IDENTIFYING AND CLASSIFYING OF KNOWN CRIMINALS USING FACIAL RECOGNITION

[1]K.MARUTHI RAO, [2]M.HEMALAKSHMI, [3]S.SWAROOPA, [4]K.GOWTHAMI,

[5]G.ASWINI, [6]P.PRATHYUSHA

[1]ASSOCIATE PROFESSOR, DEPT OF ECE, Dr.SAMUEL GEORGE INSTITUTE OF ENGINEERING AND TECHNOLOGY, MARKAPUR

[2,3,4,5,6]U.G STUDENT, DEPT OF ECE, Dr.SAMUEL GEORGE INSTITUTE OF ENGINEERING AND TECHNOLOGY, MARKAPUR

ABSTRACT

Effective crime prevention and law enforcement require reliable identification systems to track and monitor known offenders. This project aims to develop an advanced facial recognition system utilizing image processing and deep learning techniques to accurately identify and classify individuals based on their facial features. By comparing facial images against an existing criminal database, the system ensures high precision and dependability through processes such as face detection, feature extraction, and classification.

Optimized for real-time application in surveillance systems, public areas, and law enforcement databases, this AI-powered solution enhances suspect identification and helps deter criminal activity. It reduces the need for manual intervention, improves response efficiency, and strengthens public safety. Nevertheless, the implementation must consider ethical standards and privacy regulations to ensure responsible use. The system's overall effectiveness relies on the quality of datasets, environmental conditions, and algorithmic performance, making it a powerful asset in contemporary security and forensic practices.

INTRODUCTION

In the modern digital landscape, law enforcement agencies are increasingly leveraging advanced technologies to enhance security and strengthen crime prevention. Facial recognition, driven by sophisticated image processing, has become a crucial asset for the swift identification and classification of known criminals, significantly expediting investigations.

This technology combines computer vision, deep learning, and biometric analysis to detect and match facial features from surveillance footage, criminal databases, and real-time video feeds. By comparing input images against stored records, it can efficiently verify identities, assess threat levels, and issue immediate alerts to authorities.

Enhanced by artificial intelligence (AI) and machine learning (ML), the system maintains high accuracy even in complex scenarios involving low-light conditions, facial obstructions, or age-related changes. Its broad applicability spans law

enforcement, border management, public surveillance, and security enforcement, contributing to crime deterrence and public safety.

Despite its advantages, facial recognition raises important ethical concerns regarding privacy, data security, and algorithmic bias. To ensure its responsible use, the deployment of such systems must adhere to principles of fairness, transparency, and accountability.

LITERATURE SURVEY

Statistical techniques like Principal Component Analysis (PCA) and Eigenfaces, which were first presented by Turk and Pentland (1991), were used in the early development of facial recognition systems. Though they were limited in their ability to handle changes in lighting, posture, and facial emotions, these techniques served as the basis for automated facial recognition. Local Binary Patterns (LBP) and Linear Discriminant Analysis (LDA) are two feature extraction techniques that later enhanced recognition capabilities. But the true breakthrough in facial recognition came with deep learning, namely Convolutional Neural Networks (CNNs), which greatly increased the accuracy of feature extraction and categorisation. Modern models that have shown exceptional performance in facial recognition tasks, like AlexNet, VGG-16, ResNet, and EfficientNet, are perfect for applications in law enforcement.

Numerous extensive facial datasets have been created in order to train and assess facial recognition software. In the 1990s, one of the first standards for facial recognition research was the FERET dataset. Deep learning models can be trained more effectively with more recent datasets, such Labelled Faces in the Wild (LFW) and SCFace, which offer a variety of facial photos taken in natural settings. To further increase the precision of face recognition-based criminal identification, law enforcement organisations like the FBI and INTERPOL keep huge criminal databases. Nevertheless, the use of these databases presents serious ethical and privacy issues, calling for stringent laws and restrictions.

Real-time processing of facial recognition data presents another difficulty. It is challenging to implement traditional facial recognition algorithms in edge-based surveillance systems due to their high processing requirements. Real-time applications can now use lightweight facial recognition models thanks to recent developments in edge computing and AI hardware accelerators like Google Coral and NVIDIA Jetson. Large-scale criminal detection has also found scalable solutions in cloud-based face recognition systems like Microsoft Face API and Amazon Rekognition. But depending too much on cloud-based processing raises questions about data security and illegal access to private facial information.

EXISTING METHOD

Principal Component Analysis (PCA), particularly through the Eigenface technique, was among the earliest methods used in facial recognition. This approach reduced facial images into lower-dimensional feature spaces, allowing for efficient comparison and classification based on stored data. While PCA was computationally lightweight, it lacked resilience to variations in lighting, facial expressions, and partial occlusions.

To overcome these shortcomings, Linear Discriminant Analysis (LDA) was introduced. LDA aimed to enhance recognition accuracy by maximizing the separability between different classes. Although it improved upon PCA in certain aspects, it remained limited when applied to real-world criminal datasets, which often contain challenges such as pose variations, occlusions, and low image resolution.

Further progress in facial recognition came with the emergence of local feature-based techniques. Methods like Local Binary Patterns (LBP) and Histogram of Oriented Gradients (HOG) were developed to extract texture-based features, offering better robustness to illumination changes and slight pose variations. LBP, in particular, proved effective in controlled environments like police records, where image quality and conditions are consistent. However, both LBP and HOG faced difficulties in uncontrolled environments—such as live surveillance footage—where facial images may vary significantly in angle, resolution, and clarity, limiting their real-time application in dynamic scenarios.

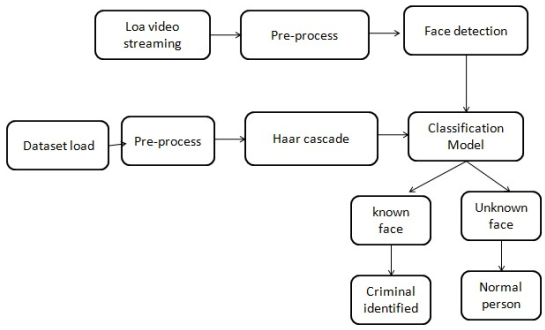
PROPOSED METHOD

The first phase is gathering pictures of people from various sources, such as criminal records, law enforcement databases, and live surveillance feeds. The lighting, posture, and sharpness of the photos are frequently inconsistent. In order to overcome these obstacles, the system uses preprocessing methods such face alignment with Dlib's facial landmark detection, Gaussian filtering for noise reduction, and histogram equalisation for light correction. Furthermore, to increase the resilience of the model, data augmentation methods including rotation, flipping, and scaling are used.

The first phase is gathering pictures of people from various sources, such as criminal records, law enforcement databases, and live surveillance feeds. The lighting, posture, and sharpness of the photos are frequently inconsistent. In order to overcome these obstacles, the system uses preprocessing methods such face alignment with Dlib's facial landmark detection, Gaussian filtering for noise reduction, and histogram equalisation for light correction. Furthermore, to increase the resilience of the model, data augmentation methods including rotation, flipping, and scaling are used.

In order to detect criminals, similarity measures such as Euclidean distance or cosine similarity are used to compare the recovered face embeddings with an existing database of known offenders. A person is designated as a known criminal if a match is discovered above a certain level. The approach classifies criminals according to characteristics including threat level, crime type (such as violence, theft, or fraud), or repeat offender status. Using face embeddings and past criminal histories, machine learning classifiers like Random Forest and Support Vector Machines (SVM) are used to classify people.

SYSTEM DESIGN



DESCRIPTION OF PROPOSED WORK

1. Video Stream Acquisition

The system begins by capturing a live video feed from surveillance cameras or loading footage from a stored video file. Frames are continuously extracted from the stream to enable real-time analysis. To ensure smooth performance and accurate detection, frame rate optimization techniques are employed, balancing speed and computational efficiency.

2. Frame Preprocessing

Each extracted frame undergoes a preprocessing stage to standardize the input data. This includes resizing the image, converting it to grayscale if necessary, and applying normalization to maintain consistency across frames. Noise reduction techniques, such as Gaussian filtering, are implemented to improve image clarity, while histogram equalization enhances contrast, making facial features more distinguishable.

3. Face Detection

In this stage, the system analyzes each frame to identify the presence of human faces using advanced detection algorithms. Techniques such as Multi-task Cascaded Convolutional Networks (MTCNN), Haar Cascades, or deep neural network (DNN) methods provided by OpenCV are applied. Once detected, face regions are cropped and forwarded to the classification model for further analysis.

4. Loading the Face Dataset

A pre-compiled dataset containing facial images of both known criminals and normal individuals is loaded into the system. The dataset is organized into labeled categories such as "Known Criminals" and "Normal Persons." To expedite the matching process, facial embeddings are precomputed, allowing for rapid comparison during real-time operation.

5. Dataset Preprocessing

Images from the dataset are also preprocessed through alignment, normalization, and feature extraction. Deep learning models like FaceNet or VGG-Face are used to generate facial embeddings, which are then stored in a dedicated feature database. This processed data serves as a reference point for identifying individuals in the video stream.

6. Face Detection with Haar Cascade (Optional Module)

In some implementations, the Haar Cascade classifier is utilized as an alternative face detection method. This machine learning-based technique identifies key facial features such as the eyes, nose, and mouth by scanning the image in multiple stages. Once detected,

the face is passed to the recognition system for identity verification.

7. Face Classification and Matching

The core of the system lies in its classification model, powered by deep learning algorithms such as Convolutional Neural Networks (CNNs), FaceNet, OpenFace, or dlib. Each detected face is converted into an embedding and compared against the embeddings stored in the dataset. A similarity score is computed to determine how closely the detected face matches known individuals.

8. Criminal Face Classification

If the computed similarity score indicates a high-confidence match with a known criminal, the system labels the face as "Criminal Identified." An immediate alert is generated and logged for further action by security personnel. Additional details, such as prior crime records, may also be displayed to assist authorities in their response.

9. Unknown Face Classification

When a detected face does not match any individual in the dataset, it is classified as an "Unknown Face." Depending on security protocols, the system may flag the face for further analysis or simply ignore it. Optionally, unknown faces can be stored for future reference or investigation, enhancing long-term surveillance capabilities.

10. Normal Person Classification

If the detected face matches an individual categorized as a normal person, it is labeled accordingly. The system considers this individual non-threatening and continues monitoring without triggering any alerts. This allows the system to focus its resources on potential threats without raising false alarms.

Final Output: Criminal Identification & Alert System

The final stage integrates all the components into a unified criminal identification and alert mechanism. The system effectively classifies individuals into three categories: known criminals, unknown persons, and normal individuals. When a criminal is identified, an automated alert is sent to law enforcement or security teams for immediate response. The categorized data supports continuous surveillance, proactive law enforcement, and in-depth investigations, ultimately contributing to enhanced public safety.

FUTURE SCOPE

One of the primary goals for the future of facial recognition technology is to improve its accuracy and robustness in real-world scenarios. Current systems often face limitations due to external factors such as inconsistent lighting, varied facial angles, occlusions like masks or sunglasses, and the natural aging of individuals. To overcome these challenges, upcoming research will emphasize the adoption of advanced deep learning models—particularly transformer-based architectures and self-supervised learning techniques. These innovations aim to ensure more reliable facial recognition across a wide range of environments and conditions.

An important direction in this evolution is the integration of multi-modal biometric authentication. By combining facial recognition with complementary biometric traits—such as fingerprints, iris scans, and voice recognition—future systems will deliver greater precision and reliability in identity verification, minimizing the risk of false positives or misidentification.

The landscape of criminal detection and surveillance is set to evolve significantly with the integration of facial recognition into real-time monitoring systems. Leveraging edge computing technologies—such as AI-powered surveillance cameras and IoT-based security infrastructure—facial recognition can now be processed directly at the source. This decentralized approach reduces reliance on cloud infrastructure, minimizes latency, and enables faster, more efficient identification and decision-making on the ground.

The deployment of 5G networks will further accelerate these capabilities by supporting high-speed data transfer and enabling real-time processing of high-definition video feeds. Additionally, the use of AI-equipped drones fitted with facial recognition systems will enhance law enforcement's ability to monitor large-scale events, high-security areas, and public spaces with greater precision and agility.

ADVANTAGES

1. Accuracy and Efficiency
2. Real-time Identification
3. Scalability
4. Non-Invasive
5. Automation and Reduced Human Error
6. Enhanced Public Safety
7. Assistance in Missing Person Cases
8. Integration with Other Technologies

DISADVANTAGES

1. Privacy Concerns
2. False Positives and False Negatives
3. Bias and Discrimination
4. Vulnerability to Evasion
5. Dependence on High-Quality Images
6. Ethical Concerns and Legal Issues
7. Resource Intensive
8. Over-Reliance on Technology
9. Security Risks
10. Legal and Regulatory Challenges

APPLICATIONS

1. Real-Time Surveillance Systems
2. Police and Law Enforcement Operations
3. Criminal Database Matching
4. Security in High-Security Areas
5. Border Control and Immigration
6. Crime Scene Investigation
7. Public Safety and Event Management
8. Automated Mugshot Classification
9. Missing Persons and Fugitives Search
10. Integrated Police Workflow Systems

CONCLUSION

Facial recognition has emerged as a groundbreaking tool in the realm of criminal identification, offering law enforcement agencies a faster, more automated, and accurate means of recognizing and classifying individuals with criminal records. Powered by advancements in image processing, deep learning, and artificial intelligence, these systems can analyze facial features with high precision, minimizing dependence on

traditional manual methods. By leveraging expansive facial databases and integrating with real-time surveillance systems, authorities are now capable of identifying suspects more efficiently—enhancing crime prevention strategies and improving public safety outcomes.

Despite these advancements, the deployment of facial recognition in criminal investigations is not without challenges. Variations in lighting, occlusions caused by accessories like masks or glasses, facial disguises, and changes due to aging can affect the reliability of recognition systems. Additionally, the technology raises critical ethical concerns, particularly around data privacy, security, and potential algorithmic bias. Addressing these issues requires the implementation of robust legal frameworks, transparent usage policies, and the use of diverse and representative training datasets. These steps are essential to ensure the technology is applied fairly, responsibly, and effectively within the justice system.

REFERENCES

1.S. Gokulakrishnan, P. Chakrabarti, B. T. Hung and S. S. Shankar, "An optimized facial recognition model for identifying criminal activities using deep learning strategy", *International Journal of Information Technology*, pp. 1-15, 2023.

2.P. Chhoriya, "Automated criminal identification system using face detection and recognition", *International Research Journal of Engineering and Technology (IRJET)*, vol. 6, no. 10, pp. 910-914, 2019.

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

4.J. Hui-Xing and Z. Yu-Jin, "Fast Adaboost Training Algorithm by Dynamic Weight Trimming", *Chinese Journal of Computers*, 2009.

5.[online] Available: https://en.wikipedia.org/wiki/Cascading_classifiers.

6.K. Rasanayagam, S. D. D. C. Kumarasiri, W. A. D. D. Tharuka, N. T. Samaranayake, P. Samarasinghe and S. E. Siriwardana, "CIS: an automated criminal identification system", *2018 IEEE International Conference on Information and Automation for Sustainability (ICIAfS)*, pp. 1-6, December 2018.

7.R. Al-Jawfi, "Handwriting Arabic character recognition LeNet using neural network", *Int. Arab J. Inf. Technol.*, vol. 6, no. 3, pp. 304-309, 2009.

8.Ritu Kaur and Susmita Ghosh Mazumdar, "Fingerprint based gender identification using frequency domain analysis", *International Journal of Advances in Engineering & Technology*, vol. 3, no. 1, 2012.

9.Jessy Alexander and E. Logashanmugam, *Image Based Human Age Estimation Using Principle Component Analysis/Artificial Neural Network*, 2006.

10.H. Verma, S. Lotia and A. Singh, "Convolutional neural network based criminal detection", *2020 IEEE REGION 10 CONFERENCE (TENCON)*, pp. 1124-1129, November 2020.