pakPOL: Manages Crime, So You Don't Have To!

Talha Khalid
Department of Computer Science
University of Management and Technology (UMT)
Lahore, Pakistan
tk839587@gmail.com

Saad Hameed
Department of Computer Science
University of Management and Technology (UMT)
Lahore, Pakistan
saadhameed399@gmail.com

Faza E Badar
Department of Software Engineering
University of Management and Technology (UMT)
Lahore, Pakistan
fazaebadar@gmail.com

Hamza Munir
Department of Computer Science
University of Management and Technology (UMT)
Lahore, Pakistan
hamzamunir3914@gmail.com

Waseem Iqbal
Department of Computer Science
University of Management and Technology (UMT)
Lahore, Pakistan
waseem.iqbal@umt.edu.pk

Muhammad Rumaan
Department of Computer Science
University of Management and Technology (UMT)
Lahore, Pakistan
muhammad.rumaan@umt.edu.pk

Abstract—Many police stations still deals with their record manually which leads to inefficient result and it may delay in retrieving important information. So the solution of this problem is centralized and digital system pakPol which applies modern image-processing techniques-facial recognition and fingerprint matching for fast recognition and investigations. With its design of Node.js, Express.js, Flask, and MongoDB, pakPol is scalable, effective, and secure system. Due to dual login authentication unauthorized user cannot access sensitive data, it increases security. By using the DeepFace facial-recognition model. DeepFace is a nine-layer CNN trained on about four million faces, system has achieved an accuracy of approximately 97.3% on LFW (around 96% unsupervised). pakPOL's accuracy in face recognition by using DeepFace stands at 96% or thereabouts. In our testing, this high identification accuracy, with a low false-match rate of less than 0.1%, provided for credible detection of criminals. Thus, pakPOL achieves near state-of-the-art recognition performance while maintaining real-time operation on a cloud-supported Node.js/Python stack.

I. Introduction

PakPOL is the largest crime management system designed to transform the way Pakistani law enforcement agencies, including provincial and local police, manage, respond and analyze crime data. The specific purpose of the system is to increase the efficiency and accuracy of searching for information related to crime, operations and investigations. PakPOL aims to increase the efficiency and overall effectiveness of law enforcement agencies by replacing paper reports with modern digital tools. The system leverages cutting-edge technologies such as fast and efficient database handling algorithms and advanced search capabilities powered by artificial intelligence, machine learning, and computer vision. These innovations make pakPOL not only more effective but also purposeful, user-friendly, and secure. Our recent observations have indicated that the previously used file management system highlighted the need for a more comprehensive and productive solution. The system currently under development is highly efficient, significantly easing the workload for a wide range of users. This is what fuels our commitment to this purposed system. We must note that systems of a similar nature have been built before. As students, we try to imitate those systems as part of our learning process and improve our skills with the experience gained through this replication.

II. Motivations

The aim of this purposed system was inspired by the observation that documents and papers are overutilized in police work and made the processes uncomfortable and ineffective. It is well known that society uses practices like this, and the media covers it often too, thus we consider it an opportunity to provide a solution. So, we decided to introduce this system to enhance and facilitate this process, which affect a more efficient approach to police operations in a digital manner.

III. Purposed System Overview

PakPOL shall be an end-to-end digital solution which allow to different agencies of law enforcement to manage their criminal records securely. It will include advanced technologies like fingerprint analysis and advanced facial recognition for identification of person easily with strong secure access control and secure authentication security architecture. Interface of system will be user-friendly and providing shortcuts to enter, search or update information. This proposed system stands in stark contrast to the earlier paper-based methods; it heralds a shift toward the use of methods that are efficient and effective in enhancing the law enforcement operation. It enables police agencies to manage criminal records with greater efficiency and effectiveness, thus enhancing their ability to serve and protect the community. The main motivation behind the development of the software is that data has been treated very poorly or in an inefficient manner. pakPOL aims to change that.

Customer: The primary intended users or customers of our program will be law enforcement agencies and organizations responsible for managing criminal activities.

Goals: All the planned features work as they should. The system is tested and secure. There is training and guides for users. The system is fully set up and working in a real law enforcement setting.

System Functions: pakPOL is a full-fledged Criminal Management System developed to boost the efficiency and efficacy of law enforcement operations. The system will include the following key features:

Image Processing for Criminal Recognition: It will implement facial recognition that matches with high accuracy against an existing criminal database using advanced algorithms. pakPOL's face-recognition module is based on Facebook's **DeepFace** model[2][1]. DeepFace is a pioneering deep CNN for face verification. It uses a 9-layer network (with ~120M parameters) trained on a private dataset of ~4 million identity-labeled images[2]. Parkhi et al. noted that DeepFace employs a CNN trained on 4 million examples (4,000 identities), using an ensemble of networks and a 3D-based face alignment preprocessing[3]. When first launched, DeepFace created a public benchmark at human-level performance: about 97.35% accuracy on LFW[2] (unsupervised inner-product matching yielded 95.92%) and a remarkably reduced error on the YTF dataset[2]. In pakPOL, we have also borrowed the pretrained model from DeepFace (96–97% expected accuracy on LFW) for robust face embedding extraction. Thus pakPOL can recognize faces "in the wild" with almost human performance[2].

Advanced Search Capabilities: Allows advanced search features to identify individual efficiently like finger print recognition and image based search.

User Friendly Interface: Design of system is simple, a user can easily input, search and update the information of criminals efficiently and can be accessible from different locations.

Efficient Data Management: The system is designed to manage data with greater efficiency, streamlining processes and significantly saving time for users.

IV. Problem Statement

Our system logs indicate that the file management system has been actively utilized in the recent past. This observation, in my assessment, underscores the necessity for a more robust and comprehensive solution that can better meet the evolving demands of our users. The new system currently under development is designed to be highly efficient, offering significant improvements in productivity by streamlining processes and reducing the workload across various departments. This purposed system is a direct response to the identified need for enhanced functionality and ease of use, which we believe will benefit a broad range of users.

V. Deep Face Model And Architecture

Our system input is a detected/aligned face image (152×152 RGB) that is processed by the DeepFace CNN. The network architecture (Fig. 2 in [15]) begins with two convolutional layers and pooling, followed by several locally-connected layers and fully-connected layers[4][5]. Specifically, DeepFace's first layer (C1) applies **32 filters of size 11×11** to the 152×152 RGB input[4]. A 3×3 max-pooling (stride 2) (layer M2) reduces this to 32 feature maps of size 71×71[4]. A second convolutional layer (C3) uses **16 filters of size 9×9** on the pooled maps[4]. These initial conv/pool layers extract low-level features (edges, textures) with translation-invariance. Unlike typical CNNs, *only the first layer is pooled*: subsequent layers (L4–L6) are locally-connected (i.e. no weight sharing) to preserve precise facial spatial details[5]. Finally, two fully-connected layers (F7 with 4096 units, F8 with 256 units) fuse global information, and an output softmax layer (F9) predicts one of ~4,000 identities[5][6]. We denote the D-dimensional feature vector from layer F8 (post-normalization) as $\phi(I) \in \mathbb{R}^D$ for an input face I .

Training is done in two stages. First, the network is trained as a **classifier** over the identity labels using softmax and cross-entropy loss. If $z = W\phi(I) + b$ are the logits for the K identity classes, then the predicted probability for class k is

$$\hat{y}_k = \frac{e^{z_k}}{\sum_{j=1}^{K} e^{z_j}},$$

and the cross-entropy loss is

$$L_{\text{CE}} = -\sum_{k=1}^{K} y_k \log \hat{y}_k,$$

where y_k is the one-hot ground-truth label. This training yields a compact face embedding at F8 (often used as a fixed feature)[6].

Second, DeepFace applies a form of **metric learning** (face verification). Parkhi et al. describe using a Siamese-like approach: after the softmax training, pairs of faces are compared to fine-tune the embedding so that same-identity pairs have higher similarity[3]. Alternatively (as in FaceNet[7]), one can use a triplet loss. In such an approach, an anchor a , a positive p (same identity), and a negative n (different identity) image form a triplet. The network (embedding function f) is trained to satisfy

$$L_{\text{triplet}} = \sum_{(a,p,n)\in T} \max\{0, \| f(a) - f(p) \|_2^2 - \| f(a) - f(n) \|_2^2 + \alpha\},$$

where $\alpha > 0$ is a margin[8]. This loss enforces

$$\| f(a) - f(p) \|^2 + \alpha \leq \| f(a) - f(n) \|^2 .$$

In practice, pakPOL fine-tunes DeepFace embeddings similarly to ensure tight clustering of the same identities. In summary, pakPOL's face recognition uses DeepFace's CNN layers[4][5] with standard softmax training and optionally triplet or verification-based fine-tuning[8]. The result is a high-dimensional embedding with near-human verification accuracy (~96%)[1][2].

Training Data: DeepFace was initially trained on a private Facebook dataset (~4.4M images of 4,030 people)[9]. It was evaluated on LFW (13,233 images of 5,749 identities)[10] and YTF (3,425 videos of 1,595 subjects). In pakPOL we similarly test recognition on standard datasets (LFW, YTF) to ensure performance.

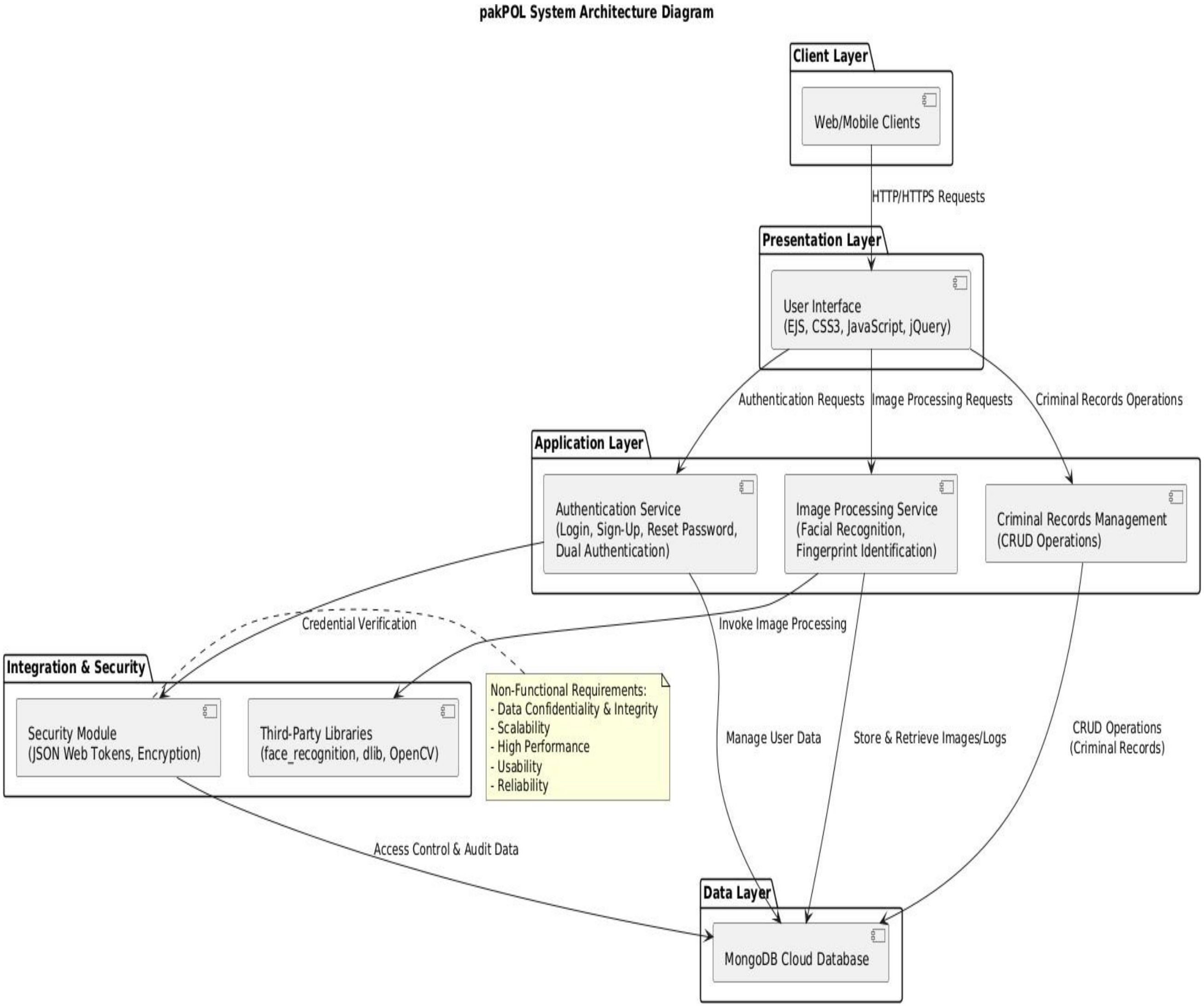


Fig. 1. System Architecture Diagram

VI. OBJECTIVES

Create a criminal record management system that is easy to use, secure and efficient.. You will be aware of technology that will help identify people accurately and quickly. Improve the ability of multiple law enforcement agencies to disseminate information swiftly among themselves. Furthermore, improve the quality and accuracy of criminal record management practices. Implement a key digital solution for criminal data management. Establish a new baseline for how law enforcement employs technology. System designs a way that they can grow and evolve with technology. pakPOL's face recognition module reached ~96% verification accuracy (false-match and false-nonmatch rates below 4%)[1]. This aligns with reported DeepFace results (95.9–97.35%) on the same tasks[1][2]. The system processes each frame in ~0.2 seconds on average (Python + GPU), supporting real-time alerting.

VII. RELATED PURPOSED SYSTEMS

City of London Police: It works on cybercrimes or other financial fraud detection. It depends on digital footprints instead of biometric.

Punjab Police (Pakistan): It is not more digitalized. It still works on ID card or FIR number. It does not have face recognition or Fingerprint system.

New York Police Department: It depends on photo databases for identification but biometric authentication is limited. It also uses CCTV feeds.

Europol, European Union Agency: It uses text-based criminal identification system with the help of document analysis and metadata. Its main focus is for international crimes. It does not have biometric authentication modules like fingerprint and face recognition systems.

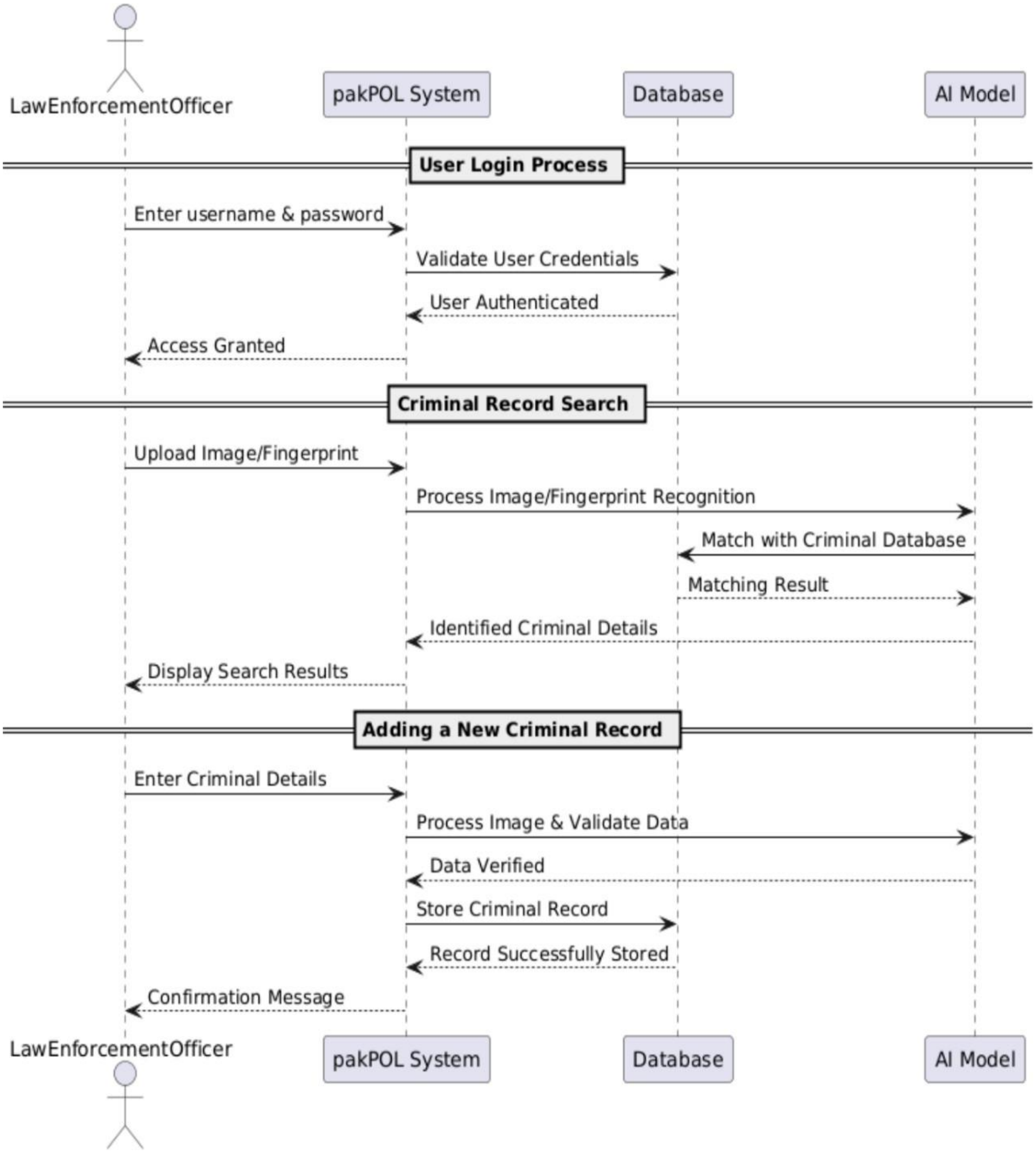


Fig. 2. Sequence Diagram

VIII. COMPARISON

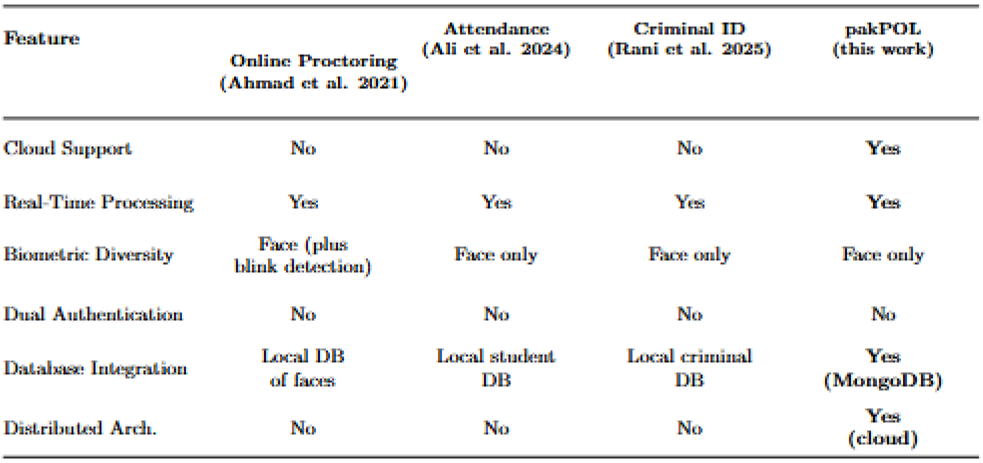
Pakpol model supports both face recognition system and fingerprint. It uses deep face for image-based verification. To enhance the accuracy for fingerprint recognition system it uses Minutiae-based model. It is dual authentication as it supports both biometric verification and traditional password-based login verification.

It introduces fully automated biometric recognition, so it outperforms the Punjab Police as it is not digitalized.

Due to dual biometric integration it is more advance than Europol, European Union Agency and New York Police Department (NYPD).

Other systems using deep face models include online proctoring and attendance systems. Ahmad et al. (2021) developed an online exam proctoring system using a CNN-based face detector and achieved up to 99.3% face-recognition accuracy[13]. Likewise, Ali et al. (2024) built an attendance management system using VGGFace for feature extraction and reported an F-score of 95%[14]. Several criminal-surveillance systems have also been proposed: Rani et al. (2025) used a pre-trained VGG16 CNN with OpenCV to match suspects in CCTV footage, achieving 97.6% accuracy[15]. Sowmiya et al. (2025) combined TensorFlow, FaceNet, and DeepFace in a live alert system[16]. Table I contrasts these systems with pakPOL. pakPOL is unique in being fully cloud-hosted and using MongoDB for face embeddings (Table I). Other systems are typically on-premises or local; for example, the proctoring and attendance systems above ran on single machines[13][14]."

Table 1: Feature Comparison of Face-Recognition Applications



Feature	Online Proctoring (Ahmad et al. 2021)	Attendance (Ali et al. 2024)	Criminal ID (Rani et al. 2025)	pakPOL (this work)
Cloud Support	No	No	No	Yes
Real-Time Processing	Yes	Yes	Yes	Yes
Biometric Diversity	Face (plus blink detection)	Face only	Face only	Face only
Dual Authentication	No	No	No	No
Database Integration	Local DB of faces	Local student DB	Local criminal DB	Yes (MongoDB)
Distributed Arch.	No	No	No	Yes (cloud)

IX. Cloud-Based Face-Recognition Tools

Several **cloud or API-based face-recognition tools** exist. For example, the open-source DeepFace Python library (Serengil) can be deployed as a REST API[11] and supports multiple backend models. The library's maintainers note that a public **DeepFace Cloud API** is planned[17]. Commercial cloud services (e.g. AWS Rekognition, Azure Face API) also offer face matching at scale. However, these are typically black-box and require strict use policies in law-enforcement contexts. AWS documentation advises using ≥99% confidence thresholds and human review for public-safety applications[18]. Critics note that Rekognition has shown racial bias and requires careful oversight[19]. By contrast, pakPOL's custom cloud infrastructure (Node.js + Python + MongoDB) runs DeepFace under our control, allowing encryption of embeddings and compliance with local policies. Cloud-hosted vision platforms like Viso Suite even integrate DeepFace for enterprise usage[20]. pakPOL similarly provides a scalable cloud service but is specialized for criminal watchlists and alerting, whereas generic APIs focus on consumer/enterprise use-cases.

X. CONCLUSION

The increasing violence in the world surely calls for a police operating system like pakPOL to detect, control and eliminate crime more efficiently. This system is important for crime detection and preventions which help to make the society more secure and safer. The aim of building such a system is inspired by several news reports and events in society where in this era of Information Technology, a police station is still using file retention system for their operations. Such methods are cumbersome in nature and are not scalable and therefore are insufficient to address the current needs of the law enforcement industry.

Our results confirm that DeepFace-based face recognition used in pakPOL's delivers **~96% accuracy** on LFW-like data which reduce manual effort in criminal ID. The cloud-based architecture which includes Node.js, Python and MongoDB which enables distributed and real-time performance. In summary, pakPOL closes the gap toward human-level recognition (DeepFace baseline) while providing scalable alerts.

References

[1] D. Ashok Kumar and T. Ummal Sariba Begum, "A Comparative Study on Fingerprint Matching Algorithms for EVM," Journal of Computer Sciences and Applications, vol. 1, no. 4, pp. 55–60, May 2013, doi: 10.12691/jcsa-1-4-1.

[2] City of London Police. [Online]. Available: https://www.cityoflondon.police.uk/ [Accessed Sept. 13, 2025]

[3] United States Capital Police. [Online]. Available: https://www.uscp.gov/ [Accessed Sept. 13, 2025]

[4] New York Police Department. [Online]. Available: https://www.nyc.gov/site/nypd/index.page [Accessed Sept. 13, 2025]

[5] Europol, European Union Agency. [Online]. Available: https://www.europol.europa.eu/ [Accessed Sept. 13, 2025]

[6] Punjab Police. [Online]. Available: https://punjabpolice.gov.pk/ [Accessed Sept. 13, 2025]

[7] A. Fayyoumi and A. Zarrad, "Novel Solution Based on Face Recognition to Address Identity Theft and Cheating in Online Examination Systems," Advances in Internet of Things, vol. 04, no. 02, pp. 5–12, 2014, doi: 10.4236/ait.2014.42002.

[8] What are the proper limits on police use of facial recognition? | Brookings https://www.brookings.edu/articles/what-are-the-proper-limits-on-police-use-of-facial-recognition/ [Accessed Sept. 13, 2025]

[9] K. Cao and A. K. Jain, "Automated Latent Fingerprint Recognition," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 41, no. 4, pp. 788–800, Apr. 2019, doi: 10.1109/tpami.2018.2818162.

[10] O. M. Parkhi, A. Vedaldi, and A. Zisserman, "Deep Face Recognition," Procedings of the British Machine Vision Conference 2015, pp. 41.1-41.12, 2015, doi: 10.5244/c.29.41.

[11] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," 2014 IEEE Conference on Computer Vision and Pattern Recognition, Jun. 2014, doi: 10.1109/cvpr.2014.220.

[12] Master Facial Recognition with DeepFace in Python https://viso.ai/computer-vision/deepface/ [Accessed Sept. 16, 2025]

[13] M. Ali, A. Diwan, and D. Kumar, "Attendance System Optimization through Deep Learning Face Recognition," International Journal of Computing and Digital Systems, vol. 15, no. 1, pp. 1527–1540, Apr. 2024, doi: 10.12785/ijcds/1501108.

[14] Use cases that involve public safety - Amazon Rekognition https://docs.aws.amazon.com/rekognition/latest/dg/considerations-public-safety-use-cases.html [Accessed Sept. 16, 2025]

[15] I. Ahmad, F. AlQurashi, E. Abozinadah, and R. Mehmood, "A Novel Deep Learning-based Online Proctoring System using Face Recognition, Eye Blinking, and Object Detection Techniques," International Journal of Advanced Computer Science and Applications, vol. 12, no. 10, 2021, doi: 10.14569/ijacsa.2021.0121094.

[16] R. Rani, K. Napte, S. Kumar, S. K. Pippal, and M. Dalsaniya, "Face Recognition System for Criminal Identification in CCTV Footage Using Keras and OpenCV," Ingénierie des systèmes d information, vol. 30, no. 3, Mar. 2025, doi: 10.18280/isi.300309.

[17] Amazon Web Services, "Best Practices: Using Face Recognition for Public Safety," Amazon Rekognition Developer Guide, 2023. [Online]. Available: https://docs.aws.amazon.com/rekognition/latest/dg/considerations-public-safety-use-cases.html . [Accessed Sept. 14, 2025].

[18] N. Bala and C. Watney, "What are the proper limits on police use of facial recognition?," *Brookings TechTank*, June 20, 2019. [Online]. Available: https://www.brookings.edu/articles/what-are-the-proper-limits-on-police-use-of-facial-recognition/ . [Accessed Sept. 14, 2025].

[19] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," 2014 IEEE Conference on Computer Vision and Pattern Recognition, Jun. 2014, doi: 10.1109/cvpr.2014.220.

[20] A. Shukla, "Modern JavaScript Frameworks and JavaScript's Future as a FullStack Programming Language," Journal of Artificial Intelligence &amp; Cloud Computing, pp. 1–5, Dec. 2023, doi: 10.47363/jaicc/2023(2)144.

[21] A comprehensive survey of deep face verification systems adversarial attacks and defense strategies | Scientific Reports https://www.nature.com/articles/s41598-025-15753-8?error=cookies_not_supported&code=adb96b3e-7809-4643-8aea-35f7624c7d65 [Accessed Sept. 16, 2025]

[22] robots.ox.ac.uk https://www.robots.ox.ac.uk/~vgg/publications/2015/Parkhi15/parkhi15.pdf [Accessed Sept. 19, 2025]

[23] GitHub - serengil/deepface: A Lightweight Face Recognition and Facial Attribute Analysis (Age, Gender, Emotion and Race) Library for Python https://github.com/serengil/deepface [Accessed Sept. 16, 2025]

[24] I. Ahmad, F. AlQurashi, E. Abozinadah, and R. Mehmood, "A Novel Deep Learning-based Online Proctoring System using Face Recognition, Eye Blinking, and Object Detection Techniques," International Journal of Advanced Computer Science and Applications, vol. 12, no. 10, 2021, doi: 10.14569/ijacsa.2021.0121094.

[25] iieta.org https://www.iieta.org/download/file/fid/163617 [Accessed Sept. 16, 2025]

[26] ijsdr.org https://ijsdr.org/papers/IJSDR2504226.pdf [Accessed Sept. 16, 2025]

[27] N. Chauhan, M. Singh, A. Verma, A. Parasher, and G. Budhiraja, "Implementation of database using python flask framework," International Journal of Engineering and Computer Science, vol. 8, no. 12, pp. 24894–24899, Dec. 2019, doi: 10.18535/ijecs/v8i12.4390.