

Interactive Orchard Intrusion Detection System Using Sensors and Human-in-the-Loop Control

Li-Chan Lu,^{1,5} Min-Chie Chiu,^{2*} Dyi-Cheng Chen,¹
Shih-Ming Cho,³ and Tian-Syung Lan⁴

¹Department of Electrical and Mechanical Technology, National Changhua University of Education,
Changhua 500, Taiwan

²Department of Mechanical and Materials Engineering, Tatung University,
No.40, Sec. 3, Zhongshan N. Rd., Taipei City 10452, Taiwan

³Department of Computer Science and Engineering, Tatung University,
No.40, Sec. 3, Zhongshan N. Rd., Taipei City 10452, Taiwan

⁴Research and Development Department, Hsing Wu University, New Taipei City, 244012, Taiwan

⁵Department of Electronic Engineering, Hsiuping University of Science and Technology,
Taichang City 412, Taiwan

(Received January 29, 2026; accepted October 19, 2026)

Keywords: interactive, security, ultrasonic sensor, sound player, remote monitoring, four-bar linkage

To mitigate agricultural crop losses caused by wildlife and unauthorized intrusions, an interactive orchard intrusion detection system combining edge-level automation and human-in-the-loop control was developed. The system integrates an Arduino Mega 2560 microcontroller, a servo-mounted 180° scanning ultrasonic sensor, multi-modal deterrents, and an Internet Protocol camera for real-time smartphone verification. Experimental results for performance evaluation showed a spatial detection accuracy of 94.0%, an average local response latency of 420 ms, and a false-positive rejection rate of 89.5% against environmental clutter such as wind-driven foliage. Despite these advantages, the system presented limitations: ultrasonic susceptibility to severe weather and dense vegetation, reliance on manual human verification under intermittent rural connectivity, and vulnerability to pest habituation and high power demands. To address these limitations, it is necessary to incorporate edge AI for autonomous threat classification, solar-assisted energy harvesting for power-supply autonomy, and long-range-based decentralized communication protocols to ensure long-range operation. The improved system serves as a scalable, low-cost solution for precision agriculture.

1. Introduction

The conflict between agricultural productivity and wildlife intrusion has been a persistent challenge. A representative example is the Eurasian Bullfinch (*Pyrrhula pyrrhula*), which plagued British fruit growers as early as the 16th century.⁽¹⁾ By pecking at fruit tree buds, bullfinches significantly reduced subsequent yields. From the 1950s to the 1970s, their

*Corresponding author: e-mail: mcchiu@gm.ttu.edu.tw
<https://doi.org/10.18494/SAM6269>

populations in southern England were so dense that lethal culling was considered the only viable strategy to mitigate damage.⁽¹⁾

The vulnerability of farms to wildlife, however, extends far beyond birds. Other species inflict diverse forms of damage, necessitating tailored sensor-based strategies. For instance, infrared detection is used in an early warning system to address external animal intrusions.⁽²⁾ Hollinshead *et al.*⁽³⁾ monitored 18 kiwifruit orchards with field cameras, identifying house sparrows, chaffinches, and silvereyes as primary culprits while documenting bud damage surveys. Rodents such as the common vole (*Microtus arvalis*) and water vole (*Arvicola amphibius*) also cause substantial economic losses by gnawing tree bark, with damage rates reaching up to 24% in Czech apple orchards.⁽⁴⁾ Similarly, black rats (*Rattus rattus*)⁽⁵⁾ and wild boars (*Sus scrofa L.*)⁽⁶⁾ considerably degrade macadamia and other crops.

Wild animal damage compounds losses already caused by invertebrate pests and nonhuman primates. Macaques, in particular, are highly destructive owing to their adaptability and opportunistic feeding habits in Nepal and Southeast Asia.⁽⁷⁾ Habitat fragmentation has intensified human–macaque conflicts, rendering traditional deterrents insufficient.⁽⁸⁾ Biological interventions, such as free-ranging dogs fitted with electronic collars, have been attempted, but these methods remain labor-intensive and require constant human oversight.⁽⁹⁾

Therefore, sensor technology has emerged as a promising solution. Modern agriculture demands sustainable, nonlethal, and automated approaches, making sensor-based systems vital for preventing wildlife intrusion. Sensor technology enables continuous monitoring and provides a data-driven bridge between pest behavior and effective deterrence.⁽¹⁰⁾ Chan *et al.* developed an ultrasonic detection system for farm intrusions, but its efficiency was constrained by a narrow detection range and the habituation of intelligent primates to repetitive sounds.⁽¹¹⁾ These limitations highlight the need for advanced sensor technology and multi-modal data processing. By replacing manual guarding with autonomous surveillance, modern sensor systems reduce the burden on farmers while enhancing precision and responsiveness.⁽¹²⁾

To address these gaps, we developed an interactive remote monitoring and orchard intrusion detection system. This system improves traditional ultrasonic sensing by mounting sensors on servo motors, enabling 180° horizontal rotation to eliminate blind spots. To respond to habituation among intelligent intruders, it integrates a mechanical four-bar red flag deterrent and a Secure Digital (SD) card-driven audio array that plays six randomized predator and environmental sounds. An Internet Protocol camera (IPCAM) provides motion-based video disturbance detection, while push notifications are sent to farmers' smartphones via an IoT network for real-time verification. Farmers can then manually trigger high-power alarms or broadcast human voices through a speaker, creating a sophisticated, multi-layered defense tailored to modern orchard management.

The developed system represents a significant advancement in the application of sensor technology to agriculture. By combining ultrasonic sensing, mechanical deterrents, audio randomization, and IoT-enabled video verification, it offers a comprehensive and adaptive solution to wildlife intrusion. Beyond its applicability for orchard protection, the results of this study demonstrate how multi-modal sensor data fusion is used to overcome the limitations of single-sensor approaches. The developed system underscores the potential of intelligent,

automated monitoring to safeguard agricultural productivity, reduce reliance on labor-intensive practices, and pave the way for more resilient and sustainable farming systems.

2. System Development

2.1 System architecture

The system developed in this study employs internet-enabled monitoring and control modules (Fig. 1). For spatial detection, an HC-SR04 ultrasonic sensor (ELECTREACKS, China) is used, operating at a 40 kHz acoustic emission frequency with an effective measuring range of 2–400 cm and a measurement accuracy of 3 mm. To expand spatial coverage without increasing the mechanical footprint, the ultrasonic transducer is mounted on an SG90 miniature servomotor (TowerPro, Taiwan), which provides a stall torque of 1.8 kg·cm and enables 180° horizontal scanning through controlled stepwise rotation.

When an object is detected within a predefined threshold distance of ≤ 170 cm, the detection signal is transmitted to an Arduino Mega 2560 microcontroller. The microcontroller activates a DFPlayer Mini audio module (DFRobot, China) connected to an external SD card, which plays prerecorded predator calls and alarm sounds through a 3 W speaker to prevent wildlife intrusion. For visual monitoring and movement verification, the system uses a pan-tilt IPCAM equipped with a CMOS image sensor. The camera supports high-definition video streaming and pixel-based motion detection. When motion is detected, IPCAM transmits push notifications and image snapshots directly to the user's mobile device through Wi-Fi for real-time intrusion verification. The related sensors, controllers, actuators, and smart sockets used by the orchard farmer are listed in Table 1.

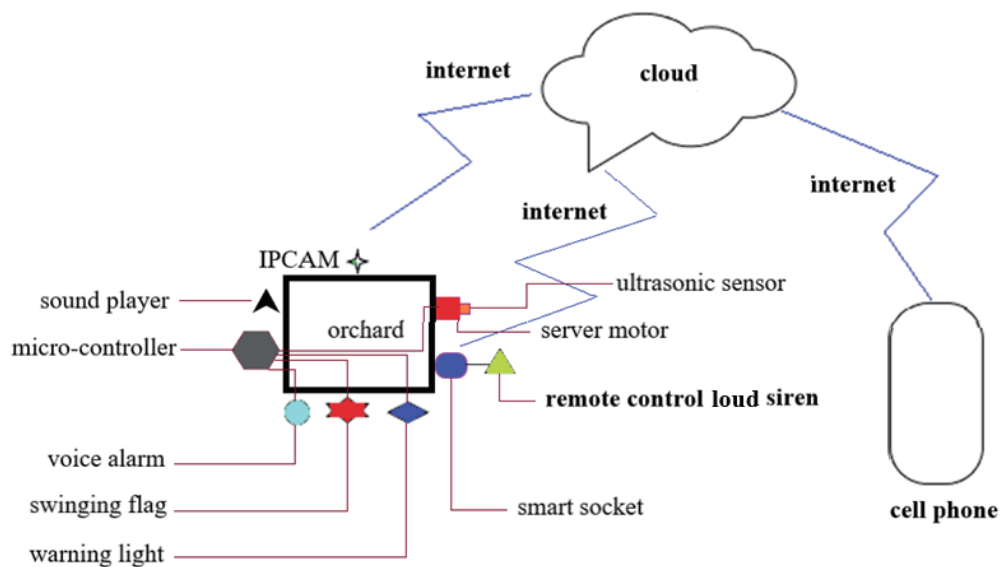


Fig. 1. (Color online) Interactive orchard intrusion detection system.

Table 1

Related sensors, controllers, actuators, and smart sockets used by the orchard farmer.

Item	Key Specifications		Primary Function		Procurement Notes
1	Arduino Uno Development Board	Arduino Uno R3 or compatible	Typical: ATmega328P MCU; 5 V logic; 14 digital I/O pins (6 PWM); 6 analog inputs; 16 MHz clock; USB programming interface; DC input through barrel jack or VIN.	Main processor and system controller. Reads sensor signals, executes detection logic, controls the servo and audio module, and coordinates alarms or communication outputs.	Confirm genuine/compatible board, connector type, and required enclosure.
2	Ultrasonic Distance Sensor	HC-SR04	Typical: 5 V DC; 40 kHz ultrasonic frequency; approximately 2–400 cm measuring range; approximately 15° sensing angle; Trigger and Echo digital interfaces.	Detects the presence and distance of an approaching object. When mounted on the servo, it scans a wider area and helps reduce fixed-sensor blind spots.	Not weatherproof by default; outdoor use requires a protective housing or an outdoor-rated alternative.
3	Micro Servo Motor	SG90	Typical: 4.8–6 V DC; PWM control; approximately 0–180° travel; approximately 1.8 kg·cm stall torque at 4.8 V; weight approximately 9 g.	Rotates the ultrasonic sensor to provide directional scanning, expand detection coverage, and reduce dead zones around the monitored area.	Use a stable external 5 V supply when needed; verify mechanical load and outdoor protection.
4	MP3 Audio Player Module and Speaker	Model not specified	Typical module features: micro SD/TF audio playback; key or serial/UART control; 3.3–5 V supply depending on model. Speaker impedance and power rating must match the selected amplifier/module (commonly 8 Ω).	Plays warning, deterrent, or notification sounds after an intrusion event is confirmed or manually triggered.	Confirm exact player model, amplifier output, speaker wattage, file format, storage capacity, and weather resistance.
5	5 MP Infrared Wide-Angle Camera with Microphone	AHD/TVI/CVI/CVBS or IP/PoE variant	5 MP resolution, typically 2592 × 1944 or 2304 × 1296; approximately 1.8 mm ultrawide/fisheye lens; built-in microphone; infrared night vision approximately 15–20 m or more. IP versions may support P2P remote viewing and PoE; analog versions require a compatible DVR and coaxial cable.	Provides wide-area visual and audio monitoring, nighttime observation, event verification, and evidence recording with fewer camera blind spots.	Select either analog or IP architecture. Confirm IP rating, ONVIF/PoE compatibility, field of view, recorder, and storage.
6	Yoosee-Compatible Smart Monitoring Camera	Yoosee platform camera (exact model TBD)	Source-described range: 1080p to 2.5K/6 MP or higher; single-, dual-, or triple-view configurations; pan/tilt with wide horizontal and vertical coverage; human tracking; infrared and full-color night modes; Wi-Fi, optional dual-band/Wi-Fi 6, Ethernet, and AP mode; two-way audio; motion alarm; TF card up to 512 GB or cloud storage.	Enables smartphone-based remote monitoring, two-way communication, movement alerts, human-in-the-loop verification, and remote response to detected events.	Features vary by model. Confirm resolution, app support, network band, storage plan, cybersecurity, IP rating, and power method.
7	TP-Link Tapo Mini Smart Wi-Fi Socket	Tapo P100	AC 100–125 V, 50/60 Hz; maximum load 10 A; IEEE 802.11b/g/n 2.4 GHz Wi-Fi; Bluetooth 4.2 for setup; remote on/off, scheduling, timer, and Away Mode; Amazon Alexa and Google Assistant support; 55 x 55 x 32.5 mm; operating temperature 0–35 °C; operating humidity 10–90% RH, noncondensing.	Provides smartphone-based remote switching of deterrent equipment, such as warning speakers or high-intensity lighting, and supports scheduled or voice-controlled operation.	Indoor use only. The connected load must not exceed 10 A. For orchard installation, place the socket in a suitable weatherproof enclosure and verify local plug and voltage compatibility.

The system incorporates an ultrasonic sensor mounted on a servo motor, enabling 180° scanning detection. When the sensor identifies an approaching object, the detection signal is transmitted to the microcontroller. The microcontroller activates a sound player, which randomly selects and plays predator or frightening sounds stored on an SD card to deter the intruder. Simultaneously, a four-bar linkage mechanism is adopted to generate a reciprocating motion in a slider, to which a red flag is attached. The four-bar mechanism consists of four rigid links connected by pivot joints, forming a closed kinematic chain. When driven by the microcontroller-controlled actuator, the mechanism converts rotary motion into oscillatory linear motion. This design ensures smooth, repeatable, and mechanically stable flag movement without requiring complex control algorithms. As the slider moves back and forth, the red flag swings continuously, providing a dynamic visual deterrent that enhances the effectiveness of the acoustic signals. The system is equipped with an alarm and warning lights, which are triggered during intrusion events to reinforce the deterrent effect. The integration of auditory, visual, and mechanical deterrents creates a multi-modal repelling strategy that increases the likelihood of deterring common and highly intelligent crop-damaging animals.

The automated detection and repelling functions are controlled by an Arduino Mega2560 microcontroller. This interactive mechanism has proven effective against common crop-damaging animals, including wild boars and birds, and is also capable of deterring highly intelligent species such as monkeys. The hardware components of the system are displayed in Fig. 2 and the wiring diagram is shown in Fig. 3.

To ensure long-term effectiveness against highly intelligent intruders, particularly monkeys, additional features have been integrated into the system. These include IPCAM and a remote smart switch. IPCAM is equipped with motion-detection capabilities that trigger alarm notifications and enable remote audio broadcasting. When motion is detected, IPCAM sends an alert to the farmer's smartphone, allowing real-time access to the live video feed for intrusion verification. If no intrusion is confirmed, the alert is disregarded. However, if the video confirms the presence of an intruder, such as a monkey or even a human trespasser, who is unresponsive to automated audio-visual deterrents, the farmer remotely broadcasts sounds using the smartphone's audio feature. If the intruder remains undeterred, the farmer activates a smart

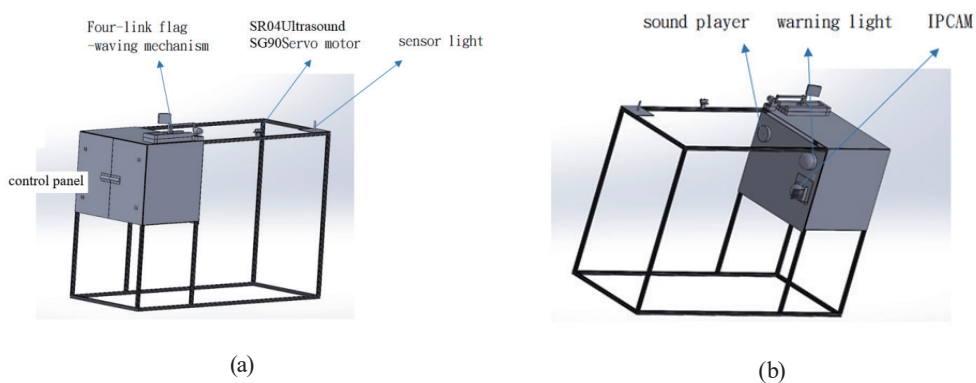


Fig. 2. (Color online) Hardware configuration of interactive orchard intrusion detection system. (a) Frontal and (b) rear views of system.

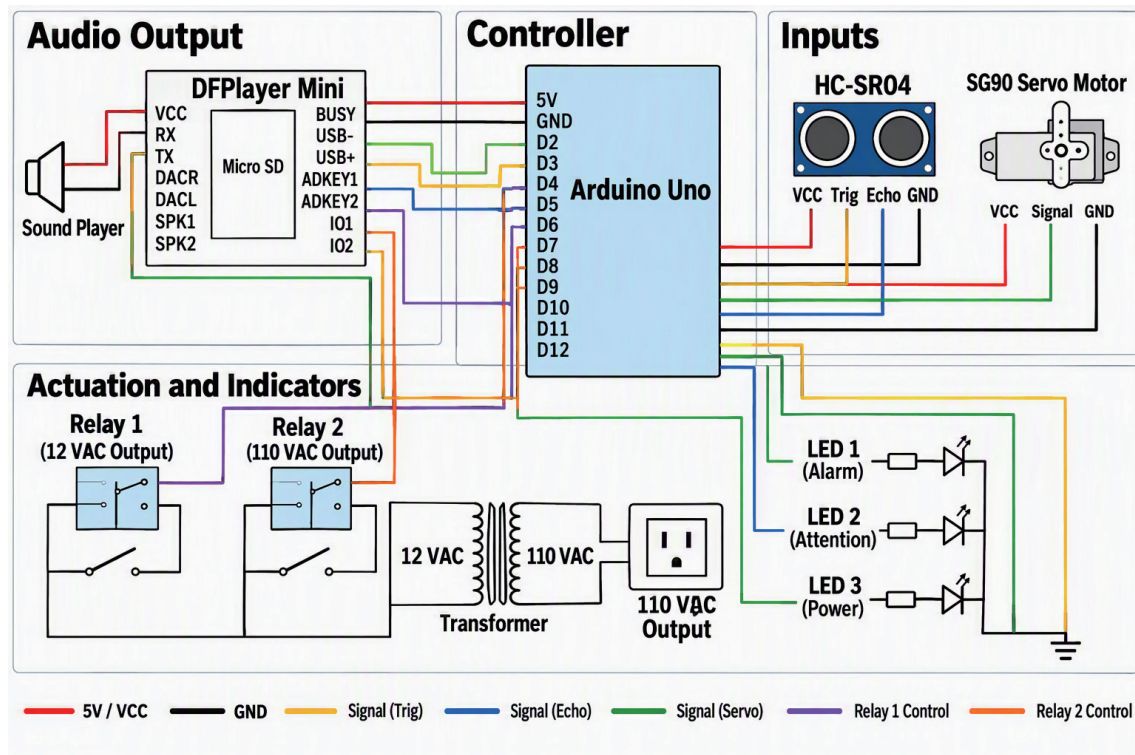


Fig. 3. (Color online) Simplified wiring diagram of orchard intrusion detection system, showing the microcontroller, ultrasonic sensor, servo motor, audio player, relay-controlled outputs, and status indicators.

switch connected to a high-decibel alarm, which effectively repels both monkeys and human trespassers.

This randomized and interactive deterrence strategy significantly enhances the system's capacity to repel highly intelligent and persistent intruders. By integrating multi-modal sensing, automated deterrents, and remote human intervention, the system provides a robust and adaptive solution for modern orchard management.

2.2 Data transmission

The primary layer of the system is an automated loop controlled by an Arduino Mega 2560 microcontroller. This layer is designed to provide immediate, multi-sensory deterrence against intruders (Fig. 4). In the detection phase, the system continuously activates an ultrasonic sensor to calculate distance and identify physical movement within a defined range.

Once an intrusion is confirmed, the Arduino executes parallel output commands. For visual deterrence, the system activates lighting and a red-flag-swinging mechanism driven by the servo motor (myservo defined in the code). For auditory deterrence, the Digital File Player Mini module (MP3 module) is triggered to play sounds of natural enemies through a speaker at a preset volume. At the same time, the system sends an alert and a captured image of the intrusion to the user's smartphone. This local detection and response layer is optimized for low latency. By

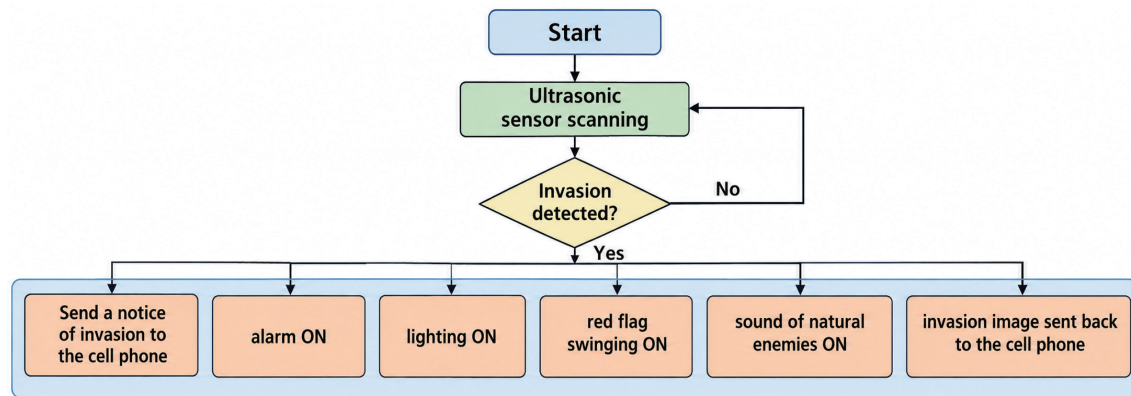


Fig. 4. (Color online) Control logic of interactive orchard intrusion detection system.

relying on local sensors and preprogrammed logic, the system can react instantly to an intruder, often before the user has checked their phone.

The secondary layer introduces a human-in-the-loop component to reduce false alarms and provide higher-intensity deterrence when necessary. In this phase, IPCAM employs image-based motion detection. When motion is detected, IPCAM sends a push notification to the user's smartphone. The user can then open the application (Fig. 5) to view the live stream and verify whether the threat is genuine, such as distinguishing between a pest and a falling branch. If the intrusion is confirmed, the user can manually initiate two high-impact responses. First, they may broadcast their voice directly to the orchard via a remote speaker. Second, they can activate a smart socket to power a high-decibel siren, providing maximum deterrence. This remote monitoring layer enhances system reliability by allowing interactive control. It ensures that disruptive alarms, such as the siren, are only activated when necessary, minimizing noise pollution caused by false triggers. By synthesizing the data from the flowcharts and code, the system's overall performance capabilities can be defined.

2.3 Experiment and performance evaluation

To evaluate the operational efficiency and reliability of the developed system, an experiment was conducted. To replicate orchard intrusions under controlled indoor laboratory conditions, three objects were introduced into the testing zone surrounding the potted citrus tree. Moving dummy targets simulating small animals (such as rodents and wild boars) and nonhuman primates (macaques) were moved along predetermined linear and angular trajectories. To test the false-positive rejection capabilities of the system, swaying artificial foliage and wind-blown branches moved mechanically within the ultrasonic beam path (≤ 170 cm). Human testers approached the perimeter at various angles along the arc of 30 to 145° to evaluate response latency and cloud-based IPCAM notification delivery. In the evaluation, detection accuracy, spatial coverage, latency, and false-positive rejection rates were calculated.

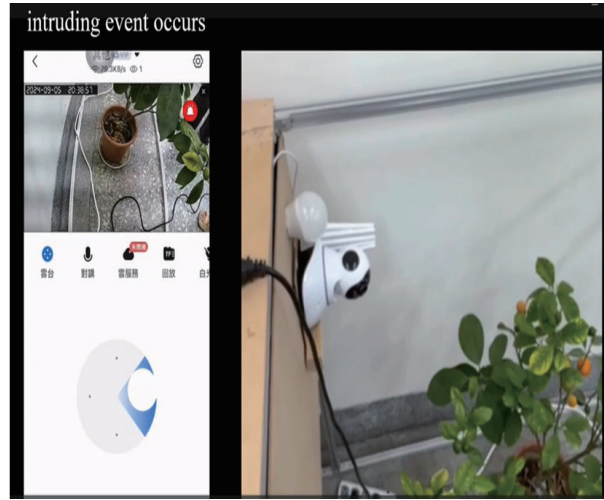


Fig. 5. (Color online) Image of plant movement detected by IPCAM.

1. Detection accuracy and spatial coverage

The ultrasonic sensor mounted on the SG90 servo motor scans a 180-degree horizontal arc divided into angular sectors θ_i ($\theta_i = 30^\circ + i \times 15^\circ$, $i = 0, 1, \dots, 8$). The servo-assisted scanning arrangement extends the sensing coverage beyond that of a fixed sensor and is commonly adopted in obstacle detection and environmental monitoring applications.^(13,14) The spatial detection probability P_d is calculated as the ratio of successfully detected events (D_{true}) to the total events (D_{total}) across varying distances up to 170 cm).

$$P_d = \left(\frac{D_{true}}{D_{total}} \right) \times 100\% \quad (1)$$

2. Latency (system response time)

Latency is evaluated as the total elapsed duration (T_{total}) from the initial ultrasonic distance threshold breach (t_{detect}) to the complete execution of local multi-modal actuators, comprising servo-halt, MP3 audio playback trigger, four-bar mechanism activation, and smartphone push notification dispatch (t_{act}).^(15,16)

$$T_{total} = t_{act} - t_{detect} \quad (2)$$

3. False-positive rejection rate

To assess the effectiveness of the dual-layer verification mechanism in filtering environmental noise (such as wind-blown foliage or falling debris), the false-positive rejection rate (R_{fp}) is defined using the number of suppressed false alarms ($F_{suppress}$) relative to the total number of nonthreatening environmental disturbance triggers (F_{total}).⁽¹⁷⁾

$$R_{fp} = \left(\frac{F_{suppress}}{F_{total}} \right) \times 100\% \quad (3)$$

The initial system test was conducted using the indoor prototype benchtop targeting a potted citrus tree. The test was conducted at threshold boundaries (≤ 170 cm), audio output sound pressure levels at varying distances (measured using a decibel meter at 1 m), and Wi-Fi data packet delivery success rates under varying network latencies.

3. Results

3.1 Prototype system

Figure 6 shows the prototype of the interactive orchard intrusion detection system, which integrates local automated responses with remote human intervention.

The first layer operates as a low-latency, autonomous response unit. By utilizing an ultrasonic sensor mounted on a servo-driven platform, the system achieves a wide-angle scanning range. This configuration enables continuous monitoring without the power consumption associated with continuous video processing. When the distance threshold is breached, the immediate activation of the four-bar linkage (visual deterrence), lighting, and species-specific acoustic sounds (natural enemies) provides an instant defense.

Labor costs and the physical limitations of manual patrolling are significant hurdles in modern orchard management. The developed system addresses these challenges by shifting the sentry role from human labor to sensor technology. The system is designed for orchards in areas where crop damage by intelligent intruders, such as nonhuman primates, is a concern. Standard automated alarms may become less effective over time as animals habituate to repetitive stimuli and learn that the alarms pose no actual threat. By integrating a reinforced remote strategy, this system overcomes such a pattern. Farmers can intervene through live voice broadcasting or remote siren activation, which is an additional response option that may help reduce habituation compared with systems that use fixed deterrent signals. In the system, the ultrasonic sensor is used as a low-power trigger for the local response system and scans a 180° horizontal arc. Environmental disturbances are further assessed through the camera-based verification process.

IPCAM motion detection in the system provides qualitative data for rapid decision-making. The system combines distance-based ultrasonic triggering with IPCAM motion detection to help reduce false-positive alerts. As shown in Fig. 7, the smartphone interface presents an intrusion alert generated by the sensor-fusion framework. The smartphone interface provides a live IPCAM video feed and event information, including the detection time and trigger status. After confirming an intrusion, the user can remotely initiate voice broadcasting or activate the high-decibel siren through the smartphone interface. This event-driven workflow enables rapid user intervention while minimizing false alarms and unnecessary deterrent activation.



(a)



(b)

Fig. 6. (Color online) Prototype orchard to test developed system. (a) Frontal and (b) bird's-eye views.

The development of the system presents directions for agricultural sensor technology.

1. Edge-to-cloud intelligence: The system needs to advance beyond simple movement detection by incorporating onboard artificial intelligence for object recognition. Such integration enables the system to automatically distinguish between a human worker, a pest, or a nonthreatening animal, reducing reliance on manual user verification.
2. Energy autonomy: As sensor technology becomes increasingly efficient, the integration of energy harvesting devices with multi-actuator systems is essential for deployment in remote, off-grid orchard zones. This approach would ensure continuous operation without dependence on external power sources.
3. Decentralized networks: The demonstrated use of the smart socket and IPCAM requires modular IoT ecosystems. A single controller can coordinate a distributed network of sensors and actuators across extensive agricultural areas, communicating through Long Range

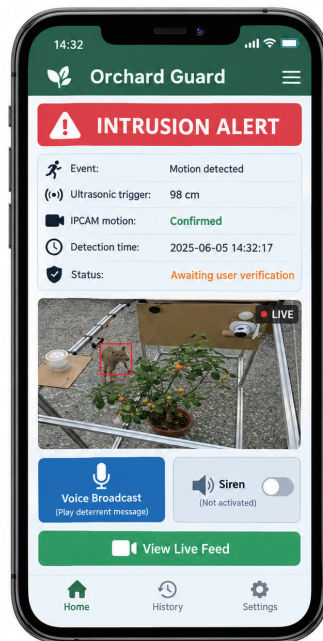


Fig. 7. (Color online) Remote user interface of developed orchard intrusion detection system (red box indicates object intruding into developed system).

protocols to a central hub. Such decentralized architectures would enhance scalability, resilience, and overall system efficiency.

3.2 Experimental results

The developed system's performance was evaluated using metrics of detection accuracy and spatial coverage, system latency, and false-positive rejection performance.^(18,19)

1. Detection accuracy and spatial coverage

Across 100 controlled intrusion tests performed at varying distances and angular positions, the system achieved an overall detection accuracy of 94.0%. Most successful detections were observed in the central scanning region, but a small number of missed detections occurred near the outermost scanning angles ($\geq 140^\circ$). The missed detections occurred in oblique target orientations since the strength of the reflected ultrasonic signal was reduced. The servo-assisted scanning mechanism showed effective perimeter coverage while maintaining a simple and low-cost sensing architecture.

2. Latency

The response time of the developed system was evaluated to measure the elapsed time from the initial distance-threshold breach to the activation of all local deterrent components. The autonomous control loop achieved an average latency (T_{total}) of 420 ms. This interval included obstacle detection, servo positioning, warning-light activation, four-bar flag deployment, and DFPlayer Mini audio triggering. In comparison, IPCAM-based cloud notifications required 1.8–3.2 s, depending on network and Wi-Fi traffic conditions. Local edge-level actuation provided rapid real-time responses, whereas smartphone notifications served as a secondary monitoring and verification mechanism.

3. False-positive rejection rate

To evaluate the effectiveness of the dual-layer verification framework, simulated environmental disturbances were used in the experiment, including wind-driven artificial foliage movement. When operating only with ultrasonic sensing, 28% of the detected events corresponded to nonthreatening disturbances. However, the addition of IPCAM motion verification enhanced system reliability. The visual verification layer rejected 89.5% of these false triggers, which reduced unnecessary alarm activation and false alerts to the user. The result supported the effectiveness of distance-based sensing with visual confirmation for environmental noise suppression.

The integrated deterrent mechanisms operated consistently in the experiment. The randomized playback of prerecorded audio files reduced stimulus predictability in repeated intrusion events, and the reciprocating motion of the four-bar flag mechanism provided a dynamic visual deterrent. The combination of acoustic and visual stimuli enhanced the deterrence strategy and supported the autonomous operation of the system without requiring immediate user intervention.

Compared with conventional single-modality agricultural intrusion detection systems, the system enhanced robustness through multi-modal sensor fusion. Previous wildlife deterrence systems rely on passive infrared sensors or fixed-position ultrasonic detectors, which are susceptible to environmental interference because they lack secondary verification methods. In contrast, vision-based deep learning approaches show high recognition accuracy. However, such approaches require computational resources for continuous image processing, which requires energy consumption. The developed system combines low-power ultrasonic sensing with event-driven visual verification. The system's performance (a detection accuracy of 94.0%, an average local response time of 420 ms, and a false-alarm rejection rate of 89.5%) implies that low-cost sensors enable reliable intrusion detection and maintain energy efficiency and operational simplicity required for smart agricultural deployments. These results support the appropriateness of the system for precision agriculture applications for which affordability, scalability, and reduced labor requirements are critical.^(19,20)

3.3 System used in practical orchard farm

The system has been deployed in an actual orchard located in a mountainous area. The crescent-shaped orchard covers approximately 4,849.6 m² and is bordered by a creek on one side. The allocation of IPCAM together with the ultrasonic device is shown in Fig. 8. From the actual orchard, the remote user interfaces of the orchard's two monitoring systems—namely, the wired system installed along the fence perimeter and the wireless system deployed within the orchard—as well as the actual arrangement of IPCAMs and ultrasonic sensors are shown in Fig. 8.

The deterrent measures triggered by ultrasonic detection, including predator sounds, high-intensity lighting, and flag-waving devices, are activated locally at the orchard. These measures constitute edge-level responses and do not require sensor data or control commands to be transmitted to the cloud or a control center. Moreover, IPCAMs capture images of the intrusion and send them to the cloud and the farm owner's smartphone.

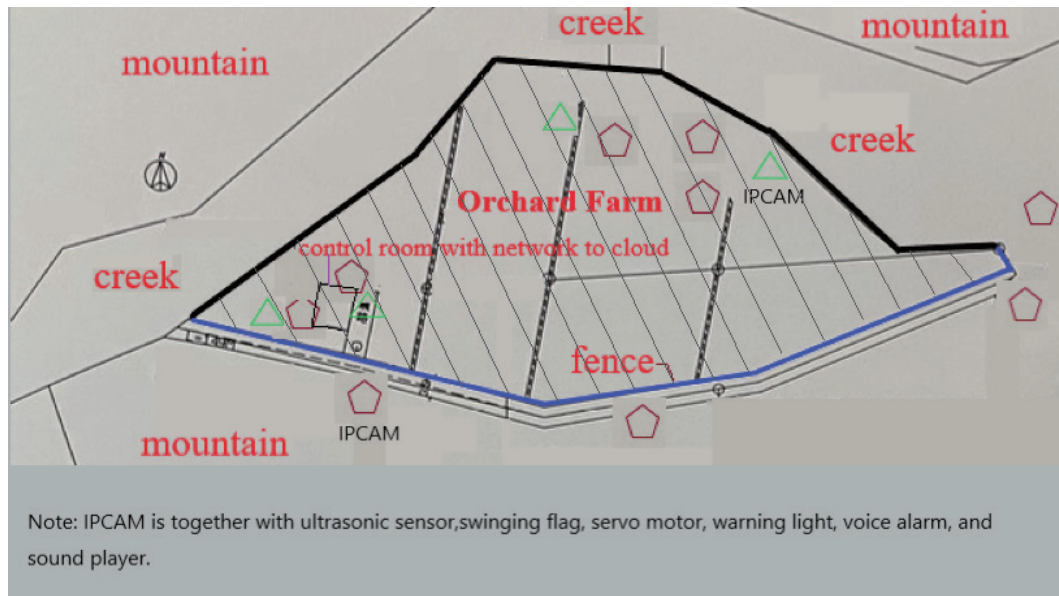


Fig. 8. (Color online) Sensor allocation in the actual orchard farm.

The farm owner can open and review the intrusion images and take further action when necessary (see Figs. 9 and 10). For example, if an unauthorized person enters the orchard, the owner can transmit a warning message through a smartphone. Alternatively, a smart socket can be used to remotely activate a high-power loudspeaker or high-intensity lighting. The smartphone interface of the smart socket is shown in Fig. 11.

The system provides stable network transmission. In addition, it combines ultrasonic sensing with IPCAM-based motion detection, thereby enabling rapid and accurate intrusion detection. The authors personally tested the system by entering the monitored area. The smartphone received a cloud-based push notification containing the intrusion image within approximately 2–3 s, demonstrating the system's near-real-time responsiveness.

The interactive human-in-the-loop control mechanism serves as a safety measure that allows the operator to cancel deterrent actions triggered by false detections or manually escalate the response to an intruder. The proposed system has been implemented to protect an actual orchard farm.

For animal intrusions, the system combines continuous ultrasonic scanning with supplementary IPCAM-based motion detection. In addition to sending warning notifications and intrusion images to the farm owner, it automatically activates high-intensity lights and predator sounds. Field observations indicate that these measures are generally sufficient to deter invading animals.

Animal intrusions were found to occur most frequently during the daytime. At night, no animal intrusions were observed, apart from farm personnel entering and leaving the orchard. Therefore, the system is configured to send intrusion-image notifications only during the daytime. When an intruder enters the orchard, the automatic deterrent mechanisms, including high-intensity lights and predator sounds, are activated immediately.



Fig. 9. (Color online) Monitoring image for IPCAM with wire connection installed along the orchard fence.

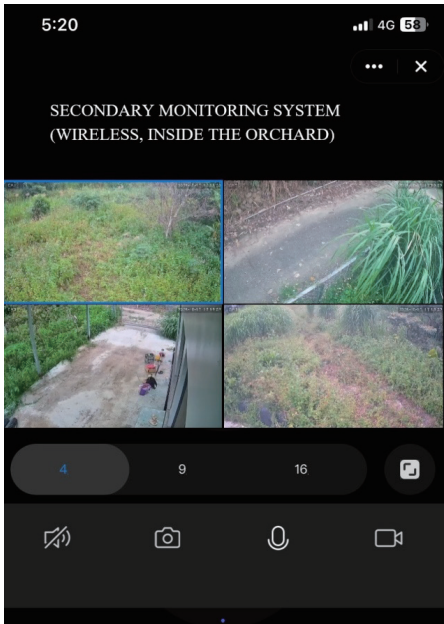


Fig. 10. (Color online) Monitoring image for IPCAM with wireless connection installed inside the orchard fence.

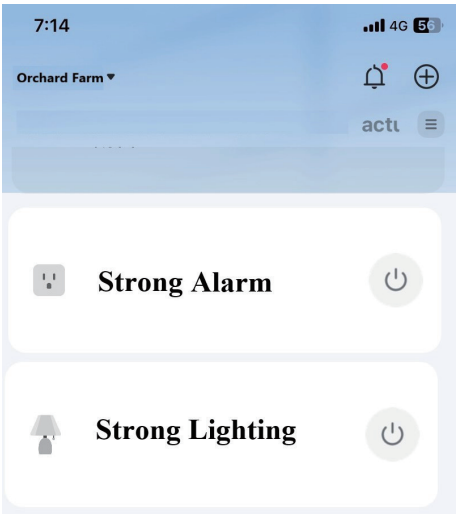


Fig. 11. (Color online) Interface of the smart socket in orchard owner’s smartphone.

If the automatic deterrent measures are insufficient, such as when an unauthorized person enters the orchard, the farm owner can verify the intrusion image and remotely play a warning message through a smartphone. The intrusion images are uploaded to the cloud for subsequent evidence collection and incident reporting.

Accordingly, the system is designed to operate primarily in a fully automated manner, thereby eliminating the need for continuous human monitoring. Although human participation is incorporated into the system, the user generally assumes a passive supervisory role and intervenes only when verification or an escalated response is required. Daytime and nighttime human-intrusion tests demonstrated rapid system response and satisfactory intrusion-detection performance.

The real-time latency between the sensor-fusion result reaching the critical threshold and the notification being delivered to the farm manager's smartphone was very low. The orchard uses a Far EasTone Telecommunications network connection in Taiwan, which provides strong and stable signal coverage. The outdoor IPCAMs installed around the orchard perimeter are connected through wired networks, while wireless signal repeaters are installed to strengthen the connections of the wireless IPCAMs within the orchard.

Field tests demonstrated rapid system response without observable signal loss. Notifications were delivered to the farm manager's smartphone with almost imperceptible delay. All intrusion events and associated images were uploaded to the cloud, allowing historical incidents to be reviewed and traced. The system has collected numerous detection images during actual orchard operation and demonstrated a very high detection success rate.

The interactive orchard intrusion-prevention system uploads real-time intrusion images to the cloud and sends them to the farm owner's smartphone. After reviewing the images, the farm owner can determine the appropriate subsequent action; this process represents cloud-based human intervention. In contrast, when an intrusion threat is detected at the orchard site, the system immediately activates the corresponding deterrent measures, representing edge-level automation. The relevant cloud-based event records and system push notifications are shown in the following Figs. 12 and 13.

The system has been implemented and tested in an actual orchard surrounded by a diamond-mesh fence. Ultrasonic sensors and 5-megapixel infrared wide-angle cameras with audio-recording capability were installed at regular intervals along the top of the fence. The system was tested during both daytime and nighttime operations. The results confirmed that it could successfully capture images of intruders and activate the corresponding deterrent mechanisms, as shown in Fig. 14. These field tests demonstrate the practical feasibility of applying the proposed system in a real orchard environment.

4. Discussion

4.1 Operational efficiency and human-in-the-loop practicality

Under normal operating conditions, the first level of protection is performed autonomously. The ultrasonic sensor is used to continuously scan the surrounding environment through servo-driven rotation, and the microcontroller automatically activates deterrent devices, including

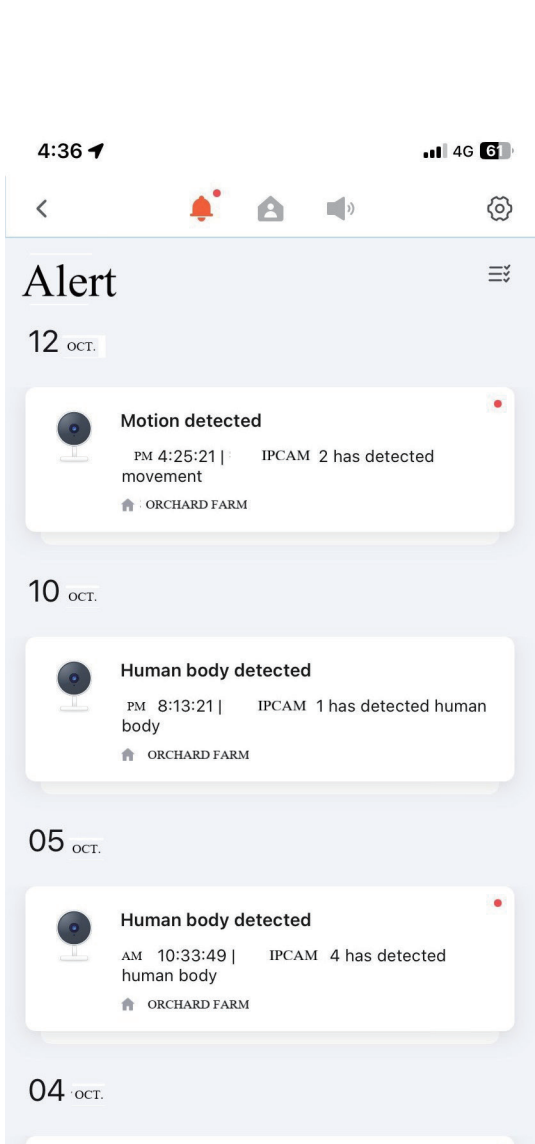


Fig. 12. (Color online) Alert of intruding event from the wireless IPCAM system forwarded to the orchard owner’s smartphone.



Fig. 13. (Color online) Alert of intruding event from the wired IPCAM system forwarded to the orchard owner’s smartphone.

warning lights, flag movements, and randomized audio playback. This sensing and response strategy operates continuously without human presence, enabling the immediate deterrence of common wildlife threats such as wild boars, rodents, and other crop-damaging animals.

However, human involvement is required when a significant intrusion event is detected. Instead of demanding continuous supervision, the system employs an event-driven notification approach. IPCAM is used to transmit alerts and images to the farmer’s mobile device only when motion activity exceeds predefined thresholds. This enables the farmer to verify the event and make decisions about additional intervention. As a result, the farmer acts as a supervisor rather than a constant operator, greatly reducing monitoring requirements.



Fig. 14. (Color online) Detected intruding events including monkeys, birds, and human. (a) Bird detected, (b) intruding car detected, (c) human detected, (d) egret silk detected, (e) eagle detected, (f) monkey detected, and (g) monkey detected.

The operational efficiency of the developed system can be enhanced by incorporating edge AI-based event filtering to distinguish genuine intrusion events from environmental disturbances such as moving vegetation, rainfall, and shadows.⁽²¹⁾ Intelligent filtering reduces false alarms and unnecessary notifications. In addition, scheduled low-disturbance operating modes minimize nighttime interruptions, and adaptive escalation strategies automatically activate higher-intensity deterrents, such as sirens or emergency notifications. These improvements further reduce user intervention, maintaining effective crop protection.

Recent studies in smart agriculture have presented the importance of balancing autonomous operation with human supervisory control in complex and dynamic agricultural environments.⁽²²⁾ In mobile-integrated cyber-physical systems, asynchronous and event-triggered notifications can be combined with human supervision without requiring continuous visual surveillance or active user engagement.⁽²³⁾

Moreover, Parasuraman *et al.*⁽²⁴⁾ proposed a classical model describing different levels of interaction between humans and automated systems, including information acquisition, information analysis, decision selection, and action implementation. An advantage of this model is that it clearly distinguishes the tasks performed by the automated system from those performed by human operators, thereby supporting the trade-off between automation efficiency and the safety provided by human control. However, because the study was published relatively early, it did not address the Internet of Things, cloud platforms, or smartphones. Furthermore, it is primarily a theoretical model, and experimental validation is still required to demonstrate its effectiveness in an actual orchard system.

Schirner *et al.*⁽²⁵⁾ investigated how humans can be incorporated into cyber-physical systems so that sensors, embedded computing, user decisions, and physical devices form a closed control loop. The principal advantage of this study is that it presents a comprehensive human-in-the-loop closed-loop concept that can support a system design in which a deterrent device is activated or deactivated following human confirmation. However, the study was not specifically designed for agricultural environments. It also did not examine nocturnal animal intrusion or unstable network connectivity in orchards, nor did it provide specific performance indicators applicable to orchard systems.

Miao *et al.*⁽²⁶⁾ proposed an iterative human–AI approach for wildlife-image identification. In this approach, images are first identified automatically, after which human operators examine images containing new species, rare species, or uncertain classifications. The resulting human feedback is then used to update the model. An advantage of this study is that its application directly involves wildlife monitoring and enables continuous model improvement through human feedback. However, the human participants are mainly responsible for image annotation rather than the real-time control of deterrent devices. The authors did not discuss alarm-transmission latency, manual overrides, or actuator-response time. Moreover, it was primarily developed for ecological monitoring rather than orchard security or intrusion response and therefore cannot directly demonstrate that remote human intervention improves deterrence effectiveness.

Norouzzadeh *et al.*⁽²⁷⁾ applied active learning to camera-trap images. Their system selects the most informative or uncertain images and submits them to human operators for annotation,

thereby reducing unnecessary human effort. The study showed that the demand for manual annotation in a large dataset can be reduced by more than 99.5%. Its advantages include its suitability for wildlife images and camera-monitoring data, as well as its ability to substantially reduce the human workload. However, the study focused primarily on model training and image annotation rather than real-time intrusion response, and it cannot directly determine whether human intervention improves the actual success rate of animal deterrence.

Mosqueira-Rey *et al.*⁽²⁸⁾ classified human-in-the-loop machine learning into several categories, including active learning, interactive machine learning, machine teaching, and explainable artificial intelligence, and discussed the control relationships between humans and algorithms. The principal advantage of this study is that it provides a comprehensive and systematic definition of human-in-the-loop systems. However, it is a general review and does not include experiments involving orchard environments or animal-intrusion control. Furthermore, it focuses primarily on machine-learning processes and provides a relatively limited discussion of alarms, actuators, and real-time override control. Consequently, it cannot directly support evaluations of communication latency or deterrence success rates in orchard systems.

A comparison of the aforementioned studies reveals an important research gap. Most existing studies focus on manual annotation, model improvement, or general supervisory control. Few systems simultaneously integrate the following functions:

1. multimodal sensor fusion,
2. real-time threat feedback,
3. smartphone notifications,
4. human confirmation or override,
5. remote activation of deterrent devices, and
6. an automatic backup mechanism when no human response is received

Therefore, the novelty of the proposed system can be defined as extending the human-in-the-loop concept from passive data annotation and result verification to real-time decision-making, alarm overriding, and deterrent control for orchard-intrusion events. Balancing automation with human supervision can preserve the labor-saving benefits of smart agriculture.

4.2 Limitations and improvements

The system demonstrates the effectiveness of sensors in detecting intrusion into orchards. The 180° scanning arc ensures perimeter coverage and maintains hardware simplicity. The results of this study show how precision agriculture contributes to addressing food security and labor shortages. Despite the results, the developed system has technical limitations and issues to address. First, single-point ultrasonic ranging is susceptible to false triggers caused by severe weather conditions or dense, wind-swept vegetation. In addition, reliance on cellular networks for cloud notifications introduces vulnerability to intermittent rural signal coverage. Second, the prolonged deployment of devices threatens animal habituation, where intelligent pests become accustomed to repetitive deterrents. Third, the continuous operation of multi-actuator systems and Wi-Fi/IPCAM modules demands substantial electrical power, necessitating additional power supply methods.

To address these limitations, advanced sensing technologies, edge AI, and energy-efficient communication frameworks must be integrated into future system iterations. By incorporating on-device machine learning algorithms, sensor data can be processed in real time to distinguish wildlife, farm personnel, and environmental disturbances with minimal dependence on cloud-based verification, reducing false alarms and enhancing response accuracy.⁽²⁹⁾ Solar-energy harvesting and intelligent battery management strategies must also be adopted to support continuous off-grid operation in remote orchard environments.⁽³⁰⁾ In addition, long-range communication protocols can be employed to enhance transmission reliability in large agricultural areas where cellular network coverage is unstable.⁽³¹⁾ Whereas the current system utilizes standard Wi-Fi for data transmission and mobile notifications, specialized long-range infrastructure must be developed. By integrating LoRa-based decentralized communication protocols and solar-assisted energy harvesting, remote connectivity barriers can be overcome to ensure robust off-grid operation.

The system prototype was constructed using commercially available components to evaluate the feasibility of the proposed orchard intrusion detection system. However, for further improvement, advanced sensor technology and functional materials must be applied. Conventional ultrasonic sensors employ bulk piezoelectric ceramic elements whose performance can deteriorate under prolonged exposure to fluctuating environmental conditions such as humidity and dust. Detection sensitivity, spatial resolution, and localization accuracy can be enhanced using robust piezoelectric ultrasonic transducers and directional beam forming, especially for small and rapidly moving pests. In addition, the integration of flexible energy-harvesting materials, such as triboelectric nanogenerators and polyvinylidene fluoride-based piezoelectric films, can be used to convert ambient wind energy and mechanical vibrations into electrical power for self-sustaining sensor nodes.

The orchard monitoring system can be deployed for extended periods by using advanced packaging materials, including hydrophobic self-cleaning coatings, corrosion-resistant encapsulation layers, and ultraviolet-resistant biodegradable polymer housings, to ensure durability and environmental resilience, reducing plastic-associated ecological impact. These technologies and materials contribute to the enhancement of energy autonomy, sensing performance, and system robustness in large-scale agricultural monitoring.⁽³²⁾

5. Conclusion

We developed an orchard intrusion detection system that integrates ultrasonic sensing, automated deterrents, camera-based verification, and remote human intervention to support crop protection and reduce reliance on continuous manual monitoring. The system employs a dual-layered strategy tailored to intruder intelligence: automated local deterrents (spotlights, alarms, a four-bar flag mechanism, and randomized audio playback) for common animals and an IPCAM-enabled visual verification method for intelligent pests, enabling farmers to remotely trigger voice broadcasts or high-decibel sirens. Quantitative prototype evaluation results showed high operational efficacy, achieving an overall spatial detection accuracy of 94.0% across a scanning

arc of 180°, an average local response latency of 420 ms, and a false-positive rejection rate of 89.5% against environmental clutter such as wind-blown foliage. The experimental results show the feasibility of combining multiple deterrent mechanisms with human-in-the-loop control in an orchard intrusion detection prototype. The orchard intrusion detection system was also deployed in an actual orchard, where it demonstrated effective intrusion detection and deterrence. However, it is necessary to introduce edge-AI classification, energy harvesting, weather-resistant packaging, and long-range communication to improve the system's reliability and support deployment in remote orchards.

References

- 1 British Birds **117** (2024) 308: <https://britishbirds.co.uk/journal/article/bullfinches-killed-commercial-orchards-1960s> (accessed January 2026).
- 2 S. Jeevitha and V. Kumar: IJERT **9** (2020) 1219. <https://doi.org/10.17577/IJERTV9IS050351>
- 3 J. A. Hollinshead, J.V. Briskie, and S.M. Kross: Crop Prot. **184** (2024) 106792. <https://doi.org/10.1016/j.cropro.2024.106792>
- 4 J. Suchomel, J. Šipoš, J. Ouředníčková, M. Skalský, and M. Heroldová: Agronomy **12** (2022) 251. <https://doi.org/10.3390/agronomy12020251>
- 5 J. White, J. Wilson, and K. Horskins: Crop Prot. **16** (1997) 727. [https://doi.org/10.1016/S0261-2194\(97\)00062-8](https://doi.org/10.1016/S0261-2194(97)00062-8)
- 6 K. V. Ramesh: Int. J. Curr. Microbiol. App. Sci. **8** (2019) 3480. <https://www.ijcmas.com/8-2-2019/K.%20Venkata%20Ramesh.pdf>
- 7 T. Y. Ke: Master Thesis, National Pingtung University of Science and Technology (2022). <https://ndltd.ncl.edu.tw/cgi-bin/gs32/gsweb.cgi/login?o=dnclcdr&s=id=%22110NPUS5746016%22.&searchmode=basic>
- 8 S. Koirala, P.A. Garber, D. Somasundaram, H.B. Katuwal, B. Ren, C. Huang, and M. Li: J. Environ. Manag. **297** (2021) 113331. <https://doi.org/10.1016/j.jenvman.2021.113331>
- 9 P. D. Curtis and R. Rieckenberg: Wildl. Damage Manag. Conf. Proc. **105** (2005) 148. https://digitalcommons.unl.edu/icwdm_wdmconfproc/105/
- 10 H. Shahab, M. Naeem, M. Iqbal, M. Aqeel, and S.S. Ullah: Smart Agric. Technol. **10** (2025) 100847. <https://doi.org/10.1016/j.atech.2025.100847>
- 11 T. J. Chan, M. C. Chiu, H. C. Cheng, L. J. Yeh, and W. C. Haung: 2019 IOP Conf. Ser. Mater. Sci. Eng. **644** (2019) 012006. <https://iopscience.iop.org/article/10.1088/1757-899X/644/1/012006>
- 12 A. J. Garcia-Sanchez, F. Garcia-Sanchez, F. Losilla, P. Kulakowski, J. Garcia-Haro, A. Rodríguez, J. V. López-Bao, and F. Palomares: Sensors **10** (2010) 7236. <https://doi.org/10.3390/s100807236>
- 13 C. H. Chan, F. L. Wen, and S. J. Wen: Eng. Proc. **108** (2025) 44. <https://doi.org/10.3390/engproc2025108044>
- 14 W. Bian, J. Li, Y. Diao, K. Tian, Z. Fan, T. Zou, and B. Kang: Appl. Syst. Innov. **9** (2026) 189. <https://doi.org/10.3390/asi9090189>
- 15 P. He, Y. Wang, G. Zheng, and H. Zhou: Mining **5** (2025) 54. <https://doi.org/10.3390/mining5030054>
- 16 A. F. Abdulqader, M. M. M. Salih, N. H. Shaker, W. A. Sajid, W. Qasem, and A. Gajewska: Proc. 2024 36th Conference of Open Innovations Association (FRUCT) (IEEE, 2024) 145. <https://doi.org/10.23919/FRUCT64283.2024.10749858>
- 17 G. R. McRee: J. Cybersecur: Priv. **2** (2022) 379. <https://doi.org/10.3390/jcp2020020>
- 18 T. S. Delwar, S. Mukhopadhyay, A. Kumar, M. Singh, Y. W. Lee, J. Y. Ryu, and A. S. M. S. Hosen: Future Internet **17** (2025) 70. <https://doi.org/10.3390/fi17020070>
- 19 T. N. Syed, J. Zhou, I. A. Lakhari, F. Marinello, T. T. Gemechu, L. T. Rottok, and Z. Jiang: Agriculture **15** (2025) 827. <https://doi.org/10.3390/agriculture15080827>
- 20 Z. Lima, H. García-Vázquez, R. Rodríguez, S. L. Khemchandani, F. Dualibe, and J. Del Pino: Appl. Syst. Innov. **1** (2018) 26. <https://doi.org/10.3390/asi1030026>
- 21 D. Davcev, S. Kalajdziski, I. Dimitrovski, I. Kitanovski, and K. Mitreski: Agri. Engineering **8** (2026) 147. <https://doi.org/10.3390/agriengineering8040147>
- 22 J. M. Fernandes, J. E. Rivadeneira, A. Rodrigues, F. Boavida, and J.S. Silva: Comput. Stand. Interfaces **91** (2025) 103895. <https://doi.org/10.1016/j.csi.2024.103895>
- 23 R. Zhang and X. Li: Sensors **21** (2021) 7502. <https://doi.org/10.3390/s21227502>
- 24 R. Parasuraman, T. B. Sheridan, C. D. Wickens: IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems and Humans **30** (2000) 286. <https://doi.org/10.1109/3468.844354>

- 25 G. Schirner, D. Erdogmus, K. Chowdhury, T. Padir: *Computer*, **46** (2013) 36. <https://doi.org/10.1109/MC.2013.31>
- 26 Z. Miao, Z. Liu, K. M. Gaynor, M. S. Palmer, S. X. Yu, W. M. Getz: *Nature Machine Intelligence* **3** (2021) 885. <https://doi.org/10.1038/s42256-021-00393-0>
- 27 M. S. Norouzzadeh, D. Morris, S. Beery, N. Joshi, N. Jovic, J. Clune: *Methods in Ecology and Evolution*, **12** (2021) 150. <https://doi.org/10.1111/2041-210X.13504>
- 28 E. Mosqueira-Rey, E. Hernández-Pereira, D. Alonso-Ríos, J. Bobes-Bascarán, Á. Fernández-Leal: *Artificial Intelligence Review* **56** (2023) 3005. <https://doi.org/10.1007/s10462-022-10246-w>
- 29 M. R. Al Mamun, A. K. Ahmed, S. M. Upoma, M. M. Haque, and M. A. E. Rabbani: *Smart Agric. Technol.* **10** (2025) 100773. <https://doi.org/10.1016/j.atech.2025.100773>
- 30 S. Bertoldo, L. Carosso, E. Marchetta, M. Paredes, and M. Allegretti: *Appl. Syst. Innov.* **1** (2018) 49. <https://doi.org/10.3390/asi1040049>
- 31 Y. Birjis, S. Swaminathan, H. Nazemi, G. C. A. Raj, P. Munirathinam, A. Abu-Libdeh, and A. Emadi: *Sensors* **22** (2022) 9151. <https://doi.org/10.3390/s22239151>
- 32 J. P. Lee, J. W. Lee, and J. M. Baik: *Micromachines* **9** (2018) 532. <https://doi.org/10.3390/mi9100532>