IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

HOME SECURITY SYSTEM USING AI

Bhuvaneshwari m, Chaitra T R, Dhinakar s, Durgaprasad s l

Student, Student, Student, Student
Department of computer science Engineering
Sri Venkateshwara College of Engineering, Bangalore, India

Abstract: Introducing an innovative new security technology - our AI-based thief detection system is the fastest, most accurate and reliable machine for detecting & classifying theft incidents. Moreover, the system is designed to be capable of learning new skills from the data. This has further helped improve accuracy and reduce false alarms.

Our strategy consists of three types of detection modules: Roof head, crowd, loitering Detection module (divert behaviors and save Liberty from the robbery. OK, and it offers an original way to improve security with the help of artificial intelligence (AI) which will provide full guarantees that if a thief enters, we can find out its face by analyzing movement as well as behavior above all at more speed thanks to constant supervision. These types of theft easily pass through other traditional ways but would be greatly served by using advanced artificial intelligence AI technologies such as computer vision and machine learning for the field interposition both in terms of efficiency increase detection speed sharply.

The system is capable and learning new skills from the new data continuously thus expected to improve over time as reduce false alarms in a whole, our Ai thief detection System an advancements of existing security systems bring incomparable speed, accuracy & reliability alerting theft incidents permanently

I. INTRODUCTION

The best innovation for security has been AI in thief detection. In today's uncertain world, we need a creative and aggressive security method to defend assets when the threat of a crime is imminent at any time. Based on this AI system, which is diligently designed for thief detection, the research shows how to apply statistical modelling and machine learning techniques for designing and implementing an intelligent video surveillance system to detect the potential occurrence of theft in an environment.

To identify, capture and discourage a person (Thief) who is involved in theft or unauthorized access. For decades the identification of such unusual activities has been based on human interference supported by surveillance devices like CCTV.

When implemented with machine learning and computer vision systems, artificial intelligence (AI) completely changes the game's view on how security works. This artificial intelligence (AI) processes and analyzes data in real-time, uses predictive analytics, and is continually learning. We use artificial intelligence (AI) because it can process large amounts of data, recognize patterns, and provide projections through manually entered data as well as through historical and current data. Proposed

II. METHODOLOGY:

1: object detection

The primary task of thief detection is to detect and track the objects i.e., humans in a given environment. YOLO (You Only Look Once) version 4, whose detection speed is much faster and it have fast response time as compared to the version 5, and faster R-CNN are the most common object detection algorithms which are usually trained on large datasets that can differentiate between different objects including humans in real-time.

2. Behavioral Analysis

Recognizing that theft often involves nuanced behaviors, AI systems can be trained to perceive and analyze patterns of human actions and interactions. Through analyzing patterns of movement, gestures, or even micro-expressions on a person's face, an AI might be able to perceive signs that someone might be stealing. Behavioral analysis is also at the heart of proactive security – i.e., detecting early warning signs of a person who may go on to commit an act of violence or terrorism.

3. Continuous Learning

Unlike static rule-based systems, AI-driven thief detection is made for learning continuously. It injects new data to refine itself periodically in a process called adaptive learning, which makes it more accurate and enables it to evolve continually against new dangerous threats and evolving environments.

III. OBJECTIVES OR CONTRIBUTIONS

The main objectives of the AI based thief detection are as follows

1.Crowd Detection

Crowded areas offer an ideal opportunity for theft as the culprit can easily hide in the crowd. Here, the crowd detection module monitors the pattern of people in a crowded area. AI can learn behaviors of people and can sense anomaly in crowd gathering and thus identify any mis happenings occurred based on same.

2. Covered head detection

The toughest and at the same time challenging task is to recognize the people who are trying to hide their identity for some or the other reason, it can be by using hoodies, masks, or any kind of accessories this module will try to recognize such people if their level of trying to hide rises for the suspicion.

3. Loitering Detection

This module is used to detect people who stay or linger around certain areas for long time and may be a prelude of criminal activities. We use object detection, behavior analysis as well as predictive modeling to improve theft prevention capability by finding suspects' behavior pattern.

IV. LITERATURE SURVEY:

1: what they proposed

As of the last update in January 2022, there were various proposals and ongoing research in ai-based thief detection. These systems leverage computer vision, machine learning and other Ai techniques to identify suspicious behavior in a person and some general concepts which was used by the existing systems.

1) Object detection or cctv surveillance

The main job of thief detection is the ability to identify and track objects, particularly individuals, within the given environment. In this we are using YOLO (You Only Look Once) version 5 These algorithms often trained on large number of datasets can be distinguish between various objects including humans in real-time.

2) Behavior analysis:

Recognizing that theft often involves nuanced behaviors, AI systems can be trained to analyze human actions and interactions. By understanding patterns of movement, gestures, and facial expressions, the system can identify behaviors indicative of the theft. This behavioral analysis is a critical component of proactive security, allowing for the early identification of suspicious activities of a person.

3)facial recognition:

Implementing the facial recognition to identify the individuals and the objects, some AI systems integrate recognition with the existing databases to enhance the security for protection purpose

4)Anomaly detection:

Detect unknown people that will be lurking inside the house or in some establishment and also detect strange motion movement or behaviors that deviates the normal activities and also tracking of individual on area.

5) real-me alerts:

Alerting security and law enforcement immediately if we detect suspicious activity so they can be there right away.

What have they achieved?

As of the update in Jan 2022 the AI in fact has shown good results as it brought better security and less crime rates to an specific area. And they have made some possible gains and other benefits that come with the development, here are some gain Improved surveillance accuracy, reduction false alarms, real-time processing, cost efficiency, data analysis and insights

V. SCOPE FOR IMPROVEMENT:

Here are some improvements that can be done in this Ai based detection system

1)data quality and diversity

Training the dataset and representative of various actions and environments which have potential thief activities also continuously update and expand the dataset to evolving the patterns and behavior's

2)algorithm optimization

Use all the algorithms and model architectures and see which one works good for the user, also you can fine tune hyperparameters to get more accuracy and efficiency of your model.

3)Behavioral Analysis:

Implement the method of understanding and modeling human behavior more accurately and collaborate with behavioral analysts to better understand suspicious activities done by the person we need to train the model to detect.

4)Continuous Monitoring and Updates:

Regularly monitor the performance of the system and try to resolve if any issues have occurred in the system. Should know about new research, technologies used in AI and security.

5)Adaptability:

The system should be adaptable as threat changes and network environment dynamics are expected as the time evolves. A mechanism should be in place to update the knowledge and algorithm of the system periodically.

VI. PROPOSED METHODOLOGY:

Goal of the research:

Security improvement, real-time detection, behavior analysis, adaptability to environment, cost effectiveness are the main goals of this research and continuous improvement.

Explication

1)improved security:

By using AI based thief detection we can enhance the security of any specific place or an area. We can train an AI system to perceive and interpret human behavior. Based on the pattern of motion, facial expressions and gestures it can derive if that person is a thief or not.The analysis of behavior forms an important part in proactive security which helps to early detect whether a person is suspected or not.

2)real-time detection:

Providing real time alerts to security and law enforcement when suspicious activity is detected, also it takes a short time to give the response and detect the crime and other susception action done by the other people or by the certain someone.

3)Behavior analysis:
Use this technique to better understand and model human behavior. Work with behavioral analysts to enhance your comprehension of the person's questionable actions. To make the model identify patterns, it must be trained.

4)Environment adaptability:
A system needs to be able to change with the times and respond to shifting threat scenarios. putting in place procedures to routinely update the information and algorithms of the system.

5) Economy of scale and ongoing enhancement.
Systems that strike a compromise between cost and effectiveness, offering long-term benefits and possible savings on security monitoring, AI-driven thief detection systems are intended for continual learning, in contrast to static rule-based systems. By adding new data over time, the system improves its skills through a process called adaptive learning. The system's ability to adapt not only improves accuracy but also enables it to change in response to hazardous hazards and shifting surroundings.

6) Analysis of Motion and Expression
Our AI-powered thief detection system's method of examining motion and facial expressions is one of its features. by using deep learning models that are capable of deciphering facial expressions and motions made by people. These actions enable the AI to identify the thief and do precise analysis on the provided data, which is already incorporated into the AI tools.

VII. RESULTS AND DISCUSSION:

1 Data regarding the dataset
The dataset is completely necessary for AI-based thief detection because it includes a variety of information that can be used to recognize and categorize suspicious activity. Some examples of these datasets are the following ones.

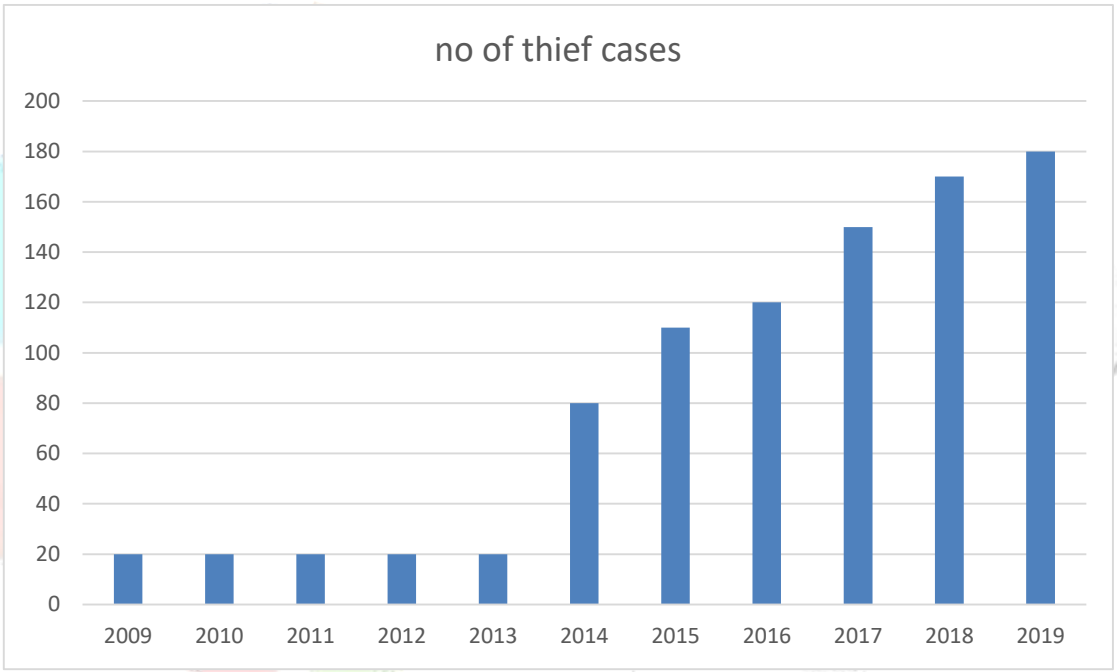
A) Image data:
The main source of information in the thief detection dataset is photos or video taken by the security camera. These images may include details about the environment, such as the illumination and the presence of people or objects.

B) Labels with annotations:
Every picture or video can have labels added to it that indicate whether it includes suspicious activity. These annotations are essential for teaching machine learning models to identify and categorize these kinds of occurrences.

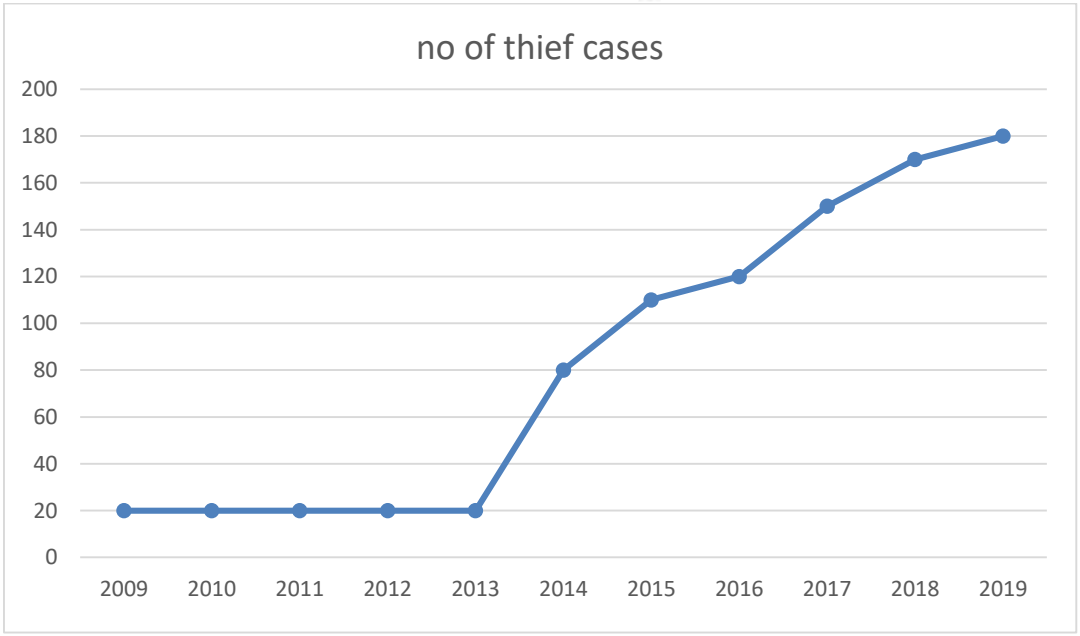
1. **Software's used in this model**
   1)OpenCV
   2)YOLO version 4
   3)Darknet
   4)Dlib
   5)Deep Stream SDK by Nvidia
   6)azure computer vision

2. Results:

Year	No of thief cases
2009	20
2010	20
2011	20
2012	20
2013	20
2014	80
2015	110
2016	120
2017	150
2018	170
2019	180

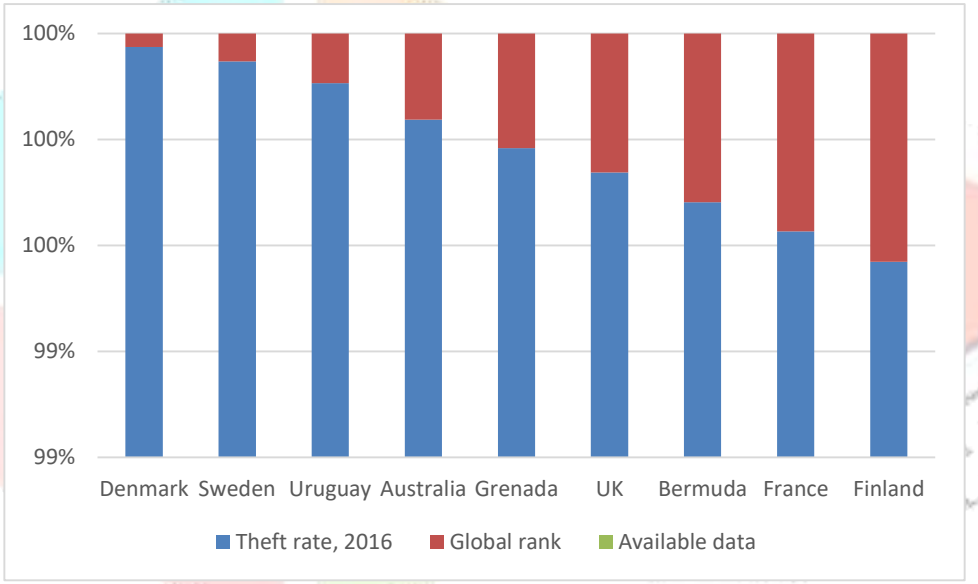


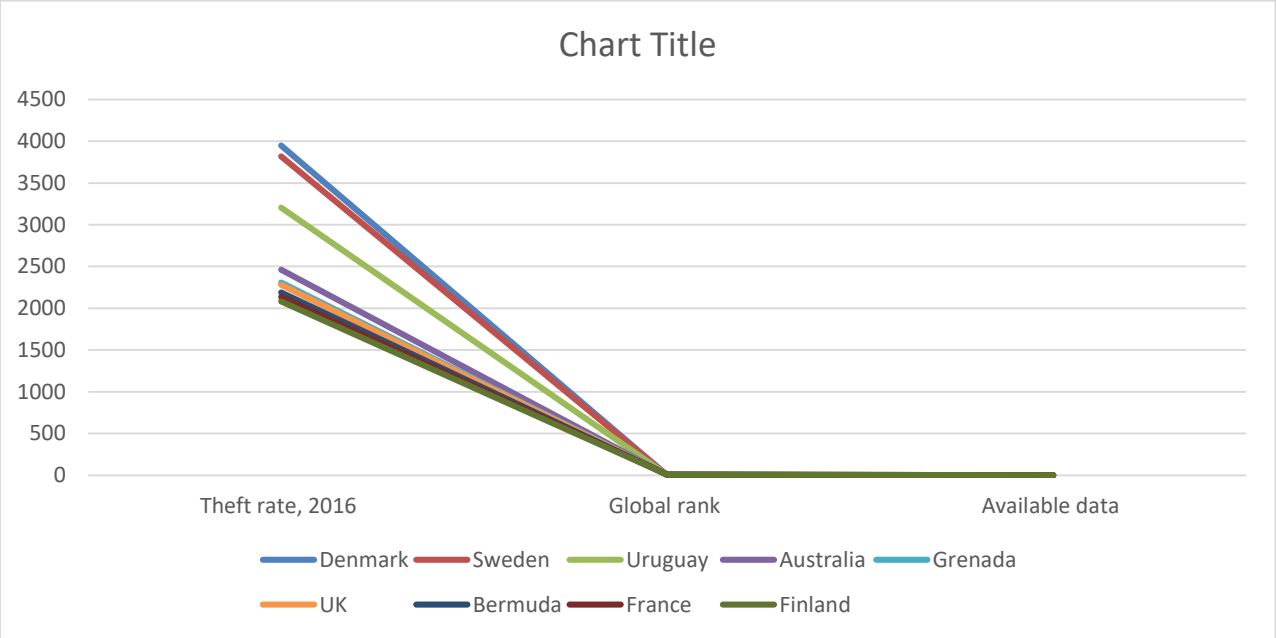
Contribution of thief in crime



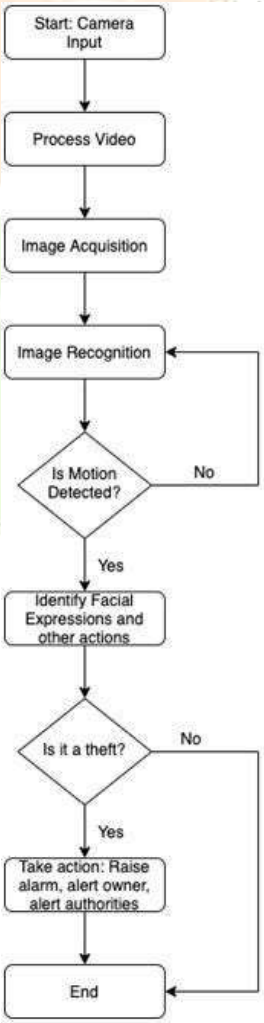
Thief rate ranking according to countries.

Countries	Theft rate, 2016	Global rank	Available data
Denmark	3949	1	2003 - 2016
Sweden	3817	2	2003 - 2016
Uruguay	3205	3	2003 - 2016
Australia	2460	4	2003 - 2016
Grenada	2307	5	2005 - 2016
UK	2283	6	2003 - 2016
Bermuda	2190	7	2003 - 2016
France	2135	8	2003 - 2016
Finland	2081	9	2003 - 2016





FLOW CHART HOW THE MODEL WORKS



VIII. CONCLUSION:

In conclusion, there will be crimes committed to safeguard our property and stop similar incidents. at this regard, our article—which uses artificial intelligence for thief detection—is proficient at anticipating and identifying thieve activity using CCTV. Our approach relies on three different types of detection modules: covered head, crowd, and loitering detection modules for alert behaviors and averting robberies. Additionally, it employs an inventive technique to enhance security by utilizing artificial intelligence (AI) to identify thieves based on their movements and facial expressions, while also implementing strong surveillance measures. While using AI techniques like computer vision and machine learning, our system is able to identify and prevent theft incidents more successfully than other traditional ways.

XI. REFERENCE:

1. Propounding First Artificial Intelligence Approach for Predicting Robbery Behavior Potential in an Indoor Security Camera SHIMA POUYAN, MOSTAFA CHARMI, ALI AZARPEYVAND AND HOSSEIN HASSANPOOR
2. D. G. Lowe, ‘‘Distinctive image features from scale-invariant key points,’ Int. J. Comput. Vis., vol. 60, no. 2, pp. 91–110, Nov. 2004.
3. Q. Xu, R. Lin, H. Yue, H. Huang, Y. Yang, and Z. Yao, ‘‘Research on small target detection in driving scenarios based on improved YOLO network,’’ IEEE Access, vol. 8, pp. 27574–27583, 2020.
4. Y. Chen, ‘‘Support vector machines and fuzzy systems,’ in Soft Computing for Knowledge Discovery and Data Mining. Boston, MA, USA: Springer, 2008, pp. 205–223
5. H. I. Öztürk, ‘‘Temporal anomaly localization,’’ M.S. thesis, Dept. Comput. Eng., Inst. Sci., Hacettepe Univ., Ankara, Turkey, 2021.