A Discriminant analysis for Anomaly detection based on Security Camera using Entropy Weighted K-means

[1]Yasoda.khumbham,[2]Musunuri Pavani, [3]Jyothsna P, [4]Satya Srinivas Maddipati,[5]A N V K Swarupa

[1,3,5]Assistant Professor, CSE Department, Sasi Institute of Technology & Engineering, Tadepalligudem, Andhra Pradesh, India.

[2]Assistant Professor, CSM Department, Sasi Institute of Technology & Engineering, Tadepalligudem, Andhra Pradesh, India.

[4]Associate Professor, CSM Department, Sasi Institute of Technology & Engineering, Tadepalligudem, Andhra Pradesh, India.

Abstract

Modern security cameras are crucial across various sectors like traffic control, health monitoring, and industrial automation, yet their high cost and complexity limit broader adoption. These systems generate extensive video data, but manual monitoring is inefficient and error-prone, necessitating automated surveillance. While video anomaly detection (VAD) for static cameras is well-researched, VAD for moving cameras lacks a unified review, despite growing inter est in anomalies from devices like dash cams and body-worn cameras. This paper proposes an Entropy-Weighted K-Means approach for anomaly detection in security camera footage. The methodology involves feature extraction from continuous video data, including motion, appearance, spatial information (bounding box coordinates), environmental factors (blur, contrast, noise levels), and detection metrics (anomaly and confidence scores). Entropy-based weighting is then applied to these features, where features with lower entropy (less variability) are assigned higher weights, influencing the weighted distance calculation in the K-Means algorithm. The iterative clustering process identifies "normal" behaviors as large, dense clusters, while anomalies are detected as outliers or small, sparse clusters. Initial results, including Pearson correlation analysis, discriminant analysis, and within-cluster sum of square values, demonstrate the potential of this method in effectively identifying anomalies within complex video data.

Keywords: Anomaly detection, Security camera, Discriminant analysis, Pearson correlation, Entropy Weighted K Means

1. Introduction:

1.1 Security Cameras:

Today, cameras are essential tools in areas like traffic control, health monitoring, industrial automation, and facial recognition. However, many current systems are costly and overly complex, which restricts their adoption in wider applications.

Security cameras are widely installed in public areas such as airports, roads, and banks to ensure safety. These systems generate vast amounts of video footage, much of which is rarely reviewed unless an unusual incident occurs. Relying on human operators for continuous monitoring is not only time-intensive but also prone to errors, highlighting the need for automated surveillance solutions. The widespread adoption of affordable, compact cameras, such as dash cams, body-worn cameras, and cameras mounted on robots, has led to increasing interest in detecting anomalies within dynamic scenes captured by moving cameras. Despite this growing focus, most existing reviews in the field of Video Anomaly Detection (VAD) primarily centre on methods designed for static camera setups. As a result, literature concerning VAD with moving cameras remains scattered and lacks a unified review. The widespread installation of surveillance cameras in both indoor and outdoor environments has led to an increased demand for intelligent systems capable of accurately recognizing human actions and detecting entities of interest in recorded video footage. While human action recognition has long been a core area in computer vision, the detection of abnormal behaviour has recently emerged as a prominent research focus. Over the years, various systems have been developed to identify unusual human activities to enhance public safety.

Surveillance cameras, a type of Cyber-Physical System (CPS), are widely employed for visual monitoring to detect activities of interest or unusual behaviour. Despite their usefulness, these systems are vulnerable to physical security threats, such as tampering with camera angles, altering recording zones, or manipulating settings like zoom and focus. These alterations can result not only from direct physical interference but also from cyber attacks exploiting software vulnerabilities to remotely modify the cameras' configurations. Such cyber-physical breaches compromise the integrity of the surveillance system, ultimately diminishing its effectiveness in ensuring security. While there has been considerable research focused on detecting cyber intrusions in CPS devices, the specific issue of safeguarding against attacks targeting physical configuration integrity remains largely unexplored.

Industrial Control Systems (ICS) are increasingly being connected to the Internet to reduce operational expenses and offer greater flexibility. These systems, commonly found in sectors like energy, manufacturing, and utilities, are designed for continuous operation and typically have extended lifespans—spanning decades, unlike the shorter cycles seen in conventional Information Technology (IT) infrastructure. Due to their critical role, ICS demand consistent, safe, and uninterrupted performance. However, they are susceptible to various cyber threats, and attacks on these systems can result in serious harm, affecting both public safety and national security. The challenge lies in protecting ICS against not only known threats but also unforeseen vulnerabilities.

1.2 Detecting anomalies:

In high-security environments, detecting anomalies through surveillance is vital for ensuring public safety. Detecting suspicious behaviour in public spaces is a recurring challenge in machine learning research. The evolution of artificial intelligence (AI) has transformed surveillance systems, especially those utilized for ensuring campus security. Given the dynamic nature and high population density of campuses, traditional surveillance methods often fall short in addressing their complex security needs. AI-based person recognition

technologies offer a more effective solution by enabling proactive threat detection, real-time data analysis, and improved accuracy. These innovations greatly enhance the protection and monitoring capabilities of educational institutions. However, despite their advantages, such systems also introduce ethical challenges, particularly related to data privacy and potential algorithmic bias. Anomalies in video content generally refer to events or behaviours that deviate from normal patterns and indicate irregular activity. The primary objective of anomaly detection is to pinpoint instances that differ significantly from typical data behaviour. In video analysis, this involves identifying both temporal and spatial deviations. As models increasingly process more complex data, particularly in security contexts, accurately analysing and interpreting the extracted features becomes crucial. After detecting these outliers, it is essential to categorize them and assess their potential impact on society. Such anomalies can encompass a wide range of incidents, including vandalism, fires, theft, traffic accidents, or unauthorized movement—such as vehicles on pedestrian pathways. Surveillance footage is capable of capturing numerous real-world abnormal events..Recent progress in camera-based technologies has led to increased security needs across multiple industries. In recent years, substantial research has been devoted to identifying previously unseen anomalies in video content. However, the majority of these studies have primarily concentrated on detecting unusual frames in surveillance footage from security cameras. In contrast, anomaly detection in videos that capture irregular mechanical behaviour remains largely underexplored. This area holds both theoretical and practical value, as it could facilitate the automated identification of mechanical failures in manufacturing, maintenance, and real-world environments.

1.2.1 Detecting anomalies for IoT systems:

The Internet of Things (IoT) has become deeply embedded in numerous industries and daily life. However, as technology advances, so do the security challenges associated with IoT devices. Particularly in smart home environments, many IoT devices are susceptible to threats due to their limited computing capabilities. Each time a new IoT device is added to a home or general network, it is crucial to promptly secure and manage it using appropriate security protocols.The Internet of Things (IoT) has significantly impacted areas such as home automation, industrial systems, and agriculture; however, security continues to be a pressing concern. IoT networks consist of numerous diverse devices that produce large volumes of varied data.The study [8] introduces an approach that links the supply current of a smart device to its functional behaviour to identify potential security breaches or manufacturing defects in IoT devices. It demonstrates that understanding a device's normal operational behaviour through functional metrics, such as supply current, can serve as a reliable security indicator, as deviations from expected patterns may signal either a fault or a security threat.

The growing need for autonomous video surveillance systems is driven by the limitations of manual video analysis, which often proves ineffective in detecting anomalies. At present, most surveillance systems rely on manual review of footage only after a suspicious event has been reported or noticed, which delays response and reduces effectiveness. Implementing real-time video monitoring—both centrally across multiple cameras and locally at the edge with a single camera—is highly challenging due to the demands for high-performance GPUs,

substantial computational resources, and the complexities involved in recognizing various types of abnormal human behaviours.

2. Literature Survey:

The study[1] presents an object detection-based method for identifying unusual activities, leveraging a model known for its real-time efficiency. The system employs YOLOv5 to detect and monitor objects, capturing irregular behaviours typically observed in security footage. A diverse dataset comprising multiple surveillance scenarios is used to train and assess the model's performance. By integrating a customized detection framework, YOLOv5 effectively distinguishes between normal and suspicious activities in real time. The approach prioritizes fast processing to enable scalability in real-world settings, and experimental results highlight the system's strong accuracy in detecting anomalies. The study [2] introduces a technique for anomaly detection in public transportation settings to help ensure passenger safety. The proposed approach utilizes a Convolutional Neural Network (CNN)-based classifier that processes images captured by existing CCTV cameras installed in vehicles for security monitoring. Several factors complicate the task, including inconsistent hardware standards, subpar image quality, and ineffective camera placement. Additionally, the dataset used for model training was highly imbalanced across classes. To validate the approach, four different CNN architectures were tested on the dataset. Experimental outcomes demonstrated that the proposed method delivered encouraging performance.

The research[3] utilized a mixed-methods design, incorporating both qualitative and quantitative analyses. Data were gathered over a six-month period from camera footage and access logs across several campuses, capturing factors such as lighting conditions, crowd density, and instances of potential security threats. The study examined three AI-based surveillance technologies: facial recognition, gait analysis, and behavioural anomaly detection. The systems were evaluated using performance indicators including processing time, scalability, accuracy, and rates of false positives and negatives. To gather qualitative insights, structured interviews and online surveys were conducted with students and campus security staff, focusing on privacy concerns and personal experiences. A comparative framework was developed to systematically assess both the operational effectiveness and ethical dimensions of the AI systems.AI-enabled identification tools were found to substantially enhance campus safety. Facial recognition achieved an average accuracy of 95% under optimal lighting, which dropped to 78% in low-light environments. Gait analysis maintained a consistent accuracy of 85%, proving beneficial in challenging scenarios. Behaviour detection systems reached an 88% accuracy rate, though they sometimes misclassified harmless actions. In terms of speed, facial recognition processed frames in 0.6 seconds, gait analysis in 0.8 seconds, and behaviour detection in 1.2 seconds per frame.While behaviour detection raised concerns around transparency and informed consent, facial recognition was praised for its seamless integration with existing infrastructure. Moreover, 85% of participants supported the implementation of anonymization techniques to protect personal data and stressed the importance of clear data usage policies. Ethical concerns such as AI bias and data privacy underscored the need for strong regulatory frameworks and privacy-preserving strategies. Although the systems demonstrated improvements in security, further refinement is needed to address these ethical challenges effectively.

The paper[4] presents a novel, affordable, and compact security solution built using the ESP32-CAM module, a microcontroller with an integrated camera and Wi-Fi capability. This system is designed to detect unauthorized access in residential areas and parking lots. It employs a laser sensor to activate an alarm via a buzzer and capture images for further review. Any detected anomalies are instantly uploaded to cloud storage using Wi-Fi, enabling real-time surveillance and alerts. With its user-friendly setup and cost-effective design, the system offers a practical approach to improving security in both private and public environments. Extensive testing and evaluation confirm the system's reliability and showcase its potential as a disruptive innovation in the field of low-cost security systems.

The paper[5] presents the first in-depth survey dedicated to Moving Camera Video Anomaly Detection (MC-VAD).Authors thoroughly examine relevant research efforts in MC-VAD, analysing their shortcomings and identifying ongoing challenges. Their study spans three key application areas, security, urban transportation, and marine settings, encompassing six specific use cases. Additionally, authors gathered and categorized 25 publicly accessible datasets representing four environments: underwater, surface water, land, and aerial views. Authors outlined the types of anomalies addressed in these datasets and classify detection methods into five principal approach categories.

In theresearch[6], authors present an automated video anomaly detection system that combines an Inflated 3D Convolutional Network (I3D-ResNet50) with deep Multiple Instance Learning (MIL). The approach treats normal and abnormal videos as negative and positive bags, respectively, where each video segment acts as an instance within the bag.An anomaly score is calculated for each video segment using a fully connected neural network. For feature extraction, we utilize the I3D-ResNet50 model on the UCF-101 dataset, applying a 10-crop augmentation technique. The dataset includes approximately 130 GB of video data encompassing 13 types of anomalous activities—such as theft, abuse, and physical altercations, alongside normal behaviour. Experimental evaluation demonstrates that their system achieves an Area Under the Curve (AUC) of 82.85% after just 10,000 iterations, outperforming existing methods and showcasing its effectiveness in detecting anomalies in real-time video streams.

The study[7] explores the effectiveness of anomaly detection models tailored to individual devices and device types, emphasizing the importance of distinct traffic patterns found in heterogeneous IoT environments. These specialized models are evaluated against a unified model trained on data from all devices, using eight different One-Class Classification (OCC) techniques, both supervised and unsupervised, applied to two IoT datasets. In practical scenarios, IoT devices usually exhibit normal traffic before experiencing any security breaches. Given the abundance of normal data and the lack of labeled attack instances, unsupervised learning methods are particularly well-suited. The study reveals that device-level and device-type-level models outperform generalized models, especially in data settings dominated by a single class. As a result, these specialized models offer a more efficient solution for real-time anomaly detection by recognizing deviations from established normal behaviour unique to each device or device category.

The study[8] presents a system that utilizes machine learning (ML) to distinguish between IoT and non-IoT devices on a network and incorporates an anomaly detection mechanism to identify unusual or suspicious behaviour. The ML model is trained using a specific dataset and evaluated in a test environment comprising IoT and non-IoT devices, a connector, and a hub to assess its effectiveness. Performance comparisons between various ML algorithms will be made using the F-measure. Additionally, the developed model will be integrated with a commercial platform named Enigma Glass, offering an end-user interface that includes analytics, visual data representations, and alerts related to the smart home network.

To explore the effectiveness of existing methods for this type of anomaly detection, L. Kart et. al, examine two basic baseline strategies: (i) anomaly detection using temporally aggregated image-based methods, and (ii) density estimation based on video features extracted using pretrained video classification models. Advancing this field requires the creation of new benchmark datasets for thorough evaluation. To this end, authors presented the PHANTOM (Physical Anomalous Trajectory or Motion) dataset, which features six video categories, each containing both normal and anomalous instances. These categories vary in terms of the depicted events, the diversity within normal behaviour, and the nature of the anomalies. Furthermore, we propose a more challenging benchmark that involves identifying anomalies within highly dynamic scenes[9].The paper[10] introduces a software-driven security framework that leverages Software Defined Networking (SDN) and Network Function Virtualization (NFV) to strengthen ICS cybersecurity. Authors have designed a security architecture based on these technologies and developed a Control System Security Application (CSSA) integrated into the SDN controller. This application enhances ICS protection by enabling real-time monitoring and adaptive, policy-based network decisions. CSSA supports secure end-to-end communication between devices, mitigates specific threats such as denial-of-service (DoS) attacks, and secures data flows from outdated control components that lack built-in security mechanisms. Additionally, it ensures dependable routing of safety-critical messages within control systems.

The study [11] introduces an innovative method for detecting anomalies such as explosions, arson, and vandalism in public areas using video feeds from CCTV cameras. This system leverages deep learning techniques to analyze video streams and identify behaviors or events that significantly diverge from expected norms. Their approach integrates Convolutional Neural Networks (CNNs) and Spiking Neural Networks (SNNs) for extracting visual features, along with Long Short-Term Memory (LSTM) networks to capture temporal relationships within video sequences. Training is conducted on the UCF Crime Dataset, enabling the model to learn typical activity patterns and detect irregularities in simulated real-time scenarios. To boost detection accuracy, authors also incorporate computer vision techniques like optical flow, creating multiple hybrid model combinations (e.g., OF-CNN, OF-CNNLSTM, OF-SNN, OF-SNNLSTM, and CNNLSTM). This system demonstrates strong potential for use in public safety and surveillance across urban settings.

The study[12] explores home security anomaly detection systems and proposes a holistic solution that addresses multiple dimensions of residential safety. This approach integrates functionalities such as motion sensing, audio monitoring, video surveillance, anomaly recognition, weapon detection, and police station connectivity. By utilizing machine learning

techniques, the system can detect irregular or suspicious activity within the household environment. Additionally, the weapon detection feature serves as an alert mechanism for potential threats, notifying the relevant authorities. High-definition cameras, strategically installed, continuously capture and record unusual behavior, while advanced audio processing algorithms identify sounds associated with emergencies. The inclusion of motion detectors strengthens the system's ability to detect unauthorized entries, thereby improving overall home security.The study [13] introduces a novel deep learning-based approach to detect such hybrid attacks, whether they originate from the physical or digital domain. Furthermore, it presents a unique application of deep learning-driven video frame interpolation, which has shown superior performance compared to conventional anomaly detection methods in spatiotemporal settings.

Surveillance cameras are widely utilized for security monitoring, but in many cases, they primarily serve to review incidents after they occur. The study [14] introduces a proactive approach to video surveillance by leveraging human pose estimation. This system analyses human actions for anomalies by computing anomaly scores derived from video descriptors, including human poses and bounding boxes, obtained through pose estimation and tracking techniques. The process involves estimating human poses, applying Principal Component Analysis (PCA), determining Gaussian Mixture Model (GMM) parameters, and ultimately calculating anomaly scores using the GMM framework.

The study [15] introduces an innovative approach for real-time detection of violent and nonviolent human activities using an enhanced deep learning framework that integrates ResNet50 with LSTM networks. This method is capable of identifying nine distinct violent behaviours, such as attacking, fighting, object hitting, kicking, punching, pushing, shooting, slapping, and stabbing, as well as one normal, nonviolent behaviour. Altogether, the model classifies ten activity types with an achieved accuracy of 87.60%, implemented using TensorFlow, Keras, and high-performance computing infrastructure.Unlike traditional methods, which typically offer binary violent/nonviolent classification in post-event analysis of short video clips, the approach presented here supports real-time, multi-class recognition, enabling early detection and potential prevention of violent acts. Developing such a multi-class system poses considerable challenges, as the accuracy and efficiency of the model depend heavily on the balanced performance across all activity classes. Moreover, training the model is a resource-intensive and time-consuming process, requiring uninterrupted computation over several days.

3. Methodology

3.1 Dataset Explanation

- Anomaly_Score: A numerical value indicating the degree to which something deviates from a normal or expected pattern. Higher scores mean more anomalous.
- Confidence_Score: A numerical value representing the certainty or reliability of a detection, classification, or measurement (e.g., how confident a model is that it correctly identified an object). Higher scores mean more confident.

- Bounding_Box_X: The X-coordinate of the top-left corner of a bounding box, defining an object's horizontal position in an image.
- Bounding_Box_Y: The Y-coordinate of the top-left corner of a bounding box, defining an object's vertical position in an image.
- Bounding_Box_Width: The horizontal extent of a bounding box.
- Bounding_Box_Height: The vertical extent of a bounding box.
- Blur_Level: A measure of image blurriness. Higher values indicate more blur.
- Contrast_Level: A measure of the difference in brightness between light and dark areas in an image. Higher values indicate higher contrast.
- Noise_Level: A measure of unwanted random variation in image pixel values. Higher values indicate more noise.

3.2 Architecture:

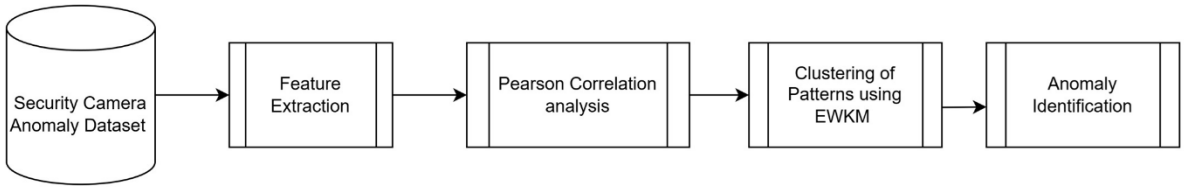

Fig 3.1 Architecture of Anomaly Detection using Entropy Weighted K Means

3.2.1 *Feature Extraction from Camera Footage:*

Security camera footage is continuous video data. To apply clustering, relevant features must first be extracted from the video frames or segments. These features could represent: Motion: Optical flow, trajectory of objects/people, Appearance: Color histograms, texture descriptors of objects, Spatial information: Bounding box coordinates (X, Y, Width, Height) of detected objects, Environmental factors: Blur_Level, Contrast_Level, Noise_Level (as these can affect detection quality and normalcy), Detection metrics: Anomaly_Score, Confidence_Score (if pre-computed by other modules).Each video segment or detected event would then be represented as a data point in a multi-dimensional feature space.

3.2.2. Assigning Feature Weights based on Entropy:

Before or during the K-Means iterations, the algorithm calculates the entropy for each feature across the dataset or within potential clusters.Features that show *less* variability (lower entropy) within a cluster or across the data might be considered more stable and therefore more important for defining distinct groups. Conversely, features with high variability (high entropy) might be less reliable indicators.Based on these entropy calculations, weights are assigned to each feature. A higher weight means that feature will have a greater influence on the distance calculation between data points, and thus on the formation of clusters.

3.2.2 *Weighted Distance Calculation in K-Means:*

In traditional K-Means, the distance between a data point and a cluster centroid is usually calculated using Euclidean distance, treating all features equally.In Entropy-weighted K-Means, the distance calculation is modified. Instead of simply summing the squared differences, each difference is multiplied by its corresponding feature weight. This means that

differences in highly-weighted (more important) features contribute more significantly to the overall distance, guiding the clustering process towards more meaningful groups.

3.2.3 Iterative Clustering and Anomaly Identification:

The K-Means algorithm then proceeds iteratively. Assignment Step: Each data point is assigned to the cluster whose *weighted* centroid it is closest to.Update Step: The centroids of the clusters are re-calculated based on the mean of the data points assigned to them, and the feature weights might also be re-evaluated and adjusted based on the characteristics of the newly formed clusters (e.g., if a feature shows low entropy within a specific cluster, its weight for that cluster might increase).This process continues until cluster assignments no longer change significantly or a maximum number of iterations is reached.

3.2.4 Anomaly Detection:

After clustering, "normal" behaviours in security camera footage will form large, dense clusters.Anomalies are identified as: Outliers: Data points that are far away from any cluster centroid (i.e., they don't fit well into any established "normal" pattern), Small, sparse clusters: Very small clusters that are isolated from the main clusters, suggesting a rare or unusual pattern of activity.

4. Results

Fig 4.1 presents Person correlation analysis of Anomaly detection and Fig 4.2 presents discriminant analysis of anomaly detection. Table 4.1 presents Sum of Square values of With in cluster Square distances.

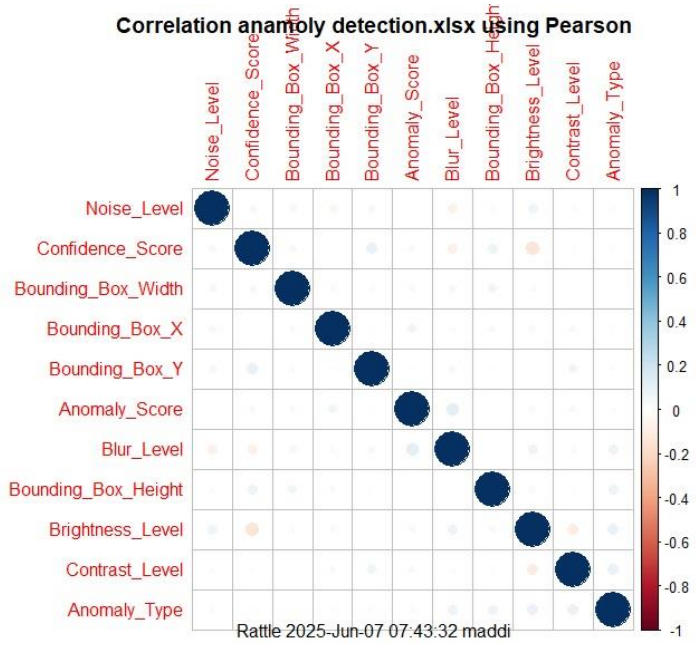

Fig 4.1 Results of Pearson Corelation between attributes

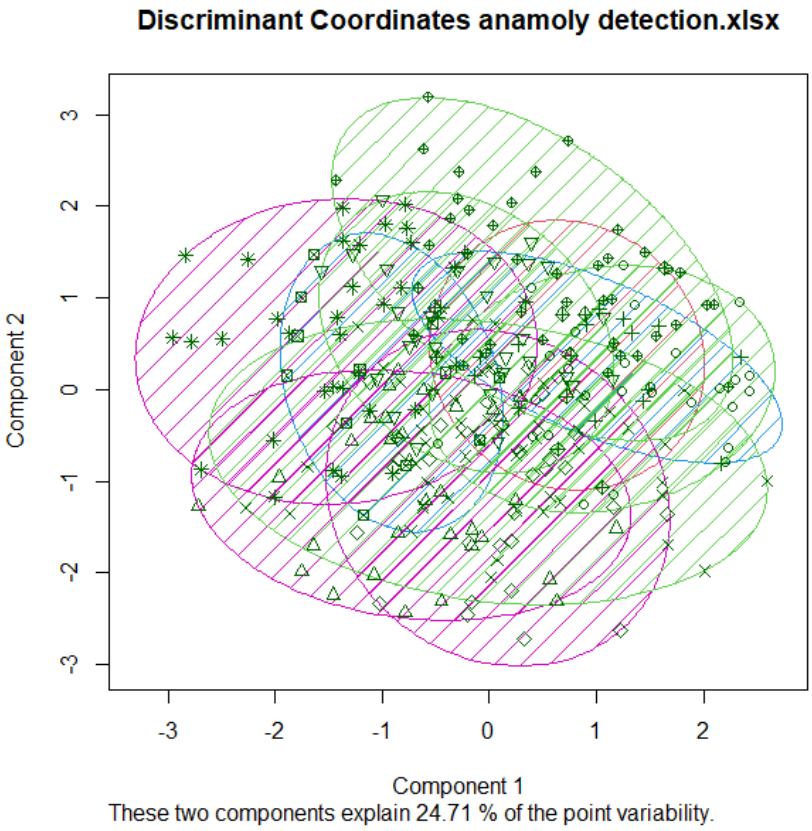

Fig 4.2 Discriminant analysis of Anomaly detection

Table 4.1 :Within cluster sum of square values

Cluster No	With In Cluster Sum of Squares
1	16.761939
2	19.310034
3	8.100868
4	34.933928
5	21.511958
6	17.140512
7	6.746775
8	23.668186
9	3.969041
10	23.842571

References:

[1].K. Gopalakrishnan, K. Kavitha, S. Manisha, S. G. Kanish, D. Dharshini and C. L. Dharshan, "Anomaly Detection in Surveillance Camera," *2024 13th International Conference on System Modeling & Advancement in Research Trends (SMART)*, Moradabad, India, 2024, pp. 156-159, doi: 10.1109/SMART63812.2024.10882190.

[2]. G. A. Affonso, A. L. L. De Menezes, R. B. Nunes and D. Almonfrey, "Using Artificial Intelligence for Anomaly Detection Using Security Cameras," *2021 International Conference*

on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Mauritius, Mauritius, 2021, pp. 1-5, doi: 10.1109/ICECCME52200.2021.9591068.

[3]. Soans, Sonia. (2025). Evaluating The Efficiency Of AI-Driven Person Identification Systems For Enhancing Campus Security: A Comparative Study Of Real-Time SurveillanceTechnologies. AMERICAN JOURNAL OF PSYCHIATRIC REHABILITATION. 28. 268-272. 10.69980/ajpr.v28i4.332.

[4]. Nhut, Do & Duat, Tran. (2025). Camera-based security system featured with laser detection and warning. Tạp chí Khoa học Lạc Hồng. 1. 1-5. 10.61591/jslhu.20.604.

[5]. Jiao, Runyu & Wan, Yi & Poiesi, Fabio & Wang, Yiming. (2023). Survey on video anomaly detection in dynamic scenes with moving cameras. 10.48550/arXiv.2308.07050.

[6]. Elmetwally, Ahmed & Eldeeb, Reem & Elmougy, Samir. (2024). Deep learning based anomaly detection in real-time video. Multimedia Tools and Applications. 84. 9555-9571. 10.1007/s11042-024-19116-9.

[7]. S. Golestani and D. Makaroff, "Device-Specific Anomaly Detection Models for IoT Systems," *2024 IEEE Conference on Communications and Network Security (CNS)*, Taipei, Taiwan, 2024, pp. 1-6, doi: 10.1109/CNS62487.2024.10735608.

[8]. A. Srinivasan, V. Parmar, T. Oh, J. Ryoo and M. Viglione, "Anomaly Detection System for Smart Home using Machine Learning," *2021 International Conference on Software Security and Assurance (ICSSA)*, Altoona, PA, USA, 2021, pp. 52-55, doi: 10.1109/ICSSA53632.2021.00018.

[9]. L. Kart and N. Cohen, "Approaches Toward Physical and General Video Anomaly Detection," *ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Singapore, Singapore, 2022, pp. 1785-1789, doi: 10.1109/ICASSP43922.2022.9747367.

[10]. Vijay Varadharajan, Uday Tupakula, Kallol Krishna Karmakar, “Techniques for Enhancing Security in Industrial Control Systems”,ACM Transactions on Cyber-Physical Systems, Volume 8, Issue 1

[11]. Aakash, L. Chauhan, S. Sharma and S. Deb, "Anomaly Detection from CCTV Camera Feed," *2024 IEEE International Symposium on Smart Electronic Systems (iSES)*, New Delhi, India, 2024, pp. 181-184, doi: 10.1109/iSES63344.2024.00045.

[12]. S. Sophia, A. Princely Nesaraj, A. Ajish Moses Raj and A. J. Dhivinkumar, "Home Security and Anomaly Detection System: A Comprehensive Solution," *2024 International Conference on Expert Clouds and Applications (ICOECA)*, Bengaluru, India, 2024, pp. 380-383, doi: 10.1109/ICOECA62351.2024.00074.

[13]. S. Sophia, A. Princely Nesaraj, A. Ajish Moses Raj and A. J. Dhivinkumar, "Home Security and Anomaly Detection System: A Comprehensive Solution," *2024 International Conference on Expert Clouds and Applications (ICOECA)*, Bengaluru, India, 2024, pp. 380-383, doi: 10.1109/ICOECA62351.2024.00074.

[14]. K. ICHIHARA, M. TAKEUCHI and J. KATTO, "Accuracy Evaluations of Video Anomaly Detection Using Human Pose Estimation," *2020 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 2020, pp. 1-2, doi: 10.1109/ICCE46568.2020.9043128.

[15]. Devang Jani, Anand Mankodia, "A Novel Approach for Real Time Multi-Scene Violent Activities Recognition with Modified ResNet50 and LSTM," *International Journal of Engineering Trends and Technology*, vol. 70, no. 8, pp. 292-309, 2022. Crossref, **https://doi.org/10.14445/22315381/IJETT-V70I8P231**