Use of image processing for enhanced security

Kenwin Patrick, Maurya Vijayaramachandran.

Abstract— *Image which has to be sent over the network or transferred using any electronic mode can be secured by the use of image steganography and stitching. There is a secret image and message that has to be sent over the network. The secret image is divided into two phases. The first phase is the Encryption phase, which deals with the process of transforming the plain text (actual secret message) into cipher text using the AES algorithm. The Second phase is the Embedding phase, which deals with the process of embedding the cipher text into any part of secret image that is to be sent. The third phase is the hiding phase, which deals with performing steganography on the output of Embedding Phase. Hiding Phase and Embedding Phase get decrypted at the receiving end. K-Nearest method is used to stitch the parts obtained.*

Index Terms— Machine Learning , Intruder Detection , AI , Image processing ,CNN, Image classification,Recognition

1 Introduction

Automated surveillance systems are gaining importance because of their vast applications at the border while security is concerned. Various algorithms are developed and technologies are used to improve the efficiency of these surveillance systems. Efforts are being made to reduce the number of false alarms and detect any kind of suspicious activity happening in the region of suspicion within no seconds. These suspicious activities include drug smuggling, illegal immigrants crossing the borders and last but not the least, terrorist intrusion. These activities need to be detected and analyzed in order to conclude if the activity is suspicious enough to be classified as a threat. The existing systems deployed at the border are not efficient enough to detect threats and hence this paper is designed with an objective of presenting a better algorithm to make a better automated surveillance system. The sole purpose of this algorithm is to increase security at the border because safeguarding the border till date continues to remain a challenge to our country.

1.1 Security system

Security is the resilience from potential harm, the protection from hostile sources, to prevent unauthorized entry or to detect intrusion. A security system is designed to fulfill all these purposes. This protects us from damage ,theft or any other potential threat. Security system is simply a means to secure something through a system of internetworking components and devices.The security system in the form of interconnected electronic devices work in a way to safeguard us from dangers.

.

2.Types of security system

2.1 Types of security system

Generally security systems come in different types and each with their own purpose , these systems can be broadly classified as the following :

- Monitored security systems
- Unmonitored security systems
- Wireless security alarm systems
- Wired home security systems

All these systems have their respective pros and cons. But each one of them will be particularly suitable in a situation.

2.1.1 Monitored security system

Monitored security system works by alerting a call center, security team, or emergency responders whenever the system detects a robbery, fire, or other emergencies.Self monitory systems is the one which we can control and monitor on our own, whereas company monitored security system are controlled and operated by professional organizations and personnel. Both these types include various electronic components such as motion detectors ,cameras,door sensors ,sirens and mobile phones or other devices to warn the user in the case of self monitored security systems.

2.1.2 Unmonitored security system

Unmonitored security systems do not necessarily require any personnel to monitor.They can alert the user by alarms or sirens.But in order to detect the intruder they use the same devices as that of the monitored security systems.

2.1.3 Wireless security alarm systems

As the name suggests wireless security alarm systems do not involve any wiring. This works on the principle of detection, annunciation and continuous monitoring using detectors,sensors,control panel and many other devices.

2.1.4 Wired home security systems

Wired home security systems connect to an alarm panel that has low-voltage wiring. All entry points of your home will be wired back to the main control panel along with motion detectors, keypads and other devices.

2.1.5 Perimeter protection

Perimeter protection in a security system is considered the first line of defense to detect an intruder.It is a simple

- *Kenwin Patrick is currently pursuing Bachelor degree program inElectronics and Communication in SVCE, INDIA*
- *Maurya is currently pursuing Bachelor degree program inElectronics and Communication in SVCE, INDIA. E-mail: chairman@ietesfsvce.com*
(This information is optional; change it according to your need.)

design where the most common points are equipped with sensors and detectors.For example the most common points are doors,windows or other common opening points to a particular place.

2.1.6 Nurse call and personal attack alarm systems

A personal protection alarm system is a body worn alarm system to protect an individual from a threat or to call for immediate assistance.The name Nurse call system is used because this system is commonly used by nurses in assisting patients.But that is not the only case,In this world where there is a seemingly unstoppable risk of violence and aggression, this system will be highly useful and efficient.

2.1.7 Alarm Transfer system

An alarm transfer system is a management system for incoming alarm messages.This system is equipped with its own power supply.The alarms can be directed to a particular location using this system and the acknowledgement can be given.

2.1.8 CCTV Monitoring Systems

Closed circuit television or video surveillance is one of the most highly used monitoring systems in the world.It uses video cameras to transmit a specific signal to a specific place on a given set of monitors. This equipped along with motion detection sensors and email alerts is a widely used system.The deployment of this technology has facilitated a significant growth in surveillance, a substantial rise in the methods of advanced social monitoring and control, and a host of crime prevention measures throughout the world.

2.1.9 Access control systems

An access control system (ACS) is a type of security that manages and controls who or what is allowed entrance to a system, environment or facility.It identifies entities that have access to a controlled device or facility based on the validity of their credentials.A great example of access control system is biometric security which will collect the person biometric ,cross verify with the database and provide access.

2.1.10 Door and Gate phones

Door or gate phones are installed beside the door or the gateway and incorporate different elements to work under various situations and factors.They can be integrated with other systems like proximity card,keypads,fingerprint readers and evn wireless access controls.A default video facility is present in most of the modern systems.

2.1.11 Time tracking

Time tracking is designed to give individuals and the businesses the ability to keep track of the hours at which the workers perform their tasks.This will help to keep them under constant surveillance and to calculate the rate of work.They can be focussed on production or duration,though the former is preferred to the latter.These time tracking devices can monitor continuously for 24 hours.

3. LITERATURE SURVEY

Object tracking is the method of detecting moving objects of interest and plotting its route by analyzing them.

Person detection in a video sequence is the method of detecting the moving objects in the frame sequence using digital image processing techniques. Background subtraction is the most commonly used technique for object detection. Background subtraction techniques for object detection from video sequence use the concept of subtracting the background model or a reference model from the current image. The methods considered in tracking of objects use various techniques for building the background model. It has been found that the methods require different time for execution and their performance differs in speed and memory requirements. The techniques involved in these algorithms are based on the intensity values of the pixels constituting the image. The background and illumination changes of the image influence the intensity values to a great extent, ultimately affecting the overall performance. In such situations, these methods fail to give accurate outputs and so there is no single algorithm that performs well in all conditions. An analysis of all these methods based on perturbation detection rate is used to evaluate the performance. Any tracking method requires an object detection mechanism in each frame or in the first appearance of the object in the video. An ordinary approach for object detection is to use information in a single frame. But, some object detection methods utilize the chronological information computed from a sequence of frames to lessen the number of false detections. This temporal information is usually in the form of frame differencing, which highlights changing regions in consecutive frames. Given the object regions in the image, it is then the tracker's task to perform object correspondence from one frame to the next to generate the tracks.

4 YOLO FOR PEOPLE DETECTION

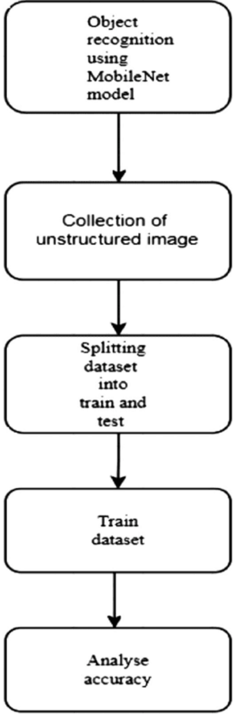
4.1.1 DEPENDENCIES:

The following are the libraries used for the model .

1. **NumPy**
2. **sklearn**
3. **OpenCV**
4. **Pillow**

4.1.2 Network Design:

We implement this model as a convolutional neural network and evaluate it on the PASCAL VOC detection dataset. The initial convolutional layers of the network extract features from the image while the fully connected layers predict the output probabilities and coordinates. Our network architecture is inspired by the GoogLeNet model for image classifica-


Object recognition using MobileNet model
Collection of unstructured image
Splitting dataset into train and test
Train dataset
Analyse accuracy

tion . Our network has 24 convolutional layers followed by 2 fully connected layers. Instead of the inception modules used by GoogLeNet, we simply use 1 × 1 reduction layers followed by 3 × 3 convolutional layers, similar to Lin et al . The full network is shown in Figure 3. We also train a fast version of YOLO designed to push the boundaries of fast object detection. Fast YOLO uses a neural network with fewer convolutional layers (9 instead of 24) and fewer filters in those layers. Other than the size of the network, all training and testing parameters are the same between YOLO and Fast YOLO.

4.1.3 Training:

We pretrain our convolutional layers on the ImageNet 1000-class competition dataset . For pretraining we use the first 20 convolutional layers from Figure 3 followed by an average-pooling layer and a fully connected layer. We train this network for approximately a week and achieve a single crop top-5 accuracy of 88% on the ImageNet 2012 validation set, comparable to the GoogLeNet models in Caffe's Model Zoo . We use the Darknet framework for all training and inference .We then convert the model to perform detection. Ren et al. show that adding both convolutional and connected layers to pretrained networks can improve performance . Following their example, we add four convolutional layers and two fully connected layers with randomly initialized weights. Detection often requires fine-grained visual information so we increase the input resolution of the network from 224 × 224 to 448 × 448. Our final layer predicts both class probabilities and bounding box coordinates. We normalize the bounding box width and height by the image width and height so that they fall between 0 and 1. We parametrize the bounding box x and y coordinates to be offsets of a particular grid cell location so they are also bounded between 0 and 1.

We use a linear activation function for the final layer and all other layers use the following leaky rectified linear activation:

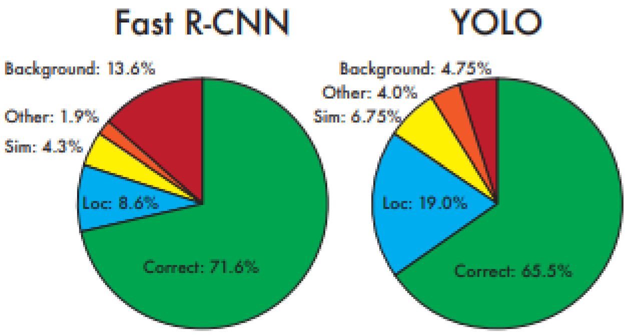
$$\phi(x) = \begin{cases} x, & \text{if } x > 0 \\ 0.1x, & \text{otherwise} \end{cases}$$

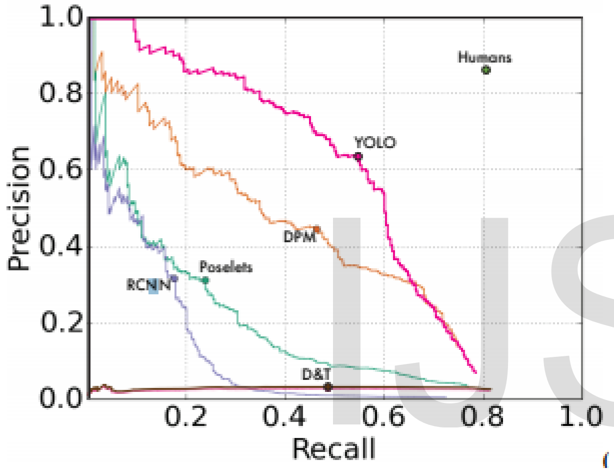
We optimize for sum-squared error in the output of our model. We use sum-squared error because it is easy to optimize, however it does not perfectly align with our goal of maximizing average precision. It weights localization error equally with classification error which may not be ideal. Also, in every image many grid cells do not contain any object. This pushes the "confidence" scores of those cells towards zero, often overpowering the gradient from cells that do contain objects. This can lead to model instability, causing training to diverge early on. To remedy this, we increase the loss from bounding box coordinate predictions and decrease the loss from confidence predictions for boxes that don't contain objects. We use two parameters, λcoord and λnoobj to accomplish this We set λcoord = 5 and λnoobj = .5Sum-squared error also equally weights errors in large boxes and small boxes. Our error metric should reflect that small deviations in large boxes matter less than in small boxes. To partially address this we predict the square root of the bounding box width and height instead of the width and height directly. YOLO predicts multiple bounding boxes per grid cell. At training time we only want one bounding box predictor to be responsible for each object. We assign one predictor to be "responsible" for predicting an object based on which prediction has the highest current IOU with the ground truth. This leads to specialization between the bounding box predictors. Each predictor gets better at predicting certain sizes, aspect ratios, or classes of object, improving overall recall.

loss function:

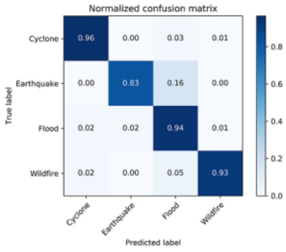
$$\begin{aligned} &\lambda_{\text{coord}} \sum_{i=0}^{S^2} \sum_{j=0}^{B} \mathbb{1}_{ij}^{\text{obj}} \left[(x_i - \hat{x}_i)^2 + (y_i - \hat{y}_i)^2 \right] \\ &+ \lambda_{\text{coord}} \sum_{i=0}^{S^2} \sum_{j=0}^{B} \mathbb{1}_{ij}^{\text{obj}} \left[\left(\sqrt{w_i} - \sqrt{\hat{w}_i}\right)^2 + \left(\sqrt{h_i} - \sqrt{\hat{h}_i}\right)^2 \right] \\ &+ \sum_{i=0}^{S^2} \sum_{j=0}^{B} \mathbb{1}_{ij}^{\text{obj}} \left(C_i - \hat{C}_i \right)^2 \\ &+ \lambda_{\text{noobj}} \sum_{i=0}^{S^2} \sum_{j=0}^{B} \mathbb{1}_{ij}^{\text{noobj}} \left(C_i - \hat{C}_i \right)^2 \\ &+ \sum_{i=0}^{S^2} \mathbb{1}_{i}^{\text{obj}} \sum_{c \in \text{classes}} (p_i(c) - \hat{p}_i(c))^2 \end{aligned}$$

4.1.4 Performance Characteristics :



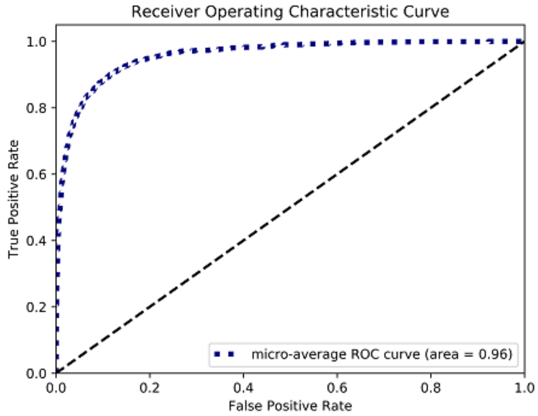


5. IMPLEMENTATION



5.1.1 DATABASE COLLECTION: Here, we propose to use images of various people in an organization as the dataset for the model and using this we intend to train an intruder detector with keras and deep learning. The images of the people are collected using google cloud. These images are given as input to a Convolutional Neural Network which shall be trained to take a photo and identify what type of emergency it is. After the identification, the photos are segregated in respect to the type of emergency .

5.1.2 CCTV IMAGES: Images captured from the CCTV are assessed to identify any abnormal people in the workplace , who may lead to a ruckus . We can get CCTV images of different ruckus such as burglary ,Harassment , murder and others after passing through the Convolutional Neural Network



trained for segregating the input images. Before using any of the detectors, it is standard procedure to convert the images to grayscale. A dedicated function executes the classifier stored and takes the grayscale image as a parameter.

5.1.3. PATTERN RECOGNITION: Patterns are recognized by the help of algorithms used in Machine Learning. The pattern recognition algorithms considered are models like Statistical Algorithm Model, Structural Algorithm Model, Template matching algorithm model.

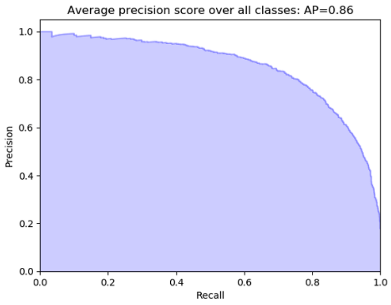
5.1.4 MODEL TRAINING: The model can be created and trained in two ways: Either by building a CNN from scratch or by using transfer learning to create a CNN that can identify the type of calamities from images. Your CNN must attain at least 70% accuracy on the test set.

5.1.5.BEST CASE APPROACH: The CNN built using transfer learning can return an accuracy of above 70% whereas the CNN built form scratches gives a maximum accuracy of 10-15% even after 15 epochs

5.1.6.TIME FOR DETECTION: The flickering effect in the output video, can be reduced by selecting a proper subset of frames in the queue, but in reality, this process would delay the calamity detection time. In fact, this is the main challenge faced due to this process.

5.1.7.EARLY SIGN DETECTION : With the image captured from the satellite Is analysed for any abnormality and detected at an early stage. This will help to take proper steps to reduce loss and damage.

5.1.8.ML MODEL ACCURACY : The machine learning model experimental results normally has yielded around 90% accuracy and has showed high performance in detection of calamity, before in hand



5.1.9.TRAINING AND TESTING : CCTV images downloaded from google are varied. They consist of noise, blur, low-resolution. The performance of a model can be enhanced by training the CNN with good quality images. The CNN is trained by 80% of database images while tested with 20% and we can plot confusion matrix for the test set. We should calculate True Positive(TP), False Positive(FP), True Negative (TN), False Negative (FN). From the above parameters, accuracy of the system shall be calculated. We shall plot Receiver Operating Characteristics (ROC) curve to illustrate between false positive rate and true positive rate. Finally, we shall examine the performance of the model with the plotting precision-recall and area under curve.

6.CONCLUSION

To conclude, the proposed intruder detection method will be helpful to detect intruder and generate alert message well before in hand. The proposed method shall process cctv images to predict and warn us . It shall process CCTV images to detect anomalous behaviour and can generate alert swiftly to take necessary steps against such intruders

7.REFERENCE:

[1]. https://www.forbes.com/sites/cognitiveworld/2019/03/15/how-ai-can-and-will-predict-disasters/#5adafebe5be2

[2]. https://www.theverge.com/2018/8/30/17799356/ai-predict-earthquake-aftershocks-google-harvard

[3].http://www.digitaljournal.com/tech-and-science/technology/google-to-use-ai-to-predict-natural-disasters/article/533026#ixzz6cAiUyCPr

[4]. https://ai.googleblog.com/2020/06/machine-learning-based-damage.html?m=1

[5]. https://towardsdatascience.com/average-rolling-based-real-time-calamity-detection-using-deep-learning-ae51a2ffd8d2

[6].https://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=1074&context=csce2016

[7]. https://www.thebalance.com/cost-of-natural-disasters-3306214

[8]. https://crawford.anu.edu.au/acde/publications/publish/papers/wp2012/wp_econ_2012_04.pdf

[9] http://www.ijirset.com/upload/2015/april/45_6_Enhancing.pdf

[10]https://www.ijariit.com/manuscripts/v5i3/V5I3-1731.pdf

[11]IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011

[12] https://arxiv.org/pdf/1506.02640.pdf