SUSPICIOUS ACTIVITY DETECTION

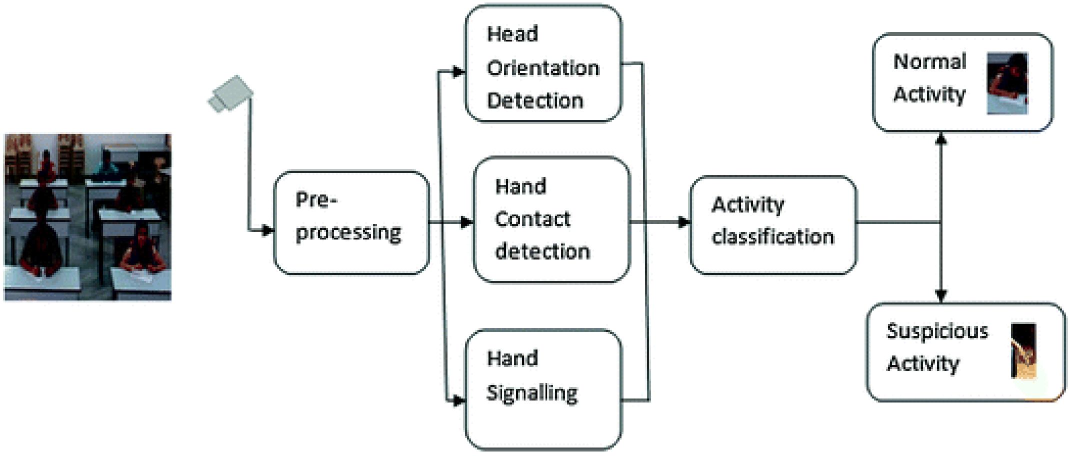
Literature Survey

Introduction:

Suspicious human activity recognition from surveillance video is an active research area of image processing and computer vision. Through the visual surveillance, human activities can be monitored in sensitive and public areas such as bus stations, railway stations, airports, banks, shopping malls, school and colleges, parking lots, roads, etc. to prevent terrorism, theft, accidents and illegal parking, vandalism, fighting, chain snatching, crime and other suspicious activities. It is very difficult to watch public places continuously, therefore an intelligent video surveillance is required that can monitor the human activities in real-time and categorize them as usual and unusual activities; and can generate an alert. Recent decade witnessed a good number of publications in the field of visual surveillance to recognize the abnormal activities. Furthermore, a few surveys can be seen in the literature for the different abnormal activities recognition; but none of them have addressed different abnormal activities in a review. In this paper, we present the state-of-the-art which demonstrates the overall progress of suspicious activity recognition from the surveillance videos in the last decade. We include a brief introduction of the suspicious human activity recognition with its issues and challenges.

This paper consists of six abnormal activities such as abandoned object detection, theft detection, fall detection, accidents and illegal parking detection on road, violence activity detection, and fire detection. In general, we have discussed all the steps those have been followed to recognize the human activity from the surveillance videos in the literature; such as foreground object extraction, object detection based on tracking or non-tracking methods, feature extraction, classification; activity analysis and recognition.

The objective of this paper is to provide the literature review of six different suspicious activity recognition systems with its general framework to the researchers of this field.



Scope of the Project:

The Scope of Suspicious Human Activity Recognition is to recognize and highlight actions or conduct that may be warning signs of danger, criminal activity, or strange behaviour. Security, surveillance, law enforcement, and even healthcare all have a keen interest in the range of Suspicious Human Activity Recognition. This scope can be outlined as follows:

1. Security and Surveillance:

Monitoring crowded areas, transportation hubs, and public events to detect suspicious behaviour that could indicate potential threats. Protecting private property by recognizing unauthorized access or unusual activities.

2. Law Enforcement:

Identifying actions that may be associated with criminal behaviour, such as theft, vandalism, or assault. Recognizing and documenting traffic violations and reckless driving behaviours.

3. Border Control and Customs:

Identifying suspicious behaviour or patterns at border crossings or customs checkpoints. Detecting smuggling attempts or illegal trade activities.

4. Healthcare:

Monitoring patients in a healthcare setting to detect unusual or harmful behaviour. Ensuring the safety and well-being of elderly individuals by identifying falls or distressing situations.

5. Transportation:

Enhancing airport security by identifying suspicious behaviours among passengers or staff. Ensuring safety on public transit systems.

6. Military and Defence:

Protecting military installations by recognizing suspicious activities near or within them. Identifying potential threats in war zones or conflict areas.

Search Strategy:

To conduct a comprehensive literature review for your project on an "" it's essential to tap into relevant databases, libraries, and online resources. Here are some valuable sources and effective search strategies:

Start by identifying the main concepts related to SHAR, such as "suspicious human activity," "activity recognition," "anomaly detection," and any specific subdomains or applications you are interested in (e.g., "security surveillance" or "healthcare").

Utilize academic databases and search engines that specialize in relevant fields, such as IEEE Xplore, ACM Digital Library, PubMed (for healthcare applications), Google Scholar, and more.

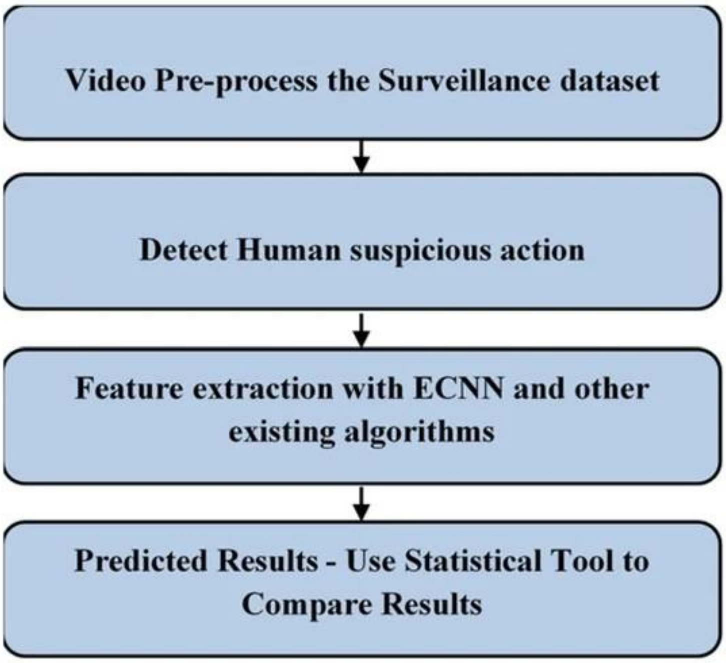
A well-structured search strategy is essential for conducting thorough literature reviews and staying up-to-date with the latest developments in Suspicious Human Activity Recognition. Additionally, consider collaborating with academic librarians or domain experts who can provide valuable guidance in your search for relevant resources.

Clearly outline the specific aspects of suspicious human activity detection you are interested in, such as the techniques, algorithms, applications, or domains.

Make a list of keywords and key phrases related to your research topic. Consider using synonyms and alternative terms. Combine keywords using Boolean operators (AND, OR, NOT) to create more specific or broader search queries.

Carefully review the abstracts and titles of the search results to assess their relevance to your research goals. Identify key journals, conferences, and publications in the field of SHAR, and search within them specifically. Examples include the International Conference on Computer Vision (ICCV), the Conference on Computer and Robot Vision (CRV), or the Journal of Pattern Recognition.

Developing a comprehensive search strategy for Suspicious Human Activity Recognition (SHAR) involves identifying relevant research papers, articles, patents, and resources related to the field.


Video Pre-process the Surveillance dataset
Detect Human suspicious action
Feature extraction with ECNN and other existing algorithms
Predicted Results - Use Statistical Tool to Compare Results

Selection Criteria:

Establishing clear selection criteria is essential for ensuring that the sources included in your literature review are relevant, credible, and align with your research objectives Here are some key selection criteria to consider:

1. Accuracy and Reliability:

- The system should have a high level of accuracy in detecting suspicious activities and minimizing false positives. Evaluate the system's performance based on metrics such as precision, recall, and F1-score.

2. Real-Time Processing:

- Depending on your application, real-time processing capabilities may be critical. Ensure that the SHAR system can analyze and respond to activities in real-time or near-real-time.

3. Scalability:

- Consider whether the system can scale to accommodate the size and complexity of the environment where it will be deployed. Scalability is crucial for large-scale surveillance or monitoring operations.

4. Customization and Adaptability:

- Determine if the system can be customized or adapted to specific use cases, environments, and types of suspicious activities. Look for flexibility in algorithm configuration and rule sets.

5. Integration:

- Check whether the SHAR system can integrate with existing security, surveillance, or monitoring infrastructure, such as cameras, sensors, alarms, and databases.

6. Alerting and Notification:

- Evaluate the system's ability to generate timely alerts and notifications when suspicious activities are detected. Ensure that alerts are configurable and can be sent to relevant personnel or systems.

7. Low False Positive Rate:

- A low false positive rate is crucial to avoid unnecessary disruptions and resource wastage. Assess the system's ability to minimize false alarms while accurately identifying genuine threats.

8. Privacy and Ethical Considerations:

- Consider the ethical and privacy implications of the SHAR system. Ensure that it complies with relevant data protection and privacy regulations and respects individuals' rights.

9. Robustness to Environmental Factors:

- Evaluate how well the system performs under various environmental conditions, such as lighting, weather, and crowd density. Robustness is crucial for outdoor and dynamic environments.

10. Training Data and Learning Capabilities:

- Assess the availability of high-quality training data and the system's ability to learn and adapt to evolving threat scenarios.

11. Cost and Budget:

- Consider the total cost of ownership, including initial setup costs, licensing fees, maintenance, and ongoing operational expenses. Ensure that the solution aligns with your budget constraints.

12. User-Friendliness:

- Evaluate the user interface and ease of use for operators and security personnel. A user-friendly interface can enhance the effectiveness of the SHAR system.

13. Support and Maintenance:

- Investigate the availability of technical support, software updates, and maintenance services. Reliable support is essential for system reliability and longevity.

14. Compliance with Regulations:

- Ensure that the SHAR system complies with relevant industry standards and regulations, such as GDPR, HIPAA (for healthcare applications), or industry-specific security standards.

15. Performance in Pilot Tests:

- If possible, conduct pilot tests or trials to assess the system's performance in your specific environment before making a final decision.

16. Vendor Reputation and References:

- Research the reputation of the vendor or provider. Seek references and case studies from organizations that have successfully implemented the SHAR system.

17. Future-Proofing:

- Consider the system's ability to adapt to future technological advancements and emerging threats. Future-proofing can help extend the lifespan of your investment.

By carefully considering these selection criteria, you can make an informed decision when choosing a Suspicious Human Activity Recognition system that best suits your organization's needs and objectives.

Developing a Suspicious Human Activity Recognition (SHAR) project involves several requirements and challenges, ranging from technical aspects to ethical considerations. Here are some key requirements and challenges you may encounter when working on a SHAR project:

Requirements:

1. Data:

- A large and well-annotated dataset of both normal and suspicious activities is required for training and evaluation. The dataset should represent a wide range of scenarios, environments, lighting conditions, and individuals.

2. Hardware and Infrastructure:

- Access to appropriate sensors and cameras for data collection and surveillance. Sufficient computational resources for data processing, model training, and real-time inference.

3. Algorithms and Models:

- Development and implementation of machine learning or deep learning models capable of recognizing suspicious activities. Efficient algorithms for real-time or near-real-time processing of video or sensor data. Techniques for anomaly detection and behaviour analysis.

4. Software Development:

- Proficiency in software development and frameworks for data preprocessing, model training, and deployment. Development of user-friendly interfaces for system operators.

5. Ethical and Legal Compliance:

- Adherence to privacy regulations and ethical guidelines, including data anonymization and consent. Compliance with local laws and regulations regarding surveillance and data collection.

6. Integration:

- The ability to integrate the SHAR system with existing security or surveillance infrastructure.

7. Performance Metrics:

- Defined metrics for evaluating the accuracy, precision, recall, and false positive rate of the SHAR system.

8. System Security:

- Measures to secure the SHAR system against hacking, tampering, or unauthorized access.

9. Training and Education:

- Training staff and operators on how to use the SHAR system effectively. A plan for continuous model retraining and improvement.

Challenges:

1. **Data Challenges:**

- Annotating large volumes of data with labels for suspicious activities can be time-consuming and costly. Ensuring the quality and consistency of data, especially in real-world, uncontrolled environments.

2. Model Challenges:

- Developing models that can handle the complexity and variability of human behaviour. Ensuring that the model generalizes well to different scenarios and demographics.

3. Real-Time Processing:

- Achieving real-time or near-real-time processing can be challenging, especially with large volumes of high-resolution video data.

4. Privacy and Ethical Challenges:

- Balancing the need for security with individuals' right to privacy.

- Addressing concerns about surveillance and potential misuse of the technology.

5. False Positives:

- Minimizing false positives is crucial to avoid unnecessary alarms and disruptions.

6. Adaptability:

- Ensuring that the SHAR system can adapt to evolving threats and changing environments.

7. Resource Constraints:

- Working within budget constraints, especially for hardware, software, and personnel.

8. Interoperability:

- Integrating the SHAR system with existing security and surveillance systems can be complex due to compatibility issues.

9. Legal and Regulatory Challenges:

- Complying with various laws and regulations governing surveillance, data collection, and privacy can be a significant challenge.

10. Bias and Fairness:

- Ensuring that the SHAR system is fair and does not exhibit bias against specific groups or demographics.

11. User Acceptance:

- Gaining acceptance from the public and stakeholders, who may have concerns about surveillance and privacy.

12. Environmental Factors:

- Dealing with challenges posed by environmental conditions such as low lighting, adverse weather, or crowded spaces.

Addressing these requirements and challenges requires a multidisciplinary approach that includes expertise in machine learning, computer vision, ethics, privacy, and legal compliance. It also involves ongoing monitoring and adaptation as technology and threats evolve.

Learning Theories and Models:

Even though there is a considerable quantity of suspicious-activity detections in different fields throughout the world, still there is a lacuna. Since no sophisticated solution with automation of suspicious-activity detection is available, there is a need to introduce efficient suspicious-activity detection with automation systems in video surveillance. A considerable number of works by the authors have been carried out with DL and ML algorithms.

The core objective of this work is to introduce an enhanced-CNN-based suspicious-human-activity detection technique and compare its performance measures, such as mean accuracy, mean precision, mean false-positive rate, and mean-false-negative rate, with existing machine learning (ML) and deep learning (DL) algorithms to warrant the novelty of the proposed approach.

The research work has identified novel suspicious-action detection from the video surveillance dataset. In this work, the ECNN algorithm has been coined to support suspicious-action detection with a surveillance video dataset. The ECNN is an improved CNN algorithm and the Leaky ReLU layer has been inserted to predict suspicious action effectively. The experiment was conducted with the ECNN algorithm for a considerable count of time and performances were noted. Later analysis has been set with the SPSS tool and graph builder alongside independent t-sample tests with their parameters inferred. The performance measures such as accuracy, precision, false positive, and false negative have been noted.

CNN:

Within Deep Learning, a Convolutional Neural Network or CNN is a type of artificial neural network, which is widely used for image/object recognition and classification. CNN is playing a major role in diverse tasks/functions like image processing problems, computer vision tasks like localization and segmentation, video analysis, to recognize obstacles in self-driving cars, as well as speech recognition in natural language processing. As CNNs are playing a significant role in these fast-growing and emerging areas, they are very popular in Deep Learning.

Leaky ReLU:

Leaky Rectified Linear Unit, or Leaky ReLU, is a type of activation function based on a ReLU, but it has a small slope for negative values instead of a flat slope. The slope coefficient is determined before training, i.e. it is not learnt during training. This type of activation function is popular in tasks where we may suffer from sparse gradients, for example training generative adversarial networks.

Classification and activity recognition:

After finding moving or stationary foreground objects in a frame, the object classification step is applied for the recognition of normal or abnormal behaviour. For example, a stationary human and abandoned object at public place will be treated as suspicious objects if there is no knowledge of the object features. Object classification distinguishes to the static human from static abandoned object, fighting from boxing, face from skin colour objects, fire from flashlight, sun light, and any artificial light, falling human pose from laying human pose etc. In general, there are three- feature based, motion based and shape-based classification methods. Several researchers have utilized the different features with different classifiers such as SVM, k-Nearest Neighbour, Multi-SVM, Cascade classifier, Neural Network, and HAR to analyse the human behaviour and recognition of abnormal activities. Table 4 shows that many researchers have utilized the different classification methods to recognize the abandoned objects and to improve the accuracy by using either tracking or non-tracking based approaches. Table 5 visualizes the different work done for theft detection with its used datasets, classification methods, and result discussion. In Table 6, research works have been categorized with three different shape based, posture based and motion based classification techniques with result discussion. Table 7 shows accidents, traffic rule breaking detection and violence detection approaches with their classification methods and result discussion. In Table 8, we have discussed the fire and smoke segmentation, detection methods and its result discussion.

Applications:

Importance of the suspicious human activities recognition from video surveillance is to prevent the theft cases, leaving abandoned objects for the explosive attacks by terrorists, vandalism, fighting and personal attacks and fire in the different highly sensitive areas such as banks, hospitals, malls, parking lots, bus and railway stations, airports, refineries, nuclear power plants, schools, university campuses, borders etc. Intelligent video surveillance protects the following areas from suspicious activities (Yilmaz et al. 2006):

University campus and academic institutions Video surveillance is being used in university campuses and other academic institutions to monitor the activities of students for the safety of assets from theft and vandalism. It also helps to prevent the inappropriate behaviour of the students and fighting among the students. It also monitors the perimeter of the university campus, school and academic institutions for the safety of the students and faculties. Video surveillance can be used at the time of examination to monitor the suspicious activity of the students in the examination hall.

Public infrastructure To save population and public infrastructures such as borders, laboratories, prisons, military bases, temples, parking lots; video surveillance is helpful to prevent the theft, vandalism, fighting and personal attacks, increasing crowd, explosive attacks.

Retail trade This is a growing market for the use of video surveillance to detect the suspicious human activity for both the internal such as warehouses, stores and external like parking lots security. Even the small shops are utilizing the cameras to monitor the human activities and to capture the video evidence in case of theft or an incident. In chain stores, much more sophisticated video surveillance systems are set up for centralized monitoring of different locations.

Suspicious activity recognition from video surveillance helps to monitor employee fraud and theft, monitor wares and inventory, protecting material goods and infrastructures, protecting staff and clients, monitoring parking lots, vehicles, entries and exits, and emergency situations such as fire.

Airports Airport are high security sensitive areas where the safety of passengers, runway and airplane is the most important in any country. Real-time suspicious human activity recognition system from video surveillance provides high level security to such security sensitive areas.

Railway and bus stations The use of video surveillance at railway and bus stations plays vital role in case of monitoring platforms, routes, parking lots, rails and tunnels. These areas are the prime targets of the terrorists for explosive attacks by leaving a bag containing bomb. Suspicious activity recognition system from video surveillance can recognize the abandoned object and can alarm to remove it from public place for the protection of passengers, personnel and infrastructures.

Suspicious human activity recognition: a review Banking sector Video surveillance play an important role in banking sectors to provide the security. The presence of cameras prevents to committing the armed robbery and assault. Automated bank machines are prime targets for criminal acts. Surveillance camera helps to detect fraud, for example; the installation of a device to read the magnetic information on bank cards. Intelligent video surveillance can increase monitoring effectiveness in banking sectors. It provides monitoring to all the branches in order to detect suspicious behaviour. In ATMs, it also helps to prevent theft cases.

Gaming industries and casinos Suspicious activity recognition from video surveillance can help to detect the cheating, heists, and other crimes. Since monitoring of casino requires watching the activity of human beings in a crowded environment, intelligent video surveillance is an interesting way of helping security personnel.

Hospitals Video surveillance can also be used in hospitals to monitor the patients at home to monitor elder people or children. It can even be found in ambulances to monitor a patient remotely. Video surveillance can monitor the activity of the patients in hospitals and can recognize the suspicious activity such as vomiting, fainting and other unusual activity of the patients.

Organization:

Detecting suspicious activity typically involves a combination of technology, processes, and trained personnel. Organizations concerned with identifying and mitigating suspicious activity often follow a structured approach, including the following components:

1. Security Operations Centre (SOC): Establishing a SOC is a fundamental step. It's a centralized team responsible for monitoring, detecting, and responding to security incidents and suspicious activities. SOC analysts use various tools and techniques to identify unusual behaviour.

2. SIEM (Security Information and Event Management) System: SIEM platforms aggregate data from various sources (logs, network traffic, etc.) to analyse and correlate events. They help identify patterns and anomalies that could indicate suspicious activity.

3. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS): These systems analyse network traffic and system logs in real-time to identify and block potentially malicious activity.

4. User and Entity Behaviour Analytics (UEBA): UEBA tools monitor user and entity behaviour to detect anomalies. They can spot unusual access patterns, privilege escalations, and more.

5. Endpoint Detection and Response (EDR) Solutions: EDR tools are used to monitor and secure individual endpoints (computers, servers, etc.) and can detect malicious activity at the host level.

6. Threat Intelligence Feeds: Organizations subscribe to threat intelligence services that provide information on known threats and vulnerabilities. This information can help in proactively identifying suspicious activity.

7. Security Policies and Procedures: Clearly defined security policies and procedures are crucial. These should outline what constitutes suspicious activity and how to respond when it's detected.

8. Incident Response Plan: Having a well-documented incident response plan is vital. It should define roles and responsibilities and provide step-by-step guidance on how to handle suspicious activity.

9. Security Awareness Training: Employees and users are often the first line of defence. Training them to recognize and report suspicious activity can be highly effective.

10. Access Controls: Implement strong access controls to limit who can access sensitive systems and data. Regularly review and audit user access.

11. Forensics and Investigation Tools: In case of a suspected breach or suspicious activity, having the tools and expertise to conduct digital forensics investigations is crucial.

12. Machine Learning and AI: Implement machine learning and AI algorithms to analyse large datasets for patterns indicative of suspicious behaviour.

13. Collaboration and Communication: Establish clear communication channels for reporting and discussing suspicious activity within the organization.

14. Third-party Services: Consider outsourcing certain security functions, such as threat hunting, to specialized security firms.

15. Continuous Monitoring and Evaluation: Regularly assess the effectiveness of your suspicious activity detection systems and processes, and make necessary improvements.

16. Legal and Ethical Considerations: Be mindful of legal and ethical considerations when monitoring and investigating suspicious activity to avoid privacy violations and other legal issues.

Remember that security is an ongoing process, and threats evolve over time. Therefore, organizations must continuously adapt and improve their suspicious activity detection strategies to stay ahead of potential threats.

Synthesis:

Synthesis for suspicious activity detection involves combining various data sources, technologies, and methodologies to create a comprehensive and effective system for identifying and responding to potentially malicious behaviour. Here's a synthesized approach to building a suspicious activity detection system:

1. Data Collection and Aggregation:

- Gather data from diverse sources, including network logs, system logs, user activity logs, application logs, and external threat intelligence feeds.

- Implement data normalization and enrichment to ensure uniformity and context in the collected data.

2. Security Information and Event Management (SIEM):

- Deploy a SIEM system to centralize and correlate data, allowing for real-time analysis and alerting.

- Create custom SIEM rules and use cases tailored to your organization's specific risks and needs.

3. Machine Learning and AI:

- Integrate machine learning and AI algorithms into the SIEM to analyse historical and real-time data for anomalies and patterns.

- Develop models for behaviour profiling and anomaly detection, such as user and entity behaviour analytics (UEBA).

4. Intrusion Detection and Prevention:

- Implement Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor network traffic and identify suspicious patterns or known attack signatures.

- Configure these systems to take automated actions when suspicious activity is detected.

5. Endpoint Detection and Response (EDR):

- Employ EDR solutions to monitor and secure individual endpoints, allowing for the detection of malicious activities at the host level.

- Utilize EDR for threat hunting and incident response on endpoints.

6. Threat Intelligence Integration:

- Integrate threat intelligence feeds into your detection system to stay informed about the latest threats and vulnerabilities.

- Use threat intelligence to enhance detection rules and indicators of compromise.

7. User and Entity Behaviour Analytics (UEBA):

- Develop UEBA models to baseline normal user and entity behaviour.

- Continuously monitor for deviations from these baselines, which may indicate suspicious activity.

8. User Training and Awareness:

- Educate employees and users about the importance of recognizing and reporting suspicious activities.

- Conduct security awareness training to enhance the human component of detection.

9. Legal and Ethical Considerations:

- Ensure that your detection system complies with legal and ethical guidelines, including privacy regulations.

- Respect user privacy and data protection while monitoring and investigating suspicious activity.

10. Continuous Improvement:

- Regularly review and analyse incidents to identify weaknesses and areas for improvement in your detection system.

- Adjust your strategy based on lessons learned and emerging threat landscape trends.

11. Collaboration and Information Sharing:

- Foster collaboration with industry peers, information sharing and analysis centres (ISACs), and relevant authorities to stay informed about emerging threats and tactics.

By synthesizing these elements into a cohesive framework, organizations can enhance their ability to detect and respond to suspicious activities effectively, thereby strengthening their overall cybersecurity posture.

Conclusion and future work:

In this survey paper, we have discussed the various techniques related to abandoned object detection, theft detection, falling detection, accidents and illegal parking detection, violence detection and fire detection for the foreground object extraction, tracking, feature extraction and classification. In past decades, several researchers proposed novel approaches with noise removal, illumination handling, and occlusion handling methods to reduce the false object detection. Many researchers have also worked for making real-time intelligent surveillance system but processing rate of the video frames is not as good as required and there is no such system that has been developed with 100% detection accuracy and 0% false detection rate for videos having complex background. Much of the attention is required in the following suspicious activities detection:

Abandoned object detection and theft detection Majority of the works have been done for the abandoned object detection from surveillance videos captured by static cameras. Few Suspicious human activity recognition: a review works detected the static human as an abandoned object. To resolve such problems, human detection method should be very effective and system should check the presence of the owner in the scene, if owner is invisible in the scene for long duration then alarm should be raised. To resolve the problem of theft or object removal, face of the person who is picking up the static object, should match with the owner otherwise an alarm must be raised to alert the security. Future work may also resolve the low contrast situation i.e. similar colour.

problem such as black bag and black background which lead to miss detections. Future improvements may be integration of intensity and depth cues in the form of 3D aggregation of evidence and occlusion analysis in detail. Spatial-temporal features can be extended to 3-dimensional space for the improvement of abandoned object detection method for various complex environments. Thresholding based future works can improve the performance of the surveillance system by using adaptive or hysteresis thresholding approaches. Few works have been also proposed for abandoned object detection from the multiple views captured by multiple cameras. To incorporate these multiple views to infer the information about abandoned object can also be improved. There is a large scope to detect abandoned object from videos captured by moving cameras. Falling detection Most of the works have been done for fall detection of single person in indoor videos based on human shape analysis, posture estimation analysis and emotion based analysis. Future works can include the integration of multiple elderly monitoring which is able to monitor more than one person in the indoor scene. Many elder people go for morning walk every day in public areas such as parks; to monitor these elder people, a future work can include one or more than one human fall detection from outdoor surveillance videos. Accidents, illegal parking, and rule breaking traffic detection Several researchers have presented accidents detection, illegal parking detection and illegal U-turn detections from static video surveillance. These systems become incapable to detect these abnormal activities in more crowded traffic on roads. Future works should be based on unsupervised learning of transportation system because of no standard dataset is available for the training. Violence detection Several research works have been done for the prevention of violence activities such as vandalism, fighting, shooting, punching, and hitting. To detect such violence activities, single view static video camera has been used but sometimes this system fails in occlusion handling. Therefore, a multi-view system has been proposed by few researchers to resolve this problem but it requires important cooperation between all views at the lowlevel steps for abnormal activity detection. Future work may be automatic surveillance system for moving videos. Improvements are required in accuracy, false alarm reduction, and frame rate to develop an intelligent surveillance system for the road traffic monitoring. Fire detection Future work can include more improvement in accuracy, frame rate, false alarms reduction and also it can be improved to detect far distant small fire covered by dense smoke.