

Face Detection and Recognition for Lawbreakers Using ML

Mary Stella^{1*}, A. Sarwath Tabassum², Ankur Pathak³, Arfa Abbs⁴, Fathimuzehra⁵

¹Professor, ^{2,3,4,5}Student

Department of Computer Science and Engineering,
HKBK College of Engineering, Bangalore, India.

***Corresponding Author**

E-Mail Id: marys.cs@hkbk.edu.in

ABSTRACT

Everyone is aware that a person's face is a distinctive and essential component of their physical makeup and identity. Consequently, we can use it to discover a criminal's identity. With the development of technology, CCTV is now installed in many public locations to record illegal activity. The criminal face recognition system can be put into use using the previously photographed criminal faces and photos that are available in the police station. In order to improve and modernize the criminal differentiating process and give the Police Department a more effective and efficient method, we suggest an automatic criminal identification system in this article. This idea will improve the current system while raising the bar for criminal detection through the use of technology. By automating processes, this proposal will improve the current system while bringing criminal detection to a whole new level. Face recognition software will be the technology at work behind it. The video footage of the person entering that public space is compared to the criminal information stored in our database. The system will display that person's image on the screen and notify you with their name that the criminal has been located and is present in this public area if any other person's face from a public place matches.

Keywords: Artificial intelligence (AI), machine learning (ML), criminal identification

INTRODUCTION

Overall View

Numerous security strategies have been created throughout the years that aid in protecting sensitive data and reducing the likelihood of a security breach. One of the few biometric techniques, face recognition, has the advantages of being both highly accurate and little intrusive. It is a computer programme that automatically recognizes and verifies a person from a digital image or a video frame from a video source by using the person's face. It can also be hardware that is used to authenticate a person by comparing specific facial traits from a picture with a database of faces to compare any suspect with the database, law enforcement in developed nations builds a

face database to be utilised with their facial recognition technology. On the other hand, thumbprint identification is used in India for the majority of instances to identify any suspects in the case. However, most thieves are aware of thumbprint recognition due to the vast knowledge provided by internet usage. As a result, they wear gloves unless it is a non-premeditated act and are more cautious about leaving thumbprints.

Purpose

- In order to enhance the present criminal face detection system.
- To give quick crime detection in the meantime.
- To simplify the image's intricacy.

- It is simple to identify a criminal by utilizing a sketch or a CCTV image, but more challenging to identify a

criminal or to match the data with the criminal record.

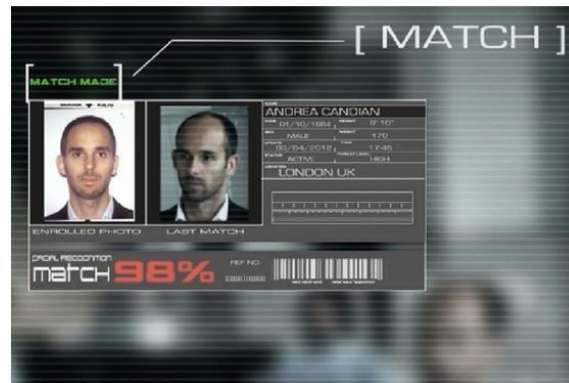


Fig. 1: Demo Image.

The goal of this technology is to locate criminals in any investigating department. The system's scope is comprehensive face identification. Finishing the system with the specified user criteria in the allotted time. The users utilise one system, while the administrators use another. It can be employed in a variety of settings, including banks, hotels, and police stations.

Pose, illumination, emotions, facial characteristics, and image quality all have a role in how accurately text and face recognition works. For the system to process real-time photos with great precision and speed, a few features must be added. Another element of the study involves creating a model that, when trained on a dataset of criminal records, can forecast a criminal's facial sketch based on features submitted by a witness.

LITERATURE SURVEY

Face recognition applications have been developing since the 1960s, as noted in [1], which also popularized the strategy of using a RAND tablet for coordinating facial features. A RAND tablet was a gadget that allowed users to input vertical and horizontal coordinates on a grid using a pen that produced

electromagnetic pulses. The entire system was used to manually record the coordinate locations of the mouth, nose, hairline, eyes, and other facial features.

Reference [2] uses 21 unique facial traits, such as the skin tone, chin, nose elevation, and hair color, to raise the bar for face identification.

Face recognition technology was first used by law enforcement in 2002. Since then, criminal identification has emerged as one of the main uses for face recognition. [5] Creates the "FRCI" criminal identification system using the principal component analysis dimensionality reduction technique. Uses the Haar-Features approach as described in [9] in [6,-8]. The detection window in a Haar features system is made up of solid rectangles where particular features are located.

In a detection window at a certain position, a Haar-like feature takes into account adjacent rectangular sections, adds the pixel intensities in each sector, and then determines the difference between these sums. A system using 18 characteristics, including RGB, was proposed by Adriana Kovashka and Margaret Martonosi.

Because of the effectiveness of neural networks insolving computer vision issues like face recognition after 2010, it makes sense to use AdaBoost and ANN in combination to develop the "ABANN" hybrid model. Numerous deep learning models, including Retinal Connected Neural Network, Rotational Invariant Neural Network, Back Propagation Neural Network, Fast Neural Network, etc., have been used specifically for face recognition.

Our project's major focus will be focused on (Face Net), an embedding method that converts facial traits into a "compact Euclidean Face-Map" that can be utilised to identify variations among the faces in the database. Each face is mapped to 128 bytes using a deep convolutional neural network technique, and the tasks of recognition, detection, and grouping are completed. For two datasets, an accuracy rate of over 95% has been seen.

METHODOLOGY

Face identification is a broad word that covers a number of smaller issues. Face detection, feature extraction, and face recognition are the three processes that make up the face identification process.

Face Detection

The method of identifying faces in pictures and environments is known as face detection. Therefore, the system correctly recognizes a certain visual region as a face. Numerous uses for this process include position estimation, face tracking, and compression.

Feature Extraction

Finding pertinent facial features from data is called feature extraction. These traits could be specific face regions, variations, angles, or measurements that may or may not be relevant to humans (such as the distance between the eyes). Other uses for this phase include emotion recognition and tracking of face features.

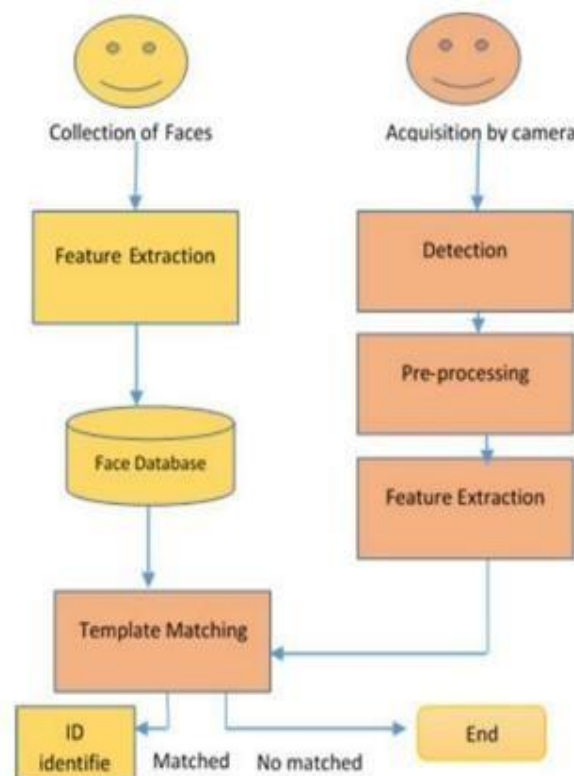


Fig. 2: Flowchart.

Face Recognition

To identify the identity of the query face, a one-to-many matching procedure compares a query face image against every template image in a face database. Finding the image in the database with the greatest similarity to the test image is how the test image is identified. An observation of a person who is already known to be in the database is taken by the sensor as part of the identification procedure, which is a "closed" test. Either Eigen features or Eigen faces are involved in the fundamental recognition. The word "eigen" in German refers to recursive mathematics used to examine distinctive facial features. When a facial feature detection system employs the Eigen face method, it interprets each facial image as a two-dimensional array of light and dark regions arranged in a specific pattern. These contrasts between light and dark are referred to as the Eigen faces. The converted method that represents the bright and dark region patterns is then temporarily stored as a combination of Eigen faces. Finally, a facial recognition system scans the current combination of Eigen faces and compares it to previously saved Eigen faces in a database. The distances between characteristics of the face like the mouth, nose, eyes, and bone structure are sought after via an Eigen feature system technique. The unique aspect of this technology is that a facial identification

system takes a picture of a person's face and then extracts specific unique elements from it to store in a database. An additional distinction between continuous and triggered facial feature systems is made here. Continuous systems are continually running and scanning face picture data. Systems that are triggered require some sort of activation before they can scan a person's face. Face identification is crucial for identifying the criminal since it makes it simple to identify the offender after they have committed the crime.

It would be simple to gather information about the person with a criminal record who is a suspect in this particular case since we are aware that we have a database about the current offenders in our records. By observing the incident, the eyewitness would be able to identify the suspected image and confirm that the portrait he painted matches the face that was observed at the specific crime. We must first divide the face into six equal sections, representing the hair, head, eyes, nose, mouth, and chin, in order to compare it to the database that already exists. Face identification would be made simpler by dividing the data. Most of the time, it would be obvious that the photos were split. As seen in the graphic below, an image is divided into six equal parts: the hair, forehead, eyes, nose, mouth, and chin.

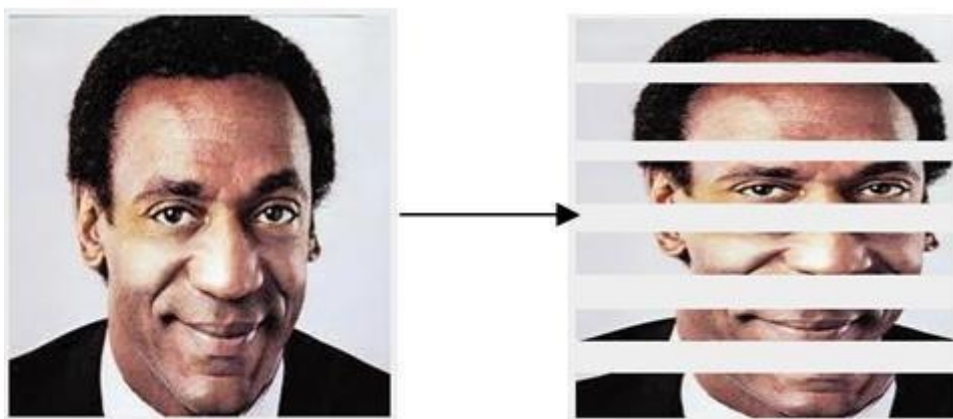


Fig. 3: Clipping a face in to various parts.

Now that the face has been broken up into sections, it will be simple to compare the offender with the database. Now that we have these components, we can put together the eye-witness. Any facial clipping can be combined with any other clipping to create a new face for the purpose of creating a new image. Now that we have these freshly created faces, we can compare them to the previously saved images in the database and begin matching the entire image with the images that share some characteristics in order to get the best match from the database that is now accessible. Finally, a specific outcome that might be regarded as the ideal suspect is displayed on the screen. It will be straightforward to compare the offender with the database now that the face has been segmented. We can put together the eye-witness now that we have these elements. For the purpose of making a new image, any facial clipping can be joined with any other clipping to generate a new face. With these newly formed faces in hand, we can now compare them to the previously saved images in the database and start matching the whole image with those that share certain traits in order to get the best match from the database that is now accessible. Finally, a particular result that could be viewed as the ideal suspect is shown on the screen. By employing the suggested method, the full bio-data of the offender would be displayed by simply providing the data as a face image if the face features are matched with the database [3,4]. The investigative team would benefit from learning one or more details that might aid in locating the culprit.

The Image Partitioning Algorithm:

Step 1: Make six equal divisions in the image for the hair, forehead, eyes, nose, mouth, and chin.

Step 2: The face has now been broken up into its component parts, making it simple to construct new faces and compare the offender to the database.

Step 3: Create new faces based on the eyewitness's perception using these parts.

Step 4: Compare the database with all the face partitions. From the database, it would produce a list of responses that had been matched—possibly more than one.

Step 5: Start a comparison procedure to match the entire image with photographs that have certain similarities so we may select the most appropriate suspect from the database of suspects available.

Step 6: We would thus arrive at a specific image that exhibits the most matches after doing recursive match calculations on all the image's components against database images. Consequently, a picture of the alleged perpetrator appears that is a perfect match.

ADVANTAGES OF THE PROPOSED SYSTEM

- For reliable multiple face detection in video streams and still photos, fast and precise facepositioning is used.
- Identification of many faces simultaneously in a single shot
- Large face databases can be handled by it

CONCLUSION

By utilizing the human capacity to remember intricate facial information, the CFD project seeks to develop an automated criminal face detection system.

Instead, then relying on police technicians to manually slice through various photographs of criminals in order to create images, which typically results in low-resolution and blurry images, dedicated criminal face detection systems can help in facial detection of criminals. The goal of this system is to locate criminals in any investigation department.

REFERENCES

1. Face detection and recognition, *IEEE Paper*
2. Cole, M. I. (1989). *Algorithmic skeletons: structured management of*

- parallel computation*. London: Pitman.
3. Komen, E. R. (1990). Low-level image processing architectures: Compared for some non-linear recursive neighbourhood operations.
4. Bureau of Justice Statistics, U.S. Department of Justice, April 1990), pp. 43-66; Search Group, Legal and Policy Issues Relating to Biometric Identification Technologies.
5. Sérot, J., Ginhac, D., & Dérutin, J. P. (1999, September). Skipper: A skeleton-based parallel programming environment for real-time image processing applications. In *International Conference on Parallel Computing Technologies* (pp. 296-305). Springer, Berlin, Heidelberg.
6. Nicolescu, C., & Jonker, P. (2001, September). A data and task parallel image processing environment. In *European Parallel Virtual Machine/Message Passing Interface Users' Group Meeting* (pp. 393-400). Springer, Berlin, Heidelberg.
7. Haddadnia, J., Faez, K., & Moallem, P. (2001). Human face recognition with moment invariants based on shape information. In *Proceedings of the International Conference on Information Systems, Analysis and Synthesis* (Vol. 20).
8. Caarls, W., Jonker, P. P., & Corporaal, H. (2002, October). SmartCam: Devices for embedded intelligent cameras. In *Proceedings of the 3rd PROGRESS Workshop on Embedded Systems* (pp. 1-4).
9. Cai, D., He, X., Han, J., & Zhang, H. J. (2006). Orthogonal laplacianfaces for face recognition. *IEEE transactions on image processing*, 15(11), 3608-3614.
10. Fatemi, H., Ebrahimmalek, H., Kleihorst, R., Corporaal, H., & Jonker, P. (2003). Real-time face recognition on a mixed SIMD VLIW architecture. *Proceedings of PROGRESS*, 1-6.
11. Deepak, N. R., & Balaji, S. (2016, April). Uplink Channel Performance and Implementation of Software for Image Communication in 4G Network. In *Computer Science On-line Conference* (pp. 105-115). Springer, Cham.
12. Thiagarajan, R., Balajivijayan, V., Krishnamoorthy, R., & Mohan, I. (2022). A robust, scalable, and energy-efficient routing strategy for UWSN using a Novel Vector-based Forwarding routing protocol. *Journal of Circuits, Systems and Computers*.
13. NR, D., GK, S., & Kumar Pareek, D. (2022). A Framework for Food recognition and predicting its Nutritional value through Convolution neural network.
14. Thanuja, N., & Deepak, N. R. (2021, April). A convenient machine learning model for cyber security. In *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 284-290). IEEE.
15. Shanmugam, P., Venkateswarulu, B., Dharmadurai, R., Ranganathan, T., Indiran, M., & Nanjappan, M. (2022). Electro search optimization based long short- term memory network for mobile malware detection. *Concurrency and Computation: Practice and Experience*, 34(19), e7044.
16. Deepak, N. R., GK, S., & Bhagappa (2021, Nov). The Smart Sailing Robot for Navigational Investigation is Used to Explore all the Details on the Zone of the Water Pura. *Indian Journal of Signal Processing (IJSP)*, 1(4).
17. Deepak, N. R., & Thanuja, N. Smart City for Future: Design of Data Acquisition Method using Threshold Concept Technique.
18. Kiran, M. P., & Deepak, N. R. (2021, May). Crop prediction based on

- influencing parameters for different states in india-the data mining approach. In *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 1785-1791). IEEE.
19. Deepak, N. R., & Balaji, S. (2015, December). Performance analysis of MIMO-based transmission techniques for image quality in 4G wireless network. In *2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)* (pp. 1-5). IEEE.