN arrangement. Second The crush and excitation blocks are extricated from the SE network.[4]

III. PROPOSED SYSTEM

This module works in a efficient way by following a particular set of instructions in proper manner are as follows:

A. Face Detection:

Finding and locating faces inside an image or video frame is the first step. This entails applying deep learning-based techniques like SSD (Single Shot MultiBox Detector) or Faster R-CNN, as well as algorithms like Haar cascades and Viola-Jones. A bounding box is formed around a face to separate it from the rest of the image once it has been identified.

B. Face Preprocessing / Encoding :

After detection, the face may undergo alignment and normalization to ensure consistency across different images. This step involves correcting for variations in pose, scale, and orientation. Techniques such as landmark detection or affine transformations are used to align the detected face to a standardized pose or orientation.

C. Feature Extraction:

Features are extracted from the aligned face region to represent its unique characteristicsmethods based on deep learning, especially those using convolutional neural networks (CNNs), are commonly used for feature extraction in modern face recognition systems. CNN architectures like VGG, ResNet, or Inception are often employed to extract high-level features from the face images. The output of a certain layer or layers of the CNN, often referred to as embeddings, serves as a representation of the face's features.

D. Face Recognition :

In the recognition phase, the feature vectors extracted from the input faces are compared to a database of known faces. Various classification algorithms can be used for this task, as deep neural networks, support vector machines (SVM), and k-nearest neighbours (KNN). The similarity between the feature vectors of the input face and the database faces is computed using distance metrics like Euclidean distance or cosine similarity. The input face is then classified or recognized based on the closest match(es) in the database.

E. Matching and Output :

The system compares the similarity scores from the previous step and determines if a match is found within a predefined threshold. If a match is found, the system might output the identity of the recognized person or trigger an alert (in real-time criminal detection scenarios).

F. ***Equations***

The HOG (Histogram of Oriented Gradients) technique is method for capturing statistical information about directional gradients in images, particularly focusing on edge detection. Its implementation involves extracting the gradient components in both the horizontal and vertical directions at each pixel location (x, y) in the original image.

The formulas (1) and (2), respectively, are used to determine the horizontal gradient (Gx) and vertical gradient (Gx) at a given pixel (x, y):

$$Gx(x, y) = H(x + 1, y) - H(x - 1, y) \quad (1)$$
$$Gy(x, y) = H(x, y + 1) - H(x, y - 1) \quad (2)$$

The pixel value at position (x, y) in the image is represented by H(x, y) in these equations. Next, we compute the gradient amplitude (G) and direction (α) at each pixel (x, y) as follows:

$$G(x, y) = \sqrt{(G_x(x, y)^2 + G_x(x, y)^2)} \quad (3)$$

$$\alpha = \tan^{-1} (G_y(x, y) / G_x(x, y)) \quad (4)$$

Next, the image is divided into smaller cells, and the gradient histograms of these cells are calculated to generate the descriptor for each cell. This descriptor represents the HOG feature of the cell.
Subsequently, multiple cell units are grouped into blocks (e.g., using a grid of 3x3 cell units per block). The descriptors of each cell unit within the block are concatenated to form the HOG feature of the block.
In essence, the HOG technique captures gradient information across the image, aggregating it into histograms within cells and blocks to create a compact representation of the image's edge structure.

IV. METHODOLOGY

A real-time criminal detection system (RTCDS) intended especially for the surveillance of high-risk ex-convicts is presented in this study. The system utilizes advanced deep learning techniques for face tracking, detection, and identification. Its primary objective is to enhance crime prevention by identifying faces in video data captured by surveillance cameras and promptly notifying relevant authorities or criminal institutions upon recognizing a criminal match from databases.
The comprehensive process structure for face detection and recognition is illustrated in Figure, which also shows the system's overall architecture. The system consists of new processes that are presented in this work as well as standard processes that are indicated by initials. The suggested system is composed of a face detector (D), tracker (T), face encoder (E), and identifier (I), just like traditional facial recognition systems. Reducing latency is essential to the suggested system in order to guarantee that every frame of recorded video data is processed instantly via the assigned steps.

A. ***System Architecture***

Aiding law enforcement officials in the identification of offenders is the primary goal of the Real-Time Criminal Identification based on Face Recognition Application. This application's goal is to provide details about a certain criminal that we are looking for. To locate a criminal, law enforcement officials can utilize this application anywhere, at any time. Any police officer can use the internet to access this program at any time and from any location. Criminals can also be located via real-time webcams.

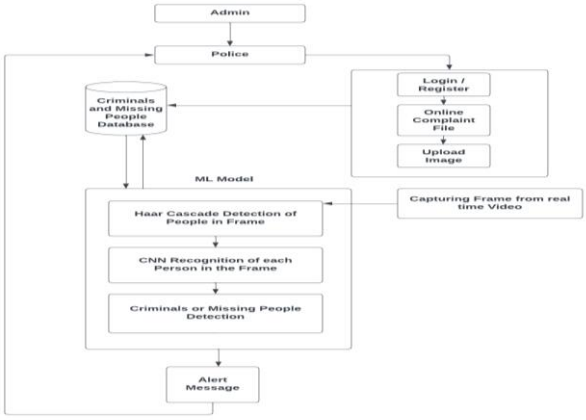

Fig. Block Diagram

• ***User:*** - Role: Initiates the identification process. - Actions: Interacts with the system through a user interface, provides necessary information, and may receive identification results.

• ***Authentication:*** - Role : Verifies the identity of the user. - Actions: Utilizes authentication methods (e.g., username/password, biometrics) to ensure that only authorized users access the system.

• ***Database :*** - Role: Stores crucial data for identification purposes. - Components: - User Data: Information about individuals (e.g., personal details, criminal records). - Training Data: Dataset used for training the system's machine learning models

• ***System :*** - Role: Orchestrates the overall functioning of the Criminal Identification System. - Functions: - Coordinates data flow between different components. - Manages the authentication process. - Initiates identification workflows based on user requests.

• ***Database Creation:*** - Role: Involves the process of populating and maintaining the database. - Actions: - Adds new criminal records and updates existing ones. - Ensures the database is current and accurate.

• ***Dataset Training*****:** - Role: Involves preparing the system's machine learning models. - Actions: - Utilizes a labeled dataset for training. - Trains models for feature extraction, classification, and detection.

• ***Web Camera Monitoring:*** - Role: Captures real-time images or videos for identification. - Actions: - Interfaces with web cameras to obtain live footage. - Feeds the captured data into the feature extraction modules.

• ***Feature Extraction:*** - Role: Extracts essential information from movies or photos.- Actions: - Analyzes input data to identify distinctive characteristics. - Extracts features such as facial features, fingerprints, etc.

• ***Detection:*** - Role: Identifies and flags potential matches or anomalies. - Actions: - Detects any matches found during the classification process. - Flags potential criminal matches or abnormalities for further investigation.

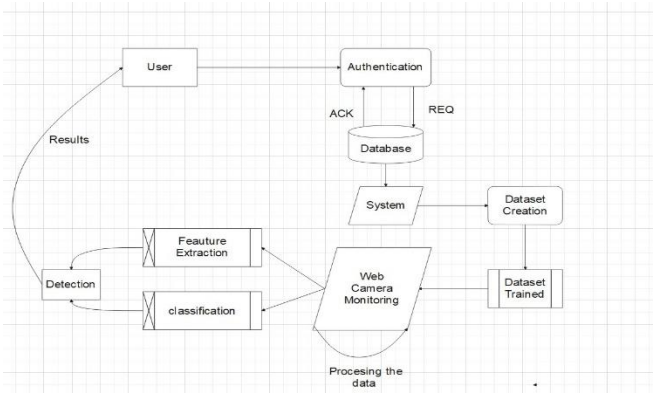

Fig. Workflow of model

V. IMPLEMENTATION APPROACH

A. ***Module 1: User Management Module:***

• The Module for user management for a criminal face detection project is a critical component that handles the authentication, authorization, and administration of users within the system. This module allows for the efficient and secure management of individuals who interact with the criminal face detection application.

• Overall, the User Management Module plays a crucial role in ensuring that only authorized and responsible users can access the criminal face detection project, maintaining data security, user accountability, and system integrity. It is an essential component for managing user interactions within the context of criminal face recognition and detection applications.Authors and Affiliations

B. ***Module 2: Face Recognition Module Module***

• A specialized part of a criminal face detection project, the Face Recognition Module makes use of cutting-edge computer vision algorithms to recognize and authenticate people in photos or video streams. It plays a pivotal role in aiding law enforcement and security personnel in quickly identifying and tracking suspects or

persons of interest. This module not only detects and extracts facial features but also matches them against a database of known individuals, enabling rapid responses and enhancing safety.

• Key functionalities of the Face Recognition Module include real-time processing, aliveness detection, database integration, and alert generation. Its seamless integration with other project components ensures efficient and accurate identification, making it an invaluable tool for law enforcement and security applications in the realm of criminal face detection.

C. ***Module 3: Criminal Database Module***

• The Criminal Database Module is a critical component within a criminal face detection project that manages a repository of information related to criminals, suspects, and individuals of interest. It serves as the backbone for cross-referencing and verifying the identities of individuals detected through face recognition technology. This module allows law enforcement agencies to maintain up-to-date records, track criminal histories, and compile watchlists, facilitating the swift identification and apprehension of individuals involved in criminal activities.

• Key features of the Criminal Database Module include data storage, indexing, and search capabilities. It ensures that the system can access and cross-check information efficiently, enabling authorities to respond effectively to security threats and enhance public safety. This module is an integral part of the overall system, providing essential data resources for the face recognition and identification components.

D. ***Module 4: Live Camera Integration Module***

• The Live Camera Integration Module is a critical component within a criminal face detection project, designed to seamlessly connect with live camera feeds and video surveillance systems. This module allows the project to continuously monitor public spaces, streets, and highsecurity areas for potential threats and persons of interest. It integrates with a variety of cameras, from CCTV to body-worn devices, and provides real-time video streams for analysis by the face recognition and detection modules.

• Key features of this module include the ability to access, manage, and process multiple camera feeds simultaneously, ensuring comprehensive coverage.

E. ***Algorithm :***

Convolutional Neural Networks (CNN): a deep learning architecture created especially for processing structured grid data, such as photographs, by employing a hierarchy of learnable filter layers to extract pertinent features automatically and accurately identify patterns.

Histogram of Oriented Gradients (HOG): a method for feature extraction used in computer vision to identify objects. It provides a representation of the shape and look of an item by counting instances of gradient orientation localized areas of a picture.

Algorithm Histogram of Oriented Gradients (HOG)

Step 1: Preprocessing

Convert image into grayscale :

```
gray_image = convert_to_grayscale(original_image)
```

Step 2: Compute Gradients

Apply gradient filters to compute horizontal and vertical gradients

```
gradient_x = apply_filter(gray_image, horizontal_gradient_filter)
gradient_y = apply_filter(gray_image, vertical_gradient_filter)
```

Step 3: Compute Gradient Magnitude and Direction

```
gradient_magnitude = compute_magnitude(gradient_x, gradient_y)
gradient_direction = compute_direction(gradient_x, gradient_y)
```

Step 4: Create Cells and Histograms

```
cell_size = choose_cell_size()
cells = divide_image_into_cells(gray_image, cell_size)
for cell in cells:
  # Initialize histogram for the cell
```

```
histogram = initialize_histogram() for pixel in cell:
   # Get gradient magnitude and direction of the pixel
magnitude = gradient_magnitude[pixel]
direction = gradient_direction[pixel]
  # Assign gradient to histogram bins based on orientation
bin_index = determine_bin_index(direction)
histogram[bin_index] += magnitude
  # Store histogram for the cell: cell.histogram = histogram
```

Step 5: Create Blocks and Concatenate Histograms

```
block_size = choose_block_size()
blocks = divide_cells_into_blocks(cells, block_size)
for block in blocks:
  # Concatenate histograms of cells within the block
concatenated_histogram = concatenate_histograms(block.cells)
block.histogram = concatenated_histogram
```

 # Step 6: Normalize Blocks

```
for block in blocks:
   # Normalize the histogram of each block
   block.histogram = normalize_histogram(block.histogram)
```

 # Step 7: Form Feature Vector

```
feature_vector = concatenate_block_histograms(blocks)
```

 # Step 8: Train or Apply Classifier

```
   # For training: Train a classifier using the feature vectors of     positive and negative samples
   # For detection: Use the trained classifier to detect objects in images
```

 # End of algorithm

In computer vision and object recognition, the Histogram of Oriented Gradients (HOG) algorithm is a popular feature extraction technique. This is a point-by-point description of the HOG algorithm.

VI. RESULTS AND ANALYSIS

The provided content describes the implementation and testing of a prototype system, as depicted in Figure, to validate the functionality of a proposed model and platform. This prototype consisted of a web server, an administrator's webpage, and a server computer with a deep learning model linked to a security camera.

Through this prototype, real-time monitoring of images from the surveillance camera was enabled, as depicted in accompanying figures. Upon detecting a criminal face in a specific area, the system displayed a mug shot of the individual along with the detection timestamp. Additionally, detailed information about the detected individual, including their address and personal details, was accessible.

Additionally, the prototype included a push notification capability that would notify workers and relevant institutions immediately upon identifying faces associated with criminal activity, thus increasing the efficacy of the system in managing and preventing crime.

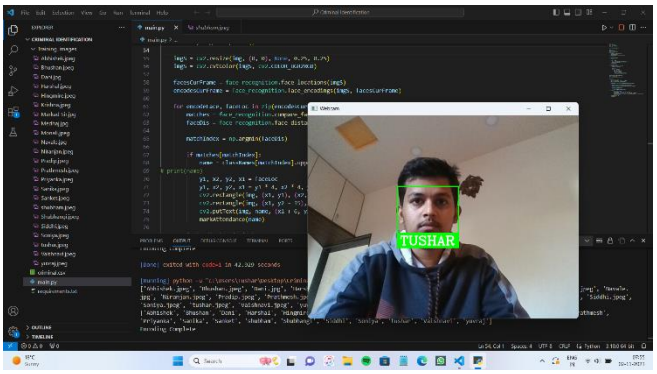

Fig : Face Encoding

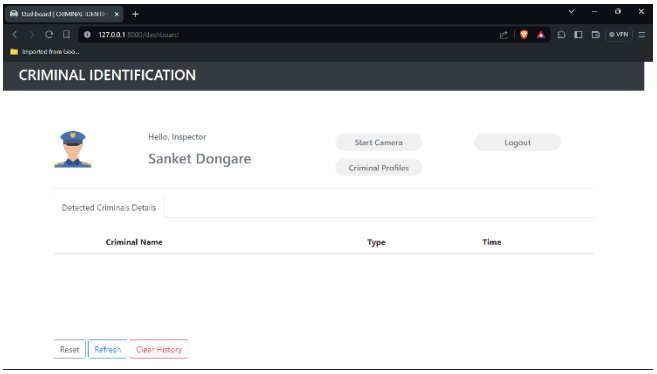

Fig : Organizational Interface

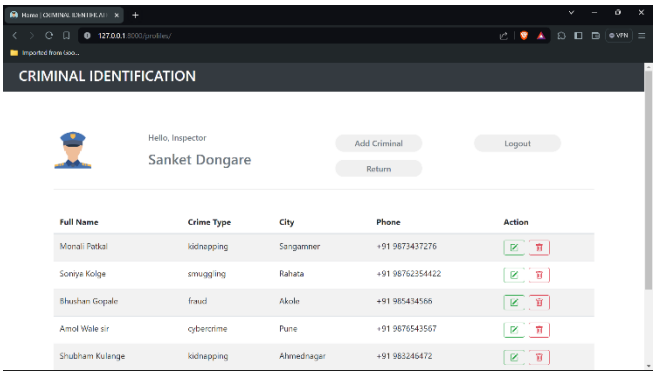

Fig : Criminal Database

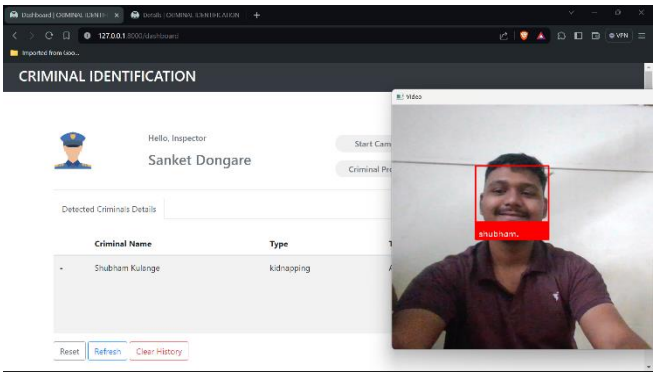

Fig : Criminal Identification

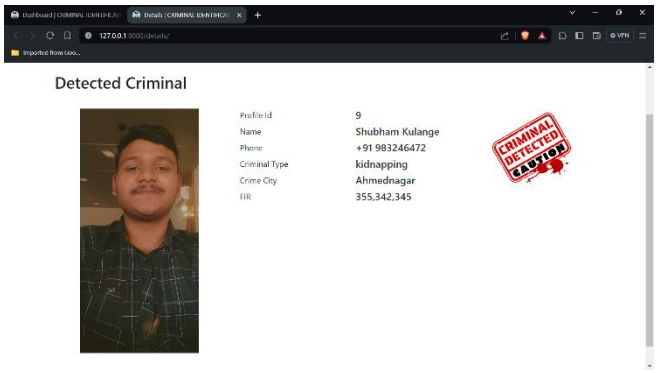

Fig : Result

VII. CONCLUSION

The project represents a vital and proactive response to the escalating challenges of criminal activities and security threats in our society. By harnessing advanced security technologies and innovative approaches, it aspires to significantly enhance crime prevention, detection, and identification. The application of predictive analytics and face recognition not only empowers law enforcement

agencies to operate more efficiently but also fosters a sense of public and private security. Continuous technological advancements and global collaboration further underline the commitment to staying ahead of evolving criminal tactics. Ultimately, the project's success will lead to a safer and more orderly environment, reducing crime rates and improving the overall quality of life for the community it serves.

VIII. FUTURE SCOPE

A sophisticated facial recognition system of this nature has the potential to automate the detection of criminals through CCTV cameras installed across various locations. Additionally, it could serve to identify missing individuals during disasters or emergencies. This system's capabilities could be expanded to simultaneously identify multiple faces, even from blurry or cropped images. Moreover, it could provide precise details regarding the exact location where a criminal was spotted, leveraging the camera's location data. The database could also be enhanced to include additional information such as age, previous criminal activity, associated individuals, and last known whereabouts, offering comprehensive insights into the individual's background.

REFERENCES:

[1] 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)

[2] Apoorva.P, 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).

[3] Rasanayagam, K.Kumarasiri, S.D.D, Tharuka, W. A. D. Samaranayake, N. Samarasinghe and P. Siriwardana "CIS: An Automated Criminal Identification System". 2018 IEEE International Conference on Information and Automation for Sustainability (ICIAfS)R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[4] Mantoro, T., Ayu, M. A., Suhendi. (2018)." Multi-Faces Recognition Process Using Haar Cascades and Eigenface Methods" 2018 6th International Conference on Multimedia Computing and Systems (ICMCS).

[5] Chang L , Yang J, Li S, Xu H, Liu K Huan, C. (2018). "Face Recognition Based on Stacked Convolutional Autoencoder and Sparse Representation". 2018 IEEE 23rd International Conference on Digital Signal Processing (DSP).

[6] V. Tsakanikas and T. Dagiuklas, "Video surveillance systems-current status and future trends," Comput. Electr. Eng., vol. 70, pp. 736–753, Aug. 2020

[7] E. L. Piza, B. C. Welsh, D. P. Farrington, and A. L. Thomas, "CCTV surveillance for crime prevention: A 40-year systematic review with metaanalysis," Criminol. Public Policy, vol. 18, no. 1, pp. 135–159, Feb. 2019.
[8] G. Alexandrie, "Surveillance cameras and crime: A review of randomized and natural experiments," J. Scandin. Stud. Criminology Crime Prevention, vol. 18, no. 2, pp. 210–222, Jul. 2017.
[9] 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.
[10] Y. Kortli, M. Jridi, A. Al Falou, and M. Atri, "Face recognition systems: A survey," Sensors, vol. 20, no. 2, p. 342, Jan. 2020.
[11] 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.
[12] J. Deng, J. Guo, E. Ververas, I. Kotsia, and S. Zafeiriou, "RetinaFace: Single-shot multi-level face localisation in the wild," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2020.
[13] S. Zafeiriou, C. Zhang, and Z. Zhang, "A survey on face detection in the wild: Past, present and future," Comput. Vis. Image Understand., vol. 138, pp. 1–24, Sep. 2019.
[14] C. Ferrari, S. Berretti, and A. Del Bimbo, "Extended YouTube faces: A dataset for heterogeneous open-set face identification," in Proc. 24th Int. Conf. Pattern Recognit. (ICPR), Aug. 2018, pp. 3408–3413.