STM JOURNALS

International Journal of
Satellite Remote Sensing

Volume 1, Issue 1, 2023
January–June
DOI (Journal): 10.37591/IJSRS

https://journals.stmjournals.com/ijsrs

Research IJSRS

Deep Guard: A Comprehensive Deep Learning System for Unmasking Suspicious Activities in Surveillance Footage

Piyush Jain[1,*], Shreyash Chole[2], Rishabh Nath Tiwari[3], Samiullah Siddiqui[4]

Abstract

These days, video surveillance is quite vital. Technology has evolved considerably as machine learning, artificial intelligence, and deep learning become increasingly widespread. There are several algorithms that assist in identifying distinct kinds of suspicious behaviour from live footage by combining the techniques. A person's behaviour is the most unpredictable thing, and it can be quite challenging to determine whether it is normal or suspicious. Video surveillance is automated to address this. On CCTV cameras, it is currently not feasible to manually watch every incident. It is a waste of time to manually look for the identical occurrence in the recorded video, even if it has already occurred. An emerging area in automated video surveillance systems is the analysis of anomalous events in video.To identify questionable or odd behaviour in the academic setting and notify the relevant authorities if any suspicious conduct is found, a deep learning technique is employed. For surveillance purposes, a collection of still photos from a video is commonly employed. Each frame is divided into two halves. In the first phase, the features are computed from the video frames; in the second, the classifier uses the retrieved features to determine whether the class is normal or suspicious.

Keywords: Suspicious Activity, Video Surveillance, Deep Learning, GPU (Graphic Processing Unit), Electronic article surveillance (EAS).

INTRODUCTION

It has numerous uses in intelligent video surveillance, real-world human behaviour recognition, and shopping behaviour analysis. There are many uses for video surveillance, particularly in indoor and outdoor environments. Being vigilant is essential to maintaining security. For reasons of safety and security, security cameras are becoming a commonplace feature in modern life. One of the main goals of Digital India, the Government of India's development programme, is e-governance. Video surveillance is still included in it. Effective surveillance, reduced labour costs, cost-effective surveillance capabilities, adoption of new security trends, etc. are some benefits of video surveillance. Humans are now in charge of tracking [1].

***Author for Correspondence**
Piyush Jain
E-mail: piyushjk89@gmail.com

[1-4]Student, Department of Computer Engineering, NBN Sinhgad School of Engineering, Sinhgad Rd, Ambegaon Budruk, Pune, Maharashtra, India

Received Date: October 27, 2023
Accepted Date: November 08, 2023
Published Date: November 29, 2023

Citation: Piyush Jain, Shreyash Chole, Rishabh Nath Tiwari, Samiullah Siddiqui. Deep Guard: A Comprehensive Deep Learning System for Unmasking Suspicious Activities in Surveillance Footage. International Journal of Satellite Remote Sensing. 2023; 1(1): 23–28p.

People may easily become overwhelmed by the volume of video data we are working with, and manual intervention will inevitably lead to mistakes. It has a significant impact on the system's efficiency. Video surveillance is automated to address this. On CCTV cameras, it is currently not feasible to manually watch every incident. It is a waste of time to manually look for the identical occurrence in the recorded video, even if it has already occurred. An emerging area in automated video surveillance systems is the analysis of anomalous events in video. In video surveillance

systems, human behaviour detection is an automated method for quickly identifying suspicious object action. Airports, train stations, banks, workplaces, exam rooms, and so forth. Several efficient techniques, including machine learning, deep learning, and artificial intelligence's use of video surveillance, can be used to automatically identify human behaviour in public areas.

Computers can think more like humans thanks to artificial intelligence. Predicting future data and learning from training data is a key aspect of machine learning. Deep learning is employed because huge databases and GPU (Graphics Processing Unit) processors are available today. Public safety and security will be guaranteed by the integration of video surveillance and computer vision technologies. The following processes are included in computer vision techniques: data fusion from multiple cameras, tracking, motion detection, classification of moving objects, understanding, and interpreting behaviour, and environment modelling. The process of extracting features from several video sequences using this method is labour intensive. Sorting techniques: supervised and unsupervised. While unsupervised classification is entirely computer-driven and does not involve human participation, supervised classification makes use of manually defined training data [2–6].

LITERATURE SURVEY

Food goods must be profiled in real time to determine their shelf life, quality, and freshness along the supply chain. This work presents the use of thin film coated sensor tags that are compatible with electronic article surveillance (EAS) and produced on a porous substrate for volatile profiling. Different amounts of volatile vapours are injected into an enclosed chamber containing the thin film coated tag and a reference tag that is not coated. To distinguish distinct volatile concentrations, the frequency shift between the reference tags and the sensor is observed. The tags are made on a flexible, porous substrate that allows capillary condensation to cause surface adsorption. The tags' wireless and adaptable design makes it simple to integrate them with current packaging technologies for real-time food supply chain monitoring [7].

Since one of our fundamental requirements is safety, we require a security system that can deter crime. We frequently employ surveillance footage to observe the surroundings and actions of people in a certain area. Nevertheless, surveillance footage is limited to capturing still photos or moving images without any other data. Therefore, to obtain more information like human position and movement, we need more sophisticated cameras. The information was extracted from security camera footage by this research using an algorithm for human detection and tracking. A highly well-liked area of artificial intelligence called deep learning convolutional neural networks serves as the foundation for the human detection framework. Channel and spatial correlation filter are employed by tracking algorithms to follow observed humans. As an extra piece of data, this system will produce, and export tracked movement on video. This tracked movement can be examined in more detail for future investigations into issues with surveillance cameras.

Block Diagram Mall television systems could be utilised to track customers' purchasing habits. Features such as the relationship with the shopping area, the head's position, the direction and speed of walking, and pauses that are thought to be related to the shopper's interest can be retrieved from the tracked journey [8]. After detecting interest, the following stage is to analyse the consumer's (non-verbal) behaviour to determine whether the shopper appreciates the focused products positively or negatively. The system's ultimate objective is to evaluate sales prospects by determining whether a client need assistance.

In this work, we outline our approach to creating such a system, which includes creating models of shopping behaviour, evaluating related aspects, and examining underlying technologies. We recorded in our shop lab to collaborate our observations. Next, we go into the tracking technology that was employed and the outcomes of the trials [9].

MOTIVATION

In recent times, video surveillance has become very complex in nature. With the advancement in technology, it has become more troublesome to analyze human actions and other object behaviors for analyzing patterns for threat detection and prevention of any kind of suspicious activities.

METHODS

Architecture

Data Cleaning: Data cleaning is the process of sanitizing the information gathered from the website. Checking the circumstances and frequency is the first step. System architecture model is shown in Figure 1. The message may consist of a single word or an n-gram. The quote's letters should all be condensed into a single letter, like lowercase or lowercase.

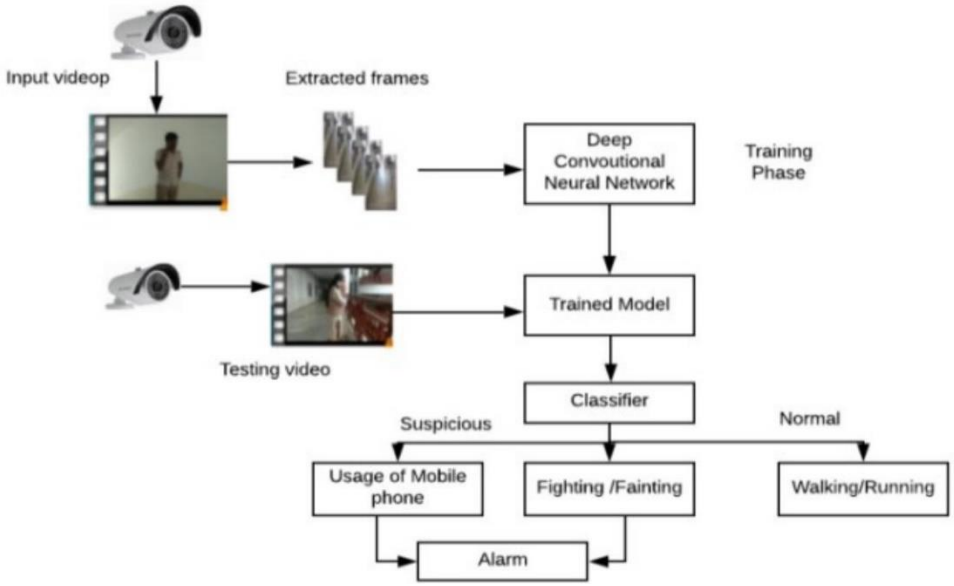

Figure 1. System architecture model.

Initially, we take the frames out of the input and feed them to Deep Neural Convolutional Networks, which feed them to the training model. The training phase includes the complete process of receiving input and extracting features. Testing video is fed through the trained model once the training phase is complete, and the input sample is classified as either suspicious or typical activity. The trained model will warn the relevant authorities if it notices questionable activity so they may act quickly and prevent unintended effects [10]. Login and Registration can be done as shown in Figures 3 and 4.

RESULT AND ANALYSIS

Almost everyone in the modern world understands the value of CCTV footage, however most of the time, these recordings are utilized for investigative purposes following a crime or occurrence. Project's Landing page is shown in Figure 2. One advantage of the suggested model is that it deters crime before it occurs. The CCTV footage captured in real time is being monitored and examined.

The analysis conclusion is a directive to the appropriate authority to take appropriate action should the conclusion suggest that an undesirable incidence will occur. Thus, we can put an end to this.

APPLICATIONS

Because deep learning, a subset of machine learning, offers great accuracy in object recognition and activity detection, it has completely changed the video surveillance industry. The following are some uses of deep learning for identifying questionable behaviour in surveillance footage:

1. *Object Detection:* Deep learning algorithms can be used to recognise suspicious activities by

identifying items in surveillance footage, such as people, cars, and weapons.

2. *Activity Recognition:* Deep learning models can identify odd or suspicious behaviours as well as human movements like walking, running, and leaping.
3. *Anomaly Detection:* Deep learning algorithms can identify odd or anomalous behaviour, such as lingering in a prohibited area or going somewhere they shouldn't.
4. *Facial Recognition:* Using deep learning techniques, facial recognition software can recognise people in surveillance videos and compare their information to a database of suspected criminals.
5. *Predictive Analytics:* By analysing vast volumes of surveillance data, deep learning models can forecast the locations and times of suspicious activities, enabling the taking of preventative action.
6. *Real-Time notifications:* When suspicious activity is discovered, deep learning algorithms can deliver real-time notifications that enable prompt action and the avertance of criminal activity.

Figure 2. Project's Landing Page.

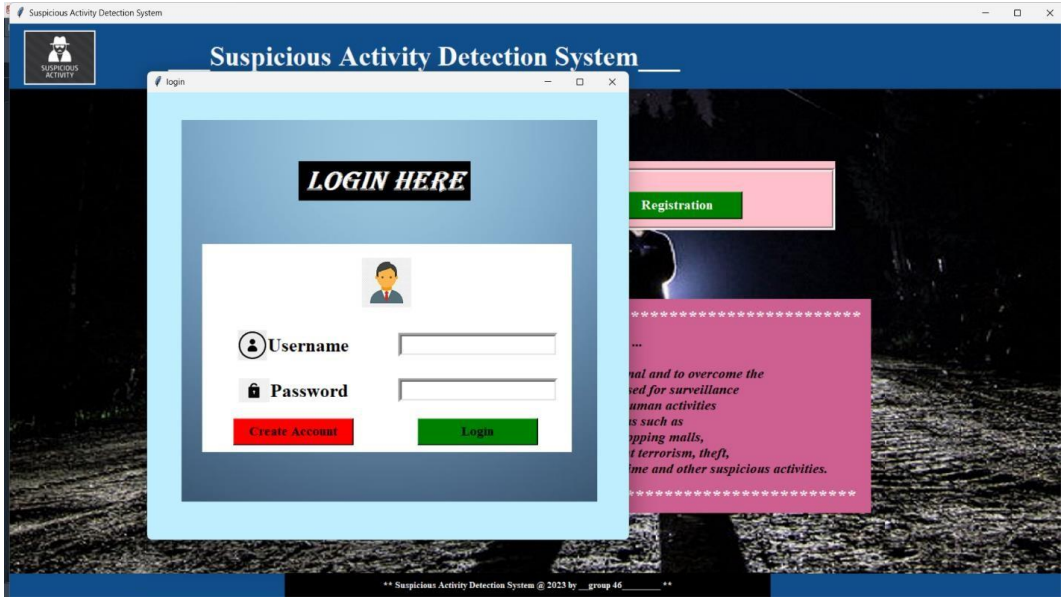

Figure 3. Login Window Page.

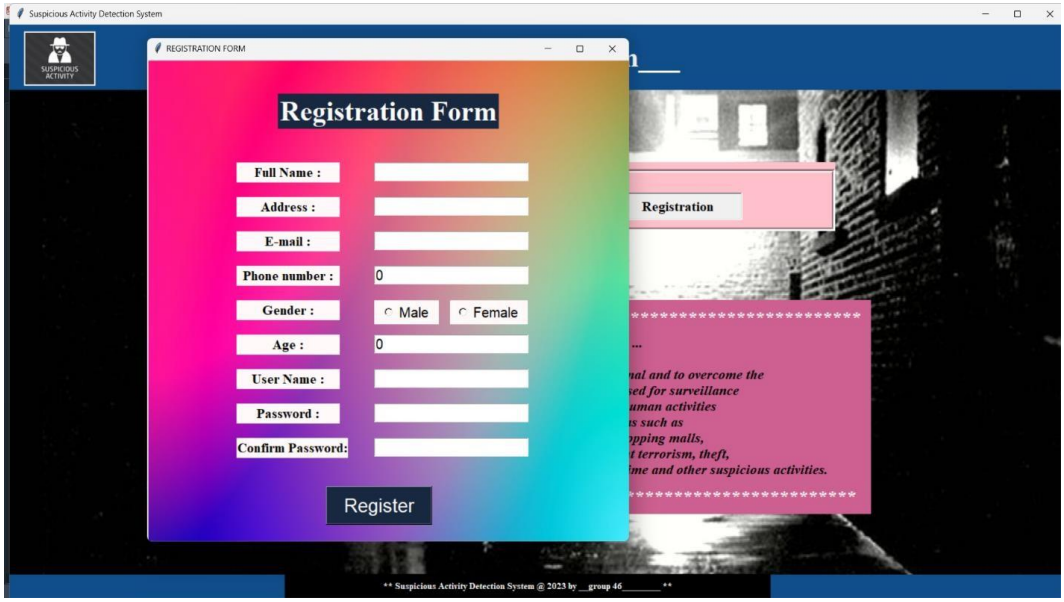

Figure 4. Registration Window Page.

CONCLUSION

Almost everyone in the modern world understands the value of CCTV footage, however most of the time, these recordings are utilised for investigative purposes following a crime or occurrence. One advantage of the suggested model is that it deters crime before it occurs. The CCTV footage captured in real time is being monitored and examined.

The analysis conclusion is a directive to the appropriate authority to take appropriate action should the conclusion suggest that an undesirable incidence will occur. Thus, we can put an end to this.The suggested method can also be used to anticipate more suspicious behaviour in public or private settings, despite some of its drawbacks. Any situation where training should be provided with suspicious activity appropriate for that scenario can use the model.

Future Works

This approach can be used in various future works for the detection of suspicious activities from surveillance films as deep learning continues to advance. The following are some possible study topics:

1. *Enhanced Object Recognition:* Deep learning methods like convolutional neural networks (CNNs) and object identification algorithms can be used to increase the accuracy of object recognition algorithms.
2. *Multi-Modal Analysis:* The accuracy of detecting suspicious activity can be increased by integrating data from several sources, including text, audio, and video.
3. *Better anomaly detection:* Deep learning models can be trained to identify more intricate and subtle anomalies in video material, like aberrant facial expressions or odd gait patterns.
4. *Human-in-the-Loop:* By adding human input to the deep learning system, it is possible to increase accuracy and decrease false positives, which in turn can aid in the more accurate identification of suspicious activity.
5. *Real-Time Adaptation:* Develop deep learning models that are capable of learning and changing on the fly. For instance, these models should be able to identify anomalous behaviour in people in real-time, even in the absence of prior knowledge.
6. *Adversarial Attacks:* To avoid false positives or false negatives in the detection of suspicious activity, it can be crucial to build models that are resistant to adversarial attacks.

Acknowledgments

It is indeed a great pleasure and moment of immense satisfaction for we to present project report on “DeepGuard: A Comprehensive Deep Learning System for Unmasking Suspicious Activities in

Surveillance Footage*"* amongst a wide panorama that provided us inspiring guidance and encouragement, we take the opportunity to thanks to thanks those who gave us their indebted assistance. We wish to extend our cordial gratitude with profound thanks to our internal guide Prof. SNEHAL RATHOD for his/her everlasting guidance. It was his inspiration and encouragement which helped us in completing our project. Our sincere thanks and deep gratitude to Head of Department, Prof. SHAILESH BENDALE and other faculty members and also to all those individuals involved both directly and indirectly for their help in all aspect of the project. At last but not least we express our sincere thanks to our Institute's Principal Dr. Shivprasad P. Patil, for providing us infrastructure and technical environment.

REFERENCES

1. S. Karuppuswami, M. I. M. Ghazali, S. Mondal, and P. Chahal, "Wireless eas sensor tags for volatile profiling in food packages," in 2018 IEEE 68th Electronic Components and Technology Conference (ECTC), pp. 2174–2179, 2018.
2. D. D. M. Dinama, Q. A'yun, A. D. Syahroni, I. A. Sulistijono, and A. Risnumawan, "Human detection and tracking on surveillance video footage using convolutional neural networks," in 2019 International Electronics Symposium (IES), pp. 534–538, 2019.
3. M. Popa, L. Rothkrantz, Z. Yang, P. Wiggers, R. Braspenning, and C. Shan, "Analysis of shopping behavior based on surveillance system," in 2010 IEEE International Conference on Systems, Man and Cybernetics, pp. 2512–2519, 2010.
4. N. Dawar and N. Kehtarnavaz, "Continuous detection and recognition of actions of interest among actions of non-interest using a depth camera," in 2017 IEEE International Conference on Image Processing (ICIP), pp. 4227– 4231, 2017.
5. C.-H. Chuang, J.-W. Hsieh, and K.-C. Fan, "Suspicious object detection and robbery event analysis," in 2007 16th International Conference on Computer Communications and Networks, pp. 1189–1192, 2007.
6. Y. Kaneko, "Fractal analysis of a grocery store shopping path," in 2016 2nd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE), pp. 1–7, 2015, IEEE Xplore.
7. H. Valecha, A. Varma, I. Khare, A. Sachdeva, and M. Goyal, "Prediction of consumer behaviour using random forest algorithm,"2019, 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), pp. 1– 6, 2018.
8. Y. Zuo, K. Yada, T. Li, and P. Chen, "Application of network analysis techniques for customer in-store behavior in supermarket,",2019, IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 1861–1866, 2018.
9. Y. Zuo and K. Yada, "Using statistical learning theory for purchase behavior prediction via direct observation of in-store behavior," in 2016, 2nd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE), pp. 1–6, 2015, IEEE Xplore.
10. S. Peker, A. Kocyigit, and P. E. Eren, "An empirical comparison of customer behavior modeling approaches for shopping list prediction," in 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp.1220–1225,IEEE Xplore.

