Library Progress International
Vol.44, No.2s, Jul-Dec 2024: P.1700-1707

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Facial Recognition For Criminal Identification

Dr. G. Indumathi[1*], Dr. K. Sujatha[2], Evans Jayson Thambi.S[3], Immanuel Jason.B[4], Mahadev Sankar[5]

[1*]Assistant Professor, Department of CSE, SRMIST, Ramapura Mailid:indumatg2 @srmist.edu.in
[2]Assistant Professor, Department of CSE, SRMIST, Ramapuram, mail id:sujathak@srmist.edu.in
[3]Department of Computer Science & Engineering, SRMIST
[4]Department of Computer Science & Engineering, SRMIST
[5]Department of Computer Science & Engineering, SRMIST

How to cite this article: G. Indumathi, K. Sujatha, Evans Jayson Thambi.S, Immanuel Jason.B, Mahadev Sankar (2024). Facial Recognition For Criminal Identification . Library Progress International, 44(2s), 1700-1707.

Abstract- Facial recognition technology holds the promise of transforming criminal identification processes by offering a highly effective tool for law enforcement. Its capacity to quickly match individuals with mugshots or surveillance footage can significantly speed up investigations and potentially act as a deterrent to criminal activity. This technology can provide crucial support in solving cases and identifying suspects more efficiently. Facial recognition technology has the potential to revolutionize criminal identification by providing a powerful tool for law enforcement. Its ability to rapidly match suspects with mugshots or surveillance footage can expedite investigations and potentially deter crime. However, its implementation must be approached with caution to address challenges such as accuracy limitations, privacy concerns, and ethical considerations. By carefully considering the benefits and drawbacks, policymakers and law enforcement agencies can harness the power of facial recognition while safeguarding individual rights and privacy.

Index Terms- Face recognition, CNN, Haar Cascade, Face matching, Face encoding, Training models

INTRODUCTION

In today's complex urban environments, law enforcement agencies face unprecedented challenges in identifying individuals swiftly and accurately. Traditional methods often prove inadequate in the face of surging populations and dynamic crime scenarios. To address this, facial recognition technology has emerged as a powerful tool, leveraging advanced algorithms to revolutionize the identification process. This rapid identification capability empowers law enforcement to respond more effectively to incidents, apprehend suspects promptly, and enhance overall public safety.

A. Characteristics of Facial Recognition system:

Facial recognition systems designed to identify criminals possess several key characteristics that enhance their effectiveness and reliability. Here are some of the most important features

Accuracy and Precision

The system's accuracy is crucial for minimizing false positives (incorrectly identifying someone as a match) and false negatives (failing to recognize a known individual).

Real-time Processing

Many modern facial recognition systems can analyze and match faces in real-time. This capability is particularly valuable for surveillance and security applications where immediate identification of suspects is required.

Feature Extraction

Advanced systems focus on unique facial features such as the distance between eyes, nose shape, and jawline. These distinctive attributes are used to create a facial template or biometric signature for comparison.

User Interface and Accessibility:

A user-friendly interface allows law enforcement officers and other users to easily operate the system, view results, and manage data. Accessibility features ensure that the system can be used efficiently in various operational contexts.

B. Advantages of Face Recognition for Criminal Identification

1. Rapid and Accurate Identification
2. Non-Intrusive and Contactless Operation
3. Proactive Public Safety
4. Efficiency and Scalability

Facial recognition technology offers several significant advantages in criminal identification. It can rapidly compare captured images against vast databases of known individuals, providing near- instantaneous results that can significantly accelerate investigations and potentially prevent crimes. Modern algorithms have become increasingly accurate, capable of matching faces with high precision even in challenging conditions. Compared to traditional methods like manual comparison of mugshots, facial recognition is far more efficient, reducing the time and resources required for investigations. Additionally, it is a non- invasive method that does not require physical contact or invasive procedures,making it a less intrusive alternative to techniques like fingerprinting. With interconnected databases and international cooperation, facial recognition technology can be used to identify individuals across borders, aiding in the apprehension of criminals who may have fled to other countries. Furthermore, the presence of facial recognition systems can deter crime by creating a sense of surveillance and increasing the perceived risk of being caught, potentially discouraging individuals from committing illegal acts.

I. USE CASES OF FACE RECOGNITION

Facial recognition technology has various use cases for criminal identification, including:

1. Suspect Identification
2. Surveillance and Monitoring
3. Cold Case Resolution
4. Identity Verification
5. Wanted Person Alerts
6. Border Control

A. Suspect Identification

*F*acial recognition technology, a powerful tool for criminal identification, compares a suspect's face to a database of known individuals, such as mugshots or watchlists. This process involves acquiring a digital image of the suspect's face,extracting key facial features, and comparing them to a database of known individuals.

B. Surveillance and Monitoring

Facial recognition technology can be used to identify individuals in public spaces, such as airports or stadiums,

and alert authorities to potential threats. By comparing live video footage to databases of known individuals, facial recognition systems can detect the presence of individuals who may pose a risk to public safety. This can help law enforcement agencies proactively identify and apprehend potential threats, enhancing security and preventing incidents.

C. Cold Case Resolution

Facial recognition technology can be used to re- examine old cases by comparing the faces of suspects or unidentified individuals to new databases or leads. This can help identify potential suspects who may have previously evaded identification or connect unsolved cases to known individuals. By leveraging the power of facial recognition, law enforcement agencies can uncover new evidence and potentially bring closure to long-standing cases.

D. Identity Verification

Facial recognition technology can be used to confirm identities during arrests, bookings, or parole checks. By comparing the faces of individuals with mugshots or other identifying images, law enforcement agencies can verify the identity of individuals and ensure that the correct person is being detained or released. This can help prevent errors and improve the efficiency of the criminal justice system.

E. Wanted Person Alerts

Facial recognition data can be shared with law enforcement agencies to quickly identify and apprehend wanted individuals. By comparing live video footage or captured images to databases of known criminals, facial recognition systems can detect the presence of wanted individuals in public spaces. This can help law enforcement agencies efficiently locate and arrest individuals who pose a threat to public safety, improving overall security.

F. Border Control

Facial recognition technology can facilitate secure border crossings by identifying travelers and detecting potential security threats. By comparing passport photos or live video footage to databases of known individuals, facial recognition systems can verify the identities of travelers and identify individuals who may pose a risk to national security. This can help improve border security, prevent unauthorized entry, and enhance national safety.

II. RELATED WORK

By comparing facial images to databases of known individuals, facial recognition algorithms can aid in identifying suspects, verifying identities, and deterring crime. However, the implementation of facial recognition systems presents several challenges, including algorithm selection, data quality, privacy concerns, and ethical considerations. To effectively utilize facial recognition in criminal identification, careful consideration must be given to these factors and the specific needs of the law enforcement agency.[2]

According to paper [3], Facial recognition algorithms have been shown to exhibit bias, particularly when identifying individuals from different racial and gender backgrounds. This bias can arise from factors such as insufficient diversity in training datasets, algorithmic limitations, and societal biases embedded within the data. Studies have consistently demonstrated that facial recognition systems are more likely to misidentify individuals with darker skin tones and women, leading to potential discrimination and wrongful arrests. Addressing this bias requires careful consideration of data diversity, algorithm design, and the societal implications of using such technology.

According to paper [4], The widespread adoption of facial recognition technology raises significant societal and ethical concerns. Privacy advocates argue that the constant surveillance enabled by these systems infringes on individual liberties and creates a sense of unease. Additionally, the potential for misuse by authoritarian regimes or for discriminatory purposes poses serious ethical challenges. Balancing the benefits of facial recognition technology with the need to protect individual rights and maintain societal trust is a complex issue that requires careful consideration and ongoing dialogue.

III.EXISTING MODEL

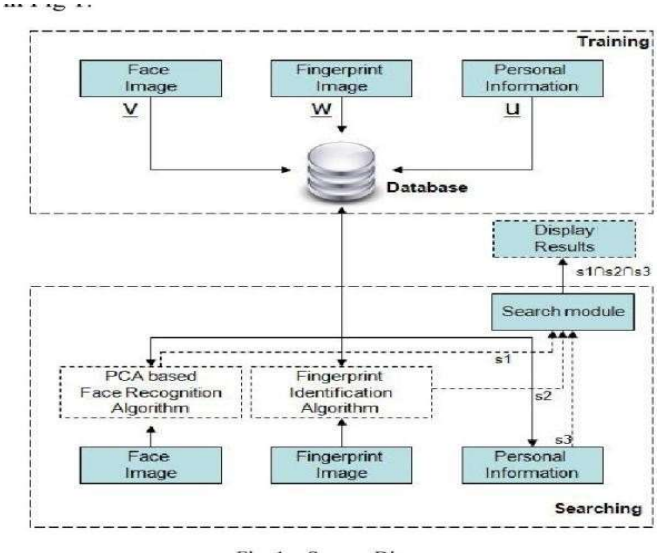

Figure 1.1 Exisitng criminal identification model The above figure 1.1 illustrates the general framework for a criminal identification system using face and fingerprint recognition. The specific algorithm used for fingerprint identification might also have limitations, such as sensitivity to image quality, partial fingerprints, or variations in fingerprint patterns. The accuracy of the system depends on the quality of the face and fingerprint images stored in the database. If the images are of poor quality, blurry, or have insufficient detail, it can hinder the identification process. A large database with millions of records can slow down the search process, especially if it is not efficiently organized or indexed.

The search module might not be optimized for efficient matching, leading to longer search times and potential delays in identification As the database grows and the number of searches increases, the system might face hardware limitations in terms of processing power, storage, and network bandwidth.

Fingerprint recognition requires physical contact with a scanner or surface, which can be inconvenient or impractical in some scenarios. In contrast, facial recognition can be performed from a distance without physical contact, making it more suitable for situations where contact is not feasible or desirable. Fingerprints can become worn or damaged over time due to various factors such as manual labor, aging, or skin conditions. This degradation can reduce the accuracy and reliability of fingerprint recognition systems. Facial recognition does not suffer from such issues since facial features remain relatively consistent over time.Touch-based fingerprint scanners can be subject to hygiene concerns, particularly in high-traffic or public settings. The need for regular cleaning and the risk of transferring germs or contaminants can be a significant drawback. Facial recognition does not have such hygiene concerns, as it is contactless.

IV.PROPOSED SYSTEM

A sophisticated facial recognition system proactively enhances public safety through the rapid identification of individuals with criminal records. The system should be capable of efficiently processing and analyzing vast volumes of facial images sourced from diverse platforms, including surveillance cameras, government databases, and live video streams. It must exhibit exceptional accuracy in matching facial features against a comprehensive criminal offender database, while simultaneously minimizing false positives and negatives to prevent wrongful accusations. To ensure ethical and legal compliance, the system should incorporate robust data privacy and security measures, as well as algorithmic bias mitigation strategies to guarantee equitable treatment.

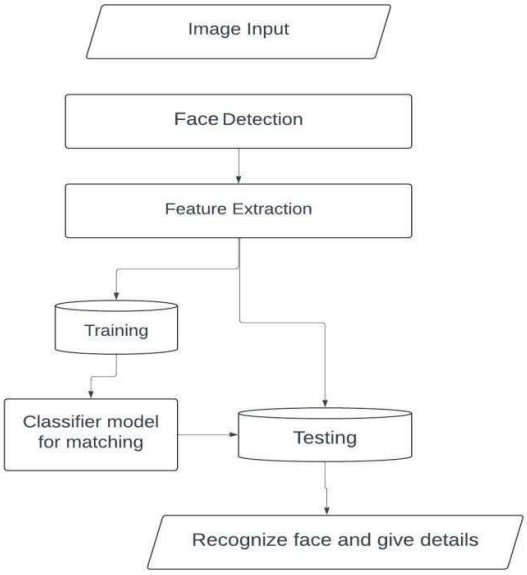

Figure 1.2 Block diagram of Proposed system To develop a facial recognition system, start by assembling a comprehensive dataset of diverse facial images, capturing various conditions such as different angles, lighting, expressions, and demographics. Enhance image quality through preprocessing techniques like normalization, resizing, and grayscale conversion, while employing robust face detection to accurately isolate facial regions. Apply data augmentation methods to increase dataset variability. Select or design a deep neural network optimized for facial recognition tasks, and proceed to train the model, either from scratch or by fine-tuning pre-trained networks on your dataset. Extract facial features into numerical embeddings for efficient comparison, and measure similarity using distance metrics such as Euclidean or cosine. Establish optimal thresholds to differentiate between matching and non-matching faces, and match query images against a database to determine identities. Assess system performance using metrics like accuracy, precision, recall, and F1-score, and continuously refine the model through retraining and hyperparameter tuning. Conduct thorough evaluations to identify strengths and weaknesses, integrate the system into operational environments, and optimize for real-time processing if required. Monitor system performance in production to address any issues, ensure robust data protection and privacy compliance, and develop strategies to mitigate potential biases. Finally, promote responsible and ethical use of the technology throughout its deployment.

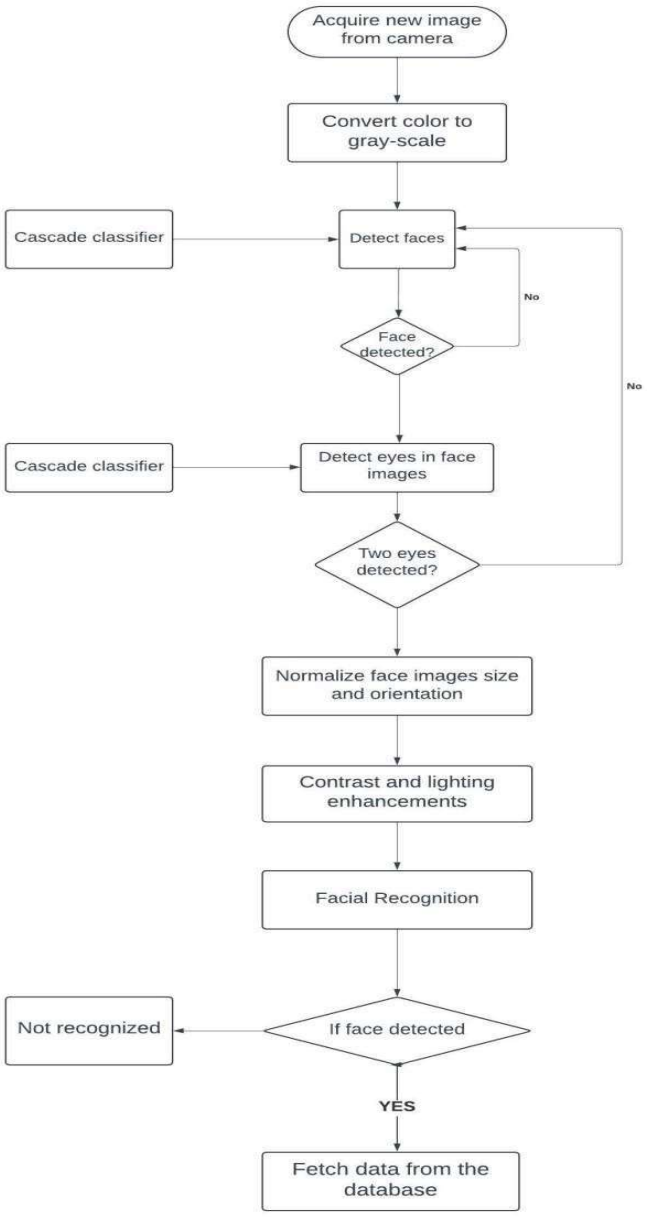

Figure 1.3 Flow diagram of the Proposed SystemThe following flow diagram explains the same:

WORKING OF FACIAL RECOGNITION SYSTEM FOR CRIMINAL IDENTIFICATION

The Facial Recognition System consist of various modules that are crucial for its working. They are:

1. User Interface and Login Module
2. Input Module
3. Processing Module
4. Output Module

User Interface and Login Module

The system presents a user-friendly login interface where the user is prompted to enter their credentials, typically consisting of a username and password. Upon entering these details, the system validates the input against its stored user profiles. If a matching profile is found, the system proceeds to authenticate the user's credentials using

secure password methods. If the authentication is successful, the user is granted access to the system, allowing them to utilize its functionalities. However, if no matching profile is found or the authentication fails, the user is denied access and may be presented with an error message or redirected to a sign-up page.

Input Module

The system utilizes a live camera or an uploaded image as input, capturing instances from the real-world environment. To ensure optimal processing, the system determines the most suitable angle for scanning, considering factors such as lighting conditions and object orientation. The captured data is then subjected to preprocessing, which involves scaling the images to a uniform size, normalizing pixel values to a consistent range, and applying filtering techniques to remove noise and enhance image quality.

Processing Module

The system processes the captured image by scanning it using the Haar Cascade algorithm, which is designed to identify facial features such as eyes, nose, and mouth. The extracted facial details are then compared against the existing database of known faces, searching for any potential matches. This comparison process enables the system to determine if the individual in the image is a recognized user or an unknown person.

Output Module

In the event that the scanned face is identified as a match within the existing database, the system will flag the individual as a known criminal. Additionally, it will provide detailed information about the criminal's identity, including their name,aliases, and any relevant criminal records. Furthermore, the system will assess the individual's threat level based on their criminal history and other factors, providing a comprehensive evaluation of the potential risk they pose.

V. CONCLUSION

A criminal face detection system, as proposed, holds the potential to revolutionize law enforcement by providing an efficient and accurate tool for identifying individuals with criminal records. By integrating face detection, alignment, feature extraction, and recognition algorithms, this system can effectively process images and videos to generate potential matches against a criminal database.

A key advantage of this system lies in its potential for offline operation. By pre-training models and storing the necessary data locally, the system can function without an active internet connection, ensuring uninterrupted surveillance and response capabilities. Additionally, by optimizing algorithms and utilizing efficient hardware, the system can be designed to operate with minimal computational resources, making it suitable for deployment in resource-constrained environments.

While offering significant benefits, it is crucial to address the challenges associated with accuracy, privacy, and ethical considerations. Continuous research and development are necessary to improve the system's performance, mitigate biases, and safeguard individual rights. By striking a balance between technological advancement and ethical responsibilities, a criminal face detection system can become a valuable asset in enhancing public safety and security.

REFERENCES

[1] Deep Face Recognition with Twins: Improving Performance and Reducing Bias (2023) by J. Deng et al
[2] A Survey Paper on Criminal Identification System Using Facial Recognition and Tracking Algorithms (2023) by S. Aherwadi et al
[3] Algorithmic Bias in Facial Recognition Systems (2020) by A. Buolamwini and J. Gebru.
[4] The Perpetual Line-Up: Race, Ethnicity, and Gender in Automated Facial Recognition Systems (2019) by M. Citron
[5] Real-Time Criminal Identification System Based on Face Recognition (2021) by S. Patil et al
[6] Face Detection And Recognition For Criminal Identification System (2024) by Apurva Pongade, Shruti Karad, Divya Ingale

[7] Enhancing Facial Expression Recognition System In Online Learning Context Using Efficient Deep Learning Model (2023) by Mohammed Aly, Abdullatif Ghallab
[8] Criminal Identification system using facial recognition (2021) by Nagnath B, Deep Chokshi
[9] Efficient Facial Expression Recognition algorithm based on Hierarchical Deep Neural Network Structure (2020) by Ji-Hae Kim, Byung-Gyu Kim,
[10] J. Luo, F. Hu, and R. Wang, ''3D face recognition based on deep learning,'' in Proc. IEEE Int. Conf. Mechatronics Automat. (ICMA), Aug. 2019, pp. 1576–1581.
[11] K. Dutta, D. Bhattacharjee, and M. Nasipuri, ''SpPCANet: A simple deep learning-based feature extraction approach for 3D face recognition,'' Multimedia Tools Appl., vol. 79, nos. 41–42, pp. 31329–31352, Nov. 2020.
[12] T. Russ, C. Boehnen, and T. Peters, ''3D face recognition using 3D alignment for PCA,'' in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., vol. 2, Jun. 2006, pp. 1 391–1398.
[13] H. Mohammadzade and D. Hatzinakos, ''Iterative closest normal point fo3D face recognition,'' IEEE Trans. Pattern Anal. Mach. Intell., vol. 35no. 2, pp. 381–397, Feb. 2012.
[14] Y. Taghizadegan, H. Ghassemian, and M. Naser-Moghaddasi, ''3D face recognition method using 2DPCA-Euclidean distance classifification,''ACEEE Int. J. Control Syst. Instrum., vol. 3, no. 1, pp. 1–5, 2012.
[15] D. Huang, M. Ardabilian, Y. Wang, and L. Chen, ''3-D face recognition using eLBP-based facial description and local feature hybrid matching,'' IEEE Trans. Inf. Forensics Security, vol. 7, no. 5, pp. 1551–1565,Oct. 2012.