V I S V E S V A R A Y A T E C H N O L O G I C A L U N I V E R S I T Y

" J N A N A S A N G A M A " B E L A G A V I – 5 9 0 0 1 8

THE SYNOPSIS REPORT ON

"Detecting Criminal Activities from CCTV by using Object detection and machine Learning Algorithms"

BACHELOR OF ENGINEERING

IN

INFORMATION SCIENCE AND ENGINEERING

PROJECT ASSOCIATES

Name	USN
Shreya	4GM20IS046
Bhoomika GB	4GM20IS008
Kavana M	4GM20IS026
Bhuvana BG	4GM20IS009

GUIDE

Miss.Nasreen Taj

HEAD OF THE DEPARTMENT

Dr. Sunil Kumar BS

S r i s h y l a E d u c a t i o n a l T r u s t ® , B h e e m a s a m u d r a

GM INSTITUTE OF TECHNOLOGY

(Affiliated to VTU Belagavi, Approved by AICTE, New Delhi & Govt. of Karnataka)

Post Box No: 4 P.B. Road, Davangere-577006, Karnataka

Phone: 08192-252560,233377, 252777, Tel/Fax: 08192 233344

ABSTRACT

Now, a day's Crime in every country is increasing day by day. Generally, Every day we listen to the news of different crimes of different categories like rape, assault, Kidnapping ,Robbery ,ATM Theft, Murders etc happening in different states, cities , countries. Almost all the newspapers, TV channels', social media are filled with the news of Criminal activities happening all around the Whole World. In earlier times there is no method to detect Crime. After That the CCTV cameras were used to detect Crimes. But Watching these Videos manually by humans for detecting crimes is a very time Consuming process especially in today's world of Artificial Intelligence and Machine learning . So this crime detection in CCTV surveillance becomes an important area of research in the field of machine learning. So, there is a very urgent need of the intelligent system which will detect the crimes from the real time CCTV Feed and classify them and provides an alert system to the nearest police stations and ambulances etc. So, that system will help in reducing the crime rate in any country. This paper reviews all prior research in this area, including approaches for object recognition and finding priority frames, techniques and algorithms like Yolo used to detect crimes , various datasets used and algorithms used to analyze crime data and train the dataset .

CONTENTS

CHAPTER-1

INTRODUCTION

Artificial Intelligence and Machine Learning are associated with human Intelligence and natural intelligence . Intelligence means the ability to think, learn and understand something . Human intelligence is the ability of the humans to think creative, understands something, learn from concepts and solve problems. Artificial intelligence is the ability of the machines to think creative, understand and analyze something or in other words ability of the machines to perform tasks like humans and think just like a human does. Artificial intelligence uses machine learning algorithms in python to train the systems and machines to think and perform like humans. Machine Learning is a branch of AI. Machine learning is the ability of the systems or Machines to automatically learn and improve from past experiences without being explicitly programmed . For Example alexa and Siri are AI based systems which we use in our daily based life. Other examples include google home and self driving tesla cars . The main purpose of AI and ml based applications and systems is to develop various applications and intelligent systems that reduce human efforts and time by automating the system. AI and Machine based systems are almost developed in every sector such as aviation, healthcare, transportation, education, medical, electronic trading, remote sensing, education, banking and finance , crime and Object detection. But In this review paper we are going to discuss only about the Crime detection and object detection methods and the approach to develop the intelligent video surveillance system. But before discussing Crime and object detection methods firstly we will discuss why this topic is important for research and why we need to develop this intelligent surveillance system. From past few years Crime and violence rate has increased all over the country in various categories like ATM Robbery , Murders, rape , assault etc specially the crime against women has been increased. In some states the crime has increased a lot like UP, Delhi, Assam etc. The states with the highest rates of violent crime are Bihar, Jharkhand, Odisha, West Bengal, Assam, Tripura, Arunachal Pradesh, Delhi, Haryana, Maharashtra, and Madhya Pradesh . In 2022, UP has the highest rape and murders rate . The per capita crime rate of UP is 7.4. According to the National Crime Records Bureau, this ratio means that Uttar Pradesh has the highest number of crimes, and thus, the state is unsafe to travel alone. So, in order to address these concerns and to reduce crime to some extent now days CCTV Cameras are now installed in almost every Crime prone area

1.1 LITERATURE SURVEY

In the subject of criminal detection, creating an intelligent surveillance system has been a significant study topic. Many studies have been conducted in this area, ranging from activity recognition to object detection.However, the majority of currently conducted research focuses on special high dimensionality or anomaly detection characteristics. As an example, a project examined various anomaly detection techniques in order to provide a basic understanding of the various approaches to anomaly detection. Numerous graph-based applications in the actual world are examined in another study. To identify unresolved problems and difficulties, a fresh survey of hybrid intrusion detection systems and anomaly detection systems was carried out. There has been some study linking anomaly detection to high dimensionality issues, either directly or indirectly To specifically address specific imaging issues, a number of recent techniques recommend CNN . Deblurring has been suggested for a network that is similar to a one-iteration ODP network and uses a single, studied deconvolution step followed by a CNN. For describing such unforeseen events, such as anomaly in complex scenes, a real-time anomaly detection and localization technique was developed in 2015. Our method uses two local and global descriptors to describe each video as a collection of nonoverlapping cubic patches (13).. After studying a lot of research papers on it the previous research and studies suggests that the existing system of the automated CCTV monitoring system is not very good at giving decisions and correct responses that are appropriate for the circumstances. Videos produced by CCTV cameras located within the ATM Or if the video required a lot of manual labour to watch it. Just in case there was an ATM heist, it became time-consuming to watch the entire, lengthy movie. Weixin Luo and Wen Liu suggested Temporally Coherent Sparse Coding (TSC) in one of their papers in 2017, motivated by the capacity to identify sparse data. The suggested technique uses identical neighbouring frames with comparable reconstruction coefficients to address the coding-based anomaly. The suggested method then uses a particular variety of stacked recurrent neural network to map the TSC (sRNN). By using sRNN to learn all parameters simultaneously, it is possible to avoid the nontrivial selection of hyper-parameters for TSC, and The computation required for learning is reduced since the reconstruction coefficients can be deduced inside a forward passage with a shallow sRNN. The CNN model's output effectively extracted suspicious activity frames from a lengthy movie, sending those suspicious frames into a neural network structure. The main goal of this research is to create summaries of films in order to be able to extract the most important information from them and shorten their length. The can be used to find strange events in videos method that Yong Sheen Chong and Yong Haur Tay demonstrated. Gaurav Kumar Sinand Vipin Shukla released a paper in 2020 titled "Automatic Alert of Security

Threat utilising Video Surveillance System." . This paper suggests a technique for using sensor systems that can alert on the existence of any suspicious activity. Sensors record events, but no information is provided about them. Analyzing the captured footage enables quick and accurate information gathering regarding the threat and its fundamental cause in order to take preventative action. As a result, it's probable that deploying CCTV camera and sensor systems alone or in combination won't be sufficient to quickly identify harmful events. They consequently developed a system that employs cameras and sensor networks to swiftly detect threats in various lighting conditions. Kooij et al use of visual and audio data from surveillance videos allowed them to identify hostile behaviour. To evade tracking, several writers have proposed and employed a number of strategies. Motion patterns , histogram-based methods , social force models , topic modelling , and context-driven techniques are all methods for learning global motion patterns. are a few examples of these difficulties in obtaining trustworthy tracks. To create a a surveillance infrastructure based on deep learning that uses object detection a Deep Learning-based surveillance framework using object detection was implemented, according to a piece written by Bharath Raj. The majority of studies have created strategies for instructing the distribution of typical movements through practise using already-existing recordings, according to the literature analysis carried out thus far.They have made an effort to recognise low partable patterns and classify them as anomalies. Some researchers have demonstrated that sparse matrices are more efficient in solving computer vision- related tasks Moreover, certain patterns that result in a sizable restoration error are labelled as abnormal during testing. Deep learning has shown to be the most efficient technique for classifying images, making it suitable for classifying video material.Deep convolutional neural networks are now widely used in the literature for object detection and localization with class-specific bounding boxes. However, still there is not clear method of finding frames from videos in any of these previous researches. According to this study, the uncertainty surrounding this field of study is the root of a lot of difficulties. There are many problems and most of the related concepts related to the problems are not explained clearly in previous researches for example:

- No particular algo or method was proposed to detect frames. So there is difficulty in getting time frames of the suspicious action in a video and it’s also difficult to train very large amount of dataset to improve accuracy of predicting Crime.
- The system may face difficulty in detecting similar types of crime and non crime videos.
- The quality of the image and camera resolution has an impact on the system's ability to forecast out In scenarios with a lot of people, it can be challenging to predict any activity.

1.2 PROBLEM STATEMENT

In earlier times there is no method to detect Crime. After That the CCTV cameras were used to detect Crimes. But Watching these Videos manually by humans for detecting crimes is a very time Consuming process ly in today's world of Artificial Intelligence and Machine learning .So this crime detection in CCTV surveillance becomes an important area of research in the field of machine learning."

1.3 OBJECTIVES

The objective of using Object Detection and Machine Learning Algorithms for detecting criminal activities from CCTV footage is to enhance the security and safety of a given area or environment. The system aims to automatically identify and flag suspicious or potentially criminal behavior captured by the cameras, allowing for timely intervention and response. Here are the key objectives for this problem statement:

Real-Time Detection: Implement a system that can analyze live CCTV footage in real-time, ensuring that suspicious activities are identified promptly.

Object Recognition: Utilize object detection algorithms to accurately identify and classify objects and people in the video frames. This includes recognizing common objects, as well as distinguishing between different types of objects (e.g., humans, vehicles, weapons).

Anomaly Detection: Employ machine learning techniques for anomaly detection to identify unusual behavior or activities that deviate from normal patterns. This can include behaviors such as loitering, aggressive movements, or suspicious interactions.

Alerting Mechanism: Implement a notification system that generates alerts or alarms when potentially criminal activities are detected. These alerts should be sent to designated personnel or authorities for immediate action.

Scalability: Ensure that the system is capable of handling a large number of CCTV cameras simultaneously, allowing for effective monitoring of a wide area.

Integration with Existing Security Infrastructure: Enable seamless integration with existing security systems, such as alarms, access control, and monitoring centers, to create a comprehensive security solution.

Privacy Compliance: Design the system with privacy considerations in mind, ensuring that it complies with legal and ethical standards for video surveillance and data handling.

Accuracy and Reliability: Strive for high accuracy in object detection and anomaly recognition to minimize false positives and negatives. This helps in reducing unnecessary alerts and ensuring that actual criminal activities are not missed.

Customizable Rules and Thresholds: Allow for the customization of detection rules and thresholds based on specific requirements and the nature of the monitored environment.

Historical Analysis and Reporting: Provide the capability to review past footage and generate reports summarizing detected activities. This can be valuable for post-incident analysis and for identifying trends or patterns over time.

User-Friendly Interface: Create a user-friendly interface for security personnel to monitor the system, review alerts, and take appropriate action.

Continuous Improvement and Maintenance*: Establish a feedback loop for system performance and conduct regular updates to incorporate advancements in object detection and machine learning techniques.

The system aims to enhance the security infrastructure and response capabilities of the monitored environment, detecting criminal activities and ensuring the safety of the area under surveillance.

1.4 SCOPE OF THE PROJECT

The scope of the project "Detecting Criminal Activities from CCTV using Object Detection and Machine Learning Algorithms" involves various components and considerations. Here are the key aspects to consider within the scope:

Camera Installation and Configuration:

- Determine the number and placement of CCTV cameras for optimal coverage of the monitored area.
- Ensure proper camera configurations, including angles, zoom levels, and lighting conditions.

Video Feed Acquisition:

- Establish a mechanism to collect and process video feeds from the CCTV cameras. This may involve hardware and software integration to access the video streams.

Object Detection and Recognition:

- Implement object detection algorithms to identify and classify objects and individuals in the video frames. Common objects of interest may include humans, vehicles, bags, etc.

Anomaly Detection:

- Develop machine learning models to recognize unusual or suspicious behavior within the video footage. This could involve identifying actions like loitering, aggressive movements, or interactions that deviate from normal patterns.

Real-Time Processing:

- Ensure that the system can process video feeds in real-time, allowing for immediate detection and response to potentially criminal activities.

Alerting Mechanism:

- Implement a notification system to generate alerts when suspicious activities are detected. This may include emails, SMS messages, or notifications sent to a monitoring dashboard.

Integration with Security Infrastructure:

- Integrate the system with existing security infrastructure, including alarm systems, access control mechanisms, and monitoring centers. This ensures a cohesive security solution.

Privacy and Compliance:

- Adhere to legal and ethical standards for video surveillance and data handling. Ensure compliance with privacy regulations and obtain any necessary permissions or consent.

Performance Metrics:

- Define and measure performance metrics, such as accuracy of object detection, false positive/negative rates, and response time.

Scalability:

- Design the system to handle a scalable number of cameras and concurrent video streams to accommodate different environments and sizes.

User Interface:

- Develop a user-friendly interface for security personnel to monitor the system, review alerts, and take appropriate actions.

Historical Analysis and Reporting:

- Provide capabilities to review past footage, generate reports, and analyze trends or patterns in detected activities.

Training and Testing Data:

- Gather and annotate a diverse dataset for training and testing the machine learning models. This dataset should encompass a variety of scenarios and activities.

Continuous Improvement and Maintenance:

- Establish a feedback loop for system performance and conduct regular updates to incorporate advancements in object detection and machine learning techniques.

Documentation and Knowledge Transfer:

- Create comprehensive documentation detailing the system architecture, algorithms used, configurations, procedures. Additionally, ensure knowledge transfer to relevant stakeholders.

CHAPTER-2

PROJECT MANAGEMENT

2.1 METHODOLOGY

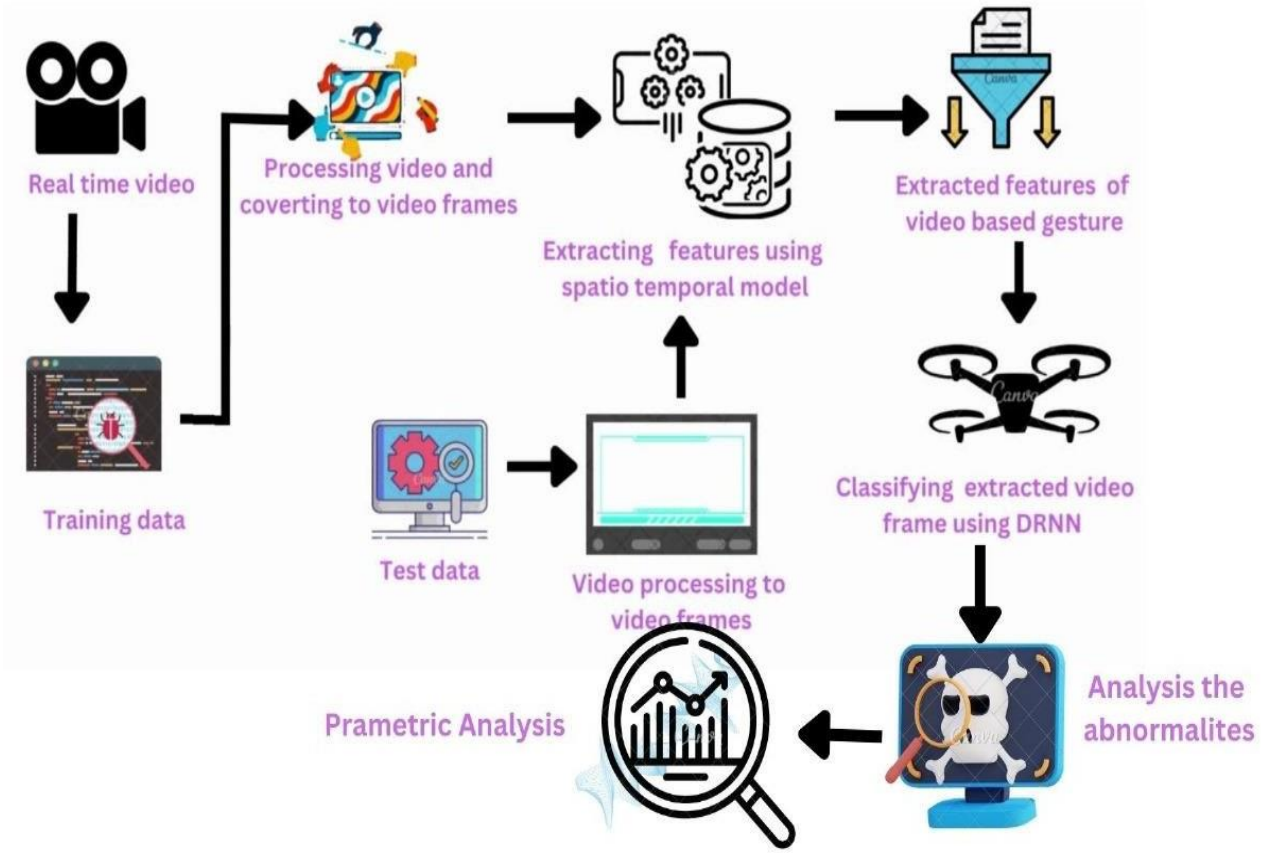

Fig 2.1 represents methodology of criminal activities through cctv using machine learning and object detection

Applications in various areas, including crime prevention, automatic smart visual monitoring and road safety, need for considerable attention to anomaly in event detection in video surveillance. In recent decades, an enormous number of surveillance cameras are installed in both private and public locations for effective real-time monitoring to prevent malfunctions and protect public safety . Most cameras, however, offer just passive logging services and are not capable of

monitoring. The number of these films grows every minute, making it easy for human specialists to comprehend and analyses them. Similarly, monitoring analysts have to wait hours for abnormal occurrences to be captured or seen for immediate reports .

Because there are few anomalous events in the real world, video anomaly detection are studied as a one-class issue, in which the model is trained on typical films and a video is tagged as anomalous when odd patterns appear. All the typical real-world monitoring events cannot be cumulated in one dataset. Different typical actions may thus be distracted from regular training events and may ultimately produce false alarms . In contemporary human action recognition research, notably in video surveillance, violence detection has been a hot area. The classification of human activity in real time, nearly instantaneously after the action has occurred, is one of the challenges with human action recognition in general. This difficulty escalates when dealing with surveillance video for a number of factors including the quality of surveillance footage is diminished, lighting is not always guaranteed, and there is generally no contextual information that can be used to ease detection of actions and classification of violent versus non-violent. Furthermore, in order for violent scene detection to be helpful in real-world surveillance applications, the identification of violence must be speedy in order to allow for prompt intervention and resolution. In addition to poor video quality, violence can occur in any given setting at any time of day, therefore, a solution will have to be robust to detect violence no matter the conditions. Some settings for video surveillance where violence detection can be applied includes the interior and exterior of buildings, in traffic, or on police body cameras .

A major purpose of video surveillance is the detection of unusual situations such as traffic accidents, robberies, or illicit activity. Human operators and manual examination are still required by most existing monitoring systems (prone to disturbances and tiredness). As a result, effective computer vision techniques for automatically detecting video anomalies/violence are becoming increasingly relevant. Building algorithms that detect specific anomalous occurrences, such as violence detectors, fight action detectors, and traffic accident detectors, is a tiny step toward resolving detection of anomalies. In recent years, video action recognition has gotten a lot of attention after achieving very promising results by leveraging CNN's incredible robustness . In most businesses and sectors, installing CCTVs for ongoing surveillance of people and their interactions is a widespread practise. Every day, every person in a developed country with a population of millions is photographed by a camera. Constant monitoring of these surveillance films by police to determine whether or not the occurrences are suspicious is practically impossible, as it necessitates a workforce and their undivided attention. As a result, we're

developing a demand for high-precision automation of this process. It is also vital to show which frame and which parts of it include unexpected activity, as this aids in determining whether the unusual activity is abnormal or suspicious. This will aid concerned authorities in finding underlying cause of anomalies while also saving time as well as effort that would otherwise be spent manually searching the records. ARS is a real-time monitoring system that recognises and records evidence of offensive or disruptive behaviour in real-time. Using a variety of Deep Learning models, this study seeks to detect and characterise high movement levels in frame. Videos are divided into portions in this project.

A detection alert is raised in event of a threat, displaying suspicious behaviour at a specific point in time. The movies in this project are divided into two classes: threat and safe. Burglary, Abuse, Explosion, Fighting, Shooting, Shoplifting, Arson, Road Traffic Accidents, Robbery, Assault, Stealing and Vandalism are amongst the 12 uncommon actions we recognise. As a result of these irregularities, people would feel safe

2.2 HARDWARE AND SOFTWARE

The paper doesn't specifically mention the software and hardware requirements to implement the proposed criminal activity detection system. However, it can be inferred from the methodologies and algorithms used in the paper that the following might be required:

Software Requirements:

1. Python: Used for implementing machine learning algorithms.
2. Keras and TensorFlow: These are open-source libraries for developing and training machine learning and deep learning models.
3. YOLO Algorithm: Used for object detection.
4. Machine Learning and Deep Learning Libraries: These may include Scikit-learn, NumPy, Pandas, Matplotlib for data handling, modeling, and visualization.

Hardware Requirements:

1. High Processing Computer: Training such models usually requires a high-end computer with good processing power.
2. GPU: Graphics Processing Units can accelerate the computational process of machine learning models, especially for deep learning.
3. High-Resolution CCTV Cameras: Good quality cameras would be needed to capture clear videos for accurate detection and recognition.
4. Adequate Storage: Large storage capacity would be needed to store high-resolution video feeds and the large datasets used for training mode

2.3 PROJECT SCHEDULE

ACTIVITIES	MONTHS					
	Sept-2023	Oct & Nov-2023	Dec-2023	Jan & Feb-2024	Mar-2024	Apr-2024
Literature survey and Problem Statement identification						
collection of Requirements & Synopsis submission						
Product Design						
Implementation						
Testing						
Documentation and project submission						

Fig 2.2 represent project cycle and tasks performed as per the assigned Time in particular months from September to april

Problem Statement:

The problem statement is chosen and finalized in the month of September.

Synopsis & requirements:

The synopsis report is made in the month of October. The requirements need to the project are listed in the month of November.

Collecting Data:

The requirements include the CCTV. The analysing the use of Symbols is donein the month of December.

Project Design:

The project flow, methodology or the architecture are analysed in project design. The project design is done in the month of February.

Implementation and Testing:

All the trained dataset are implemented in the system. The testing is done to the errorsand faults of the implemented dataset. It is implemented and performed in the month of March.

Document submission:

The result and accuracy of the project is documented. The final report is submitted within the month of April.

CHAPTER-3

SUMMARY

In conclusion, the project need for an intelligent surveillance system to detect crime, given the limitations of manual crime detection and the increased crime rate. The authors propose a system that uses machine learning and real-time CCTV feed for crime detection. The key advantage of the proposed system is its ability to detect and classify various crimes quickly based on object and activity detection, with an emphasis on the effective use of the YOLO algorithm.

The project also points out the importance and reliability of the UCF Crime dataset in training the system with multiple real-time crime videos. The authors envision this system to reduce the crime rate significantly by providing an automatic, efficient, and reliable crime detection mechanism.

It's also noted that this research area has a lot of scope for future improvement. The authors suggest the potential for the proposed system to predict the severity of crimes and help in criminal identification by cross-referencing with previous databases. Further research can be done to increase the system's accuracy and train it on more crime categories.

3.1 REFERENCES

[1] N. Hnoohom, P. Chotivatunyu, S. Yuenyong, K. Wongpatikaseree, S. Mekruksavanich and A. Jitpattanakul, "Object Identification and Localization of Visual Explanation for Weapon Detection," 2022 Research, Invention, and Innovation Congress: Innovative Electricals and Electronics (RI2C), 2022, pp. 144-147

[2] J. Candamo, M. Shreve, D. B. Goldgof, D. B. Sapper and R. Kasturi, "Understanding Transit Scenes: A Survey on Human BehaviorRecognition Algorithms," in IEEE Transactions on Intelligent Transportation Systems, vol. 11, no. 1, pp. 206-224, March 2010

[3] N. Y. Katkar and V. K. Garg, "Detection and Tracking the Criminal Activity using Network of CCTV cameras," 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), 2022, pp. 664-668, doi: 10.1109/ICOSEC54921.2022.9952104.

[4] Jebur SA, Hussein KA, Hoomod HK, Alzubaidi L, Santamaría J. Review on Deep Learning Approaches for Anomaly Event Detection in Video Surveillance. Electronics. 2022 Dec 22;12(1):29.

[5] Choudhari, S.J., Singh, S.A., Kumar, A.S. and Desai, K.A., 2022, June. Machine Setup Abnormality Detection Using Machine Vision and Deep Learning. In International Manufacturing Science and Engineering Conference (Vol. 85802, p. V001T04A009). American Society of Mechanical Engineers.