Criminal Identification Using Machine Learning And Face Recognition Techniques

[1]**Peram Siva Krishna Reddy**, sivakrishnareddy082@gmail.com
[2]**M Naresh**, nareshmtech08@gmail.com
[1&2]Newton's Institute of Engineering, Guntur, Andhra Pradesh

Abstract

The system utilizes CCTV cameras to capture images in public places, allowing for the identification of criminals present in these areas for easier apprehension. It extracts features from the captured images by encoding the faces. The captured image encoding is then compared with encoding values stored in a database. If there is a match between the captured and database image encodings, the criminal's image, name, and a message indicating that the criminal has been identified will be displayed on the screen. Additionally, the image of the identified person will be saved in a designated folder on the desktop, enabling law enforcement to easily distinguish the criminal from other individuals in the public.

Keywords: *Face Recognition, Machine Learning, Criminal Identification*

1. INTRODUCTION

In today's world, public safety and crime prevention are top priorities for law enforcement agencies. Rapid urbanization and increasing population densities have made manual surveillance challenging and less efficient. The use of advanced technologies such as Closed-Circuit Television (CCTV) systems and computer vision techniques has revolutionized the way criminal identification and monitoring are conducted. This study explores a comprehensive system that leverages CCTV cameras to capture real-time images in public spaces. The proposed solution focuses on extracting essential features from captured images by encoding facial data and comparing them with an existing database of criminal profiles. When a match is found, the system displays crucial details such as the criminal's name and photograph, along with an alert message. Additionally, the identified individual's image is automatically stored in a dedicated folder for future reference by law enforcement officials. The implementation of such a system significantly enhances the efficiency of criminal detection and apprehension, providing a proactive tool for public
security. By utilizing cutting-edge image processing techniques and automated facial recognition, authorities can quickly and accurately identify suspects, thereby promoting a safer public environment.

2. LITERATURE SURVEY

The growing demand for automated criminal identification and public safety has led to significant advancements in image processing, computer vision, and facial recognition systems. Several studies have explored innovative methods and frameworks for detecting and identifying individuals from surveillance footage in public places. This literature survey reviews key research contributions that have laid the foundation for developing efficient criminal identification systems. Belhumeur et al. [1] explored two prominent face recognition approaches—Eigenfaces and Fisherfaces. They demonstrated the effectiveness of Fisherfaces in handling variations such as lighting and facial expressions due to its class-specific linear projection method. This work serves as a foundational study for developing robust face recognition systems. Bornet [2] emphasized the practical implementation of face detection using Intel's Open Source Computer Vision Library (OpenCV). The research highlighted the efficiency of learning-based techniques in real-world applications, contributing to the evolution of real-time surveillance systems. Brunelli and Poggio [3] compared feature-based and template-based face recognition approaches. Their findings demonstrated that feature-based methods, which involve extracting distinct facial landmarks, often perform better in varying environmental conditions. This insight has significantly influenced the development of adaptable recognition algorithms. Viola and Jones [4] introduced a revolutionary framework for real-time object detection using a boosted cascade of simple features. Their work drastically reduced the computational requirements for face detection while maintaining high accuracy, making it a widely adopted standard in security systems. In their follow-up research, Viola and Jones [5] emphasized the importance of robustness and efficiency in real-time detection applications. Their algorithm provided a scalable solution for integrating reliable face detection into surveillance systems. Schroff et al. [6] proposed the FaceNet model, which uses deep convolutional neural networks (CNNs) to directly learn embeddings for face verification and clustering. This approach offered state-of-the-art accuracy and formed the basis for modern facial recognition systems. Kazemi and Sullivan [7] presented an efficient method for real-time face alignment using ensemble regression trees. Their approach significantly improved the accuracy of facial feature extraction, contributing to better recognition and detection outcomes. Howard et al. [8] developed MobileNets, lightweight deep learning models optimized for mobile and embedded vision applications. Their architecture is particularly useful in surveillance scenarios where computational efficiency is critical. Redmon et al. [9] proposed the You Only Look Once (YOLO) object detection framework, which achieved real-time detection with high accuracy. YOLO's ability to simultaneously detect multiple objects made it a preferred choice for public surveillance systems. Zhao et al. [10] investigated multi-modal approaches for face recognition in complex environments. Their research highlighted the benefits of combining facial, contextual, and behavioral features for enhanced criminal identification accuracy.

3. MATERIALS AND METHODS

Fig.1. depicts a comprehensive system for real-time criminal identification using CCTV cameras and facial recognition technology. This process starts with video footage captured by security cameras installed in public spaces, which continuously monitor individuals in the area. The video feed is then decomposed into individual frames, allowing the system to analyze each frame independently for the presence of human faces. This step ensures that dynamic video footage is converted into actionable static images for subsequent processing. Once frames are extracted, the system performs pre-processing to enhance image quality and eliminate noise. This critical step includes operations such as resizing, normalization, and color adjustment to standardize the input images and improve the accuracy of the subsequent feature extraction process. The pre-processed frames are then passed to a feature extraction module, which identifies and encodes essential facial characteristics. These encoded features, often represented as multi-dimensional numerical vectors, capture unique facial traits such as the shape of eyes, nose, and mouth, forming a distinctive "face signature" for each individual. The system maintains a database of known criminals, where each entry includes a facial encoding and corresponding identifying details. The extracted features from the captured images are compared against this criminal database using advanced face-matching algorithms. If a match is found, the system triggers an alert by displaying the criminal's name, image, and a notification that a suspect has been identified.

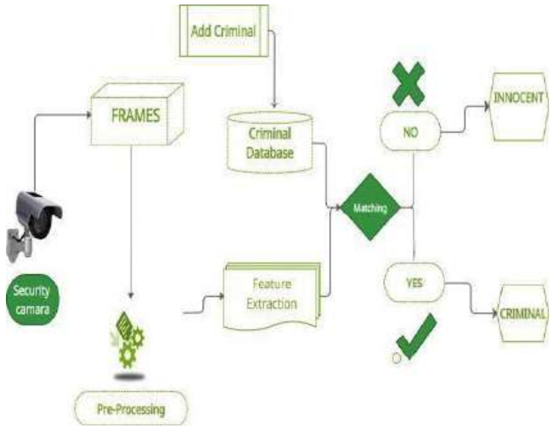


Fig.1. Proposed Model Architecture

Additionally, the image of the identified individual is automatically saved into a dedicated folder on the system's desktop, ensuring that law enforcement personnel can easily access and verify the captured evidence. In cases where no match is found, the system identifies the individual as "Innocent" and does not raise any alerts. This decision-making process is critical for distinguishing potential criminals from the general public, thereby minimizing false positives and enhancing system reliability. The real-time integration of surveillance, pre-processing, feature extraction, and database matching ensures a streamlined and efficient workflow for identifying and apprehending criminals in public spaces. This system exemplifies the practical application of computer vision and machine learning techniques to enhance public safety and assist law enforcement agencies in proactive crime management.

4. RESULTS AND DISCUSSION

Fig.2. showcases a graphical user interface (GUI) developed for criminal identification using machine learning (ML) and face recognition techniques. The interface includes multiple components designed to streamline the process of identifying criminals from a dataset of facial images. First, the user selects a folder containing the necessary files for the criminal detection system. The folder options include "Dataset," which stores images of known criminals, "Model," which contains the pre-trained models for recognition, and "Test Images," which are used to evaluate the system's performance. Once the folder is selected, the system allows the user to upload the criminal dataset into the platform for processing. The next step is preprocessing the dataset, which involves preparing the images for further analysis by standardizing their format, removing noise, and performing necessary adjustments. After preprocessing, the user can initiate the training process by clicking the "Train SVM using MTCNN & FaceNet Features" button. This step involves using Multi-task Cascaded Convolutional Networks (MTCNN) for accurate face detection and FaceNet for feature extraction, both of which are essential for building a robust facial recognition model. Following training, the user can view a "Comparison Graph" to evaluate the performance of the model, comparing various metrics such as accuracy, precision, and recall. The most crucial functionality of the system is the "Criminal Identification" button, which allows the user to test the system by comparing a test image against the database of known criminals. If a match is found, the system identifies the individual as a criminal. Lastly, the "Exit" button provides a way for the user to close the application. Overall, this GUI-based system offers a seamless and structured approach to criminal identification, integrating advanced face recognition algorithms and machine learning techniques to enhance the efficiency and accuracy of public safety operations. Fig.3. shows the loading of dataset, and Fig. 4. Shows the train test split of input dataset. Fig.5. shows the performance metrics. Fig.6. and Fig.7. shows the face recognition results in test images.

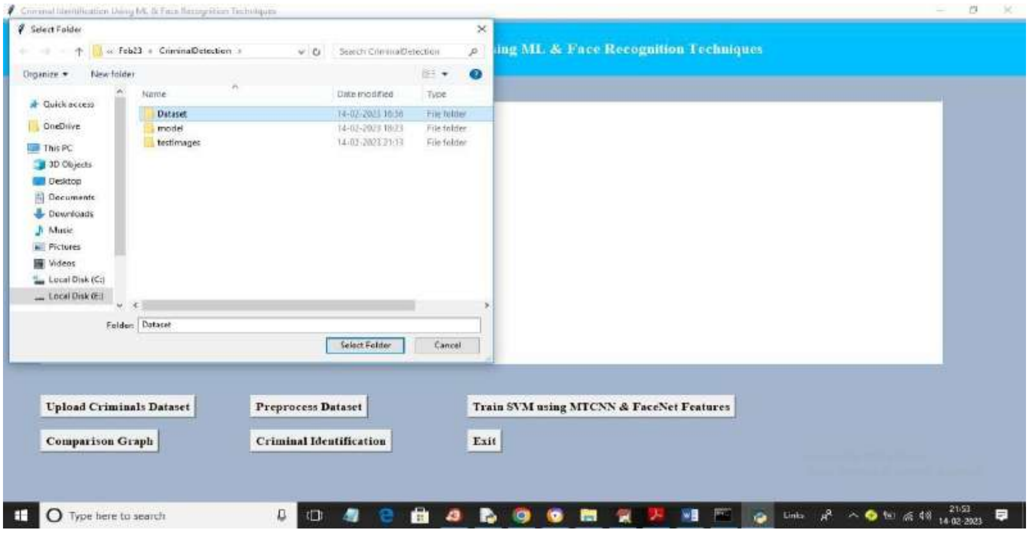
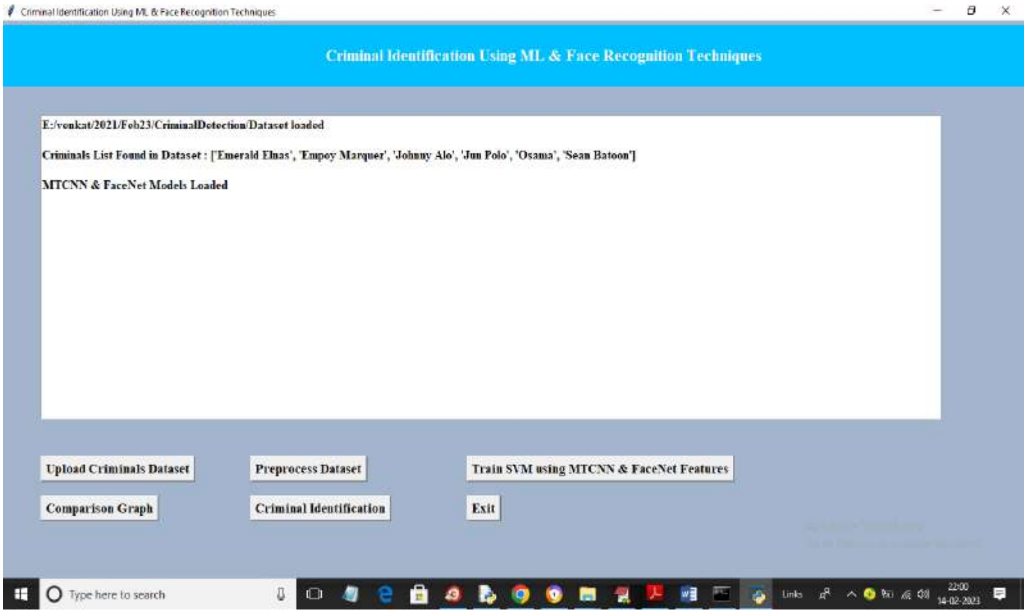
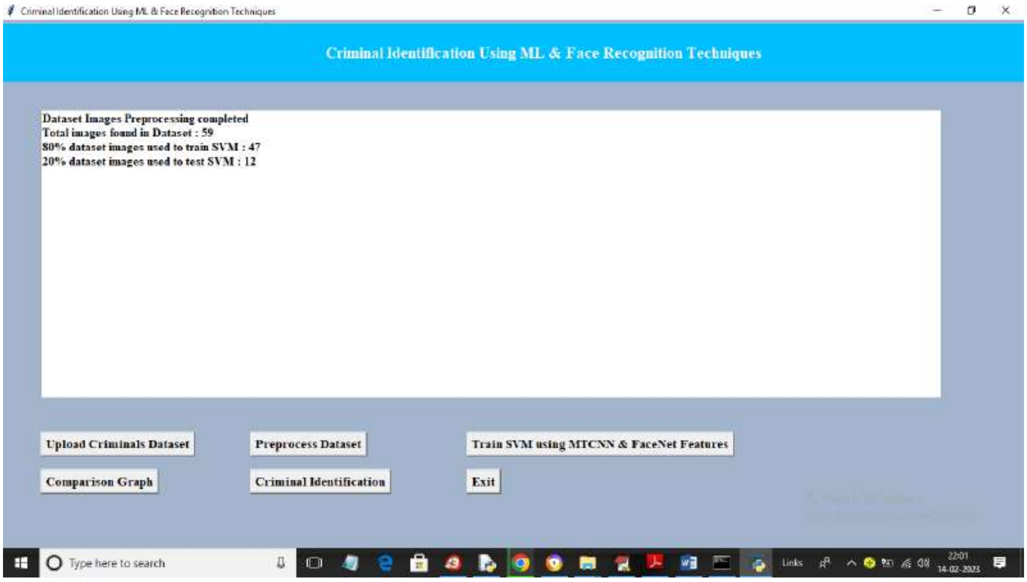


Fig.2. Graphical user interface (GUI) developed for criminal identification


Criminal Identification Using ML & Face Recognition Techniques
Criminal Identification Using ML & Face Recognition Techniques
Upload Criminals Dataset
Preprocess Dataset
Train SVM using MTCNN & FaceNet Features
Comparison Graph
Criminal Identification
Exit
Type here to search
22:00
14-02-2023

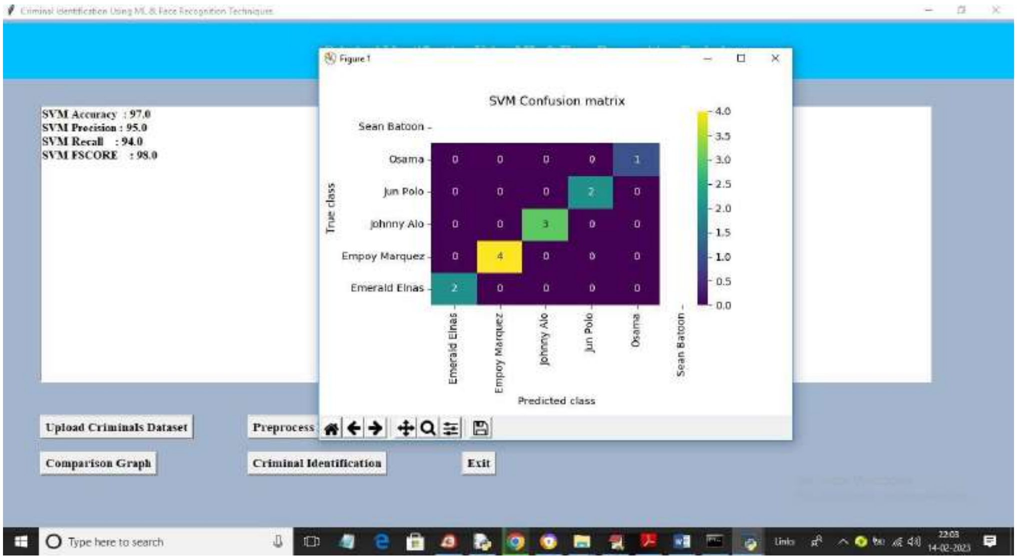
```
E:/venkat/2021/Feb23/CriminalDetection/Dataset loaded

Criminals List Found in Dataset : ['Emerald Elnas', 'Empoy Marquer', 'Johnny Alo', 'Jun Polo', 'Osama', 'Sean Batoon']

MTCNN & FaceNet Models Loaded
```

Fig.3. Loading of Dataset


Criminal Identification Using ML & Face Recognition Techniques
Criminal Identification Using ML & Face Recognition Techniques
Upload Criminals Dataset
Preprocess Dataset
Train SVM using MTCNN & FaceNet Features
Comparison Graph
Criminal Identification
Exit
Type here to search

```
Dataset Images Preprocessing completed
Total images found in Dataset : 59
80% dataset images used to train SVM : 47
20% dataset images used to test SVM : 12
```

Fig.4. Train Test Split of Dataset



```
SVM Accuracy  : 97.0
SVM Precision : 95.0
SVM Recall    : 94.0
SVM FSCORE    : 98.0
```

Fig.5. Performance Metrics

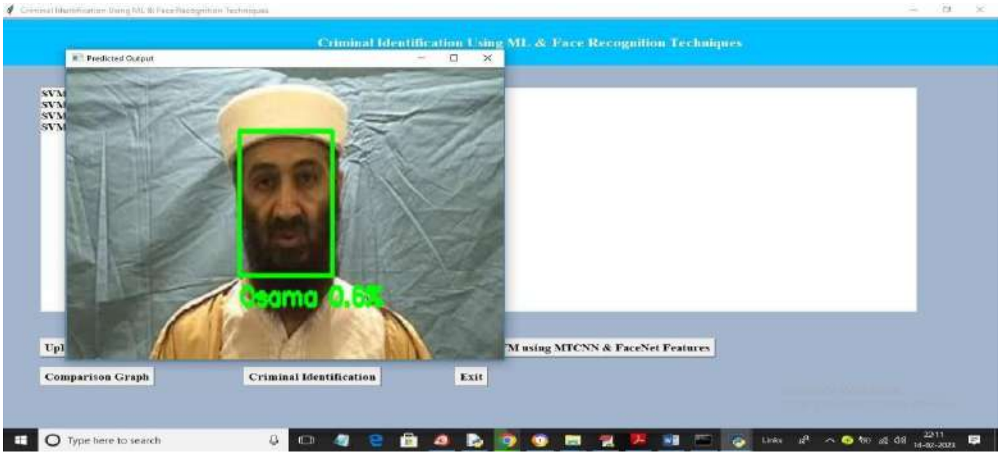
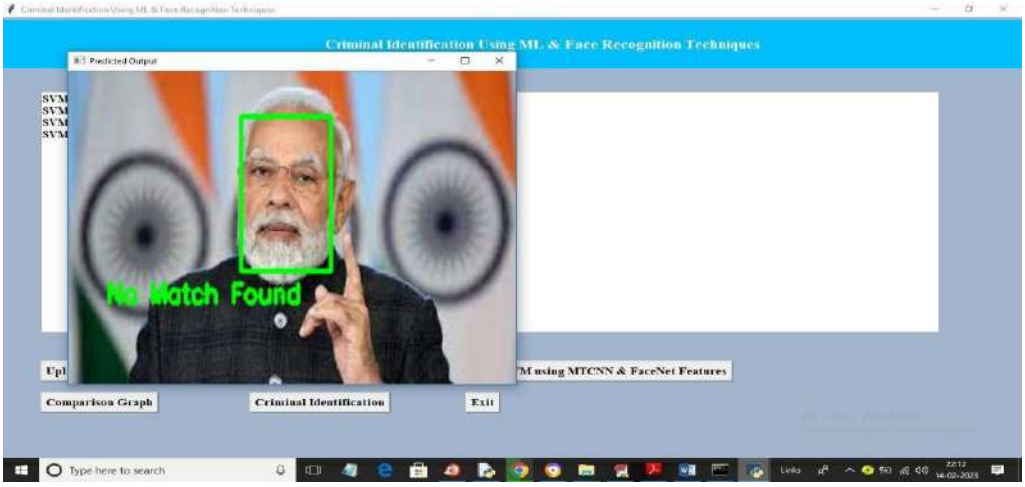

Criminal Identification Using ML & Face Recognition Techniques
Predicted Output
Osama 0.6%
Upl
M using MTCNN & FaceNet Features
Comparison Graph
Criminal Identification
Exit
Type here to search

Fig.6. Face recognized in test image 1 with confidence score



Criminal Identification Using ML & Face Recognition Techniques

Predicted Output

SVM
SVM
SVM
SVM

No Match Found

Fig.7. Face recognized in test image 2

5. CONCLUSION

We were able to detect and recognize the faces of criminals in both images and video streams obtained from a camera in real-time. We used Haar feature-based cascade classifiers in OpenCV for face detection. This machine learning-based approach involved training a cascade function with a large set of positive and negative images, which was then used to detect objects in other images. Additionally, we employed Local Binary Patterns Histograms (LBPH) for face recognition. Several advantages of this algorithm included efficient feature selection, a scale and location invariant detector (which scaled the features rather than the entire image), and the ability to train a generic detection scheme for detecting other types of objects (e.g., cars, signboards, number plates, etc.). The LBPH recognizer could accurately identify faces in varying lighting conditions and was effective even when a single training image was used for each person. However, our application also had some disadvantages: the detector was most effective only on frontal face images and struggled with 45° face rotations along both the vertical and horizontal axes.

REFERENCES

[1] 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.

[2] Bornet, O. (2005, May 19). Learning-Based Computer Vision with Intel's Open Source Computer Vision Library. Retrieved April 2007 from Intel.com Website: Intel Technology Journal

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

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

[5] Viola, P., & Jones, M. (2004). Robust Real-time Object Detection. *International Journal of Computer Vision*.

[6] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 815-823.

[7] Kazemi, V., & Sullivan, J. (2014). One millisecond face alignment with an ensemble of regression trees. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 1867-1874.

[8] Howard, A. G., et al. (2017). MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications. *arXiv preprint arXiv:1704.04861*.

[9] Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You Only Look Once: Unified, Real-Time Object Detection. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 779-788.

[10] Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). Face Recognition: A Literature Survey. *ACM Computing Surveys*, 35(4), 399-458.