ijamrsd.com
ISSN: 2583-6404
Journal of Advanced Multidisciplinary Research Studies and Development
Peer Reviewed Referred Journal
Bi-monthly
Open Access

AI-POWERED MILITARY BORDER SURVEILLANCE SYSTEM USING FACE RECOGNITION AND MILITARY VEHICLE DETECTION

Dhanashree Kamble[1], Harshal Mhaske[2], Hemarshi Mahale[3]
[1,2,3] Dept. of Computer Science, Sharadchandra Pawar College of Engineering, India.
Email: dhanashreekamble847@gmail.com[1], harshalmhaske101@gmail.com[2], hemarshimahale@email.com[3]

Abstract
National defense needs to protect the country's borders. To do this safely, they need to monitor the borders 24/7 for any type of unauthorized intrusion or suspicious activity. Traditional methods of surveillance rely on people actively watching for suspicious activity, which makes them susceptible to fatigue and other errors due to the limitations of a human observer. We are proposing a method to implement an AI-based border security surveillance system utilizing both facial recognition and military vehicle detection, both of which are two-dimensional artificial intelligence (AI) to increase security and automation. The facial recognition module will provide user authorization through Haar Cascade face detection combined with Local Binary Pattern Histogram (LBPH) face identification. The module that detects the vehicle will utilize the YOLOv8 deep learning model to identify and classify military vehicles in real-time. Pre-processed video streams from all of the above for each surveillance camera will be captured and then all images will be pre-processed, etc., in order to identify items of interest. There will also be real-time alerts to law enforcement personnel of time-stamped images and the coordinates of where the item of interest was detected. The experimental results of the implementation of this AI-based border surveillance system demonstrated how easy it was to accurately detect suspects and how all systems are able to perform efficiently in real-time. There is a noticeable difference in monitoring efficiency as well as the number of human hours that the AI-based system saves and its impact on the speed with which law enforcement responds to border security operations..
Keywords: Border Surveillance, Artificial Intelligence, Face Recognition, YOLOv8, Military Vehicle Detection, Computer Vision, Deep Learning, Security Monitoring.

► *Corresponding Author: Dhanashree Kamble*

Introduction

The aspect of border security is essential to overall national defense because both unauthorized entrance through borders into a country and smuggling, as well as infiltrating into a nation's territory do represent serious dangers to the security of that country. Traditional systems of surveillance use primarily manual processes relying on personnel to monitor security through cameras, and by doing security patrols. The issues with traditional systems of surveillance are that humans get fatigued while monitoring, that delayed responses occur and that large border areas cannot all be covered by monitoring efforts, thus impacting the overall effectiveness of security efforts [1], [2].

The introduction of Artificial Intelligence (AI) and computer vision has made it possible to design intelligent systems of surveillance that allow for automated monitoring of the border and

identification of threats. Through AI-based video analysis systems, the processing of significant quantities of video footage can be conducted almost instantly along with identifying suspicious actions being taken without the benefit of and the need for continuous oversight of a person(s). The use of intelligent surveillance systems described herein have resulted in increasing the overall effectiveness, and reliability, of the systems currently in place for security and defense [3], [4], [5].

Face recognition is a frequently utilized technology in surveillance. Face Recognition is the way a system identifies an individual based upon the attributes of that individual's face. Face detection techniques, such as Viola-Jones Algorithms (which use Haar-like features and Use Cascade Classifiers), have been able to detect faces quickly and accurately from video streams, in real time [6][7]. Recognition algorithms, such as Local Binary Pattern histograms (LBPH), can then compare an individual's facial attributes to templates the system has stored in a database for the purposes of authentication and identification [8][9].

In addition to identifying individuals, vehicles must also be monitored while they are traveling in close proximity to the border in order to maintain safety. If a vehicle is detected operating in close proximity to a border that is unauthorized, that vehicle could potentially be involved in illegal activity or could potentially be a threat. Deep learning-based object detection techniques are proving to be very beneficial in terms of identifying & classifying objects that exist within complex environments and can therefore be successfully utilized as part of a surveillance system.[10][11][12]

Among the many different deep learning frameworks available, the YOLO framework is one of the most notable due to its real-time detection and ability to detect multiple objects using only one pass through a neural network. YOLO-based models can process video data in real-time because they can detect multiple objects in a single image with only one evaluation of the neural network. YOLO's latest versions (the YOLOv8 series) have demonstrated increased accuracy, increased inference speed, and overall improved performance in handling complex situations [13], [14], [15].

There has been considerable research on the application of artificial intelligence (AI) technologies to create intelligent surveillance systems to detect anomalies. These AI-based systems utilize computer vision techniques along with machine learning algorithms to automate the detection of suspicious activity, identity of an unauthorized person, or the identification of abnormal behavior in surveillance footage. The implementation of intelligent surveillance systems reduces the amount of manual effort required to monitor locations for security breaches and helps minimize response times during security events by improving response to security incidents [16], [17], [18].

Additionally, the combination of edge computing and smart sensors enables AI algorithms to handle video data on local devices, decreasing network latency for quicker threat detection. In real-time environments, edge-based surveillance systems can improve privacy and decrease bandwidth consumption while providing accurate threat detection rates [19], [20], [21].

This paper presents an AI-based military border surveillance system that combines face recognition and military vehicle identification to provide intelligent border monitoring. The proposed solution applies Haar Cascade and LBPH for identifying and recognizing personnel’s faces and YOLOv8 for identifying military vehicles using surveillance footage. The proposed system will provide real-time processing of video streams/detect potential threats from the streaming video, estimate the distances of identified objects, and generate alerts to support security resources with timely decisions based on detected threats. The goal of this system is to automate surveillance operations to improve accuracy, reduce human effort, and create comprehensive border security effectiveness [22], [23], [24].

Literature Review

The application of artificial intelligence and computer vision to security and surveillance systems has been studied extensively. Early research on detecting objects concluded with the development of an algorithm for detecting faces called Viola and Jones' Viola–Jones Face detection created with Haar-like features and Cascade classifiers. The implementation of the algorithm has produced real-time face detection which is used as a basis for many computer vision applications [1], [2]. The algorithm detects faces by utilizes sliding windows and boosted (trained) classifiers such that the detection occurs in real-time [3].

Since that time many researchers have enhanced the performance of the Viola–Jones algorithm by changing various aspects to how the features are extracted or optimised. These studies indicate that while the algorithm has a reliable speed of detection, it also has the potential of being inaccurate under low-light or non-frontal face conditions [4], [5]. Nevertheless, due to being computationally efficient the algorithm is still widely used for embedded and low-power security and surveillance systems [6].

There has been a significant amount of work done on using face recognition systems for authentication, surveillance and other applications. Local Binary Pattern Histogram (LBPH) is commonly used to recognize faces based on texture patterns. It has been shown that LBPH works well in real-time recognition situations and is also effective in low-resource computation environments [7], [8]. Recognition accuracy has been found to be affected by image pose variation or occlusion [9].

Over the past few years, the use of deep learning has greatly improved the performance of both facial recognition and object detection systems. Convolutional Neural Networks (CNNs) are used to learn complex visual patterns and allow for higher accuracy in recognition than previously established methods [10], [11]. CNN-based facial recognition systems have been used in many security applications, such as biometric authentication, surveillance monitoring, and automated border control [12].

Object detection has changed a lot since modern deep learning models began to be used. Joseph Redmon's You Only Look Once (YOLO) is a single-phase object detection architecture that is able to predict both bounding boxes and class probabilities (given an input image). YOLO was a radical improvement in object detection speed with little impact on overall detection accuracy, making it ideal for real-time object recognition applications [13].

Subsequent versions of YOLO (YOLOv3, YOLOv5, and YOLOv8) have continued to push the state of the art in terms of detection accuracy and speed. YOLOs can successfully identify multiple objects in complex environments, such as in modern surveillance systems, automated vehicles and security monitoring [14, 15]. YOLOs are typically best suited for detecting vehicles, people and other objects within continuously changing video inputs [16].

Researchers are investigating the potential use of AI in border security systems. Intelligent surveillance uses cameras, sensors, and AI algorithms for automatic monitoring of dangerous or restricted areas, as well as for the automatic detection of suspicious activity within those areas [17]. By having reliable and accurate, continuous monitoring capabilities, these systems have less reliance on hand-monitoring and provide a far greater level of operational efficiency [18].

Some research has proposed AI-based border monitoring systems that use computer vision techniques to identify intruders and/or suspicious vehicles. By evaluating the video feeds from the monitoring cameras, these systems can generate alerts when an unusual level of activity is detected [19]. By integrating object detection algorithms along with the video/image feed, the real time detection of vehicles or people becomes much more accurate and reliable [20].

Recent studies have explored multi-sensor surveillance systems, which combine cameras, drones, and edge computation devices. Systems such as these allow for faster processing of surveillance data and improved response times in cases of security incidents or breaches within a facility [21]. Edge-based processing decreases the utilization of network bandwidth and enables real-time decision making in remote border regions [22].

Another avenue of investigation in the realm of surveillance video is that of anomaly detection. Machine learning techniques have been implemented to detect unusual activities or movements within the video footage, thus providing authorities with potential threats to monitor prior to their escalation [23]. Such anomaly detection systems assess video footage through the analysis of motion and visual characteristics to automatically identify suspicious behaviours [24].

Research has also been conducted on the use of deep learning models for vehicle detection and classification. Such models employ convolutional neural networks to both detect and classify various types of vehicles at high levels of accuracy [25]. Vehicle detection systems have been used extensively in traffic monitoring systems, intelligent transportation systems, and border surveillance applications [26].

Recent research indicates that there is a growing need for the development of privacy preserving surveillance systems that can offer protection from the security risks often associated with the use of biometric data, while still providing a valid level of security through the use of facial recognition systems. Methods to help provide privacy to individuals being monitored by facial recognition systems include the use of encrypted storage of features, and secure transmission of data collected using these systems [27].

The area of low-resolution/facial recognition (of faces captured from low-quality/surveillance cameras) has generated a lot of recent research interest. Methods such as super-resolution techniques (to enhance resolution and enable facial recognition from low-resolution images) and deep-learning-based features (to improve face recognition accuracy) have been developed by researchers to facilitate face recognition [28].

Multiple surveys of the development and implementation of object detection systems using YOLO technology have indicated that YOLO-based systems are advantageous in terms of speed and the ability to detect discrete objects from video in real time. They also provide compelling evidence that YOLO-based systems are well suited for use in surveillance and monitoring capabilities, [29].

AI-enabled border surveillance systems that combine facial recognition and vehicle detection provide improved monitoring accuracy and response time by automatically detecting suspicious persons/vehicles, capturing imaging evidence, and notifying security personnel, making them effective solutions for the protection of borders [30].

Proposed System Architecture

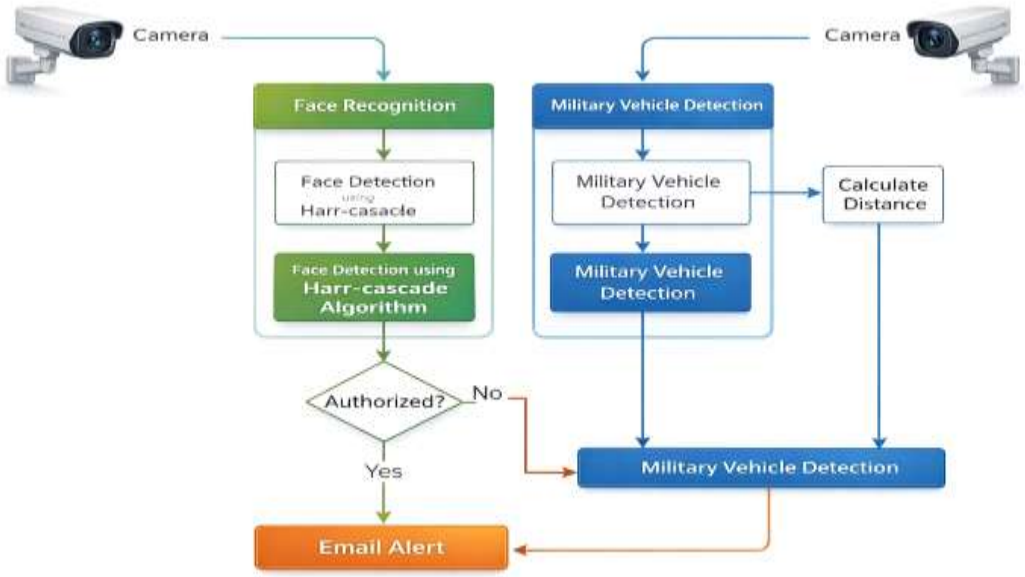

Fig. 1. System Architecture

1. Camera (Collecting Data)

There are cameras located within an area of the border that constantly capture and stream video of the surrounding area. These cameras are the system's primary source of input. The frames produced by the video capture will contain an image of the individuals or vehicles that are approaching the monitored area. These video data are then sent to processing modules for further processing and analysis.

2. Face Recognition Module

The face recognition module processes video frames to detect and recognize human faces in a video frame. If a detected face meets an authorization requirement of being part of either Military, the face recognition module provides a positive identification of authority and therefore assists the overall security of the border region by automatically identifying unknown or suspicious individuals. Since the face recognition module automatically identifies both known and unknown faces, the need for continuous physical monitoring of the face recognition module's output by security personnel is reduced.

3. Face Detection Using Haar Cascade Algorithm

In this phase, the system will apply the Haar Cascade algorithm to the images created by the video capture to detect human faces. The Haar Cascade algorithm uses trained classifiers to identify and extract the face features of human beings including eyes, nose and mouth from the images. The Haar Cascade algorithm is also equipped to quickly process and detect faces in real-time within a video frame. Once detected, those faces will proceed to the authorization verification phase for further processing.

4. Authorization Validation

The system compares the detected facial features of a face with the authorized personnel database after identifying a face. If the detected face matches the database, the person will be considered an authorized user. If there is no match between the face and The database, the person will be

classified as unauthorized. This will help to prevent unauthorized access to restricted areas of the border.

5. Military Vehicle Detection Module

The purpose of this module is to detect vehicles in the surveillance camera images from multiple locations. A modern object detection model such as YOLOv8 is used to identify and classify military vehicles. The system will analyze each of the images captured in order to locate all military vehicles in the images and plot bounding boxes around them. This Process will allow for continued observation of vehicle movements near the border.

6. Distance Measurement

The system will calculate the distance from the vehicle to the surveillance camera once it has located a vehicle. The ability to estimate the distance will allow security teams to assess how close the vehicle is positioned from the restricted area of the border. This measurement will assist teams in responding quickly to suspicious movement in and around the restricted area on the border.

7. Alert System via Email

Whenever the security camera system detects unauthorized persons and suspicious vehicles, an alert is automatically transmitted. An Image of the detected Event is stored in the security camera system and an e-mail notification is sent to the appropriate security personnel. The e-mail alert will include all pertinent information concerning the detected Event including; captured image(s), date/time of detection, and Event detection information, providing appropriate security personnel with the necessary information required for timely response to any potential security threat.

Methodology

The AI-Powered Military Border Surveillance System would automatically monitor the border region and identify suspicious behavior by utilizing computer vision and deep learning techniques. The methodology can be broken up into several stages, including data acquisition, image preprocessing, facial detection and recognition, vehicle detection, distance estimation, and alert generation. All of these different steps will work in conjunction to allow the system to analyze surveillance footage in order to identify possible security threats in real-time.

1. Data Acquisition

The first step of the system is collecting real-time video data through the use of the various surveillance cameras that are located throughout the border area. These cameras will continuously provide a video stream of individuals as well as vehicles that are either travelling towards or within the monitored region. To facilitate the analysis of each of the video streams, they will be converted to individual frames using regular time intervals. This will allow the system to continuously monitor border activity every minute of every day without interruption.

2. Image Pre-processing

Capturing images requires pre-processing of the images to improve image quality and/or improve accuracy of detection before processing the image. The first step of this pre-processing stage involves resizing to have a consistent fixed resolution for all images to allow processing the images using the same dimensional format. The second step involves applying noise reduction methods to eliminate unwanted distortions from the digital image. Thirdly, converting from RGB (Red, Green, Blue) images to grayscale images through a color conversion method is often necessary because most detection algorithms work more effectively when working with grayscale images. Finally, normalizing the intensity values of the pixel values in the digital image through image normalization methods enhances the ability to extract features.

3. Detecting Faces

Face detection occurs after completing the pre-processing steps and will use Haar Cascade algorithms to detect faces. The Haar Cascade algorithm uses machine learning techniques to identify human faces within an image using Haar-like feature detection. The Haar Cascade will search the image for specific parts of a face by applying sliding window detection on various sub-areas of the detected object location and detecting the existence of parts of the identified object (the part of the face); for example, the eyes, nose, and mouth. The Haar Cascade algorithm uses a cascade classifier to eliminate non-face region detections and only detect the regions of an image that are mesh likely to be human faces. This detection process allows the detection of a human face in real-time from the video frames being processed.

4. Face Recognition Principal Summary

Subsequent to detecting a human face, facial recognition for identifying the detected human individual commences. The means utilized for performing the facial recognition procedure is the Local Binary Pattern Histogram (LBPH) method; LBPH obtains facial texture information from the input face and converts this texture information into numeric feature vectors. These obtained feature vectors are compared to known stored facial database entries for all authorized military personnel. If a match is made, the individual recognized by the facial recognition system will be determined to be authorized personnel (no further action is taken against authorized personnel). If no match entry is located, the recognized individual will be determined as an unauthorized individual, alerting personnel to generate an alert.

5. Military Vehicle Detection Principal Summary

Beyond detecting human individuals, the proposed facial recognition system will detect military vehicle movement (vehicle detection) that occurs along the borders. The YOLOv8 deep learning (artificial intelligence) object detection method will detect military vehicle presence within the surveillance camera images. YOLO (You Only Look Once) is an algorithm that uses a real-time method by detecting and classifying an identified object by making one pass of the full detection image through the assigned neural network. Following the detection phase of the identified object, the algorithm will create a bounding box around the detected object, and label the detected object as belonging to the respective object type. Through the use of a trained algorithm from various identified military vehicle datasets, the YOLO object detection algorithm will identify and classify all identified military vehicle movement captured by a camera view.

6. Distance Estimation

When the system detects a vehicle, it also determines how far away that vehicle is from the surveillance camera. This is done by looking at how big the detected object appears on the screen and comparing it to objects with known dimensions (known reference dimensions). Knowing how far away a vehicle is from the restricted border area allows security personnel to evaluate the seriousness of any potential threats and take appropriate action.

7. Alert Generation System

If the system detects an unauthorized individual or suspicious military vehicles, it automatically generates an alert notification. In addition to generating the alert notification, the system will store a relevant image frame and details regarding the detection (detection type and time) in the database. The alert system will then send an email or be made available via a monitoring dashboard notifying security personnel of the situation. The notification will include the captured image along with detection information to enable security teams to respond quickly to the situation.

8. Recording Events

Recording events of an automated monitoring system will enable security personnel to view the results of the monitoring activity. The system produces the captured images and outputs the detection results and alerts to officials who can then review the surveillance activity, both in real time and historically, on a centralized monitoring interface. By providing a method for authorities to monitor their borders, the automated monitoring system has enhanced the effectiveness of border patrols while also decreasing the reliance on human monitoring forces and providing quicker detection and response to potential threats.

Result

The AI Military Border Surveillance System will use the web-based interface for integration with computer vision modules, specifically for facial recognition and military vehicle detection. Evaluation criteria will include usability, real-time detection and alerting capability. The interactive dashboard of the system allows users to operate the surveillance features and to view security alerts. The face recognition module will detect and verify authorized personnel, while any unauthorized persons will produce an automatic alert. The vehicle detection module will detect military vehicles and allow the system to calculate the distance of the vehicle from the camera.
Experimental results indicate the system operates in a real-time environment and that the detection modules work in parallel to create prompt alerts when suspicious activity is detected; thus, improving the efficiency of monitoring and freeing personnel to conduct their own surveillance.

Fig. 1: Military Surveillance System Home Page

This is the main home page of the RakshaVision platform; it describes how RakshaVision uses AI to provide real-time face recognition and military vehicle detection services. Users will find action buttons on the home page to help them learn about the features and functions of the system. These include: `Get Started` and `Learn More`.

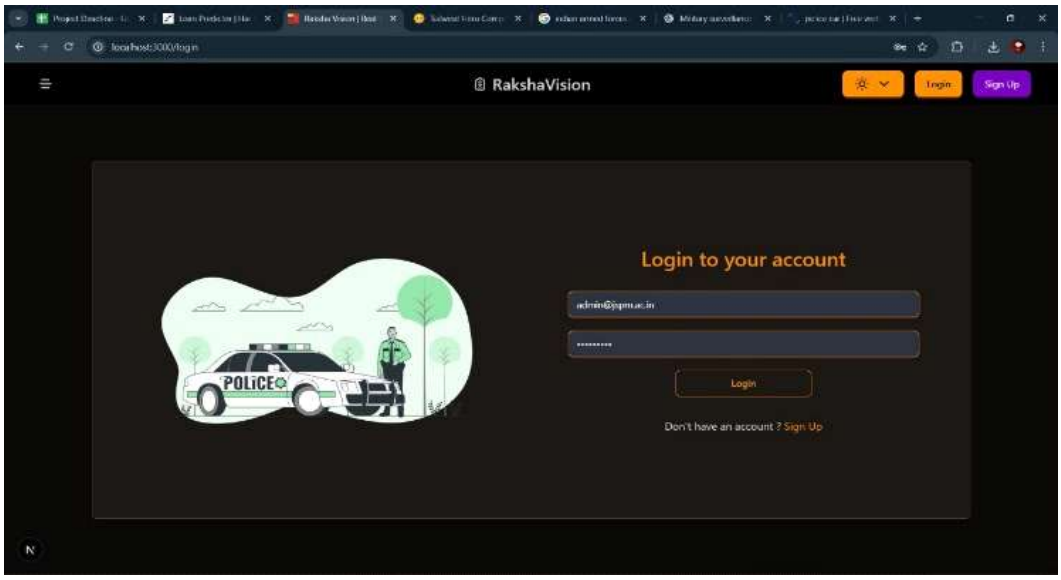

Fig 2: System Login Interface

The login interface of the RakshaVision surveillance system is shown above. Users who have been granted permission can log into the RakshaVision system by entering their email and password credentials. The login page of RakshaVision only permits authenticated users to access the system and monitoring dashboard. There is also a signup feature for new users to create an account.

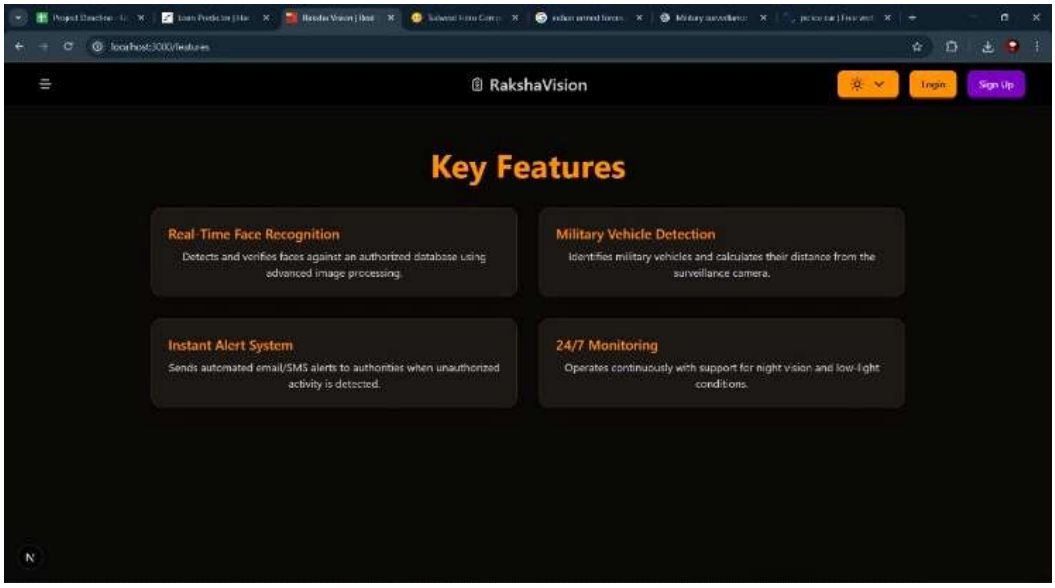

Fig 3: Secure User Authentication Page

This illustration depicts an authentication page for authorized users accessing the RakshaVision system by entering their credentials. The authentication page has a dark interface that makes it easy for a user to see what they are doing. The authentication method is implemented to enhance security and prevent unauthorized access to sensitive surveillance data.

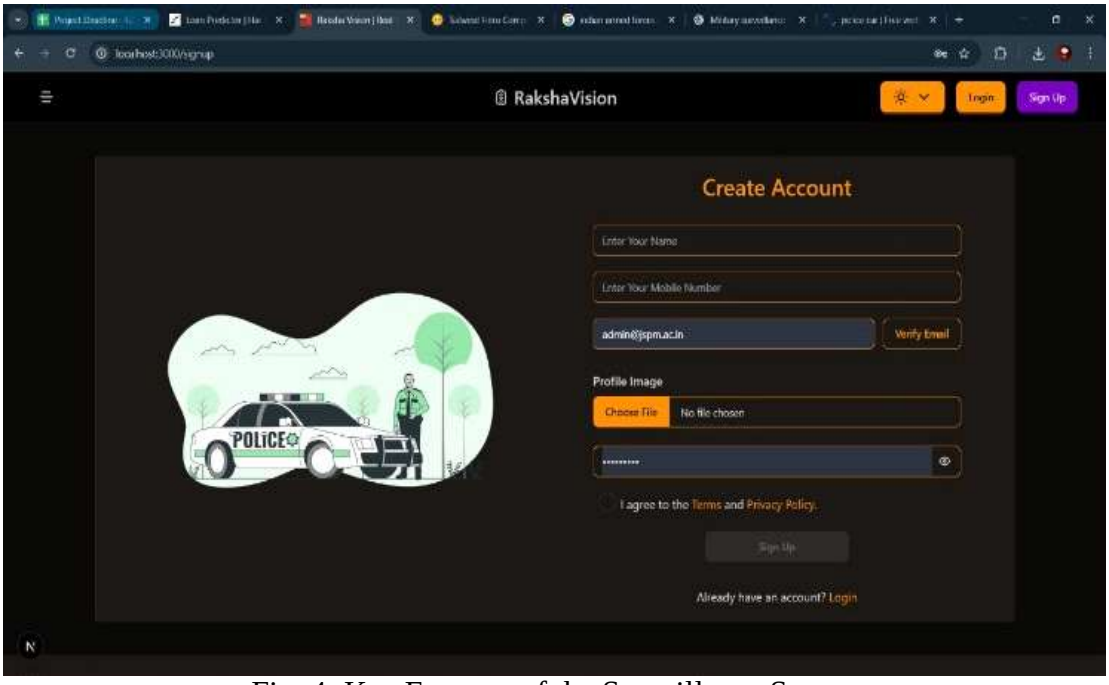

Fig. 4: Key Features of the Surveillance System

Features of the RakshaVision Surveillance System are illustrated in this figure. The automatic detection of individuals in real-time, military vehicle detection in real-time, an instant alert system, and continuous monitoring all enhance security operations by providing automated detection of threats and real-time monitoring of those threats.

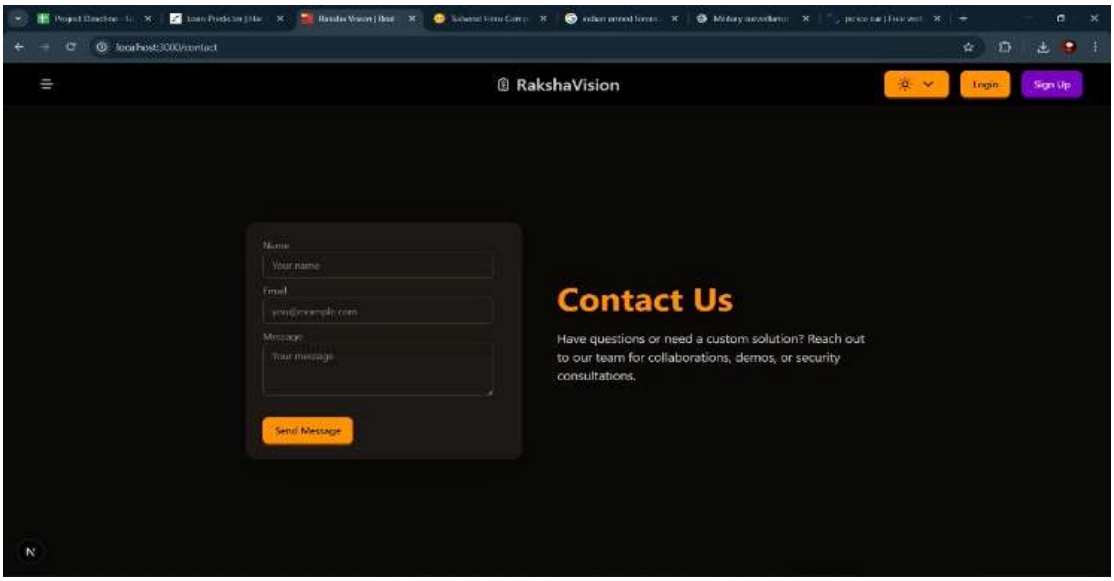

Fig. 5: Contact Interface

This figure illustrates the contact feature of the surveillance system's platform. This buffer allows users to communicate with system administrators and developers via a contact form that allows users to submit their name, email address and message. This creates an opportunity for support enquiries, feedback about the system and requests to collaborate.

Conclusion

This research presents an "AI-Enhanced Military Border Security and Monitoring System" as a new solution for strengthening border guard security by improving the border monitoring process and automating the early detection of threats. The system combines facial recognition technology with military vehicle identification via computer vision and deep learning algorithms. The face recognition component can identify both authorized individuals and unauthorized individuals; and the military vehicle detection component can identify military-type vehicles and compute how far away from the camera they are. The developed system allows users to access secure monitoring functionality over a web-based interface where they can view and monitor the system's activity. Experimental testing indicates that the proposed system can detect events in real-time and generate alerts to improve efficiency in monitoring while decreasing the reliance of human beings to perform these security and monitoring tasks. And, based upon what has already been described, this proposed program has the potential to be a reliable and effective solution to enhancing intelligent border/personnel monitoring activity, improving the ability of security personnel to respond to potential threats, and, in total, strengthening our border security and surveillance infrastructure through the combined application of artificial intelligence and automated alerting systems.

References

1. S. Khatal, D. A. Kamble, H. V. Mhaske, H. M. Mahale, and M. D. Rokade, *"AI-Powered Military Border Surveillance System Using Face Recognition and Military Vehicle Detection,"* International Journal of Innovative Research in Technology (IJIRT), vol. 12, no. 6, 2025.
2. P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, 2001, pp. 511–518.
3. T. Ahonen, A. Hadid, and M. Pietikäinen, "Face recognition with local binary patterns," *European Conf. Computer Vision (ECCV)*, 2004, pp. 469–481.
4. J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You Only Look Once: Unified, real-time object detection," *Proc. IEEE CVPR*, 2016.
5. J. Redmon and A. Farhadi, "YOLO9000: Better, faster, stronger," *Proc. IEEE CVPR*, 2017.
6. J. Redmon and A. Farhadi, "YOLOv3: An incremental improvement," *arXiv preprint arXiv:1804.02767*, 2018.
7. G. Jocher et al., "YOLOv5 by Ultralytics," *GitHub Repository*, 2020.
8. G. Wang et al., "YOLOv8: A state-of-the-art object detection model," *Ultralytics AI Documentation*, 2023.
9. S. Z. Li and A. K. Jain, *Handbook of Face Recognition*, Springer, 2011.
10. A. Krizhevsky, I. Sutskever, and G. Hinton, "ImageNet classification with deep convolutional neural networks," *Advances in Neural Information Processing Systems*, 2012.
11. R. Girshick, "Fast R-CNN," *Proc. IEEE Int. Conf. Computer Vision (ICCV)*, 2015.
12. S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards real-time object detection with region proposal networks," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 39, no. 6, pp. 1137–1149, 2017.
13. N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," *Proc. IEEE CVPR*, 2005.
14. M. A. Turk and A. P. Pentland, "Eigenfaces for recognition," *Journal of Cognitive Neuroscience*, vol. 3, no. 1, pp. 71–86, 1991.

15. K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *arXiv preprint arXiv:1409.1556*, 2014.
16. Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, pp. 436–444, 2015.
17. M. Everingham et al., "The Pascal visual object classes challenge: A retrospective," *International Journal of Computer Vision*, 2015.
18. H. Choi, M. Kim, and K. Park, "Visitor authentication using face recognition in CCTV surveillance systems," *Sensors*, vol. 22, no. 9, 2022.
19. Y. Ouyang, L. Chen, W. Zhang, and H. Liu, "Military vehicle detection based on hierarchical feature representation," *IEEE Access*, vol. 10, pp. 102341–102352, 2022.
20. X. Wang, Y. Li, H. Chen, and K. Zhang, "Privacy-preserving edge computation-based face verification," *IEEE Internet of Things Journal*, 2019.
21. S. Chen, F. Liu, G. Wang, and H. Yang, "Steganographic secret sharing with GAN-based face synthesis," *IEEE Access*, vol. 9, 2021.
22. Y. Wang, X. Li, S. Chen, and M. Zhou, "Robust facial authentication for low-power edge AI devices," *IEEE Transactions on Artificial Intelligence*, 2022.
23. T. Lee, Y. Choi, and H. Kim, "Reinforcing deep learning-enabled surveillance with smart sensors," *Sensors*, vol. 25, no. 11, 2025.
24. S. Soltani-Nejad and A. Haque, "Weakly supervised anomaly detection in surveillance videos," *IEEE Trans. Pattern Analysis and Machine Intelligence*, 2024.
25. Y. Liu et al., "Generalized video anomaly event detection: A survey," *ACM Computing Surveys*, 2023.
26. J. Singh and R. Ramachandra, "Reliable face morphing attack detection in border control systems," *IEEE Transactions on Information Forensics and Security*, 2022.
27. A. Sardar, P. Kumar, and R. Sharma, "Enhanced biometric template protection schemes in IoT," *IEEE Internet of Things Journal*, 2024.
28. H. Hunkeler, H. L. Truong, and A. Stanford-Clark, "MQTT-S—A publish/subscribe protocol for wireless sensor networks," *Proc. IEEE Int. Conf. Mobile Ubiquitous Systems*, 2008.
29. A. Banerjee, S. Roy, and P. Mukhopadhyay, "3D face authentication software test automation," *IEEE Access*, 2020.
30. M. Elhoseny et al., "Advanced deep learning techniques for surveillance systems," *Future Generation Computer Systems*, vol. 113, pp. 326–336, 2020.
31. S. Khanam et al., "Anomaly recognition in surveillance systems using deep learning," *IEEE Access*, vol. 13, 2025.