IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp697-706

PREDICTING ROBBERY BEFORE IT HAPPENS: AN AI-DRIVEN APPROACH FOR INDOOR SURVEILLANCE

[1]K.Hemalatha, MCA Student, Department of MCA
[2] Dr. Dhanaraj Cheelu, Ph.D, Professor, Department of MCA
[12]Dr KV Subba Reddy Institute of Technology, Dupadu, Kurnool

ABSTRACT

For video surveillance systems to avoid incidents and safeguard assets, crime prediction is necessary. In this regard, our paper suggests the first artificial intelligence method for predicting and detecting Robbery Behaviour Potential (RBP) in an interior camera. Three detection modules—head cover, crowd, and loitering detection modules—are the foundation of our approach, which enables prompt response and deters robberies. The YOLOV5 model is retrained using the manually annotated dataset we collected to create the first two modules. Furthermore, we provide a new definition for the DeepSORT algorithm-based loitering detection module. After converting expert information into rules, a fuzzy inference system makes a final determination about the likelihood of robbery. The robber's various style, the security camera's variable viewpoint, and the poor quality of the video photos make this tedious. We successfully completed our experiment using actual video surveillance footage, achieving an F1-score of 0.537. Therefore, we design a threshold value for RBP to assess video pictures as a robbery detection issue in order to do an experimental comparison with the other relevant research. Assuming this, the experimental findings clearly reflect an F1-score of 0.607, indicating that the suggested approach performs much better in identifying the heist than the robbery detection methods. We firmly think that by anticipating and averting robbery incidents, the implementation of the suggested strategy might reduce the harm caused by robberies in a security camera control centre. However, the human operator's situational awareness improves, and additional cameras may be controlled.

I. INTRODUCTION

In order to improve public safety and deter crime, surveillance cameras are now routinely deployed in a variety of locations, including residences, banks, businesses, and airports. Alternatively, by examining these films and trying to identify the offender, it is possible to determine the time and location of the incident and, more precisely, the perpetrator. In the meanwhile, someone is required to monitor the cameras from behind the scenes and identify any unusual activity. However, since anomalies are so uncommon, they cause fatigue, and when they do occur, they might often be unaware of it. That is, he no longer has the oddity [1]. Additionally, the anomaly-detection procedure is founded on human intuition, which is acquired over time. However, further issues with non-automated crime prediction and detection systems that rely on monitoring surveillance recordings include the skill level of the individual for recognising signals of crime happening and the expense of hiring him.

Machine learning and deep learning methods must be used to extract certain visual cues in order to automate anomaly detection [2], [3]. Specific characteristics for various anomaly classes [4], such as vandalism [5], violence detection [6], and robbery [7], might be helpful for improving the performance of these algorithms. Reducing the damage by anticipating the crime's scene and timing. However, security personnel are also on time. For example, in an experiment produced in Santa Cruz, California, cops get daily crime estimates every morning. They are guided to patrol certain areas by this predicting. According to a Santa Cruz

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp697-706

spokeswoman, during the first six months of the program, thirteen wrongdoers were stopped in the designated regions [8]. Predictive policing is important for federal funding and security systems since it reduces crime and costs money, according to papers [8], [9], and [10]. According to a 2021 Seattle Police Department (SPD) study in Washington, USA, violent crimes have grown by 20%, making them more hazardous owing to the likelihood of victimisation [11]. Robbery is among the top five crimes in the US, according to statistics gathered by the Federal Bureau of Investigations' Uniform Crime Reporting System (FBI-UCR) [12]. One of the reasons security cameras are installed in numerous locations is to detect robberies. Robbery is defined by the Oxford Dictionary as the crime of stealing or trying to take any property by force, threat, or weapon [13]. It is distinguished from other types of theft, such as shoplifting, pickpocketing, or burglary, by its inherently violent nature [14], [15]. Robbery is usually a crime in places where several other forms of theft are treated as misdemeanours. Criminologists categorise robberies according to their time and location, whether they are armed or unarmed, the kind of weapon used, and the level of force used. Thus, street and commercial robbery are two common examples [16]. The majority of street robberies occur in impoverished, congested areas without closed-circuit televisions (CCTV). There are two ways that commercial robberies happen: either the criminal approaches the scene disguised as a client or hides his face with a mask or helmet, then unexpectedly draws a weapon and frightens the staff. The other is where criminals forcefully enter, usually in groups, and most often hide their heads or faces [17]. Both kinds of commercial robberies took place in indoor locations that often have CCTVs installed in order to identify criminals or perhaps forecast future commercial robberies. Furthermore, criminals who are equipped with a knife or other weapon often use force to intimidate others. However, it is more likely that a large force will be used if the criminals are unarmed or carrying a stick [16], [17]. Commercial robberies, whether armed or unarmed, may result in harm, suffering, and even death.

Therefore, anticipating the behaviour of commercial robberies, whether by a human, a computer, or a mix of these, is crucial to averting their occurrence and the associated risks [18].

Generally speaking, certain techniques for automating crime detection or prediction rely on extracting various criminal situations and applying them in various domains. However, none of these techniques have been able to foresee the likelihood of robbery. Consequently, an algorithm for RBP prediction in video pictures has to be developed. It is easy to see that in order to make predictions, characteristics and evidence from surveillance footage must be extracted. Investigating the possibility of robbery behaviour in video pictures is one way to do this. Because every location chosen for a heist has varied variables and cultural norms, robbery scenarios change from one setting to another [19]. Consequently, there is no assurance associated with strong feature extraction.

A typical scenario with key aspects may be taken into consideration for commercial robbery movies, even if there are many different robbery occurrence situations and because of scenario-based techniques [20], [21]. In particular, someone picking a sparsely populated area, frequently hiding their face or head with a helmet, mask, glasses, or any other clothing to avoid detection, and then waiting for a chance to display their force, threat, or weapon. This situation perfectly aligns with the concept of the first kind of commercial robbery behaviour and the expertise of an expert [17], [22]. We take into consideration similar traits seen in the majority of robbery instances under three modules, including head cover, crowd, and loitering detection, in order to construct a system based on this common scenario abstracted from other situations inferred

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp697-706

from robbery footage. Following the extraction of these characteristics, an inference machine is required to complete the RBP for module implementation. For possible derivation, the conclusion procedure has to be as competent as human decision-making. The capacity of fuzzy set theory to simulate human inference [23] allows experience to be translated into fuzzy rules, and fuzzy measurement suggests that it makes diagnosing and reasoning through complicated decisions easier [24], [25]. Conversely, deep learning techniques lack this flexibility and may not be able to effectively handle the subtleties and variances of unknown data [25]. For these reasons, this study proposes a fuzzy inference engine.

In summary, our paper's primary contributions are as follows:

1. The suggested algorithm is predicated on a new technique that can forecast RBP and stop the harm that comes from its presence inside. To the best of our knowledge, this is the first study to concentrate on predicting robbery behaviour. It is based on three primary modules: loitering detection, crowd detection, and head cover.
2. A manually annotated dataset with and without a head cover has been produced for our system. We add the outcomes of the two states that the head cover detection module reported in order to count the number of people. The technique outperforms security video limitations including poor quality and single camera footage.
3. Our notion of the loitering point provides a new way to calculate loitering. Regarding the tracking techniques, the Deep Simple Online Real-time Tracking (Deep SORT) algorithm has been used to determine the quantity of loitering for every individual. Each one has been given a point after the quantity of loitering was analysed using the Euclidean distance computation.
4. Using a fuzzy inference engine with optimised rules, fuzzification, and defuzzification processes is our algorithm's main contribution. The outcomes of these three modules were examined using an inference machine and an expert's understanding of robbery behaviour.

The remainder of the document is organised as follows: Section II examines some of the literature that is relevant to our work, such as studies about our modules and predictions or detections of suspicious behaviour. In Section III, the suggested method is explained, along with the ideas of RBP prediction, the suggested modules, and the results for low-resolution video pictures via YOLOV5 improvement. Section IV presents and discusses the experimental outcomes. The last portion wraps up the study and outlines next projects.

II. LITERATURE SURVEY

"Detection of anomalies in real-world surveillance footage,"

M. Shah, C. Chen, and W. Sultani,

A wide range of realistic abnormalities may be captured in surveillance footage. In this work, we suggest using both normal and anomalous films to learn abnormalities. We suggest using weakly labelled training videos—that is, training labels (normal or anomalous) are at the video-level rather than the clip-level—to learn anomaly through the deep multiple instance ranking framework in order to avoid annotating the anomalous segments or clips in training videos, which takes a lot of time. Our method automatically learns a deep anomaly ranking model that predicts high anomaly scores for anomalous video segments by treating normal and anomalous films as bags and video segments as instances in multiple instance learning (MIL). In order to properly localise anomaly during training, we also add temporal smoothness and sparsity restrictions to the ranking loss function. We also provide a brand-new, extensive dataset with 128 hours of films. It is made up of 1900 uncut real-world surveillance movies that include 13 actual anomalies, including robberies, fights, car crashes, and burglaries, in addition to everyday activity. There are two uses for this dataset. The first step is general anomaly identification, which takes into account all regular

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp697-706

activity in one group and all abnormalities in another. Second, for identifying each of the thirteen unusual acts. Our experimental findings demonstrate that, in comparison to state-of-the-art techniques, our MIL method for anomaly identification significantly improves anomaly detection performance. We provide the findings from a number of recent deep learning baselines on the identification of aberrant behaviour. These baselines' poor recognition performance indicates how difficult our dataset is and provide more room for further research. At http://crcv.ucf.edu/projects/real-world, you may access the dataset.

"A survey on deep learning methods for detecting anomalies in videos,"

P. C. Naval Jr. and J. James P. Suarez,

The issue of video anomaly detection has been researched for over ten years. Researchers' attention has been drawn to this field because of its broad application. Because of this, a variety of methods have been put out over the years, ranging from machine learning-based methods to statistical-based methods. Although a lot of surveys have previously been done in this topic, the main goal of this study is to provide a summary of the most current developments in anomaly detection using deep learning. Numerous artificial intelligence domains, including computer vision and natural language processing, have effectively used deep learning. However, the main emphasis of this study is on how Deep Learning has advanced and added new information to the field of video anomaly detection. The various Deep Learning methodologies are categorised in this study according to their goals. Additionally, it talks about the often used datasets and assessment criteria. A summary of all the current methods is then discussed in order to provide guidance and potential directions for further study.

"Using deep learning to analyse videos intelligently,"

C. Zhang and T. Mei,

For many years, one of the core issues in computer vision and multimedia content analysis has been video analysis. Since video is an information-intensive medium with many variants and complexity, the work is very difficult. Researchers in the computer vision and multimedia fields may now greatly improve video analysis performance and start new research avenues for video content analysis because of the recent advancements in deep learning methods. Beginning with a unified deep learning toolkit—the Microsoft Cognitive Toolkit (CNTK)—that supports common model types like convolutional nets and recurrent networks, this tutorial will cover recent developments in the field of video understanding. From there, it will cover the fundamental problems of learning video representations and classifying and recognising videos, as well as a developing field of video and language.

"Classifying images by combining the latent deep CNN feature,"

X. Liu, R. Hong, and H. Yan

Convolutional neural networks (CNNs) have advanced significantly in image categorisation in recent years. It is capable of automatically extracting and classifying characteristics from a vast amount of visual data. The convolutional neural network may perform better and does not need manually created picture features when compared to these conventional feature extraction approaches (such as SIFT, HOG, and GIST). However, academic research is still focused on how to improve the algorithm's performance even further. In order to train a more reliable classifier, we thus provide in this study a technique for fusing the latent features that are taken from the CNN's intermediate layers. Initially, we extract visual characteristics of the 3-layer CNN models using the pretrained CNN models via caffe. After that, we get their trained classifier by applying the SVM classifier to the 3-layer features, accordingly. Lastly, a classifier that is comparable to a 3-layer SVM classifier is created by combining three pretrained classifiers.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp697-706

Caltech-256 datasets are used in the experiment. The experimental outcome demonstrates that, in comparison to the traditional CNN, the combined classifier achieves excellent performance.

"Automated real-time identification of vandalism in video clips,"

A. Amer, M. Ghazal, and C. Vazquez,

A technique for the real-time identification of vandalism in video sequences is presented in this research. The suggested approach uses a single camera and robustly extracts a series of high-level events that precede vandalism in order to identify it without the need for object identification. When an item, such a pay phone or a sign, enters the scene and makes an unauthorised alteration within a designated vandalisable area, it is considered vandalism. Both offline and online testing of the suggested approach revealed that it is reliable in identifying graffiti or vandalism in security footage.

III. SYSTEM ANALYSIS & DESIGN

EXISTING SYSTEM

Anomalies are sporadic observations, occurrences, or actions that raise suspicions because they deviate greatly from typical patterns. Any behaviour that deviates from a typical activity is considered an anomaly, and crime is one kind of abnormality [2]. One may argue that the rise in crimes in public areas is the reason for the widespread use of CCTV. Suspicious behaviour detection may be used to anticipate crime. Inaccurate, ambiguous, and uncertain information is necessary for prediction [26]. The focus of our suggested method is indoor RBP prediction. Robbery is a kind of crime, and the suggested algorithm requires the identification of head covers, crowds, and loitering. Providing a general RBP prediction framework, which is not covered in any other research, is a key idea of our approach. This section will cover a few related works that are pertinent to the detection or prediction of suspicious behaviour, crime detection or prediction, including articles regarding loitering or head cover detection.

In order to update the objects meant in each frame, Elhamod and Levine [27] suggested a semantics-based suspicious behaviour identification system based on object tracking by blob matching with colour histograms and geographical information. The intersection of the histogram's values is computed and compared with the specified threshold for the blob and object similarity specification. It then allocates the proper classes, which include objects for lifeless items and humans for living ones. Behaviours are semantically defined by computing their 3D motion attributes and storing them as historical records. The following suspicious behaviours have been identified: fighting by computing merge, split, and simultaneous movement of the blob's centroid; fainting by comparing the assumed 2D and actual 3D location of a person's feet and also head coordinates; abandoned luggage by background subtraction methods; and finally loitering by aggregating presence time of a person in an area.

An automatic normal method for detecting suspicious pedestrians by lingering detection was presented by Ishikawa and Zin [18]. [18] claims that a suspicious individual walks, pauses, and circles the area many times over an extended period of time with an increase in the frequency of direction changes. He has a higher distance value than the average individual, and his acceleration changes significantly. [18] splits the video frames into 25 blocks in order to apply these characteristics, then counts the frequency of block numbers that correspond to the feet of people in each block. If the frequency exceeded the threshold, the individual would be regarded as a suspicious pedestrian. It computes the angles of movement direction in order to determine shifting of direction. All necessary characteristics are extracted via the computation of distance and acceleration changes. Lastly, a decision fusion procedure aggregates the scores of every stage to identify suspicious pedestrians.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp697-706

Two components make up the E-police system that Rajapakshe et al. [28] presented: a crime prediction system and a video surveillance monitoring system. [28] use human activity recognition techniques to identify suspicious behaviours, including violence and vandalism, and divides them into normal and abnormal groups. They identify suspicious people who hide their faces by using Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) for feature extraction. In order to anticipate the location and timing of a crime, [28] uses public information resources in conjunction with classification techniques like SVM and decision trees.

An expert real-time system for detecting suspicious behaviours in shopping malls was suggested by Arroyo et al. [22]. They use an algorithm for background removal and picture segmentation to find foreground items. The blobs of each subdivided section are then collected using a blob fusion technique in order to identify humans. With the aid of a novel two-step technique, a tracking algorithm is employed: a) a Kalman filter is utilised for human identification and tracking, b) SVM kernels are used for occlusion management. Human behaviours are then examined using the trajectories of individuals that were acquired. Trajectory analysis is used to identify the entry or existence alarm, which is triggered when too many individuals enter or when someone flees. Additionally, some danger locations are interior spaces that include more costly items and are selected by human security agents. Individuals' loitering is assessed based on their paths and the amount of time they spend in certain areas. Their technology sounds an alert if the time exceeds the 30-second limit set by security professionals. To keep the cash counter safe, they installed a camera on it. An alarm goes off if someone is hanging around it and no store employees are in the area around the cash desk. Additionally, a naturalistic dataset given by many cameras placed at a store's entrance, interior, and pay desk is used for the assessment process.

Disadvantages

• Data complexity: To identify Robbery Behaviour, the majority of machine learning models now in use need to be able to correctly analyse large and intricate datasets.

• Data availability: In order to provide precise predictions, the majority of machine learning models need a lot of data. The accuracy of the model may degrade if data is not accessible in large enough amounts.

• Inaccurate labelling: The accuracy of the machine learning models that are now in use depends on how well the input dataset was used for training. Inaccurate labelling of the data prevents the model from producing reliable predictions.

PROPOSED SYSTEM

1. The suggested algorithm is based on a new technique that can forecast RBP and stop the harm that comes from its presence inside.As far as we are aware, this is the first study to concentrate on predicting robbery behaviour and is based on three primary modules: loitering detection, crowd, and head cover.
2. A manually annotated dataset with and without a head cover has been produced for our system. We add the outcomes of the two states that the head cover detection module reported in order to count the number of people. The technique is prevalent in surveillance video formats, including single-camera and low-resolution recordings.
3. Our notion of the loitering point provides a new way to calculate loitering. Regarding the tracking techniques, the Deep Simple Online Real-time Tracking (DeepSORT) algorithm has been used to determine the quantity of loitering for every individual. Each one has been given a point after the quantity of loitering was analysed using the Euclidean distance computation.
4. Using a fuzzy inference engine with optimised rules, fuzzification, and defuzzification processes

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp697-706

is our algorithm's main contribution. The outcomes of these three modules were examined using an inference machine and an expert's understanding of robbery behaviour.

Advantages

• A module for detecting head covers.

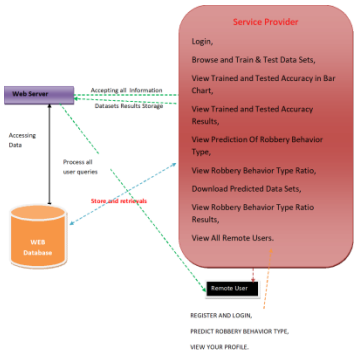
• A crowd detection module to determine how many people are present in an area.

• A module to identify loitering.

Our team collected the dataset in order to construct head and crowd detection modules for the suggested robbery scenario. After that, the data was manually annotated and convolved to reduce its resolution. To fully customise it, two first modules are supplied by retraining YOLOV5s. The DeepSORT algorithm is used to track the person and the Euclidean technique is utilised to compute the distance he has travelled. Our specific loitering detection module is introduced based on the innovative formulation of our unique thresholds, which determine the label of loitering assigned to each individual. Lastly, the possible prediction of robbery behaviour is done using a fuzzy inference engine. The three primary components of RBP prediction are feature extraction, feature analysis, and RBP prediction.

SYSTEM DESIGN

SYSTEM ARCHITECTURE



IV. IMPLEMENTATIONS

Modules

Service Provider

The Service Provider must use a working user name and password to log in to this module. He can do a number of tasks after successfully logging in, including browsing and training and testing data sets. See the Bar Chart for Trained and Tested Accuracy. View Accuracy Tested and Trained Results, See Robbery Behaviour Type Prediction, Robbery Behaviour Type Ratio, Get Predicted Data Sets here. View All Remote Users and Robbery Behaviour Type Ratio Results.

View and Authorize Users

The administrator may see a list of all registered users in this module. Here, the administrator may see the user's information, like name, email, and address, and they can also grant the user permissions.

Remote User

A total of n users are present in this module. Before beginning any actions, the user needs register. Following registration, the user's information will be entered into the database. Following a successful registration, he must use his password and authorised user name to log in. The user will do many tasks after successfully logging in, including registering and logging in, predicting the kind of robbery behaviour, and seeing their profile.

ALGORITHMS

Logistic regression Classifiers

The relationship between a collection of independent (explanatory) factors and a categorical dependent variable is examined using logistic regression analysis. When the dependent variable simply has two values, like 0 and 1 or Yes and No, the term logistic regression is used. When the dependent variable contains three or more distinct values, such as married, single, divorced, or widowed, the technique is sometimes referred to as multinomial logistic regression.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp697-706

While the dependent variable's data type differs from multiple regression's, the procedure's practical application is comparable.

When it comes to categorical-response variable analysis, logistic regression and discriminant analysis are competitors. Compared to discriminant analysis, many statisticians believe that logistic regression is more flexible and appropriate for modelling the majority of scenarios. This is due to the fact that, unlike discriminant analysis, logistic regression does not presume that the independent variables are regularly distributed.

Both binary and multinomial logistic regression are calculated by this software for both category and numerical independent variables. Along with the regression equation, it provides information on likelihood, deviance, odds ratios, confidence limits, and quality of fit. It does a thorough residual analysis that includes diagnostic residual plots and reports. In order to find the optimal regression model with the fewest independent variables, it might conduct an independent variable subset selection search. It offers ROC curves and confidence intervals on expected values to assist in identifying the optimal classification cutoff point. By automatically identifying rows that are not utilised throughout the study, it enables you to confirm your findings.

Naïve Bayes

The supervised learning technique known as the "naive bayes approach" is predicated on the straightforward premise that the existence or lack of a certain class characteristic has no bearing on the existence or nonexistence of any other feature. However, it seems sturdy and effective in spite of this. It performs similarly to other methods of guided learning. Numerous explanations have been put forward in the literature. We emphasise a representation bias-based explanation in this lesson. Along with logistic regression, linear discriminant analysis, and linear SVM (support vector machine), the naive bayes classifier is a linear classifier. The technique used to estimate the classifier's parameters (the learning bias) makes a difference.

Although the Naive Bayes classifier is commonly used in research, practitioners who want to get findings that are useful do not utilise it as often. On the one hand, the researchers discovered that it is very simple to build and apply, that estimating its parameters is simple, that learning occurs quickly even on extremely big datasets, and that, when compared to other methods, its accuracy is rather excellent. The end users, however, do not comprehend the value of such a strategy and do not get a model that is simple to read and implement.

As a consequence, we display the learning process's outcomes in a fresh way. Both the deployment and comprehension of the classifier are simplified. We discuss several theoretical facets of the naive bayes classifier in the first section of this lesson. Next, we use Tanagra to apply the method on a dataset. We contrast the outcomes (the model's parameters) with those from other linear techniques including logistic regression, linear discriminant analysis, and linear support vector machines. We see that the outcomes are quite reliable. This helps to explain why the strategy performs well when compared to others. We employ a variety of tools (Weka 3.6.0, R 2.9.2, Knime 2.1.1, Orange 2.0b, and RapidMiner 4.6.0) on the same dataset in the second section. Above all, we make an effort to comprehend the outcomes.

Random Forest

Random forests, also known as random decision forests, are ensemble learning techniques that build a large number of decision trees during training for tasks like regression and classification. The class chosen by the majority of

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp697-706

trees is the random forest's output for classification problems. The mean or average forecast of each individual tree is given back for regression tasks. The tendency of decision trees to overfit to their training set is compensated for by random decision forests. Although random forests are less accurate than gradient enhanced trees, they often perform better than choice trees. However, their performance may be impacted by data peculiarities.

Tin Kam Ho[1] developed the first algorithm for random decision forests in 1995 by using the random subspace technique, which in Ho's definition is a means of putting Eugene Kleinberg's "stochastic discrimination" approach to classification into practice.

Leo Breiman and Adele Cutler created an algorithm extension and filed for a trademark in 2006 for "Random Forests" (owned by Minitab, Inc. as of 2019).The extension builds a set of decision trees with controlled variance by combining Breiman's "bagging" concept with random feature selection, which was initially proposed by Ho[1] and then separately by Amit and Geman[13].

Businesses often employ random forests as "blackbox" models since they need minimal setup and provide accurate forecasts across a variety of inputs.

V. CONCLUSION

An technique for RBP prediction in video surveillance pictures is presented in this research study. There are a number of issues with CCTV footage, such as the varied methods that robberies may occur, the different camera angles that can be installed in different locations, and the poor quality of the pictures that CCTVs capture. By addressing these barriers, prompt action is taken and robberies that are partly or completely visible on security footage are avoided. This study is being done because, according to our thorough literature analysis, no RBP prediction has ever been made previously, despite the importance of avoiding robberies. By studying several robbery footage from CCTVs and consulting with an expert, we are able to extract some typical situations of robbery occurrences. We look at these situations in order to identify additional similarities between them and put a workable strategy for RBP prediction into practice. Our work suggests a deep learning-based method for estimating the likelihood of robbery with the use of a fuzzy inference machine. By collecting appropriate datasets of people with and without head coverings, this method yields a retrained YOLOV5 algorithm. The head cover and crowd detection modules are implemented effectively using this deep learning-based approach. Additionally, this study uses our established approach to perform the loitering module, which uses the Deep SORT technique to determine the Euclidean travelled distance of people. Based on the findings of three modules, a fuzzy inference machine is described to infer the theft potential of films for every ten frames and average them for each clip. The F1-score of the suggested approach is 0.537 when it is applied to the Robbery folder of the UCF-Crime dataset. This result demonstrates that over half of the films can be accurately predicted to have robbery potential using our suggested technique.

As a result, we switch the prediction problem to the robbery detection issue. Therefore, we can compare it to earlier research that focused on anomaly detection, particularly robbery detection, using the UCF-Crime dataset. The detection method's F1-score is 0.607, the highest of all the approaches. The outcome demonstrates that our suggested scenario-based method is very effective at both identifying and forecasting robbery behaviour. Any location with video cameras that want to deter robbery crimes may apply our suggested strategy. They don't need to hire someone to closely examine the live footage from these cameras and determine the likelihood of a heist. To avoid making a mistake, this individual should view the videos continuously. Furthermore, anybody may modify our methods in private by altering the threshold values because of cultural differences.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp697-706

By increasing the accuracy of loitering detection, we can raise the F1-score. In our next effort, we want to refine the Deep SORT approach in order to get a better tracking algorithm for low-resolution video pictures. It is unable to accurately recognise and track humans in low-resolution movies. This is due to the fact that the Deep SORT algorithm uses FRR CNN as its detector. As a result, we will modify the Deep SORT algorithm's detection architecture to retrain YOLOV5 using low-resolution human photos. There will only be one object class and poor quality photos in the planned YOLOV5.

REFERENCES

[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*,vol. 76, no. 11, p. 18, 2009.

[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 ontology 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.