IJARSCT



International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 4, Issue 1, April 2024

Crime Activity Detection System

Fija Sayyad¹, Puja Parasur², Sarala Chattar³, Dnyaneshwari Rakshe⁴, Prof. Dipali Dube⁵

Students, Department of Computer Engineering^{1,2,3,4}
Professor, Department of Computer Engineering⁵
Vidya Niketan College of Engineering, Ahmednagar, Maharashtra, India
fijasayyad2001@gmail.com, pujaparasur30@gmail.com, saralachattar@gmail.com
dnyaneshwari55@gmail.com, dipalidube555@gmail.com

Abstract: Video Surveillance plays a pivotal role in today's world. The technologies have been advanced too much when artificial intelligence, machine learning and deep learning pitched into the system. Using above combinations, different systems are in place which helps to differentiate various crime behaviors from the live tracking of footages. The most unpredictable one is human behavior and it is very difficult to find whether it is detecting crime or not. Deep learning approach is used to detect crimeor normal activity in an academic environment, and which sends an alert message to the corresponding authority, in case of predicting a crime activity. Monitoring is often performed through consecutive frames which are extracted from the video.

Keywords: Deep Learning, Crime detection, CNN, image processing etc.

I. INTRODUCTION

In most nations, it is the job of the police to find criminal activity, while specialised enforcement organisations may be tasked with finding certain kinds of criminal activity. The recognition of a crime as having been committed, the identification of a suspect, and the gathering of adequate evidence to bring the suspect before a court are the three distinct stages of crime detection. Other than the police, many crimes are detected and reported. Certain crimes, especially those that require a subject's consent, like the sale of illegal drugs or prostitution, or those in which there may be no clearly defined victim, like obscenity, are frequently not identified until the police take proactive measures to ascertain whether they have been committed. To detect such crimes, therefore, controversial methods are sometimes required (e.g., Elec- tonic eavesdropping, surveillance, interception of communications, and infiltration of gangs).

II. LITERATURE REVIEW

This chapter will provide research of different paper, including author requirements, research perspective, and overview of project idea, general constraints. In addition, it will also provide the information of algorithm and functionality needed for this system - such as algorithm, tech- niques, functional requirements and performance requirements. With the event of Information and Communication Technology, various varieties of information security threats may be seen. In this paper, Umair Muneer Butt et al. [1Real-Patio-Temporal Crime Hostspot Detection Prediction:The Authors were unable to find a comprehensive study on crime hotspot detection and predetection while conducting this SLR.

Lijun Cai*1, Dian Li2 and YuYu Wang3 et al. [2] Network Crime information Retrieval Frame Work based on Facial Image Recognition:Network crime information retrioval framework based on facial image recognition is designed in this article. Due to the intel Facial Image licence and profess- singlism of crime methods, the variety of crime final methods, and the high degreen of concealment of crimes, the detection of cybercrime is much more difficult than traditional cases, which brings great difficulty to the investigation of the case which leads to the detection with low rate. Qingcheng Yuet et al. [4] Design of Crossborder Network Crime Detection System Based on PSE and Big Data Analysis:In order to speed up the detection of cybercrime worldwide, a new crossborder cybercrime detection system is designed by introducing the PSE the- or and the prince- plex of big data analysis. In the TFTP server, the U-boot network development board and OpenStack crime information detection com- ponente are con- nested to build the hardware running environment of the cross border network crime detection system.

DOI: 10.48175/IJARSCT-16910

Copyright to IJARSCT www.ijarsct.co.in

58

IJARSCT



International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

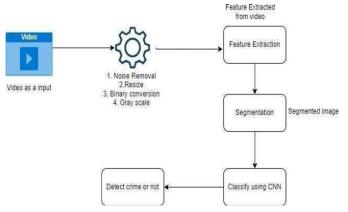
Impact Factor: 7.53

Volume 4, Issue 1, April 2024

By Luca Amaro, et al. [5] Abnormal New Logic Synthesis as Nanotechnology fogy Enabler: Nanoelectronics comprises a VArite of devices whose electrical properties are more complex as compared to CMOS, thus enabling new compute- tonal paradigms. The potentially large space for innovation has to explored in the search for technologies that can support large-scale and hithertominee circuit design. Within this space, we analyse a set of emerge in technologies characterized by a similar computational abstraction at the design level, i.e., a binary comparador or a majority voter. Zijin Wu et al. [6] Optimal Control of Multiroom HVAC System: An Event Based Ap- preach: Building energy saving is of great practical interest due to the increase- in energy consumption in build- ins. The optimal control of the heating, ventilation, and airconditioning (HVAC) systems leads to great energy saving potential. How- ever, this problem is chalk- longing due to the exponentially increasing state space and policy space. In this brief, we consider this important problem and make the follow- in major contributions.

Erin Kushan et al. [7] Financial Crime Fraud DetectionUsing Graph Computing: In recent years, the unprecedented growth in digital payments fuelled consequential changes in fraud and financial crimes. In this new landscape, tradetonal fraud detection approaches such as rule-based endgenes have largely become infecttie. AI and machine learning soultons using graph computing printcripples have gained significant intersest. Graph neural networks and emerging adaptive so- lotions provide compelling opportunities for the future of fraud and financial crime detection.

III. SYSTEM ARCHITECTURE



IV. EXPERIMENTAL METHODOLOGY

Module

Data is interpreted and analyzed using Deep Learning. It can also classify patterns and model data. It enables decisions to be made that would otherwise be impossible to make using routine systems, while saving time and effort.

- Using data mining, a large amount of raw crime activity data is transformed into information that can be used to make better decisions and predictions.
- The proposed system employs Deep Learning algorithms such as CNN. We must upload the Crime Activity video Dataset and train the model using a CNN technique in the proposed system.
- We are aware that we are performing data processing functions on the system, so we employ three data
 processing modules: pre-processing, feature extraction, and classification, each of which employs a different
 algorithm
- Then, build a model and assess its effectiveness. You can Detect crime activity using this model.

Tools and Technology Used:

Machine Learning: Supervised machine learning models are trained with labeled data sets, which allow the models to learn and grow more accurate over time. For example, an algorithm would be trained with pictures of dogs and other things, all labeled by humans, and the machine would learn ways to identify pictures. There are many applications and companies that used machine learning for doing their day to day process as it is being more accurate and precise than

Copyright to IJARSCT DOI: 10.48175/IJARSCT-16910 2581-9429 JARSCT 59

IJARSCT



International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 1, April 2024

manual interventions. Simply put, machine learning allows the user to feed a computer algorithm an immense amount of data and have the computer analyze and make data-driven recommendations and decisions based on only the input data.

Algorithm used:

CNN Algorithm If you are writing a project report on the CNN algorithm, here are some key points you can include: Introduction: Start by introducing the topic of deep learning and the importance of convolutional neural networks for image processing and computer vision.

- **Architecture:** Describe the architecture of the CNN algorithm, including the different types of layers and their functions. Explain how the convolutional layers extract features from the input image, how the pooling layers down sample the feature maps, and how the fully connected layers perform the final classification.
- Training: Explain how the CNN algorithm is trained on a large dataset of labeled images, using back propagation to optimize the network parameters for accu- rate predictions. Discuss the importance of data preprocessing, regularization, and hyperparameter tuning for improving the performance of the network.
- Applications: Describe some of the real-world applications of the CNN algorithm, such as object detection, image classification, and image segmentation.
- Challenges and Future Directions: Discuss some of the challenges and limitations of the CNN algorithm, such as the need for large amounts of labeled data, the potential for overfitting, and the difficulty of interpreting the learned features. Identify some of the future directions for research in CNNs, such as improving the efficiency of training and inference, developing more interpretable models, and applying CNNs to new domains such as natural language processing.

V. CONCLUSION

In Present world, almost all the people are aware of the importance of CCTV footages, but most of the Cases these footage are being used for the investigation purposes after a crime /incident have been happened. The Proposed model has the benefit of Stopping the crime before it happens. The real time CCTV footages are being Tracked and Analyzed. The result of the analysis is a command to the respective authority to take an action if in case the result Indicates an unto word incident is going to happen. Hence this case is stopped.

REFERENCES

- [1]. Bhagya Diva, Shalini, Deepa, Baddeley Saravia Reddy, "Inspection of suspicious human activity in the crowdsourced areas captured in surveillance cameras", International Research Journal of Engineering and Technology (IRJET), December 2017.
- [2]. F. Yuan, "An integrated fire detection and suppression system based on widely available video surveillance," Mach. Vis. and Apps., vol. 21, pp. 941–948, 2010.
- [3]. Y. Luo, L. Zhao, P. Liu, and D. Huang, "Fire smoke detection algorithm based on motion characteristic and convolutional neural networks," Multimedia Tools and Applications, pp. 1–18, 2017.
- [4]. S. Guler and M. K. Farrow, "Abandoned Object Detection in Crowded Places," 9th IEEE International Workshop on PETS, 2006.
- [5]. L. A. Lim and H. Y. Keles, "Foreground Segmentation Using a Triplet Convolutional Neural Network for Multiscale Feature Encoding".
- [6]. A., Singh, M., Bhatia, K., Kumar, A., Jain, P., and Varma, M. (2018). Fastgrnn: A fast, accurate, stable and tiny kilobyte sized gated recurrent neural network. In Advances in Neural Information Processin Systems, pages 9017-9028
- [7]. U.M. Katha, C.G. Patil "Suspicious Activity Recognition in Video Surveillance System", Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018.
- [8]. Zahraa Kain, Abir Youness, Ismail El Sayad, Samih Abdul-Nabi, Hussein Kassem, "Detecting Abnormal Events in University Areas", International conference on Computer and Application

Copyright to IJARSCT www.ijarsct.co.in

DOI: 10.48175/IJARSCT-16910

2581-9429

IJARSCT