DOI: 10.22413/ijastems/2026/v12/i5/2

Facial Recognition Based On Criminal Alert And Tracking System

A.M. Rangaraj, Y. Sai sree, K. Sandhya, T. Teja Sree, R. Sai Pragathi,B. Sireesha
Department of Computer Science and Engineering, Aditya college of Engineering, Madanapalli

Abstract: In recent years, the increasing demand for public safety has led to the development of intelligent surveillance systems. Traditional CCTV-based monitoring systems rely on human operators, which can result in fatigue, delayed responses, and missed detections. To overcome these limitations, this paper proposes a Facial Recognition Based Criminal Alert and Tracking System that integrates Artificial Intelligence with secure data transmission. The system captures real-time video input, detects human faces using computer vision techniques, and extracts facial features using Convolutional Neural Networks (CNN). These features are compared with a criminal database to identify suspects [4]. Upon successful identification, an automated alert containing the suspect's details such as image, time, and location is generated. To ensure data security and privacy, RSA encryption is applied to protect sensitive information during transmission [6]. The proposed system enhances surveillance efficiency, enables real-time detection, and ensures secure communication, making it suitable for modern security application.

I. INTRODUCTION

In recent years, rapid advancements in technology have significantly transformed the field of security and surveillance systems. With the continuous growth of urban populations and the development of smart cities, ensuring public safety has become more challenging and important than ever before. Surveillance systems are widely deployed in public places such as airports, railway stations, banks, shopping malls, and government institutions to monitor activities and prevent criminal incidents [1], However, traditional surveillance systems mainly rely on Closed-Circuit Television (CCTV) cameras that require continuous monitoring by human operators [2].

Manual monitoring of multiple video streams is a difficult and time-consuming task. Security personnel often experience fatigue, distraction, and reduced attention levels when observing surveillance footage for long durations [3]. As a result, important events may go unnoticed, leading to delayed responses and reduced efficiency in crime prevention. Furthermore, traditional systems do not have the capability to automatically identify individuals or detect suspicious activities in real time, which limits their effectiveness in modern security environments [4].

To overcome these limitations, the integration of Artificial Intelligence (AI) and machine learning technologies into surveillance systems has gained significant attention [5]. AI-based systems are capable of analyzing large volumes of visual data automatically and identifying patterns that indicate suspicious behavior. One of the most important applications of AI in surveillance is facial recognition technology, which enables the identification of individuals based on their unique facial features [6].

Facial recognition systems use advanced algorithms and deep learning techniques such as Convolutional Neural Networks (CNN) to extract and analyze facial features from images or video frames [7]. These features are then compared with a stored database to determine whether a match exists. This technology allows automated identification of individuals and plays a crucial role in enhancing security in various applications, including law enforcement, access control, and public surveillance [8].

However, the use of facial recognition systems also raises concerns regarding data security and privacy. Surveillance systems store sensitive information such as biometric data, personal details, and criminal records. If this data is not properly protected, it may be vulnerable to unauthorized access, cyberattacks, and data breaches. Therefore, it is essential to incorporate strong security mechanisms to ensure the confidentiality and integrity of sensitive information [9].

Cryptography plays a vital role in securing digital data. One of the most widely used cryptographic techniques is the RSA encryption algorithm, which is a public-key encryption method that ensures secure communication and data protection. RSA encryption helps prevent unauthorized access by encrypting sensitive information during storage and transmission .

In this context, the proposed Facial Recognition Based Criminal Alert and Tracking System combines AI-based facial recognition with RSA encryption to develop a secure and efficient surveillance solution. The system captures real-time video input, detects human faces, extracts facial features, and compares them with a criminal database to identify suspects [10]. When a match is detected, the system generates an alert containing the suspect's details such as image, time, and location. This alert is securely transmitted to authorized personnel using encrypted communication.

By integrating intelligent detection with secure data handling, the proposed system aims to improve the efficiency of surveillance systems, reduce human effort, and enhance public safety. It provides a reliable, scalable, and secure solution suitable for modern security applications.

II.Related Work

DOI: 10.22413/ijastems/2026/v12/i5/2

2.1 Face Detection and Recognition Systems

Face detection and recognition play a crucial role in modern surveillance systems. Many researchers have developed computer vision-based techniques to automatically detect and identify human faces from images and video streams. Earlier systems used traditional methods such as Haar Cascade Classifiers for face detection and Principal Component Analysis (PCA) for face recognition. These methods were simple and computationally efficient but had limitations in terms of accuracy and performance under varying lighting conditions and facial expressions.

With the advancement of deep learning, Convolutional Neural Networks (CNN) have become widely used for face recognition tasks. CNN models are capable of automatically extracting important facial features such as eyes, nose, and mouth patterns, and generating accurate feature representations. These models have significantly improved recognition accuracy and can handle variations in pose, lighting, and facial expressions. However, some face recognition systems still face challenges such as occlusion, low image quality, and real-time processing requirements in crowded environments.

2.2 Surveillance and Video Monitoring Systems

Traditional surveillance systems are widely used in public and private environments for monitoring activities and ensuring security. These systems mainly consist of CCTV cameras connected to recording devices, where video footage is continuously captured and stored. Security personnel are responsible for monitoring the live video feeds or reviewing recorded footage when required.

Although these systems are useful for recording events, they rely heavily on manual observation, which can lead to human errors such as fatigue and delayed response. To improve efficiency, some systems have introduced basic video analytics techniques such as motion detection and object tracking. These systems can detect movement and generate alerts, but they lack the ability to accurately identify individuals or detect criminals. Additionally, false alarms are common due to environmental changes such as lighting variations or moving objects .

2.3 AI-Based Smart Surveillance Systems

Recent advancements in Artificial Intelligence have led to the development of smart surveillance systems that can automatically analyze video data and detect suspicious activities. These systems use machine learning and deep learning algorithms to process video frames and identify patterns. Techniques such as object detection, face recognition, and behavior analysis are commonly used in these systems.

AI-based surveillance systems reduce the need for continuous human monitoring and improve detection accuracy. Some systems also support real-time alert generation, enabling faster response to potential threats. However, challenges such as high computational requirements, real-time processing delays, and dependency on large datasets still exist [5]. In addition, many AI-based systems do not focus on secure data handling, which raises concerns about data privacy and protection [6].

2.4 Secure Surveillance and Encryption Techniques

Security of data is an important aspect of surveillance systems, especially when handling sensitive information such as facial images and criminal records [6]. Several research works have focused on integrating encryption techniques to protect data during storage and transmission. Cryptographic methods such as symmetric and asymmetric encryption are used to ensure confidentiality and prevent unauthorized access .

RSA encryption is one of the most commonly used public-key cryptographic algorithms for secure communication. It provides strong security by encrypting data using a public key and decrypting it using a private key [6]. Some modern systems combine facial recognition with encryption techniques to enhance both security and functionality. However, many existing systems still lack proper integration of real-time detection with secure communication mechanisms .

III. Literature Review

3.1 Face Recognition Using Deep Learning Techniques (2024)

Nishu Mishra et al. (2024) proposed a face recognition system based on Convolutional Neural Networks (CNN) for extracting facial features and identifying individuals from images [10]. The system processes input images, detects faces, and converts them into feature vectors for comparison with a stored database. The use of CNN significantly improves recognition accuracy compared to traditional methods such as PCA and LDA [5]. The system is capable of handling variations in lighting conditions, facial expressions, and pose changes. However, the model requires a large amount of training data and high computational resources. Additionally, real-time implementation can be challenging due to processing delays.

3.2 Real-Time Face Recognition-Based Surveillance System (2023)

This study presents a real-time surveillance system that detects and recognizes faces from live video streams [2]. The system uses computer vision techniques for face detection and machine learning algorithms for recognition. It captures video frames continuously and compares detected faces with a database to identify individuals.

The system is effective in providing real-time monitoring and improves the efficiency of surveillance. It can detect multiple faces simultaneously and track their movement across frames. However, the system performance is affected by poor lighting conditions, low-resolution images, and occlusion. It also lacks strong data security mechanisms, making it vulnerable to unauthorized access [2].

3.3 Smart Surveillance System Using AI and Computer Vision (2022)

In this research, an intelligent surveillance system is developed using Artificial Intelligence and computer vision techniques [3]. The system uses object detection and face

DOI: 10.22413/ijastems/2026/v12/i5/2

recognition algorithms to monitor activities and identify suspicious behavior. Deep learning models such as CNN are used to improve detection accuracy.

The system reduces manual monitoring and provides automated alerts when unusual activities are detected. It can be used in public places for enhanced security. However, the system mainly focuses on detection and does not provide strong encryption techniques to secure sensitive data. This creates potential risks related to privacy and data protection.

3.4 Secure Face Recognition System Using Cryptographic Techniques (2025)

Swetha Kambham et al. (2025) proposed a secure face recognition system by integrating cryptographic techniques. The system uses facial recognition for identification and applies encryption algorithms to protect stored and transmitted data. RSA encryption is used to ensure secure communication between different system modules [5].

The proposed approach enhances data security and prevents unauthorized access to sensitive information. It ensures confidentiality and integrity of facial data. However, the integration of encryption increases computational complexity and may affect system performance in real-time applications.

3.5 Real-Time Criminal Detection and Alert System (2024)

This study presents a system designed specifically for criminal detection using facial recognition. The system captures real-time video, detects faces, and compares them with a criminal database to identify suspects. When a match is found, it generates an alert message to notify authorities [5].

The system improves response time and reduces dependency on manual surveillance. It is suitable for use in public safety applications such as airports and railway stations. However, the system does not include strong data encryption methods, which makes it less secure when handling sensitive information [5].

IV. PROBLEM STATEMENT

Existing surveillance systems are widely used in public and private environments to monitor activities and ensure security. These systems mainly rely on CCTV cameras that continuously capture video footage, which is monitored by security personnel. However, this approach depends heavily on manual observation, which is time-consuming and prone to human errors such as fatigue, distraction, and lack of attention. As a result, important events may go unnoticed, and the response to criminal activities is often delayed.

Most traditional surveillance systems do not have the capability to automatically identify individuals or detect criminals in real time. In many cases, video footage is reviewed only after an incident has occurred, making it difficult to take immediate action. This limitation reduces the effectiveness of surveillance systems in preventing crimes and ensuring public safety. Additionally, monitoring multiple camera feeds simultaneously is a challenging task for human operators, which further increases the chances of missing critical events.

Although some modern systems use basic video analytics techniques such as motion detection and object tracking, they still lack accurate identification capabilities. These systems may generate false alarms due to environmental factors such as lighting changes, shadows, or movement of non-threatening objects. Moreover, they cannot reliably recognize individuals or match faces with a criminal database, which limits their usefulness in real-world applications.

Another major issue with existing systems is the lack of proper data security mechanisms. Surveillance systems store sensitive information such as facial images, biometric data, and criminal records. If this data is not protected using strong encryption techniques, it may be vulnerable to unauthorized access, data breaches, or cyberattacks. This raises serious concerns regarding privacy and data protection.

Furthermore, many existing solutions do not provide automated alert systems. Security personnel are often required to manually analyze footage and report incidents, which delays response time. The absence of real-time alert generation makes it difficult for authorities to take immediate action against suspicious activities.

Therefore, there is a need for an intelligent surveillance system that can automatically detect and recognize individuals in real time while ensuring secure handling of sensitive data. The proposed system aims to overcome these limitations by integrating facial recognition using deep learning techniques with RSA encryption for secure communication. This approach improves detection accuracy, reduces human dependency, enables real-time alerts, and ensures data security, thereby enhancing the overall efficiency of surveillance systems.

V. PROPOSED SYSTEM

The proposed system aims to develop an intelligent and secure Facial Recognition Based Criminal Alert and Tracking System that can automatically detect and identify criminals in real time. Unlike traditional surveillance systems that depend on manual monitoring, this system integrates Artificial Intelligence, deep learning, and cryptographic techniques to improve efficiency, accuracy, and security. The system is designed to reduce human effort, provide instant alerts, and ensure the protection of sensitive data.

The system captures real-time video input using surveillance cameras such as webcams or CCTV cameras. The captured video is processed continuously, and individual frames are extracted for analysis. This real-time processing ensures that the system can detect and respond to events instantly without any significant delay. The captured frames mainly focus on human faces, which are the key elements for identification.

The first stage of the system involves face detection using computer vision techniques. In this stage, the system identifies and isolates human faces present in the video frames. Advanced algorithms are used to accurately locate

DOI: 10.22413/ijastems/2026/v12/i5/2

faces even in complex environments with multiple people. Once the faces are detected, they are cropped and prepared for further processing.

In the next stage, feature extraction is performed using deep learning models such as Convolutional Neural Networks (CNN). The CNN model analyzes the detected faces and extracts important facial features such as the structure of the eyes, nose, and mouth. These features are then converted into numerical representations known as face embeddings, which uniquely represent each individual.

After feature extraction, the generated face embeddings are compared with the data stored in a criminal database. The database contains facial images and identification details of known criminals. The system performs a matching process to determine whether the detected face corresponds to any record in the database. If a match is found, the system identifies the individual as a suspect or criminal.

Once a criminal is identified, the system automatically generates an alert message. The alert includes important details such as the suspect's image, detection time, and location. This alert is useful for law enforcement authorities to take immediate action. Unlike traditional systems, this process is fully automated and does not require manual intervention.

To ensure the security of sensitive information, the system uses RSA encryption. Before transmitting the alert, the data is encrypted using the RSA algorithm. This ensures that only authorized users can access the information, thereby protecting it from unauthorized access or cyber threats. The encrypted alert is then securely transmitted to concerned authorities through a communication network.

The system also supports continuous monitoring and can handle multiple faces simultaneously in crowded environments. It is designed to work efficiently under different conditions such as variations in lighting and facial expressions. Additionally, the system maintains logs of detected events for future analysis and investigation purposes.

Overall, the proposed system provides a smart, automated, and secure solution for modern surveillance needs. By combining facial recognition with encryption techniques, it enhances detection accuracy, reduces response time, and ensures data protection. This system can be effectively implemented in real-world applications such as public security, law enforcement, and smart city surveillance.

VI SYSTEM ARCHITECTURE

The proposed system architecture for the Facial Recognition Based Criminal Alert and Tracking System is designed to provide an efficient and secure solution for real-time surveillance. The architecture consists of multiple modules that work together to detect faces, recognize individuals, and generate secure alerts. Each module performs a specific function, and the overall system operates in a sequential and automated manner.

Fig 6.1:System Architecture

The process begins with the video capture module, where real-time video input is collected using surveillance devices such as webcams or CCTV cameras. The camera continuously captures video footage from the monitoring area and converts it into frames for further processing. These frames act as the primary input for the system and contain visual information required for face detection and recognition.

The next stage is the face detection module, which uses computer vision techniques to identify human faces present in the captured frames. The system scans each frame and detects facial regions accurately, even in the presence of multiple individuals. Once the faces are detected, they are extracted and passed to the next module for further analysis.

Following face detection, the system performs feature extraction using deep learning models such as Convolutional Neural Networks (CNN). In this stage, important facial features such as the shape of the eyes, nose, and mouth are analyzed. These features are converted into numerical representations known as face embeddings, which uniquely represent each individual. This step is crucial for accurate face recognition.

After extracting features, the system moves to the matching and identification module. Here, the generated face embeddings are compared with the stored data in the criminal database. The database contains images and details of known criminals. If the system finds a match between the detected face and the stored data, the individual is identified as a suspect. If no match is found, the system continues monitoring without generating any alert.

Once a match is detected, the system activates the alert generation module. This module creates a real-time alert message that includes important details such as the suspect's image, time of detection, and location information. This alert helps authorities take immediate action to prevent or control criminal activities.

To ensure the security of sensitive data, the system incorporates a data encryption module using RSA encryption. Before transmitting the alert, the information is encrypted to prevent unauthorized access. This ensures that only authorized personnel can view and access the alert data, thereby maintaining confidentiality and data integrity. The encrypted alert is then sent through the notification module, which delivers the information to law enforcement authorities or system administrators. The system may use network communication methods such as internet-based

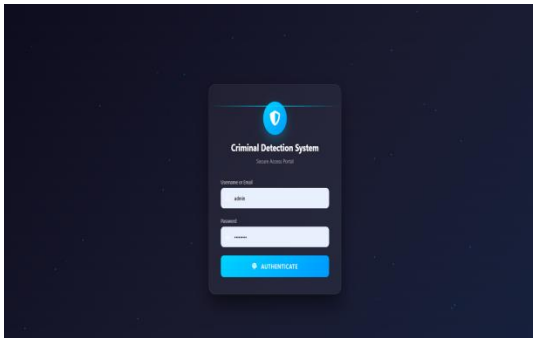
DOI: 10.22413/ijastems/2026/v12/i5/2

messaging or secure channels to send notifications in real time.

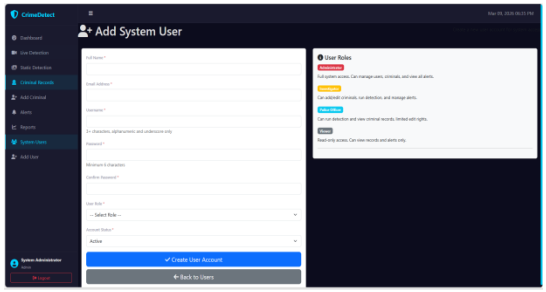
Finally, the system includes a central monitoring and management module, where all alerts and detected information are displayed. This module allows authorized users to monitor activities, view detected suspects, and manage the surveillance system efficiently. It also maintains records of detected events for future analysis and investigation.

Overall, the system architecture integrates video capture, face detection, feature extraction, database matching, alert generation, encryption, and notification into a unified framework. This structured approach ensures accurate detection, fast response, and secure data handling, making the system suitable for real-world surveillance applications.

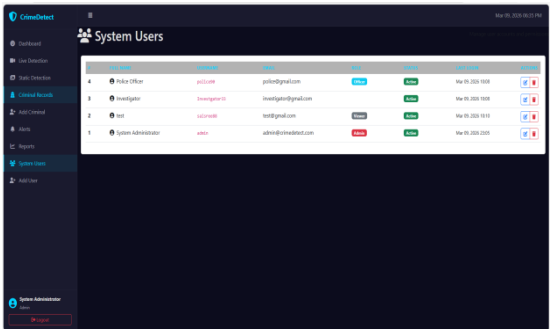
VII. RESULT



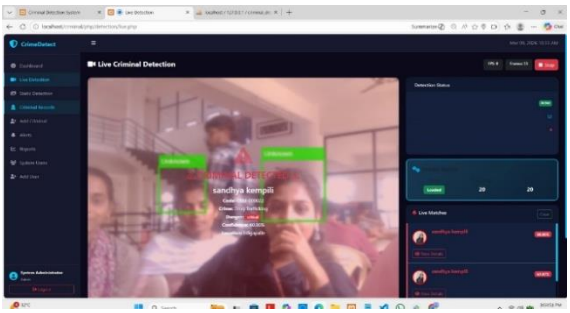
SS 7.1:Login Page



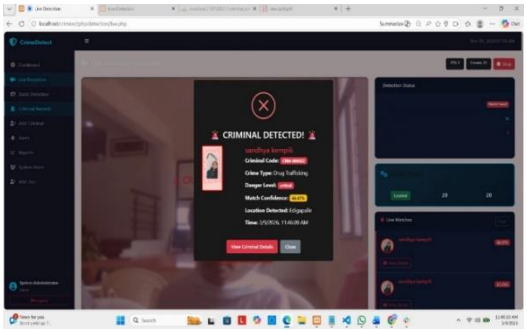
SS 7.2: Add User Dashboard Page



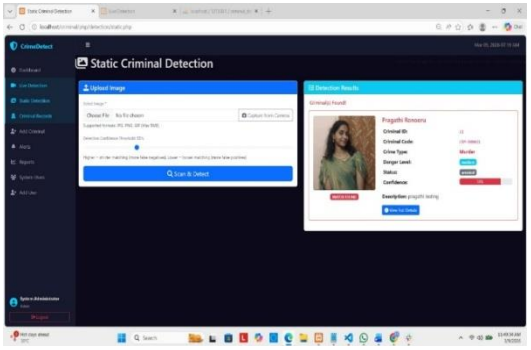
SS 7.3:System Users Page



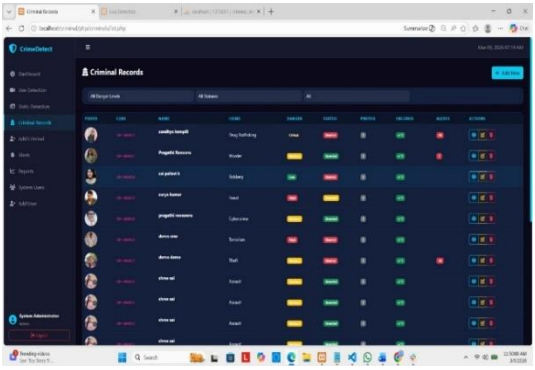
SS 7.4:Live criminal Detection Page



SS 7.5:Criminal Detected Page

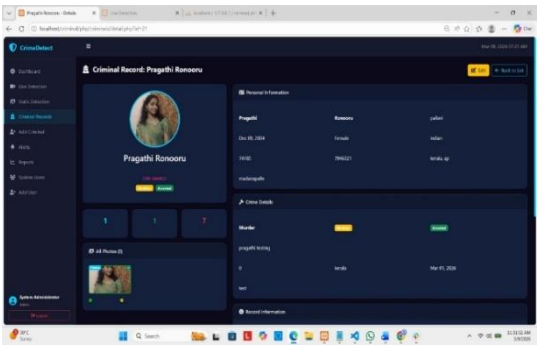


SS 7.6:Static Criminal Detection Page

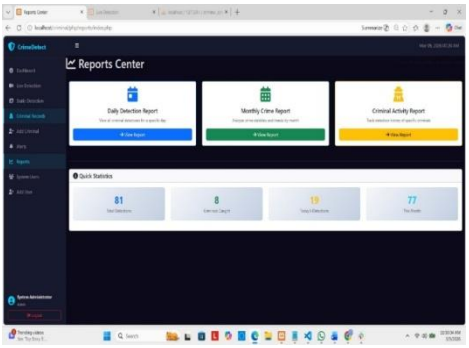


SS 7.7:Criminal Records

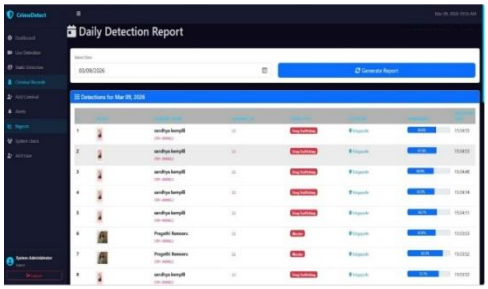
DOI: 10.22413/ijastems/2026/v12/i5/2



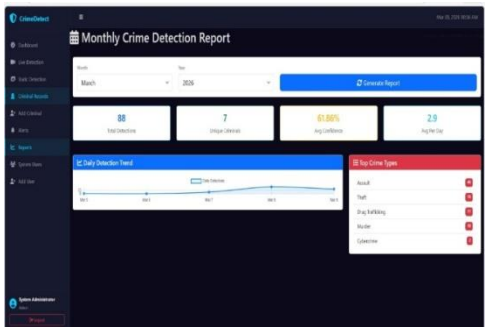
SS 7.8:Specific Criminal Record



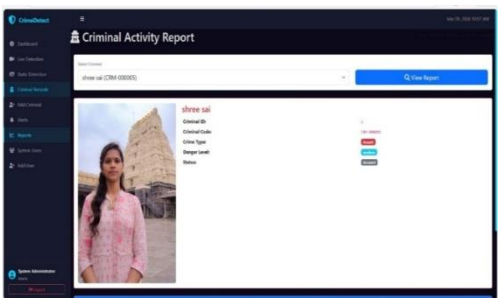
SS 7.9:Reports Dashboard



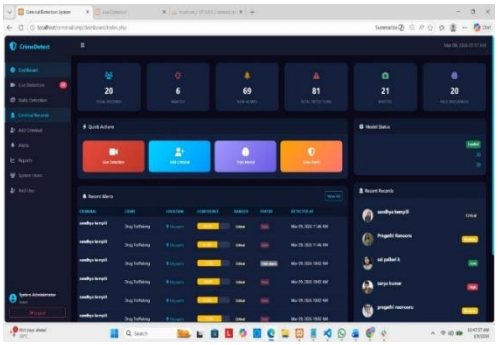
SS 7.10:Daily Reports



SS 7.11:Monthly Reports



SS 7.12:Criminal Activity Report



SS 7.12:Dashboard Page

VIII. APPLICATIONS

8.1 Public Safety and Crime Prevention

The system can be deployed in crowded public places such as airports, railway stations, shopping malls, and bus terminals to monitor activities continuously. By detecting and identifying criminals in real time, the system helps law enforcement authorities take immediate action and prevent potential threats. This improves overall security and reduces the chances of criminal activities in public areas.

8.2 Smart City Surveillance

The proposed system can be integrated into smart city infrastructure to enhance urban security. Smart cities rely on advanced technologies for efficient management of resources and safety. By incorporating facial recognition and real-time alert systems, the system can monitor large areas automatically and provide quick responses to suspicious activities. This contributes to the development of intelligent and secure urban environments.

8.3 Law Enforcement and Investigation

The system is highly useful for police departments and investigation agencies. It helps in identifying criminals by comparing real-time facial data with existing criminal databases. The system can also maintain logs of detected individuals, which can be used for further investigation and evidence collection. This reduces manual effort and speeds up the investigation process.

8.4 Access Control and Restricted Areas

The system can be used in restricted areas such as government offices, military zones, research laboratories, and corporate buildings. It ensures that only authorized individuals are allowed entry while detecting and alerting authorities about unauthorized persons. This improves security in sensitive areas and prevents unauthorized access.

8.5 Banking and Financial Institutions

Banks and financial institutions require high levels of security to prevent fraud and theft. The proposed system can be used to monitor suspicious individuals and identify known criminals entering the premises. Real-time alerts can help security personnel take immediate action, thereby

DOI: 10.22413/ijastems/2026/v12/i5/2

reducing risks and enhancing safety in financial environments..

8.6 Educational Institutions and Campus Security

The system can be implemented in schools, colleges, and universities to ensure campus safety. It can monitor entry points and detect unauthorized individuals, providing a secure environment for students and staff. The system can also help in tracking suspicious activities within the campus.

8.7 Transportation Systems

The proposed system can be used in transportation systems such as metro stations, bus stations, and airports to monitor passengers and detect criminals. Real-time identification and alert generation improve security and help authorities manage large crowds effectively.

REFERENCE

[1] S. Li and W. Deng, "Deep Facial Expression Recognition: A Survey," IEEE Transactions on Affective Computing, 2020.

[2] M. A. Turk and A. P. Pentland, "Face Recognition Using Eigenfaces," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 1991.

[3] P. Viola and M. Jones, "Rapid Object Detection using a Boosted Cascade of Simple Features," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2001.

[4] Singh, Laishram Hemanta, et al. "Advancements in Detecting Deepfakes: AI Algorithms and Future Prospects − a Review." Discover Internet of Things, vol. 5, no. 1, May 2025, p. 53.

[5] A.Krizhevsky, I. Sutskever, and G. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," Advances in Neural Information Processing Systems, 2012.

[6] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, 1978.

[7] G. Bradski, "The OpenCV Library," Dr. Dobb's Journal of Software Tools, 2000.

[8] P D. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints," International Journal of Computer Vision, 2004.

[9] Z. Zhang, "Microsoft Kinect Sensor and Its Effect," IEEE Multimedia, 2012.

[10] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2014.