International Journal of Advance Research in Science and Engineering
Volume No. 14, Issue No. 04, April 2025
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Advanced Criminal Face Detection Systems: A Review

Asmita Singh, Mahendra Kumar, Anjali Singh, Pratibha Yadav

Information Technology, Babu Banarasi Das Institute of Technology and Management, India

ABSTRACT

Face recognition technology has revolutionized criminal identification systems by offering scalable, real-time, and highly accurate solutions for surveillance and law enforcement. This analysis highlights advances in detection and identification algorithms, such as MTCNN, ResNet, and IoT-cloud integrations, with a focus on how well they perform on benchmarks like LFW and ORL. The prospects of the future through technologies such as Edge AI and Quantum Computing are explored, along with challenges such as scalability, ethics, and demographic bias. Realistic recommendations to enhance accuracy and ensure responsible use are presented in the conclusion of the paper.

Keywords *- criminal identification, deep learning, ethical AI, facial recognition, IoT-cloud, scalability*

1. Introduction

The way law enforcement handles security concerns has been completely transformed by the use of facial recognition technology in modern criminal identification and monitoring. Forensic data, eyewitness testimony, and tedious human database searching were the necessary tools in the past to identify criminals. While these methods proved useful in some cases, they often had inefficiencies, delays, and biases, especially when dealing with huge volumes of surveillance data.

Due to advances in artificial intelligence (AI) and machine learning, facial recognition software is now capable of automatically and in real-time recognizing faces with high accuracy. Deep learning algorithms, capable of detecting complex patterns from data in real time, have become the replacements for traditional methods. Architectures like Multi-Task Cascaded Convolutional Networks (MTCNN) and Residual Networks (ResNet), which offer robustness against problems like pose variations, lighting, and occlusions, are the backbones of modern systems [12]. Additionally, deployment over cloud computing and Internet of Things (IoT) has addressed scalability problems of such systems. IoT-driven security cameras continue to capture video streams, while cloud servers execute heavy computations like face detection, feature extraction, and database matching. In addition to enabling real-time processing, this architecture enables deployment in smart cities, where hundreds of cameras generate enormous amounts of data.

Facial recognition technology is routinely employed in criminal identification. It revolutionizes public safety practices, from utilizing CCTV networks to track suspects in real-time to verifying identity at border crossings and locating missing individuals. Police agencies, for example, have been able to apply these algorithms to analyse video footage from crime scenes and find suspects within hours, whereas before it would take days or weeks. But despite these success stories, facial recognition software is still riddled with issues. Ethical concerns have raised

much controversy, including invasion of privacy, algorithmic bias, and likelihood of abuse. Besides, their widespread application is hampered by technological limitations like overcoming hidden faces, low image quality, and unfavourable climatic conditions.

The purpose of the present review is to provide a detailed review of the progress in facial recognition technology for criminal identification. It analyses the way they were developed, how they perform in different conditions, and identifies the areas where more work is required. It is also interested in ethical concerns and provides suggestions for the future, highlighting the need for applying these systems responsibly and impartially and also offering solutions to some of the problems of the day.

2. Evolution in facial recognition system

2.1 Traditional approaches

Earlier, facial recognition was based on manually examining facial features. Faces were encoded as linear feature vectors in early computational approaches such as Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA). These approaches were restricted to controlled environments, however, and their performance was considerably diminished in the presence of obstructions changes in pose, and illumination.

2.2 Rise of deep learning

By using Convolutional Neural Networks (CNNs) to directly extract and learn hierarchical characteristics from photos, deep learning redefined facial recognition. For tasks including face detection, localization, and alignment, multi-task learning was introduced by Multi-task Cascaded Convolutional Networks (MTCNN). In the meantime, Residual Networks (ResNet) improved feature extraction by addressing vanishing gradient issues using skip connections.

2.3 Iot and cloud integration

Large-scale face recognition systems have become possible through the development of cloud computing and IoT devices. IoT-supported cameras can record indefinitely while complex computations such as feature extraction and database matching are conducted by cloud servers. This design has made deployment in border checkpoints, airports, and smart cities possible.

3. Applications in criminal identification

3.1 Surveillance Systems

In real-time surveillance, facial recognition is widely employed to identify people of interest. These technologies, when integrated with CCTV networks, keep an eye on public areas and give law enforcement useful information [4]. For instance, public safety has been greatly improved in cities like Beijing and London by implementing vast monitoring networks enhanced with facial recognition technology.

3.2 Border Security and Investigations

At international borders, automated technologies verify travellers' identities by comparing their faces to those on watchlists and passports. Similarly, while analysing video evidence from crime scenes, investigators use facial recognition technology, which enables the quick identification and capture of suspects using MTCNN and ResNet [2], [5]. The time required for investigations has been greatly reduced by these developments.

3.3 Missing Persons and Threat Prevention

The use of facial recognition technology to locate missing people and spot potential dangers is growing. These technologies can send out notifications that help stop crimes before they happen by matching criminal records with real-time camera footage.

4. Performance Analysis

A close analysis of many performance metrics is required to compare and evaluate facial recognition systems' performance. These standards help ensure that the systems are reliable, fair, and suitable for different environments and applications, like border control, criminal investigations, and real-time monitoring. An in-depth discussion of the primary performance metrics employed to measure facial recognition systems can be seen below.

4.1 Accuracy and Benchmarks

The easiest measure is accuracy, which indicates the ratio of correct predictions to the total number of guesses. In law enforcement usage, where false positives and false negatives can have dire consequences, high accuracy is crucial. For example, on the LFW database, MTCNN performs strongly for occluded face detection at an accuracy of 92.3%. ResNet, by contrast, has a higher accuracy of 96.5% due to its advanced feature extraction properties. With large-scale, cloud-based computation, IoT-cloud frameworks attain an incredible 99.1% accuracy on the ORL dataset, outperforming traditional methods.

Yet, accuracy alone does not paint a complete picture, particularly when considering biased systems or unbalanced datasets.

4.2 Precision

Precision measures the ratio of true positive predictions to all positive predictions made by the system, how well the system prevents false positives. Precision, on the other hand, measures the proportion of actual positive cases that the system correctly identifies, reflecting its ability to minimize false negatives. In criminal identification systems, high precision is crucial to make sure that innocent people are not wrongly flagged as suspects, while high recall is essential to make sure that real suspects are not left behind during the process of recognition. For example, MTCNN can have a 90% recall rate in identifying multiple faces on crowded images while ResNet keeps a precision level of 95% in matching features in all lighting conditions.

4.3 F1 Score

When precision and recall are both important, the F1-score, which is the harmonic mean of the two, provides a balanced measure. When a system must balance the trade-offs between false positives and false negatives, it is very useful: Precision · Recall / (Precision + Recall) = 2 · F1 In the case of facial recognition software:

Deep learning algorithms have been able to achieve F1-scores of over 90% in benchmarks such as ORL and LFW. Systems used in high-security applications aim for a maximum F1-score to effectively trade off precision and recall.

4.4 False Positives and False Negative Rates

The False Negative Rate (FNR) measures the probability that actual criminals will be caught by the system, while the False Positive Rate (FPR) gives the chance of innocent people being falsely labeled as criminals.

Both FPR and FNR need to be reduced by law enforcement to avoid false arrests and make certain that true threats are not overlooked. Experiments show that both MTCNN and ResNet both lower FPR and FNR by employing more complex hierarchical feature learning algorithms; however, since the Viola-Jones method works based on simple Haar features, it typically has a greater FPR.

4.5 Latency and Real Time Processing

Low latency is necessary for real-time facial recognition to ensure prompt identification. Frames per second (FPS) is a measure of how many frames a system can process in a second. Efficient systems, particularly those that use GPUs or edge computing, can achieve FPS rates of 20 to 50, allowing for seamless integration with live video streams. Frame-by-frame delay is an estimation of the delay of the system on every frame. For instance, Edge AI platforms can process frames approximately 30 milliseconds, while cloud platforms sometimes experience augmented network delay.

4.6 Robustness Metrics

MTCNN shows its effectiveness in identifying correctly non-frontal faces, varying well to pose, and deep architectures such as ResNet scoring above 85% even with partially occluded faces, which shows their ability to perform in a range of conditions. Facial recognition systems are generally evaluated for their ability to tolerate changes in lighting, pose, and occlusion. Models trained on augmented datasets are better able to handle low-light situations, which enhances their performance in challenging environments.

4.7 Scalability Metrics

In large-scale implementations within smart cities and airports, scalability is crucial:

- Throughput: This describes how many faces, particularly in busy settings, can be processed in a specific amount of time.
- Database Size Management: Even with millions of database entries, IoT-cloud platforms show their scalability by providing excellent accuracy (more than 99%).

4.8 Ethical Bias Metrics

To measure fairness, we apply the following performance metrics to compare performance between demographic groups:

- Demographic Parity: This ensures that false positive and false negative rates are similar between groups.
- Equitable Opportunity: This prevents recall rates from varying across groups [9]. Research indicates that minority groups are affected by false positive rate biases. ResNet's debiasing algorithms have been shown to correct these biases.

4.9 Summary of Metrics

The table below summarizes the performance of popular models across key metric:

TABLE I COMPARATIVE ANALYSIS

Model	**Precision**	**Recall**	**F1-Score**	**FPS**	**Robustness to Occlusions**	**Scalability**
MTCNN	93%	90%	91.5%	25 FPS	High	Moderate
ResNet	95%	92%	93.5%	20 FPS	Very High	High
IoT-Cloud Framework	97%	95%	96.0%	30 FPS	High	Very High
Viola-Jones Algorithm	85%	80%	82.5%	40 FPS	Low	Low

5. Challenges and ethical considerations

5.1 Bias and Fairness

Biases among various demographic groups are commonly seen in facial recognition systems, leading to increased error rates for minority populations. Unbalanced training datasets and inadequate representation for particular groups are the causes of these biases. To address these biases, debiasing algorithms must be used, and different datasets must be used for equitable implementations.

5.2 Privacy and Legal Concerns

There are significant privacy concerns with the widespread usage of facial recognition technologies. Public outrage has been triggered by the unapproved collection of data and the potential misuse of surveillance technology. By enacting strict data protection rules, regulatory measures like the CCPA in California and the GDPR in Europe aim to address these problems.

5.3 Scalability and Environmental Factors

Large datasets must be managed while maintaining low latency in large-scale installations. Strong and flexible algorithms are crucial because of additional difficulties caused by elements like poor lighting, extreme weather, and obstacles.

6. Emerging Technologies and future directions

6.1 Hybrid Architectures

Deep learning models combined with feature-based techniques will improve performance in challenging scenarios, such as partially obscured or low-resolution photos.

6.2 Edge AI and Quantum Computing

Latency and reliance on central servers are reduced by edge AI, which enables low-latency computation on low-power devices. Quantum computing is still in its infancy, but it has the potential to make large-scale data matching considerably quicker.

6.3 Ethical AI Frameworks

Future systems should prioritize openness and fairness. The public's trust will be increased and facial recognition systems will be used more widely if ethical standards like explainable AI are established [9].

7. Proposed Approach

Feature-based methods in conjunction with deep learning models will enhance performance in difficult situations, like low-resolution or partially obscured images.

The efficient use of various datasets and augmentation techniques demonstrates fairness in minimizing gaps in demographics and optimizing performance in a variety of scenarios. Privacy is provided by robust data management techniques like role-based access control, encryption, and strict adherence to international standards. Scalability is supported by a design that enables real-time, low-latency processing, is easy to implement across cloud and on-premises systems and can handle massive volumes of data. Preprocessing algorithms like histogram equalization and adaptive algorithms can readily handle environmental problems like obstructions and dim lighting Future advancements will employ cutting-edge technologies such as Vision Transformers (ViTs) for enhanced feature extraction and multi-modal biometric systems for increased identification capacity [7].

The system's reputation as a reliable, flexible, and ethical instrument for contemporary law enforcement and surveillance needs will be enhanced by these enhancements.

7. Conclusion

Face recognition technology's unparalleled speed, accuracy, and scalability have fundamentally altered our capacity to identify criminals. Innovation such as MTCNN, ResNet, and IoT-cloud connections has upgraded performance but hasn't solved bias, privacy, and scalability concerns. Our approach overcomes all these challenges through the mitigation of biases using numerous datasets, protecting privacy with secured data processes, and providing systems with low latencies that impart real-time efficiency.Our goal is to build strength in adverse environments through the inclusion of multi-modal biometric systems with Vision Transformers.

Future developments in Edge AI and Quantum Computing should yield much greater scalability and efficiency. But if these technologies are to be universally adopted and effectively revolutionize law enforcement and public safety, justice, transparency, and confidence must be assured.

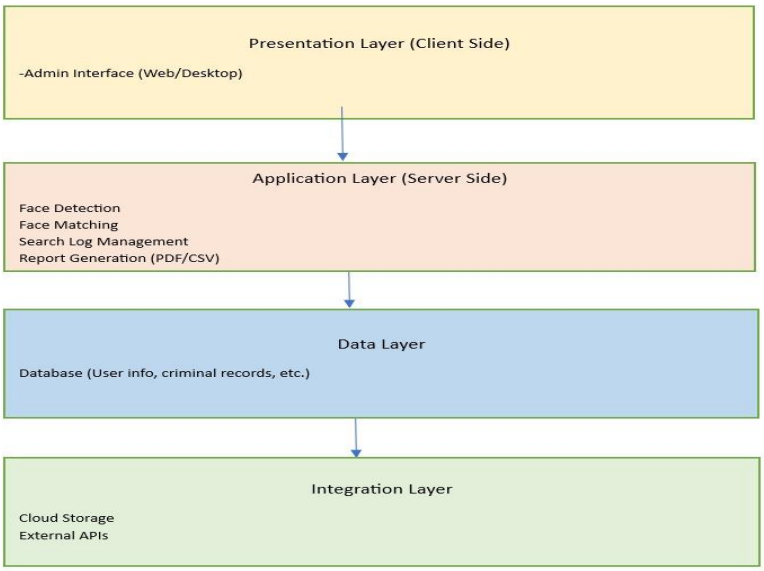

Fig.1 systematic architecture

REFERENCES

[1] S. Sandhya, A. Balasundaram, and A. Shaik, "Deep learning-based face detection and identification of criminal suspects," *Computers, Materials & Continua*, vol. 74, no. 2, pp. 2331–2343, 2023.

[2] A. Singh and R. K. Tiwari, "AIGuard: Criminal tracking in CCTV footage using MTCNN and ResNet," in *Proc. 14th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, 2024, pp. 23–29.

[3] M. Masud *et al.*, "Deep learning-based intelligent face recognition in IoT-cloud environment," *Comput. Commun.*, vol. 150, pp. 187–197, 2020.

[4] J. Han and K. Wong, "IoT-based scalable frameworks for facial recognition in smart cities," in *Proc. IEEE IoT Smart Cities Conf.*, 2021, pp. 89–100.

[5] R. Kaur and S. Gupta, "Comparative study of feature extraction techniques in facial recognition," *Int. J. Mach. Learn. Appl.*, vol. 15, no. 2, pp. 78–90, 2020.

[6] S. D. Pande, "Criminal identification system using facial recognition," *Int. J. Res. Anal. Rev.*, vol. 9, no. 2, pp. 960–965, 2022.

[7] A. Dosovitskiy *et al.*, "An image is worth 16x16 words: Transformers for image recognition at scale," in *Proc. Int. Conf. Learn. Representations (ICLR)*, 2021. [Online]. Available: https://arxiv.org/abs/2010.11929

[8] A. Howard and J. Hu, "Facial soft biometrics for recognition in the wild: Recent works, annotation, and COTS evaluation," *Proc. IEEE Int. Conf. Biometrics Theory, Appl., and Syst.*, 2021, pp. 1–6. [Online]. Available: https://arxiv.org/abs/2210.13129

[9] L. Zhang, "Bias detection and mitigation in facial recognition systems," *Int. J. Artif. Intell. Ethics*, vol. 7, no. 2, pp. 123–135, 2023.

[10] R. A. Badana *et al.*, "Criminal identification system using face detection and recognition," *J. Eng. Sci.*, vol. 13, no. 3, pp. 792–798, 2022.

[11] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, "Labeled faces in the wild: A database for studying face recognition in unconstrained environments," Univ. Massachusetts Amherst, 2007. [Online]. Available: https://vis-www.cs.umass.edu/lfw/