Grenze International Journal of Engineering and Technology, January Issue

Deep Learning-based Intrusion Detection in Agricultural Fields using Cameras

Balaji V[1], Harshavardhan V[2], Kanchana R[3], Mirnalinee T T[4], Madav Naveen Kumar M[5] and Thanis Annal Jenifer K[6]
[1-6]Department of Computer Science and Engineering, Sri Sivasubramaniya Nadar College of Engineering, Chennai, India
Email: {balaji2220025, harshavardhan2220003, rkanch, mirnalineett, madavnaveenkumar2220032, thanis2220059}@ssn.edu.in

***Abstract*— The agricultural sector in India faces persistent challenges stemming from crop damage inflicted by intruding animals and humans, necessitating innovative solutions to safeguard farmers livelihoods and bolster food security. This work proposes a novel approach centered on the development and deployment of advanced intruder detection systems leveraging convolutional neural network (CNN) models, including Residual Neural Network (ResNet) and EfficientNetB0, tailored for real-time object detection within agricultural fields. Integrated with Raspberry Pi devices and web cameras, these systems are designed to swiftly identify intruders and relay alerts to farmers, enabling prompt intervention to mitigate crop losses. Furthermore, a robust communication framework is established to facilitate seamless transmission of alerts to user's mobile applications, while MongoDB serves as the backbone for secure storage of intrusion event data in the cloud, ensuring data integrity and accessibility for comprehensive analysis and informed decision-making. This interdisciplinary endeavor aims to enhance field security measures, foster resilience in the agricultural landscape, and contribute to sustainable agricultural practices in India.**

***Index Terms*—Animal Intrusion Detection System, Convolutional Neural Network (CNN), Deep Learning, EfficientNetB0 and Residual Neural Network (ResNet).**

I. INTRODUCTION

Agriculture remains a cornerstone of the Indian economy, providing sustenance to millions while meeting the demands of a burgeoning population. However, the sector faces persistent threats from intruders, both natural and human, which continually undermine farmers' efforts and livelihoods. Traditional deterrents like scarecrows have proven inadequate, particularly as agricultural operations expand across vast expanses of land. In response, there is an increasing call for innovative solutions leveraging cutting-edge technology to address this pressing challenge. Enterprises within the agricultural domain are increasingly exploring modern advancements to fortify their fields against intruders.

Animal intrusion detection systems (AIDS) are crucial for protecting agricultural lands and managing wildlife encroachment in farmlands. These systems leverage deep learning techniques to automatically identify and prevent potential damage caused by wild animals. Deep learning models have proven highly effective in this domain due to their ability to analyze complex patterns in visual data, detect anomalies, and distinguish between animal species, thereby improving detection accuracy and response times.

Grenze ID: 01.GIJET.11.1.331

Convolutional Neural Networks (CNNs) are widely utilized for image-based animal detection due to their proficiency in visual pattern recognition, as demonstrated by Xue et al. (2017) [11]. CNNs excel in extracting features from surveillance images, allowing for reliable classification and detection of various species based on visual cues. Furthermore, Recurrent Neural Networks (RNNs) are sometimes used to monitor time-series data, which can help track animal movements and predict intrusion events over time [9].
In addition to CNNs, hybrid frameworks, which combine multiple deep learning methods, have been developed to enhance detection efficiency and accuracy. Kethineni and Pradeepini proposed a hybrid deep learning framework that integrates various models to improve intrusion detection in IoT-enabled smart farming environments [1]. Another promising approach is the Federated Learning-based Intrusion Detection System (FELIDS), which allows models to be trained across decentralized devices without data sharing. This technique enhances privacy and data security while enabling robust real-time intrusion detection in agriculture, as explored by Friha et al [4].
The fusion of deep learning and IoT has also led to innovative applications, such as the use of Digital Twin technology in animal intrusion systems. Teschner et al proposed a Digital Twin-based model that simulates agricultural environments, offering a virtual testing platform to monitor and assess intrusion detection systems, enabling proactive responses to potential threats [3]. In another IoT-enabled approach, Panda et al. incorporated advanced deep learning algorithms into a model specifically tailored for animal intrusion detection in agriculture, demonstrating the effectiveness of these integrated systems in providing reliable, real-time detection [5].
These advancements highlight the transformative role of deep learning techniques, particularly CNNs and hybrid deep learning frameworks, in enhancing the robustness, accuracy, and operational efficiency of animal intrusion detection systems in agricultural settings. The integration of IoT further optimizes these systems, allowing continuous monitoring and quick responses to wildlife threats, ultimately supporting sustainable farming practices.

II. Literature Review

Agriculture, a vital component of our society, faces numerous challenges, including environmental factors and human-animal intrusions. As technological advancements emerge, innovative solutions become essential for effectively addressing these issues. This section examines the integration of advanced technologies such as deep learning, the Internet of Things (IoT), and edge computing in developing a state-of-the-art agricultural security system, analyzing the benefits and drawbacks of various intrusion detection and threat mitigation approaches.
The authors of [1] emphasize the importance of a hybrid deep learning framework combining DNN, CNN, and RNN models for intrusion detection in smart farming, highlighting its potential for enhanced accuracy, particularly in identifying Distributed Denial of Service (DDoS) attacks. In [2], the focus shifts to network topologies within IoT frameworks, particularly the Message Queuing Telemetry Transport (MQTT) protocol for agricultural intrusion detection. In the work of [3], advocate for utilizing digital twin technology to enhance drone-based protection mechanisms in agriculture is proposed. They illustrate how digital twins can synthesize real-time drone data with historical information, enabling farmers to make informed decisions about potential threats. Focusing on data privacy and scalability, the authors of [4] propose FELIDS, a federated learning-based intrusion detection system designed for agricultural IoT environments. However, they acknowledge challenges such as computational demands and non-IID data distribution.
Addressing the challenges posed by wild animal intrusions, the authors of [5] present an IoT-based system for real-time monitoring and response. They highlight the advantages of IoT infrastructure in detecting wild animal intrusions rapidly, although they also note concerns regarding false positives and the logistical difficulties of maintaining IoT sensors in remote locations. In [6], the authors have proposed a low-cost, customizable Arduino-based intrusion detection system for crop protection, emphasizing the accessibility of Arduino boards for farmers with limited resources. In the study of [7], the authors have proposed a deep learning system for wild animal intrusion detection using Convolutional Neural Networks (CNNs). They emphasize the high accuracy and adaptability of these models for classifying wild animals from camera trap data. With affordability and customization in mind, the authors of [8] introduce a Raspberry Pi-based smart farmland system for crop protection and animal intrusion detection, but there are limitations in processing power and potential false positives.
The authors of [9] explore Support Vector Machines (SVMs) with Gabor features for detecting animal intrusions in agricultural fields, however there are challenges such as computational complexity and the need for expertise in feature extraction. In [10], the authors examine using optical cameras with PIR sensor arrays for outdoor intrusion detection. The authors of [11] and [13] focus on animal intrusion detection through CNNs, highlighting

their ability to provide continuous monitoring without manual supervision. But there exists challenges as data acquisition, computational demands, and ensuring model interpretability. In [12], the authors analyze IoT-based intrusion detection systems using PIR sensors, detailing their advantages such as cost-effectiveness and scalability. The authors of [14] introduce an improved image detection system for identifying elephant intrusions along forest borders, suggesting enhancements in image retrieval techniques, but its effectiveness is dependent on the quality of the image dataset.

Existing research on agricultural security investigates methods such as hybrid deep learning, IoT systems, and cost-effective hardware solutions like Arduino and Raspberry Pi. These approaches offer notable advantages, including improved accuracy, scalability, and cost-efficiency, while also encountering challenges such as computational complexity, data privacy concerns, and the risk of false positives. Building on the insights from these studies, the proposed system integrates the strengths of these methods while addressing their limitations. By utilizing IoT infrastructure, specifically Raspberry Pi, the system facilitates real-time monitoring of agricultural areas and enables swift responses to wild animal intrusions, thereby optimizing agricultural security through a robust and adaptable approach.

III. PROPOSED SYSTEM

The proposed system represents a significant advancement in agricultural security, seamlessly integrating state-of-the-art deep learning algorithms with real-world image data for unparalleled intrusion detection capabilities. By leveraging cutting-edge technologies, it establishes a new benchmark for efficiency and reliability in agriculture. The System Architecture is illustrated in Figure 1 as follows. The dataset selected is an animal image dataset with 90 different categories of animals organized into separate folders for training and testing data. Prior to training, both dataset images and real-world captures undergo preprocessing and are fed into deep learning algorithms such as CNN, ResNet, and EfficientNetB0. These algorithms are trained using the training data, following which the model's performance is evaluated using the test data. Upon completion of training, the performance of each deep learning model is evaluated, and the best model (EfficientNetB0) is deployed and integrated into Raspberry Pi.

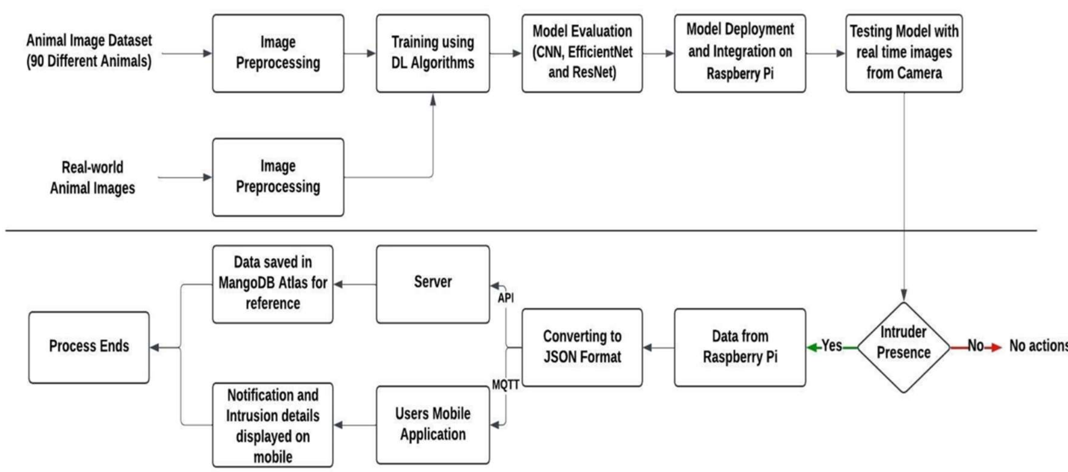

Fig 1. Workflow of the proposed architecture

The model is then tested on real-time images, i.e., the camera in the field. Its primary task is to accurately classify the presence of intruders while also identifying the position of the animals within the image. In the event of an intrusion, the given data is first converted to JSON format. Using an API, the details are sent to the server, and then all pertinent details are logged into the MongoDB Atlas cloud Database. In the case of a mobile application, a notification and message are promptly dispatched to the owner via a dedicated application with the use of the MQTT protocol. If the detected intruder poses no threat, no further action is taken. The various functional modules of the proposed system are as follows:

A. Preprocessing

The preprocessing steps encompass resizing images to conform to standardized dimensions, normalization procedures to enhance data uniformity, and data augmentation techniques aimed at enriching the training set.

B. Deep learning Model Development and Deployment

The module is dedicated to the development and optimization of models tailored for real-time object detection, with a specific focus on identifying intruders in agricultural fields. Central to this endeavor are the creation and refinement of Convolutional Neural Network (CNN), EfficientNetB0, and ResNet models. The CNN architecture is custom-designed with eight layers, beginning with two convolutional layers, followed by a max-pooling layer to capture spatial features and reduce dimensionality. This structure is repeated once more, after which the output is flattened and passed through a dense layer for classification. The model is trained using the Adam optimizer and categorical cross-entropy loss function. While the CNN model effectively learns basic features, it struggles with capturing more complex patterns, leading to certain limitations in performance.

In contrast, EfficientNetB0, a pre-trained model sourced from TensorFlow Hub, utilizes 54 layers and employs efficient scaling techniques to enhance performance while minimizing the number of parameters. Fine-tuning is performed by adding a dense classification layer atop the pre-trained feature extractor. This model is further optimized through transfer learning, rendering it highly suitable for real-time deployment owing to its high performance. Similarly, ResNet, a pre-trained model featuring 45 layers and residual connections, is employed to address the vanishing gradient problem. The fine-tuning process involves adding a classification layer and training only this newly added layer while retaining the pre-trained weights. Despite being slightly shallower than EfficientNetB0, ResNet is a viable option for real-time object detection, particularly within the context of agricultural applications. The selection of EfficientNetB0 for deployment on a Raspberry Pi underscores its superior accuracy and its suitability for real-time applications.

C. Model Deployment and Integration on Raspberry Pi

This module presents a comprehensive methodology for integrating a Raspberry Pi with web cameras to enable real-time animal intrusion detection in agricultural fields. The setup process begins with the Raspberry Pi, involving the acquisition of necessary hardware components, installation of an operating system (such as Raspbian), establishment of network connectivity, and configuration of fundamental settings, including IP address assignment. The integration of web cameras entails selecting compatible devices and ensuring their proper recognition and configuration within the Raspberry Pi environment. After the hardware setup, the required software libraries are installed for image processing and deep learning tasks. These include OpenCV for image manipulation and TensorFlow with TensorFlow Hub for deep learning functionalities.

Additionally, a Python environment is configured, and the software is prepared to interface with the connected web cameras. The deep learning model deployed for this application is an EfficientNetB0 model, pre-trained for image classification. The model is loaded from a pre-trained state stored in a file, and custom objects such as KerasLayer are defined to facilitate model loading through TensorFlow Hub. Frames captured by web cameras are processed using the deployed model to detect harmful animals in real-time.

From the functionality perspective, the script subscribes to MQTT messages on the "Animal-NS" topic, receiving notifications about animal sightings. Upon receiving a message, the script updates a configuration file with the received data and sends push notifications via Firebase Cloud Messaging (FCM) to alert users. Continuous video streaming from the web cameras is handled through a dedicated function that captures frames, processes them for animal detection, and displays the results. Notifications and API calls are triggered upon detecting harmful animals, ensuring that data is logged appropriately. For user interaction, a Flask-based web application streams video from the web cameras, allowing users to monitor the agricultural field in real time.

D. Communication and Alerting Module with Cloud Storage Integration

This module focuses on ensuring secure communication between the Raspberry Pi and the user's mobile application, developed using React Native. Its primary objective is to facilitate the transmission of intrusion alerts from the Raspberry Pi to the user's mobile device, enabling real-time notifications and providing access to detailed intrusion information. Additionally, it includes the setup of a data storage mechanism utilizing MongoDB to store all intrusion event data in the cloud. This stored data serves as a resource for future reference and analysis, enhancing the overall security framework.

The system employs MQTT communication for message exchange between devices, Firebase Cloud Messaging (FCM) for push notifications, and MongoDB Atlas for cloud storage. MQTT communication is established using the MQTT client library, which connects to an MQTT broker (broker.hivemq.com). The script subscribes to the MQTT topic "Animal-NS" to receive messages regarding animal sightings. Upon receiving a message, the callback function is triggered. Relevant data, such as the device's IP address, is extracted from the message and used to construct a push notification. Firebase Cloud Messaging (FCM) is utilized to send push notifications to users about animal sightings. The script sends a notification message to the FCM server, specifying the title and body of the notification. The FCM server is responsible for delivering the notification to the target device, identified by its unique token.

Integration with MongoDB Atlas enables cloud storage of data related to animal sightings. When a harmful animal is detected, pertinent information, such as the date, time, GPS coordinates, harmful animal species, and device IP address, is collected. This data is formatted into a JSON object and sent via an HTTP POST request to an API endpoint hosted on MongoDB Atlas. The API endpoint processes and stores the received data in the MongoDB Atlas database, ensuring persistent storage and accessibility. The Communication and Alerting Module with Cloud Storage Integration provides a comprehensive solution for real-time monitoring and alerting in agricultural fields, leveraging MQTT communication, Firebase Cloud Messaging, and MongoDB Atlas for seamless communication, notification delivery, and data storage.

IV. Experimental Results

The assessment of Deep Learning models commences with their evaluation on real-time data to discern the optimal performer for deployment onto the Raspberry Pi platform. Below delineates the individual model's intrusion detection capabilities. Notably, EfficientNetB0 demonstrates superior performance relative to its counterparts, thus warranting its integration into the Raspberry Pi for intrusion detection purposes. Figures 2, 3 and 4 show the sample prediction results. Figures 5 and 6 represent the detection of the intrusion of harmless and harmful animals. The accuracy obtained using the CNN, ResNet and EfficientNet models are 52%, 94.3% and 96.2% respectively.

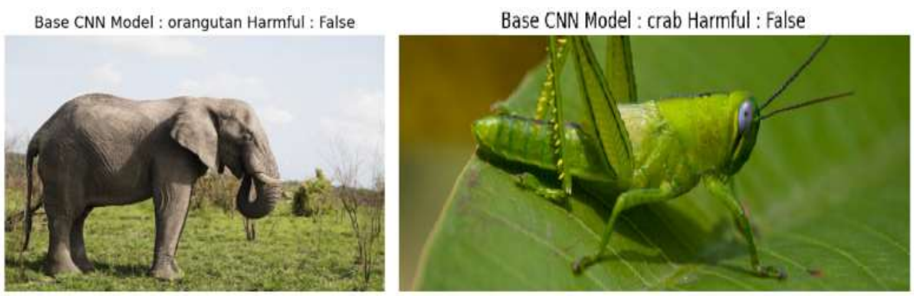

Fig 2. Prediction results using CNN

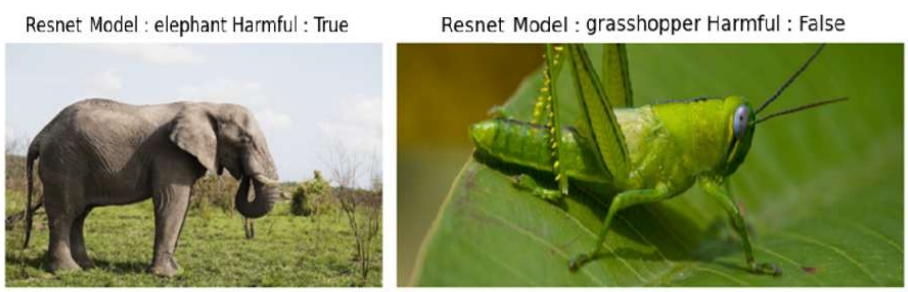

Fig 3. Prediction results using ResNet

Fig 4. Prediction results using EfficientNet

The EfficientNetB0 is now integrated with Raspberry Pi for testing images in real-time. Initially, essential libraries for image processing, deep learning, and optimization are imported. Real-time frames are captured from a webcam for intrusion detection purposes. Each frame undergoes processing using the loaded model to predict the animal present, annotating the frame with information about the predicted animal's potential harm based on a predefined list. The images tested with the model on Raspberry Pi are displayed below.
When a frame is determined as harmful, a quick detail of it is sent to the user's mobile application. Also, the Intrusion Details are saved in MongoDB Atlas for reference. This iterative process of capturing frames, making predictions, and displaying results continues until the user opts to quit by pressing a specific key. The animals that cause harm to the field are considered intruders according to our model. After identifying harmful animals, notifications, along with intrusion details, are dispatched to users' mobile applications and stored in MongoDB Atlas for future reference.

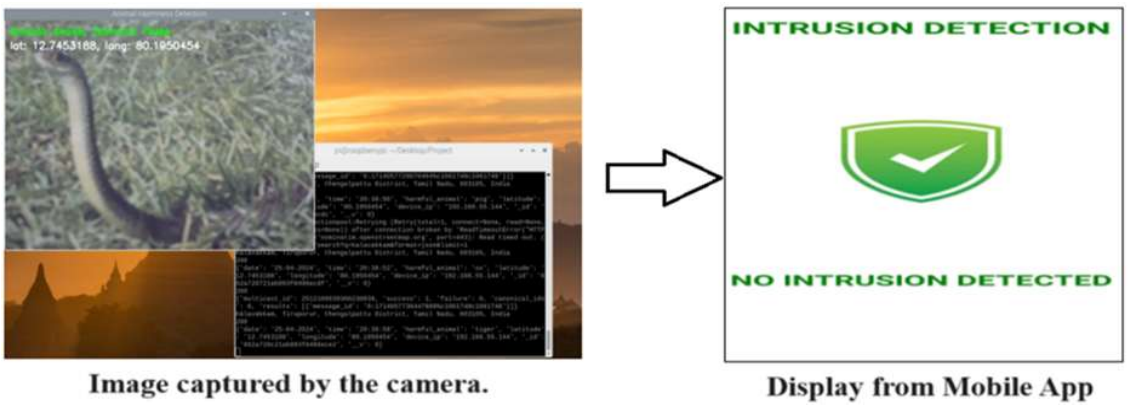

Fig 5. Detection of harmless animals using Raspberry Pi

Fig 6. Detection of harmful animals using Raspberry Pi

V. CONCLUSION

The proposed deep learning-based intrusion detection system offers a transformative solution for safeguarding agricultural fields against intrusions. By integrating CNN models such as ResNet and EfficientNetB0 with Raspberry Pi and real-time monitoring, the system ensures rapid detection and response to threats, minimizing potential crop damage. The use of a robust communication framework and secure cloud storage further strengthens the system's reliability and timely intervention.
This approach not only addresses the immediate needs of farmers but also contributes to the long-term sustainability and resilience of agricultural practices, making it a valuable tool in enhancing food security in India. Future work will focus on integrating GPS services into the mobile application to enhance user navigation with real-time location tracking and optimized route suggestions.

REFERENCES

[1] Kethineni, K. and Pradeepini, G. (2024) ‘Intrusion detection in internet of things-based smart farming using hybrid deep learning framework’, Cluster Computing, 27(2), pp.1719-1732.

[2] Chakravarthy, R. (2022) ‘An experimental study of IoT-Based topologies on MQTT protocol for agriculture intrusion detection’, Measurement: Sensors, 24, p.100470.

[3] Teschner, G., Hajdu, C., Holl´ osi, J., Boros, N., Kovacs, A. and Ballagi, A. (2022) ‘Digital twin of drone-based protection of agricultural areas’, In 2022 IEEE 1st International Conference on Internet of Digital Reality (IoD) (pp. 000099-000104). IEEE.

[4] Friha, O., Ferrag, M.A., Shu, L., Maglaras, L., Choo, K.K.R. and Nafaa, M. (2022) ‘FELIDS: Federated learning-based intrusion detection system for agricultural Internet of Things’, Journal of Parallel and Distributed Computing, 165, pp.17-31.

[5] Panda, P.K., Kumar, C.S., Vivek, B.S., Balachandra, M. and Dargar, S.K. (2022) ‘Implementation of a wild animal intrusion detection model based on internet of things’, In 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS) (pp. 1256-1261). IEEE.

[6] Yadahalli, S., Parmar, A. and Deshpande, A. (2020) ‘Smart intrusion detection system for crop protection by using Arduino’, In 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 405-408). IEEE.

[7] Sabeenian, R., Deivanai, N. and Mythili, B. (2020) ‘Wild animals intrusion detection using deep learning techniques’, Int. J. Pharm. Res, 12(4), pp.1053 1058.

[8] Santhiya, S., Dhamodharan, Y., Priya, N.E.K., Santhosh, C.S. and Surekha, M. (2018) ‘A smart farmland using Raspberry Pi crop prevention and animal intrusion detection system’, Int. Res. J. Eng. Technol, 5(3), pp.3829-3832.

[9] Radhakrishnan, S. and Ramanathan, R. (2018) ‘A support vector machine with Gabor features for animal intrusion detection in agriculture fields’, Procedia computer science, 143, pp.493-501.

[10] Choubisa, T., Mohanty, S.B., Kashyap, M., Gambhir, S., Chaitanya, K.K., Sridhar, A. and Kumar, P.V. (2017) ‘An optical-camera complement to a PIR sensor array for intrusion detection and classification in an outdoor environment’, In 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops) (pp. 44-52). IEEE.

[11] Xue, W., Jiang, T. and Shi, J. (2017) ‘Animal intrusion detection based on convolutional neural network’, In 2017 17th international symposium on communications and information technologies (ISCIT) (pp. 1-5). IEEE.

[12] Sahoo, K.C. and Pati, U.C. (2017) ‘IoT based intrusion detection system using PIR sensor’, In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp. 1641 1645). IEEE.

[13] Maheswari, P.U. and Rajan, A.R. (2016) ‘Animal intrusion detection system using wireless sensor networks’, International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST), 2(10).

[14] Sugumar, S.J. and Jayaparvathy, R. (2014) ‘An improved real time image detection system for elephant intrusion along the forest border areas’, The Scientific World Journal, 2014.