iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59081

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

ANOMALY XPERT: A Deep Learning Approach to Anomaly Detection

B. Gayathri[1], A. Abhinav[2], C. Harishwar Reddy[3], G. Praneeth[4]
[1, 2, 3]*UG Student, Department of CSE, CMR College of Engineering & Technology, Hyderabad, Telangana*
[4]*Professor, Department of CSE, CMR College of Engineering & Technology, Hyderabad, Telangana*

Abstract: ***In response to increasing crime rates, organizations are deploying surveillance systems with CCTV cameras to detect suspicious activities autonomously. This paper proposes an automated system using transfer learning-based CNN models to track and classify activities like 'Shoplifting,' 'Robbery,' or 'Break-In' in real-time CCTV footage. The framework processes raw camera data, detects objects, tracks activities, and classifies them, generating alerts for authorized personnel. Leveraging transfer learning enhances the precision and effectiveness of the CNN model in identifying security threats. Preliminary evaluations demonstrate promising outcomes, yet additional investigation is warranted to address obstacles such as occlusions and lighting variations. Overall, this system offers a proactive security solution for retail environments, ensuring timely detection and intervention against potential security breaches***

Keywords: Crime rates, surveillance systems, CCTV cameras, autonomous detection, transfer learning, CNN models, real-time footage, generating frames, security threats, alerts, authorized personal, optimization, lighting variations, retail environments, security breaches..

I. INTRODUCTION

Suspicious behavior encompasses actions indicating potential involvement in criminal activities or imminent criminal intent, readily identifiable through surveillance videos. Examples include unfamiliar individuals lingering in neighborhoods or vehicles repeatedly traversing streets. Additionally, behaviors such as peering into cars or windows, loitering near schools, parks, or secluded areas, and discovering open or broken doors/windows at unoccupied residences raise suspicion. Visual surveillance serves to monitor human activities in sensitive and public areas like bus/railway stations, airports, banks, malls, schools, parking lots, and roads to prevent terrorism, theft, accidents, illegal parking, vandalism, and altercations. Continuous monitoring of public spaces necessitates intelligent video surveillance capable of real-time human activity monitoring, categorization as usual or unusual, and alert generation.Top of Form

II. EXISTING SYSTEM

1) *Statistical analysis and Threshold-based Detection:* Traditional statistical methods, like mean and standard deviation examination are frequently employed to identify irregularities in time-series data. Threshold-based approaches involve setting predefined thresholds and Identifying data points that deviate significantly from expected values. Nonetheless these methods can face difficulties with complex and non-linear data patterns, leading to high false positive rates
2) *Ensemble Methods:* Ensemble techniques combine multiple anomaly detection algorithms to improve overall detection performance and robustness. By aggregating the outputs of individual detectors, ensemble methods can reduce false positives and enhance anomaly detection accuracy. Common ensemble approaches include bagging, boosting, and stacking, which lverage diverse models to capture different aspects of anomalies.
3) *Streaming Data Processing:* With the advent of big data technologies, streaming data processing frameworks like Apache Kafka and Apache Flink enable real-time anomaly detection on high-velocity data streams. These platforms facilitate the rapid ingestion, processing, and analysis of large-scale data streams, allowing for timely detection and response to anomalies as they occur..

III. LITERATURE SURVEY

1) Amrutha presented a surveillance system employing the pre-trained VGG-16 model to monitor student behavior during examinations. This system employs neural networks and Gaussian distribution to classify behavior as normal or suspicious. Although initially designed for academic settings, This framework holds promise for wider utilization across public and private sectors, facilitating the identifying of suspicious individuals based on their activities.

2) Sathyajit introduced an image-based approach for anomaly detection, focusing on the efficient identification of abandoned baggage. By leveraging captured images for training, this method offers computationally efficient detection, with minimal computational time required for each frame. However, further enhancements are necessary to enable real-time detection of firearms and other suspicious objects.
3) Guillermo proposed a 3D CNN model trained under various approaches, including binary and multi-class classification, for detecting suspicious activities. While effective in distinguishing between normal and suspicious behaviors, the model's binary classification approach limits its ability to identify specific types of crimes. Additionally, the multi-class training stage introduces the risk of false positives among different criminal classes.
4) Om introduced a surveillance system utilizing transfer learning-based CNN models to detect activities such as 'Shoplifting,' 'Robbery,' or 'Break-In' in retail stores. By analyzing real-time CCTV footage, the system promptly alerts owners upon detecting suspicious behavior. The framework involves extracting frames, passing them through a trained CNN model, and aggregating predictions to identify anomalies. Despite its effectiveness, the system experiences a flickering effect, which warrants further refinement for seamless operation.

IV. METHODOLOGY

A. Classification of Attacks

Anomaly xpert system utilizing deep learning techniques are essential for identifying a range of security threats across various domains. These threats include intrusion attempts targeting network security, malware infections compromising system integrity, insider actions posing internal risks, denial of service attacks disrupting services, data breaches compromising sensitive information, fraudulent transactions impacting financial systems, and adversarial attacks targeting deep learning models themselves. By classifying attacks into distinct categories, deep learning-based anomaly detection systems can effectively analyze and respond to anomalous behaviors, thereby enhancing security and mitigating potential risks across diverse environments.

B. Dataset

For Anomoly xpert project, datasets like UCF-Crime, Avenue, UCSD Pedestrian, ShanghaiTech Campus, and public safety datasets containing real-world instances of theft, robbery, assault, loitering, vandalism, and other abnormal behaviors are crucial for training and evaluating detection models. Additionally, synthetic datasets and surveillance video datasets complement real-world data, offering diverse scenarios for algorithm development. Traffic surveillance datasets and crowd monitoring datasets capture anomalous behaviors in road and public settings, further enriching the training data. By leveraging these datasets, researchers can build robust detection systems capable of identifying a wide variety of suspicious activities across different environments, facilitating enhanced security and public safety measures.

C. Data Analysis

Data analysis for Anomoly xpert involves Gathering information from security cameras and sensors, preprocessing it to remove noise and standardize formats, and then engineering relevant features to characterize suspicious behavior. Exploratory data analysis aids in recognizing patterns and anomalies, guiding the creation of machine learning or deep learning model for detection. After training and evaluation, models are fine-tuned and optimized for deployment in real-time environments. Continuous monitoring ensures system performance and allows for updates to adapt to evolving threats

D. Algorithms

In Anomaly xpert, various algorithms are employed to effectively identify and classify abnormal behaviors. This includes supervised learning algorithms like Support Vector Machines(SVM’s), Random Forests, and Gradient Boosting Machines for classification tasks with labeled data, where as unsupervised learning algorithms such as k-means clustering and DBSCAN are used when labeled data is scarce. Deep learning architectures such as Convolutional Neural Network(CNN’s) and Recurrent Neural Networks process visual and sequential data respectively, aiding in detecting suspicious activities from surveillance videos or sensor data. Dimensionality reduction methods such as Principal Component Analysis Method are applied for feature extraction, where as ensemble learning methods like Isolation Forest and probabilistic models such as Gaussian Mixture Models are employed for anomaly detection in high-dimensional datasets. These algorithms also be used in isolation or combination to develop robust suspicious activity detection systems capable of identifying security threats efficiently.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

E. Implementation Block Diagram

In the realm of suspicious activity detection, diverse implementations are deployed to enhance security measures across various domains. Video processing techniques play a pivotal role, enabling the extraction of valuable insights from surveillance footage. Through methods like motion detection and object tracking, these systems can discern anomalies amidst regular activities. Feature extraction mechanisms further aid in identifying pertinent patterns, allowing for the characterization of suspicious behaviors effectively. By Measuring these techniques, the systems can distinguish between normal activities and potential threats, facilitating proactive intervention when necessary. Machine learning algorithms serve as the backbone of many suspicious activity detection systems, offering robust capabilities in classification and anomaly detection. Supervised learning models such as Support Vector Machine(SVM's) and Random Forests are adept at categorizing activities based on labeled datasets, while unsupervised techniques like k-means clustering excel in identifying irregular patterns without explicit guidance.Additionally, Advanced learning frameworks, encompassing Convolutional Neural Network(CNN) and Recurrent Neural Networks (RNNs), are extremely beneficial for grasping intricate characteristics from unprocessed data., enabling precise identification of suspicious behaviors in real-time scenarios. Integration with alerting systems is crucial to ensure swift responses to detected anomalies. These systems are engineered to promptly notify relevant authorities or Security personnel are called upon when there are indications of suspicious behavior. enabling timely intervention and mitigation of potential threats. Real-time processing capabilities further enhance the efficacy of these implementations, allowing for instantaneous analysis of incoming data streams and immediate action when anomalous behavior is detected. Scalability and adaptability are key considerations in the design of suspicious activity detection systems, enabling them to be deployed in diverse environments and scenarios. Whether in small-scale premises or large-scale public spaces, these machines are engineered to effectively enhance security measures and ensure the safety of individuals and assets. By harnessing advanced technologies and implementing robust strategies, suspicious activity detection systems playing a part in preventing possible risks and ensuring a safe setting for all parties concerned.

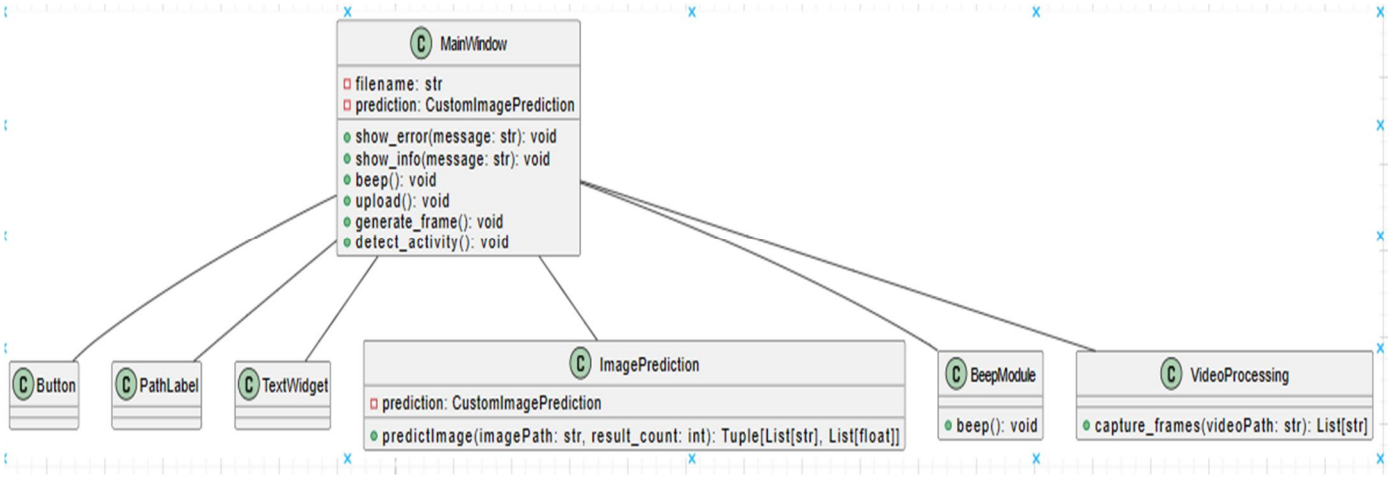


Fig.1 Architecture of the proposed model

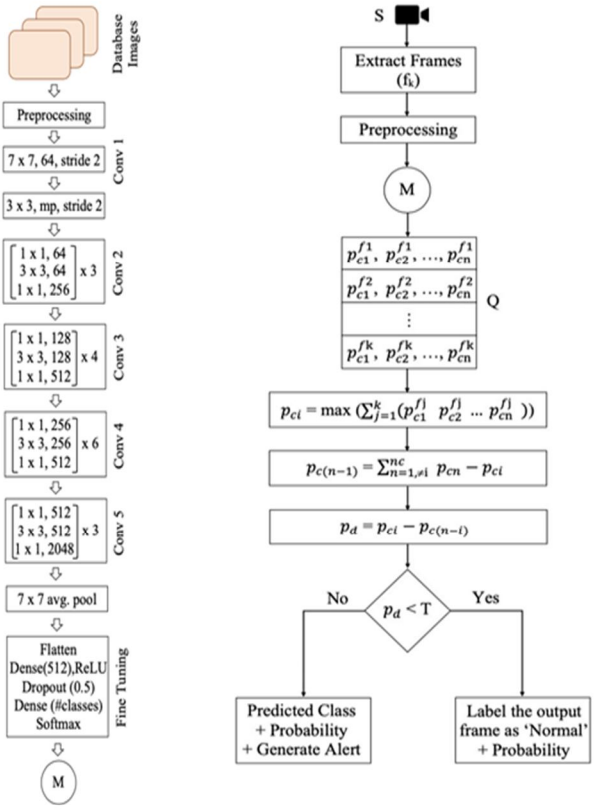
V. RESULTS AND DISCUSSION

A. Traning and Testing

In our system, a wide array of input videos is harnessed, originating from the DCSASS dataset, the KTH dataset, YouTube, and shop surveillance recordings, totaling 16,853 videos portraying both normal and suspicious behaviors. These videos undergo preprocessing, wherein frames are extracted and resized to suit the model's requirements. The model architecture consists of five fundamental layers: a convolutional layer for feature extraction, a pooling layer for downsampling, a fully connected layer for classification, a dropout layer to prevent overfitting, and an activation function to introduce non-linearity into the network. This modular design ensures robust performance and adaptability across various scenarios.

Real-time operation of the system involves the continual processing of live video streams. Frames extracted from these streams undergo preprocessing and are individually analyzed by the model. Each frame is assigned a class label and corresponding probability, which are then overlaid onto the output frame.

This process, repeated for every frame, yields a labeled video stream in real-time, enabling immediate action in response to detected anomalies. By providing instantaneous feedback, our system empowers authorities to intervene swiftly and effectively, potentially preventing security breaches or criminal activities before they escalate. For training purposes, our dataset function as the foundation, containing CCTV footage captured in diverse settings such as shops. This footage is converted into frames and fed into the trained model, which accurately classifies the videos as either exhibiting suspicious or normal behavior. Object tracking within the video frames is facilitated through the utilization of color histograms. Each detected object is associated with three histograms representing its red, green, and blue components. By comparing these histograms across consecutive frames, objects can be tracked consistently, allowing for the continuous monitoring and analysis of activities over time.



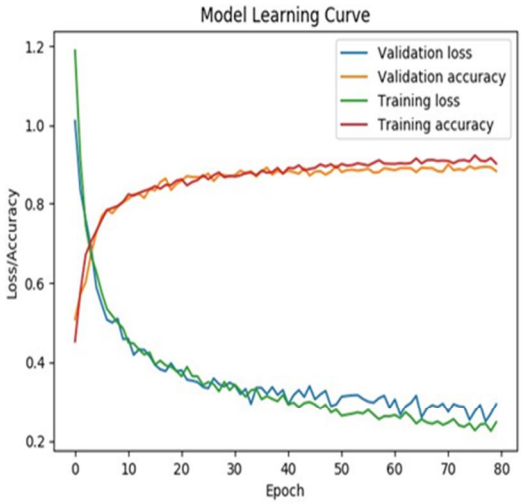


fig 3:preprocessing algorithm

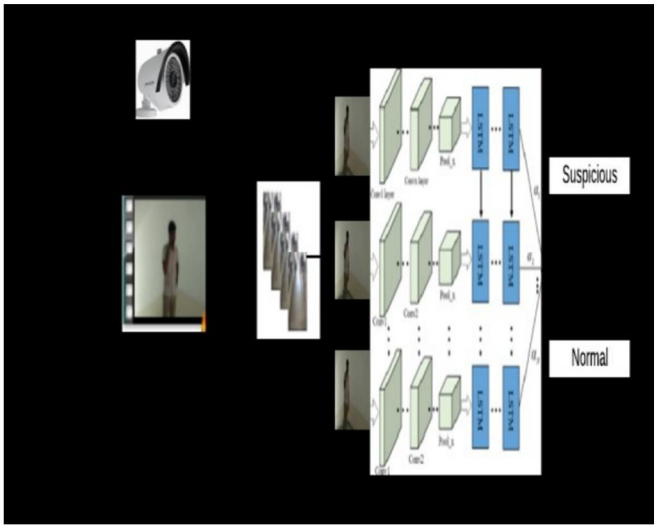


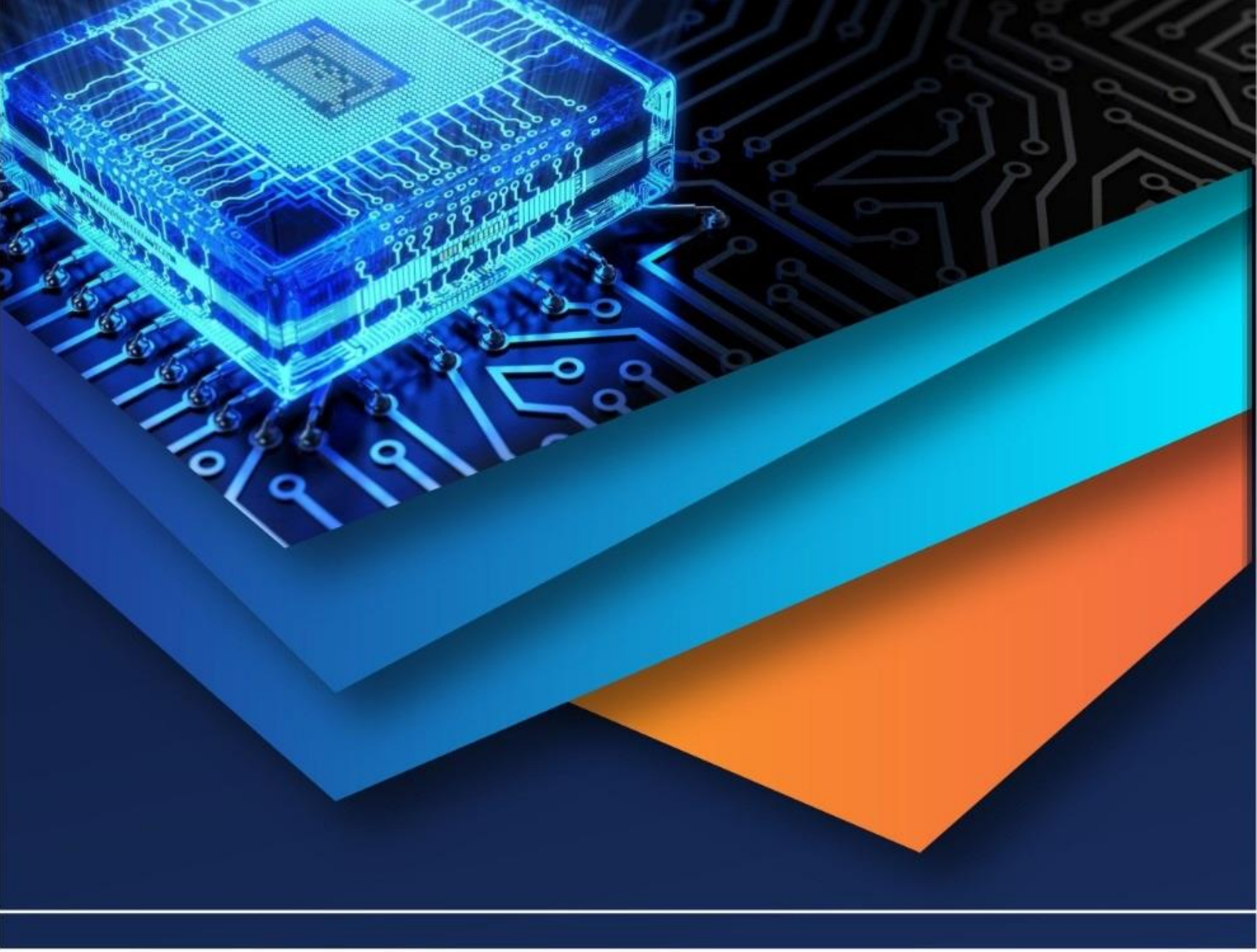
Fig 2:processing framework

VI. CONCLUSION

In today's world, the significance of CCTV footage is widely acknowledged, yet its utilization primarily occurs post-incident for investigation purposes. However, our proposed model offers a proactive approach by leveraging real-time CCTV footage analysis to prevent crimes before they occur. By continuously monitoring and analyzing live feeds, the system can promptly alert relevant authorities upon detecting potential threats, enabling preventive actions to be taken in a timely manner. While initially designed for academic settings, this model holds promise for broader applications in public and private spaces. With tailored training, it can effectively predict suspicious behaviors across various scenarios. Future enhancements may involve refining the system to not only detect suspicious activities but also identify individuals exhibiting such behaviors, further enhancing its preventive capabilities.

REFERENCES

[1] P. Bhavya Divya, S. Shruti, R. Devika, B. Sreya Reddy, “Investigation of suspicious human activity in crowdsourced areas captured in surveillance cameras”, International Research Journal of Engineering and Technology(IRJET), December 2017.
[2] Jatin Musale, Alisha Gaikwad, Liyakat Sheikh, Pournima Haghvane, Sneha Tadke, “Detection and tracking of suspicious movements in human behavior and objects with fire detection using Closed Circuit TV (CCTV) cameras”, Global Symposium for Research in Applied Science & Engineering Technology (IJRASET), Volume 5 Issue XII, December 2017.
[3] U. M. Karthik, C. G. Patil, “Recognition of suspicious activities in video surveillance systems”, Fourth Global Symposium on Computing, Communication, Control and Automation (ICCUBEA), 2018.
[4] Zara Khan, Abeer Youssef, Ibrahim El Sayed, Sameh Abdul-Nabi, Hassan Qasim, “Detection of unusual events in university areas”, Global Symposium on Computers and Applications, 2018.
[5] Tina Wang, Mina Qian, Ying Deng, Ida Zhou, Hana Wang, Qian Lu, Hisham Snoussi, “Detection of abnormal events based on analysis of movement information in video sequences”, Article-Optics, vol. 152, January 2018.
[6] Eliza Susan, Aby Abraham, and Elizabeth Isaacs, “Detection of suspicious activity in surveillance video using Discriminative Deep Belief Networks”, International Journal of Control Theory and Applications, Volume 10, Number 29 -2017.
[7] Daniel Jackson Samuel R, Fenil E, G. Manogaran, V. Ganesh N., T. Thanjaivadivel, S. Jeevan, A. Ahilan, “Framework for real-time detection of violence in football stadiums comprising big data analysis and deep learning using bidirectional LSTM”.
[8] Kwang-Eun Ko, Kwee-Bo Sim“Deep convolutional framework for abnormal behaviour detection in an intelligent surveillance system.”Engineering Applications of Artificial Intelligence ,67 (2018).
[9] Yuke Li “A Deep Spatiotemporal Perspective for Understanding Crowd Behavior”, Institute of Electrical and Electronics Engineers(IEEE) Transaction on multimedias, Vol. 20, NO. 12, December 2018.
[10] Javier Abellan-Abenza, Alberto Garcia-Garcia, Sergiu Oprea, David Ivorra-Piqueres, Jose Garcia-Rodriguez “Classifying Behaviours in Videos with Recurrent Neural Networks”, International Journal of Computer Vision and Image Processing,December 2017.
[11] Asma Al Ibrahim, Gibrael Abosamra, Mohamed Dahab “Real-Time Anomalous Behavior Detection of Students in Examination Rooms Using "Exploring Neural Networks and Gaussian Distribution Patterns" in the International Journal of Scientific and Engineering Research, published in October 2018.
[12] G. Sreenu and M. A. Saleem Durai “Intelligent video surveillance: a review through Advanced learning methods for crowd analysis” , Journal Big Data ,2019.
[13] Radha D. and Amudha, J., “Detection of Unauthorized Human Entity in Surveillance Video”, Worldwide Journal of Engineering and Technology ,2013.
[14] K. Kavikuil and Amudha, J., “Leveraging deep learning for anomaly detection in video surveillance”, Advances in Intelligent Systems and Computing,2019.
[15] Sudarshana Tamuly, C. Jyotsna, Amudha J, “DeepLearning Model for Image Classification”, Global Symposium on Computational Vision and Bio Inspired Computing (ICCVBIC),2019.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY