International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Face Recognition and ID Card Integration for Criminal Identification: Trends and Applications

Puneet Kaur[1*], Taqdir[2]

[1*] *Department of Computer Science, Guru Nanak Dev University, Amritsar, Punjab, India*
[2] *Department of Computer Science and Engineering, Guru Nanak Dev University Regional Campus, Gurdaspur, Punjab, India*

----------s----------***----------

Abstract - The success of security infrastructure relies heavily on face recognition technology which provides dependable and fast identity verification through its systems. An analysis reviews the way facial recognition combines with ID card processing to authenticate criminal identities. The research evaluates seven different sectors that use face recognition systems: law enforcement agencies and border security departments alongside banking institutions and corporate access control points and smart city surveillance operations and healthcare establishments. The analysis includes a complete comparison of domain advantages alongside their barriers through an organized matrix system. The study first addresses implementation barriers while showing national and professional limitations (including legal and ethical restrictions) before focusing on present-day approaches (such as edge computing and multi-modal biometrics) that enhance system capabilities or emergency functions.

***Key Words*:** optics, photonics, light, lasers, templates, journals

1.INTRODUCTION

The nature of security breaches along with identity fraud cases evolves through complex methods which attack manual verification system weaknesses. The manual credential inspection techniques involving security teams and physical identification assessment cause both performance inefficiencies and human mistakes. Significant security gaps exist because of these vulnerabilities so new automated solutions must be developed because illicit individuals could leverage them.

The power of automated face recognition technology enables security professionals to tackle facial recognition problems through comparison between registered biometric templates with current facial images. The verification success rates of Face Net and VGGFace2 reach higher than 99% due to their processing of controlled data samples [1], [2]. The automated systems decrease processing duration and minimize false approvals rates through automated methods which subsequently improves operational effectiveness while strengthening security results [3].

Using face recognition in operational settings requires handling multiple obstacles such as changing illumination and hidden facial features along with aging characteristics and different camera setups. Research indicates unregulated environments decrease performance accuracy by at most 10% [4]. The combination of ID card verification as an additional data source with high-resolution images and document metadata proves essential for improving facial identity checks by combating environmental changes[5].

The article researches the joint operation of facial recognition technology with ID card validation when confirming criminal identities. First the article delivers an abbreviated review of integration protocols before performing an in-depth assessment of identity applications in police departments alongside border protection and financial institutions and corporate security measures and municipal surveillance and medical settings. This paper explores deployment challenges alongside legal barriers and ethical factors together with strategic directions that will support practical tracking systems during implementation.

2. Methodological Overview

A complete deployment process for a Face Recognition-Based Criminal Identity Verification System needs to follow technical steps that maintain accuracy as well as security and efficiency during ID card processing. An

expanded review follows regarding the necessary steps for this system implementation:

1. **Biometric Capture:**

The verification procedure starts by obtaining authentic facial images in real time. Current surveillance techniques employ high-resolution cameras found either within mobile units or surveillance systems to carry out this function. Today's face recognition technology depends on advanced modern cameras together with adaptive sensors to obtain excellent facial images across all environmental conditions during night time and in various viewing positions. The recognition system operates effectively when detecting faces regardless of facial expression variations and angular positioning and minor impeded views including glasses and hats[6]. The cameras allow the integration of extra sensing technologies which improve facial recognition abilities to a higher level.

2. **Document Processing:**

An ID card processing module inside the system enables extraction of data from physical or digital identification cards with real-time facial image capture capabilities. The Optical Character Recognition (OCR) technology helps the system to perform image and text scans across the ID card by extracting name information and date of birth and photo along with other identification characteristics. Modern OCR technologies alongside image enhancement techniques guarantee precise data extraction from scans of both poor and old-quality documents. Once ID details are retrieved from captured data, they become useful for face cross-referencing along with personal identification information. Additional security features present on an ID card can be checked by the system through its configuration settings.

3. **Feature Encoding:**

The system processes captured facial images using deep convolutional neural networks including FaceNet, VGGFace2 and other alternative pretrained architectures for facial embedding generation. These models transform facial pictures through a mathematical process into embedded vectors consisting of 128–512 dimensions to identify individual facial characteristics. The unique vector representation stands up well against changes in lighting and pose and aging differences thus making it highly suitable for comparison needs. Embedding quality plays a vital role since it determines how well the system distinguishes between people and handles difficult situations involving twins and similar faces. The models adapt their functionality through practical implementation to extract matching-relevant features from facial embeddings for operations used by law enforcement and banking.

4. **Similarity Matching**:

Moving forward with the process requires matching the embeddings from facial appearance with the reference image from the ID card. The comparison between embeddings uses similarity matching algorithms which include Euclidean distance and cosine similarity for these calculations. The distance value should be low along with the cosine similarity score to indicate a match between two images belonging to the same individual. The system controls the trade-off between two types of errors by establishing an acceptance threshold which determines correct matching of non-valid faces and correct identification of genuine faces. The threshold gets adjusted based on security requirements of particular applications to strike a balance between system accuracy and user experience.

5. **Criminal Database Cross-Reference:**

The subsequent operation requires a system to check the matched facial image against criminal watchlists and databases. The system will send an alert to security authorities and law enforcement upon discovering matches between present individuals in its system and information on criminal databases or watchlists. Users can set the cross-referencing process to check for matches in different levels of criminal databases such as law enforcement, Interpol’s criminal watchlist and specialized law enforcement databases at national, regional and international levels. The system's real-time alert system stands out as its essential feature because it allows quick responses to security threats. The system configuration determines that additional responses can include facility access lockdowns as well as passport accumulation for border surveillance purposes and automatic database updates for criminal records.

The unified system uses these procedures to deliver both comprehensive and time-sensitive methods for checking identity against criminal records databases. Vulnerable business sectors experience increased security performance through integration of biometric face recognition with ID card validation procedures. The following part will examine applications of this united

system through extended explanations about its practical industrial applications.

3. Applications of face recognition system in identity verifications

The system of face recognition for criminal identity confirmation linked with ID card management produces tangible benefits across six core operational areas. The analysis includes detailed information about distinct application fields alongside usable cases and operational advantages alongside illustrative examples.

A. Law Enforcement & Criminal Tracking

1. Real-Time Patrol Verification: Patrolling officers use portable or vehicular-mounted face recognition systems to scan faces of people they meet in their encounters. The device performs a mugshot database and ID card record comparison as soon as it captures a live image during processing. The verification process which once took officers minutes has been shortened to less than one second through recent pilot studies which led to faster detection of persons of interest and improved officer task execution [7]

2. Surveillance Footage Analysis: Security operations centers can evaluate hours of CCTV footage through automated systems which detect suspicious characters and their appearance. The combination of facial recognition technology and timestamped ID card metadata allows investigators to complete their work 70% faster when conducting forensic investigations which shortens their evidence collection period [8].

3. Missing and Wanted Persons: The comparison of real-time public camera footage against missing or wanted databases maintained at national and local levels enables identification of persons. During major events the integrated system has achieved optimal results by identifying missing children through its matching processes which link database images to real-time camera feeds to recover lost children swiftly[9].

B. Border Security & Immigration Control

1. eGate Automation: Automated border gates (eGates) match human faces to passports while performing watchlist database checks to manage busy airport times. World airports handle each lane of passengers at a rate exceeding 400 per hour based on automated systems that show less than 0.1% error rates leading to reduced waiting times of 50% compared to paper-based procedures [10].

2. Document Integrity Checks: The system performs multiple checks that validate embedded RFID chip data, optical character recognition of MRZ text and holographic security features. The extensive passport validation system has successfully decreased passport fraud at international transit hubs by 90%.

C. Banking & Financial Transactions

1. Remote Onboarding: Financial institutions provide users with step-by-step instructions to capture high-quality facial scans along with government ID upload processes through their selfie-to-ID systems. Algorithm processes perform identification through the assessment of both biometric data along with living confirmation procedures. The 40% improvement rate of remote bank onboarding increases its effectiveness alongside a 30% reduction of identity fraud [11].

2. Transaction Authorization: The combination of face and ID verification serves as a vigorous biologic security element specifically designed for high-value financial operations and wire transfers. This system led institutions to reduce unauthorized transactions by 25% while enabling them to fulfill their responsibilities regarding anti-money laundering regulations.

D. Corporate & Workplace Security

1. Secure Facility Access: Enterprises establish multi-zone access controls which allow employees to authenticate their identity through face recognition of their corporate ID badge system. The implementation of facial authentication reduced entry times from 3 seconds to less than 1 second through badge swipe connection yet it stopped both tailgating and badge-sharing events[12].

2. Time & Attendance: The replacement of manual punch-in systems with automated facial check-ins prevents employees from using other workers for time tracking purposes. Time theft incidents result in decreased occurrences by 15% which leads to more accurate payroll processing.

E. Smart City Surveillance

1. Crowd Analytics: City CCTV network linked with face-ID systems performs live scanning of persons present on security watchlists. Law enforcement narrowed down their response time to incidents during festivals by 60 percent through integrating their systems [13].

2. Traffic and Transit Security: Biometric kiosks verify monthly pass holder IDs at major transit stations

thus they decrease unauthorized entry by 80% while optimizing traffic during peak hours.

F. Healthcare & Patient Safety

1. Patient Identity Verification: Within hospital registration areas patients must submit to facial identification checks which verify their images with insurance documentation. The implementation of face-ID checks at registration desks has succeeded in reducing medical records mismatches by more than 90% thus improving patient safety along with billing precision [14].

2. Controlled Substance Tracking: Controlled substance dispensaries utilize face+ID verification to validate patients before dispensing opioids and related medications thus helping to prevent prescription drug diversion and counterfeit activities[15].

4. **Comparative Application Matrix**

The table below lists the uses of face recognition-based criminal identity verification throughout different sectors. Table1. presents essential benefits with challenges and performance metrics for each criminal identity verification application.

Table 1. Comparative Application Matrix

Application	Sector	Primary Benefit	Challenges	Key Metrics	Technologies Used
Real-Time Patrol Verification	Law Enforcement	Instant criminal record checks in the field	Environmental factors (lighting, occlusion)	Processing time (seconds per individual), Accuracy (~98%)	Mobile Face Recognition, Criminal Databases
Surveillance Footage Analysis	Law Enforcement	Speeding up suspect identification	Low-resolution video, occlusion, camera angle	Resolution time (minutes), False Positive Rate (~5%)	CCTV, Face Recognition Software
Missing and Wanted Persons Detection	Law Enforcement	Proactive detection of high-risk individuals	Data privacy, system integration across jurisdictions	Detection time (minutes), Success Rate (90%)	Facial Recognition, National Registries
eGate Automation	Border Security	Enhanced passenger throughput, fraud reduction	Privacy concerns, passport document variations	Throughput rate (400 passengers/hour), Error Rate (<0.1%)	Facial Recognition, OCR, Document Processing
Document Integrity Checks	Border Security	Detection of forged documents and IDs	Fake biometric features (e.g., synthetic face photos)	Fraud Detection Rate (~98%)	Biometric ID Scanning, OCR
Remote Onboarding	Banking & Finance	Accelerating Know Your Customer (KYC) process	Data privacy, cross-system integration issues	Onboarding time (minutes), Success Rate (~98%)	Selfie-to-ID Matching, KYC System
Transaction Authorization	Banking & Finance	Enhanced security for high-value transactions	User resistance, integration with legacy systems	Authorization time (seconds), Fraud Reduction (%)	Biometric Authentication, Transaction Verification
Secure	Corpor	Controll	Privacy	Access time	Face + ID

Application	Sector	Primary Benefit	Challenges	Key Metrics	Technologies Used
Facility Access	ate Security	ed access to restricted areas	concerns, access control management	(seconds per individual), Error Rate (~1%)	Verification, HR Database Integration
Time & Attendance	Corporate Security	Preventing time fraud (buddy punching)	Real-time clock-in reliability	Fraud Reduction (90%+), Attendance Accuracy (~99%)	Face Recognition, Payroll Systems
Crowd Analytics	Smart City Surveillance	Threat detection and crowd management	High-density areas, privacy concerns	Detection Speed (seconds), False Positive Rate (~5%)	City Surveillance, Face Recognition
Traffic and Transit Security	Smart City Surveillance	Enhanced security at transit hubs	Privacy concerns, integration with existing systems	Verification Speed (seconds), Success Rate (~95%)	Biometric Kiosks, Facial Recognition
Patient Identity Verification	Healthcare	Reducing medical errors and fraud	Data privacy, system compatibility	Verification Speed (seconds), Error Rate (<1%)	Face + ID Verification, Medical Records Integration

3. CONCLUSION

The combination of face recognition technology with ID card verification creates an important development in both security verification and crime tracking systems. The integration of real-time biometrics with official document authentication using these systems leads to enhanced security measures and operational efficiency together with reduced fraud across various sectors which include police forces alongside border protection and financial sector access control and urban observation systems and medical facilities. A multi-layer security system can protect against identity crimes as it applies facial recognition with ID validation to achieve fast verification processes.

Several difficulties persist in this technology because it raises privacy issues and deals with environmental lighting conditions and infrastructure compatibility requirements. Continuous technology advancements combined with policy developments will solve current concerns which include data protection standards and anti-spoofing methods and system interoperability systems. The growing implementation of artificial intelligence including liveness detection and edge AI processing shows promise in addressing specific issues that arise in these systems to improve overall reliability.

Looking ahead, the potential for face recognition-based criminal identity verification systems to revolutionize security and public safety is immense. As technology continues to evolve, it will become increasingly important to balance the need for robust security with the rights of individuals to maintain privacy. Future developments, including the integration of blockchain for secure ID management and improved AI-driven matching algorithms, will further strengthen the reliability, scalability, and adoption of these systems, making them an indispensable tool in modern security infrastructure.

REFERENCES

[1] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015, pp. 815–823. doi: 10.1109/CVPR.2015.7298682.

[2] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, "VGGFace2: A dataset for recognising faces across pose and age," in *2018 13th IEEE International Conference on Automatic Face & Gesture Recognition*, Oct. 2017, pp. 67–74. [Online]. Available: http://arxiv.org/abs/1710.08092

[3] P. Kaur and Taqdir, "Automated Facial Recognition: Technological Innovations, Challenges and Real-World Applications," *International Journal of Engineering Research & Technology (IJERT)*, vol. 14, no. 1, Jan. 2025, doi: 10.3390/s20020342.

[4] L. S. Luevano, L. Chang, H. Heydi Mendez-Vazquez, Y. Martinez-Diaz, and M. Gonzalez-Mendoza, "A Study on the Performance of Unconstrained Very Low Resolution Face Recognition: Analyzing Current Trends and New Research Directions," *IEEE Access*, vol. 9, pp. 75470–75493, 2021, doi: 10.1109/ACCESS.2021.3080712.

[5] P. Kaur, "Exploring the Challenges of Aadhaar based Face Recognition in Unrestricted Environments," *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, vol. 09, no. 01, pp. 1–9, Jan. 2025, doi: 10.55041/IJSREM41021.

[6] P. Kaur and S. Singh, "Emerging Trends in Image Processing and Pattern Recognition: Exploring Transformative Technologies and Their Applications," *International Journal of Computer Science Trends and Technology*, vol. 13, [Online]. Available: www.ijcstjournal.org

[7] H. Bin Kim, N. Choi, H. J. Kwon, and H. Kim, "Surveillance System for Real-Time High-Precision Recognition of Criminal Faces From Wild Videos," *IEEE Access*, vol. 11, pp. 56066–56082, 2023, doi: 10.1109/ACCESS.2023.3282451.

[8] L. HarikaPalivela, P. M. A. Kumar, and V. V. R. Krishna, "Smart Surveillance System Using Face and Optical Character Recognition for Secure Environment," *Advances in Parallel Computing*, vol. 41, no. 1, pp. 387–393, 2022, doi: 10.3233/APC220054.

[9] S. Ayyappan and S. Matilda, "Criminals and Missing Children Identification Using Face Recognition and Web Scrapping," in *2020 International Conference on System, Computation, Automation and Networking, ICSCAN 2020*, Institute of Electrical and Electronics Engineers Inc., Jul. 2020. doi: 10.1109/ICSCAN49426.2020.9262390.

[10] J. Sanchez del Rio, D. Moctezuma, C. Conde, I. Martin de Diego, and E. Cabello, "Automated border control e-gates and facial recognition systems," *Comput Secur*, vol. 62, pp. 49–72, 2016, doi: https://doi.org/10.1016/j.cose.2016.07.001.

[11] K. Verma, A. P. Rao, R. Kumar, and R. Ranjan, "Efficient e-KYC Authentication System: Redefining Customer Verification in Digital Banking," in *2023 9th International Conference on Signal Processing and Communication, ICSC 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 319–324. doi: 10.1109/ICSC60394.2023.10441596.

[12] P. Kaur, "CHAPTER-4 A REVIEW ON COMPUTER SECURITY, CYBER ATTACK DETECTION AND MITIGATION TECHNIQUES."

[13] Gopal Sathe, "Cops In India Are Using Artificial Intelligence That Can Identify You In a Crowd."

[14] J. Mason, R. Dave, P. Chatterjee, I. Graham-Allen, A. Esterline, and K. Roy, "An Investigation of Biometric Authentication in the Healthcare Environment," *Array*, vol. 8, p. 100042, 2020, doi: https://doi.org/10.1016/j.array.2020.100042.

[15] P. Kaur, "Face Recognition Techniques: A Survey." [Online]. Available: https://www.researchgate.net/publication/388405938