



Securing Criminal Identification: Leveraging Blockchain for Face Detection and Recognition

K.Chandra Sekhar¹, Palika Hemasri², Metta Durga Priya Mounika², Puthukula Sasank², Akshay Bangaru², Girijala Bhoga Avinash²

¹Associate Professor, Department of Computer Science Engineering, Pragati Engineering College, Surampalem, Andhra Pradesh, India.

²Department of Computer Science Engineering, Pragati Engineering College, Surampalem, Andhra Pradesh, India.

To Cite this Article

K.Chandra Sekhar, Palika Hemasri, Metta Durga Priya Mounika, Puthukula Sasank, Akshay Bangaru, Girijala Bhoga Avinash, Securing Criminal Identification: Leveraging Blockchain for Face Detection and Recognition, International Journal for Modern Trends in Science and Technology, 2024, 10(04), pages. 354-358.
<https://doi.org/10.46501/IJMTST1004054>

Article Info

Received: 06 April 2024; Accepted: 18 April 2024; Published: 26 April 2024.

Copyright © K.Chandra Sekhar et al; This is an open access article distributed under the [Creative Commons Attribution License](#), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ABSTRACT

Finding and apprehending a criminal is a complex and time-consuming process. Criminals' tactics for leaving no fingerprints or biological evidence at crime scenes are becoming increasingly complicated. A simple and straightforward approach is to implement cutting-edge facial recognition technology. As security technology has progressed, most buildings and traffic lights now have CCTV cameras to provide monitoring. The camera's video footage can help identify criminals, runaways, missing people, and suspicions. This project investigates the use of deep neural networks and machine learning to create a criminal detection system. The concept detailed below is a clever approach to streamlining law enforcement.

Keywords: machine learning, face recognition, neural networks, criminal identification, CCTV

1. INTRODUCTION

Biometrics is a means of identifying or authenticating individuals based on their distinct patterns of physical or behavioral features. As biometric technology advances, biometric scanners become more inexpensive. A increasing number of procedures and services are also available, providing exceptional security and a positive client experience. Biometric technology is gradually replacing traditional authentication systems. Facial recognition is one of the most advanced biometric technologies. A person's face is the most important

portion of their mortal body in terms of relationships. A person can be recognized by their face. Facial recognition is a difficult subject that is utilized for identification in security systems, financial services, search, and other applications. A computer needs a different approach to recognize a face than a person does. People often and readily execute the task of facial recognition in their daily lives. Programmers are ecstatic to create motorized film and recordings for a variety of applications, including biometric evidence, observation, mortal-PC organization, sight and sound administration, and so on,

because of the wide availability of outstanding and easy to maintain work areas and fitted registering fabrics. It is standard practice to study new ways to programmed facial recognition. Face recognition systems are expected to automatically recognize faces in photos and videos. It operates in two modes: face identification (also known as recognition) and face verification (also known as authentication). A face check is a coordinated match of a format face (datasets) image with a shifted point to a black-and-white grayscale image. Face recognition evidence consists of one-to-many matches, which look for matching between a person's photo or videotape and every format film in the database [1]. A watch-list check is an extra facial recognition scenario in which a suspect list and an inquiry face are synced (one-to-many). Face recognition research is driven by large-scale, real-time operations that can speed up and simplify standard identification systems. Face recognition encourages the experimenter to accurately detect faces by presenting barriers. Face recognition has become the most popular biometric due to its simplicity of use and identification. The relevance of the trend might be attributed to easily available digital cameras and rising desire for security. The benefit of face recognition over other biometric technologies is that it is natural, nonintrusive, and simple to use.

2. LITERATURE SURVEY

Face recognition applications have evolved since the 1960s, [2] when the technique of utilizing a RAND tablet to coordinate facial characteristics was developed. A RAND tablet was a gadget that allowed users to input vertical and horizontal coordinates on a grid using a pen that emitted electromagnetic pulses. The entire system was used to manually record the coordinate positions of many facial characteristics, such as the eyes, hairline, mouth, and nose. It takes face recognition to a different level by employing 21 distinctive facial attributes including the color of hair, chin, nose elevation, skin color, etc. [5].

During the, we presented the world to eigenfaces and a statistical method to face recognition. Eigenfaces employ Eigenvalues and Eigenvectors to decrease dimensionality and project sample/training data onto tiny feature faces. This is the fundamental notion underlying Principal Component Analysis (PCA).

The first instance of employing facial recognition for law enforcement occurred in 2002. Since then, criminal identification has emerged as a key use of facial recognition. The "FRCI" [7],[8] criminal identification system is created using a dimensionality reduction approach known as principal component analysis. [12] And employs the Haar-Features technique, as described in. In a Harr feature system, the detection window is made up of solid rectangles that represent distinct characteristics. A Haar-like the feature evaluates neighboring rectangular sections in a detection window at a specified position, adds the intensities of the pixels in each sector, and computes the difference between these sums. Adriana Kovashka and Margaret Martonosi presented a method in [10] that incorporates 18 elements, including RGB [12].

After the success of neural networks for computer vision issues like face recognition in 2010, a hybrid model called "ABANN" [13] was developed by combining AdaBoost and ANN. Many deep learning models have been used particularly for face recognition, such as Retinal connected Neural Network, Rotational Invariant Neural Network, Back Propagation Neural Network, Fast Neural Network, and so on.

The primary focus of our study will be on (FaceNet), [14] an embedding approach that maps facial characteristics to a "compact Euclidean Face-Map" that is utilized to discover differences between the faces in the database. A deep convolutional neural network technique is utilized, with each face transferred to 128 bytes and the tasks of identification, detection, and grouping performed. Two datasets had an accuracy rate of more than 95%.

3. SYSTEM ANALYSIS

METHODOLOGY

Orders for Face Recognition Facial recognition may be done in one of two ways: geometric, which is based on points, or photometric, which is based on views.

Geometric

This technique relies on the geometric connection between face milestones. It identifies the spatial arrangement of the characteristics on the face. This technology identifies facial characteristics such as the eyes, nose, mouth, and eyebrows. It learns the locations of these characteristics. The faces are uniquely connected by calculating the geometrical distances and angles between the characteristics (4). The geometric method to

face recognition works as follows. It indicates the spots on the face's prominent corridors, such as the eyes, nose, and lip border. Furthermore, just these points are analysed, and the geometrical distance between them is determined to uniquely identify the face.

Photometric stereo

This approach employs several prints/images of a person taken in various lighting conditions and from different angles. Recover the form of the face using a grading chart. This picture consists of an array of normal faces. In the photometric stereo technique, several photos of the same face are used to create a grade chart and determine the single image. This research proposes the use of a geometric-based technique to detect and describe facial features. Both of them are good for feting faces. When working with merely software, the geometric system is the most fashionable solution for openCV. () Haar point is used to identify the object, just faces to be uprooted. The Haar waterfall method has four stages: (a) Haar Point Selection (b) Generating Integral Images (c) Adaboost Training (d) Slings Classifier. This technique requires a large number of positive and negative photos; thus, it reduces the facial images to a grayscale image. The grayscale picture fragments are from it. A Haar point extracts adjoining blockish in each specific section of the discovery window and determines the discrepancy between these entries. A separate point, such as an edge point, line point, or four-cube point, will be indicated on the face. The distance between the brows will be a line point, and the side of the eye will be an edge point, however various kernel sizes and positions are employed. Occasionally, it becomes inapplicable for application on the cheekbones or any other region, so AdaBoost ().

Face Discovery A human can descry the face naturally.

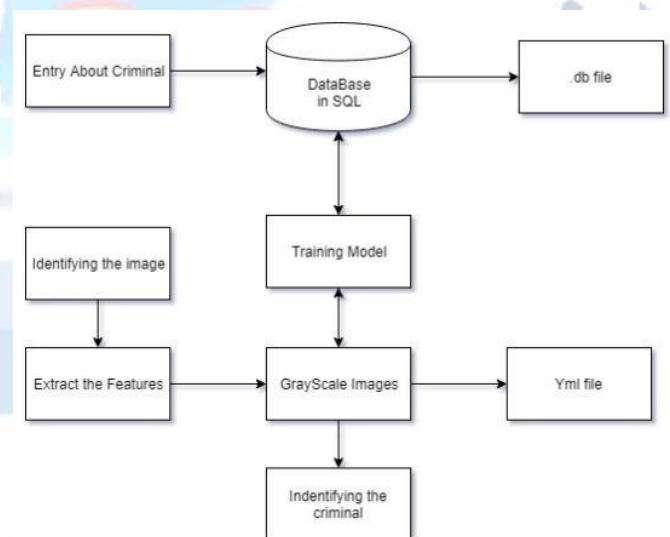
It is a difficult problem for a computer to find and recognize faces. A computer requires data in the form of a finite number of rudiments, each with a specific place and value. The values are expressed in terms of pixels, bit images, and picture elements. These rudiments serve as the prerequisite for descrying the face. Face discovery entails dividing picture windows into two categories: faces and on-faces. First, use point birth to recognize faces. Facial point birth is either texture or shape anchored. Texture-based styles use the original texture and the pixel values surrounding a given spot. Log Gabor. Some of the texture-based face point birth

methods include the sea network, neural-network-based eye point sensor, and hierarchical two-positional sea network. The shape-based facial point birth techniques include direct appearance models, active sea networks, and element-based 3D morphable models. Some cold-blooded approaches, such as AdaBoost with form restrictions and elastic bunch graph matching, employ both textures and shapes. This mongrel approach is used in OpenCV grounded face finding, particularly by the AdaBoost system. The process of face finding may be separated into

(a) Pre-processing: To lessen the variety in faces, images are repeated before bracketing. Only positive anterior face photos are utilized for bracketing. It compares the contrast between dark and white borders of faces. Using the usual approach, reused photos are rectified.

(b) Bracket: The OpenCV bracket classifies pictures as faces or no faces using neural networks trained on various exemplifications. To maximize the findings, several network configurations are explored with.

(c) Localization: OpenCV searches for faces in images using a trained neural network. If the picture is present, place it in the bounding box. The input entered via VHS, photos, or webcam passes through the preprocessing.



The point birth is performed utilizing localization to determine the specific face. Figure 1 depicts the whole process of relating and feting the face. Face Recognition operates in the fields of identity, authentication, security, surveillance systems, mortal-computer commerce, psychology, and so on.

OpenCV

OpenCV (Open-Source Computer Vision collection) might be a collection of programming functions primarily geared at real-time computer vision. The classifier determines the distinctions between positive and negative images.

The positive picture represents the face, while the negative image represents the Farnon face. OpenCV trains the classifier on any face specified in the program, resulting in a fully trained and ready-to-enforce face discovery classifier. Two lines haarcascade_frontalface_alt.xml and hear cascade eye are utilized to detect the face and eye Independently. OpenCV also provides the LBP (Original Double Pattern) waterfall classifier, which uses original double patterns to train grayscale images ranging from hundreds to thousands of pixels. LBP analyses every 9 pixels in a 3×3 window. Compare the value of the central pixel to that of the eight pixels around it. Each pixel that is smaller than the central pixel value is replaced with a 1; for lower values, the value is changed to 0. Eventually, it builds the block histogram to make one picture, and one point image turns it into a yml format for further presenting the face.

4. SYSTEM DESIGN

SYSTEM ARCHITECTURE

Below diagram depicts the whole system architecture.

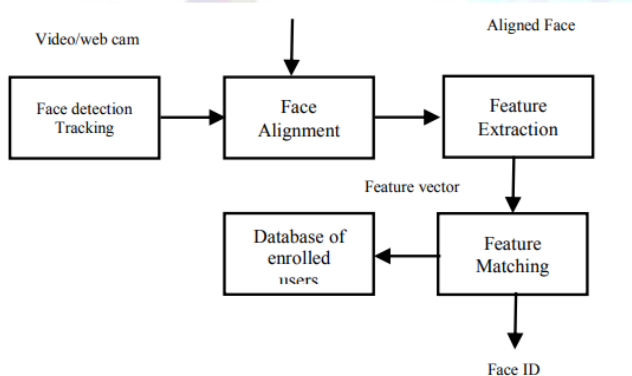


Fig 1. Methodology followed for proposed model

5. SYSTEM IMPLEMENTATION

MODULES

The "Blockchain-Powered Facial Recognition" project may be divided into components to enable efficient development and usefulness. Here are the five main modules for this project:

Data Acquisition and Preprocessing: This lesson focuses on gathering and creating a collection of criminal photographs. Data preparation procedures, such as scaling, normalization, and augmentation, are used to guarantee that the data is acceptable for training the deep learning model.

Deep Learning Model Development: In this module, the Convolutional Neural Network (CNN) model is created and trained to recognize criminal facial patterns in photos. This module defines the model architecture, hyperparameters, and training techniques that maximize model performance.

Real-time Image Processing: This module entails gathering and processing visual data in real time with cameras or other imaging devices. The trained deep learning model detects face patterns in incoming photos.

Alert and Notification System: When the system detects a probable fire or face pattern, this module is in charge of sending notifications. It may involve the creation of audible alerts, notifications for users, and potential interaction with emergency response services or communication networks.

Monitoring and Reporting: This module includes a user interface or dashboard for monitoring system performance and the status of the criminal detection procedure. It may also create reports and logs for analysis, review, and future changes to the system.

6. RESULTS AND DISCUSSION

The above method was completed in a Jupiter notebook using the Python programming language. During the face detection step, pixels for the face and bounding boxes were precisely produced. The next graphic displays pixels for recognized faces of one offender from

```

[[[ 41 41 41]
 [ 49 49 49]
 [ 62 62 62]
 ...
 [203 203 203]
 [195 195 195]
 [191 191 191]]

[[ 20 20 20]
 [ 21 21 21]
 [ 20 20 20]
 ...
 [ 45 45 45]
 [ 45 45 45]
 [ 43 43 43]]

[[ 38 38 38]
 [ 46 46 46]
 [ 57 57 57]
 ...
 [205 205 205]
 [194 194 194]
 [188 188 188]]

[[ 18 18 18]
 [ 18 18 18]
 [ 18 18 18]
 ...
 [ 40 40 40]
 [ 41 41 41]
 [ 43 43 43]]

[[ 39 39 39]
 [ 47 47 47]
 [ 57 57 57]
 ...
 [204 204 204]
 [194 194 194]
 [188 188 188]]

[[ 20 20 20]
 [ 19 19 19]
 [ 18 18 18]
 ...
 [ 44 44 44]
 [ 43 43 43]
 [ 43 43 43]]
  
```

Fig.5. Pixels for detected faces of one criminal

Moving on, face embeddings for all of the photos in the dataset were produced using FaceNet. It is plainly noted that the FaceNet model is loaded 40 and 88 photos were transformed to face embedding, each with 128 vectors.

```
Loaded Model
WARNING: tensorf1
(40, 128)
(88, 128)
```

The model is trained during the classification phase, and the accuracies achieved after evaluating the training and testing datasets are listed below. Finally, random pictures were displayed, and the random face's identity and likelihood were predicted. The following table displays the findings.

Accuracy: train=92.500, test=90.909

Search Result

The screenshot shows a web interface for criminal identification. At the top left is a profile picture of a man, and at the top right is a red 'VALID' stamp. Below this, there are two main sections: 'Personal Details' and 'Crime Details'.

Personal Details:

- Criminal Name: John
- Criminal Email: john@gmail.com
- Criminal Aadhar: 987654321000
- Criminal Address: Hyderabad

Block Used:

- 14f5e2ed4b47db5e372f35716f604b9d2a23c
- c5b909a95694ccc6ae7982a64636
- a07873eb4c72ba61382e4b38c393c2b67844
- 4f2ade61a57e3f84c4ed3b09c30fe3f0998c3

Crime Details:

S.no	Crime Type	Crime Description
34	Fraud	Bank Credit Card Fraud

fig 2. Criminal Identification

7. CONCLUSION AD FUTURE WORK

The substantiation is accessible; at the crime scene, it is simple to identify the perpetrator using sketches and other evidence. However, when a crime occurs without evidence, a facial recognition technology can be utilized to identify the perpetrators. These models are extremely beneficial for identifying the perpetrator following a crime. The technology identifies felonies, which is beneficial in stopping the crime. The system's limitations include the fact that most of the time, the criminals do not face the camera or evade it. The precise face may be anatomized by roots the lower characteristics of the face, such as the depth of the eye.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

- [1] Di Huang, Caifeng Shan, Mohsen Ardebilian, Yunhong Wang, and Liming Chen, "Original Double Patterns and Its Application"
- [2] Abdellatif Hajraoui, "Robust System of Face Recognition," unpublished.
- [3] L. Chen, et al., "3D Shape Constraint for Facial Point Localization using Probabilistic-suchlike Affair", Proc. IEEE Int'l Factory Analysis and Modeling of Faces and Gestures, pp. 302-307, 2004.K. Elissa.
- [4] Cristinacce, T. Cootes, "Facial Point Discovery Using AdaBoost with Shape Constraints", British Machine Vision Conference, 2003.
- [5] L. Wiskott, et al., "Face Recognition by Elastic Bunch Graph Matching," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 19, no. 7, pp. 775-779, 1997.
- [6] Morphable Models," 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'04), June 27-July 2, 2004, Washington DC, USA.
- [7] B. Weyrauch, et al, "Element- grounded Face Recognition with 3D.
- [8] S. Yan, et al., "Face Alignment using View- Grounded Direct Appearance Models," Int'l J. Imaging Systems and Technology, vol. 13, no. 1, pp. 106-112, 2003.
- [9] C. Hu, et al., "Real- time view- grounded face alignment using active sea networks," Proc. IEEE Int'l Factory Analysis and Modeling of Faces and Gestures, pp. 215-221, 2003.
- [10] M.J.T. Reinders, et al., "Locating countenance in Image Sequences using Neural Networks," Proc. IEEE Int'l Conf. Face and Beckon Recognition, pp.230-235, 1996.
- [11] E. Holden, R. Owens, "Automatic Facial Point Discovery," Proc. The 5th Asian Conf. on Computer Vision, 23-25 January 2002, Melbourne, Australia.
- [12] Sushil Kumar Paul, Mohammad Sharif Uddin, Saida Bouakaz, "Face Recognition using Eyes, Nostrils, and Mouth Features", Page 1-3.
- [13] Gary Bradski and Adrian Kaehler, "Learning OpenCV", September 2008 First Edition, Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.