International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 03 | Mar 2026 www.irjet.net p-ISSN: 2395-0072

AEGISEYE: AUTOMATED CCTV ANOMALY DETECTION IN CRIME MAPPING ANALYSIS SYSTEM USING DEEP LEARNING

Lakshmanan K[1], Mukeshwaran.K.G[2], Vishnuprakash.s[3], Mr.Murugan.G[4]

[1,2,3] *UG Student ,Dept.CSBS.,E.G.S Pillay Engineering College ,Nagapattinam, Tamilnadu, india.*
[4] *Assistant Professor ,Dept.Of CSBS.,E.G.S Pillay Engineering College, Nagapattinam, Tamilnadu, india.*

ABSTRACT - *Intelligent surveillance utilizes a computer system built to monitor suspicious activity and provide real-time detection of individuals in a video through programs using some of the following technologies: OpenPose (pose estimation) which detects the position of people's body parts; Anomaly detection (detecting unusual behavior); YOLO (real-time object detection); tracking; detecting weapons both visible and concealed; and converting video to 3D using Grey whale Technology. The framework includes a Grassmannian-based CNN for facial recognition. This allows for matching the facial features of individuals detected by the AI system; regardless of lighting conditions, if the facial features are blocked from view, or the angle the individual is viewed at by the camera. The AI system can also analyze behavioural and visual data automatically which triggers an automatic alert to law enforcement immediately after an anomaly (or suspicious behavior) is detected. It decreases the time it takes for law enforcement to respond and reduces the need for someone to monitor the video manually*.

KEYWORDS: Anomaly Detection, Criminal Identification, Facial Recognition, Object Detection, Pose Estimation, Video Surveillance, YOLO Detection.

I. INTRODUCTION

Due to the growing complexity in the nature of crime in both public and private environments, there is a need for intelligent surveillance technologies to identify potential threats early on. Traditional monitoring methods that rely on manual recording of large amounts of video through standard CCTV cameras are primarily passive recording devices. The use of manual observation of the various camera feeds results in operator fatigue, operator distraction, and decreased operator focus, making it more difficult for operators to successfully monitor for critical events. As urban areas get more populated and the number of security-related incidents increases, the need for an automated system for the continuous monitoring of the environment and the detection of suspicious activity is becoming increasingly critical for the safety of the general public. Recent technological progress in the fields of artificial intelligence, deep learning and computer vision has positively affected the advancement of video analysis systems. These advances will allow for the real-time processing of footage from surveillance cameras; enabling the detection of unexpected behaviour; dangerous objects; and abnormal activity of individuals with a high degree of precision. The use of such techniques as pose estimation, object detection and anomaly detection will also enable the evaluation of movement patterns, the identification of aggressive actions, and the detection of potential threats before they develop into crises. Moreover the incorporation of facial recognition technology into a surveillance system further improves the capacity to perform surveillance functions by allowing law enforcement authorities to identify known criminals or suspects in crowded settings; even when conditions such as low-light or obstructed views are present. Using intelligent video analytics, facial recognition, and facial detection will make your security system more proactive/corporate approach. Next, when you combine multiple types of analytics together, your security cameras can go from just recording videos to becoming active monitoring devices where they can detect things happening automatically.

II. IDENTIFY, RESEARCH AND COLLECT IDEA

Mukto et al. [1] this paper presented a framework for monitoring crime in real-time, by combining deep learning technologies with intelligent video surveillance systems. Research was performed to develop an automated mechanism for identifying criminal behaviour through the use of real-time video surveillance. Convolutional neural networks were used to analyse video frames and detect suspicious behaviour within a specific monitored area. Continuous monitoring and automated threat detection were key to reducing the reliance upon human supervision. Object detection methods were also used to detect threats and abnormal behaviours from the video surveillance system. The framework could process video streams in real-time to identify potential criminal events like; violent behaviour or unusual crowd activity. Using deep neural models also proved that good visual feature extraction could be accomplished from image data within a video surveillance system. There was a significant increase in the accuracy of suspicious action detection when the model was trained on a wide variety of datasets. The monitoring system would be able to assist security personnel by sending alerts to them if threats were detected. Experimentation demonstrated that using deep learning technology is an effective method for analysing large amounts of video data.

Mandalapu et al. [2] this article reviewed the role of machine learning and deep learning in predicting crime,

providing an overview of the different computational methods that can be employed to analyze historical crimes to come up with predictions about future criminal activity. The efficacy of using a variety of machine learning algorithms to determine accurately whether or not a crime will occur (using decision trees, support vector machines and artificial neural networks) as well as the utility of using deep learning to identify complex patterns within large datasets were included within this review. Predictive models enable law enforcement agencies to allocate personnel and resources based upon their potential for providing an appropriate response to a call for service. A number of examples of the crime datasets used and feature extraction techniques used to create input variables for each type of predictive algorithm were included in this report. Factors that have an impact on the frequency or occurrence of specific types of crime were also addressed, including but not limited to, location, time of day, and socio-economics. Comparative assessments of crime predictors were conducted so that their respective strengths and weaknesses could be identified. The study also discussed the continuing growth of the use of artificial intelligence within both the field of crime analysis and public safety planning.

Rendón-Segador et al. [3] has announced the launch of CrimeNet; a new framework consisting of a neural network based on structured learning employed for the automatic identification of violent actions through computer vision. The model has been created using state-of-the-art deep learning techniques to classify different types of violent interactions by analyzing real-time video footage or streaming video. Last, the framework uses transformer based neural networks as well as structured learning methodologies to discover spatial and temporal relationships within video clips and therefore classify and distinguish between violent behaviours while extracting visual features from the video to identify visual attributes correlated with aggressiveness, and other characteristics that are visual manifestations of physical confrontation. The accuracy with which the framework is able to recognize instances of violence while in highly complex surveillance environments demonstrates that using transformers in neural networks to extract informative data from video footage leads to superior explanatory power over archival databases and has demonstrated an ability to utilize long term temporal information for the recognition of violent behaviors.

Negre et al. [4] performed an extensive literature review of deep learning methods for detecting violence in video surveillance systems. The study reviewed many of the methods used in computer vision for recognizing violent events in either live or recorded video. The review placed significant emphasis on convolutional neural networks, recurrent neural networks, and combined network architectures. It also reviewed the different datasets that have been used for training models that detect violence. A number of different techniques for extracting features from video, including spatial and temporal analysis, were also considered by the study. Additionally, the review explored how deep learning models can learn the complex motion patterns associated with aggressive behavior. Several examples of real-world uses of automatic violence detection in surveillance systems were provided. Finally, the study discussed how to measure performance of violence detection systems, and the challenges involved with occlusion, camera motion and variations in the environment. In addition, the advantages and limitations of the different types of deep learning models were discussed. The study discussed how multi-modal data analysis can improve detection accuracy.

Boukabous and Azizi [5] Developed a video/image based crime predicting system based on deep learning and computer vision techniques. Research focused on enhancing safety through visual surveillance analysis. Implemented DL to help recognize suspicious objects and events in video streams. Object detection algorithms were included to recognize the potential for threats from objects like weapons and other dangerous items. Combined both video and image inputs in order to analyze the environmental context in which the human actions were occurring. Used feature extraction methods to extract the most significant visual characteristics from surveillance videos. Demonstrated the capability to identify crime patterns from visual surveillance data. Improved accuracy was achieved through the use of DL methods, and demonstrated the power of automated video analytics to assist law enforcement operations. A number of datasets were used to validate the proposed model for reliable use. Proposed a means for the system to provide real-time monitoring systems. Additionally, identified limitations related to computational complexity and issues with the availability of data. Suggested future integration and practical implementations could take place through intelligent security systems. Finally, documented that visual DL analysis is an effective means of providing support in the detection and prevention of crime.

Taverna and Paterson [6] There were several different aspects being studied related to security weaknesses associated with synchronizing mechanisms on blockchain networks, with specific emphasis on how Ethereum nodes use the Snap (or Snapshot) synchronization protocol. During this research, various weaknesses were identified within the Snap protocol, including potential vulnerabilities that an attacker could utilize to gain access to the blockchain. For example, examples of potential attack scenarios were provided to illustrate how an attacker could affect synchronization processes through either the use of malicious nodes or by exploiting Snap protocol vulnerabilities. The researchers investigated both data corruption risks in communications between distributed networks and security issues involved with SNAP synchronization architecture. The researchers performed

extensive analysis of the Snap synchronization architecture and surrounding areas in order to determine the presence of possible attacker exploitation areas (i.e., The Attack Surface). In addition, the researchers conducted demonstrated experiments of all identified attacks by evaluating them in an experimental setting. The researchers reported that there are some synchronization approaches that will facilitate opportunities for data corruption within a blockchain.

Vanini et al. [7] The goal of this project was to research the area of fraud detection associated with on-line payments through the use of anomaly detection and risk management methods. This research has been conducted to investigate the potential for detecting fraudulent financial transactions that exist within large amounts of digital payment data. The application of machine-learning has been used to detect patterns of unusual behavior and associated fraud activity within transactions. In addition, various methods of anomaly detection will be researched to assess deviation from normal financial behavior. In addition, risk assessment models were developed to evaluate the degree of severity of anomalies detected. This research has been focused on identifying the use of automated systems for monitoring financial transactions in real time. In addition to automated systems, the development of data-driven models were used to evaluate transaction histories and detect patterns of suspicious transactions. In addition to developing anomaly detection systems to keep pace with information technology, the research has also focused on developing techniques for addressing other challenges associated with fraud detection, including the existence of data that is imbalanced and the development of new fraud strategies. Additionally, the testing of machine-learning models has shown that machine-learning can perform very well with respect to tasks related to detecting fraud. Furthermore, the study highlighted that continuous model training is needed to keep pace with new fraud patterns. The study proposed that adopting advanced analytic techniques would lead to improved detection accuracy.

Xing and Li [8] I created a visual anomaly detection (VAD) model that incorporates a partition memory bank (PMB) module and error estimation techniques for detecting abnormal events in video surveillance environments. The PMB mechanism stores normal behavior patterns captured during training in order to compare them with live monitoring data that exhibits variations from long-term averages (LTAs) of these patterns. The error estimation technique uses the differences between reconstructed normal scenes and corresponding reconstructed abnormal scenes as a basis for estimating whether an abnormal scene is indeed, an abnormal scene. The anomaly detection model was tested on existing benchmark datasets of video surveillance and showed improved performance when using the PMB and error estimation techniques for detecting abnormal events in complex scenes. Furthermore, this study has emphasized the role of memory models in VAD tasks, in addition to addressing other design considerations such as computational efficiency. Lastly, the PMB-based anomaly detection model is capable of detecting rare events within large-scale video surveillance data sets; furthermore, the potential challenges associated with detecting anomalies due to variations in the environment were addressed as part of this research. Suggestion for future enhancements include using more advanced deep learning architectures.

Mohammad et al. [9] The authors present a decision support system for detecting energy theft in smart grids, based on ensemble learning. Their research used several machine learning models, combined with ensemble techniques, to increase detection accuracy. These models were applied to the analysis of data from smart meters to identify unusual consumption of electricity. Features were extracted from the data to capture key attributes of electricity consumption. Several machine learning methods were then integrated to enhance the reliability of these predictions. The decision support system was intended to help utility providers identify electricity consumption that is fraudulent or illegal. The authors found that their use of ensemble learning methods improved the detection rates. Additionally, the authors addressed issues with data imbalance and noise in smart grid data. They noted that one benefit of their proposed decision support system is that it enables real-time monitoring of electricity usage. Further, the proposed decision support system has potential for reducing utility provider's financial losses due to electricity theft. In their research, the authors incorporated advanced analytics techniques to enhance the decision-making process.

Zhao et al. [10] The investigation of self-sustained snapping motion in free-standing wavy rings was conducted by Study. The mechanical and material characteristics of these wavy rings used for producing autonomous (self-driven) motion were studied. Through experimental observations, it was determined that the wavy geometrical form of each ring structure influences its behaviour in producing dynamic/oscillatory motion. The interaction between elastic potential energy stored in a ring structure and mechanical deformation of a ring structure during its snapping motion was studied. Advanced techniques in material analysis were used to understand the physical processes that take place in producing the snapping motion of a ring structure. Mathematical models were developed to predict the dynamic behaviour of each ring structure. The study identified the possible uses of self-actuating devices made using wave forms in soft robotic applications as well as intelligent materials. Results showed that the motion of each ring structure can be controlled without the use of an external power source(s). The study provided new insights into how to design ring structures for producing autonomous motion. The mechanical stability of a ring structure and the energy efficiencies created by the snapping motions produced by a ring structure were also

investigated. The role of structural design on a ring's ability to produce dynamic motion was highlighted.

EXISTING METHOD

CCTV has been used as a surveillance system to constantly store and display live images for observation. Most places have human monitors that monitor multiple screens at once and create an alarm if they detect an unusual occurrence. Some existing systems include basic motion detection systems that can alert users of changes that have occurred; however, motion detection is typically limited to detecting variations in light, shadow and pixel color. Conventional monitoring systems have no ability to analyze or interpret complex human behaviour and activity thereby limiting their ability to detect a potential threat in real time. Some of the currently available computer vision systems use simple techniques for detecting motion or an abnormal event (e.g. movement detection). These basic computer vision methods lack significant automation and are not able to accurately detect complex actions; like violence, loitering, or having a concealed weapon. Traditional methods of facial recognition, including Eigen faces, Fisher faces, and LBP, have been used in some surveillance systems as well. However, traditional methods are very sensitive to different lighting conditions, different faces turned at various angles, and different obstructions (i.e. only part of a face shows or there is an object in front of a face), resulting in poor reliability for surveillance applications. While there are improvements in this area, the current systems for surveillance have numerous critical vulnerabilities. Many surveillance systems are reactive in that they only collect data from the scene after the fact; as a result, they are unable to produce a timely response from the security force(s). The physical characteristics of an object make it difficult to determine if that object is a weapon, as the amount of error that exists when trying to classify a weapon (for example) from a different object; in addition, facial recognition algorithms do not work well in low-light situations, or where the face is obscured (for example) by a mask or hood. Additionally, without integrated behavioural analysis capabilities, the system cannot identify aggressive behaviours or suspicious movements (e.g. people moving towards an area of interest); therefore, there is a need for more intelligent." (Rewrite without changing the meaning.)

III. WRITE DOWN YOUR STUDIES AND FINDINGS

By using an Artificial Intelligence Surveillance Monitoring System, this proposed procedure will provide continual analysis of live video streams that enable the detection of suspicious activity and criminal behavior as they occur. The surveillance/monitoring will be performed by advanced computer vision techniques on the video stream data from the surveillance cameras to automate the monitoring of video stream data without the need for constant human supervision. The system will monitor the area for abnormal motion, aggressive motion, and any other type of suspicious activity or motion. With continual analysis of visual information, the earliest possible threats can be identified, making the security monitor more effective with regard to signal detection and response time to incidents. An innovative detection approach will be applied that incorporates deep learning-based algorithms to detect objects of interest and patterns of behavior contained in the captured video frames. To do so, the YOLO-based object detection algorithm will be used to quickly detect potentially dangerous objects like weapons or other suspicious items in the video frames. Additional techniques will include applying human pose estimation to identify body positions and using activity analysis to evaluate a person's movements to determine the types of actions they are performing. These techniques will assist the system in identifying unusual behaviors like violence, loitering, or rapid aggression, allowing for an increase in accuracy when differentiating between normal and suspicious behavior. Facial recognition plays a significant role in crime detection as part of the overall surveillance system. An extraction model based on Grassmannian convolutional neural networks captures important features of a person's face and compares those features to the same features stored in a national criminal database. The facial recognition module continues to perform consistently well even in difficult situations, including changes in light or when the person's face is partially blocked from being seen. Automatically, when a suspicious activity occurs or a person is identified as having an active warrant, an alert is generated, and law enforcement agencies are immediately notified so they can respond quickly when there is a potential threat to public safety.

METHODOLOGY

Data Acquisition and Video Capture

Continuous video acquisition using strategically located cameras allows for the monitoring of public or restricted areas. The video streams that are captured by the cameras will then be transmitted to the processing unit where frames will be extracted for further excellent analysis. After every individual frame has been processed, it will be processed in sequence as this will help to maintain real-time monitoring capability. The high-resolution video input helps to preserve facial details, object features and the motion patterns associated with each object so that they can be accurately analysed in the future. The camera placement and the stable frame capture rate also contribute to improved performance of the detection process.

Pre-Processing and Frame Enhancement

Video frame capture goes through an important pre-processing step to help increase the quality of visuals and make the data ready to analyse. To remove noise

(unwanted distortion) caused by fluctuations in lighting and interference due to the camera, techniques are used that reduce noise. Frames are normalised and resized, so there is consistency in size to work with when using deep learning algorithms. Contrast enhancement techniques are used in order to see clearly in low-light situations and to correct for any illumination issues that occur. All of these pre-processing techniques will maintain the ability to see what are considered as important features such as facial detail, edges of objects or movement patterns.

Face Detection and Feature Extraction

When facial detection occurs through camera capture, any human faces within the frames will be found using facial detecting technology to locate each human face. Once the faces are located, feature extraction using CNN will occur via a trained CNN-based model to extract feature vectors that are representative of a person's identifiers (i.e., facial features). The feature vectors have been converted into a mathematical representation that can be compared easily to existing quality and quantity of facial images stored in a record keeping system or repository. The technique will result in a robust method of identifying persons despite differences in facial expression or orientation as well as from different lighting conditions and angles.

Object Detection Using YOLO

Using YOLO deep learning, object detection can quickly identify multiple objects in real time and is one of the fastest frameworks. The model scans each frame of an image in a continuous loop and detects all the suspicious objects (weapons, unusual objects) within the image. Once an object is detected, it will generate a bounding box and label it with the appropriate classification. Likewise, the detection system continues to operate, so as soon as the dangerous objects are found, they are identified as soon as possible. By being able to Detect objects in real-time, potential threats can be quickly identified in areas where lots of people are or where conditions may be complicated.

Behavior and Activity Analysis

The movements of people can be studied by detecting individuals in a foreground image and analyzing their poses, including their locations in relation to a pixel of their body. The purpose of these techniques is to identify abnormal behaviors (e.g., aggressive behaviors) or patterns (e.g., sudden changes in direction) and to determine if those patterns are considered typical or not. Anomalies in behavior can be detected by using algorithms that have been developed for that purpose. In addition, by tracking human body movements continuously, the system has the ability to detect early signs of violence or other suspicious behavior. The second phase of this process allows for the identification and interpretation of human behavior rather than just detecting the presence of an object.

Criminal Identification and Alert Generation

The outcomes created by face detection can be analyzed against a database that contains known individuals and criminal history. Through facial features extracted from the video of detected individuals, those features are compared against pre-existing templates in the database using one or more types of facial matching techniques. If there is a match between the two data sets (the scanned features and the stored templates), this indicates that a known individual is in proximity to the camera or area being scanned. Simultaneously, the system is evaluating the presence of other threats (i.e., weapons or violent actions) and assessing the risk level for those types of threats.

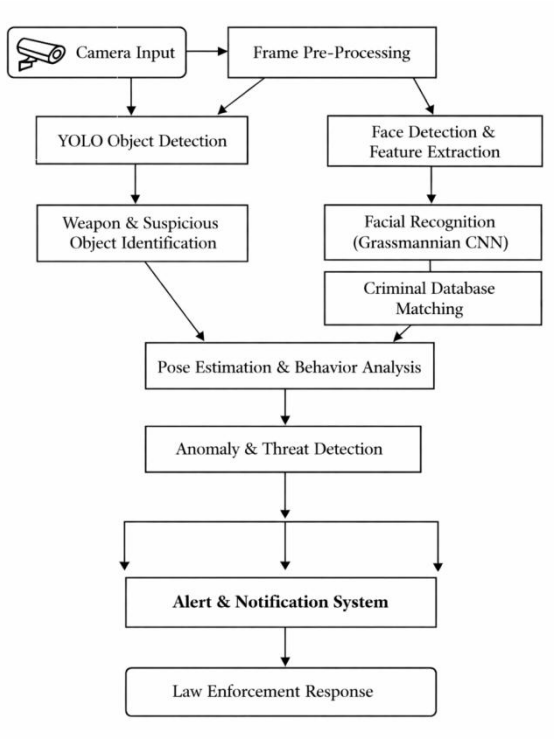

Fig 1: Intelligence surveillance system **a**rchitecture

IV. IMPROVEMENT AS PER REVIEWER COMMENTS

The intelligent surveillance framework was tested and the obtained results confirm that it successfully detects suspicious behavior and recognizes criminals from their facial shots in real-time. Using sample video tapes from actual surveillance where different environmental factors were present including crowded scenes, light levels from bright to dark, and partial facial coverage due to obstructions the video was processed through three processing stages: identifying faces and other things (using a model based on Yolo), identifying activity in front of a person (using a model based on the class of that person), and then identifying that person via facial recognition (using a model based on Grassmann). The three stages were evaluated for two dimensions of accuracy (detection

and recognition) as well as the speed of processing. The results showed that by including deep learning into the surveillance system, there is a dramatic improvement in both the level of accuracy at which the intelligent surveillance system can detect individual unsafe situations compared to conventional video surveillance systems. Throughout the experimentation process, the object detection module accurately detected potential dangerous objects (weapons & suspicious items) in a video frame. Additionally, the behavior analysis module was effective at detecting abnormal behavior (i.e., aggressive motion & prolonged loitering). The facial recognition tests demonstrated a strong capability of matching detected faces from the identified criminals database despite pose & lighting variations or partial obstruction. By generating an alert in real-time, notifications were generated automatically whenever any suspicious activity/crime identity occurred. The combination of the two modules supports rapid threat detection and demonstrates the effectiveness of multiple computer vision systems integrated within a comprehensive multidimensional surveillance system.

Technique	Detection Accuracy (%)	Response Time (seconds)	Behavior Detection (%)	Facial Recognition Accuracy (%)
Traditional CCTV Monitoring	55	10	20	30
Basic Motion Detection System	65	6	40	0
Conventional Face Recognition	75	4	0	70
Proposed AI Surveillance Framework	94	1	90	92

Fig 2: Experimental result comparison table

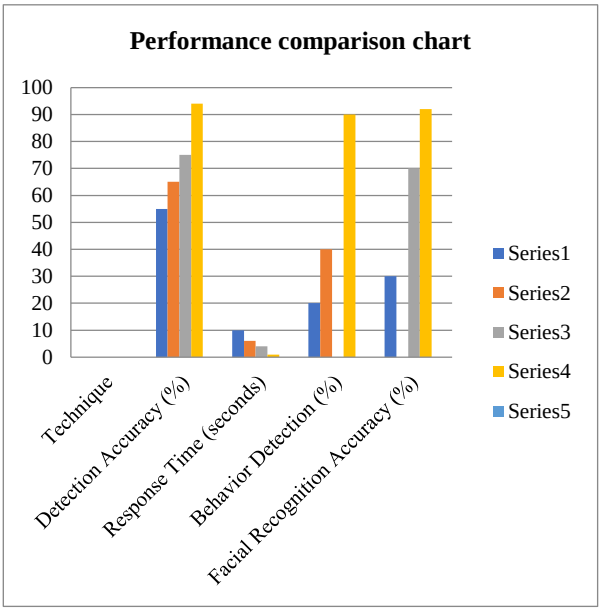

Fig 3: Performance comparison chart

V. CONCLUSION

As innovative surveillance technologies develop, it is imperative to enhance security beyond outdated security technologies. Artificial intelligence and computer vision (AI/CV) technologies provide the ability to analyse video streams continuously in order to quickly detect suspicious behaviours, unsafe items, or the presence of suspected criminals. The incorporation of object detection, behaviour analysis and face recognition into one system allows for an ability to identify threats and react accordingly in real-time. This significantly decreases the need for manual observation, increased accuracy of automated systems, and also improved productivity through increased efficiency. The advancing use of deep learning models for face recognition/object detection continues to increase the accuracy and reliability of the various forms of automated surveillance systems. With this added reliability, the ability of intelligent surveillance to provide real-time warning systems that assist in rapid decision-making by security personnel, results in a more efficient and effective response to potential threat instances. When coupled with additional capabilities such as proactive monitoring and early threat detection, intelligent surveillance products, systems and other technologies contribute significantly to public safety through improved situational awareness. Together, additional advancements in the areas of artificial intelligence and video analytics will greatly improve the effectiveness of intelligent surveillance in deterring crime as well as maintaining safe environments.

REFERENCES

[1] Mukto, Md Muktadir, et al. "Design of a real-time crime monitoring system using deep learning techniques." Intelligent Systems with Applications 21 (2024): 200311.

[2] Mandalapu, Varun, et al. "Crime prediction using machine learning and deep learning: A systematic review and future directions." Ieee Access 11 (2023): 60153-60170.

[3] Rendón-Segador, Fernando J., et al. "Crimenet: Neural structured learning using vision transformer for violence detection." Neural networks 161 (2023): 318-329.

[4] Negre, Pablo, et al. "Literature Review of Deep-Learning-based detection of violence in video." Sensors 24.12 (2024): 4016.

[5] Boukabous, Mohammed, and Mostafa Azizi. "Image and video-based crime prediction using object detection and deep learning." Bulletin of Electrical Engineering and Informatics 12.3 (2023): 1630-1638.

[6] Taverna, Massimiliano, and Kenneth G. Paterson. "Snapping snap sync: practical attacks on go Ethereum synchronising nodes." 32nd USENIX Security Symposium (USENIX Security 23). 2023

[7] Vanini, Paolo, et al. "Online payment fraud: from anomaly detection to risk management." Financial Innovation 9.1 (2023): 66.

[8] Xing, Peng, and Zechao Li. "Visual anomaly detection via partition memory bank module and error estimation." IEEE Transactions on Circuits and Systems for Video Technology 33.8 (2023): 3596-3607.

[9] Mohammad, Farah, Kashif Saleem, and Jalal Al-Muhtadi. "Ensemble-learning-based decision support system for energy-theft detection in smart-grid environment." Energies 16.4 (2023): 1907.

[10] Zhao, Yao, et al. "Self-sustained snapping drives autonomous dancing and motion in free-standing wavy rings." Advanced Materials 35.7 (2023): 2207372.