PREDICTING ROBBERY BEHAVIOR POTENTIAL IN INDOOR SECURITY CAMERAS USING PROPOUNDING FIRST AI APPROACH

[1] *Darruru Munemma,*[2] *Dr. K .V. Uma Maheswari*
[1] *Student ,*[2]*Associate Professor*
Department Of Computer Science & Engineering
Dr. K. V. Subba Reddy Institute Of Technology,Kurnool

ABSTRACT

Crime prediction in video-surveillance systems is required to prevent incident and protect assets. In this sense, our article proposes first artificial intelligence approach for Robbery Behavior Potential (RBP) prediction and detection in an indoor camera. Our method is based on three detection modules including head cover, crowd and loitering detection modules for timely actions and preventing robbery. The two first modules are implemented by retraining YOLOV5 model with our gathered dataset which is annotated manually. In addition, we innovate a novel definition for loitering detection module which is based on DeepSORT algorithm. A fuzzy inference machine renders an expert knowledge as rules and then makes final decision about predicted robbery potential. This is laborious due to: different manner of robber, different angle of surveillance camera and low resolution of video images.We accomplished our experiment on real world video surveillance images and reaching the F1-score of 0.537. Hence, to make an experimental comparison with the other related works, we define threshold value for RBP to evaluate video images as a robbery detection problem. Under this assumption, the experimental results show that the proposed method performs significantly better in detecting the robbery as compared to the robbery detection methods by distinctly report with F1-score of 0.607. We strongly believe that the application of the proposed method could cause reduction of robbery detriment in a control center of surveillance cameras by predicting and preventing incident of robbery. On the other hand, situational awareness of human operator enhances and more cameras can be managed.

I. INTRODUCTION

Today, surveillance cameras are widely used in various places such as stores, banks, airports and homes, to increase public safety and prevent the occurrence of crime. Alternatively, the time and place of the crime and specifically the wrongdoer, can be achieved by analyzing these videos and aiming to identify the delinquent. Meanwhile, someone is needed behind the scene, watching the videos and noticing whenever something anomaly is happening. However, due to very rare occurrence of an anomaly, the person becomes tired and if an anomaly happens, sometimes he cannot realize its occurrence. In other words, he loses the anomaly [1]. Furthermore, the anomaly-detection process is based on human common feeling which is learned during years. On the other hand, skill amount of the person for signs of crime occurrence understanding ability and the cost of employing him are other problems of non automated crime prediction and detection systems which are based on watching surveillance videos.

To automate anomaly detection, some visual features must be extracted using machine learning and deep learning algorithms [2], [3]. For better performance of these algorithms, specific features for different anomaly classes [4] like vandalism [5], violence detection [6] and robbery [7] can be useful.Predicting the location and time of the crime reducing the destruction. On the other hand, security forces are also present on time such as an experiment, manufactured in Santa Cruz, California, where officers benefit from daily crime forecasts every morning. This forecasting navigates them to patrol determined regions. A Santa Cruz spokesperson declared that thirteen

wrongdoers have been stopped in the determined areas during first the six month of experiment [8].Due to paper [8], [9], and [10], some main symptoms prove that predictive policing is significant to be used for federal financing and security systems including: cost saving and crime reduction. Violent crimes are more dangerous because of their victimization probability and they increased by 20%due to Seattle Police Department (SPD) report during 2021 in Washington, USA [11]. According to statics acquired from Federal Bureau of Investigations-Uniform Crime Reporting System (FBI-UCR), robbery is one of five common crimes in the United States [12]. The detection of robbery is one of the purposes of installing surveillance cameras in many places. Robbery is the crime of taking or attempting to grab any property by force, threat or weapon [13] based on oxford dictionary definition and differentiated from other forms of theft such as shoplifting, pickpocket or burglary, by its intrinsically violent essence [14], [15]. Whiles many lesser types of theft are punished as misdemeanors, robbery is always a felony in jurisdictions. Criminologists distinguish different types of robbery with regards to time and space of occurrence, armed or unarmed robberies, weapon types and force amount. Therefore, one typical scissor is commercial robberies and street robberies [16].Street robberies usually happens in poor crowded locations with no Closed-circuit televisions (CCTV). Commercial robberies occur in two ways: one where the offender enters the scene dressed up as a customer or conceal his face with normal covers like mask or helmets then suddenly out of the blue pulls a weapon and scares the employee. The other which offenders enter with force, typically in a group and probably conceal their face or head [17]. Both types of commercial robberies occurred in the indoor places which have customarily CCTVs so that detecting offenders or detection and even prediction of commercial robberies can be possible. Additionally, offenders who armed by weapon or knife usually threaten human with force. On the other hand, for offenders bearing any stick or be unarmed, a massive force is more probable [16], [17]. Hereupon, armed or unarmed commercial robberies force causes injury, pain and even death.

Thus, predicting commercial robbery behavior by human, machine or combination of these two, plays an important role in preventing its occurrence and its arisen dangers [18].

In general, there are some methods to automate detection or prediction of crimes based on extracting different crime scenarios and implementing them in different fields. But none of these methods have predicted the potential of robbery behavior. Therefore, there is a need to develop an algorithm for RBP prediction in video images. One could easily notice that, extracting the evidences and features in the surveillance videos is needed for prediction. To do this, the potential of robbery behavior in video images should be investigated. Scenarios of robbery occurrence, vary from one context to another [19] due to different conditions of each place selected for robbing and different cultures of countries. Therefore, robust feature extraction is not accompanied with certainty.

Despite the variety of robbery incidence scenarios and due to scenario-based approaches [20], [21], a common scenario with main points can be considered for commercial robbery videos. Specifically, one or some person choosing a poorly attended place who are usually covering their face or head by helmet, mask, glasses or any garment to not be recognized and they are loitering to get an opportunity for showing their weapon, threat or force. This scenario is completely matched with the knowledge of an expert person and definition of first type of commercial robbery behavior [17], [22]. To implement a system based on this common scenario abstracted from different scenarios inferred from robbery videos, we consider common features found in most robbery cases under three modules including: head cover, crowd and loitering detection. After extracting

these features, for modules implementation, an inference machine is needed to conclude on the RBP. The conclusion process must be as competence as a human decision making for potential derivation. Due to the ability of fuzzy set theory to mimic human inference [23], experience could be put in the form of fuzzy rules and according to fuzzy measurement, it facilitates the diagnosis and reasoning of a complex decision [24], [25]. Deep learning methods on the other hand, do not offer such adaptability and may not be able to deal with the nuances and variations of uncertain data well [25]. Owing to these reasons a fuzzy inference machine is proposed in this paper.

To sum up, main contributions of our paper are as below:

1. The proposed algorithm is based on a novel method

which can predict RBP and prevent damages resulted by its occurrence in indoor places. To the best of our knowledge, his is the first work focusing on robbery behavior prediction and grounded on three main modules: Head cover, crowd and loitering detection modules.

2. A dataset has been prepared for our system and annotated manually as two states: with or without head cover. For crowd counting, we sum the results of two states reported by head cover detection module. The method dominates the constraints of surveillance videos such as low resolution and single camera videos.

3. The loitering point we have defined, is a novel definition for loitering calculation. A Deep Simple Online Real-time Tracking (Deep SORT) algorithm has used with respect to the tracking methods to calculate amount of loitering for each person. By analyzing the obtained amount of loitering based on Euclidean distance calculation, a point has assigned to each one.

4. The key contribution of our algorithm is using a fuzzy inference machine with optimized rules, fuzzification and defuzzification steps. Obtained results of these three modules analyzed based on an expert person knowledge about robbery behavior and an inference machine.

The rest of paper is arranged as follows: Section II reviews some literature related to our work including suspicious behavior prediction or detection and also papers related to our modules. Section III explains proposed algorithm and outlines concepts of RBP prediction, the proposed modules and outcome to low-resolution video images by improving YOLOV5. Experimental results are presented and discussed in section IV. The last section concludes the research work and presents future works.

1.1 PURPOSE:

The purpose of proposing an artificial intelligence (AI) approach for predicting robbery behavior potential in an indoor security camera system can be multi-faceted, including:

1. Enhancing Security and Safety:

- **Proactive Measures:** By predicting robbery behavior, AI can enable security personnel to take proactive measures to prevent crimes before they happen, enhancing overall safety.
- **Real-Time Alerts:** AI systems can provide real-time alerts to security staff, enabling quick responses to potential threats.

2. Improving Surveillance Efficiency:

- **Automated Monitoring:** AI can continuously monitor security footage without fatigue, ensuring constant vigilance.
- **Resource Allocation:** Security teams can focus their efforts on verified threats, optimizing resource allocation and reducing the need for continuous manual monitoring.

3. Advanced Threat Detection:

- **Behavioral Analysis:** AI can analyze patterns of behavior that might indicate potential criminal activity, which may be missed by human observers.

-Pattern Recognition: By recognizing suspicious activities based on historical data and patterns, AI can identify potential threats more accurately.

4. Data-Driven Decision Making:

-Predictive Analytics: AI can leverage

historical data to predict future incidents, helping organizations to make informed decisions on security protocols and preventive measures.

-Trend Analysis: Understanding trends in robbery behaviors can help in formulating strategies to mitigate risks.

5. Cost Reduction:

- Lowering Operational Costs: By automating surveillance and reducing the need for a large number of security personnel, organizations can lower their operational costs.

- Preventing Losses: Preventing robberies can significantly reduce financial losses due to theft and damage.

6. Technological Advancement:

- Innovation in Security: Implementing AI for robbery prediction can position an organization as a leader in adopting innovative security technologies.

-Integration with Existing Systems: AI can enhance existing security systems by integrating with current surveillance infrastructure, improving overall system capabilities.

7. Legal and Compliance:

-Adherence to Standards: Using AI can help organizations comply with security standards and regulations that require advanced monitoring and threat detection capabilities.

-Evidence Collection: AI can aid in collecting and analyzing evidence in the event of an incident, supporting legal and investigative processes.

Overall, the primary purpose is to leverage AI's capabilities to create a more secure, efficient, and cost-effective surveillance system that can predict and prevent robbery behaviors, thus safeguarding people and property.

1.2 EXISTING SYSTEM:

Anomalies are infrequent observations, events or behaviors which are suspicious because they are significantly different from normal patterns. Crime is a kind of an anomaly which is any behavior deviating from a normal activity [2]. One could say that the proliferation usage of CCTV has been because of increasing crimes in public places. Crime can be predicted according to suspicious behavior detection. Prediction needs defective, vague and unsure information [26]. Our proposed approach concentrates on RBP prediction in indoor places. Robbery is a kind of crime and the proposed algorithm needs loitering, crowd and head cover detection. One important concept of our algorithm is providing a generic RBP prediction framework which is not addressed in any other paper. In this section, we will discuss about some related works relevant for suspicious behavior detection or prediction, crime detection or prediction and articles concerning with the loitering or head cover detection.

Elhamod and Levine [27] proposed a semantics-based suspicious behavior recognition algorithm based on object tracking by blob matching with color histograms and spatial information, for updating objects intended in each frame. For blob and objects similarity specification, intersection of histogram’s value is calculated and compared with the defined threshold. Next it assigns appropriate classes contains people for animated and objects for inanimated things. By calculating their 3D motion features and recording it in the form of historical records, behaviors are semantically determined. detected suspicious behaviors include: abandoned luggage by background subtraction methods, fainting by comparing assumed 2D and actual 3D location of person’s feet and also head coordinates of that person, fighting by computing merge, split and simultaneously movement of blob’s centroid and eventually loitering by aggregating presence time of a person in an area.

Ishikawa and Zin [18], introduced an automated normal system for questionable pedestrian detection by loitering detection. According to [18], a questionable person walks, stops and goes around the location repeatedly for a long time with enhancement

of direction changing number. His distance value is greater than the normal person and changing in acceleration is so much. To implement these features, [18] divides the video frames into 25 blocks and counts the frequency of block numbers which feet of person are in that location. if this frequency was more than threshold value, that person descent as suspicious pedestrian. To compute changing of direction, it calculates angles of moving direction. Computing of distance and acceleration changing extracts all needed features. Finally, a decision fusion process detects suspicious pedestrians by aggregating the scores of each step.

Rajapakshe et al. [28] presented an E-police system which contains two components: video surveillance monitoring system and crime prediction.To detect suspicious behaviors such as violent and vandalism, [28] uses human activity recognition methods and classifies them into normal and abnormal categories. They use Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) for feature extraction and detect suspicious human who conceal their faces. Crime prediction process of [28] is based on public information resources for place and time of crime occurrence prediction with the help of classification algorithms such as SVM and Decision tree.

Arroyo et al. [22] proposed an expert real-time suspicious behaviors detection system in shopping malls. They locate foreground objects by an image segmentation and background subtraction algorithm. Next, a blob fusion algorithm is used to gather the blobs of each segmented parts to detect human. A tracking algorithm is used with the help of a new two-step method: a) using a Kalman filter for detection and tracking human, b) SVM kernels for occlusion management. Then, the obtained trajectories of people are used to analyze human behaviors. The entrance or existence alarm is for the time that too many people enter or a person runs away and it is detected by trajectory analyzing. Moreover, specific risk areas are interiors with more expensive articles and chosen by the human security officers. Loitering of people is evaluated according to their trajectories and the length of time they present in those zones. If the time be more than 30 seconds, which has specified by security experts, their system gives off an alarm. They mounted a camera on the cash desk to protect it. If someone loiters around it, and no shop personnel attended in the cash desk zone, an alarm gives off. Additionally, evaluation process is done on a naturalistic dataset they provided by multi cameras located on entrance, interior and cash-desk of a shop.

Disadvantages:

• The complexity of data: Most of the existing machine learning models must be able to accurately interpret large and complex datasets to detect Android Malware Detection.

• Data availability: Most machine learning models require large amounts of data to create accurate predictions. If data is unavailable in sufficient quantities, then model accuracy may suffer.

• Incorrect labeling: The existing machine learning models are only as accurate as the data trained using the input dataset. If the data has been incorrectly labeled, the model cannot make accurate predictions.

1.3 Proposed System

1. The proposed algorithm is based on a novel method which can predict RBP and prevent damages resulted by its occurrence in indoor places.To the best of our knowledge, this is the first work focusing on robbery behavior prediction and grounded on three main modules: Head cover, crowd and loitering detection modules.

2. A dataset has been prepared for our system and annotated manually as two states: with or without head cover. For crowd counting, we sum the results of two states reported by head cover detection module. The method dominates the constraits of surveillance videos such as low resolution and single camera videos.

3. The loitering point we have defined, is a novel definition for loitering calculation. A

Deep Simple Online Real-time Tracking (DeepSORT) algorithm has used with respect to the tracking methods to calculate amount of loitering for each person. By analyzing the obtained amount of loitering based on Euclidean distance calculation, a point has assigned to each one.

4. The key contribution of our algorithm is using a fuzzy inference machine with optimized rules, fuzzification and defuzzification steps. Obtained results of these three modules analyzed based on an expert person knowledge about robbery behavior and an inference machine.

Advantages:

• An intelligent AAMD-OELAC technique comprising data preprocessing, ensemble learning, and HPO-based hyper parameter tuning is presented for Android malware detection. To the best of our knowledge, the AAMD-OELAC technique never existed in the literature.

• Perform ensemble learning-based classification process comprising LS-SVM, KELM, and RRVFLN models for Android malware detection.

• The combination of the HPO algorithm and ensemble learning process improves the detection accuracy of Android malware. By utilizing multiple classifiers and optimization strategies, the model can effectively identify malicious patterns and behaviours in Android applications.

II. LITERATURE SURVEY

"Real-world anomaly detection in surveillance videos." Sultani, Waqas, Chen Chen, and Mubarak Shah.

Surveillance videos are able to capture a variety of realistic anomalies. In this paper, we propose to learn anomalies by exploiting both normal and anomalous videos. To avoid annotating the anomalous segments or clips in training videos, which is very time consuming, we propose to learn anomaly through the deep multiple instance ranking framework by leveraging weakly labeled training videos, i.e. the training labels (anomalous or normal) are at video-level instead of clip-level. In our approach, we consider normal and anomalous videos as bags and video segments as instances in multiple instance learning (MIL), and automatically learn a deep anomaly ranking model that predicts high anomaly scores for anomalous video segments. Furthermore, we introduce sparsity and temporal smoothness constraints in the ranking loss function to better localize anomaly during training. We also introduce a new large-scale first of its kind dataset of 128 hours of videos. It consists of 1900 long and untrimmed real-world surveillance videos, with 13 realistic anomalies such as fighting, road accident, burglary, robbery, etc. as well as normal activities. This dataset can be used for two tasks. First, general anomaly detection considering all anomalies in one group and all normal activities in another group. Second, for recognizing each of 13 anomalous activities. Our experimental results show that our MIL method for anomaly detection achieves significant improvement on anomaly detection performance as compared to the state-of-the-art approaches. We provide the results of several recent deep learning baselines on anomalous activity recognition. The low recognition performance of these baselines reveals that our dataset is very challenging and opens more opportunities for future work. The dataset is available at: http://crcv.ucf.edu/projects/real-world.

"A survey on deep learning techniques for video anomaly detection." Suarez, Jessie James P., and Prospero C. Naval Jr.

Anomaly detection in videos is a problem that has been studied for more than a decade. This area has piqued the interest of researchers due to its wide applicability. Because of this, there has been a wide array of approaches that have been proposed throughout the years and these approaches range from statistical-based approaches to machine learning-based approaches. Numerous surveys have already been conducted on this area but this paper focuses on providing an overview on the recent advances in the field of anomaly detection

using Deep Learning. Deep Learning has been applied successfully in many fields of artificial intelligence such as computer vision, natural language processing and more. This survey, however, focuses on how Deep Learning has improved and provided more insights to the area of video anomaly detection. This paper provides a categorization of the different Deep Learning approaches with respect to their objectives. Additionally, it also discusses the commonly used datasets along with the common evaluation metrics. Afterwards, a discussion synthesizing all of the recent approaches is made to provide direction and possible areas for future research.

"Deep learning for intelligent video analysis." Mei, Tao, and Cha Zhang.

Big data applications are consuming most of the space in industry and research area. Among the widespread examples of big data, the role of video streams from CCTV cameras is equally important as other sources like social media data, sensor data, agriculture data, medical data and data evolved from space research. Surveillance videos have a major contribution in unstructured big data. CCTV cameras are implemented in all places where security having much importance. Manual surveillance seems tedious and time consuming. Security can be defined in different terms in different contexts like theft identification, violence detection, chances of explosion etc. In crowded public places the term security covers almost all type of abnormal events. Among them violence detection is difficult to handle since it involves group activity. The anomalous or abnormal activity analysis in a crowd video scene is very difficult due to several real world constraints. The paper includes a deep rooted survey which starts from object recognition, action recognition, crowd analysis and finally violence detection in a crowd environment. Majority of the papers reviewed in this survey are based on deep learning technique. Various deep learning methods are compared in terms of their algorithms and models. The main focus of this survey is application of deep learning techniques in detecting the exact count, involved persons and the happened activity in a large crowd at all climate conditions. Paper discusses the underlying deep learning implementation technology involved in various crowd video analysis methods. Real time processing, an important issue which is yet to be explored more in this field is also considered. Not many methods are there in handling all these issues simultaneously. The issues recognized in existing methods are identified and summarized. Also future direction is given to reduce the obstacles identified. The survey provides a bibliographic summary of papers from Science Direct, IEEE Xplore and ACM digital library.

"Real-time auto-matic detection of vandalism behavior in video sequences." Ghazal, Mohammed, Carlos Vázquez, and Aishy Amer.

This paper proposes a method for the real time detection of vandalism in video sequences. The proposed method detects vandalism through the robust extraction of a sequence of high-level events leading to it without resorting to object recognition and using a single camera. Vandalism is declared when an object enters the scene and causes an unauthorized change inside a predefined vandalisable area in the scene such as a pay phone or a sign. The proposed method was tested offline and on-line and our results show that it is robust in detecting vandalism or graffiti in surveillance video sequences.

"Automatic video-based human motion analyzer for consumer surveillance system." Lao, Weilun, Jungong Han, and Peter Hn De With.

With the continuous improvements in video-analysis techniques, automatic low-cost video surveillance gradually emerges for consumer applications. Video surveillance can contribute to the safety of people in the home and ease control of home-entrance and equipment-usage functions. In this paper, we study a flexible framework for semantic analysis of

human behavior from a monocular surveillance video, captured by a consumer camera. Successful trajectory estimation and human-body modeling facilitate the semantic analysis of human activities and events in video sequences. An additional contribution is the introduction of a 3-D reconstruction scheme for scene understanding, so that the actions of persons can be analyzed from different views. The total framework consists of four processing levels: (1) a preprocessing level including background modeling and multiple-person detection, (2) an object-based level performing trajectory estimation and posture classification, (3) an event-based level for semantic analysis, and (4) a visualization level including camera calibration and 3-D scene reconstruction. Our proposed framework was evaluated and has shown its good quality (86% accuracy of posture classification and 90% for events) and effectiveness, as it achieves a near real-time performance (6-8 frames/second).

"Automated visualsurveillance in realistic scenarios." Shah, Mubarak, Omar Javed, and Khurram Shafique.

In this article, we present Knight, an automated surveillance system deployed in a variety of real-world scenarios ranging from railway security to law enforcement. We also discuss the challenges of developing surveillance systems, present some solutions implemented in Knight that overcome these challenges, and evaluate Knight's performance in unconstrained environments.

III. SYSTEM DESIGN

Flow Chart : Remote User

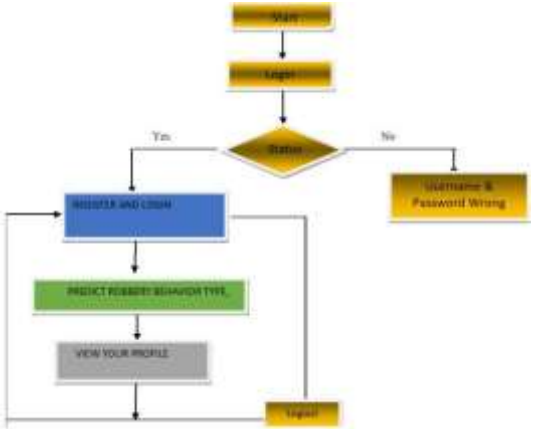


fig:2.1

- **Flow Chart :** Service Provider

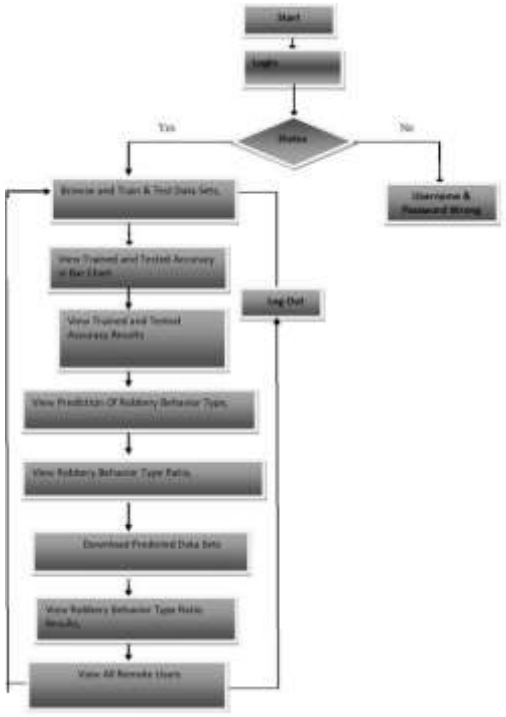
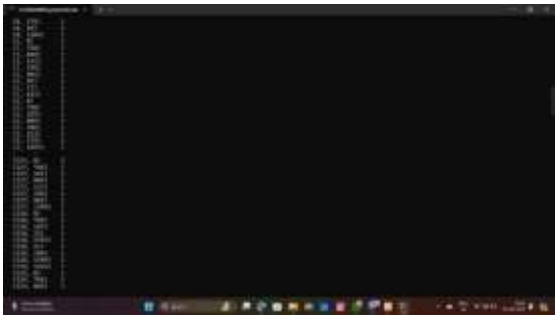
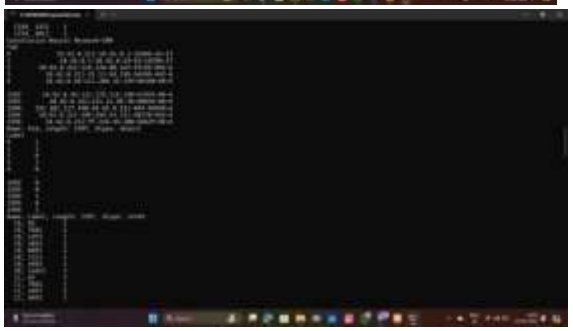


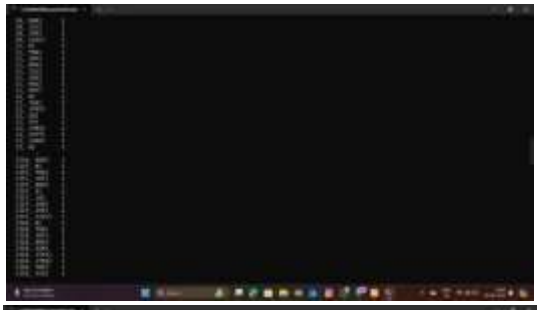
fig:2.2

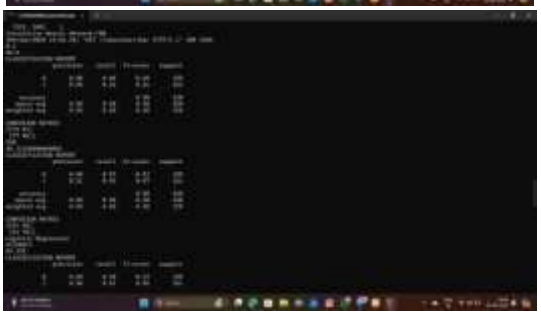
IV. SCREENSHOT

CODE

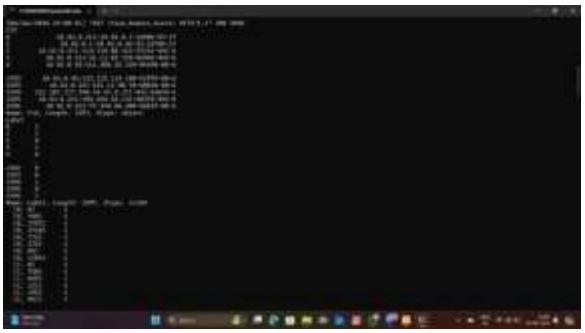








5.2.2.3 Result:



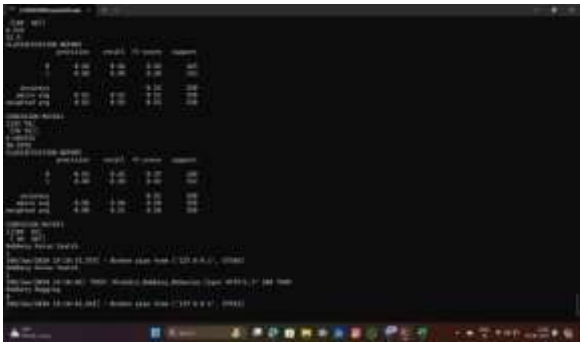


Fig: View all Remote Users

Fig: Datasets Trained and Tested Results

Fig: View Trained and Tested Accuracy in Bar Chart

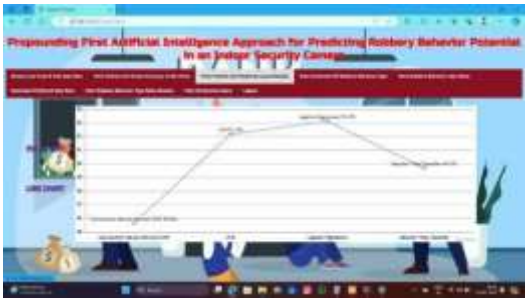


Fig: View Trained and Tested Accuracy Results

Fig: View Robbery Behavior Type Prediction Details

Fig: View Robbery Behavior Ratio Details

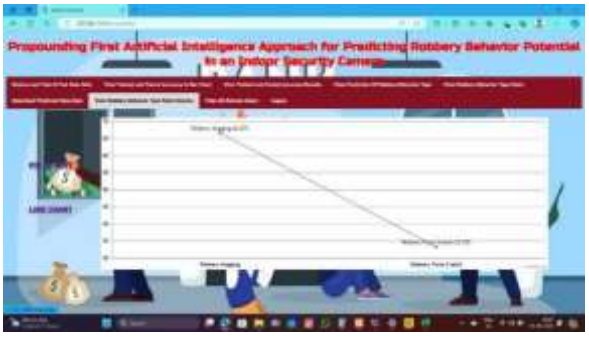


Fig: View Robbery Behavior Ratio Results

Fig: Prediction of Robbery Behavior Type

V. CONCLUSION

This research work proposes an approach for RBP prediction in video surveillance images. There are several challenges of CCTV videos like the various ways for robbery incidence, variety in camera angle mounted in different places and low resolution of video images acquired by CCTVs. Tackling these obstacles ensues timely actions and prevents robbery fully or partially observable from surveillance videos. This work is conducted because based on our extensive literature review, despite significance of preventing robbery occurrence, no RBP prediction has been done before. We extract some common scenarios of robbery occurrence with the help of an expert comments and by watching several robbery videos from CCTVs. We investigate these scenarios to deduce more common features between them and implement a practical approach for RBP prediction. Our study proposes a deep-learning based approach with the help of fuzzy inference machine to calculate potential of robbery. This approach provides a retrained YOLOV5 algorithm by gathering proper dataset of human with or without head cover. This deep-learning based algorithm is used to efficiently implement crowd and head cover detection modules. This paper also executes loitering module by our defined methodology which calculates the Euclidean traveled distance of individuals using Deep SORT method. A fuzzy inference machine is delineated to infer robbery potential of videos for every 10 frames and average them for every snippet based on three module results. The proposed method is applied to the Robbery folder of UCF-Crime dataset and F1-score of proposed system is 0.537. This result shows that our proposed methodology can correctly predict robbery potential for more than half of the videos.

Accordingly, we change the problem of predicting to robbery detection one. Thus, we can compare it with prior literature which have worked on the anomaly-detection specially the robbery detection and their dataset is UCF-Crime. F1-score of detection method is 0.607 and it is utmost among other methods. The result proves that our proposed scenario-based system works correctly with high ability in detecting and also predicting robbery behavior. Our proposed approach can be used by any places which have surveillance cameras and want to prevent robbery crime. They do not need to employ a person to watch the real time videos of theses cameras precisely and infer the robbery potential. However, this person should watch the videos uninterruptedly to not make a mistake. Additionally, any one can make our methodology privately by changing the thresholds value due to particular culture.

We can increase F1-score by improving loitering detection accuracy. As future work, we intend to achieve an improved tracking algorithm for low-resolution video images by improving Deep SORT method. Human of low- resolution videos cannot be detected precisely to track. This is because the detector of Deep SORT algorithm is FRR CNN. Therefore, we will change detection framework of Deep SORT algorithm to retrained YOLOV5 by low-resolution human images. The proposed YOLOV5 will have only one object class, low resolution images.

BIBLIOGRAPHY

[1] W. Sultani, C. Chen, and M. Shah, ‘‘Real-world anomaly detection in surveillance videos,’’ in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, Jun. 2018, pp. 6479–6488.

[2] J. James P. Suarez and P. C. Naval Jr., ‘‘A survey on deep learning techniques for video anomaly detection,’’ 2020, *arXiv:2009.14146*.

[3] T. Mei and C. Zhang, ‘‘Deep learning for intelligent video analysis,’’ in *Proc. 25th ACM Int. Conf. Multimedia*, Oct. 2017, pp. 1955–1956.
[4] H. Yan, X. Liu, and R. Hong, ‘‘Image classification via fusing the latent deep CNN feature,’’ in *Proc. Int. Conf. Internet Multimedia Comput. Service*, Aug. 2016, pp. 110–113.
[5] M. Ghazal, C. Vazquez, and A. Amer, ‘‘Real-time automatic detection of vandalism behavior in video sequences,’’ in *Proc. IEEE Int. Conf. Syst.,Man Cybern.*, Oct. 2007, pp. 1056–1060.
[6] I. P. Febin, K. Jayasree, and P. T. Joy, ‘‘Violence detection in videos for an intelligent surveillance system using MoBSIFT and movement filtering algorithm,’’ *Pattern Anal. Appl.*, vol. 23, no. 2, pp. 611–623, May 2020.
[7] W. Lao, J. Han, and P. De With, ‘‘Automatic video-based human motion analyzer for consumer surveillance system,’’ *IEEE Trans. Consum. Electron.*, vol. 55, no. 2, pp. 591–598, May 2009.
[8] A. G. Ferguson, ‘‘Predictive policing and reasonable suspicion,’’ *Emory Law J.*, vol. 62, no. 2, p. 259, 2012.
[9] C. Beck and C. McCue, ‘‘Predictive policing: What can we learn from Wal-Mart and Amazon about fighting crime in a recession?’’ *Police Chief*, [1] W. Sultani, C. Chen, and M. Shah, ‘‘Real-world anomaly detection in surveillance videos,’’ in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, Jun. 2018, pp. 6479–6488.
[10] K. J. Bowers and S. D. Johnson, ‘‘Who commits near repeats? A test of the boost explanation,’’ *Western Criminol. Rev.*, vol. 5, no. 3, pp. 12–24, 2004.
[11] Seattle Police Department, ‘‘SPD 2021 year-end crime report,’’ Seattle, WA, USA, 2021.[Online].Available:https://www.seattle.gov/documents/Departments/Police/Reports/2021_SPD_CRIME_REPORT_FINAL.pdf
[12] (2019). *FBI*. [Online]. Available: https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/topic-pages/robbery
[13] B. Fawei, J. Z. Pan, M. Kollingbaum, and A. Z.Wyner, ‘‘A semi-automated On tology construction for legal question answering,’’ *New Gener. Comput.*,vol. 37, no. 4, pp. 453–478, Dec. 2019.
[14] R. Thompson, ‘‘Understanding theft from the person and robbery of personal property victimisation trends in England and Wales,’’ Nottingham Trent Univ., Nottingham, U.K., Tech. Rep. 2010/11, 2014.
[15] P. J. Cook, ‘‘Robbery violence,’’ *J. Criminal Law Criminol.*, vol. 78, no. 2, pp. 357–376, 1987.
[16] J. D. McCluskey, ‘‘A comparison of Robbers’ use of physical coercion in commercial and street robberies,’’ *Crime Delinquency*, vol. 59, no. 3, pp. 419–442, Apr. 2013.
[17] D. F. Luckenbill, ‘‘Patterns of force in robbery,’’ *Deviant Behav.*, vol.1, nos. 3–4, pp. 361–378, Apr. 1980.
[18] T. Ishikawa and T. T. Zin, ‘‘A study on detection of suspicious persons for intelligent monitoring system,’’ in *Proc. Int. Conf. Big Data Anal. Deep Learn. Appl.* Singapore: Springer, 2018, pp. 292–301.
[19] J. R. Medel and A. Savakis, ‘‘Anomaly detection in video using predictive convolutional long short-term memory networks,’’ 2016, *arXiv:1612.00390*.
[20] M. Shah, O. Javed, and K. Shafique, ‘‘Automated visual surveillance in realistic scenarios,’’ *IEEE Multimedia Mag.*, vol. 14, no. 1, pp. 30–39, Jan. 2007.
[21] A. Biswas, S. C. Ria, Z. Ferdous, and S. N. Chowdhury, ‘‘Suspicious human-movement detection,’’ Ph.D. dissertation, Dept. Comput. Sci. Eng., BRAC Univ., Dhaka, Bangladesh, 2017.
[22] R. Arroyo, J. J. Yebes, L. M. Bergasa, I. G. Daza, and J. Almazán, ‘‘Expert video-surveillance system for real-time detection of suspicious behaviors in shopping malls,’’ *Expert Syst. Appl.*, vol. 42, no. 21, pp. 7991–8005, Nov. 2015.

[23] R. Nawaratne, D. Alahakoon, D. De Silva, and X. Yu, ‘‘Spatiotemporal anomaly detection using deep learning for real-time video surveillance,’’ *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 393–402, Jan. 2020.

[24] F. Wu, G. Jin, M. Gao, Z. HE, and Y. Yang, ‘‘Helmet detection based on improved YOLO V3 deep model,’’ in *Proc. IEEE 16th Int. Conf. Netw.,Sens. Control (ICNSC)*, May 2019, pp. 363–368.

[25] Y. Liu, X.-K. Wang, W.-H. Hou, H. Liu, and J.-Q. Wang, ‘‘A novel hybrid model combining a fuzzy inference system and a deep learning method for short-term traffic flow prediction,’’ *Knowl.-Based Syst.*, vol. 255, Nov. 2022, Art. no. 109760.vol. 76, no. 11, p. 18, 2009.