Global Journal of Engineering and Technology Advances

eISSN: 2582-5003

Cross Ref DOI: 10.30574/gjeta

Journal homepage: https://gjeta.com/

(Review Article)

Leveraging openCV and image processing for crime identification through facial recognition

Mahjabeen [*], Swapna T, Shazia Anjum and Megha D

Department of Computer science & Engineering, Navodaya Institute of Technology, Raichur, India.

Global Journal of Engineering and Technology Advances, 2024, 21(01), 146–153

Publication history: Received on 13 September 2024; revised on 20 October 2024; accepted on 23 October 2024

Article DOI: https://doi.org/10.30574/gjeta.2024.21.1.0196

Abstract

To maintain the safety and security of communities, law enforcement agencies provide vital functions such as crime prevention and identification. Identifying people with a criminal record efficiently and accurately is one of the biggest hurdles in this field. This study delves into a fresh strategy for taking on this problem by making use of state-of-the-art image processing methods and machine learning algorithms. The project's main goal is to identify convicted felons by utilizing OpenCV, a robust open-source computer vision toolkit, and different facial recognition algorithms. By giving them a tool that guarantees a faster reaction rate and improved accuracy in suspect identification, the system is aimed to boost the capacities of law enforcement organizations. This project is based on the tenet of criminal psychology, which states that criminals are prone to committing new crimes. The system's goal is to detect and track repeat criminals both before and after they commit crimes by making use of this information. The method works by taking pictures of people who are known to be criminals and putting them in a database. From there, they can be compared to either live video streams or static photographs taken by surveillance cameras. In order to analyze and identify facial characteristics effectively, algorithms like LBPH and the Haar cascade classifier are also used. The system's robustness and efficiency are guaranteed by integrating these approaches into the OpenCV framework. This research makes a valuable contribution to the field of crime prevention by offering law enforcement authorities a dependable and scalable alternative. This system provides a streamlined interface for storing, retrieving, and matching facial photos. It was built using Python 3.5 and uses SQLite to manage the database of offenders' details. Proactively monitoring persons with a criminal record is made easier and faster with the suggested method. Suspect identification is also made easier. This research showcases the possibility of integrating machine learning and image processing to enhance public safety and crime prevention initiatives. It is an early step towards more complete video surveillance systems.

Keywords: Facial recognition; Image processing; Suspect identification; Public safety; Machine learning algorithms; Surveillance systems;

1. Introduction

A photograph and other personal details are part of an individual's criminal record. Detailed information regarding any person having a criminal past is necessary for us to be able to identify them. Facial recognition is one way. As a primary means of communicating one's personality and emotions, the human face commands our undivided attention in all social encounters [1]. An astounding ability of the human mind is the ability to recall and recognize individual faces. In an effort to catch repeat offenders, this technology offers real-time details on a person and seeks to imitate the human capacity to identify them. In a dispersed situation, a criminal face identification system[2] can locate an individual whose image matches an existing record in a database of known offenders. In the realm of video-based facial recognition and monitoring, this initiative will be a major milestone.

[*] Corresponding author: Mahjabeen

The use of technology in identifying criminals and preventing crime has become crucial due to the increasing impact of technology in our daily lives. Law enforcement agencies and security systems now have powerful tools at their disposal to enhance public safety and combat criminal activities thanks to the utilization of advanced image processing techniques like OpenCV [3] (Open Source Computer Vision Library), Haar Cascade, and Local Binary Patterns (LBP).

In this study, we look into how OpenCV, Haar Cascade[4], and LBP algorithms [5] can be used for criminal identification and crime prevention, particularly in face recognition. Given its great accuracy and lack of invasiveness, facial recognition has quickly become a popular biometric method.

The OpenCV package was specifically designed for real-time computer vision, therefore we will start by exploring it [6]. Object detection, image processing, and machine learning are just a few of the many uses for OpenCV's extensive library of functions and algorithms. It is an essential component in the development of several security applications because of its effectiveness and adaptability.

We will now go into Haar Cascade classifiers [7], which are machine learning-based approaches used for object detection. In order to detect objects like faces, eyes, or smiles in images or video streams, these classifiers use a succession of basic classifiers. Haar Cascade may be trained to recognize and differentiate particular patterns using training data, making it a vital tool for face identification and recognition.

An important part of our conversation is Local Binary Patterns (LBP) [8]. In computer vision, LBP is used as a texture descriptor for classification purposes. Making a binary pattern requires looking at each pixel in context with its neighbors. The detailed textural information of an image is then encoded using this pattern. Because it can withstand changes in both lighting and facial expressions, the Local Binary Patterns (LBP) algorithm performs exceptionally well on face recognition tasks.

Numerous uses in crime prevention [9] and criminal identification are made possible by integrating these technologies. When combined with facial recognition technology, surveillance systems [10] can detect suspicious persons in real-time and keep tabs on them, alerting authorities to potential threats. Also, using surveillance footage or forensic photos, these technologies can help law enforcement agencies identify perpetrators.

Although these technologies provide great potential, they also raise concerns about privacy and ethics. Addressing concerns like data security, consent, and misuse potential is critical for responsible deployment.

This research will look at the hows and whys of using these technologies, how well they work to deter crime, and what ethical questions arise when using them. By mastering and applying OpenCV, Haar Cascade, and LBP, we can build robust systems that strengthen society's safety and security.

2. Literature Survey

Our tool of choice was OpenCV, which has a Haar cascade classifier tailored to face detection. To identify different facial features, the Haar cascade classifier uses the AdaBoost algorithm. The first step is to read the target image and turn it into a grayscale version. The next step is to load a Haar cascade classifier so it can identify if the picture has a face. When this checkbox is checked, the system draws a rectangle around the detected face after analyzing its features. Instead, it looks at the next picture and decides what to do with it [3].

In its most fundamental form, a rectangular Haar-like feature [4] is defined as the difference between the sum of all pixels inside and outside the rectangle. You have complete control over the placement and size of this rectangle within the source image. The modified set of characteristics is called the 2rectangle feature. At this point, we are looking at facial pictures and analyzing them for Haar traits. Each feature's weight, size, and features are generated using the AdaBoost machine learning method.

A pixel's contrast information relative to its neighbors can be described using the LBP operator. The 3x3 frame specifies the original Local Binary Patterns (LBP) [5] operator. The technique examines the grayscale values of the 8 pixels around the median pixel to determine the window's threshold. A pixel is given the value 1 if its neighboring pixel value is greater than or equal to the median pixel value. In all other cases, a value of 0 is used. In accordance with equation 1, the function is defined.

$$N(x) = \begin{matrix} 1, x \geq 0 \\ 0, x < 0 \end{matrix} \quad \text{……………….eq. (1)}$$

The SQLite database has been successfully utilized by many desktop applications, including those for financial analysis, record keeping, version control, media cataloging and editing, and computer-aided design (CAD). The file format is on-disk.

Using SQLite for this specific application has many advantages:

- Small and Light: SQLite is a great database for embedded software in devices like mobile phones, cameras, TVs, and other household electronics since it is efficient and uses few resources.
- Improved Speed: SQLite databases are known for their lightning-fast reading and writing capabilities. The speed difference between it and the File system is more than 35%. Instead of reading the whole file and storing it in memory, it loads only the data that is needed. If you make changes to smaller areas of the file, only those sections will be rewritten.
- SQLite is very accessible and easy to use; no installation is necessary. Setting anything up or installing anything is not necessary. To facilitate database construction, all you need to do is install the SQLite libraries on your PC.
- Reliable: The system regularly updates your stuff, so there's less chance of data loss in case of a power outage or system crash.
- SQLite is portable because it works with both big-endian and little-endian architectures and all operating systems, whether they are 32-bit or 64-bit.
- Less Complexity and Money Spent: Short SQL queries, as opposed to long and prone to error procedural queries, cut down on application costs by making content access and updates faster.

3. Methodology

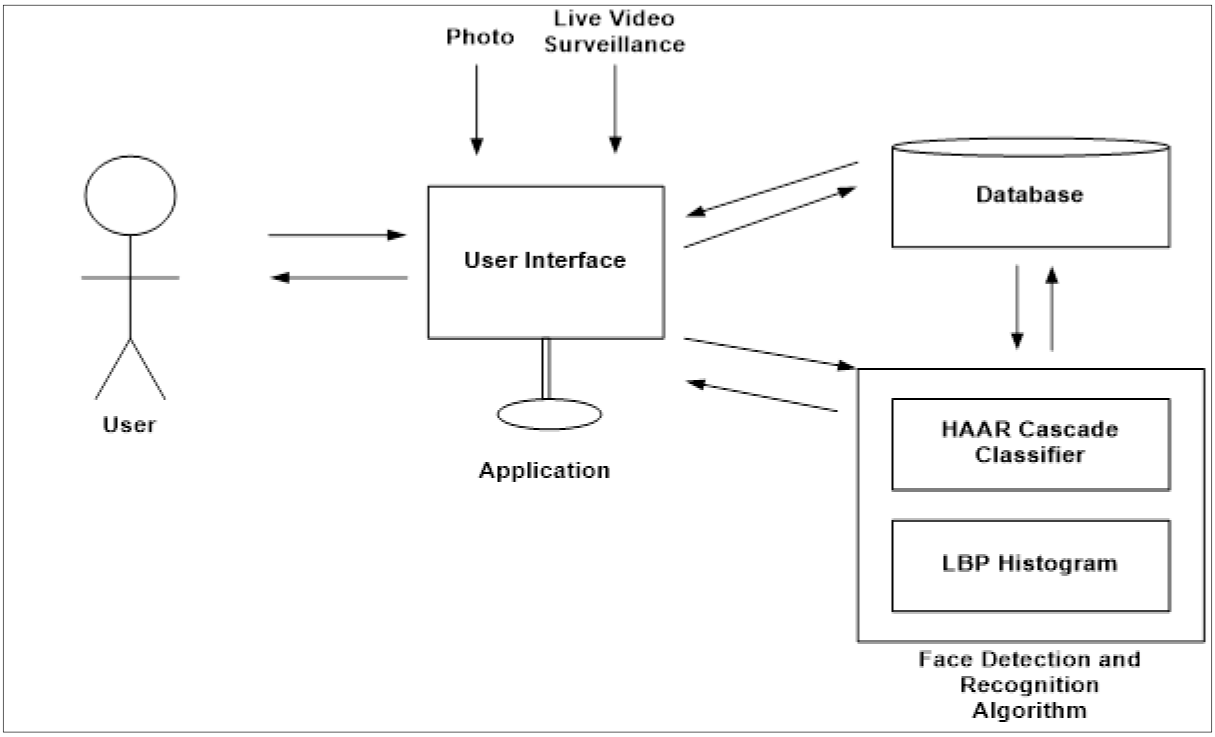


Figure 1 System Architecture

3.1. Import the necessary modules

Facial recognition requires the following modules: numpy, the image module, cv2, and os. Face detection and recognition capabilities are provided by the cv2 module, which is an OpenCV component. Image and directory path manipulation will be carried out by means of the operating system (OS). At the outset, we access the database directory for picture names using this module. The faces in each picture are then identified using the unique identifiers extracted from these names. To read the grayscale picture, the PIL picture module is used.

3.2. Load the cascade for face detection

First thing to do while loading the face detection cascade is to check if each image has a face. We use the face-containing region of interest that we obtained to train the recognizer. The OpenCV Haar Cascade method will be employed for face detection. You may find OpenCV's supplied Haar cascades in the directory where you installed OpenCV. For face detection, the haarcascade_frontalface_default.xml file is used. To load the Cascade, we use the cv2 CascadeClassifier method. To use it, you must provide the location of the cascade.yml file.

3.3. Create the face recognizer object

Making the face recognizer object is the next step. Features like FaceRecognizer are available in the face recognizer object. To train the recognizer and FaceRecognizer, use the train() function. For precise face recognition and classification, use the predict() function. Current face recognition algorithms available in OpenCV include Eigenface Recognizer, Fisherface Recognizer, and Local Binary Patterns Histograms (LBPH) Face Recognizer. Because of the flaws that exist in real-life situations, we have used the LBPH recognizer. Neither can we promise you ten separate shots of the same person under ideal lighting circumstances.

Picture feature extraction from localized regions is the main focus of the LBPH algorithm. Instead of seeing the whole picture as a multi-dimensional vector, the idea is to zero in on describing the object's unique attributes. By comparing the size of each pixel to its immediate surroundings, the core idea of Local Binary Patterns is to compress the local arrangement in an image. Modifications made in a monotonic grayscale cannot affect the LBP operator.

3.4. Assemble the training set and Conduct the training

In order to construct the training set, we will define a function that takes the absolute path to the image database as an input parameter and returns a tuple with two lists. The faces that have been identified will be in one list, while the labels that go with them will be in another. For example, the value at the ith position of the label list will be 4 if the ith place in the face list corresponds to the 4th person in the database. The next step in training with the Face Recognizer is to move forward with this. Training function. Here, the features are the face pictures, and the labels are the extracted individual numbers from the image names, which are used to identify each face. These two parameters are required by the function.

3.4.1. Dataset Used

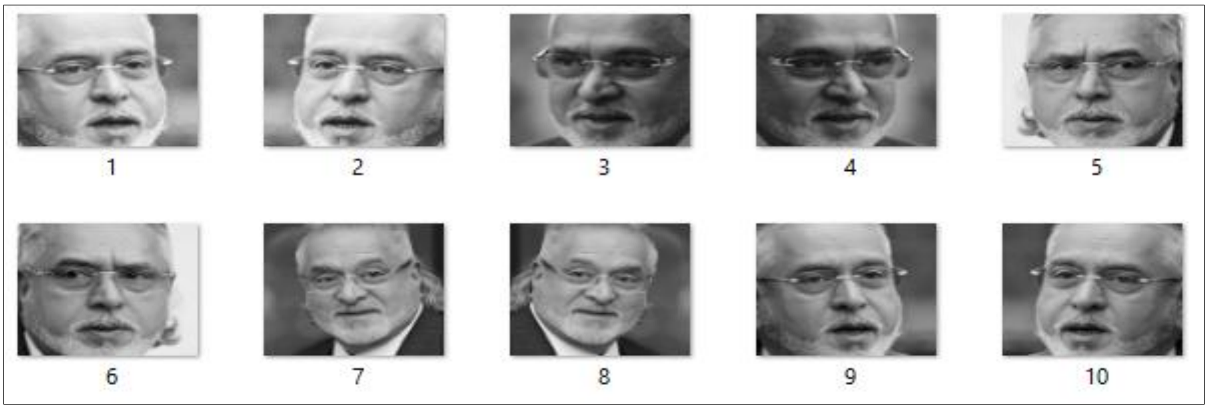


Figure 2 Dataset of a person generated by System

4. Results

4.1. Home Page

This section contains the sequential addition of the results displays. The Criminal Identification System application's homepage is shown in Figure 3 below. There are three buttons on it: Video Surveillance, Photo Match, and Register Criminal.

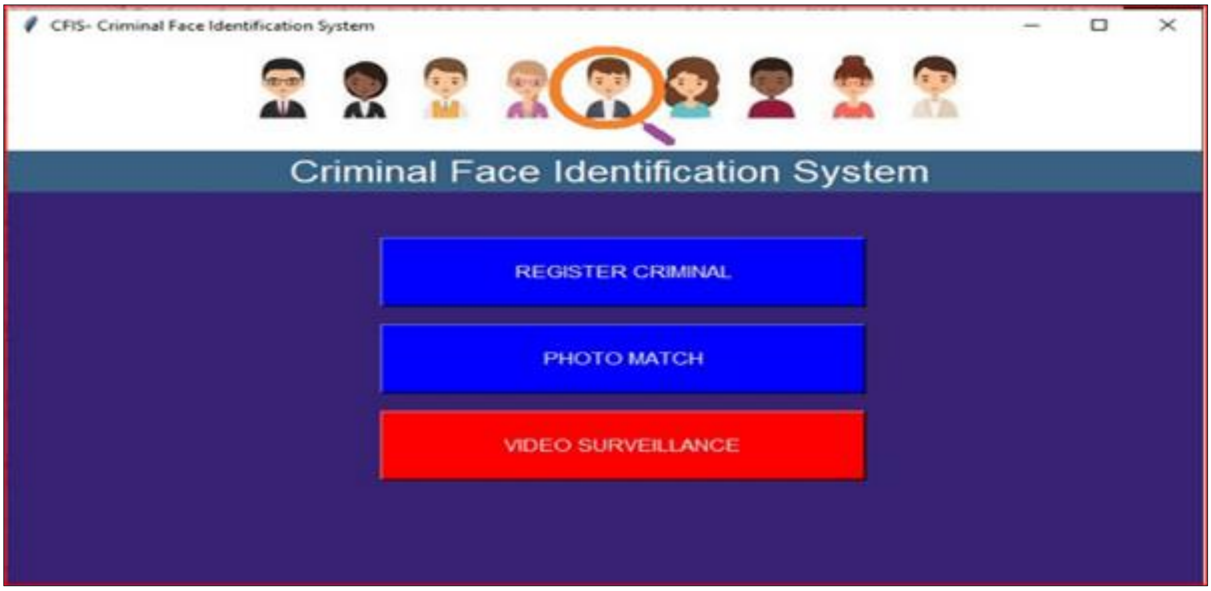
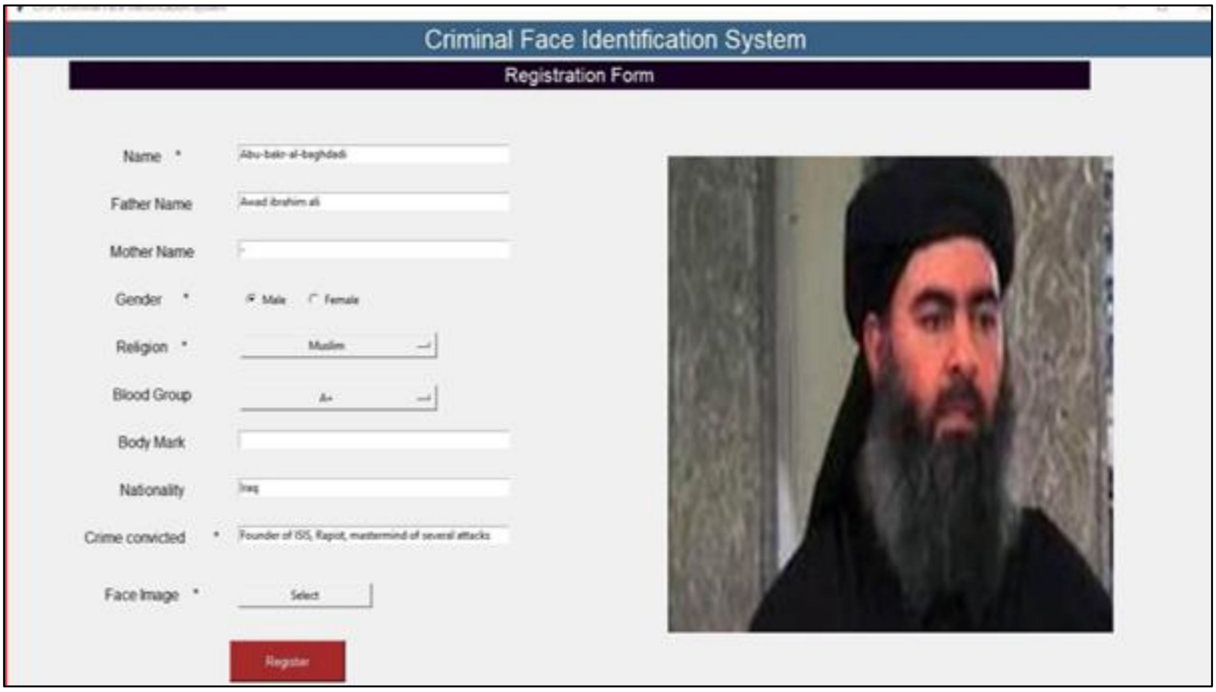

CFIS- Criminal Face Identification System
Criminal Face Identification System
REGISTER CRIMINAL
PHOTO MATCH
VIDEO SURVEILLANCE

Figure 3 Home Page

4.2. Criminal Registration

Figure 4 shows the layout of the criminal registration page, which will capture a minimum of 20 photographs of each offender before adding them to a database of those who need to be registered. The page also includes an input form where users can enter the offender's name, date of birth, identification mark, profile picture, and other personal details. A user will be able to register after they have chosen their photographs and entered their details. If all goes according to plan, the criminal will be officially recorded.



Criminal Face Identification System

Registration Form

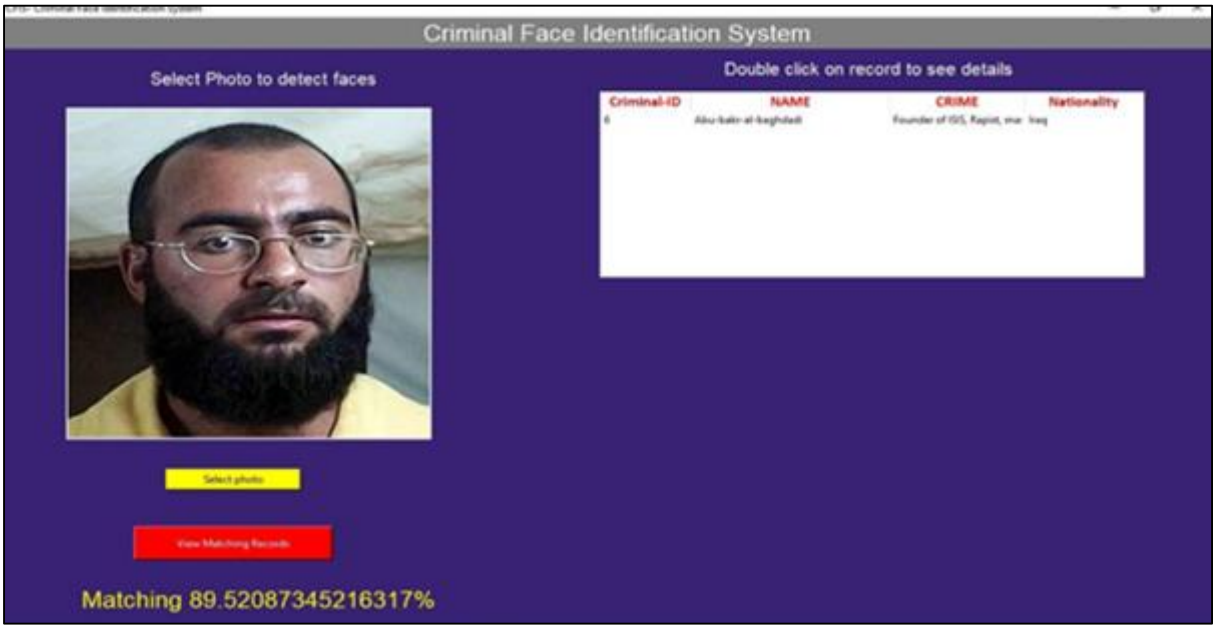
Name *	Abu-bakr-al-baghdadi
Father Name	Awad ibrahim ali
Mother Name	
Gender *	● Male ○ Female
Religion *	Muslim
Blood Group	A+
Body Mark	
Nationality	Iraq
Crime convicted *	Founder of ISIS, Rapist, mastermind of several attacks
Face Image *	Select

Register

Figure 4 Registration page

4.3. Detect Criminal Page

Below figure 5 is a page that lets the user view a system image and maybe spot a criminal or crooks in it. By clicking on the names of the detected criminals, the user may also view their profile.



Criminal Face Identification System

Select Photo to detect faces

Double click on record to see details

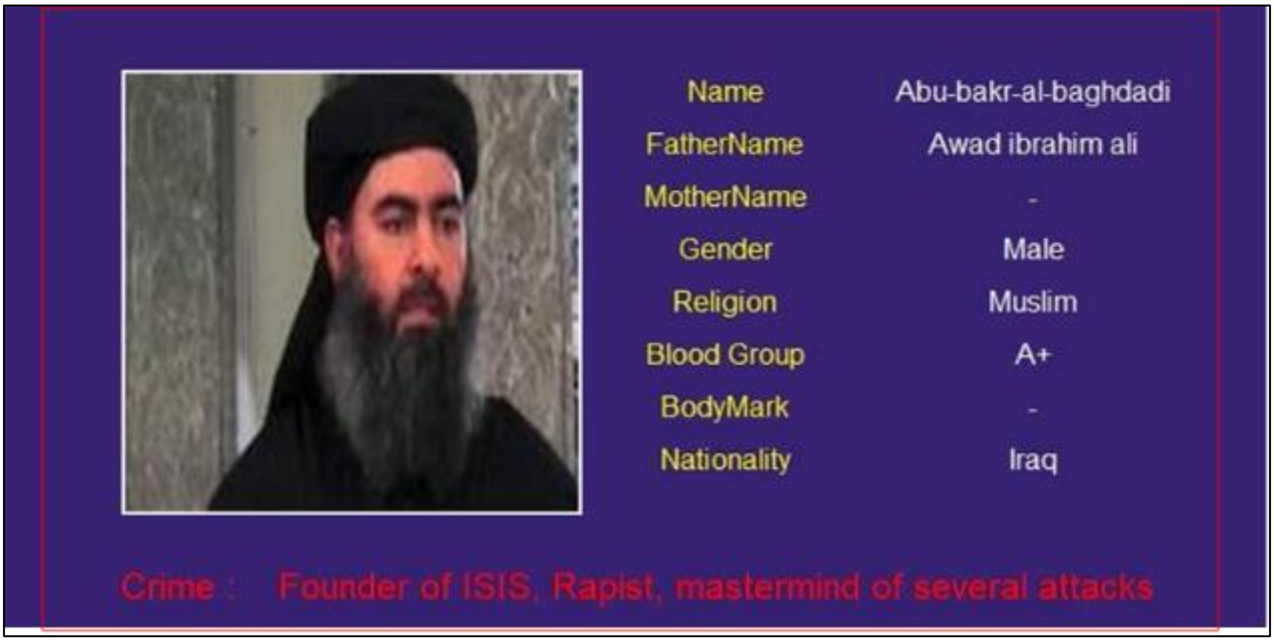
Criminal-ID	NAME	CRIME	Nationality
6	Abu-bakr-al-baghdadi	Founder of ISIS, Rapist, mas	Iraq

Matching 89.52087345216317%

Figure 5 Detect face from image

4.4. Criminal Profile Page

After clicking on a criminal's name on the page that says "detect criminal" or "video surveillance," the page shown in figure 6 below will display the criminal's profile.



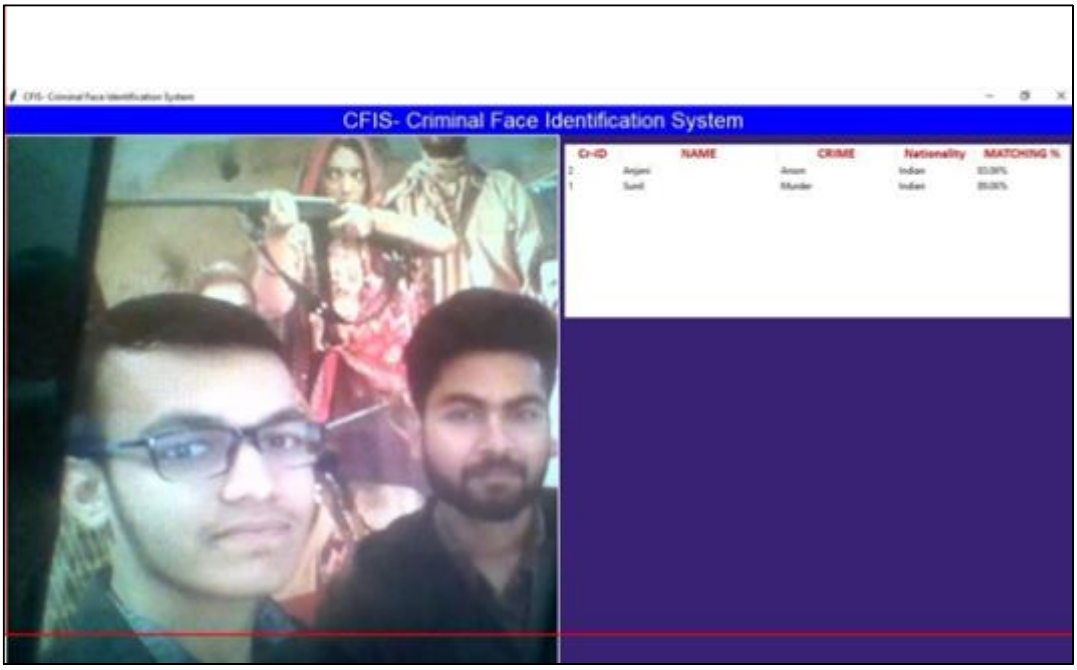
Name	Abu-bakr-al-baghdadi
FatherName	Awad ibrahim ali
MotherName	-
Gender	Male
Religion	Muslim
Blood Group	A+
BodyMark	-
Nationality	Iraq

Crime : Founder of ISIS, Rapist, mastermind of several attacks

Figure 6 Details of Criminal

4.5. Video Surveillance

Figure 7 up top shows the website that will take real-time video frames using the computer's webcam. The system will then identify and apprehend perpetrators in the video as they happen by using a facial detection module to every frame. The user can also view the criminal's profile by clicking on the names of those who have been detected.


CFIS- Criminal Face Identification System
CFIS- Criminal Face Identification System

Cr-ID	NAME	CRIME	Nationality	MATCHING %
2	Anjani	Arson	Indian	83.06%
1	Sunil	Murder	Indian	85.06%

Figure 7 Video Surveillance

5. Conclusion

This research details a system that can identify and identify criminal faces in live video and still photos. In our approach utilizing OpenCV for face detection, we have utilized Haar feature-based cascade classifiers. Using a big dataset of both positive and negative images, this method trains a cascade function using machine learning. Furthermore, we have used LBPH (Local Binary Patterns Histograms) to identify faces. Research like this will be a huge step forward for facial recognition and surveillance systems that use video. Using this approach has several advantages: The best way to choose features, It is not necessary to scale the image in order for a detector that is invariant to position and scale to identify objects. The detection qualities are instead scaled. Because of this, it is possible to teach a general detection system to recognize a wide variety of items, including vehicles, signs, license plates, and more. When faced with a wide range of illumination conditions, the LBPH recognizer consistently produces accurate face recognition results. Even with just one training image provided for each person, LBPH can still efficiently recognize them. One restriction of our application is that our detector works best with frontal face images. It also has trouble correctly handling 45-degree horizontal and vertical face rotations.

An in-depth three-dimensional examination of the face using a combination of cameras is one potential future endeavor; another is to improve face recognition by zeroing down on particular facial characteristics like the space between the eyes. A more accurate system will be the outcome of combining these two approaches, which will reduce the possibility of inaccuracy.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Alireza Chevelwalla , Ajay Gurav , Sachin Desai , Prof. Sumitra Sadhukhan “Criminal Face Recognition System” International Journal of Engineering Research & Technology (IJERT) Vol. 4 Issue 03, March-2015

[2] Belhumeur, P. N., Hespanha, J. P., & Kriegman, D. J. (1997). Eigenfaces vs. Fisherfaces:Recognition Using Class Specific Linear Projection. IEEE Transactions on Pattern Analysis and Machine Intelligence. 19, pp. 711-720. IEEE Computer Society

[3] Bornet, O. (2005, May 19). Learning Based Computer Vision with Intel's Open Source Computer Vision Library. Retrieved April 2007, 2007, from Intel.com Website: http://www.intel.com/technology/itj/2005/volume09issue02/art03_learning_vision/p04_face_dete ction.htm

[4] Brunelli, R., & Poggio, T. (1993). Face Recognition: Features versus templates. IEEE Transaction on Pattern Analysis and Machine Intelligence , 15 (10), 1042- 1052.

[5] Viola, P. and Jones, M. Rapid object detection using boosted cascade of simple features. IEEE Conference on Computer Vision and Pattern Recognition, 2001.

[6] P. Viola and M. Jones. Robust Real-time Object Detection. International Journal of Computer Vision, 57(2):137–154,2002.https://en.wikipedia.org/wiki/Cascading_classifiers

[7] Open Computer Vision Library Reference Manual. Intel Corporation, USA, 2001.

[8] LBPH Based Improved Face Recognition at Low Resolution Aftab Ahmed, Jiandong Guo, Fayaz Ali, Farha Deeba and Awais Ahmed 2018 International Conference of Artificial Intelligence and Big Data, China

[9] Criminal Identification System Using Face Detection and Recognition Piyush Kakkar and Vibhor Sharma International Journal of Advance Research in Computer and Communication Technology Vol 7 issue 3 march 2018

[10] Criminal Face Recognition System. Alireza Chevelwalla, Ajay Gurav, Sachin Desai and Prof. Sumitra Sadhukhan International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 4 Issue 03, March-2015.