

Enhancing Public Safety: A Comprehensive Analysis of Crime Vision Strategies

Dr. S. Gnanapriya¹, Anitha IR²

¹Assistant professor, Department of Computer Applications, Nehru college of management, Coimbatore, Tamilnadu, India

²Student of II MCA, Department of Computer Applications, Nehru College of Management, Coimbatore, Tamilnadu, India

Abstract

There is an abnormal increase in the crime rate and also the number 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. With the advent of security technology, cameras especially CCTV have been installed in many public and private areas to provide surveillance activities. The footage of the CCTV can be used to identify suspects on scene. 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. This Framework has been widely used by researchers in order to detect the location of faces and objects in a given image. Face detection classifiers are shared by public communities, such as OpenCV. 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 using CNN algorithm which takes human skin colour 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.

Keywords: CNN, Face Identification, Face detection, Face Recognition

1. Introduction

The criminal record contains personal data about a specific person together with a photo. In order to identify any criminal, we need an eyewitness identification of that person. Identification can be done using fingerprint, eyes, DNA etc. One application is facial identification. The face is the main focus of our attention in social interaction and plays a major role in conveying identity and emotions. The facial recognition system uses a database of stored images and compares the captured image to find a match, if any. For each face image, identification can be done using RGB values for eye colour, face width, and height. This system is aimed at identifying offenders in any investigative department. In this system, we

store the criminal's image in the database. Eyewitnesses select the slices that appear on the screen, and with this we get a face image from the database. Thus, this system provides a very friendly environment for the operator as well as the eyewitness to easily identify the criminal if the crime record exists in the database. The developed system is also the first milestone for image detection and recognition based on surveillance video. The number of recorded criminal incidents is increasing, including robbery, vandalism, assault, murder, and kidnapping. However, the conventional methods of criminal investigation and prevention are often labour-intensive and inefficient. To address this challenge, a novel deep learning based system named "Spot Crime" has been proposed. Spot Crime is a web application designed to enhance public safety and support law enforcement efforts by automating the monitoring of live CCTV footage and alerting police officials to suspicious activities. This innovative system employs custom convolutional neural networks (CNNs) and advanced models for behaviour classification, allowing it to analyse human activity in real-time video frames. The selection of the best performing model is based on validation accuracy, and its purpose is to aid in the early detection of criminal incidents. In light of the increasing crime rates in India, especially during lockdowns, the need for such a system has become paramount. Spot Crime offers a solution to the challenges posed by manual surveillance, providing a more effective means of crime prevention and promoting public safety by promptly notifying authorities of potential criminal activity and its location.

2. Problem Statement of Analysis

In criminal tracking systems, identifying and monitoring suspects through multiple data sources is crucial to law enforcement operations. Criminal identification includes facial recognition, gait analysis, and object detection, all of which involve precise detection and extraction of features from raw data such as video feeds or images. The use of AI and deep learning offers advanced solutions for tracking criminals efficiently and in real time.

Traditionally, criminal tracking systems relied on manual surveillance and basic machine learning techniques, which were prone to delays and inaccuracies. Recent advancements in deep learning, particularly with convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have dramatically improved the accuracy of criminal identification, movement tracking, and predictive analysis. These approaches help process large volumes of data more efficiently, resulting in faster and more reliable outcomes.

In this study, we aim to analyse and enhance existing criminal tracking techniques using deep learning methods, integrating key components such as video feed pre-processing, feature extraction, and movement prediction. The algorithm we propose will streamline the criminal identification process by extracting facial features, analysing behavioural patterns, and integrating multiple data sources to accurately predict criminal activity.

3. Idea of Proposed Work

This project is focused on the development of an application called Real-Time Criminal Identification System based on facial recognition. We are able to detect and recognize criminals from both image and video, a stream obtained from images in real time. An authorized person logs in through the welcome page to upload images for viewing. Images are stored in a database. A web camera installed at the airport records captured people and images. Image processing and segmentation is performed on the captured images. Using dlib's point detection algorithm, only faces are identified and the identified images are

compared with the images stored in the database. If a match is found, the captured image is sent to the authorized person along with the date and time via application. This saves a lot of time and is a highly secure process and criminals can be easily detected. Our application is percent accurate and is fast, robust, reliable and easy to use.

3.1 Proposed Work

The proposed criminal tracking system leverages deep learning and AI technologies to accurately identify, track, and predict criminal activities and behaviours. The system integrates various AI-driven components, including face recognition, movement tracking, and predictive analysis, to provide law enforcement agencies with a powerful tool for monitoring suspects in real-time.

3.1.1 Face Detection and Recognition:

- **Face Detection:** The system captures video or image data from surveillance cameras, isolating faces from the background using deep learning techniques such as convolutional neural networks (CNNs).
- **Pre-Processing:** Detected faces undergo normalization (resizing, lighting adjustments, etc.) to ensure consistent quality across different sources.
- **Face Recognition:** The system compares the extracted facial features to a criminal database using feature extraction techniques, identifying potential matches with high accuracy.
- Movement Tracking and Behaviour Analysis:

3.1.2 Movement Tracking and Behaviour Analysis:

- **Real-Time Tracking:** Using recurrent neural networks (RNNs), the system tracks the movement of suspects across different cameras or geolocations. It analyses behaviour to detect suspicious actions, such as loitering, abnormal speed, or evasive movements.
- **Predictive Analytics:** The system uses historical data and movement patterns to predict potential future actions or locations of the suspect, assisting law enforcement in proactive measures.

3.1.3 Feature Fusion and Integration:

The system combines multiple data sources (e.g., facial recognition, gait analysis, video feeds, geolocation) to improve the accuracy of criminal identification and tracking. By fusing various features, the system can handle complex scenarios like partial occlusion or varying lighting conditions.

3.1.4 Real-Time Alerts and Notifications:

Once a criminal is identified or a suspicious activity is detected, the system sends real-time alerts to law enforcement agencies. These alerts can include suspect details, location, and predicted movements.

3.1.5 Data Storage and Privacy:

The system securely stores video feeds, images, and processed data in a centralized database. It ensures compliance with data privacy regulations by encrypting sensitive information and restricting access to authorized personnel.

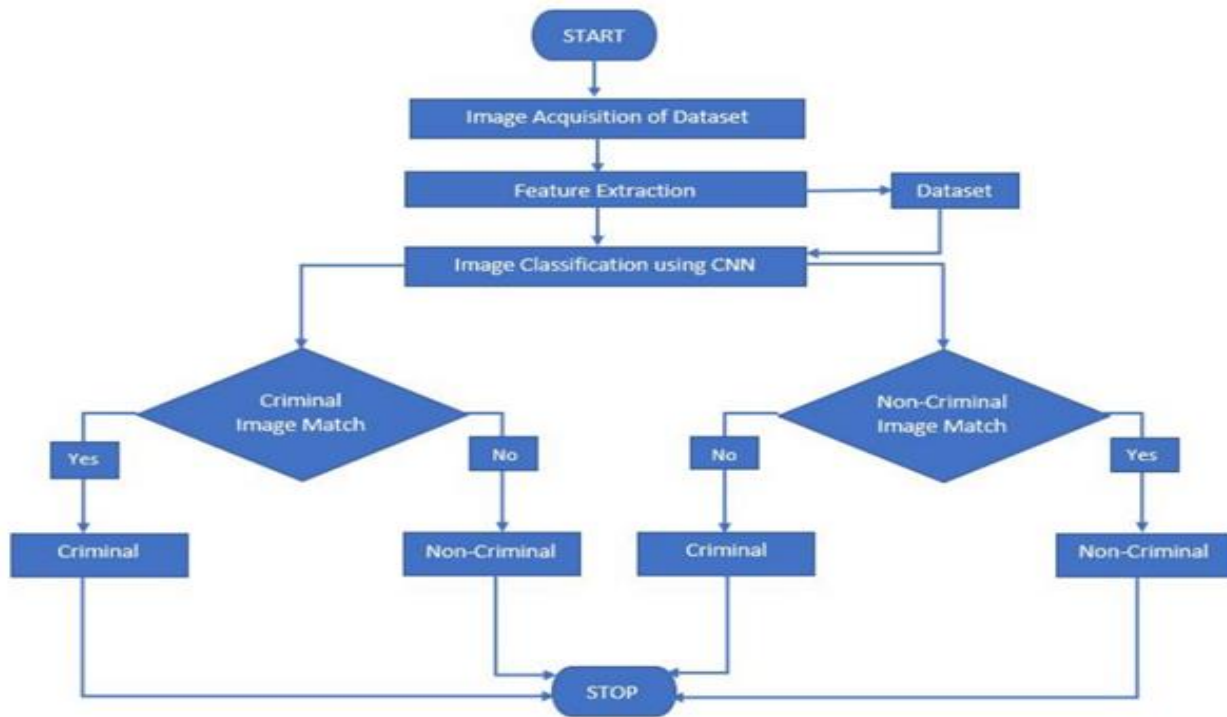


Figure 1: Fundamental steps in digital image processing

The proposed work focuses on developing an advanced criminal tracking system that utilizes deep learning and AI to identify, track, and predict criminal activities. This system will significantly enhance the capabilities of law enforcement by enabling accurate, real-time identification and monitoring of suspects across various data sources such as video feeds, images, and geolocation data.

3.1.6. Pre-Processing

Pre-processing plays a crucial role in the proposed criminal tracking system as it involves extracting essential facial features from raw image data. The goal of this stage is to prepare the facial images for further analysis by normalizing them and enhancing their quality. Specifically, the system resizes the extracted facial images to a standardized dimension of 100x100 pixels.

One of the most widely used techniques in this stage is Histogram Equalization, which enhances the contrast of the image. This method adjusts the intensity distribution across the image, thereby making facial features more distinct and easier to detect. By extending the intensity values, the technique ensures that the facial features stand out more clearly, facilitating more accurate recognition in the subsequent stages.

3.1.7. Database Development

Since the system relies on a biometric-based approach, developing a comprehensive database is vital for accurate identification. The database development phase involves capturing images of individuals and extracting their biometric features, such as facial characteristics.

These captured images undergo pre-processing, where they are enhanced and normalized. The processed biometric features are then stored in a secure database. This database serves as the reference point for the system when identifying or tracking criminals. Each individual's unique facial features are indexed and ready for comparison when the system processes new input.

3.1.8. Post-Processing

Post-processing in the proposed system occurs after the face recognition process has been completed. In

this stage, the names of identified individuals are overlaid onto a live video output. The system matches the identified face with the data stored in the database and displays the corresponding name in real-time. If the system fails to correctly identify a face, the unrecognized individual's details are flagged for review. This post-processing step allows for corrective actions, where the database can be updated with the correct information. This iterative approach helps improve the system's stability and accuracy over time.

3.1.9. Proposed Algorithm

The criminal tracking system operates using the following algorithm:

- **Capture the Individual's Image:** The system captures an image from a video feed or surveillance camera.
- **Apply Face Detection Algorithms:** The system employs face detection algorithms to locate and identify the face within the captured image.
- **Use Viola-Jones and KLT Algorithm:** These algorithms are applied to extract the region of interest (the face) within a rectangular bounding box.

Pre-Processing:

- Convert the image to grayscale.
- Apply histogram equalization to enhance contrast.
- Resize the image to 100x100 pixels.

If Enrolment Stage:

- During the enrolment phase, the system stores the processed image in the database.
- If not in enrolment, the system applies Principal Component Analysis (PCA) for feature extraction to identify the individual.

Post-Processing: Once the face is recognized, the system displays the individual's name on the video output. If recognition fails, the system marks the individual for further review and updates the database accordingly.

This algorithm ensures efficient face detection, pre-processing, and identification, facilitating accurate criminal tracking in real-time.

4. Related Work

Deep learning and artificial intelligence (AI) have significantly advanced the field of criminal tracking and surveillance. Various studies and approaches have contributed to the development of robust systems for identifying and tracking individuals, often focusing on face recognition, behavioural analysis, and pattern recognition.

4.1 Image preprocessing module

Processing features to be extracted to improve face recognition speed. The face image is cropped and resized to a smaller pixel value. If the images contain disturbances, it will be difficult to train the model, resulting in an inaccurate histogram.

4.2 Image segmentation module

This is the main step. Various facial features are extracted. The grayscale images from this step are used to identify the criminal.

4.3 Criminal identification module

The extracted images are identified for faces using dlib library and deep learning algorithm. So the person's face alone is captured without any interruption of the background.

4.4 Database and Dataset module

It is a tool for collecting and organizing information. Databases and datasets can store information about people, crime, law, or cases else. Many pictures of criminals along with their identities are stored in the database and dataset.

4.5 Image Matching Module

The resulting images are compared with existing images in the dataset. If a match is found, data related to that image is returned from the dataset, otherwise the recognized person is not a criminal.

4.6 Warning module

If a criminal is detected, an alert message is sent to the person along with the captured images and details of the criminals using this application.

4.7 Alert and notification generation:

If a significant match is found, the system generates an alert or notification that is sent to the relevant authorities or security personnel in real time. An alert provides information about a potential criminal, including their appearance, location and relevant details, enabling quick action.

5. Neural Networks

Neural networks have revolutionized the field of criminal tracking by providing advanced methods for pattern recognition and data analysis. In this study, we focus on the application of neural networks to enhance criminal tracking systems, particularly through face recognition and anomaly detection.

5.1 Introduction of CNN

Convolutional Neural Networks (CNNs) have emerged as one of the most powerful tools in deep learning, particularly for image recognition and pattern analysis tasks, which are crucial in criminal tracking systems. By mimicking the way the human brain processes visual data, CNNs can efficiently recognize faces, detect objects, and analyse movements, making them ideal for use in AI-based criminal tracking systems. CNNs are a class of deep learning models designed specifically for analysing visual data. They consist of multiple layers that automatically learn to extract features from images through a series of operations like convolution, pooling, and activation functions. Unlike traditional methods that require manual feature extraction, CNNs autonomously learn the relevant patterns and features from the data, making them highly effective in tasks like face recognition and object detection.

5.2 Feedforward Organization

In a feedforward neural network, each neuron processes input from the previous layer and passes the output to the next layer without any feedback loops. The network can be represented by a directed acyclic graph, where information flows in one direction—from input to output. This structure is ideal for understanding the transformation of signals from the input space (such as images) to the output space (such as classification). The power of this network lies in its ability to process data through recombination's of simple nonlinear functions across layers. Feedforward networks are relatively simple to implement and are widely used in practical applications, including criminal tracking. A typical feedforward network is the backpropagation neural network, which is used for training. Here, the error is propagated backward through the layers to adjust the weights, improving the model's accuracy over time.

5.3 Feedback Network

In a feedback neural network, neurons within the network communicate bidirectionally, meaning there is feedback between layers. This type of network can be represented by an undirected complete graph, where every neuron can interact with others, allowing the network to handle dynamic system processing. The

behaviour of this network is governed by state transitions that are well suited to dynamic system theory. Feedback networks are essential for tasks where the system needs to remember and adjust to previous inputs. Two well-known examples of feedback networks include the Hopfield network and the Boltzmann machine, both of which rely heavily on collaborative memory functions and are useful in scenarios that require recalling or maintaining previous information, such as tracking criminals through time-based or sequential data.

5.4 Face Recognition Model with CNN

Face recognition is a critical task in criminal tracking and has seen substantial improvements with the introduction of CNNs. Currently, face recognition algorithms are broadly classified into two main categories:

5.4.1 Representation-Based Methods: These methods transform two-dimensional facial inputs into another space and then use statistical analysis to identify patterns. Some widely used representation-based methods include:

- **Eigenface:** A method that reduces the dimensionality of facial images and represents them as linear combinations of eigenfaces, which are the principal components of the face dataset.
- **Fisherface:** A variation that focuses on maximizing class separability in face recognition.
- **SVM (Support Vector Machine):** A classifier that uses hyperplanes to separate different classes based on facial patterns.

5.4.2 Feature-Based Methods: Feature-based methods focus on extracting local or global facial features and then use classifiers to identify faces. For example:

- **Set Feature-Based Recognition:** Utilizes a set of predefined features for face recognition.
- **HMM (Hidden Markov Model):** A probabilistic model used to model sequences of data, particularly useful for recognizing time-based changes in facial expressions.

6. Network With CNN

In this section, we explore the use of Siamese Networks to address challenges in criminal tracking where the number of available samples per category (e.g., a criminal’s image) is relatively small, but the number of categories (e.g., different criminals) is large. Traditional neural networks, such as those used in classification, often require a large number of labelled samples per class to train effectively. In cases where data is sparse, these traditional approaches become inadequate. The Siamese Network, however, offers a powerful alternative by focusing on measuring similarity between pairs of inputs, making it well-suited for face recognition and criminal tracking systems.

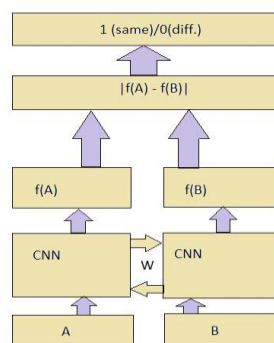


Figure 3: Siamese Network Work Flow

The training process for Siamese Networks involves minimizing the distance between images from the same category (positive pairs) and maximizing the distance between images from different categories (negative pairs). Over time, the network becomes adept at distinguishing between similar and dissimilar images, allowing it to perform well even with small datasets.

7. Results

The proposed method utilizes large databases and pattern recognition to enable computers to interpret visual elements effectively. By leveraging neural networks, the system can recognize and match faces with high accuracy. When the similarity score falls below a predefined threshold, the system can appropriately classify the result as 'not matched.'

Our approach incorporates a semi-supervised learning method, complemented by support vector machines for face recognition. This recognition system is straightforward yet demonstrates high efficiency. Performance evaluations reveal that the proposed method significantly improves accuracy compared to existing face recognition techniques.

Additionally, the KLT (Kanade-Lucas-Tomasi) algorithm and the fusion of Principal Component Analysis (PCA) contribute to enhanced accuracy in face recognition. The system's performance is particularly notable in applications requiring high precision in identifying individuals.

The developed system has successfully created its own database and employs techniques to highlight faces using rectangles. This allows for the reconstruction of original facial images by integrating proper characteristics in the correct proportions. Although each face model only represents specific features, the overall system maintains high fidelity in image reconstruction and recognition.

Conclusion

The proposed model processes a human face image by converting it into a vector representation. The distance between these vectors is then analysed to determine if faces from different images belong to the same individual. Through comprehensive testing and evaluation, the system was developed, designed, and built around this neural network model.

Our study demonstrates that the face recognition system performs effectively, with the proposed methods yielding successful results. The system can accurately identify unknown individuals in real-time scenarios, with Principal Component Analysis (PCA) proving to be superior to other algorithms in this context.

Acknowledgement

I would like to express my sincere gratitude to my institute Nehru college of Management for their invaluable support and guidance throughout this research. Special thanks to my Advisor Dr.S. Gnanapriya for their insightful feedback and encouragement, which greatly contributed to the success of this project.

References

1. Harguess, J., Aggarwal, J.K., A case for the average- half-face in 2D and 3D for facerecognition, IEEE Computer Society.
2. IEEE ,Boda, R., & Priyadarsini, M. J. P. (2016). Face Detection and Tracking Using KLT And Viola Jones. ARPN Journal of Engineering and Applied Sciences, 11(23), 13472-1347.
3. Kavia, M. Manjeet Kaur, (2016). "A Survey paper for Face Recognition Technologies". International

Journal of Scientific and Research Publications, 6(7).

4. Deshpande, N. T., & Ravishankar, S. (2017). Face Detection and Recognition using Viola-Jones algorithm and Fusion of PCA and ANN. *Advances in Computational Sciences and Technology*, 10(5), 1173- 1189.
5. H. A. C. H. a. S. L. Bo Wu, "Fast rotation invariant multi-view face detection based on real Adaboost," *Sixth IEEE International Conference on Automatic Face and Gesture Recognition*, pp. 79-84, 2004.
6. M. J. Paul Viola, "Robust Real-time Object Detection," *International Journal of Computer Vision*, pp. 137-154, 2004.
7. xlvector, "JIANSHU," 25 7 2016. [Online]. Available: <https://www.jianshu.com/p/70a66c8f73d3>. [Accessed 18 9 2018].
8. V. Chu, "Medium.com," 20 4 2017. [Online]. Available: <https://medium.com/initialized-capital/benchmarking-tensorflow-performance-and-cost-across-different-gpu-options-69bd85fe5d58>. [Accessed 19 9 2018].
9. B. Hill, "HOTHARDWARE," 20 8 2018. [Online]. Available: <https://hothardware.com/news/nvidia-geforce-rtx-1080-rtx-1080-ti-799-1199-september-20th>. [Accessed 10 9 2018].
10. W. Hwang, "Face Recognition System Using Multiple Face Model of Hybrid Fourier Feature under Uncontrolled Illumination Variation," 2017. [Online]. Available: <http://ispl.korea.ac.kr/~wjhwang/project/2010/TIP.html>.