JOURNAL OF BASIC SCIENCE AND ENGINEERING

EARLY DETECTION OF SECURITY CAMERA TAMPERING FOR VIDEO CONTENT ANALYSIS SYSTEM

R.Ganapathyraja[1] and S.P. Balamurugan[2]

[1] ,Deparment of Computer & Information Science,Annamalai University, Chidambaram, TamilNadu, India, r.ganapathyrja@gmail.com

[2],Department of Computer & Information Science,Annamalai University, Chidambaram, TamilNadu, India, spbcdm@gmail.com

Corresponding author: S.P. Balamurugan, Email: spbcdm@gmail.com

ABSTRACT

The objective of this paper is to early detect security camera tampering with the proposed algorithm to address the two major issues of camera tampering attacks such as camera defocus and camera-lens block. These anomaly events such as screen shaking, flickering, color casting and lens cover significantly impact the effectiveness of video surveillance systems. The purpose of the algorithm is to measure the distance between a moving object and the camera's field of view. Because of this close distance estimation can detect camera tampering earlier. To evaluate the performance of the proposed algorithm, three video datasets with various types of camera attacks were tested with 64 anomalous events in video sequences. The proposed algorithm demonstrated its efficiency with an average of 3.1% missing events and an average of 7.8% false alarms in the experimental results.

Keywords: Camera Tamper, Video Content Analysis, Object Detection, Object Tracking, Object Distance, Camera Defocused, Camera-Lens Blocked, Focal Length, Anomaly Events.

1. INTRODUCTION

Video surveillance systems known as CCTV cameras are deployed on every premise for safety purposes for monitoring illicit activity and crime prevention[1].In today's technologically advanced world, intelligent video analytics have replaced traditional video surveillance in most places. Consequently, it reduces the time and difficulties associated with long-term screen monitoring, and address the issue of cameras being left unattended by operators[2]. Additionally, the use of automatic systems has significantly improved content analysis performance. This shift towards intelligent video analytics has brought about transformative improvements in video surveillance technology. However, after the offender has entered the premises, first they tamper with the CCTV camera to prevent the crime from being captured. Therefore, camera tamper detection should be an essential initial component of intelligent video content analysis (VCA)[3] systems. Afterward, there should be a system that detects other abnormal events.

Security Camera tampersAttack

A camera tamper attack is asustained event that disturbs or blocks the video surveillance camera process. In order to secure tamper with cameras, the initially is to identify the various

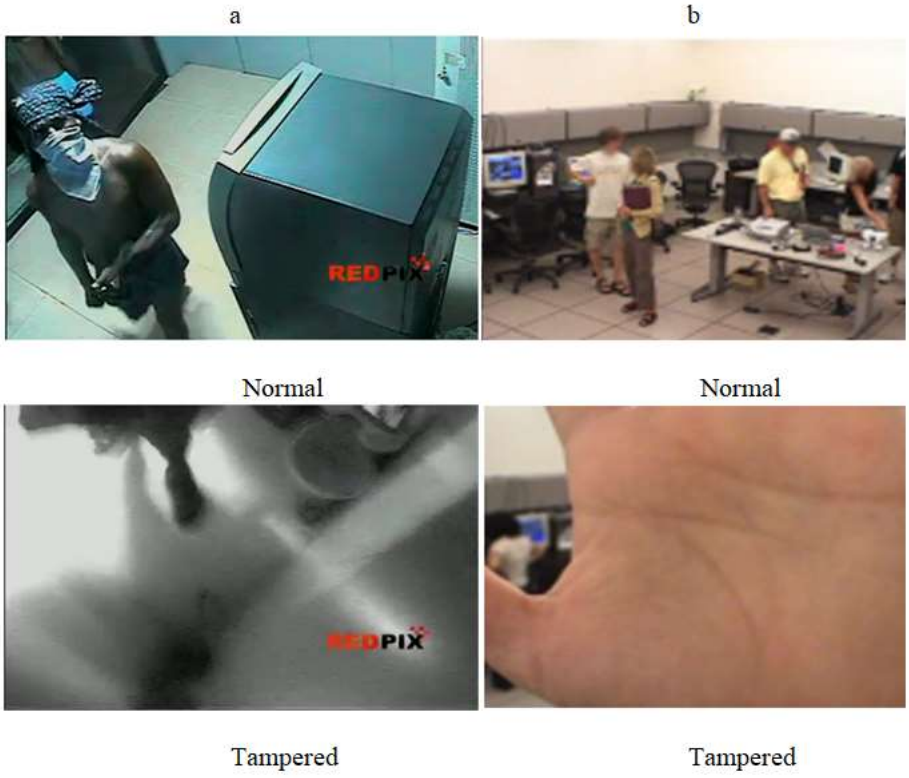


Figure 1. Camera Tamper: (a) Camera Defocused (b) Camera lens Blocked

methods of camera tampering[4]. There are two most common Camera tampering attacks. One is the camera defocused and another is the camera lens blocked as in shown Figure 1. It includes several types of camera tampering attacks. A defocused camera attack is one in which the focus of the camera direction changes the direction from the focused position based on the moved camera intentionally changing the camera focus or physically attacking and damaging the security camera. A camera lens-blocked attack is one in which the camera lens is partially or completely occluded by external objects based on spaying the foam or paint[5].Mostly, these incidents happen in ATMs and banking premises[6]. During the robbery, the offender aims to hide his identity, and robbery events are blocked to capture on the security camera.

Research Objective

The objective of this article is to provide a solution for the above attack events involving changing focused image frames and a sudden change in block out image frames. The early camera tamper detection algorithm is a proposed methodology to detect early tamper and send alert notifications to security officers based on dynamic scene changes in camera object distance estimation.

The rest of this paper is organized as follows. Section 1 introduces a proposed method for early detection of camera tampering attacks and discusses the most common camera tampering

attacks. Section 2 examines previous studies on camera tamper detection-related works and tampering attacks in various methods. In Section 3, architecture for early camera tamper detection is proposed in video content analysis. Section 4 presents the experimental results and discussions, while Section 5 includes the conclusion and future research work.

2. Related Work

Most previous literature studies focused on camera tampering attacks classified as defocussed, moved, and covered. Most researchers work on camera tamper detection based on sudden color changes, intensity histograms, and image edges.

Deng-Yuan Huang et al.[5] proposed an automated video surveillance system for rapidly detecting camera tampering and various abnormalities based on brightness analyses, image edges, histogram distribution, and high-frequency information. This method's abnormalities have focused on screen shaking, defocus, color cast, and screen flickering events.it is computationally efficient average of 4.4% of missed events. Gil-beom Lee et al. [4]proposed a novel unified camera tamper detection algorithm to detect the tampering attack types like covered, moved, and defocused. The algorithm measured the amount of edge pixels that disappear in the current frame from the background frame while excluding edges in the foreground and object information from the video analytics algorithms. The performance of the proposed algorithm tamper attacks are detected by comparing the difference between the EDR and the AEDR, with the adaptive threshold reflecting environmental conditions. Pranav Mantini et al.[7] Researchers have proposed a large-scale synthetic dataset called the University of Houston Camera Tampering Detection dataset (UHCTD) to test and develop camera tampering detection methods. It consists of a total of 576 tampers with over 288 hours of video captured from two surveillance cameras. The algorithm used four classifications, Alexnet, Resnet18, Resnet50, and Densenet161, to detect four classes of images: normal moved, defocused, and covered. Evan Ribnick et al.[8] introduced a new method for detecting camera tampering in real time. The technique involves comparing recent and older frames of video using three distinct measures of image dissimilarity, leading to accurate results. By setting optimal threshold values, the system can determine whether tampering has taken place with high precision. The approach proposed by the authors shows promise in addressing the issue of camera tampering in various applications.

Most of the researchers have been camera tamper detected after the camera tampered events happened, not to prevent before this event. In this proposed algorithm, early detect the tampering of the security camera in real-time video surveillance.

3. Proposed Method

Conventional video content analysis is used to detect abnormal activity events. It is not focused on camera tamper detection. In the proposed method, to early detection of camera tampering

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

attacks events embedded into are video content analysis systems based on object distance measurements.

3.1. Architecture of camera tamper detection

The proposed method addresses and resolves two common camera tampering issues such as defocused the cameras and blocked the camera lenses. A novel and efficient algorithm was developed by VCA to prevent camera tampering by utilizing computer vision techniques for object detection, tracking, and distance estimation methods as shown in Figure 2.

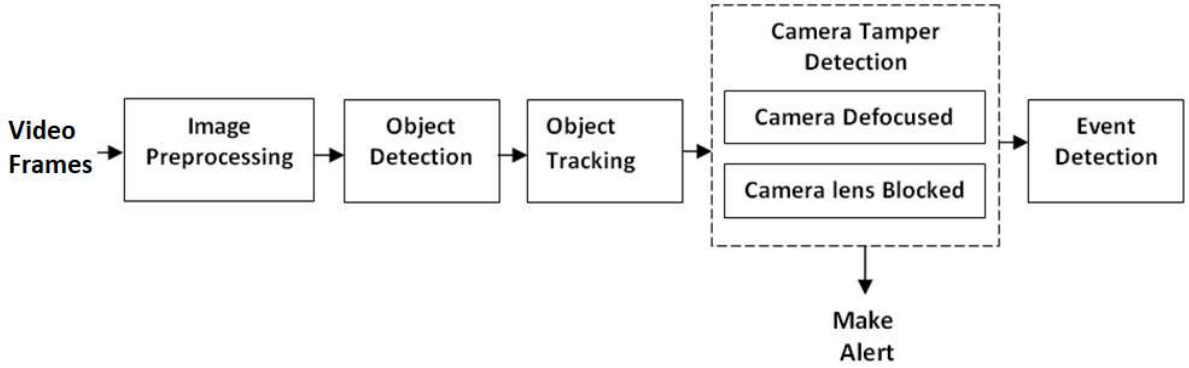


Figure 2.Camera Tamper Detection in Video Content Analysis (VCA)

3.2. Pre-processing

Video preprocessing is a crucial first step to eliminate unwanted noise and enhance the image quality, leading to better performance and accurate detections. The first step in this proposed is that method input video is converted into RGB image frames, and then those images are processed into grayscale image frames. A Histogram Equalization (HE) is applied to the image frame to reduce illumination noise and enhance intensity[9]. Finally, image frames are smoothed using Gaussian blur.

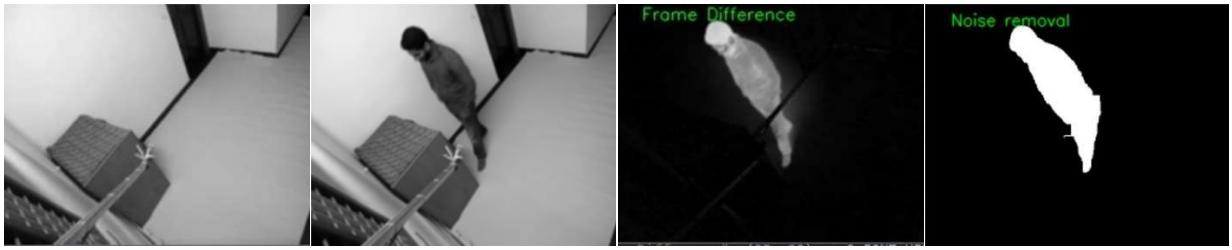
3.3. Object Detection and Segmentation

Object detection is a vital role of the first processing stage in VCA[10]. If the object is detected first segment the If the object is detected first segments the foreground from the background scene in the video frames and extracts the foreground objects. In this object may be static or moving in the video frames. The proposed method requires both foreground moving and static objects detection in the videos. In general background subtraction method not performed well the static object detection while moving object detection[11].Hence, in this work to utilize the Adaptive Frame Difference (AFD) method[10]. In AFD, the number of inter-frames varies based on the variations in the images. The threshold value is calculated automatically using a modified triangular algorithm to reduce the noise. Its detects well both static and moving objects

in the videos. And also It detects objects which move fast or slow. The interframe difference method computes FD by finding the absolute difference of adjacent frames using Equation 1.

$$FD_k(x,y) = \left| f_k(x,y) - f_{k-n}(x,y) \right| \geq T_k \quad (1)$$

Where FD_k is the difference image, k is the current image frame, n is the background reference frame of the current frame, and a variables T is threshold. The static or moving foreground object region is separated from the background scene using the AFD method. The result of frame difference image is converted into a binary image and segments the region of interest (ROI) objects using binary threshold techniques[12]. Finally, remove the noise in the binary frame applied morphological closing operation as shown in Figure 3.



(a) (b) (c) (d)

Figure 3. (a) Reference frame (b) current frame (c) foreground segment frame (d) ROI Object noises removed in the binary image frame

3.4. Object Tracking

Object tracking is the vital role of video surveillance in the trajectory position and orientation of objects[1][13] in each video frame. In this work, a contour-based object tracking method is used to track the detected objects. Segmented object contour features image moments(Eq.2),centroid(Eq.3) and Contour Area(Eq.4) are important of this proposed method[14][15]. Hence Contour-based object tracking algorithms[16] are used to find the shape of contour in the segmented objects, as well as to track the centroid position of the objects as shown Figure 4.

$$M_{ij} = \sum_x \sum_y x^i y^j I(x,y) \quad (2)$$

$$C_x, C_y = \sum_x \sum_y \left(x - \bar{x}\right)^p \left(y - \bar{y}\right)^q f\left(x,y\right)$$
$$\bar{x} = \frac{M_{10}}{M_{00}} \text{ and } \bar{y} = \frac{M_{01}}{M_{00}} \quad (3)$$

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

$$CA = \sum_{x=0}^{w} \sum_{y=0}^{h} f(x, y) \tag{4}$$

In Equation 2: x and y denotes the row and column of pixel position and the pixel intensity of current location is I(x, y). Equation 3: Centroid of pixels p, q at the location of x, y in the ROI. Equation 4: w and h represents the contour boundaries width and height. X and Y represent the pixel location.

Most of the proposed methods detected objects represented axis-aligned bounding boxes (AABB). Since this bounding box object coordinates of the bounding boxes parameters of xmin, ymin, width and height are calculated, the area of the rectangular object will be high aspect ratio[17] . Thus proposed method detected object shape is contour-based tracking in the video frames representing the orientation rotated boundary box. Objects with these two bounding boxes are compared with critical dimensions width and height as shown in Figure 4 (a) to (d).

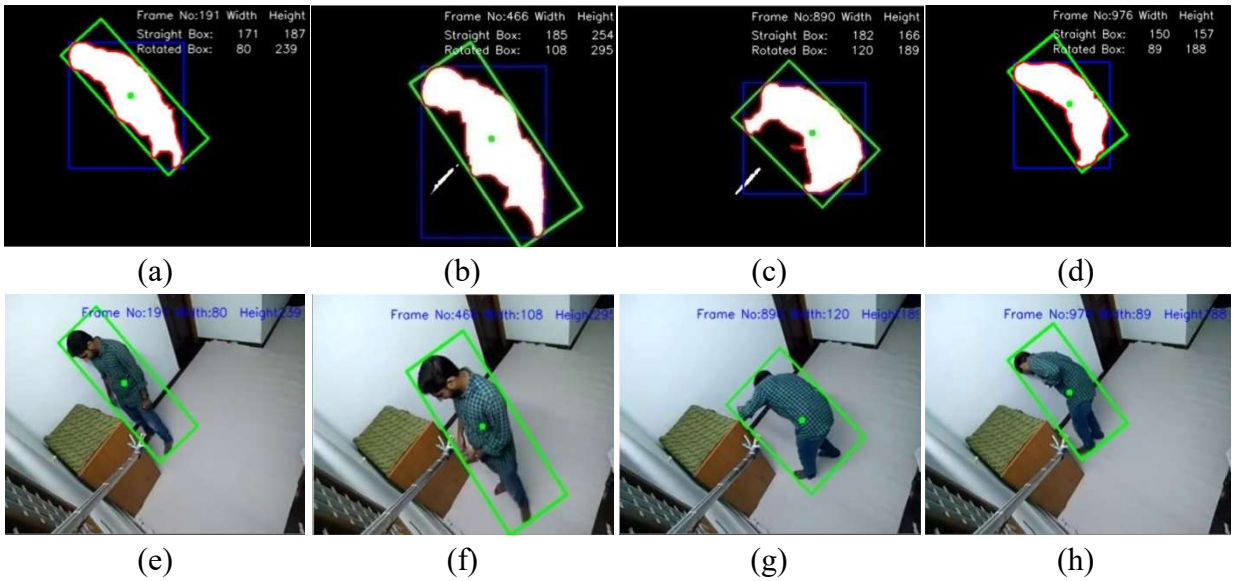


Figure 4. (a) to (d) comparsion of axis-aligned bounding blue box and rotated green box width and height. (e) to (h) r real-time frames detect the human shape object perfect in the green box and accurately.

In this method object's dimensions (width and height) play a vital role in distance measurement[18]. The point is set as the centroid point of the contour shape target objects as shown in Figure 4. An accurate representation of an object's centroid is especially important for tracking objects in small regions of image frames.

3.5. Camera Tamper Detection Algorithm

This proposed algorithm is developed for early detection of camera tampering based on the camera defocused and camera lens blocked. These two main attacks are made with objects such as metal sticks, clothes, foams, paints, and more. Hence, in this scenario, the purpose of the method

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

is to measure the distance between a moving object and the camera's field of view. By measuring the distance to these objects the camera can detect attack events earlier.

Object Distance Estimation

A distance estimate of humans or any objects from a video surveillance camera is essential to the proposed method. Accordingly, a camera calibration system[19] can transform and measure real-world object coordinates into image coordinates using a set of parameters such as focal length, tilt angle, and camera height as shown in the Figure 5.

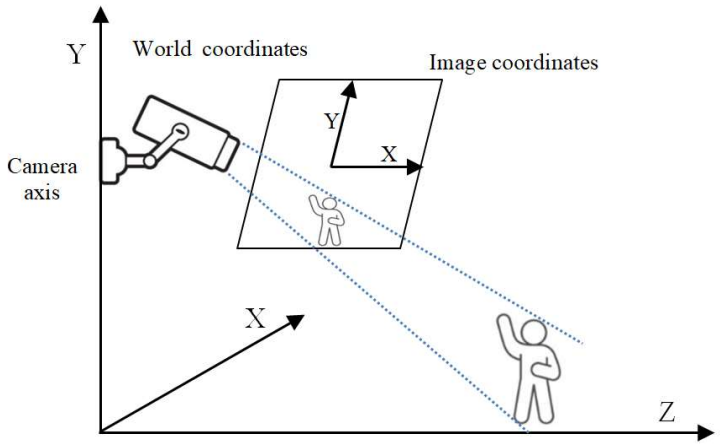


Figure 5.Camera coordinate system in video surveillance

To find the focal length[20], initially to measure the camera's distance from the camera to the reference image frame, the object width in the reference image frame and the detected object width. The focal length (F) is calculated as:

$$FL = \frac{m\_distance \times refimg\_obj\_width}{real\_obj\_width} \quad (5)$$

Where m_distance is the actual known distance from the camera to the object in the while captured image frame height, refimg_obj_width is the object width in reference image frame and real_obj_width is the detected moving real object width. The main objective is to calculate the moving distance of the tracked object from the camera's point of view. The object distance (OD) is calculated as follows:

$$OD = \frac{refimg\_obj\_width \times FL}{real\_obj\_width} \quad (6)$$

These equations 5 and 6 accurately estimate the distance of a moving object in front of the camera view. As a result of this estimated distance of the object that comes closest to the camera focus, it generates an alert for tamper detection events. The pseudo code of the camera tamper detection is as follow:

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

```
Input :measured distance, reference image object width, real object width
Output: Alert for early camera tamper

COMPUTE Focal Length FL (using Eq.5)
COMPUTE Object Distance OD(using Eq.6)
SET Framecount=0
If  OD < 100 then // Defining a distance limit
    Marked as RED box detected object in current frame
    //Frame time counter started
      If Framecount > 30 then // pre-defined Frame time
        Confirmed  Anomaly event & Make Alert Sound
      end if
else
    Discard and marked as Green box detected object in current frame
end if
```

4. Experimental Results and Discussions

4.1. Experimental Environments

This system is implemented using Python 3.8 and OpenCV 4.1.2, and the processor is a Ryzen 5 3500U running at 2.10 GHz with 8 GB of RAM. To evaluate the performance of the proposed algorithm, video sequences with three kinds of camera tampering with a total of 64 anomaly events were tested in the experiment, these are Mock ATM setup video datasets[21] for camera-defocused(26), real-time camera attacks in ATM premises CCTV footage from YouTube[22] for camera-defocused(20), and IP camera real-time videos for camera-lens blocked(18).

Experiment1: To evaluate the performance of the proposed algorithm the Immanuel Varghese's test video contains a scene of a person walking near the camera. In experimental conditions, it requires object distances to be outside predefined boundaries. This algorithm accurately detects, tracks, and measures the distance of a moving person in the testing video. The person who crosses the limit will be detected (red mark) and an alert will be made as shown in the Figure 6.

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

a b c

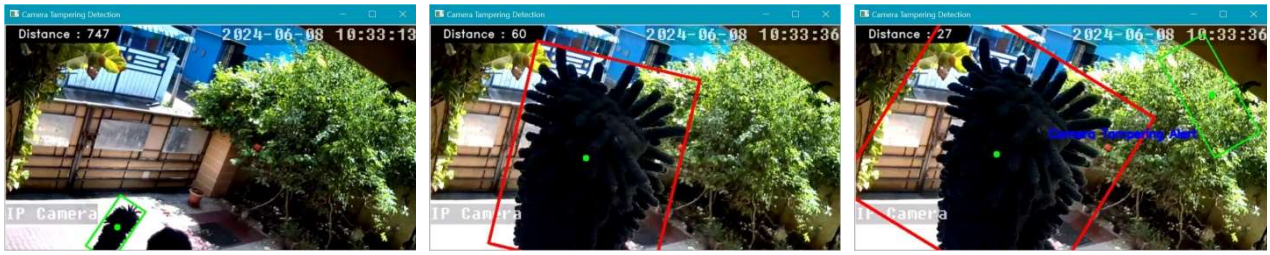
Figure 6. (a) Person accesses the ATM (b) Person crosses the limit (c) Person sustained the frame time & tamper alert

Experiment2: This experiment evaluated real-time CCTV camera attack footage on a YouTube video. Two persons enter the ATM premises. A person attacks the camera multiple times with iron stick. The Figure 7 shows that this algorithm can preemptively detect objects and people as they move too close to the camera before the camera strikes.

a b c

Figure 7. (a) Person enter ATM premises (b) Person crosses the limit (c) A person tries to attack the camera and earlier alert.

Experiment3: A real-time IP camera is used to perform a blocked assessment of the camera lens. In this real-time experiment, a cloth stick tries to cover the camera lens and the algorithm detects it early as shown in Figure 8.



a b c

Figure 8. (a) Object detects in Real-time IP camera (b) cloth crosses the limit (c) The cloth tries to cover the camera lens and also earlier alert

4.2. Performance Measures and Evaluations

The performance of the experimental results in the proposed algorithm is presented in terms of the number of false alarms, number of events Detected, percentage of true alarm rate and percentage of events detected rate for the camera defocused and blocked attacks in Table 1.

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

Table1 Camera tampering detection accuracy of the proposed algorithm

Experiments	False Alarms	Missed Events	True Alarm Rate	Event Detection Rate
Experiment 1	0	1	100%	96.5%
Experiment 2	3	1	85.0%	95.0%
Experiment 3	2	0	88.9%	100%

In the above Table1, shows that a total of 2 anomalous events were missed, indicating an average of 3.1% missed events, and a total of 5 false alarms, indicating an average of 7.8% false alarms were obtained from the proposed algorithm.

5. Conclusion

This paper implemented an algorithm for real-time camera tamper detection at an early stage. A proposed algorithm for detecting camera tampering demonstrates that it can detect both camera defocusing and blocking attacks based on object distance estimation. The other approaches use separate methodologies for each camera attack. The proposed algorithm reduces the processing time compared to the conventional algorithms and gives better results. Video sequences captured at nighttime in the same environment with an IR mode IP camera can be monitored for tamper attacks by the proposed algorithm. Furthermore, this system operates in real-time with a video frame rate of 20 to 30 frames per second. This algorithm provides a very low false alarm rate while providing high event detection rates in the experimental results.

References

[1] G. Mathur and M. Bundele, “Research on Intelligent Video Surveillance techniques for suspicious activity detection critical review,” *2016 International Conference on Recent Advances and Innovations in Engineering, ICRAIE 2016*, vol. 2016, pp. 1–8, 2016, doi: 10.1109/ICRAIE.2016.7939467.

[2] R. Ganapathyraja and S. P. Balamurugan, “An Extensive Review on Various Techniques for Suspicious Activities Detection in Intelligent Video Surveillance System,2021 IEEE International Conference on Emerging Trends in Industry 4.0 (ETI 4.0),” vol. 0, p. 6, 2021.

[3] M. Rai, A. Asim Husain, T. Maity, and R. Kumar Yadav, “Advance Intelligent Video Surveillance System (AIVSS): A Future Aspect,” *Intelligent Video Surveillance*, 2019, doi: 10.5772/intechopen.76444.

[4] G. B. Lee, M. J. Lee, and J. Lim, “Unified camera tamper detection based on edge and object information,” *Sensors (Switzerland)*, vol. 15, no. 5, pp. 10315–10331, 2015, doi: 10.3390/s150510315.

[5] D. Y. Huang, C. H. Chen, T. Y. Chen, W. C. Hu, and B. C. Chen, “Rapid detection of camera tampering and abnormal disturbance for video surveillance system,” *Journal of Visual Communication and Image Representation*, vol. 25, no. 8, pp. 1865–1877, 2014,

doi: 10.1016/j.jvcir.2014.09.007.

[6] T. Sikandar, K. Hawari, G. Mohammad, and F. Rabbi, "ATM crime detection using image processing integrated video surveillance : a systematic review," *Multimedia Systems*, vol. 25, no. 3, pp. 229–251, 2019, doi: 10.1007/s00530-018-0599-4.

[7] P. Mantini and S. K. Shah, "UHCTD: A comprehensive dataset for camera tampering detection," *2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance, AVSS 2019*, no. September 2019, 2019, doi: 10.1109/AVSS.2019.8909856.

[8] E. Ribnick, S. Atev, O. Masoud, N. Papanikolopoulos, and R. Voyles, "Real-time detection of camera tampering," *Proceedings - IEEE International Conference on Video and Signal Based Surveillance 2006, AVSS 2006*, pp. 10–15, 2006, doi: 10.1109/AVSS.2006.94.

[9] V. Tsakanikas and T. Dagiuklas, "Video surveillance systems-current status and future trends," *Computers and Electrical Engineering*, vol. 70, pp. 736–753, 2018, doi: 10.1016/j.compeleceng.2017.11.011.

[10] M. Zabłocki, D. Frejlichowski, R. Hofman, and K. Gościewska, "Intelligent video surveillance systems for public spaces – a survey," *Journal of Theoretical and Applied Computer Science*, vol. 8, no. 4, pp. 13–27, 2014.

[11] R. Ganapathyraja, "A Comprehensive Analysis of Motion and Motionless Object Detection in Real Time Video Surveillance using Frame Difference and Background Subtraction,2022,Internatinal conference on Innovative Technologies and its Application in Higher Education-Science,." pp. 45–51, 2022.

[12] G. Thapa, "Moving Object Detection and Segmentation using Frame differencing and Summing Technique,International Journal of Computer Applications (0975 – 8887)," *International Journal of Computer Applications (0975 – 8887)*, vol. 102, no. 7, pp. 20–25, 2014.

[13] S. Chaudhary, M. A. Khan, and C. Bhatnagar, "Multiple Anomalous Activity Detection in Videos," *Procedia Computer Science*, vol. 125, pp. 336–345, 2018, doi: 10.1016/j.procs.2017.12.045.

[14] R. Ganapathyraja and S. P. Balamurugan, "Suspicious Loitering detection using a contour-based Object Tracking and Image Moment for Intelligent Video Surveillance System," *JOURNAL OF ALGEBRAIC STATISTICS*, vol. 13, no. 2, pp. 1294–1303, 2022.

[15] A. Mondal, S. Ghosh, and A. Ghosh, "Efficient silhouette-based contour tracking using local information," *Soft Computing,Springer*, 2014, doi: 10.1007/s00500-014-1543-y.

[16] H. Y. Cheng and J. N. Hwang, "Integrated video object tracking with applications in trajectory-based event detection," *Journal of Visual Communication and Image Representation*, vol. 22, no. 7, pp. 673–685, 2011, doi: 10.1016/j.jvcir.2011.07.001.

[17] S. C. A. * and A. S. J. Rajesh Kumar Tripathi, "Real-time based human-fall detection from an indoor video surveillance,Int. J. Applied Pattern Recognition," vol. 5, no. 1, pp.

72–86, 2018.

[18] R. Mahajan and D. Padha, “Human detection and motion tracking using machine learning techniques: A review,” *PDGC 2018 - 2018 5th International Conference on Parallel, Distributed and Grid Computing*, pp. 127–131, 2018, doi: 10.1109/PDGC.2018.8745852.

[19] S. Li, V. H. Nguyen, M. Ma, C. Bin Jin, T. D. Do, and H. Kim, “A simplified nonlinear regression method for human height estimation in video surveillance,” *Eurasip Journal on Image and Video Processing*, vol. 2015, no. 1, pp. 1–9, 2015, doi: 10.1186/s13640-015-0086-1.

[20] N. Kim, J. Bae, C. Kim, S. Park, and H. G. Sohn, “Object distance estimation using a single image taken from a moving rolling shutter camera,” *Sensors (Switzerland)*, vol. 20, no. 14, pp. 1–17, 2020, doi: 10.3390/s20143860.

[21] E. Varghese, J. Mulerikkal, and A. Mathew, “Video Anomaly Detection in Confined Areas,” *7th International Conference on Advances in Computing & Communications,Procedia Computer Science,Elsevier*, vol. 115, pp. 448–459, 2017, doi: 10.1016/j.procs.2017.09.104.

[22] “ATM Anomaly Video Dataset- camera attack 75 https://www.kaggle.com/datasets/mehantkammakomati/atm-anomaly-video-dataset-atmav,” p. 75.