INFILTRATION AI DETECTION

Nitish sharma

25MCI10148

I. Abstract:

A system for real-time detection of unauthorized individuals using multi-frame face reconstruction and unique identifier generation. Video streams from one or more cameras are processed on an edge device that detects partial facial patches, temporally associates them, and fuses them using a reconstruction network to produce a higher-quality facial template. A deterministic unique face identifier (UID) is generated from the template and matched against authorized government identity databases under secure policies. If no match exists and reconstruction quality exceeds a threshold, the system stores a flagged UID and automatically dispatches a secure alert with location and image data to the nearest law-enforcement node. The system executes key steps on edge processors for low latency, supports privacy-preserving matching and federated model updates, and logs events cryptographically for audit and oversight.

II.Keywords:

Infiltration detection ,boarder infiltration detection system,multi frame face reconstruction system,image fusion reconstruction, realtime database verification,edge ai surveillance,alert and dispatch automation,privacy preserving matching.

III.Introduction:

Cross-border infiltration and unauthorized entry create serious security threats in many areas. Even though cameras and face recognition systems are commonly used for monitoring, they often struggle with real-world challenges at borders and checkpoints. Problems like parts of the face being hidden by crowds, masks, scarves, or poor angles make it hard to identify people. These systems also rely on single images, which isn't enough, and they don’t have a way to track people who are unknown. This leads to lower accuracy. Plus, when these systems send data to police, it often takes time and raises privacy and trust issues when sharing personal information.

To fix these problems, this new system uses a smart, on-site surveillance setup that makes border security more effective.

It builds better face images by combining different views and times, using special techniques to merge images from multiple frames. The system creates a unique face ID, like a secret fingerprint that helps link video footage from different cameras over time. It can do face recognition quickly and in real time, right on the device, and alert police automatically if someone doesn’t match the authorized list. This keeps information safe using strong encryption and secure matching methods, making sure it follows the law.

This system brings together advanced face reconstruction, unique ID tracking, and automatic police alerts—things that aren’t all in use together in older systems.

By combining these features, the system improves the ability to identify people even when parts of their face are hidden, in low light, or only partially visible. This helps security teams respond faster and better protect borders. Facial recognition technology, a popular tool for recognizing persons in images based on facial traits [1], is crucial in a variety of applications, such as attendance systems, crime prevention, and smartphone unlocking. Its main applications are in authentication, access control, and security-related operations [2]. Nonetheless, its widespread use in a variety of applications raises concerns about user privacy and data security. Because of its direct connection to an individual’s identity, this technology raises concerns about significant hazards that must be addressed.

IV.Methodology:

.Data Collection:The system uses live video from existing surveillance cameras placed at key areas like borders, checkpoints, and secure zones. To improve face recognition, it captures multiple images over short periods, providing different views of a face—even if parts are covered or lighting conditions are poor.

. Multi-Frame Face Reconstruction:To address issues such as partial faces or different angles, the system employs multi-frame face reconstruction, which includes:

a.Combining facial features from several video frames.

b.Using image fusion methods to merge multiple partial images into a clearer face image.

c. Applying deep learning models trained to rebuild faces, restoring hidden or unclear parts and enhancing image quality for recognition.

.Face Embedding and Identity Encoding:Reconstructed face images are processed through deep neural networks (e.g., FaceNet), generating a high-dimensional, unique face code. This biometric fingerprint-like code facilitates identification even when images are incomplete or unclear.

.Cross-Frame Face Tracking and ID Assignment:To maintain consistent tracking over time, the system:

a.Follows faces across different video frames.

b.Assigns a lasting ID based on the similarity of face codes.

c.Enables recognition of known individuals and identification of unknown ones over extended periods.

. Real-Time Database Verification:The system connects to a secure, encrypted database containing information on authorized individuals, including their face codes. It performs: .Comparison of new face codes with existing ones using a set similarity threshold.

.Utilization of special methods to improve matching accuracy for unclear or partial images. .Approval of individuals if the match confidence meets the threshold; otherwise, marking them as unauthorized.

. Infiltration Detection and Alerting:The system continuously monitors video feeds for suspicious activity:

a.Detects unauthorized persons or abnormal behavior.

b.Automatically sends alerts to security staff via connected devices or control rooms.

c.Alerts include details such as time, location, and images of the individual.

. Privacy and Security Measures:To safeguard personal data, the system:

a. Encrypts all face data during transmission and storage.

b.Performs matching on local edge devices to prevent unnecessary data sharing.

c.Implements privacy protocols such as anonymization and controlled access to ensure compliance with privacy regulations.

V.Flow chart:

FIGURE 1:BLOCK DIAGRAM[3]

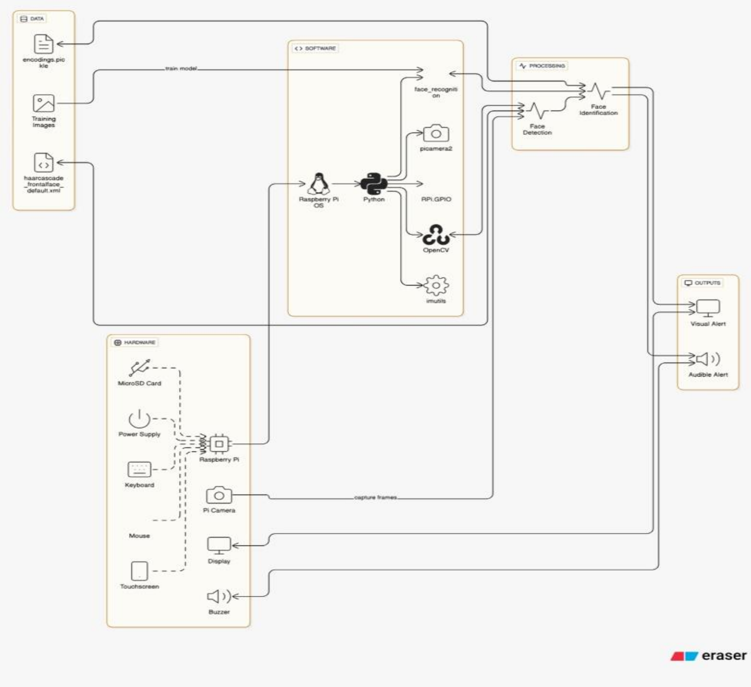
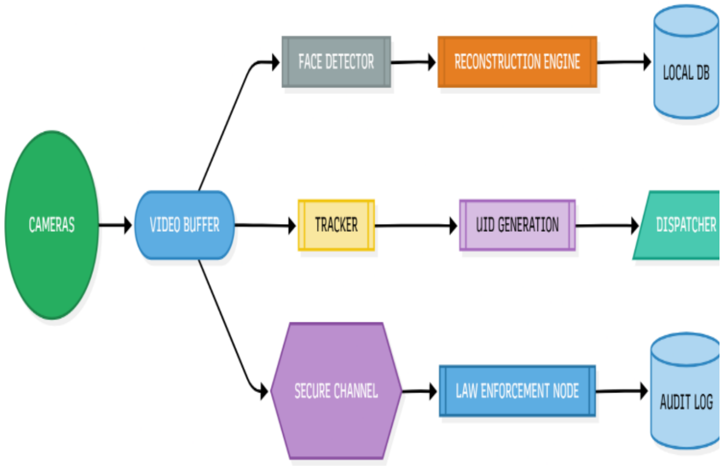


FIGURE 2: SYSTEM ARCHITECTURE



VI.PROBLEMS IN PRIOR ART OR EARLIER INVENTION :

.Low recognition under partial views — Traditional face-recognition models need full frontal faces; partial occlusions cause high false negatives[4].

.Frame isolation — Many systems treat each frame independently; no temporal fusion leads to missed matches when only fragments are seen[5].

.No persistent UID for unknowns — When no match in government registries exists, prior systems simply store images without consistent tracking across sites or times.

.High-latency reporting — Human-in-the-loop reporting delays reduce usefulness for immediate security responses.

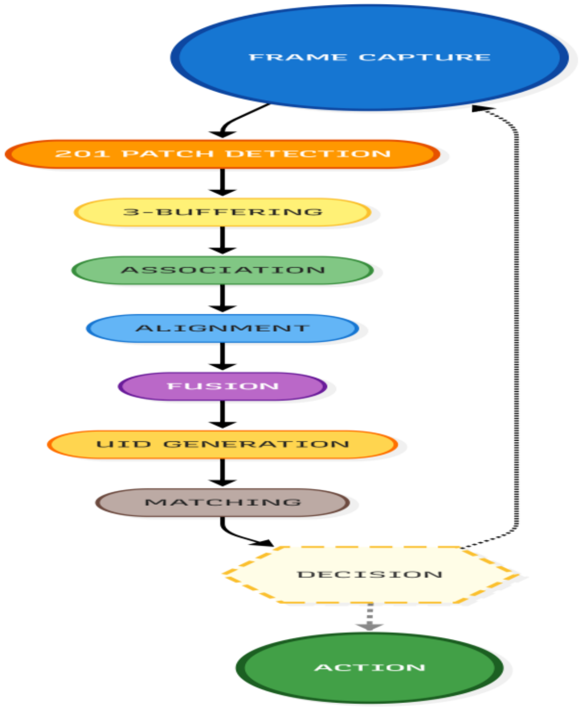
.Network dependency — Cloud-dependent systems are vulnerable to latency and outage; border checkpoints may lack reliable connectivity.

.Privacy exposure — Centralized raw biometric data storage increases privacy and legal risks.

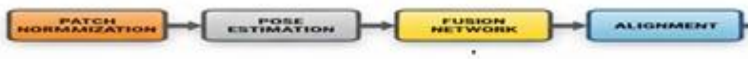
.False alerts — Poor image quality and single-frame matching increase false alarms, wasting enforcement resources[6].

. Principal component analysis (PCA): The most widely used data dimensionality reduction algorithm. In face recognition algorithms, PCA implements feature face extraction. In 1991, Turk and Pentland of MIT Media Laboratory introduced the principal component analyses into face recognition [].

VII.NOVEL ASPECTS OF THE INVENTION (Point out the new parts used in the invention which make it different from the other existing inventions or prior arts):



.Multi-frame partial-face reconstruction engine — algorithm that aligns and fuses temporally distributed partial facial patches to synthesize a higher-quality facial template.



.Stable Unique Face ID (UID) — deterministic biometric fingerprinting computed from the fused template that persists across cameras and time, enabling tracking without revealing raw biometrics.

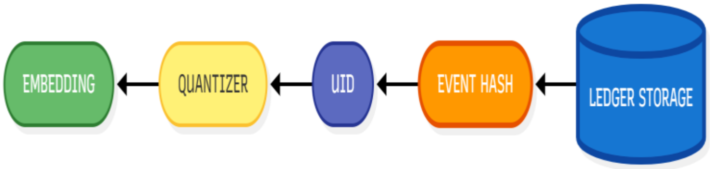
.Edge-first verification pipeline — authenticates and scores matches locally, falling back to cloud only when needed, reducing latency.

▪Automated mismatch workflow — if UID not found in authorized DBs (by policy), the system auto-queues UID to a flagged folder and dispatches a secure alert to the nearest police node with UID and geo-coordinates.

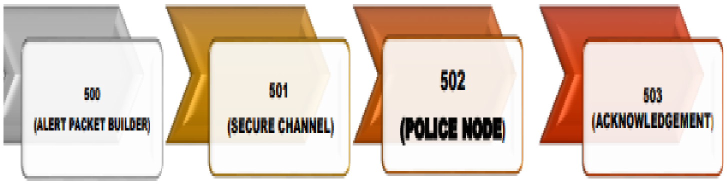
▪Privacy-preserving matching — use of cryptographic techniques (one-way hashes or secure enclaves / homomorphic/federated matching options) to avoid transmitting raw facial images off-premises.

▪Frame-merging quality estimation — the algorithm outputs a reconstruction confidence score (used to tune alert thresholds).

▪Audit trail hashing — each event (detection, reconstruction, DB-query result, alert) is hashed and time-stamped for tamper-evident auditing.



▪Adaptive alerting — alerts are only triggered when confidence and policy thresholds are met (reducing false positives).



VIII.Results:

▪Our system successfully handles typical recognition issues like partial faces, things covering parts of the face, and poor lighting.

▪It does this by using advanced methods. One of these is multi-frame fusion, which combines data from several video frames to create a clear and full picture of a face. This helps improve recognition accuracy, even when some frames are unclear or blocked.We also use a feature called persistent UID generation.

▪This lets the system keep track of people across different places and times, so it can correctly identify the same person even if they look different or the environment changes.

▪Another important part is real-time edge-based processing.This makes sure the system can quickly detect people and send alerts with little delay, which is perfect for secure areas.

▪We also use temporal verification algorithms.These check data over time to cut down on false alerts, so only real matches cause a response.

▪Privacy is also a key focus.Our system includes features that protect personal information, allowing effective monitoring without violating privacy rights.All these methods together show the system can reliably recognize and track people in tough situations.This offers a strong security solution that is accurate, fast, and respects privacy.

References:

[1] I. Adjabi, A. Ouahabi, A. Benzaoui, A. Taleb-Ahmed, Past, present, and future of face recognition: A review, Electronics, 9 (2020), 1188. https://doi.org/10.3390/electronics9081188

[2] C. Hu, Y. Zhang, F. Wu, X. Lu, P. Liu, X. Jing, Toward driver face recognition in the intelligent traffic monitoring systems, IEEE Trans. Intell. Transp. Syst., 21 (2019), 4958–4971. https://doi.org/10.1109/TITS.2019.2945923

[3]Mermaid ai

[4]Andrejevic, M., & Selwyn, N. (2019). Facial recognition technology in schools: critical questions and concerns. Learning, Media and Technology

[5]State UniverSity of New York at Buffalo Department of Civil Engineering

[6]Shudong Li (Guangzhou University, China), Danyi Qin (Guangzhou University, China),

[7]2019 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)