iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** XI **Month of publication:** November 2021

DOI: https://doi.org/10.22214/ijraset.2021.39187

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XI Nov 2021- Available at www.ijraset.com

Thief Detection with Deep Learning using Yolo Predictive Analysis

Pavithra.S[1], Dr. B. Muruganantham[2]
[1]Research Scholar, [2]Associate Professor, Department of Computing Technologies, SRMIST, Chennai, India

***Abstract:** This paper discusses thief detection, which is one of the important applications of suspicious human activity detections. Individual safety is a major concern in our busy scheduling life. The main reason for this concern is an ever-increasing number of activities that pose a threat. A simple closed-circuit television (CCTV) installation system is not sufficient enough because it usually requires a person to be alert and monitoring the cameras always is inefficient. The necessitates for the development of a fully automated security system detects anomalous activities in real-time, and provides instant assistance to the victim. As a consequence, we proposed a framework that examines and detects suspicious human activity from real-time Surveillance video using deep learning techniques and generates an alert if abnormal activity occurs. The method was tested on a dataset with both normal and abnormal activity and yielded better results.*
***Keywords:** Thief detection, deep-learning, surveillance video, predictive analysis, yolo.*

I. INTRODUCTION

Object detection is one of the new technologies which is related to image processing and deep learning, which deals with the detection of an object that belongs to the particular actions (such as persons, large areas, or buses) appearing in videos and images. Detection of faces and pedestrians is one of the well-studied areas of detecting the objects. It has lots of applications in deep learning including autonomous driving and video surveillance, as well as finding objects in images. The term "analysis of the scene" is usually used as a synonym for detection of each object in the scenes, classifies each of their labels, and determines their bounding boxes more conveniently. The process of detecting objects includes many approaches including fast R-CNNs, Retina-Nets, and Single-Shot Detectors (SSDs). It is under these approaches that data limitation and modeling challenges have been solved in the area of object detection. However, still they are not capable of detecting all objects in a given algorithm run. In recent years, the Yolo algorithm has gained a great deal of attention due to its superior performance when compared to other methods of object detection. So, we are interested in "You Only Look Once" (YOLO) is a kind of Convolutional neural network. When tested, it will give accurate results and satisfactory speed.

A. You only look once (Yolo)

It is an object detection model. Object detection entails determining the position of objects on the image as well as classifying those objects. The existing methods, such as the Fast-RCNN, Faster-RCNN, RCNN, and others, are robust, and the component that is trained separately is time-consuming and difficult to optimize. It is a real-time object detection convolutional neural network (CNN). This algorithm first uses a single neural network to process the whole image, and later divides it into regions to predict probabilities and bounding boxes. The prediction is used to weigh these bounding boxes.

B. Yolo Algorithm Importance

The yolo algorithm is significant for the following reasons:
Accuracy: Yolo model is a predictive analysis technique to produce an accurate result with minimum noise.
Learning Abilities: Yolo model first allows it to learn the object representation and then later applies it in object detection.
Speed: This algorithm increases the detection speed to predict objects in real-time.

C. Techniques of Yolo

There are three techniques that the yolo algorithm works for:
1) Intersection Over Union (IoU)
2) Residual Blocks
3) Bounding Box Regressions

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XI Nov 2021- Available at www.ijraset.com

D. Working of Yolo for Thief Detection

As part of Yolo, the idea of dividing images into grid cells are unique in YOLO by defining grids as **S x S.** If the center of the object is to which grid of cells, the cell grid will predict the object.

Each cell grid consists of:

$$y = \begin{bmatrix} pc \\ bx \\ by \\ bw \\ bh \\ c \end{bmatrix}$$

Outputs each grid cell

- ***pc* -** the probability of having an object in the grid cell. If there are no objects, then ignore them.
- ***bx, by* –** a center of the object found in the grid cell. Object's center does not fall within that grid cell, there is no need for calculation.
- ***bw, bh* -** height and width of the boxes.
- ***c* -** number of classes that will be calculated according to the specified class.

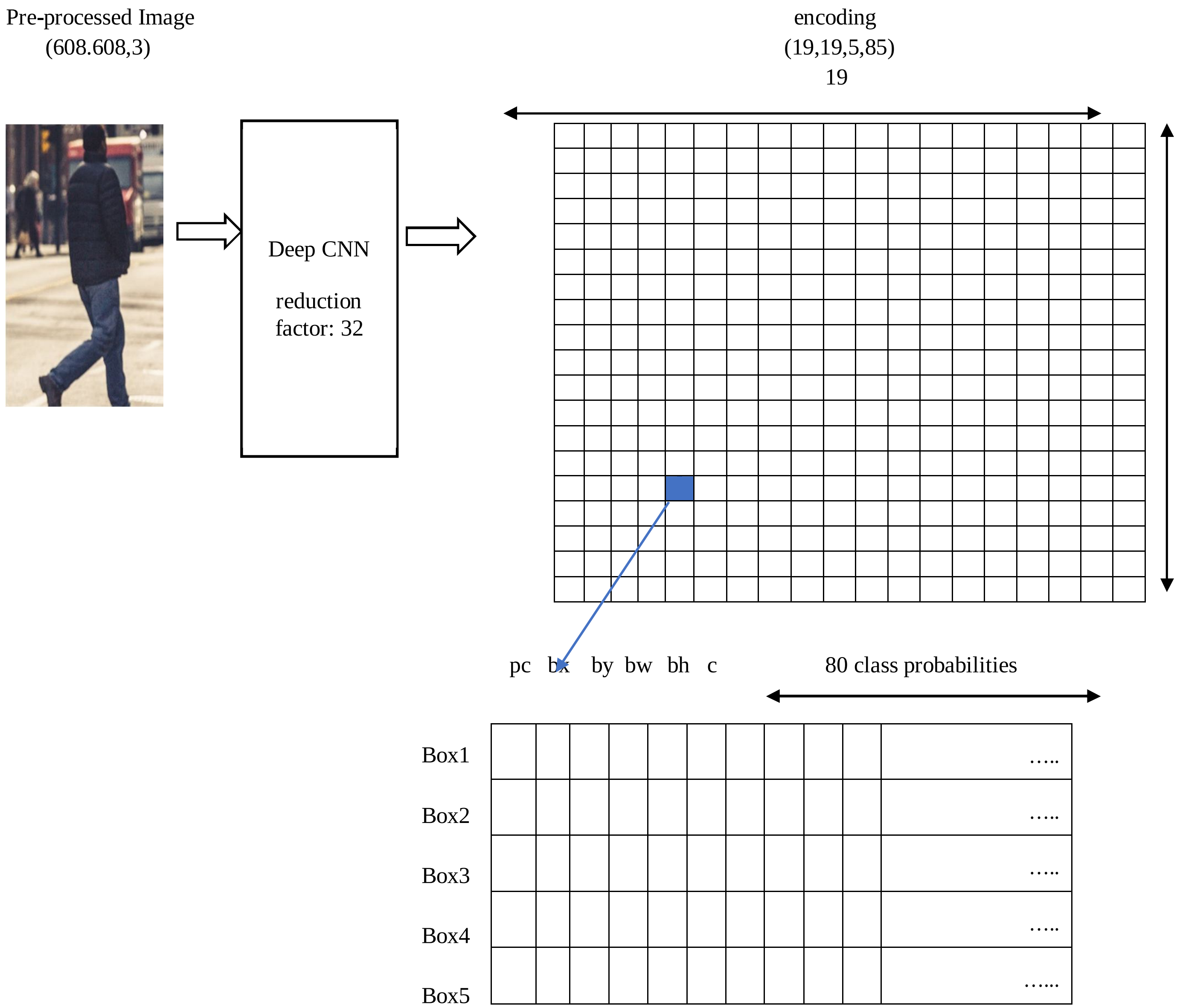


Figure 1. Encoding architecture for thief detection using yolo

II. HISTORY AND BACKGROUND

In this paper [1], the authors have proposed the technique of sparse coding that has built anomaly detection for better performance and it includes theories such as dictionary learning, feature learnings, and sparse representation. Therefore, in this proposed model single network is used for detecting the anomalies and which is also known as Anomaly Net. This system fully accomplishes the sparse representation, feature learnings, as well as dictionary learnings. To know about the features, they have created feature transfer blocks and motion fusion blocks to enjoy the benefits of removing motion capturing, improving data insufficiency and background noise. Paper [2], states that suspicious activity is a continuous observation of behavior, suggesting that the person is about to involve in a crime or going to commit a crime. The process of detecting suspicious activity is also known as anomaly detection. The surveillance camera is one of the most effective solutions to the problem of security in various places. Because identifying a crime or detecting a crime is difficult in daily life it requires manpower to monitor it. As a result, this paper looks closely at video surveillance of anomaly detection in deep learnings such as CNN. The authors of the paper [3], we're impressed with the functions of suspicious activities and proposed the sparse coding where the frames are mysterious with the reconstruction of the coefficient. The TSC was then mapped using a specific type of sRNN. The author's contributions are as follows: i) Creating datasets larger than the already existing dataset for detecting the anomaly. ii) It uses a TSC for recording the sRNN to examine the speed and parameter optimization. In this system [4], the authors have presented an effective technique for detecting anomalies in the video footage. CNN applications have recently demonstrated the capability of object recognition, object detections, in the videos. CNN on the other hand is supervised and requires labeled as research. This system uses Spatio-temporal architecture for detecting suspicious activity in the crowded areas from the videos. The authors of the paper [5], proposed the technique for detecting and localizing actual time anomalies in the crowd places. The videos can be described as a collection of global and local descriptors with cubic spots. Therefore, the descriptions used here is to capture the video footage according to various stages.

A. Research Gap

1) Different detection techniques are implemented to find suspicious activity.
2) Some researches are carried out from scratch without considering the features of the pre-trained model.
3) There is a large number of computations that result in high computation costs.
4) Classification accuracy is low.

III.METHODOLOGY

In this paper, we propose to use the yolo model to detect suspicious theft activities and identify the thefts happening in residential areas.

The architecture diagram of yolo can be represented with the following figure:

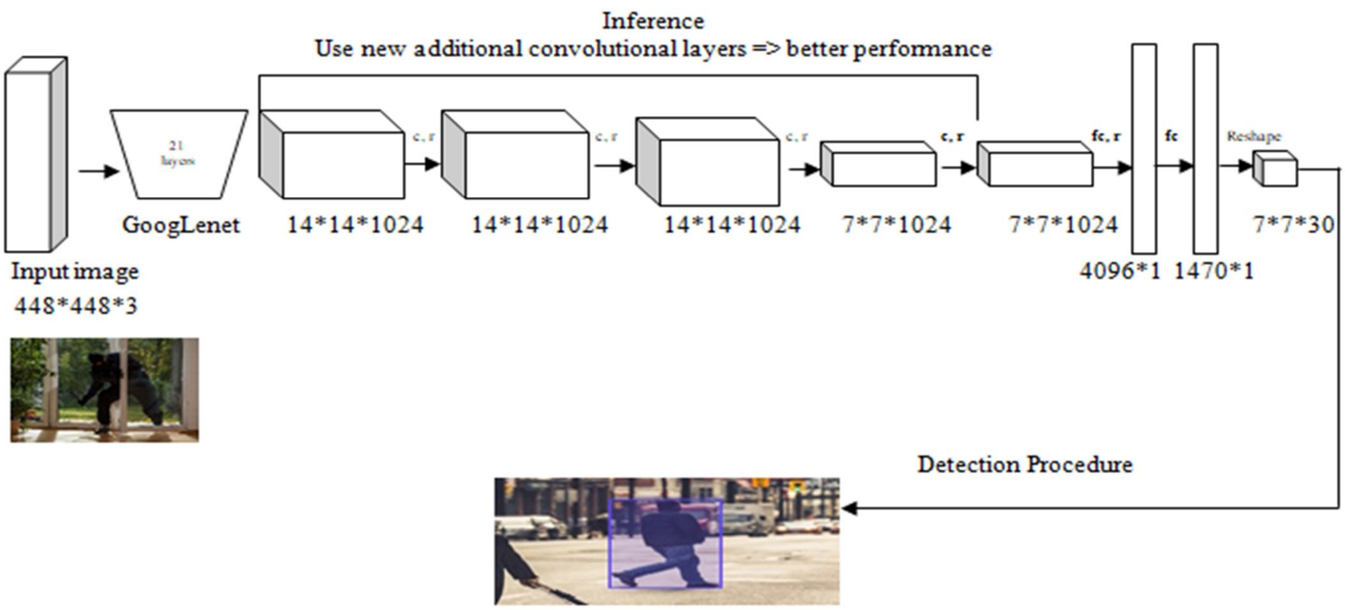


Figure 2. Yolo architecture for thief detection

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XI Nov 2021- Available at www.ijraset.com

The description of figure 2 above diagram explanation describes that the yolo model accepts an input image with a fixed dimension. In theory, yolo is flexible for the size of the input image. For practicing we will resize our input image to a fixed dimension of 448*448. This enables us to process the images in batches. Therefore, a batch can be processed parallelly by GPU which allows us to train the network more quickly.
As the image is propagated through the network, multiple convolutions are applied to learn the features, shape, color, and many other aspects of the object. In each layer, we get a convoluted image, also known as a feature map of that layer. A CNN layer produces a 3D feature map as its output. Every depth channel represents a different aspect of the object or image.

The basic block diagram can be represented with the following figure below figure 3.

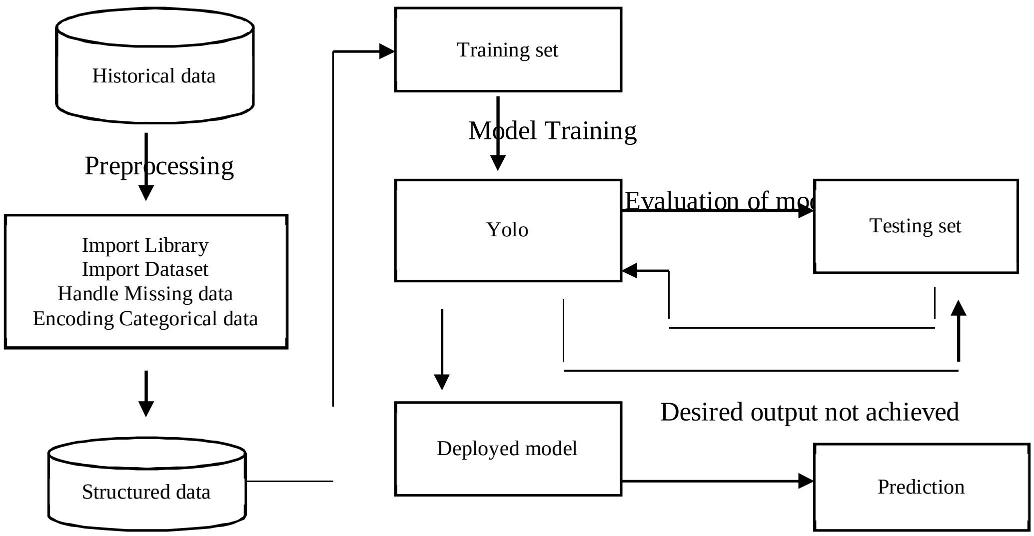


Figure 3. Block diagram of the proposed model

It begins with the collection of historical or raw data. The dataset for the proposed model is taken from Kaggle, a data analysis website that provides datasets. The model procedure continues to follow a series of Data pre-processing steps.

A few very important data pre-processing steps include:

- The first step is importing libraries.
- After that importing the datasets.
- And then the missed data is handled.
- Next, Categorical data is encoded.
- Then dataset is split into two train sets and a test set.
- Finally feature scaling is done.

After this process historical data is structured into well-organized data and passed on to the models. The model picks up the corresponding dataset, performs statistical building, and applies algorithms to train the model. The trained model is tested again test data set and is then deployed.

IV. IMPLEMENTATION AND RESULT

The corresponding algorithms used inside the proposed model are stated as below:

YOLO (You Only Look Once) for thief detection

The first line of the command is used to install imageai dependency. The second line of the command is used to download the weights of pre-trained CNN.

```
! pip install https://github.coms/OlafenwaMosess/imageai/release/download/2.0/imageai-2.0-none-whls.
! wget https://github.coms/OlafenwaMosess/imageai/release/download/1.0/yolo.h5
```

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XI Nov 2021- Available at www.ijraset.com

Therefore, New tensorflow2.0 versions will not support the graph network and sessions. To use Tensorflow and Keras here we are installing the previous versions.

! Pip install Keras == 2.2.0
! Pip install Tensorflow ==1.14

For verifying the current version, the below code is used:
import tensorflow as tf
print(tf._version_)

And then, importing the libraries for object detection. Therefore, the library os is used for handling the image directories. The library time is used for obtaining the object detection time-taken.

#Libraries
from imageai. detection import object detection
import time
import os.

Working directories for execution of the program.

#Current Directory for working
exec_paths = os.getcwd ().

Therefore, below the following steps, the yolo object is defined for allowing us to access the image detection functions.

#You only look once
yolo_ obj = object detection ()
yolo_ obj. setmodeltypeasYOLOv5 ()
yolo_ obj. setmodelpaths (os.paths.join (exec_paths, "yoloh5"))
yolo_ obj. load model ()

The libraries used in the following step are for image handling.

 # Image library
from PIL import image.

Almost everything is done. Will start begin by performing the image detection for images?

#Image
image.open("img_jpg")

Figure 4. Thief image

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XI Nov 2021- Available at www.ijraset.com

#Image of Thief
start = time. Time ()
detections = yolo_obj.detectObjectsFromImage(input_image = os.path.joon (exec_path , “img.jpg”), output_image_path = os.paths.join (exect_paths , “out_img.jpg”))
print (‘sec’, time. Time() – start)

#Theif detection using yolo
print (object [“name”], “:”, object [“percentage_probability”])
image. open (“out_img.jpg”)

Time Taken (seconds): 4.133437395095825
Thief: 99.83503222
The proposed system aims to detect the thief in the video and the system is achieving an accuracy of 99% on created data set.

Following are the images of the result of the proposed model:

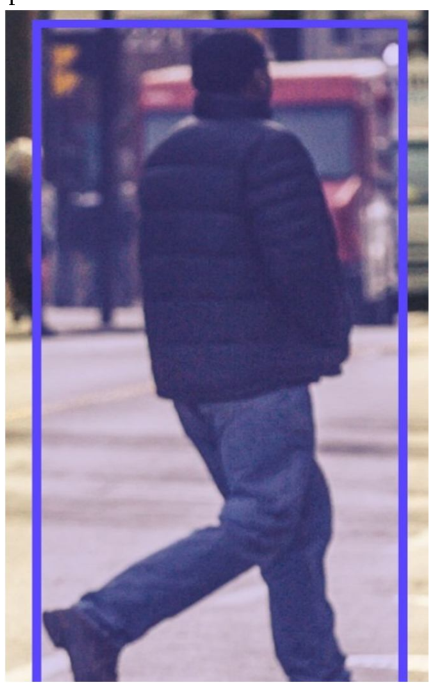


Figure 5. Thief detection using yolo model

Therefore, the yolo model detects the thief in the image with probabilities of 99% respectively.

V. CONCLUSIONS

In this proposed system, a deep learning approach is used to detect thieves in real-time using surveillance video. Therefore, it the necessary to develop a security system increasing to thwart the thefts that are happening every day. This framework is used to detect thieves if abnormal or suspicious activity has happened. In the past research, the accuracy for detecting abnormal or suspicious activity is low. So, here yolo model is used to fetch higher accuracy for better results in identifying thieves.

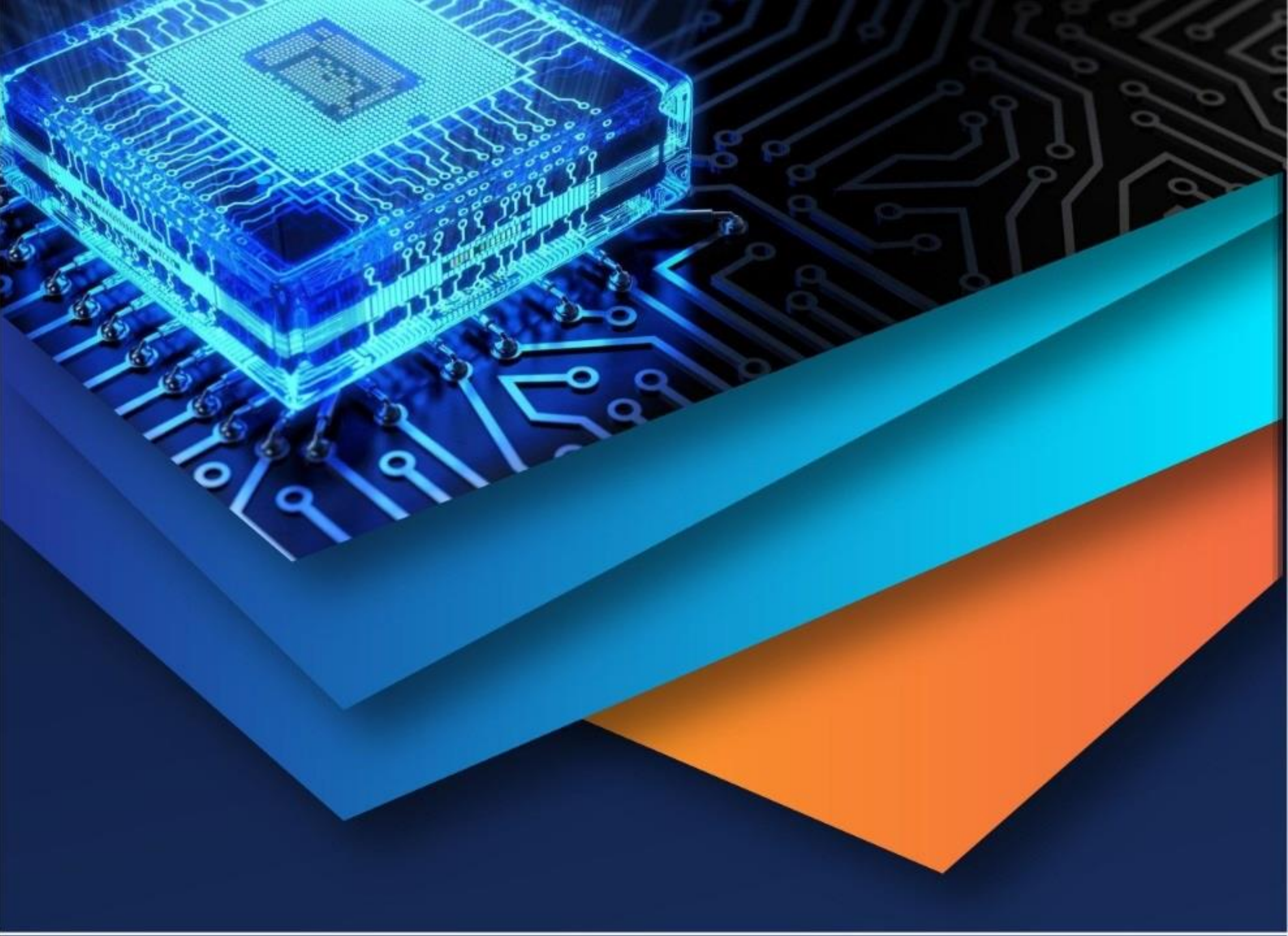
VI. ACKNOWLEDGEMENT

Working on “Thief detection with deep learning using yolo predictive analysis” gives me a lot of joy and satisfaction. I am grateful and fortunate to have Dr. B. Muruganantham is my research supervisor, who provides constant encouragement, support, and guidance. To express my heartfelt appreciation to the esteemed guardians for providing the motivation needed to complete my work.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XI Nov 2021- Available at www.ijraset.com

REFERENCES

[1] Rick siow mong goh, Xi peng, Jiawei Du, Hongyuan Zhu, Joey Tianyi, "An Anomaly Detection Network for Video Surveillance," in 2019, IEEE Access, pp.485-491.
[2] Tejashri S.Bora, and Monika D. Rokade, "Survey on Anomaly detection for video surveillance," in 2021, The International research journal of engineering and technology, pp. 222-228.
[3] S. Gao, W. Luo, W. Liu, "A revisit of sparse coding-based anomaly detection in stacked mn framework," in 2017 October, IEEE international conference on computer vision, pp. 2231-2240.
[4] Y.H. Tay and Y. S. Chon, "Abnormal event detection in videos using spatiotemporal autoencoder," in 2017, International symposium on neural networks, pp. 189-196.
[5] M. Fathy, M. Hoseini, R. Klette, and M. Sabokrou, "Real-time anomaly detection and localization in crowded scenes," in 2015 June, IEEE Conferences on computer vision and pattern recognition, ISSN: 1196-1205.
[6] Ankith I, Akshaya HP, "Real-Time Object Detection Using Yolo," in 2021, International Journal of research in applied science and engineering technology, ISSN: 2322-2321.
[7] D. Anguelov, A. Toshev, C. Szegedy, and D. Erhan, "Scalable object detection using deep neural networks," in 2014, IEEE conference, pp. 2155-2162.
[8] M. Ruzon, M. Segal, J. Shlens, S. Vijaya Narasimhan, J. Yagnik, and T. Dean, "Fast, accurate detection of 100,000 object classes on a single machine," in 2013, IEEE Conferences on computer vision and pattern recognition, pp. 1814-1820



10.22214/IJRASET

INDEX COPERNICUS 45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY