JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

AI based Criminal Detection Using Face Recognition

Nikita Nikam [1], Payal Maind [2], Kaveri Jadhav [3], Sneha Padewar [4], Dr. B. S. Shirole[5]
Department of Computer Engineering
Sanghavi College of Engineering and Research Center,Nashik

Abstract: In our modern era there is an abnormal increase in the crime rate and also the numbers of criminals are increasing, this leads towards a great concern about the security issues. Crime preventions and criminal identification are the primary issues before the police personnel, since property and lives protection are the basic concerns of the police but to combat the crime, the availability of police personnel is limited. This Real time criminal identification system based on face recognition works with a fully automated facial recognition system. Haar feature-based cascade classifier and OpenCV LBPH (Local Binary Pattern Histograms) Algorithms are used for Face detection and recognition. This system will be able to detect face and recognize face automatically in real time. An accurate location of the face is still a challenging task. Viola-Jones framework has been widely used by researchers in order to detect the location of faces and objects in a given image. we represent a methodology for face detection robustly in real time environment. Haar cascading is one of the algorithm for face detection. Face recognition is a biometric based technique that mathematically maps an individual's facial traits and retains the data as a face print. It generates a unique pattern for each face and compares it to other images that are included in the collection. If a match is identified for the input face, the details linked with the relevant image will be displayed.

Keywords: biometrics; emerging technology; policing; artificial intelligence

I. Introduction

Face recognition which is a combination of machine learning and the biometic techniques which holds the qualities of not only high precision but also the reliability. For automatically detecting the human's face from the databases this system can be used. In recent years open computer vision has been widely used in different kinds of applications such as surveillance camera, robotics etc. This technology is used for authentication, validation, authorization, and identification. In developed countries, the government creates a datasets which is helpful for recognize the human face which compares the suspicious act with trained dataset and information stored in database. The automatically tagging feature adds a new dimension to sharing pictures among the people who are in the picture and also gives the idea to other people about who the person is in the image. In our project, we have studied and implemented a pretty simple but very effective face detection algorithm which takes human skin color into account. Our aim, which we believe we have reached, was to develop a system that can be used by police or investigation department to recognize criminal from their faces. The method of face recognition used is fast, robust, reasonably simple and accurate with a relatively simple and easy to understand algorithms and technique. Face recognition based on the geometric features of a face is probably the most instinctive approach for Human identification. The whole process can be divided in three major steps where the first step is to find a good database of faces with multiple images for each individual. The next step is to detect faces in the database images and use them to train the face recognizer and the final step is to test the face recognizer to recognize faces it was trained for.

II. PURPOSE

The rapid advancement of **technology-enabled surveillance** has transformed **criminal detection and investigation**. Modern surveillance methods, including **facial recognition technology, large-scale data analytics, and automatic number plate recognition (ANPR)**, enable law enforcement agencies to track individuals and vehicles in **real-time**. These technologies facilitate the identification of **suspects, criminal networks, and suspicious activities**, significantly improving crime prevention and investigation.

User Authentication:

- Police personnel must log in using secure credentials to access the system.

Image Capture & Input:

- The system should support capturing criminal face images using a webcam or uploading from existing files.
- Police stations can input detection data through a connected camera.

Preprocessing:

- The system will preprocess the captured images to enhance quality, adjust for lighting, and normalize image dimensions.
- It should perform face alignment, scaling, and filtering as part of the preprocessing step.

Feature Extraction:

- The application must extract unique facial features using deep learning algorithms or feature extraction techniques.
- The extracted features will be used for comparison against stored criminal records.

Model Training & Dataset Management:

- The system should allow for training a machine learning model with a dataset of criminal faces.
- The dataset should be periodically updated with new images and labels for accuracy.
- It should support re-training the model as new data is added.

Criminal Identification:

- The system will compare the features of input faces against the trained dataset.
- If a match is found, it should identify the criminal and display their details.
- If no match is found, the system will provide a "Not Found" status

III. OBJECTIVE OF SYSTEM

- To primary objective of the Real-Time Criminal Identification Application using facial recognition is to assist police personnel in swiftly identifying criminals.
- To application aims to provide detailed information about specific criminals that law enforcement may be searching for.
- To Police officers can utilize this application to identify suspects in real-time, from any location, at any time.
- With internet access, any police personnel can access this application, ensuring flexibility and convenience in criminal investigations.

IV. Literature Survey

Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection: We develop a face recognition algorithm which is insensitive to large variation in lighting direction and facial expression. Taking a pattern classification approach, we consider each pixel in an image as a coordinate in a high-dimensional space. We take advantage of the observation that the images of a particular face, under varying illumination but fixed pose, lie in a 3D linear subspace of the high dimensional image space-if the face is a Lambertian surface without shadowing. However, since faces are not truly Lambertian surfaces and do indeed produce self-shadowing, images will deviate from this linear subspace. Rather than explicitly modeling this deviation, we linearly project the image into a subspace in a manner which discounts those regions of the face with large deviation. Our projection method is based on Fisher's linear discriminant and produces well separated classes in a low-dimensional subspace, even under severe variation in lighting and facial expressions.

Face Recognition: Features versus templates: Two new algorithms for computer recognition of human faces, one based on the computation of a set of geometrical features, such as nose width and length, mouth position, and chin shape, and the second based on almost-gray-level template matching, are presented. The results obtained for the testing sets show about 90% correct recognition using geometrical features and perfect recognition using template matching. However, since faces are not truly Lambertian surfaces and do indeed produce self-shadowing, images will deviate from this linear subspace. Rather than explicitly modeling this deviation, we linearly project the image into a subspace in a manner which discounts those regions of the face with large deviation. Our projection method is based on Fisher's linear discriminant and produces well separated classes in a low-dimensional subspace, even under severe variation in lighting and facial expressions. The eigenface technique, another method based on linearly projecting the image space to a low dimensional subspace, has similar computational requirements. Yet, extensive experimental results demonstrate that the proposed "Fisherface" method has error rates that are lower than those of the eigenface technique for tests on the Harvard and Yale face databases.

Rapid object detection using boosted cascade of simple features: This paper describes a machine learning approach for visual object detection which is capable of processing images extremely rapidly and achieving high detection rates. This work is distinguished by three key contributions. The first is the introduction of a new image representation called the "integral image" which allows the features used by our detector to be computed very quickly. The second is a learning algorithm, based on AdaBoost, which selects a small number of critical visual features from a larger set and yields extremely efficient classifiers. The first is the introduction of a new image representation called the “Integral Image” which allows the features used by our detector to be computed very quickly. The second is a learning algorithm, based on AdaBoost, which selects a small number of critical visual features and yields extremely efficient classifiers. The third contribution is a method for combining classifiers in a “cascade” which allows background regions of the image to be quickly discarded while spending more computation on promising object-like regions. A set of experiments in the domain of face detection are presented. The system yields face detection performace comparable to the best previous systems. Implemented on a conventional desktop, face detection proceeds at 15 frames per second.

Fast Adaboost Training Algorithm by Dynamic Weight Trimming: This paper presents a novel fast Adaboost training algorithm by dynamic weight trimming, which increases the training speed greatly when dealing with large datasets. At each iteration, the algorithm discards most of the samples with small weight and keeps only the samples with large weight to train the weak classifier. Then it checks the performance of the weak classifier on all the samples, if the weighted error is above 0.5, it will increase the number of training samples and retrain the weak classifier. During training, only a small portion of the samples are used to train the weak classifier, so the speed is increased greatly. Fig.2: Face recognition system. 2.6 Feature-Based Face Recognition Using Mixture Distance: We consider the problem of feature-based face recognition in the setting where only a single example of each face is available for training. The mixture-distance technique we introduce achieves a recognition rate of 95% on a database of 685 people in which each face is represented by 30 measured distances. This is currently the best recorded recognition rate for a feature-based system applied to a database of this size. A mixture perspective is also taken for individual Gaussians to choose between first order (variance) and second order (covariance) models. Here an approximation to flat combination is proposed and seen to perform well in practice. Our results demonstrate that even in the absence of multiple training examples for each class, it is sometimes possible to infer from a statistical model This paper describes a visual object detection framework that is capable of processing images extremely rapidly while achieving high detection rates. There are three key contributions. The first is the introduction of a new image representation called the “Integral Image” which allows the features used by our detector to be computed very quickly.

VI. SYSTEM ARCHITECTURE

Finding criminal and decrease crime in real time very difficult task,so we are developing innovative system to helping police to detect criminal using face recognition.

SYSTEM ARCHITECTURE

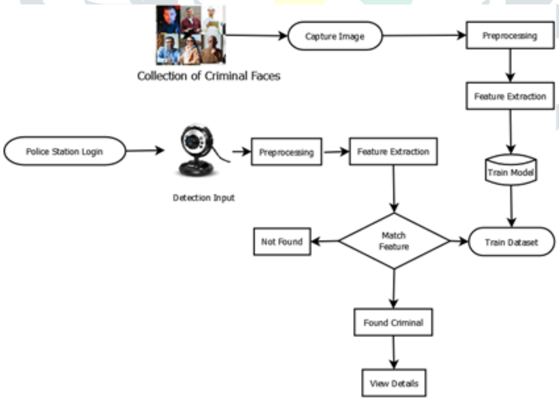


Figure 1. System Architecture

1. This project is aimed at developing an application called Real-Time criminal identification system based on face recognition. We are able to detect and recognize faces of the criminals in an image and in a video stream obtained from a camera in real time. We have used Haar feature based cascade classifiers in OpenCV approach for face detection. It is a machine learning based approach where a cascade function is trained from a lot of positive and negative images. It is then used to detect objects in other images. Also, we have used Local Binary Patterns Histograms (LBPH) for face recognition.
2.

   1. Collection of Criminal Faces

   A database of known criminals' faces is created by collecting images of individuals with criminal records.

   These images are stored in a dataset for future comparisons. In a criminal face detection system, capturing an image refers to the process of acquiring and processing a visual representation of a person's face, typically for the purpose of identification, verification, or investigation.

2. Capturing Image

When an unknown person needs to be identified, an image is captured. The captured image is usually a digital photograph or video frame that contains the face of the individual. This image is then analyzed using facial recognition algorithms, which extract unique features from the face, such as:

1. Facial landmarks (e.g., eyes, nose, mouth)
2. Geometric measurements (e.g., distance between eyes)
3. Texture and pattern analysis (e.g., wrinkles, scars)

3. Pre-processing

Captured images go through a preprocessing stage to enhance quality and remove noise. In a criminal face detection system, pre-processing refers to the steps taken to prepare and enhance the captured image of a face, making it suitable for feature extraction and analysis. The goal of pre-processing is to improve the quality and accuracy of the face detection and recognition process.

Common pre-processing steps in a criminal face detection system include:

1. **Image resizing**: Scaling the image to a standard size to reduce computational complexity.
2. **Image normalization:** Adjusting the brightness, contrast, and color balance to ensure consistency across images.
3. **Face alignment:** Rotating and aligning the face to a standard position, ensuring that facial features are properly oriented.
4. **Face cropping:** Removing unnecessary background and focusing on the face region.
5. **Noise reduction**: Removing random variations in the image, such as salt-and-pepper noise.
6. **Image enhancement**: Sharpening or smoothing the image to improve feature visibility.
7.**Illumination normalization:** Compensating for varying lighting conditions to reduce shadows and highlights.
8. **Pose normalization:** Adjusting the face to a standard pose, reducing the impact of pose variations.
9. **Facial landmark detection**: Identifying key facial features, such as eyes, nose, and mouth, to aid in face alignment and feature extraction.
10. **Data augmentation:** Artificially generating additional images through techniques like rotation, flipping, and scaling to increase the diversity of the training dataset.

By applying these pre-processing steps, the face detection system can:

1. Improve face detection accuracy
2. Enhance feature extraction and analysis
3. Increase robustness to variations in lighting, pose, and expression
4. Reduce the impact of noise and other image artifacts

Pre-processing is a critical component of a criminal face detection system, as it lays the foundation for accurate and reliable face recognition and analysis.

3. Feature Extraction

key facial features are extracted using advanced techniques. In a criminal face detection system,feature extraction is the process of identifying and isolating distinctive characteristics or features from a face image. These features are used to create a unique representation of the face, which can be compared to other face images to identify matches.

Feature extraction is a critical step in face recognition, as it enables the system to:

1. Discriminate between faces: Identify unique characteristics that distinguish one face from another.
2. Robustly recognize faces: Accurately recognize faces despite variations in lighting, pose, expression, and other factors.

Common feature extraction techniques used in criminal face detection systems include:

1. Geometric features: Measuring distances and angles between facial landmarks, such as the eyes, nose, and mouth.
2. Appearance-based features: Analyzing the texture, pattern, and shape of facial features, such as wrinkles, scars, and facial hair.
3. Local Binary Patterns (LBP): Extracting features from local patterns in the face image, such as edges and corners.
4.. Deep learning-based features: Using convolutional neural networks (CNNs) to extract features from face images, which can learn to recognize patterns and relationships.

The extracted features are typically represented as a:

1. Feature vector: A numerical representation of the face features, which can be compared to other feature vectors.
2. Face template: A compact representation of the face features, which can be stored in a database for comparison.

By extracting distinctive features from face images, a criminal face detection system can accurately identify and verify individuals, aiding in investigations and crime solving.

5. Train Model

A **machine learning or deep learning model** is trained using the **dataset of criminal faces**. In a criminal face detection system, a train dataset is a collection of face images used to train a machine learning algorithm to recognize and identify faces. The train dataset plays a crucial role in the development of an accurate and reliable face recognition system.

Training involves:

- Learning unique **facial patterns**
- Creating a **recognition model**
- Saving trained patterns for future matching
- Social media datasets: Collections of face images extracted from social media platforms.

6. Train Dataset

The criminal face dataset is continuously updated with new images to improve detection accuracy. In a criminal face detection system, a police station login refers to a secure authentication process that allows authorized personnel from a police station to access the system. The login process ensures that only authorized users can:

1. Upload images: Add face images of suspects, criminals, or missing persons to the system.
2. Search databases: Query the system's databases to identify potential matches.
3. View results: Access search results, including images, profiles, and other relevant information.
4. Manage data: Update, edit, or delete face images and associated data.

The police station login typically involves:

1. Username and password: Authorized personnel enter their unique username and password to access the system.
2. Role-based access control: Users are assigned specific roles, such as administrator, investigator, or analyst, which determine their level of access and permissions.
3. Two-factor authentication: An additional layer of security, such as a fingerprint scan, facial recognition, or one-time password, may be required to ensure the user's identity.
4. Secure connection: The login process is typically encrypted to prevent unauthorized access or data interception.

Once logged in, authorized personnel can utilize the criminal face detection system to:

1. Investigate crimes: Identify suspects, track movements, and gather evidence.
2. Identify missing persons: Locate missing individuals by matching face images.
3. Enhance public safety: Monitor and respond to potential security threats.

By implementing a secure police station login, the criminal face detection system ensures that sensitive information is protected and only accessible to authorized personnel.

7. Police Station Login (Detection Input)

A police officer logs into the system to scan a suspect's face using a webcam or CCTV footage.
The captured image is sent for preprocessing and feature extraction just like in step 3 and 4.

In a criminal face detection system, the collection of criminal faces refers to a database or repository of face images of known criminals, suspects, or individuals of interest. This collection is used to:

1. Identify matches: Compare face images from surveillance footage, mugshots, or other sources to identify potential matches.
2. Track movements: Monitor the movements and activities of known criminals or suspects.
3. Investigate crimes: Use face recognition to identify suspects, gather evidence, and solve crimes.

VII. Advantages

High Accuracy and Speed

- AI-powered facial recognition can quickly identify criminals from large databases, significantly reducing the time required for manual verification**.**

Real-Time Identification

- Security agencies and law enforcement can detect and track suspects in real-time using surveillance cameras and AI-based systems**.**

Automated Crime Prevention

- AI can analyze video footage and alert authorities when a known criminal is detected in restricted or high-security areas, preventing potential crimes.

Enhanced Public Safety

- The system can be deployed in public places like airports, train stations, and malls to identify and apprehend criminals before they commit unlawful acts.

Integration with Existing Security Systems

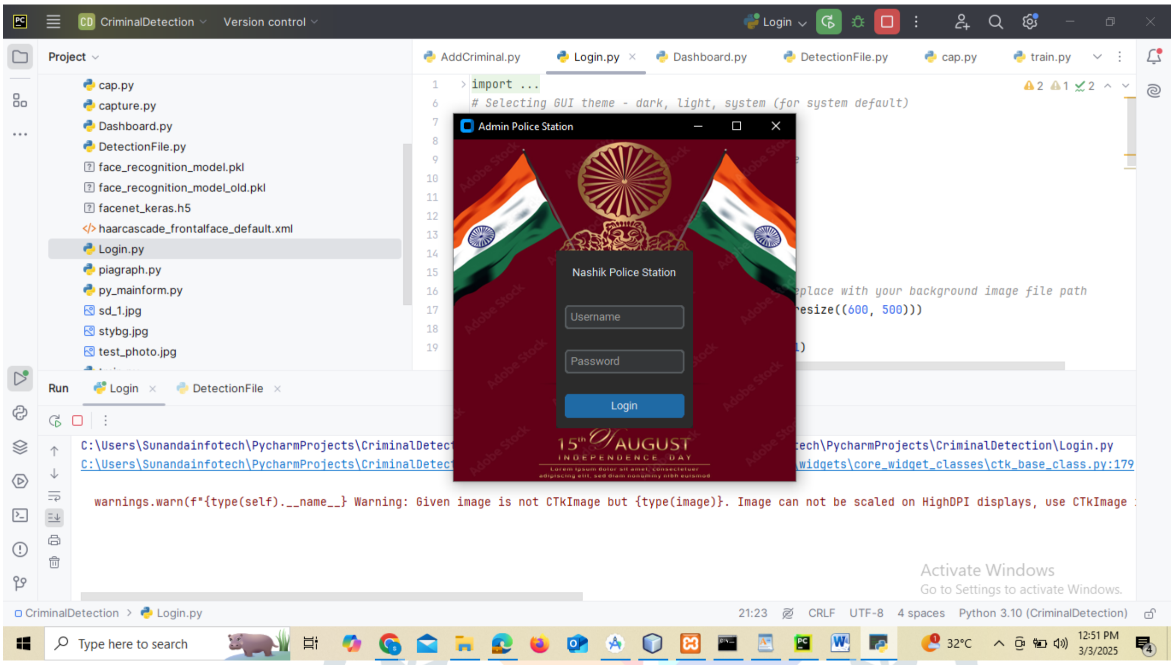
- AI-based facial recognition can be integrated with CCTV cameras and law enforcement databases to improve security monitoring and crime detection.

Reduction in Human Error

- AI eliminates the risks of human biases and mistakes, ensuring accurate and consistent criminal identification.

VIII. Implementation & Result

Login:
A user authentication page where credentials are entered to access the system.



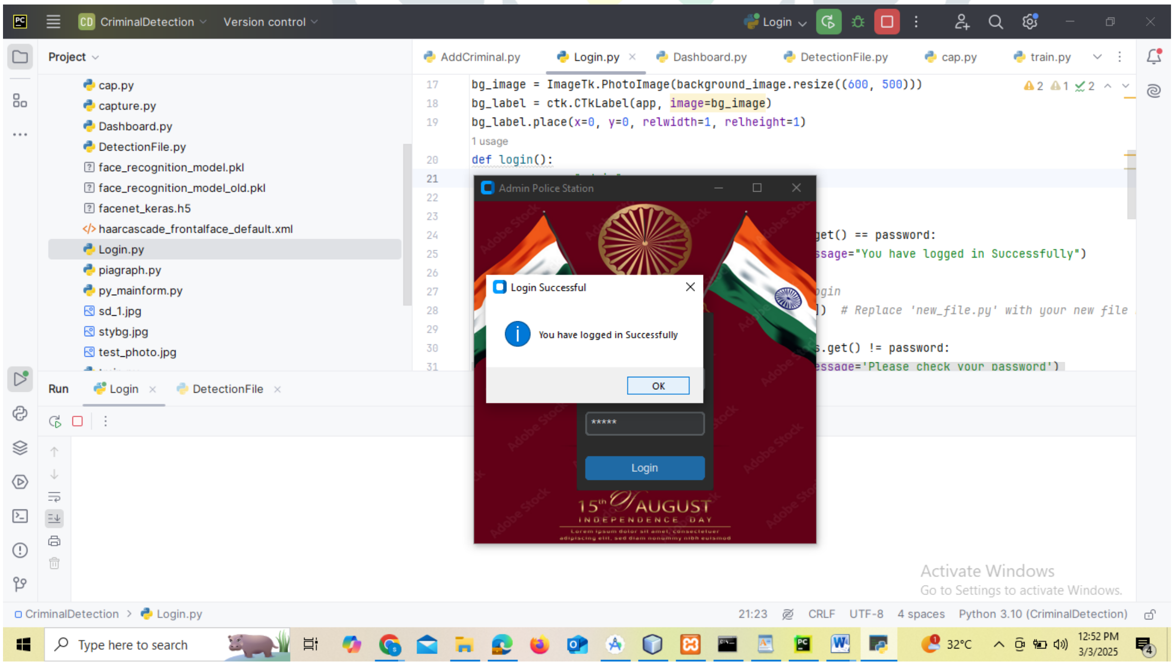
```
import ...
# Selecting GUI theme - dark, light, system (for system default)
eplace with your background image file path
esize((600, 500)))
1)
```

```
C:\Users\Sunandainfotech\PycharmProjects\CriminalDetect                tech\PycharmProjects\CriminalDetection\Login.py
C:\Users\Sunandainfotech\PycharmProjects\CriminalDetect                widgets\core_widget_classes\ctk_base_class.py:179

  warnings.warn(f"{type(self).__name__} Warning: Given image is not CTkImage but {type(image)}. Image can not be scaled on HighDPI displays, use CTkImage
```

Figure 2. Login

Login Successfully:
Confirmation screen showing successful login and redirection to the dashboard.



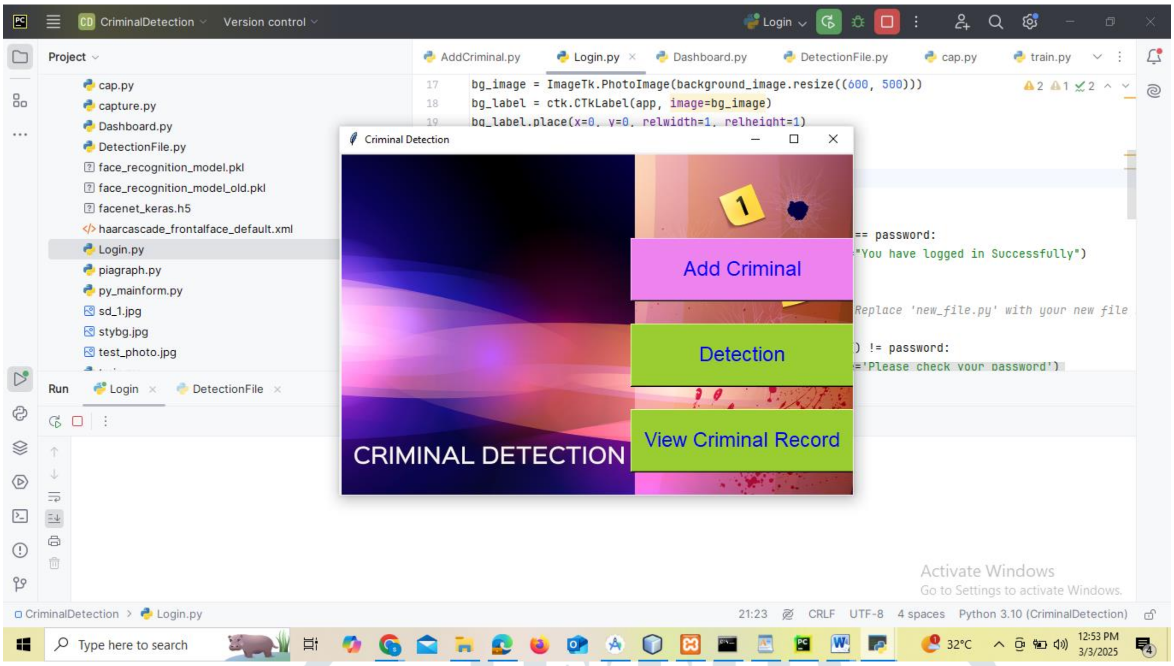
```
bg_image = ImageTk.PhotoImage(background_image.resize((600, 500)))
bg_label = ctk.CTkLabel(app, image=bg_image)
bg_label.place(x=0, y=0, relwidth=1, relheight=1)
1 usage
def login():
get() == password:
ssage="You have logged in Successfully")
ogin
) # Replace 'new_file.py' with your new file
s.get() != password:
essage='Please check your password')
```

Login Successful

You have logged in Successfully

Figure 3. Login Successfully

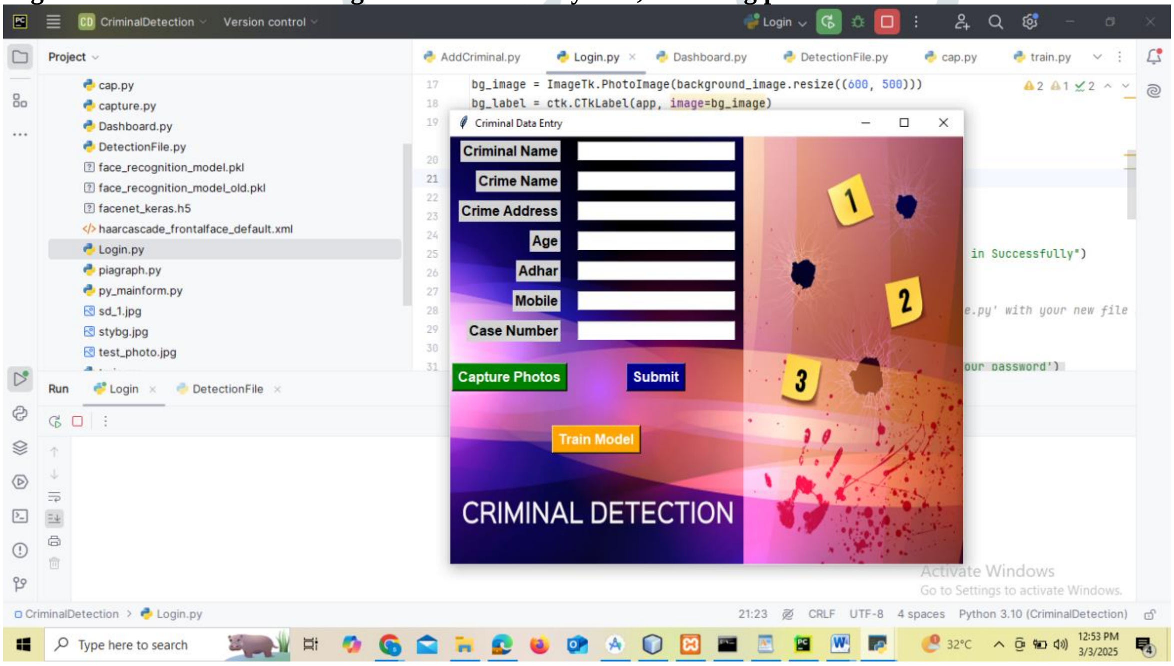
Home/Dashboard: The main interface displaying key system features and navigation options



```
bg_image = ImageTk.PhotoImage(background_image.resize((600, 500)))
bg_label = ctk.CTkLabel(app, image=bg_image)
bg_label.place(x=0, y=0, relwidth=1, relheight=1)
== password:
"You have logged in Successfully")
Replace 'new_file.py' with your new file
) != password:
='Please check your password')
```

Figure 4. Dashboard

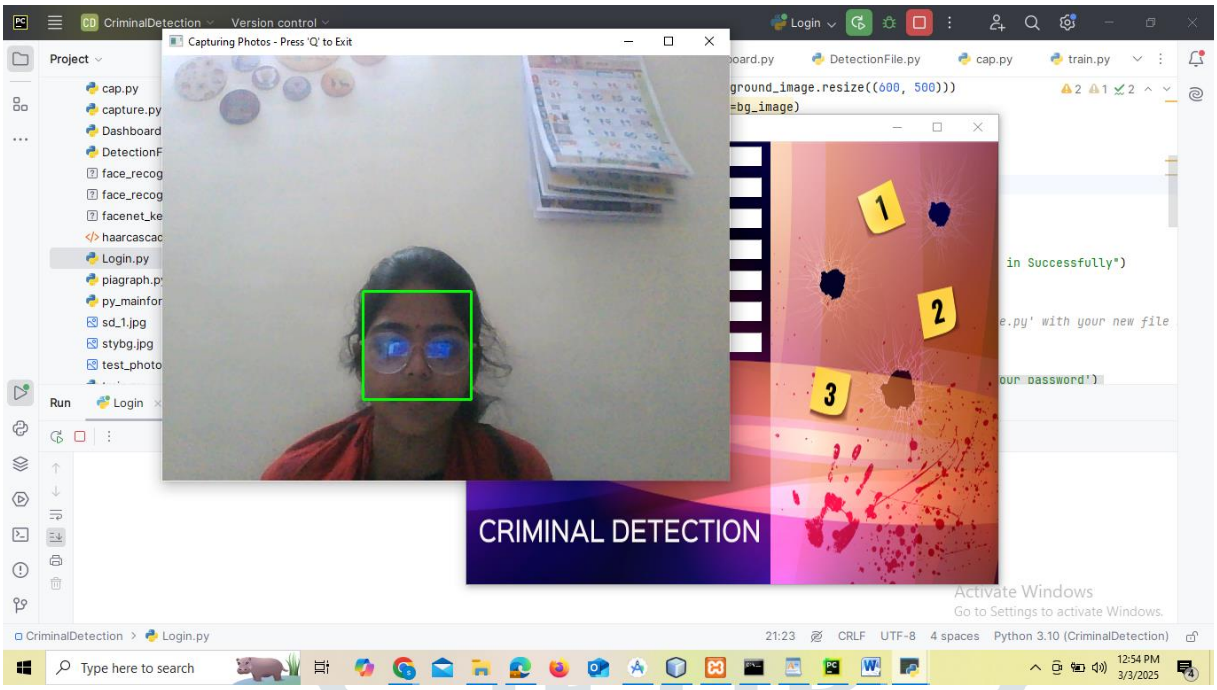
Criminal Registration: A form for adding new users to the system, including personal details and credentials.



```
bg_image = ImageTk.PhotoImage(background_image.resize((600, 500)))
bg_label = ctk.CTkLabel(app, image=bg_image)
in Successfully")
e.py' with your new file
our password')
```

Figure 5. Add Criminal

Add Criminal Face: Here we are train face

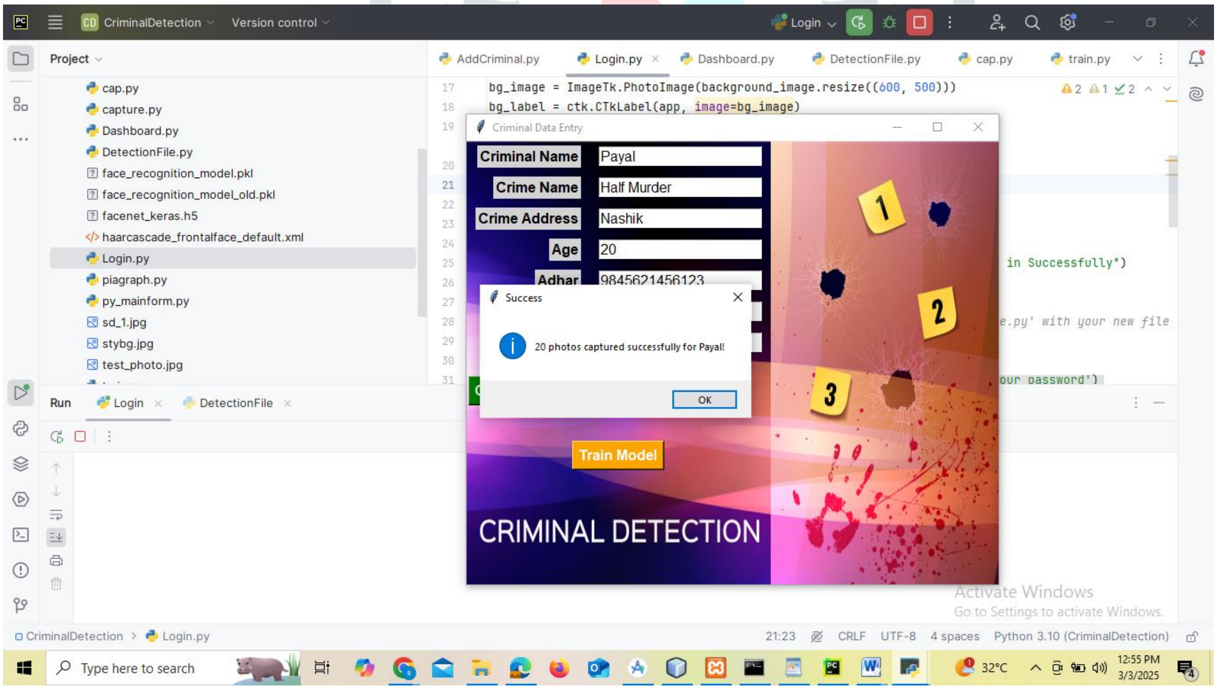


Capturing Photos - Press 'Q' to Exit

```
ground_image.resize((600, 500)))
=bg_image)
```

Figure 6. Train Criminal

Update Criminal Details/Faces: A form allowing modifications to an existing criminal record.



```
bg_image = ImageTk.PhotoImage(background_image.resize((600, 500)))
bg_label = ctk.CTkLabel(app, image=bg_image)
```

Criminal Data Entry

Criminal Name: Payal

Crime Name: Half Murder

Crime Address: Nashik

Age: 20

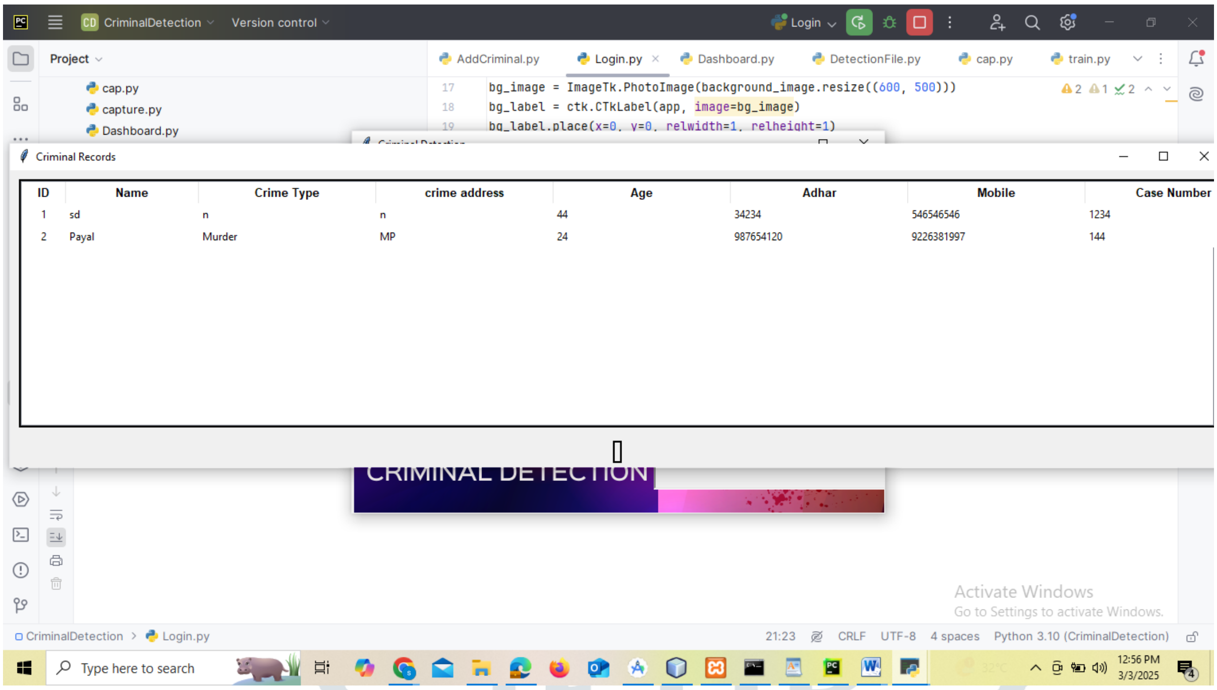
Adhar: 9845621456123

Success

20 photos captured successfully for Payal!

Figure 7. Update Criminal

View Criminal Records: A list of registered criminals with search and filtering options

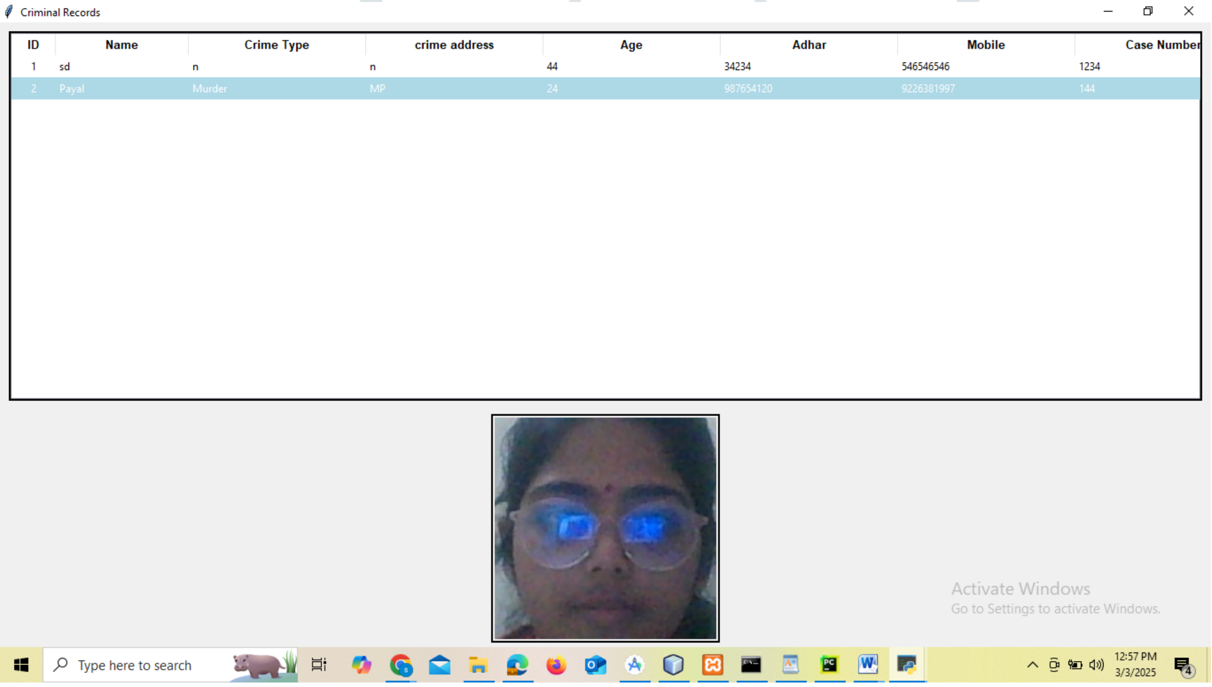


```
bg_image = ImageTk.PhotoImage(background_image.resize((600, 500)))
bg_label = ctk.CTkLabel(app, image=bg_image)
bg_label.place(x=0, y=0, relwidth=1, relheight=1)
```

Criminal Records

ID	Name	Crime Type	crime address	Age	Adhar	Mobile	Case Number
1	sd	n	n	44	34234	546546546	1234
2	Payal	Murder	MP	24	987654120	9226381997	144

Figure 8. View Criminal Record

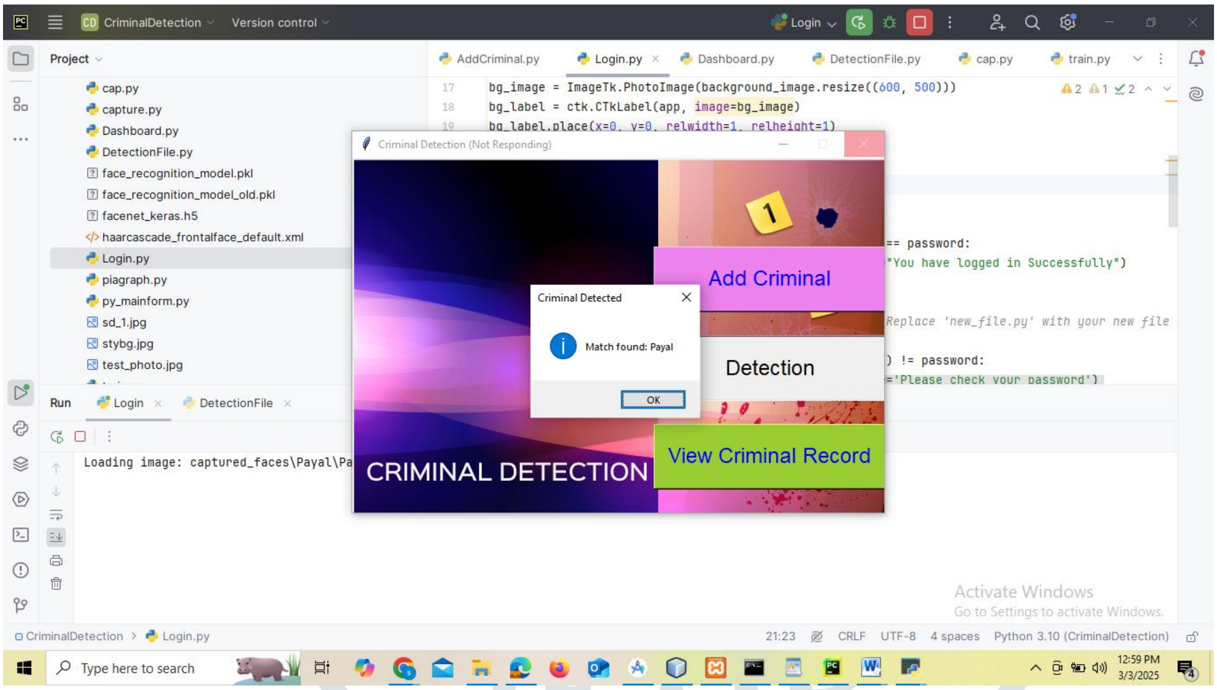


Criminal Records

ID	Name	Crime Type	crime address	Age	Adhar	Mobile	Case Number
1	sd	n	n	44	34234	546546546	1234
2	Payal	Murder	MP	24	987654120	9226381997	144

Figure 9. View Criminal Record

Detection of Criminal: After match face criminal details will be show



```
bg_image = ImageTk.PhotoImage(background_image.resize((600, 500)))
bg_label = ctk.CTkLabel(app, image=bg_image)
bg_label.place(x=0, y=0, relwidth=1, relheight=1)
```

```
== password:
"You have logged in Successfully")
Replace 'new_file.py' with your new file
) != password:
='Please check your password')
```

Criminal Detected

Match found: Payal

OK

```
Loading image: captured_faces\Payal\Pa
```

Figure 10. Detection Criminal Record

IX. CONCLUSION

There has been considerable scholarly treatment of the human rights impacts of FRT deployment by police and security services. The parameters and details of principled regulation have had comparatively less analysis, but with recent rapid developments in global regulation, it is possible to observe distinct categories of regulatory approaches to FRT. This contribution has considered three diverse case studies of regulation of FRT in the policing and security contexts—self-regulation through policy and practice guidelines, wide-ranging cross-national regulation, and national attempts to provide specific legislation. Each shows different challenges and opportunities in regulating the spectrum of use of FRT in policing and security. The overarching theme in each of these is a struggle to properly define the interests at play. Technology supplier and police-led developments are a feature of early adoption examples. While innovation in technology use in policing and security is absolutely necessary, these instances are unlikely to properly take public and community views into account or have the necessary transparency and legitimacy requirements. There are many examples of good practice in terms of robust guidelines or oversight by independent observers and reviewers, but there is the ever-present risk of internal policy settings changing due to changes in leadership or attitudes.

X. ACKNOWLEDGMENT

We express our heartfelt gratitude to our esteemed mentors and professors, especially **Dr. B. S. Shirole**, for their invaluable guidance in our academic and project endeavours. We also extend our thanks to the Computer Engineering Department and its staff for their continuous support. Our sincere thanks go to Principal of **SANGHAVI COLLEGE OF ENGINEERING**, for his support and permission to complete this project. We appreciate the assistance of our department's support staff, and we're grateful to our parents, friends, and all those who supported us
throughout this project.

REFERENCES

[1] Akbari, Ali. 2024. Facial Recognition Technologies 101: Technical Insights. In The Cambridge Handbook of Facial Recognition in the Modern State. Edited by Rita Matulionyte and Monika Zalnieriute. Cambridge Law Handbooks. Cambridge: Cambridge University Press, pp. 29–43.

[2] Bradford, Ben, Julia A. Yesberg, Jonathan Jackson, and Paul Dawson. 2020. Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology. The British Journal of Criminology 60: 1502–22. [CrossRef]

[3] Bragias, Adelaide, Kelly Hine, and Robert Fleet. 2021. 'Only in our best interest, right?' Public perceptions of police use of facial recognition technology. Police Practice and Research 22: 1637–54. [CrossRef]

[4] Bright, Jo-Anne, Hannah Kelly, Zane Kerr, Catherine McGovern, Duncan Taylor, and John S. Buckleton. 2020. The interpretation of forensic DNA profiles: An historical perspective. Journal of the Royal Society of New Zealand 50: 211–25. [CrossRef]

[5] Canal, Felipe Zago, Tobias Rossi Müller, Jhennifer Cristine Matias, Gustavo Gino Scotton, Antonio Reis de Sa Junior, Eliane Pozzebon, and Antonio Carlos Sobieranski. 2022. A survey on facial emotion recognition techniques: A state-of-the-art literature review. Information Sciences 582: 593–617. [CrossRef]

[4] V. B. Kumar, S. S. Kumar, and V. Saboo, ”Dermatological disease detection using image processing and machine learning,” 2016 Third International Conference on Artificial Intelligence and Pattern Recognition (AIPR) Lodz, 2016 , pp.1-6.

[5] Department of Justice. 2023. Minister McEntee Receives Cabinet Approval for Draft Facial Recognition Technology Bill. Available online: https://www.gov.ie/en/press-release/797e2-minister-mcentee-receives-cabinet-approval-for-draft-facial-recognitiontechnology-bill/ (accessed on 1 June 2024).

[6] Fenwick, Helen. 1999. The right to protest, the Human Rights Act and the margin of appreciation. Modern Law Review 62: 491. [CrossRef] Fontes, Catarina, and Christian Perrone. 2021.

[7] Ethics of Surveillance: Harnessing the Use of Live Facial Recognition Technologies in Public Spaces for Law Enforcement. Technical University of Munich Research Brief. Available online: https://ieai.sot.tum.de/wpcontent/uploads/2021/12/ResearchBrief_December_Fontes-1.pdf (accessed on 1 June 2024).

[8] Fussey, Pete, Bethan Davies, and Martin Innes. 2021. ‘Assisted’ facial recognition and the reinvention of suspicion and discretion in digital policing. The British Journal of Criminology 61: 325–44. [CrossRef]

[9] Fussey, Peter, and Daragh Murray. 2019. Independent report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology. Available online: https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-TechReport-2.pdf (accessed on 1 June 2024).