Deep Learning Based Criminal Identification System

[1] Sagar Jadhav [2]Satyam kangle [3]Om Pandav [4]Nikhil Palve
[1]B.Tech Information Technology, Vishwakarma Institute of Information Technology, Pune
sagar.22010365@viit.ac.in
[2]B.Tech Information Technology, Vishwakarma Institute of Information Technology, Pune
satyam.22010972@viit.ac.in
[3]B.Tech Information Technology, Vishwakarma Institute of Information Technology, Pune
om.22010411@viit.ac.in
[4]B.Tech Information Technology, Vishwakarma Institute of Information Technology, Pune
nikhil.22010648@viit.ac.in

***Abstract*— the criminal identification system is a cutting-edge technology that identifies suspects in criminal investigations using a variety of biometric data, including fingerprints, facial recognition, and DNA analysis.**

A recognized Python programming language-based automatic facial recognition system for criminal databases was proposed in the project. The system will be able to automatically identify and recognize faces. CNN will be the facial recognition algorithm used. This system was created to give law enforcement organizations a reliable and effective tool for apprehending offenders and resolving crimes.

Keywords*— criminal identification, CNN, facial recognition, CCTV, Image processing.

I. Introduction

A sort of artificial intelligence technology called deep learning-based criminal identification systems employs neural networks to analyze enormous volumes of data and identify people who may have committed a crime. These systems can automatically discover patterns and links within massive datasets by utilizing the strength of deep learning algorithms. This enables law enforcement personnel to swiftly identify prospective suspects and locate people who may be involved in criminal activities.

Numerous applications for these systems exist, such as video surveillance, facial recognition, and audio analysis. They are frequently employed by law enforcement organizations to support criminal investigations and aid in the identification of suspects in situations when conventional investigative techniques have fallen short.

Current One of the few biometric techniques that has the advantages of both accuracy and little intrusion is face recognition. For this reason, face recognition has captured the interest of academics in disciplines ranging from security and image processing to computer vision since the early 1970s. Additionally helpful in the processing of multimedia information is face recognition. The process of determining whether a previously observed item is a known or unknown face is known as face recognition. The issue of face detection and face recognition are frequently conflated. On the other hand, to authenticate this input face, it must be determined whether the face belongs to a known or unknown person by utilizing a database of faces for this purpose. The primary goal of this project is to use a neural network to build an effective architecture for facial recognition while viewing videos. In order to discover and identify faces in areas with a dense cluster of Accelerated Segment Test (FAST) characteristics, this solution uses two self-contained neural networks (CNNs). Figuring out if the face image of any particular individual matches any of the face images kept in a database. A notice is forwarded to the closest police station if a match is identified.

II. Related Works

Using various machine learning (ML) and deep learning techniques, some research and work has been done to identify the offender or detect the crime.

A system that makes use of machine learning (ML) and computer vision methods and methodologies was proposed by Neil Shah et al. in [1]. The author has conducted research to ascertain how law enforcement agencies and authorities may employ a mix of ML and computer vision to identify, prevent, and solve crimes considerably more accurately and quickly. KNN, decision trees, SVM, Naive Bayes classifiers, random forest regression, and other machine learning techniques have all been compared, as well as the accuracy rates of each method. Overall, the author created a system that consists of a variety of technologies that can do everything from track down crime hotspots to identify persons based on voice notes.

As well as proposing a new method for criminal detection and recognition utilizing cloud computing and machine learning, article [2] attempted to examine the available technology. This research study suggests using the cloud and cognitive services provided by Microsoft Azure to create the suggested system. Several facial recognition techniques were encountered while creating this system. HAAR, Eigen Faces, Cam Shift, CNNs, Viola-Jones Algorithm, Gaussian, Euclidian distance, AdaBoost, and more algorithms were encountered. The suggested technique may be applied to a variety of tasks, such as searching for missing children at a train station.

The performance of data mining techniques that may be used to analyze the gathered information regarding prior crimes was examined in Paper [3]. Evaluations of the data revealed that "Decision Tree" is the strategy that performs best. The author gathered information from law enforcement organizations and saved it in CSV format. Artificial Neural Networks (ANNs), Naive Bayes Classifier, Support Vector Machine, decision tree, and other classification data mining techniques are applied. These techniques were all utilized to find the offender or perpetrator.

The author of article [4] created a method for criminal face detection. A notice is delivered to the police staff with all the facts and the location where the criminal was being watched by a camera after this technology recognizes the criminal's face and obtains the data contained in the database for the identified criminal. Face Net, OpenCV, MTCNN (Multi Task Cascade Neural Network), and other methods were utilized to construct this system. The advantage of the recommended methodology is that it can capture criminals in the act of committing their first crime.

Dr. Jayavrinda Vrindavanam created a system that watches CCTV footage and identifies suspicious behaviors in real-time videos while sending notifications to the appropriate authorities in paper [5]. Two distinct functioning machine learning models were combined into one working model by the author. A mode receives video or an image from CCTV footage in order to identify criminal faces. For the detection of weapons, another model is employed. To detect the target item, a dark net framework and the YOLOv4 algorithm must be used.

In paper [6], six distinct machine learning algorithms, including the random forest method, the KNN algorithm, the SVM algorithm, and the LSTM algorithm, have been implemented as a system for crime prediction. For crime prediction, this system makes use of both historical data and the built-in surroundings. The LSTM model was shown to have higher prediction accuracy than other models.

In this study [7], several algorithms such e KNN, Artificial Neural Network, Decision trees, Extra trees, and Support Vector Machine are used to analyze and predict crime. Results indicated that MLP accuracy was quite poor and SVM training time was lengthy. With ideal training and excellent accuracy, decision tree, KNN, and extra tree classifiers are determined to be the best.

III. Proposed System

Criminal identification involves determining if a previously discovered object is a recognized or unknown face. The issue of criminal identification and the issue of face detection are frequently mixed together. On the other hand, to determine if the "face" is a known or unknown person, using a database of faces for this purpose, is necessary to validate this input face. The primary goal of the project is to design an effective criminal identification architecture.

Python programming is used to create the project as a web-based application. The faces will be photographed using the laptop webcam. The CNN algorithm will be employed. The database will first get the criminal face, and a training model will be developed. The offender will be recognized as they match the database when they appear in front of the camera for testing and their image will be matched at the rear end with the current database. We create a method that will be extremely helpful for any investigation department in order to fix the flaws in the present one. Here, the program maintains track of pictures of faces from various angles. Based on this record number, the program collects the suspect's personal information (which is then displayed to the user if there is a match of more than 90%).

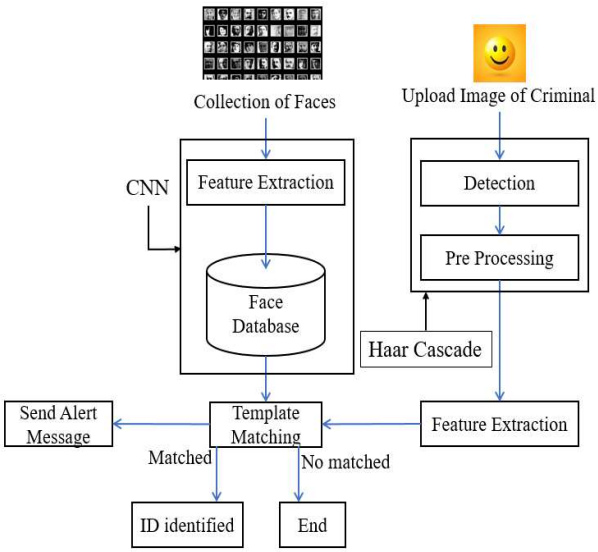

Fig.1 Proposed System Flow

A. Modules/techniques Used

a) Open CV: Open CV (Open Source Computer Vision) is a well-known computer vision library. The cross-platform library's main focus is real-time image processing, but it also includes patent-free implementations of the most advanced computer vision algorithms. It gives you a foundation for doing whatever you want with photos and videos, whether using Open CV techniques or your own, without having to worry about allocating and reallocating RAM for your images. It may also be used to process video and images in real time. The very effective HAAR Cascade algorithm of OPENCV was used to construct this system for real-time image processing of live video coming from the camera.

b) HAAR Cascade Classifier: The Haar cascade classifier is a prominent approach in computer vision applications for object recognition, notably face detection. Viola and Jones initially proposed it in their 2001 publication, "Rapid Object Detection Using a Boosted Cascade of Simple Features."

Face identification using Haar cascade classifier involves training a cascade of classifiers to identify characteristics such as eyes, nose, and mouth, which are then merged to detect a face. The Haar features employed in the cascade are basic rectangular filters that compute the difference between the sum of pixel intensities in the filter's white and black areas.

The trained cascade of classifiers is applied to the input picture at various sizes and places during the detection phase. The method returns the coordinates of the bounding box around the observed face if a face is detected. This method has been found to be one of the fastest and most efficient in face identification.

c) **CNN:** CNN, or Convolutional Neural Networks, are used in criminal identification systems for analyzing and recognizing patterns in photos and videos.

Facial recognition technology is one of the most important uses of CNNs in criminal identification. CNNs is trained on massive datasets of facial photographs to recognize and identify persons properly.

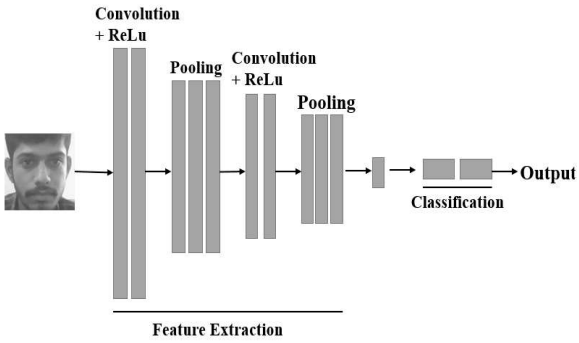

Fig.2 CNN Architecture

CNN contains numerous layers with distinct filters in charge of detecting certain traits of the target individual. We employed five convolutional layers for feature extraction (in fig.2). These layers attempt to focus on broad traits while also attempting to detect unique aspects. These layers make use of functions such as convolution, max pooling, and Relu. The last layer is used to categories the results, and it employs functions such as softmax.

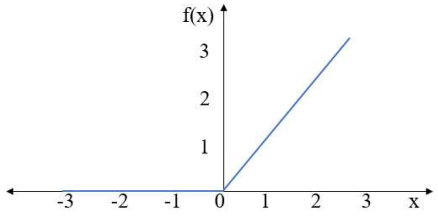

Fig.3 ReLu function working graph

Convolution is a linear operation that is followed by a non-linear function, i.e. relu. The working graph (in fig.3) for the relu activation function is shown above.

$$f(x) = \begin{cases} 0 & \text{for } x<0 \\ X & \text{for } x\geq 0 \end{cases} \qquad \textbf{(1)}$$

Fig 4 is an example of how the relu operates on an nxn matrix picture. The pixel value changes as a result of equation (1).

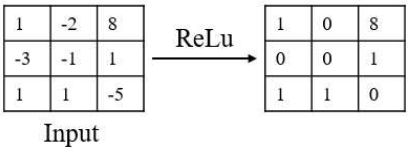

Fig.4 Relu on input image

Subsampling is another term for pooling. It is used following the convolution and relu operations. It decreases the dimensionality of the input feature map while retaining critical information. The maximum value from the complete feature map is tallied by the filter, as illustrated in (fig.5).

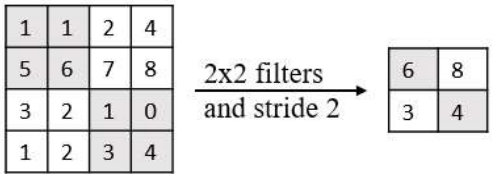

Fig.5 Max Pooling on input image

Softmax is the final layer of a CNN that is utilized for classification. It assigns decimal probability to each class in multiclass categorization. The class with the highest probability will be chosen as anticipated. Its result indicates the chance of a specific image belonging to a specific class. To compute probability, it use the following equation (2).

$$softmax(z_i) = \frac{\exp(z_i)}{\sum_j \exp(z_j)} \qquad \textbf{(2)}$$

Training on a specific training set yields values for filters in each convolution layer. After training, we have a unique set of filter values that we can use to recognize certain features in the dataset. This collection of filter settings is applied to fresh photos in order to forecast what is included inside the image.

B. ALGORITHM STEPS

Step 1 – Adding a New Criminal: Gathering personal information and images from criminal histories.

Step 2 – Preprocessing: Preprocessing is the process of cleaning up and normalizing the acquired data. When images include disruptions, training the model will be challenging.

Step 3 – Feature Extraction: The system takes the preprocessed data and extracts distinguishing characteristics. This step's grayscale photographs were used to train the model and identify the culprit.

Step 4 – Feature Matching: To find possible matches, the retrieved characteristics are matched to the database of criminal records already in existence. For feature matching, a variety of methods can be utilized, such as pattern recognition, machine learning algorithms, and statistical analysis.

Step 5 – Identification & Reporting: If there is a positive match, the offender is identified and the appropriate authorities are contacted. The system provides a report including information on the identification process, such as the matching characteristics and verification methodologies employed.

IV. FACE RECOGNITION METHODS

This is a simple face detection pipeline that can be utilized by any face detection model or program.

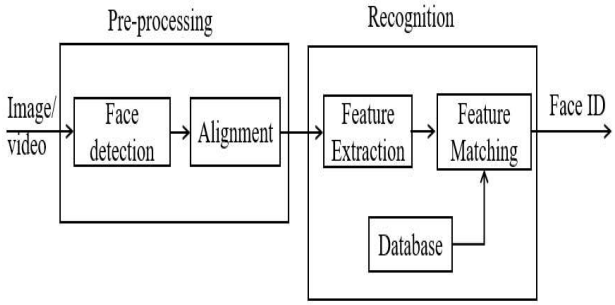

Fig.6 Face Recognition Processing Flow

a) Face Detection: To recognize the presence of faces in photos or videos, face detection techniques are utilized. It entails analyzing picture or video frames using algorithms and machine learning models. These algorithms estimate the location of a face by analyzing the pixel values of an image or video. Face detection begins by dividing an image or video frame into smaller bits known as pixels. The system then examines these pixels for patterns that correlate to face characteristics like the eyes, nose, and mouth. The system can then detect the presence and placement of a face (shown in fig.7) inside an image or video frame based on these patterns.

Fig.7 Face marked with rectangle

b) Face Alignment: Face alignment entails normalizing the face to be consistent with the database, using techniques such as geometry and photo metrics. A computer program recognizes numerous important facial features, such as the corners of the eyes, the tip of the nose, and the corners of the mouth, to align a face. The method then computes the transformation required to relocate those landmarks to a standard position, such as a set distance apart or at a specific angle relative to each other.

c) Training: The training phase follows the preprocessing stage. It is critical that after face identification, the computer saves the photographs in the "yml" format in a database shown in (fig.8). The preprocessed dataset is used to train the algorithm. All photographs of the same individual must have the same ID. Through back propagation, the CNN algorithm learns the patterns and characteristics of the pictures and modifies its weights to minimize the prediction error.

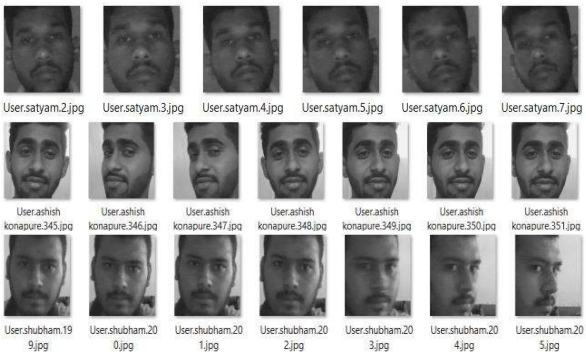

Fig.8 Training Dataset

d) Face Recognition: It comprises two types of techniques: feature extraction and matching. Extract facial traits that are unique to each person and may be used for the recognition job. The feature matching job follows, which compares the face to one or more known faces in a predefined database.

V. ANALYSIS & RESULT

We collected photos of 7 to 8 people for this criminal identification model and categorized them into training and testing data. Around 400 photographs taken, out of 320 are saved in the training folder to train this model (shown in fig.8), and 80 images are put in the testing folder. Every image has a name and an id number that will be used to identify the individual. We put all of the photographs of one consumer under one customer ID because they were all of the same person. To collect real-time pictures from a live camera, we employed the Haar cascade classifier. All of the collected photos are cropped to 164x164 pixel size and saved in a database for identification (see fig.9).

This software is a real-time face recognition system that captures real-time video from a live webcam, extracts the image from it, detects the human face in it, and attempts to match that image with the existing database; if a match is found, it labels the image with the name of the criminal in the database and sends an alert to the appropriate authorities.

This program was tested on several cases and found to be capable of identifying criminals with an accuracy of more than 80%. The table is shown below.1 for the number of people utilized to test this model.

NO.	Name
1.	Sagar
2.	Satyam
3.	Om

Tabel.1

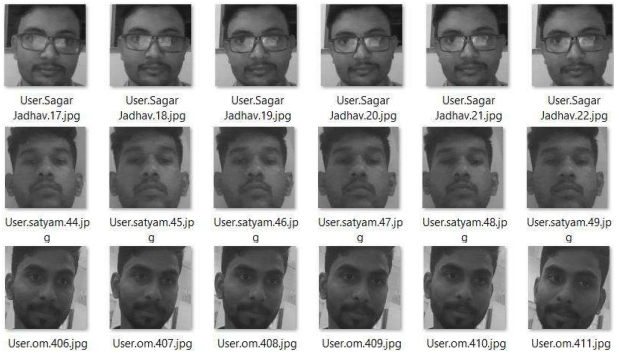

Fig.9 Testing Dataset

Pycharm was used to execute this system on the laptop. The model's home screen is seen in Fig.10 below.

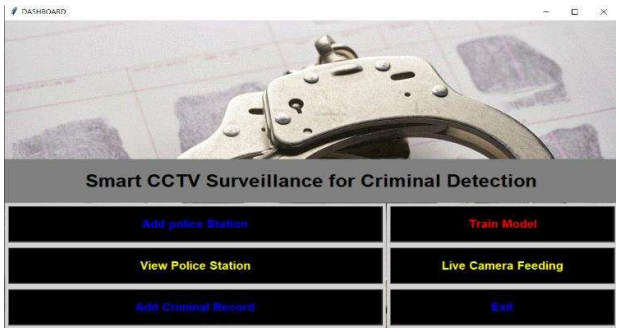

Fig.10 Home Screen

The model functioned properly. We may enter police station information and save it in the database using MySQL. Fig.11 and fig.12 indicate that the police station information were successfully inserted. We may also erase specifics by clicking on them.

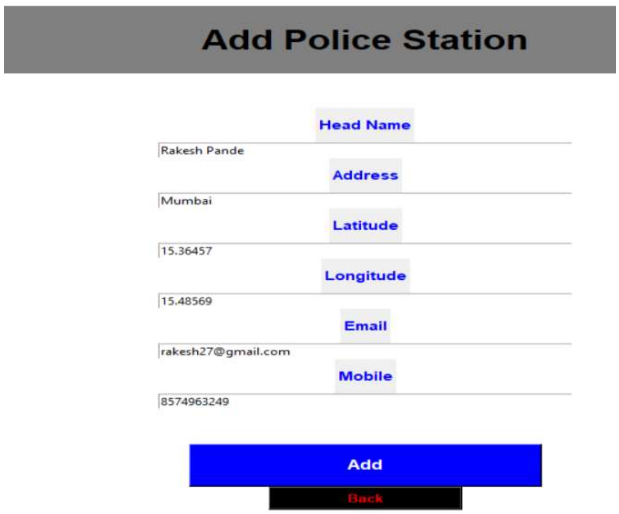

Fig.11 Add police station Screen

Fig.12 View Police Screen

Figure 13 and figure 15 indicates that the system is capable of successfully detecting criminals and showing the criminal's name on the screen. And, as shown in fig.14 and fig.16, after identifying a criminal, it is capable of sending a message to the respected authorities of a local police station head, including its name, location, and crime details.

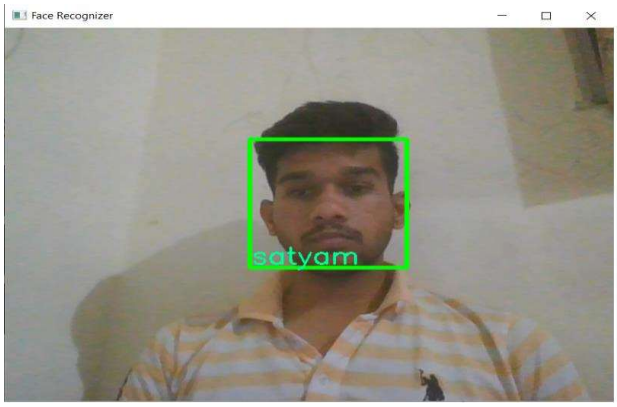

Fig.13 Face recognition Screen (Person 1)

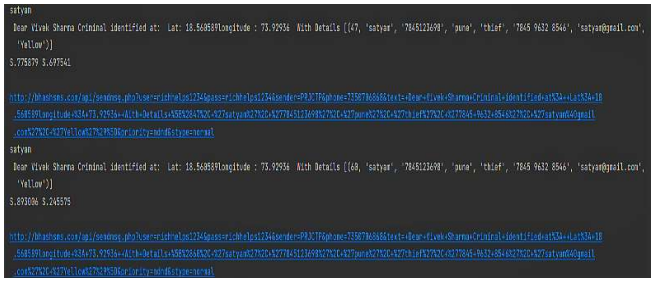

Fig.14 Message Box

Fig.15 Face recognition Screen (Person 2)

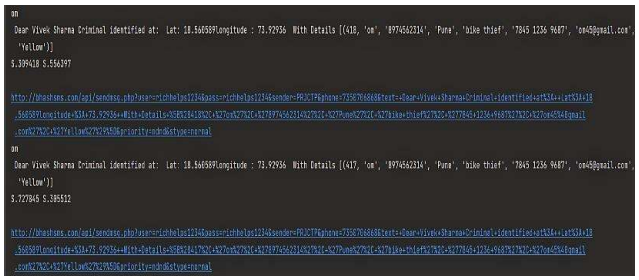

Fig.16 Message Box

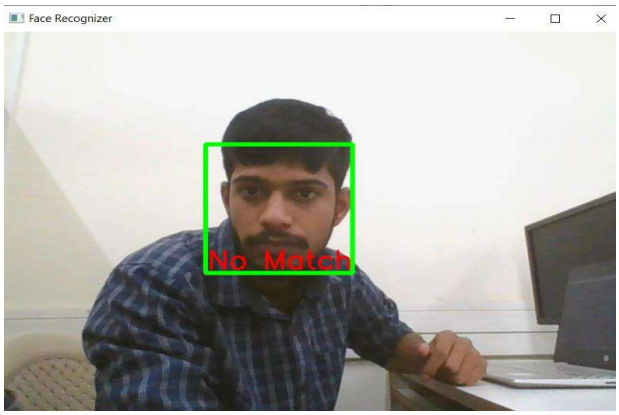

Fig.17 Face recognition (unknown person)

In fig.17, we tested the algorithm on an unknown face, that is, a person who is not in the criminal database. And the technology may recognize that the individual does not match the current database and that the person is innocent.

Fig.18 X_train and Y_train plot

The plot above (fig.18) depicts the distribution of training data (X_train) in relation to their respective labels (y_train). The scatter plot depicts the distribution of training data across labels or classes. It indicates how effectively the data is divided and whether there is any overlap across classes. If there is overlap between the different classes, it may suggest that the classifier is having trouble differentiating between them. If the data points are well spaced, the classifier may be able to discriminate between the various classes. As a result, before developing a classifier, it is critical to visualize the data and look for patterns or trends.

The neural network model was trained using a dataset of 400 photos, 320 of which were used to train the model and 80 to test it. The algorithm properly identifies 70 of the 80 photos during testing.

Then, the accuracy of the model can be calculated as follows:

Accuracy = (Number of Correct Predictions / Total Number of Test data) * 100%

= (70 / 80) * 100%

= 87.5%

Therefore, the accuracy of the neural network model is 87.5%.

We utilized the haar cascade technique for face detection, which is a famous face detection algorithm. The Haar Cascade technique is well-known for its excellent accuracy and quick processing speed, making it ideal for real-time object identification applications. But however, it struggles to recognize objects in low-light or high-contrast settings.

While researching, CNN and LBPH (Local binary pattern histogram) were discovered to be popular facial recognition algorithms. Changes in lighting conditions can have an influence on how photographs are taken and processed, lowering the accuracy of face recognition systems. However, both algorithms are affected by light exposure. However, CNN has evolved strategies such as supplementing training data using photos captured under varied lighting conditions and employing increasingly complicated CNN structures. As a result, CNN is shown to be more accurate than LBPH.

VI. Conclusion

In this research, we implemented a criminal identification system that will record criminals based on facial recognition. It will save time and effort, especially if the location is sociable. The automated criminal identification system was designed to address the shortcomings of the conventional (manual) approach. This system illustrates how image processing methods may be used in public spaces. The use of this technology will greatly boost security standards. Because it is totally automated, this technology provides a more effective method of detecting criminals. It may be used in public spaces like airports to identify criminals.

Because it is a facial recognition system, it has a wide range of applications, including attendance systems, authentication systems, and the ability to locate missing children. This approach can aid not just the criminal investigative system, but also the government's goodwill.

VII. References

[1] Shah, N., Bhagat, N. & Shah, M. Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention. Vis. Comput. Ind. Biomed. Art 4, 9 (2021). https://doi.org/10.1186/s42492-021-00075-z

[2] S. Shirsat, A. Naik, D. Tamse, J. Yadav, P. Shetgaonkar and S. Aswale, "Proposed System for Criminal Detection and Recognition on CCTV Data Using Cloud and Machine Learning," 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, 2019, pp. 1-6, doi: 10.1109/ViTECoN.2019.8899441.

[3] Llaha, Olta. (2020). Crime Analysis and Prediction using Machine Learning. 496-501. 10.23919/MIPRO48935.2020.9245120.

[4] https://www.irjmets.com/uploadedfiles/paper/volume3/issue_4_april_2021/8940/1628083365.pdf

[5] https://ijcrt.org/papers/IJCRT2106136.pdf

[6] X. Zhang, L. Liu, L. Xiao and J. Ji, "Comparison of Machine Learning Algorithms for Predicting Crime Hotspots," in IEEE Access, vol. 8, pp. 181302-181310, 2020, doi: 10.1109/ACCESS.2020.3028420.

[7] Pratibha, A. Gahalot, Uprant, S. Dhiman and L. Chouhan, "Crime Prediction and Analysis," 2nd International Conference on Data, Engineering and Applications (IDEA), Bhopal, India, 2020, pp. 1-6, doi: 10.1109/IDEA49133.2020.9170731.

[8] K. Rasanayagam, S. D. D. C. Kumarasiri, W. A. D. D. Tharuka, N. T. Samaranayake, P. Samarasinghe and S. E. R. Siriwardana, "CIS: An Automated Criminal Identification System," 2018 IEEE International Conference on Information and Automation for Sustainability (ICIAfS), Colombo, Sri Lanka, 2018, pp. 1-6, doi: 10.1109/ICIAFS.2018.8913367.

[9] S. S. Kshatri, D. Singh, B. Narain, S. Bhatia, M. T. Quasim and G. R. Sinha, "An Empirical Analysis of Machine Learning Algorithms for Crime Prediction Using Stacked Generalization: An Ensemble Approach," in IEEE Access, vol. 9, pp. 67488-67500, 2021, doi: 10.1109/ACCESS.2021.3075140.

[10] S. Abdullah, F. I. Nibir, S. Salam, A. Dey, M. A. Alam and M. T. Reza, "Intelligent Crime Investigation Assistance Using Machine Learning Classifiers on Crime and Victim Information," 2020 23rd International Conference on Computer and Information Technology (ICCIT), DHAKA, Bangladesh, 2020, pp. 1-4, doi: 10.1109/ICCIT51783.2020.9392668.

[11] S. T. Ratnaparkhi, A. Tandasi and S. Saraswat, "Face Detection and Recognition for Criminal Identification System," 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2021, pp. 773-777, doi: 10.1109/Confluence51648.2021.9377205.

[12] P. R. and K. V. Suresh, "Fingerprint Image Identification for Crime Detection," 2019 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2019, pp. 0797-0800, doi: 10.1109/ICCSP.2019.8698014.

[13] S. Kim, P. Joshi, P. S. Kalsi and P. Taheri, "Crime Analysis Through Machine Learning," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2018, pp. 415-420, doi: 10.1109/IEMCON.2018.8614828.

[14] S. Shilpa and A. Sajeena, "Hybrid Deep Learning Approach For Face Spoofing Detection," 2019 International Conference on Intelligent Computing and Control Systems (ICCS), Madurai, India, 2019, pp. 412-416, doi: 10.1109/ICCS45141.2019.9065468.

[15] A. Mary Shermila, A. B. Bellarmine and N. Santiago, "Crime Data Analysis and Prediction of Perpetrator Identity Using Machine Learning Approach," 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2018, pp. 107-114, doi: 10.1109/ICOEI.2018.8553904.