

# NeuroSentinel: An Intelligent Computer Vision Framework for Real-Time Surveillance and Intruder Detection

Karunamurthy A.\* T. Thamizhselvan\*\*

\*Department of Computer Applications, Sri Manakula Vinayagar Engineering College (Autonomous), Puducherry 605008, India

\*\*Department of Computer Applications, Sri Manakula Vinayagar Engineering College (Autonomous), Puducherry 605008, India

Email: thamizh868@gmail.com

---

**Abstract**—Traditional surveillance is limited and relies heavily on manual monitoring. These limitations have been exposed by the growing demand for intelligent security systems. In this paper, we propose an intelligent computer vision framework for real-time surveillance and intruder detection called *NeuroSentinel*. The system utilises live video feeds, face detection, and facial recognition technologies to identify authorised and unauthorised individuals. If an intruder is detected, the framework automatically captures evidence and generates real-time alerts to improve security response. *NeuroSentinel* is an efficient, scalable, and cost-effective surveillance solution built using Python, OpenCV, Flask, and MySQL. The proposed system improves security monitoring accuracy, decreases human effort, and enables automated detection of threats across diverse real-world environments including educational institutions, offices, and residential areas.

**Keywords**—Computer Vision, Smart Surveillance, Face Recognition, Intruder Detection, Real-Time Monitoring, Security Intelligence.

---

## I. INTRODUCTION

The recent increase in urbanisation and security concerns has led to a growing demand for efficient surveillance solutions. Conventional surveillance depends heavily on continuous human monitoring, requiring operators to manually observe multiple camera feeds simultaneously. This process is labour-intensive and prone to errors, including delayed responses to security incidents.

Advances in computer vision and artificial intelligence now enable automated smart systems to analyse video in real time and respond whenever a threat is detected. Face detection and recognition techniques can effectively differentiate between authorised and unauthorised individuals within a monitored environment, significantly reducing the need for human involvement across educational institutions, office buildings, residential complexes, and similar facilities.

In this paper, a novel face recognition based intelligent surveillance solution named **NeuroSentinel** is presented. The proposed system applies computer vision algorithms to analyse real-time

video feeds, detect human faces, and classify each detected individual as either an authorised user or an intruder.

## II. LITERATURE SURVEY

The widespread deployment of surveillance cameras has driven extensive research in intelligent monitoring. Traditional surveillance methods that rely on manual supervision or simple video recording fail to satisfy modern security requirements. Conventional CCTV systems primarily serve as recording and manual observation tools and lack the capability for intelligent analysis and immediate threat identification. Several studies have documented the ineffectiveness of manual monitoring across large camera networks, where such systems cause significant delays in detecting and responding to security events.

Advances in computer vision have greatly contributed to intelligent surveillance through object detection, motion analysis, and face detection. Techniques such as the *Haar Cascade Classifier* are widely used for face detection due to their computational efficiency and real-time performance in extracting human faces from video frames for subsequent recognition and identification.

Facial recognition is a core technique in contemporary security systems, enabling comparison of detected faces against pre-stored databases of known individuals for authentication and filtering of unknown visitors. Existing recognition systems have found widespread adoption in institutional, office, and controlled-access environments where their role is focused on access control and personnel authentication.

More recent surveillance systems incorporate automated notification mechanisms to improve response time. Upon detecting an unrecognised individual, these systems can alert authorities via email or other communication channels, capture photographic evidence, and log the event. This enables a unified intelligent framework that integrates detection, recognition, storage, and notification to prevent security threats.

Based on the reviewed literature, the majority of existing systems either focus solely on video recording or implement only basic face detection, lacking automatic real-time intruder identification, evidence capture, and automated alert generation. The proposed *NeuroSentinel* aims to address these shortcomings by integrating real-time video surveillance with face detection, face recognition, database storage, and automated email alert generation.

### III. PROPOSED SYSTEM

NeuroSentinel is an intelligent computer vision framework developed for real-time surveillance and automated intruder detection. Unlike traditional surveillance systems that rely on continuous human monitoring, the proposed system automatically analyses live video streams, detects human faces, and identifies authorised and unauthorised individuals. The framework improves security by reducing manual effort and enabling rapid response to potential threats.

The system captures video through surveillance cameras and processes each frame using computer vision techniques. The face detection algorithm identifies human faces present in the video stream, while the facial recognition module compares detected faces with stored records in the database. If a match is found, the individual is recognised as an authorised user; otherwise, the person is classified as a potential intruder.

Upon detecting an unauthorised individual, NeuroSentinel automatically captures images as evidence, stores the event details in the database, and generates real-time email notifications to security personnel or administrators. This enables immediate awareness of security incidents and supports quick decision-making. The framework is implemented using Python, OpenCV, Flask, and MySQL, ensuring efficient processing and reliable system performance.

The proposed system offers several advantages: automated monitoring, accurate face recognition, real-time intruder detection, evidence collection, and instant alert generation. By integrating computer vision with intelligent security mechanisms, NeuroSentinel provides a scalable, cost-effective, and efficient surveillance solution suitable for educational institutions, offices, residential communities, and public security environments.

#### A. System Architecture

The general architecture of NeuroSentinel is presented in Fig. 1. The pipeline begins with the *Video Capture Module*, which acquires real-time video streams from CCTV cameras and webcams. Captured frames are forwarded to the *Face Detection Module*, which applies image pre-processing and Haar Cascade algorithms to localise faces within each frame.

Detected faces are then passed to the *Face Recognition Module*, which extracts facial features and compares them against registered entries in the face database to determine whether the individual is a known user or an intruder. Based on this result, the *Intruder Detection Module* classifies the person accordingly. If classified as unknown, the *Alert and Notification Module* captures the intruder's image, records the event, and dispatches real-time email notifications to the administrator.

All registered user details, face datasets, captured images, and event history are persisted by the *Database and Data Management Module*. Live monitoring, alert management, report generation, and administration are handled through the *Web Dashboard Module*. Camera configuration, user registration, and dataset maintenance are managed via the *System Management Module*. Together, these modules enable intelligent, automated surveillance with real-time face recognition and scalable intruder detection.

NeuroSentinel: An Intelligent Computer Vision Framework for Real-Time Surveillance and Intruder Detection

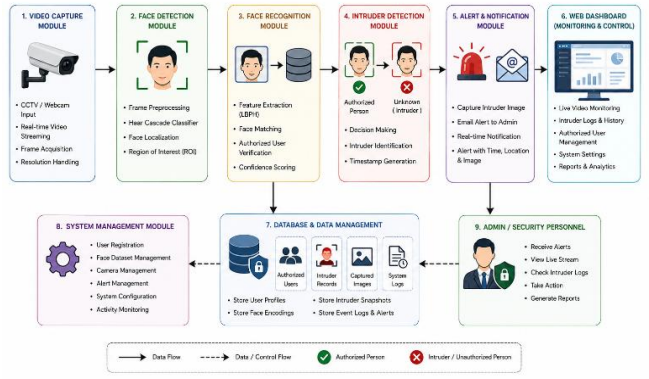


Figure 1: System Architecture of NeuroSentinel

#### B. Data Flow Diagram

Fig. 2 presents the Data Flow Diagram of the NeuroSentinel surveillance system. The process begins with live video input from a CCTV camera or webcam. Captured video frames are passed to the face detection module, which identifies human faces using computer vision techniques.

After detection, the face is forwarded to the face recognition module, which compares it against stored user records in the database. If the person is recognised, the system grants authorised access and logs the activity. If the person is unknown, the intruder detection module classifies the individual as an intruder, captures their image, stores the event details, and dispatches an email alert to the administrator. The web dashboard displays live video, alerts, logs, and stored records for ongoing monitoring and management.

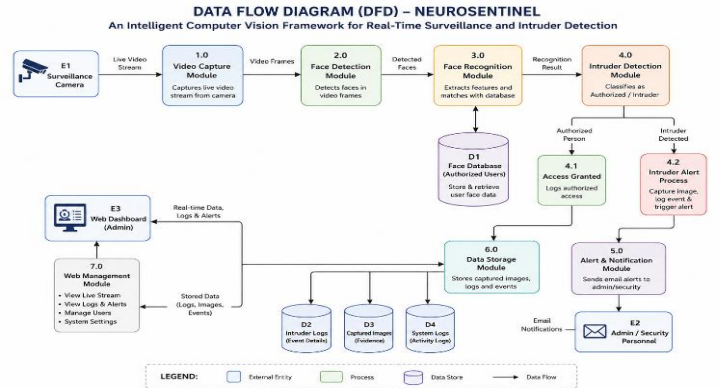


Figure 2: Data Flow Diagram of NeuroSentinel

### IV. COMPONENTS AND TECHNIQUES OF THE NEUROSENTINEL FRAMEWORK

Table 1 summarises the key components of the proposed framework along with the techniques that enable intelligent security monitoring. The framework integrates video capture, face detection, face recognition, intruder identification, alert generation, and secure data management to deliver an automated surveillance solution.

Table 1: COMPONENTS AND TECHNIQUES OF NEUROSENTINEL FRAMEWORK

Component	Description	Techniques Used	Purpose
<b>Video Capture Module</b>	Captures live video streams from CCTV cameras or webcams for surveillance monitoring	OpenCV Video Capture, Frame Acquisition	Real-time monitoring
<b>Face Detection Module</b>	Detects and localises human faces from captured video frames	Haar Cascade Classifier, Image Processing	Face localisation
<b>Face Recognition Module</b>	Compares detected faces with stored user records to verify identity	LBPH Face Recognition, Feature Extraction	Authorised user recognition
<b>Intruder Detection Module</b>	Identifies unknown or unauthorised individuals in the surveillance area	Face Matching, Classification Techniques	Threat and intruder detection
<b>Alert Module</b>	Generates alerts and sends notifications when an intruder is detected	SMTP Email Service, Event Trigger Mechanism	Real-time security alert generation
<b>Database &amp; Data Management Module</b>	Stores user profiles, face datasets, captured images, and event logs	MySQL Database, Data Storage Management	Data management
<b>Web Dashboard Module</b>	Provides an interface for live monitoring, alert management, and reporting	Flask Framework	System control
<b>Security Layer</b>	Protects system resources and controls authorised access to surveillance data	Authentication, Access Control	Data security

## VII. FRAMEWORK OPERATIONAL LEVELS

The NeuroSentinel framework operates across three progressive levels, each adding greater intelligence and automation to the surveillance process.

### D. Basic Surveillance Monitoring Level

The basic level focuses on real-time video monitoring and face detection within the surveillance environment. The system continuously captures video streams from cameras and processes each frame to identify human presence. This level forms the foundation of the surveillance framework by collecting visual information and detecting faces from live video feeds.

Key activities at this level include:

- Capturing live video streams from surveillance cameras.
- Detecting human faces from video frames.
- Performing continuous basic monitoring activities.
- Recording detected face data for further processing.

The primary objective is to perform real-time surveillance, detect human presence, collect visual data for security analysis, and establish the foundation for intelligent surveillance.

### E. Intelligent Recognition Level

At the intermediate level, the system performs face recognition and identity verification. Detected faces are compared with the stored database of authorised users. The system automatically differentiates between known and unknown individuals, improving security monitoring efficiency.

Characteristics of this level include:

- Extraction and analysis of facial features.
- Matching detected faces against stored records.
- Automatic identification of authorised and unauthorised users.
- Automated processing of recognition results.

This level delivers accurate identification of authorised individuals, reduced dependency on manual monitoring, faster identity verification, and improved overall surveillance effectiveness.

### F. Advanced Intruder Detection and Alert Level

The advanced level focuses on automated intrusion detection and security response. When an unknown individual is detected, the system captures evidence, stores event details, and generates real-time notifications for administrators.

During this phase:

- Unauthorised individuals are classified as intruders.
- Intruder images are captured automatically.
- Real-time email alerts are generated and dispatched.
- Security events are recorded in the database.

Key capabilities include automated intruder detection, real-time security alert generation, intelligent surveillance monitoring, secure storage of surveillance records, and enhanced security response and threat management.

## VIII. CONCLUSION AND FUTURE ENHANCEMENT

The proposed NeuroSentinel: An Intelligent Computer Vision Framework for Real-Time Surveillance and Intruder Detection successfully addresses the limitations of conventional surveillance systems by providing an intelligent and automated security monitoring solution. The framework combines real-time video monitoring, face detection, face recognition, intruder identification, and alert generation within a unified platform. By continuously analysing live video streams, the system accurately identifies authorised individuals and detects unauthorised access without requiring constant human supervision. The integration of automated notifications and secure data management further enhances the effectiveness of security operations.

The implementation demonstrates that computer vision technologies can significantly improve surveillance efficiency, reduce incident response time, and strengthen overall security management across diverse environments including educational institutions, offices, residential communities, and public spaces. Future enhancements of NeuroSentinel may focus on integrating advanced artificial intelligence and deep learning techniques to improve recognition accuracy and system intelligence. The framework can be extended to support multi-camera surveil-

lance, cloud-based monitoring, and remote access capabilities for large-scale security environments. Additional features such as real-time object detection, suspicious activity analysis, behavioural monitoring, and predictive threat assessment can further enhance the system's ability to identify potential security risks. These advancements will enable NeuroSentinel to evolve into a more intelligent, scalable, and autonomous surveillance framework capable of meeting future security requirements.

#### ACKNOWLEDGMENT

The authors would like to thank the Department of Computer Applications, Sri Manakula Vinayagar Engineering College (Autonomous), Puducherry, for providing the necessary resources and support to carry out this research.

#### REFERENCES

13. T. Sahoo, B. Mohanty, and B. K. Pattanayak, "Moving object detection using deep learning method," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 9s, pp. 282–290, 2024.
14. W. Liang, X. Xu, and X. Fu, "VioNets: efficient multi-modal fusion method based on bidirectional gate recurrent unit and cross-attention graph convolutional network for video violence detection," *J. Electron. Imaging*, vol. 32, no. 2, pp. 023031, 2023.
15. N. Jain, V. Gupta, U. Tariq, and D. J. Hemanth, "Fast violence recognition in video surveillance by integrating object detection and Conv-LSTM," *Int. J. Artif. Intell. Tools*, vol. 32, no. 3, pp. 2340018, 2023.
16. B. Sauvalle and A. de la Fortelle, "Autoencoder-based background reconstruction and foreground segmentation with background noise estimation," in *Proc. IEEE/CVF Winter Conf. Appl. Comput. Vis. (WACV)*, Jan. 2023, pp. 3243–3254.
17. B. N. Subudhi, M. K. Panda, T. Veerakumar, V. Jakhetiya, and S. Esakkirajan, "Kernel-induced possibilistic fuzzy associate background subtraction for video scene," *IEEE Trans. Comput. Social Syst.*, vol. 10, no. 3, pp. 1–12, Jan. 2022.
18. M. K. Panda, B. N. Subudhi, T. Bouwmans, V. Jakhetiya, and T. Veerakumar, "An end to end encoder–decoder network with multi-scale feature pulling for detecting local changes from video scene," in *Proc. 18th IEEE Int. Conf. Adv. Video Signal Based Surveill. (AVSS)*, Nov. 2022, pp. 1–8.
19. P. K. Sahoo, P. Kanungo, S. Mishra, and B. P. Mohanty, "Entropy feature and peak-means clustering based slowly moving object detection in head and shoulder video sequences," *J. King Saud Univ.—Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5296–5304, Sep. 2022.
20. L. Fan, T. Zhang, and W. Du, "Optical-flow-based framework to boost video object detection performance with object enhancement," *Expert Syst. Appl.*, vol. 170, May 2021.
21. Q. Zhang, T. Xiao, N. Huang, D. Zhang, and J. Han, "Revisiting feature fusion for RGB-T salient object detection," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 31, no. 5, pp. 1804–1818, May 2021.
22. M. Mandal, L. K. Kumar, M. S. Saran, and S. K. Vipparthi, "MotionRec: A unified deep framework for moving object recognition," in *Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV)*, Mar. 2020, pp. 2723–2732.
23. F. U. M. Ullah, A. Ullah, K. Muhammad, I. U. Haq, and S. W. Baik, "Violence detection using spatiotemporal features with 3D convolutional neural network," *Sensors (Basel)*, vol. 19, no. 11, pp. 2472, May 2019.
24. A.-M. R. Abdali and R. F. Al-Tuma, "Robust real-time violence detection in video using CNN and LSTM," in *Proc. 2nd Sci. Conf. Comput. Sci. (SCCS)*, 2019, pp. 104–108.