AI and Machine Learning for Remote Suspicious Action Detection and Recognition

Sreekanth Dekkati[1*], Sai Srujan Gutlapalli[2], Upendar Rao Thaduri[3], Venkata Koteswara Rao Ballamudi[4]

[1]Assistant Vice President (System Administrator), MUFG Bank, Arizona, **USA**
[2]Data Engineer, TechnoVision Solutions LLC, Farmington Hills, MI 48335, **USA**
[3]ACE Developer, iMINDS Technology Systems, Inc., Pittsburgh, PA 15243, **USA**
[4]Sr. Software Engineer, HTC Global Services, **USA**

[*]Corresponding Contact:
Email: sreekanthd041987@gmail.com

Manuscript Received: 10 Sept 2022
Revised Submission: 22 October 2022
Article Accepted: 29 October 2022

ABSTRACT

There is little question that the unchecked rise in population is to blame for the alarming increase in crime rates seen in industrialized and developing nations. As a direct consequence of this, there has been an increase in the number of calls for the use of video surveillance to address concerns about ordinary life and private property. As a consequence of this, we need a system that is capable of accurately recognizing human activity in real-time. Researchers have lately investigated machine learning and deep learning as potential methods for identifying human activities. To prevent fraud, we devised a technique that employs human activity recognition to examine a series of occurrences, evaluate whether or not a person is a suspect, and then take appropriate action. This system used deep learning to assign labels to the video based on human behavior. We can detect suspicious behavior based on the categories mentioned above of human activity and time duration by utilizing machine learning, which achieves an accuracy of around one hundred percent. This research article will detect suspicious behavior using optimal, effective, and quick methods. Using popular public data sets, the experimental findings described here highlight the approach's remarkable performance while only requiring a small amount of computational complexity.

Keywords: Behavior Recognition, Suspicious Action, Remote Areas, Machine Learning

INTRODUCTION

The goal of an automated surveillance system is to notify the personnel monitoring the system whenever a suspicious behavior that the user has predefined takes place (Amin & Mandapuram, 2021). Two challenges must be overcome before fully automated behavior recognition can be achieved. To begin, it is necessary to locate, classify, and keep track of persons and other items of interest in a scene as much as possible throughout the investigation. Second, an established method for describing the events (Gutlapalli et al., 2019). This is especially difficult for complex occurrences with various possible outcomes, such as a fight between two parties. They are, without a doubt, challenging to define in many different contexts.

The most significant limitation of machine learning is that it depends on using standard data sets during the training and testing phases (Ballamudi et al., 2022). These are difficult to come by, particularly for those with unique behavior. This is an essential factor to consider while determining the parameters and thresholds of the classifier. On the other hand, the semantic technique does away with the requirement for training in favor of a more fundamental process based on human thinking and logic (Mandapuram, 2017). This is the most reasonable and workable option. It removes the necessity, for instance, of specifying complex learning parameters such as decision-tree pruning thresholds, which are challenging to calibrate and require the assistance of industry professionals. In the semantic approach, these are substituted by parameters that are more readily apparent and meaningful (Bodepudi et al., 2019). This study presumes that the foreground blobs will be retrieved using a conventional background subtraction method for each picture. These blobs are the semantic entities that are the events that arescribed, and they represent the silhouettes of living (such as persons) and inanimate (such as baggage) elements in the scene. In actual use, however, a single blob can commonly represent many items, either occluding or standing quite close to one another. When all of the blobs have been extracted, the next step is to conclude how to segment, track, and classify the things those blobs represent. At this point, it is necessary to determine the nature of the peculiar occurrences (Desamsetti, 2016).

What a person does sheds light on who they are as a person, what their personality is like, and how their emotions are processed. Human Activity Recognition, also known as HAR, is essential to the suspect detection process (Bodepudi et al., 2021). HAR aims to recognize activities based on observations of individuals' actions and environmental factors. It is possible to categorize suspects in several ways, depending on characteristics such as criminal behavior, trends seen at the crime scene, and motive. Machine learning and deep learning algorithms can assess whether or not a crime scene is orderly and premeditated or whether or not it is disorganized and unplanned. Some relevant publications regarding classifying objects and recognizing human behavior from a video have been presented. These papers used Long Short-Term Memory networks in conjunction with convolutional neural network approaches. These papers were discussed using a computer vision approach. Another critical study, which provides an overview of various classification techniques for detecting human activities based on data from wearable inertial sensors, is also noteworthy. Recently, human activity recognition or the detection of suspects from video surveillance has become a hot topic of discussion in the study communities of image processing and computer vision (Thodupunori & Gutlapalli, 2018). Applying Deep Learning or Machine Learning can accomplish most of this work on HAR and suspicious detection. The author uses a sophisticated neural network to analyze the activities of many people within a single video frame. Security cameras may lag or encounter a delay because of the high-quality video processing, the time it takes for data to travel over the network, and the time it takes to access and present the feed on a screen. However, to limit the effects of such a problem, we presented a new architecture for our system. This new architecture can identify potentially suspicious behavior based on video footage in real-time and gives the most effective and reliable performance possible (Thaduri et al., 2016). In a general sense, we split the architecture of our system into two distinct pieces (Gutlapalli, 2017b). The first category of information is data based on videos, while the second category is data based on analyses of videos.

SUSPICIOUS BEHAVIOR DETECTION

The Fast Suspicious Behavior Detection component scans photos of people and objects and then analyzes those images to find suspicious behavior as quickly as possible (Gutlapalli, 2017a). The component makes monitoring operations more efficient, helps prevent accidents and crimes, and enables a rapid response to accidents and crimes when they do occur. Actlyzer, our behavior analysis tool, has the best level in the world for recognizing even the most subtle body elements. The technology enables us to distinguish frequent examples of conduct that could be considered suspicious, such as looking around, loitering, and intruding, from security camera footage in public spaces and other institutions. For example, looking around, loitering, and intruding are all examples.

Identify potentially troubling conduct and make monitoring activities more efficient.

This component is responsible for identifying individuals with suspicious behavior, such as loitering and looking around, and into restricted areas and committing violent crimes. It does away with the requirement for manual supervision and is capable of managing many cameras at once (Mandapuram et al., 2020). For instance, by utilizing a previously taught model of behaviors, you can identify suspicious behavior in real-time. This includes the detection of unauthorized item pickups, car break-ins, and incursions through windows and doors (Mandapuram et al., 2018). In addition, it is simple to modify and add new behaviors, including sophisticated behavior recognition, and very straightforward to use.

Enable a speedy response with notifications of potentially questionable conduct.

The dashboard will automatically sound an alarm if it identifies any behaviors that are considered suspicious (Desamsetti & Mandapuram, 2017). This system provides a chronological perspective of when and what types of suspicious behaviors have been noticed, and it facilitates immediate responses to avoid accidents and crimes. Additionally, it ensures that nothing is missed in the event of an accident or a crime, which enables the shortest possible response.

REVIEW RESULTS

Evaluating behavior recognition tests is difficult due to various difficulties operating on multiple levels (Dekkati & Thaduri, 2017). To begin, the most intriguing activities are complex, presenting a challenge in the setting with clutter. Another area for improvement is the limited availability of rigorous, professional, and high-quality data sets for testing (Reddy et al., 2020; Gutlapalli, 2016). In addition, the criteria for performance evaluation, like a standard measure, hit-and-miss weighting, and ground truth construction, are still up for discussion (Mandapuram & Hosen, 2018). As a result of these challenges, the experimental results reported in various articles throughout the body of research could be more consistent.

Unusual and Suspect Behavior Detection Methods Used in the Identification of Theft:

Installing CCTV cameras at your place of business or in your stores fitted with smart sensors and connected to AI-powered analysis will make it impossible for thieves to steal from you. Receive warnings in real time if theft is detected.

Unusual and Suspect Behavior Observation of Unwanted Loitering: The Loitering Detection model offered by Visionify is responsible for generating warnings based on the movement of objects and people. It can count loiterers, detect line crossings, recognize suspicions, resolve lineups, and do many other things.

Detection of Suspicious Activity Regarding Firearms and Knives: The firearm Detection model can determine whether or not knives and firearms are present in an area. When the system recognizes a weapon, alarms are triggered, and security personnel and the appropriate authorities are informed about the occurrence.

Unusual and Suspect Behavior Behavior Monitoring for Aggression Detection: Our analytics program listens for specific sound patterns that indicate compulsion, rage, verbal violence, or fear, and then sends an alarm to the security people so that any potential physical or verbal aggression can be avoided.

Unusual and Suspect Behavior Detection of Solicitation for Contribution: Determine which solicitation activities allow other competitors to get an unfair advantage over you. Our model for the identification of solicitation, which is integrated with your cameras, may help guarantee that distribution and solicitation are kept to a minimum.

Observation of Suspicious Behavior about Vandalism: Utilizing our Vision-AI system, you may identify individuals responsible for workplace vandalism. Based on the tape, workers and others implicated should be punished, appropriate steps should be taken, and losses should be recovered.

CONCLUSION

It is possible to anticipate an occurrence by observing suspicious movement or behavior in a person before the event takes place. Any examination of any given time or two or one activity based on the utilization of the most recent moment does not in any way imply that there will be criminal behavior in the foreseeable future.

Real-time performance, adaptability, resistance to clutter and nonlinearities in the camera, ease of interface with human operators, and the elimination of training requirements for machine-learning-based systems are some benefits that may be gained from the technology. Experiments were carried out on a wide variety of standard data sets that are accessible to the public, each of which had a different crowd density, camera angle, and lighting condition. The findings of the trials demonstrated that a significant number of the behaviors of interest were successfully identified.

To control all security systems, we want to experiment with a more significant number of activities, some of which will involve challenging physical challenges. In addition, we will deal with suspicious circumstances relating to the experiment. Incorporating additional camera kinds and analysis will allow us to broaden the scope of our data sets along other dimensions. The results of this system's analysis of human behavior for a select number of events and times are unreliable. As a result, the next challenge will be to monitor human behavior for extended periods to identify potentially suspicious conduct.

REFERENCES

Amin, R., & Mandapuram, M. (2021). CMS - Intelligent Machine Translation with Adaptation and AI. *ABC Journal of Advanced Research*, *10*(2), 199-206. https://doi.org/10.18034/abcjar.v10i2.693

Ballamudi, V. K. R., Desamsetti, H., & Mandapuram, M. (2022). Influence of Digitization on Human Resources (HR) Services and Processes. *ABC Research Alert*, *10*(3), 32–36. https://doi.org/10.18034/ra.v10i3.653

Bodepudi, A., Reddy, M., Gutlapalli, S. S., & Mandapuram, M. (2019). Voice Recognition Systems in the Cloud Networks: Has It Reached Its Full Potential? *Asian Journal of Applied Science and Engineering*, *8*(1), 51–60. https://doi.org/10.18034/ajase.v8i1.12

Bodepudi, A., Reddy, M., Gutlapalli, S. S., & Mandapuram, M. (2021). Algorithm Policy for the Authentication of Indirect Fingerprints Used in Cloud Computing. *American Journal of Trade and Policy*, *8*(3), 231–238. https://doi.org/10.18034/ajtp.v8i3.651

Dekkati, S., & Thaduri, U. R. (2017). Innovative Method for the Prediction of Software Defects Based on Class Imbalance Datasets. *Technology & Management Review*, *2*, 1–5. https://upright.pub/index.php/tmr/article/view/78

Desamsetti, H. (2016). Issues with the Cloud Computing Technology. *International Research Journal of Engineering and Technology (IRJET), 3*(5), 321-323.

Desamsetti, H., & Mandapuram, M. (2017). A Review of Meta-Model Designed for the Model-Based Testing Technique. *Engineering International*, *5*(2), 107–110. https://doi.org/10.18034/ei.v5i2.661

Gutlapalli, S. S. (2016). Commercial Applications of Blockchain and Distributed Ledger Technology. *Engineering International*, *4*(2), 89–94. https://doi.org/10.18034/ei.v4i2.653

Gutlapalli, S. S. (2017a). The Role of Deep Learning in the Fourth Industrial Revolution: A Digital Transformation Approach. *Asian Accounting and Auditing Advancement*, *8*(1), 52–56. Retrieved from https://4ajournal.com/article/view/77

Gutlapalli, S. S. (2017b). An Early Cautionary Scan of the Security Risks of the Internet of Things. *Asian Journal of Applied Science and Engineering*, *6*, 163–168. https://ajase.net/article/view/14

Gutlapalli, S. S., Mandapuram, M., Reddy, M., & Bodepudi, A. (2019). Evaluation of Hospital Information Systems (HIS) in terms of their Suitability for Tasks. *Malaysian Journal of Medical and Biological Research*, *6*(2), 143–150. https://doi.org/10.18034/mjmbr.v6i2.661

Mandapuram, M. (2017). Security Risk Analysis of the Internet of Things: An Early Cautionary Scan. *ABC Research Alert*, *5*(3), 49–55. https://doi.org/10.18034/ra.v5i3.650

Mandapuram, M., & Hosen, M. F. (2018). The Object-Oriented Database Management System versus the Relational Database Management System: A Comparison. *Global Disclosure of Economics and Business*, *7*(2), 89–96. https://doi.org/10.18034/gdeb.v7i2.657

Mandapuram, M., Gutlapalli, S. S., Bodepudi, A., & Reddy, M. (2018). Investigating the Prospects of Generative Artificial Intelligence. *Asian Journal of Humanity, Art and Literature*, *5*(2), 167–174. https://doi.org/10.18034/ajhal.v5i2.659

Mandapuram, M., Gutlapalli, S. S., Reddy, M., Bodepudi, A. (2020). Application of Artificial Intelligence (AI) Technologies to Accelerate Market Segmentation. *Global Disclosure of Economics and Business* *9*(2), 141–150. https://doi.org/10.18034/gdeb.v9i2.662

Reddy, M., Bodepudi, A., Mandapuram, M., & Gutlapalli, S. S. (2020). Face Detection and Recognition Techniques through the Cloud Network: An Exploratory Study. *ABC Journal of Advanced Research*, *9*(2), 103–114. https://doi.org/10.18034/abcjar.v9i2.660

Thaduri, U. R., Ballamudi, V. K. R., Dekkati, S., & Mandapuram, M. (2016). Making the Cloud Adoption Decisions: Gaining Advantages from Taking an Integrated Approach. *International Journal of Reciprocal Symmetry and Theoretical Physics*, *3*, 11–16. https://upright.pub/index.php/ijrstp/article/view/77

Thodupunori, S. R., & Gutlapalli, S. S. (2018). Overview of LeOra Software: A Statistical Tool for Decision Makers. *Technology & Management Review*, *3*(1), 7–11.

--0--