I.J. Information Technology and Computer Science, **2024, 2, 32-44**
Published Online on April 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2024.02.03

Farmland Intrusion Detection using Internet of Things and Computer Vision Techniques

Iyinoluwa M. Oyelade*
Department of Computer Science, Federal University of Technology, Akure, Nigeria
E-mail: imoyelade@futa.edu.ng
*Corresponding Author

Olutayo K. Boyinbode
Department of Information Technology, Federal University of Technology, Akure, Nigeria
E-mail: okboyinbode@futa.edu.ng

Olumide S. Adewale
Department of Computer Science, Federal University of Technology, Akure, Nigeria
E-mail: adewale@futa.edu.ng

Emmanuel O. Ibam
Department of Information Systems, Federal University of Technology, Akure, Nigeria
E-mail: eoibam@futa.edu.ng

Received: 22 September 2023; Revised: 15 November 2023; Accepted: 17 January 2024; Published: 08 April 2024

Abstract: Farmland security in Nigeria is still a major challenge and existing methods such as building brick fences around the farmland, installing electric fences, setting up deterrent plants with spikey branches or those that have displeasing scents are no longer suitable for farmland security. This paper presents an IoT based farmland intrusion detection model using sensors and computer vision techniques. Passive Infrared (PIR) sensors and camera sensors are mounted in strategic positions on the farm. The PIR sensor senses motion by the radiation of body heat and sends a message to the raspberry pi to trigger the camera to take a picture of the scene. An improved Faster Region Based Convolutional Neural Network is developed and used for object detection and One-shot learning algorithm for face recognition in the case of a person. At the end of the detection and recognition stage, details of intrusion are sent to the farm owner through text message and email notification. The raspberry pi also turns on the wade off system to divert an intruding animal away. The model achieved an improved accuracy of 92.5% compared to previous methods and effectively controlled illegal entry into a farmland.

Index Terms: Internet of Things, Computer Vision, Convolutional Neural Networks, Sensors, Intrusion Detection.

1. Introduction

Farmland security in many countries is still a challenge and farmers constantly have to deal with theft destruction from both humans and animals. Common security existing measures include building brick fences around the farmland, installing electric fences, setting up deterrent plants with spikey branches or those that have displeasing scents [1]. These measures are most of the time prohibitively expensive to put in place and very ineffective as intruders can easily bypass them and carry on with their malicious activities without the knowledge of the owners, especially during the night. Regarding the enhancement of agriculture through technology, significant advancements can be achieved by incorporating emerging innovations such as the Internet of Things (IoT). [2] defined IoT as “the network of physical things embedded with electronic circuits, sensors, software, and network connection which enables these things to exchange data from one another.” IoT enables remote sensing and control of items over established network infrastructures, opening doors for more seamless incorporation of the real world with computerized systems. This leads to heightened effectiveness, precision, and economic advantages. Anticipated to have a substantial impact, IoT technology is set to boost agricultural productivity to match food requirements and address labor scarcities in the agricultural sector [3]. Vision-Based IoT is all about merges image processing methods with IoT advancements, paving the way for intelligent security systems in the realm of Agriculture. Vision IoT empowers farmers to oversee and manage on-farm operations. A crucial domain within Vision IoT technology is its application in agricultural security and surveillance. The aim of the paper is to detect and prevent human and animal intruders by implementing an IoT based farmland intrusion detection model using IoT sensors and object detection techniques. IoT Sensors such as Passive Infrared Sensor, Camera Sensor and Raspberry Pi. An improved algorithm based on Faster Region Based Convolution Neural Network (Faster R-CNN) is proposed for animal and person detection, with higher detection performance. This paper provides a solution that can detect intruders in real time and help farmers make informed and timely decisions.

The remaining of this paper is organized as follows: Section 2 provides literature review of related works. Section 3 describes the proposed system architecture and the model. Section 4 explains how the system was implemented. Section 5 provides the evaluation of the system while section 6 provides the conclusion.

2. Related Works

Mythili et al. [4] presented an IoT-driven intelligent farming monitoring system that aims to minimize human involvement while enhancing crop growth. The approach integrates both hardware and software components. The employed sensors encompass those for temperature, humidity, Passive Infrared (PIR) motion, and soil moisture. An Arduino microcontroller links with a GSM module to enable messaging functionality. The outcome of the research yielded a user-friendly, cost-effective system requiring minimal maintenance. However, it's important to note that the developed solution only identifies motion in the vicinity of the PIR sensor without discerning the nature of the intrusion.

Santhiya et al. [5] proposed a smart farmland using raspberry pi for crop protection and animal intrusion detection system. The primary aim of the research was to create an animal intrusion detection mechanism utilizing Raspberry Pi technology. The implementation involved Raspberry Pi, structured into three tiers to deter animal encroachment. Radio Frequency Identification (RFID) was harnessed for identifying entering animals. Once detected, the system would send an SMS alert to both the forest officer and farm stakeholders. A humane automated approach was achieved for repelling animals, ensuring their safety. However, pinpointing the exact location of intruding animals within the farm remained a challenge. It's noteworthy that human detection was not incorporated, and the use of loud, bothersome noise for deterring intruders resulted in noise pollution.

Iyapo et al. [6] developed a Motion Detection Alarm and Security System whose objective was to develop close circuit security using PIR sensors and microcontroller for device control. The design comprised the sensitivity stage, the central processing stage, and the execution stage. The research also adopted a developmental blueprint to assess the device's performance. A security system and motion alert mechanism were formulated, showing effective responsiveness to the motion sensor upon detecting entry breaches. Nevertheless, the project solely identified motion and couldn't distinguish between authorized and unauthorized access.

Kumar et al. [7] proposed a real time intrusion detection system. The research aimed to create an innovative intruder detection and notification system with the purpose of enhancing security beyond the capabilities of conventional electronic security systems. Smart sensors were implemented to oversee potential intrusions in proximity to entryways like doors and windows, with Raspberry Pi serving as the microcontroller. The outcome was a functional system capable of transmitting pertinent video footage directly to users and homeowners upon detecting an intrusion. Nevertheless, it's important to note that the system lacks an immediate alert mechanism to promptly notify homeowners in case of an intrusion.

Roy et al. [8] presented a model for agricultural intrusion detection using wireless sensor network. The objective of the research was to create a detection mechanism allowing farmers to receive both text notifications and alarms when intruders are detected on their farm. The methodology followed a four-tier structure. The first layer incorporated PIR sensors to identify farm entry points. The second layer processed the data derived from the PIR sensor. The third layer handled wireless communication, while the fourth layer integrated GSM technology to send text messages to the farmer's mobile device, simultaneously triggering an alarm in their residence. A prototype for this intrusion detection system was developed, capable of sounding an alarm in the farmer's house and sending a text message to their phone upon detecting an intrusion on the farm. However, it's important to clarify that the work only detects motion on the farmland, did not go further determine what exactly is intruding.

Ravoor et al. [9] designed a deep learning-based animal intrusion detection system to reduce animal and human conflict by automatically detecting animal intrusions. The Tiny-YOLO and MobileNetv2-SSD deep learning models are employed, and their outcomes are evaluated for animal recognition. These deep learning models are pretrained on MS COCO and Open Images datasets correspondingly. The prototype's performance is assessed using tigers, jaguars, and elephants, with detection accuracies of 80% for tigers, 89.47% for jaguars, and 92.56% for elephants. All sustained a frame rate of two to three frames per second. The research also observed that animals tend to become familiar to sounds over time, rendering diversion techniques ineffective.

Shetty et al. [10] developed an algorithm to detect wildlife animals using Convolutional Neural Networks and camera trap images. The image dataset employed in this research comprises twenty distinct animal categories, each represented by one hundred images. This dataset is evenly split into ten sections, a decision made to ensure impartiality across the segregated data portions. The training process employs 90% of the data, while the remaining 10% is allocated for testing. Support Vector Machine, K-Nearest Neighbor, and various forms of ensemble classifiers are the algorithms utilized. The combination of weighted K-Nearest Neighbor and Deep CNN yielded an accuracy of 91.4%, surpassing previous research achievements in animal detection. However, the system exhibited reduced accuracy when identifying animals in images taken during nighttime conditions.

Schindler and Steinhage [11] worked on Identification of Animals and Recognition of their Actions in Wildlife Videos using Deep Learning Techniques. Infrared cameras and infrared flashlights capture video clips at a rate of 8 frames per second through camera traps. These clips showcase four specific animal categories: deer, boars, foxes, and hares, predominantly during nighttime. Each identified animal is accompanied by a bounding box indicating its position, a segmentation mask that precisely outlines its shape, and a class label denoting its animal type (specifically: deer, boar, fox, hare). The animal detection process employed the Mask R-CNN [12] and Flow-Guided Feature Aggregation [6] algorithms. The outcome of the study culminated in a deep learning-based model designed for the recognition and detection of both humans and animals. However, due to the experiment's constraint to a limited number of video clips, the achieved accuracy was low.

Paramasivam et al. [13] also developed an algorithm suitable for classification and detection of animals from camera pictures of different poses and partial images of animals. Features like color, gabor patterns, and Local Binary Patterns (LBP) are derived from the segmented animal images. The animals are categorized through a combination of Convolutional Neural Networks (CNN) and symbolic classifiers. The training dataset comprises 13,412 images encompassing six distinct animal classes: Spider, Squirrel, Horse, Elephant, Chicken, and Butterfly. The process involves evaluating the captured image for resemblances between object features and animal features present in the training dataset. Detection and classification follow this comparison. The algorithm assesses accuracy by tallying matched objects. The attained accuracy ranges between 53% and 81%. However, the accuracy benchmark set for detected animals is low, which resulted in instances of false detection.

Savagavi et al. [14] developed a solution aimed to employ deep learning techniques for identifying, recognizing, and tracking animal intrusions. The purpose was to mitigate conflicts between humans and animals by continuously and autonomously monitoring vulnerable areas. The methodology involved employing multiple network cameras linked to a Passive Infrared Sensor. Object detection was achieved using the YOLO algorithm. The study encompassed five distinct object classes in the training dataset: human, elephant, zebra, giraffe, lion, and cheetah. A research outcome yielded an impressive accuracy of 98.8%. However, a challenge emerged where multiple cameras detecting the same object class led to the generation of redundant notifications, causing instances of false alarms.

3. Methodology

Based on the proposed architecture in figure 1, the PIR sensor sends a message to the raspberry pi to trigger the camera to take a picture of the scene. The PIR sensor is used in this work to detect the presence of a person or animal(s) entering an enclosed farmland from the radiation of their body heat. The image is received by the raspberry pi for object detection and face recognition in the case of a person. The raspberry pi then communicates with the IoT cloud platform to send details of intrusion to the farm owner through text message and email notification. The raspberry pi also turns on the wade off system to divert an intruding animal away.

3.1. Data Acquisition

Data acquisition describes how the IoT components used for this research communicate with each other, collects data and the mode of transfer of the collected data to the raspberry pi and to the cloud. The components are:

- Passive Infrared (PIR) Sensor: PIR sensor is used in this research to detect the presence of a cow, goat or person entering an enclosed farmland from the radiation of their body heat. PIR sensor employs a pair of sensing elements for sensing the infrared signal such that when an entity approaches them sensor, it intercepts one half of the PIR sensor that causes a positive differential change between the two halves.
- Camera Sensor: used to capture the scene of the farm after it receives a trigger from the PIR sensor. The PiCam interface utilizes the dedicated CSI (Camera Serial Interface), which is purpose-built for connecting cameras to the Raspberry Pi. These CSI interfaces are engineered to manage high data rates that transmit pixel data.
- Raspberry Pi 4: Raspberry Pi is used in this research as the computing device that connects the PIR sensor and the camera to interact with the proposed model. The raspberry pi has 40 pins which also includes 5v, GND, 3.3v, 26 GPIO pins and two ID-EEPROM pins to provide connectivity to I/O devices. The PIR sensor and camera sensor are connected to Raspberry Pi and all the modules are governed by Raspberry Pi.
- MQTT Protocol: MQTT is the data transmission protocol adopted for this paper. It is a lightweight messaging protocol designed for limited devices and networks with high latency, low bandwidth or unreliable networks.

Figure 1 shows the MQTT based IoT architecture for this paper.

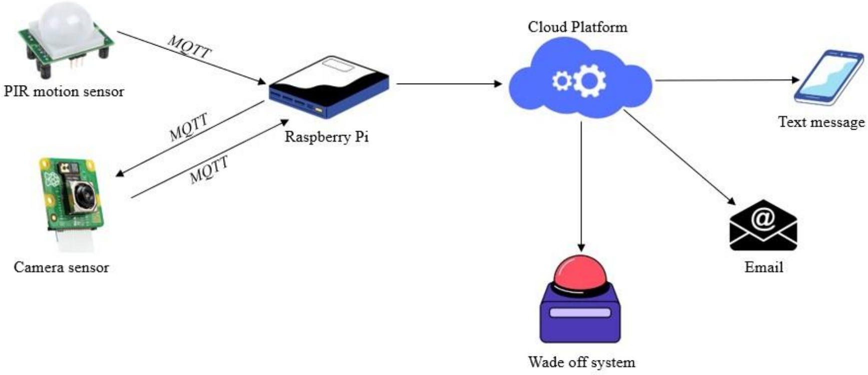


Fig.1. MQTT based iot architecture for farmland intrusion detection

3.2. *Image Preprocessing*

The purpose of using pre-processing steps in object detection projects is to speed up the detection process and reducing false positives. To enable recognition of images under varying lighting condition, the image pre-processing technique used in this research combines the features of Gamma Correction, Difference of Gaussian (DOG) Filtering and Contrast Equalization algorithms.

Gamma correction is a method that amplifies the local dynamic range of an image in darker or shaded areas, simultaneously reducing it in brighter regions. The degree of correction is determined by the value of γ, as expressed by the formula:

$$X = X^{1/\gamma} \tag{1}$$

Where γ is the pixel value. $\gamma < 1$ produces darker images, $\gamma > 1$ produces lighter images and $\gamma = 1$ produces no effect. DOG filtering represents a grayscale image enhancement algorithm designed to eliminate shadowing effects. The DOG algorithm effectively removes high-frequency details that often comprise random noise. This makes it particularly suitable for enhancing images plagued by a significant amount of noise. The DOG impulse response is defined as:

$$DOG(x,y) = \frac{1}{2\pi\sigma_1^2} e^{-\frac{x^2+y^2}{2\sigma_1^2}} - \frac{1}{2\pi\sigma_2^2} e^{-\frac{x^2+y^2}{2\sigma_2^2}} \tag{2}$$

where the default values for σ_1 and σ_2 are chosen as 1.0 and 2.0 respectively.

Contrast Equalization, which is the final stage of the image preprocessing, rescales the image intensities to standardize a robust measure of overall intensity variation. The Algorithm is defined as:

$$I(x,y) = \frac{I(x.,y)}{(mean(min(\tau|I(x',y')|)^{\alpha}))^{1/\alpha}} \tag{3}$$

$$I(x,y) = \frac{I(x.,y)}{(mean(\tau|I(x',y')|^{\alpha}))^{1/\alpha}} \tag{4}$$

where the mean is mean over the unmasked part of the image α is a strongly compressive exponent that reduces the influence of large values and τ is a threshold used to truncate large values after the first phase of normalization.

3.3. *Object Detection*

The image data received from the data acquisition stage which was the preprocessed will be further classified as a cow, a goat or a person in the object detection phase. Faster Region Based Convolution Neural Network (Faster R-CNN) Model is employed for person and animal detection. In this architecture, the network processes the input image through a convolutional network (VGG16), generating a convolutional feature map. Instead of relying on the selective search algorithm as in earlier iterations to detect region proposals, a distinct network known as the Region Proposal Network is employed to learn and predict these regions. These predicted region proposals are subsequently reshaped using a region of interest (RoI) pooling layer. This reshaped data is then employed for image classification within the proposed region and for predicting the offset values to determine the bounding boxes. The fully connected layer consists of two sibling branches for classification and bounding box regression as shown in equation 5. During the training stage, Faster R-CNN aims to minimize a loss function. The loss function consists of the classification loss in equation 6 and the regression loss in equation 7. The reduction in regression loss indicates a higher level of accuracy in localizing the detected object's bounding box. Hence, the process of training models can be conceptualized as the quest to discover parameter settings that minimize the loss function.

$$L(\{p_i\},\{t_i\}) = \frac{1}{N_{cls}}\sum_i L_{cls}\,(p_i, p*_i) + \lambda\frac{1}{N_{reg}}\sum_i p*_i\, L_{reg}\,(t_i, t*_i) \tag{5}$$

$$L_{cls}(p_i, p_i^*) = -\log[p_i^* p_i + (1-p_i)(1-p_i^*)] \tag{6}$$

$$L_{reg}(t_i, t_i^*) = R(t_i - t_i^*) \tag{7}$$

$$R(x) = \begin{cases} 0.5x^2, |x| < 1 \\ |x| - 0.5, others \end{cases} \tag{8}$$

where *i* is the index of an anchor in a batch, p_i is the probability of anchor *i* being predicted as an object, the ground-truth label $p*_i$ is 1 if the anchor is positive, and 0 if the anchor is negative, t_i is a vector of the predicted bounding box coordinates, $t*_i$ is a vector of the actual bounding box coordinates, N_{cls} and N_{reg} are the normalization parameters, λ is the balancing parameter and R is the robust loss function.

This paper goes further to present an enhanced Faster R-CNN Model. The overall framework of the enhanced approach is shown in figure 2. Instead of using VGG-16 architecture [15] as the backbone layer, the MobileNet architecture [16] is adopted to extract high level features [16]. Thus, the proposed framework enhances both computation cost and inference time. In the region proposal network, Soft Non-Maximum Suppression algorithm (Soft-NMS) is used to solve the issue of detecting clustered objects as a single object, improving the region proposal operation. Finally, the classifier is built using the depthwise separable convolution structure found in MobileNet-v3 architecture. In the MobileNet architecture, the convolution process on the pre-processed image is divided into two steps: a 3 × 3 depthwise convolution and a 1 × 1 pointwise convolution at the pixel level. This approach effectively reduces both computational costs and the number of parameters involved. Depthwise convolution with one filter per input channel of an image is computed as:

$$G_{k,l,m} = \sum_{i,j} K_{i,j,m} \cdot F_{k+i-1,l+j-1,m} \tag{9}$$

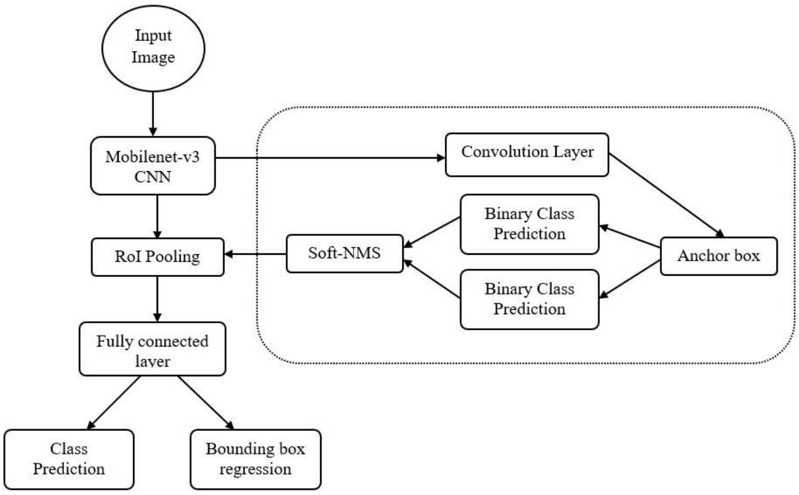


Fig.2. Enhanced faster r-cnn model architecture

where *K* is the depthwise convolutional kernel of size $D_K \times D_K \times M$, the *m_{th}* filter in *K* is applied to the m_{th} channel in feature map *F* to produce the m_{th} channel of the filtered output feature map *G*. Depthwise convolution has a computational cost of:

$$C_G = D_K . D_K . M . D_F . D_F \tag{10}$$

Where D_K is the spatial width and height of the square convolution kernel, D_F is the spatial width and height of a square input feature map and M is the number of input channels. The combination of depthwise convolution and 1 × 1 (pointwise) convolution is called depthwise separable convolution and it has a computational cost of:

$$C_{G,P} = D_K . D_K . M . D_K . D_K + M . N . D_F . D_F \tag{11}$$

Where N is the number of output channels and $C_{G,P}$ is the sum of the depthwise and 1 × 1 pointwise convolution. By expressing convolution as a two-step process of filtering and combining, a reduction in computation is achieved in equation 3.11.

$$\frac{D_K.D_K.M.D_K.D_K+M.N.D_F.D_F}{D_K.D_K.M.N.D_F.D_F}=\frac{1}{N}+\frac{1}{D_K^2} \tag{12}$$

The Region Proposal Network (RPN) initially creates a collection of anchor boxes based on the convolution feature map produced by the MobileNet architecture. Each anchor box is centered at the sliding window and is characterized by a specific scale and aspect ratio. Next, the RPN processes all the anchor boxes and produces two outputs. The first output is the objectiveness score, indicating the likelihood that an anchor represents an object, such as a cow, goat, or person. The second output is the bounding box regression, which fine-tunes the anchors to better align with the object. By utilizing the final proposal coordinates and their objectiveness scores, a well-constructed set of intrusion proposals is generated. Given that anchors often overlap, these proposals may also overlap the same object. For this research, a Soft Non-maximum Suppression (Soft-NMS) algorithm [17] is employed to address the problem of duplicate proposals. In many advanced object detection methods, including Faster R-CNN, Non-maximum Suppression (NMS) is utilized to eliminate duplicate proposals. The conventional NMS approach discards any additional proposal that shares more than a predefined threshold of overlap with the winning proposal. However, when dealing with clustered animals like cows and goats, the conventional NMS method may unintentionally discard valid proposals. With soft-NMS, the neighboring proposals of a winning proposal are not entirely eliminated. Instead, their suppression is determined by recalculated objectiveness scores based on the degree of overlap between these neighboring proposals and the winning proposal.

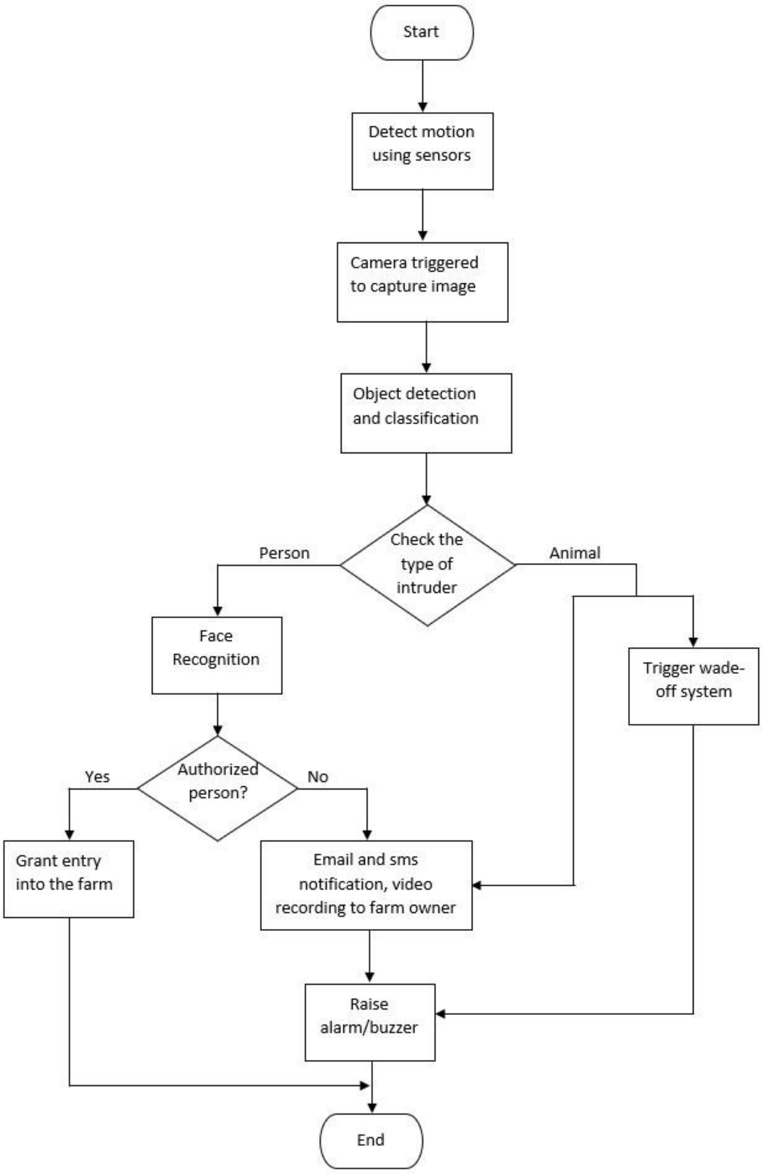

Start
Detect motion using sensors
Camera triggered to capture image
Object detection and classification
Check the type of intruder
Person
Animal
Face Recognition
Trigger wade-off system
Authorized person?
Yes
No
Grant entry into the farm
Email and sms notification, video recording to farm owner
Raise alarm/buzzer
End

Fig.3. IoT based animal and human intrusion detection model

Consider an initial set of proposals denoted as $P_{in} = \{p_1, p_2, p_3, \dots p_n\}$ where these proposals have been sorted based on their respective objectiveness scores. For any proposal p_i any other proposal that exhibits an overlap greater than a predefined threshold T with proposal p_i is referred to as a neighbour proposal of p_i. For this paper, the threshold for neighbour proposals T has been determined through cross-validation and set to 0.5. Let S_i represent the objectiveness score of p_i which is essentially the highest value within the classification score vector of p_i. Within a proposal set, the proposal with the highest objectiveness score is termed the winning proposal. Suppose p_i is the winning proposal and p_j is a neighbour proposal of p_i, the updated objectiveness score of p_j denoted by S_j^u is given as:

$$S_j^u = S_i\left(1 - O_{p_i,p_i}\right) \tag{13}$$

where O_{p_i,p_j} denotes the Intercession over Union (IoU) between proposal p_i and proposal p_j and is computed in equation 14.

$$O_{p_i,p_j} = \frac{area(p_i \cap p_j)}{area(p_i \cup p_j)} \tag{14}$$

The flow chart of the proposed IoT Based Animal and Person Intrusion Detection Model is presented in figure 3.

4. Results and Discussions

This section presents the implementation of the Internet of Things Based Human and Animal Intrusion Detection on a Farmland using object detection and face recognition techniques to prevent animals and persons intruding a farmland, and a safe defensive mechanism to scare away intruders. The tools used in development of the system consist of the software and hardware specifications. The hardware specifications are:

- Raspberry Pi 4
- Pi Camera Version 2 8MP
- Passive Infrared Sensor
- Google Colab Jupyter Notebook with 12 GB of GPU memory

The software specifications are:

- 64-bit Operation system, Microsoft Windows 10
- Google Earth Engine Python API
- Associated Python Libraries such as Open CV, PyTourch and face recognition library.

4.1. Dataset

Images of each class (cow, goat, person) were obtained online from Roboflow and combined to form the PECOGO dataset used in this research. The PECOGO dataset was firstly divided into training, validation and test sets with approximately 70:20:10 ratio. This was done to ensure that distinct images were used in the training and test sets to avoid over-fitting which might result from exposing the model to the test images. The data has a total of 3752 images with several samples of cow, goat and person. 2734 images are used for training, 627 images are used for validation and 391 images are used for testing.

4.2. Testing on the Farm

The experiment for testing the IoT based Farmland Intrusion Detection Model was setup in the cow and goat section of Federal University of Technology, Akure Teaching and Research farm. The setup includes Pi Camera, PIR sensor, Raspberry Pi4 and power supply. The arrangement of the prototype was arranged in the best possible way the animals could be captured. Figure 4 shows the setup of the prototype for experimentation. Figure 5 is a snippet of the result from the raspberry pi. Section (a) shows that when an unauthorized person/intruder is detected, the wade-off system is activated, a recording of the intrusion scene is taken, and notification is sent to the registered farm owner. Section (b) show that no action is taken when an authorized person is detected and captured by the camera.

The intrusion detection result is presented in three categories namely, one cow, goat or person in a picture frame, clustered cow, goat or person in a picture frame and cow, goat or person in a night picture frame. A confidence threshold of 0.7 is set which means that any confidence less than 0.7 will not be considered as a detection.

- One cow, goat or person in a picture frame: Cow was detected with confidence score of 0.97, goat was detected with confidence of 1.0 and an unauthorized person was detected with a confidence score of 0.94 as shown in figure 6.
- Clustered cow, goat or person in a picture frame: The purpose of testing clustered animals is to see how well the soft-NMS algorithm perform. From figure 7b, the model detected 5 out of 6 goats in the picture frame with confidence scores ranging from 1.0 to 0.85. In Figure 7a, the model detected 6 cows with confidence scores ranging from 0.96 to 0.70 in a heavily clustered picture frame. In figure 8, the model could detect an

unauthorized person with confidence score of 0.96 and 5 cows with confidence scores ranging from 0.99 to 0.70 in a heavily clustered picture frame.

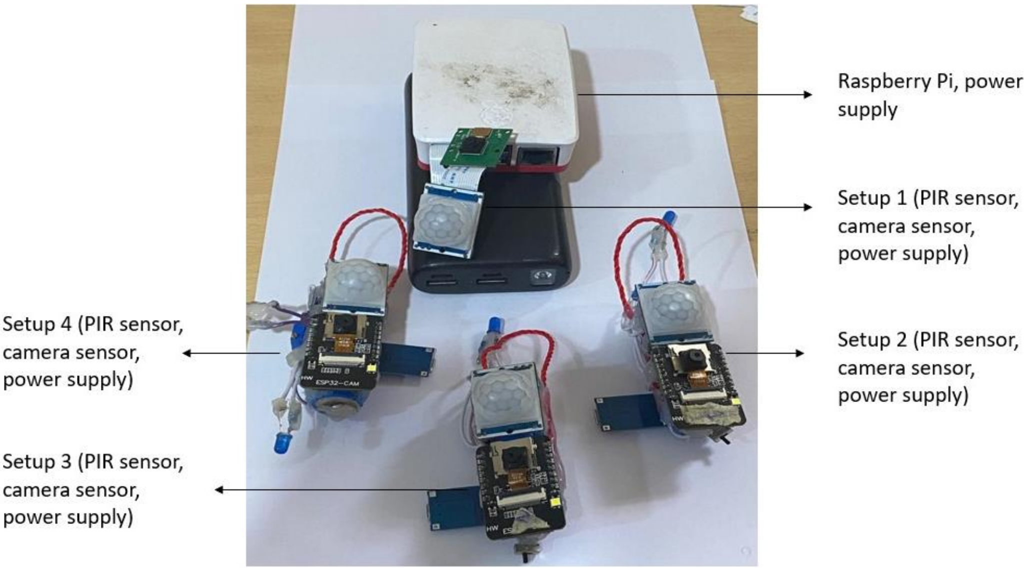
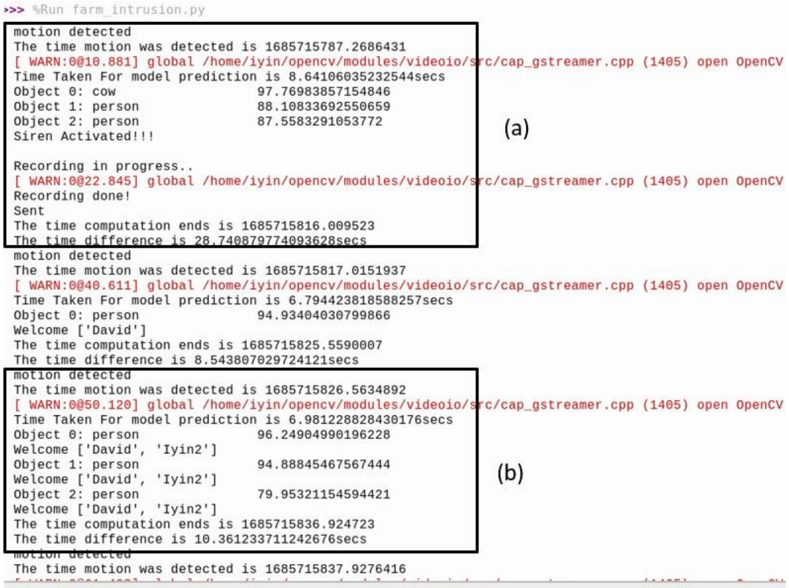

Raspberry Pi, power supply
Setup 1 (PIR sensor, camera sensor, power supply)
Setup 4 (PIR sensor, camera sensor, power supply)
Setup 2 (PIR sensor, camera sensor, power supply)
Setup 3 (PIR sensor, camera sensor, power supply)
ESP32-CAM
HW

Fig.4. Experimental setup



```
>>> %Run farm_intrusion.py
motion detected
The time motion was detected is 1685715787.2686431
[ WARN:0@10.881] global /home/iyin/opencv/modules/videoio/src/cap_gstreamer.cpp (1405) open OpenCV
Time Taken For model prediction is 8.64106035232544secs
Object 0: cow                  97.76983857154846
Object 1: person               88.10833692550659
Object 2: person               87.5583291053772
Siren Activated!!!

Recording in progress..
[ WARN:0@22.845] global /home/iyin/opencv/modules/videoio/src/cap_gstreamer.cpp (1405) open OpenCV
Recording done!
Sent
The time computation ends is 1685715816.009523
The time difference is 28.740879774093628secs
motion detected
The time motion was detected is 1685715817.0151937
[ WARN:0@40.611] global /home/iyin/opencv/modules/videoio/src/cap_gstreamer.cpp (1405) open OpenCV
Time Taken For model prediction is 6.794423818588257secs
Object 0: person               94.93404030799866
Welcome ['David']
The time computation ends is 1685715825.5590007
The time difference is 8.543807029724121secs
motion detected
The time motion was detected is 1685715826.5634892
[ WARN:0@50.120] global /home/iyin/opencv/modules/videoio/src/cap_gstreamer.cpp (1405) open OpenCV
Time Taken For model prediction is 6.981228828430176secs
Object 0: person               96.24904990196228
Welcome ['David', 'Iyin2']
Object 1: person               94.88845467567444
Welcome ['David', 'Iyin2']
Object 2: person               79.95321154594421
Welcome ['David', 'Iyin2']
The time computation ends is 1685715836.924723
The time difference is 10.361233711242676secs
motion detected
The time motion was detected is 1685715837.9276416
```

Fig.5. Snippet of result of testing from the raspberry Pi4

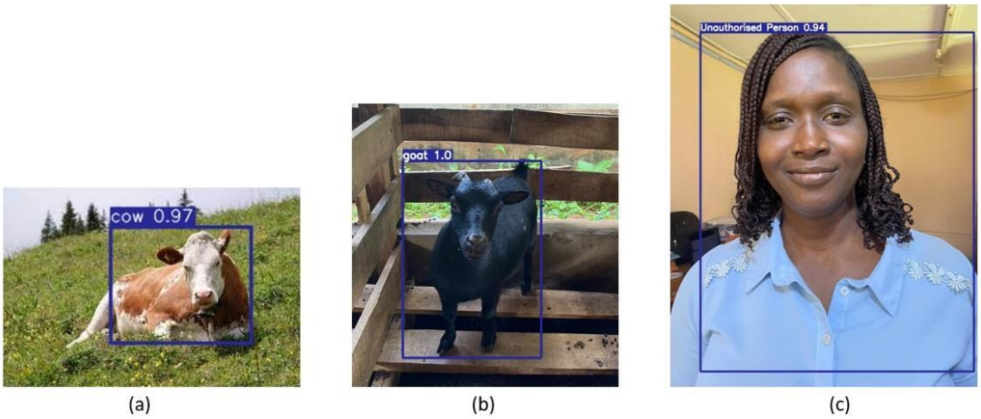


Fig.6. Detection results of cow, goat and person

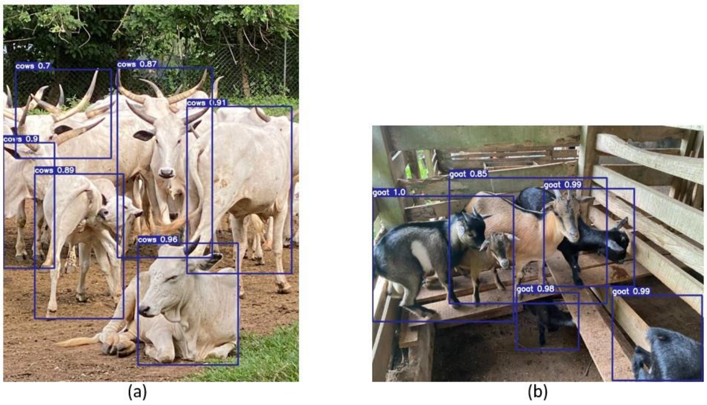


Fig.7. Detection results of clustered cow and clustered goat

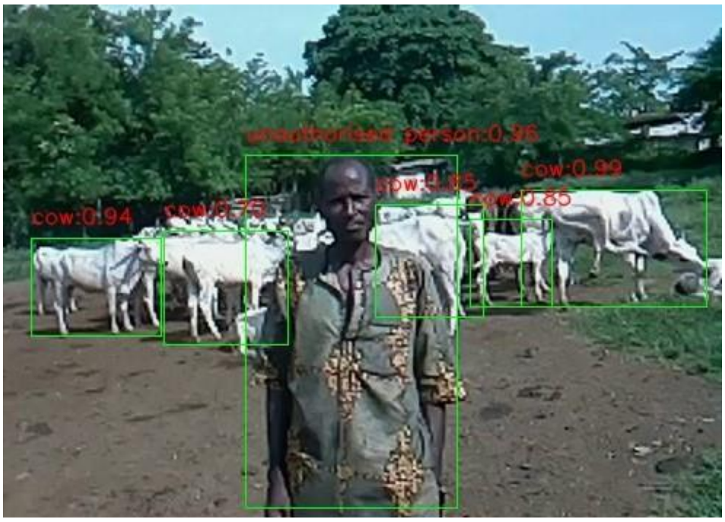


Fig.8. Detection results of clustered cow and unauthorized person

- Cow, goat or person in a night picture frame: The purpose of testing in the night is to see how well the developed model works at night. From figure 9a, cows were detected with high confidence scores ranging from 0.99 to 0.71 in a night picture frame. Also, in figure 9b, goat was detected with high confidence scores of 1.0 and 0.99 in a night picture frame. Therefore, the accuracy of the developed model detecting intrusion at night is derived by averaging the highest confidence score of each class. The highest confidence score for cow is 0.99 and the highest confidence score for goat is 1.0. Therefore, the average is $\frac{0.99+1}{2} = 0.995$ or 99.5%.

4.3. Alert and Notification

If-This-Then-That (IFTTT) is the IoT cloud platform that the developed model connects to send notifications of intrusions on the farm to the registered farm owner. The farmer receives notification of intrusion within 18 to 25 seconds on the intrusion. Figures 10 show the samples of the email notification. The email tells the date and time the intrusion occurred, the nature of the intrusion whether it is a person, cow, goat or a combination of either, a link to the 15 seconds video of intrusion scene.

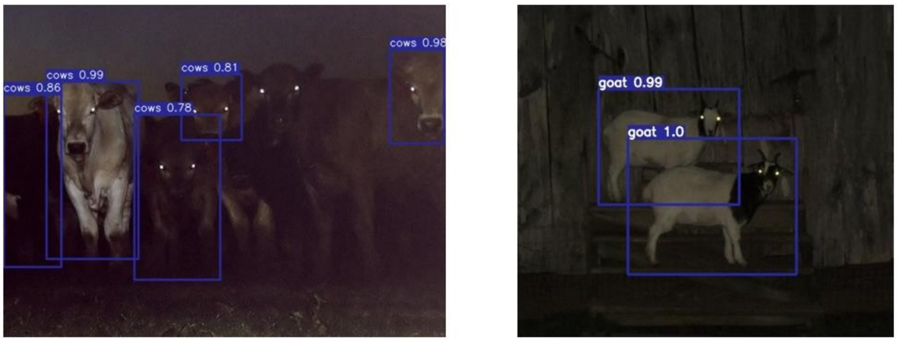
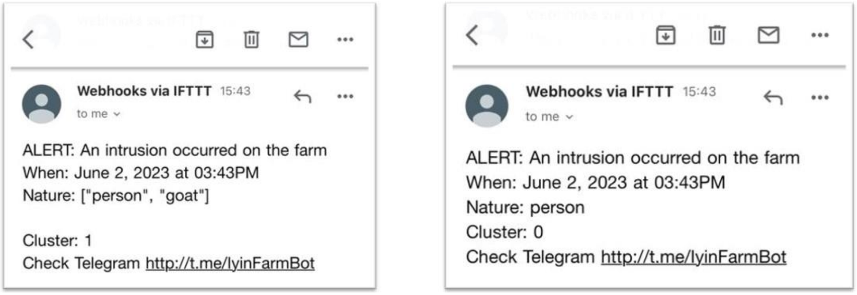


Fig.9. Detection results for dark images



Webhooks via IFTTT 15:43
to me

ALERT: An intrusion occurred on the farm
When: June 2, 2023 at 03:43PM
Nature: ["person", "goat"]

Cluster: 1
Check Telegram http://t.me/lyinFarmBot

Webhooks via IFTTT 15:43
to me

ALERT: An intrusion occurred on the farm
When: June 2, 2023 at 03:43PM
Nature: person
Cluster: 0
Check Telegram http://t.me/lyinFarmBot

Fig.10. Screenshots of email notification

5. Performance Evaluation

The developed model is evaluated based on some standard metrics. The model evaluation metrics are used to assess goodness of fit between the model and the data and to compare different models' prediction accuracies. The evaluation metrics considered to determine the performances of the model are: Confusion matrices, accuracy, precision, recall, F1 Score and mean average precision. They are for model evaluation for classification task. They are presented as follows.

- Confusion Matrix: This is a table that describes and summarizes the performance of a classification algorithm on the test dataset. A confusion matrix describes the number of correct and incorrect predictions made by the classification model compared to the actual target values. To create a confusion matrix, four attributes are needed.
- Accuracy: This is the measurement of the closeness of the predicted output to the target output. It is the ratio of number of correct predictions to the total number of input samples.

$$Accuracy = \frac{TruePositives+TrueNegatives}{Total\ Samples} = \frac{1094}{1183} = 0.925\ or\ 92.5\%$$

- Precision: This is the ratio between the true positive and the total number of class predictions (equivalently the sum of true positive and false positive) made by the model.

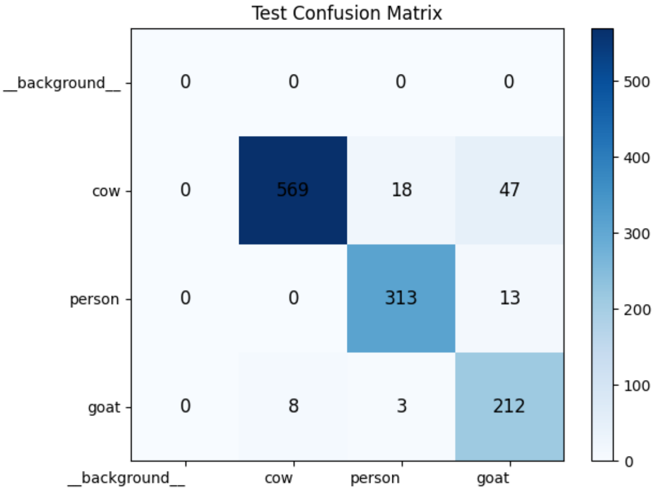
$$Precision = \frac{TP}{TP+FP} = \frac{0.919+0.927+0.903}{3} = 0.916$$

- Recall: This is the ratio between the true positives and the total number of ground truth classes (equivalently the sum of true positive and false negative) made by the model.

$$Recall = \frac{TP}{TP+FN} = \frac{0.930+0.935+0.974}{3} = 0.910$$

- F1-Score: The F1 Score is the Harmonic Mean between precision and recall. F1 considers both precision and recall rate and gives a more balanced view of the performance of the classifier.

$$F1\ Score = 2 \times \frac{\text{Precision}\times\text{recall}}{Precision+\ recall} = 2 \times \frac{0.916\times0.910}{0.916+0.910} = 0.913$$



	__background__	cow	person	goat
__background__	0	0	0	0
cow	0	569	18	47
person	0	0	313	13
goat	0	8	3	212

Fig.11. Confusion matrix for the developed model

Table 1. Results of the developed model

Class	Accuracy	Precision	Recall	F1-Score
Cow	92.5%	0.986	0.897	0.939
Person		0.937	0.960	0.948
Goat		0.779	0.951	0.856
Averaging	**92.5%**	**0.901**	**0.936**	**0.918**

Table 2 shows the performance of Enhanced Faster R-CNN Model compared to other Faster R-CNN Models during testing using detection speed and earlier stated metrics while table 3 shows the comparison of the developed system with existing systems using metrics stated above.

Table 2. Performance of faster r-cnn models

Models	Accuracy	Precision	Recall	F1 Score	mAP	Detection Speed/sec
Faster R-CNN + VGG16	73.6%	0.762	0.812	0.738	0.258	2.04
Faster R-CNN + ResNet50	90.8%	0.894	0.768	0.820	0.625	2.07
Faster R-CNN + EfficientNet	84.6%	0.832	0.730	0.771	0.242	2.28
Faster -RCNN + AlexNet	75.5%	0.775	0.807	0.742	0.201	1.94
Faster R-CNN + MobileNetV3 (this paper)	**92.5%**	**0.901**	**0.936**	**0.918**	**0.562**	**1.44**

Table 3. Comparison of the developed model with existing works

Author and Year	Technique Used	Accuracy
Vidhya *et al.* (2019)	Traditional CNN	90%
Paramasivam *et al.* (2020)	Traditional CNN	81%
Ravoor *et al.* (2021)	MobileNetv2-SSD	87.34%
Ravoor *et al.* (2021)	Tiny-YOLO	86.67%
This research work (2023)	**Faster R-CNN – MobileNetv3**	**92.50%**

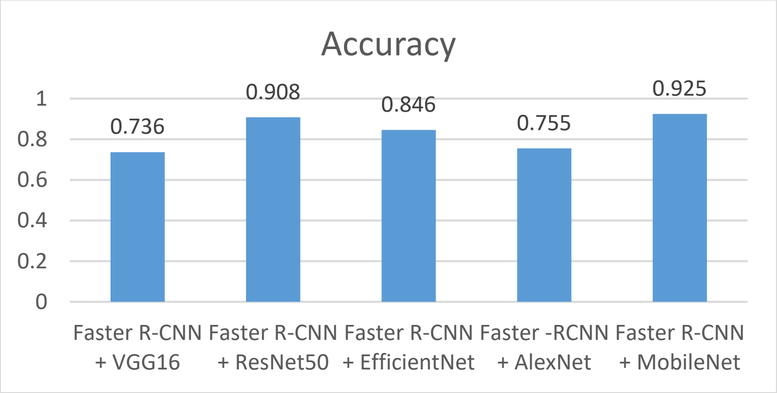


Fig.12. Results of faster r-cnn models during testing – accuracy

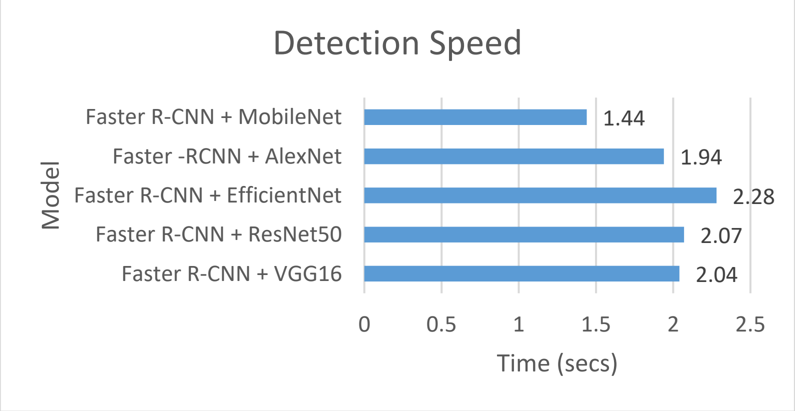


Fig.13. Results of faster r-cnn models during testing – detection speed

6. Conclusions

This research has established an efficient farmland intrusion detection model using IoT and improved Faster R-CNN algorithm to prevent animals and unauthorized person intrusion, notify the farm owner about intrusion and a safe defensive mechanism to chase intruders away. Once the PIR sensor senses motion, it triggers the camera to take a picture of the scene via the raspberry Pi which is the microcontroller. The image is received by the raspberry pi for object detection and face recognition in the case of a person. The raspberry pi then communicates with the IoT cloud platform to send details of intrusion to the farm owner through text message and email notification. The raspberry pi also turns on the wade off system to divert an intruding animal away. The detection accuracy of the developed model is 92.5% which is an improvement of previous related works. This research also established that the enhanced model has the shortest detection speed of 1.44 seconds compared to other models. For future research, we recommend that more animals can be detected to improve the detection capacity of the system.

References

[1] Ajayi O. and Olaifa O. “Detecting Intrusion in Large Farmlands and Plantations in Nigeria Using Virtual Fences”. Retrieved from https://ininet.org/detecting-intrusion-in-large-farm-lands-and-plantations-in-nig.html. 2017.

[2] Shaji A.P. “Raspberry Pi based real time monitoring of Agricultural and Irrigation using IoT”. International Journal of Engineering Development and Research, Vol.6 No.2, pp. 652-656, 2018

[3] Angadi S. and Katagall R. “Agrivigilance: A Security System for Intrusion Detection in Agriculture Using Raspberry Pi and Opencv”. International Journal of Scientific & Technology Research, Vol.8 No.11, pp.1261-1267, 2019.

[4] Mythili R., Kumari M., Tripathi A. and Pal N. “IoT Based Smart Farm Monitoring System”. International Journal of Recent Technology and Engineering (IJRTE), Vol.8 No.4, pp. 2277-3878 ,2019.

[5] Santhiya S., Dhamodharan Y., Kavi Priya N. E., Santhosh C.S. and Surekha M. “A Smart Farmland Using Raspberry Pi Crop Prevention and Animal Intrusion Detection System”. International Research Journal of Engineering and Technology (IRJET), Vol.5, No.3, pp.2395-0056, 2018

[6] Iyapo K.O., Fasunla O.M., Egbuwalo S.A., Akinbobola A.J. and Oni O.T. “Design and Implementation of Motion Detection Alarm and Security System”. International Journal of Engineering and Advanced Technology Studies, Vol.6, No.1, pp. 26-38, 2018

[7] Kumar M., Kaul S., Singh V.K. and Bohara V.A. “iDART-Intruder Detection and Alert in Real Time”. Wirocomm Research Group, Indraprastha Institute of Information Technology, New Delhi, 2015

[8] Roy S.K., Roy A., Misra S., Raghuwanshi N.S. and Obaidat M. S. “AID: A Prototype for Agricultural Intrusion Detection Using Wireless Sensor Network”. Communications Software, Services and Multimedia Applications Symposium IEEE, pp 7059-7064, 2015

[9] Ravoor P.C, Sudarshan T.S. and Rangarajan K. “Digital Borders: Design of an Animal Intrusion Detection System Based on Deep Learning”. International Conference on Computer Vision and Image Processing, pp.186-200, 2021

[10] Shetty H., Sing H. and Shaikh F. “Animal Detection using Deep Learning”. International Journal of Engineering Science and Computing (IJESC), Vol.11, pp 28059-28061, 2021.

[11] Schindler F. and Steinhage V. Identification of Animals and Recognition of their Actions in Wildlife Videos Using Deep Learning Techniques”. International Journal on Computational Ecology and Ecological Data Science., Vol.61, No.35, 2021

[12] He K., Gkioxari G., Dollar P. and Girshick R. “Mask R-CNN”. The IEEE International Conference on Computer Vision (ICCV), 2017

[13] Paramasivam K., Krishnaveni S., Sowndarya S. and Kavipriya E. “Convolutional Neural Network Based Animal Detection Algorithm for Partial Image”. Aegaeum Journal, Vol.8, No.6, pp. 1461-1469, 2020

[14] Sayagavi A.V., T Sudarshan T.S. and P.C. Ravoor. “Deep Learning Methods for Animal Recognition and Tracking to Detect Intrusions”. Information and Communication Technology for Intelligent Systems, Vol.196, pp.617-626, 2021

[15] Simonyan K, Zisserman A. “Very Deep Convolutional Networks for Large-Scale Image Recognition”. arXiv Cornell University. Retrieved online from https://arxiv.org/abs/1409.1556, 2014.

[16] Howard A. G., Zhu M. and Chen B. “MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications”. Retrieved online from https://arxiv.org/pdf/1704.04861.pdf., 2017.

[17] Bodla N., Singh B., Chellappa R. and Davis R. “Soft-NMS -- Improving Object Detection with One Line of Code”. arXiv Cornell University. Retrieved from https://arxiv.org/abs/1704.04503v2, 2017.

Authors’ Profiles

Iyinoluwa M. Oyelade received her Masters and Ph.D degrees in computer science from the Federal University of Technology, Akure in 2018 and 2023 respectively. Since 2016, she worked as a professional and then crossed to become a lecturer in the Department of Information Technology, Federal University of Technology, Akure in 2022. Her research interests are computer vision, Internet of Thing, Deep Learning and Machine learning.

Olutayo K. Boyinbode is a professor of computer science at the Department of Information Technology, Federal University of Technology, Akure. Her research areas are software intelligent systems, artificial intelligence, human-computer interaction, and cloud computing.

Olumide S. Adewale is a professor of computer science at the Department of Computer Science, Federal University of Technology, Akure. His research areas are e-learning, computer architecture, computer communications, parallel computing.

Emmanuel O. Ibam is a professional teacher, programmer, and team player with passion for research and excellence. Every classroom encounter rekindles my passion for the teaching profession and spurs me to make incisive inquiries on how to awaken students' interest and improve the teaching and learning process. A Senior Lecturer in the Department of Information Systems, Federal University of Technology, Akure. His research areas include business informatics.

How to cite this paper: Iyinoluwa M. Oyelade, Olutayo K. Boyinbode, Olumide S. Adewale, Emmanuel O. Ibam, "Farmland Intrusion Detection using Internet of Things and Computer Vision Techniques", International Journal of Information Technology and Computer Science(IJITCS), Vol.16, No.2, pp.32-44, 2024. DOI:10.5815/ijitcs.2024.02.03