TYPE Original Research
PUBLISHED 10 October 2025
DOI 10.3389/fpls.2025.1634408

A privacy-protecting eggplant disease detection framework based on the YOLOv11n-12D model

Jiao Han, Zhenzhen Wu, Yandong Ding, Yantong Guo and Rui Fu*

Weifang University of Science and Technology, Weifang, China

Check for updates

OPEN ACCESS

EDITED BY
Hao Wang,
Laoshan National Laboratory, China

REVIEWED BY
Maragatharajan M,
VIT Bhopal University, India
Matthew Oladipupo,
University of Salford, United Kingdom
Xiaotong Li,
China University of Petroleum
(East China), China

*CORRESPONDENCE
Rui Fu
✉ furui19891209@wfust.edu.cn

RECEIVED 27 May 2025
ACCEPTED 03 September 2025
PUBLISHED 10 October 2025

CITATION
Han J, Wu Z, Ding Y, Guo Y
and Fu R (2025) A privacy-protecting
eggplant disease detection framework
based on the YOLOv11n-12D model.
Front. Plant Sci. 16:1634408.
doi: 10.3389/fpls.2025.1634408

COPYRIGHT
© 2025 Han, Wu, Ding, Guo and Fu. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

The growing global population and rising concerns about food security highlight the critical need for intelligent agriculture. Among various technologies, plant disease detection is vital but faces challenges in balancing data privacy and model accuracy. To address this, we propose a novel privacy-preserving eggplant disease detection system with high accuracy. First, we introduce a lightweight 3D chaotic cube-based image encryption method that ensures security with low computational cost. Second, a streamlined YOLOv11n-12D framework is employed to optimize detection performance on resource-constrained devices. Finally, the encryption and detection modules are integrated into a real-time, secure, and accurate identification system.Experimental results show our framework achieves near-ideal encryption security (entropy=7.6195, Number of Pixel Change Rate(NPCR)=99.63%, Unified Average Changing Intensity(UACI)=32.85%) with 23× faster encryption (0.0127s) versus existing methods. The distilled YOLOv11n-12D model maintains teacher-level accuracy (mAP@0.5=0.849) at 3.6× the speed of YOLOv12s (2.7ms/inference), with +6.5% mAP improvement for small disease detection (e.g., thrips). This system balances privacy and real-time performance for smart agriculture applications.

KEYWORDS

image encryption, eggplant disease detection, YOLOv11n-12D, privacy protection, intelligent agriculture

1 Introduction

With the rapid advancement of agricultural digitalization, crop disease detection has become critical for ensuring food security and improving agricultural productivity (Elijah et al., 2018; Cornia, 1985). In many remote or underdeveloped regions, due to the lack of professional expertise and detection equipment, farmers often transmit crop images to external agricultural centers for manual or automated analysis (Baldi and La Porta, 2020). However, existing methods frequently struggle to balance model accuracy with data privacy protection. In addition, the detection systems must operate efficiently on resource-constrained devices typical of rural environments, while ensuring secure handling of sensitive data during transmission and storage. Consequently, the development of efficient, automated, and privacy-preserving disease detection systems that are both lightweight and reliable is crucial for promoting smart agriculture.

In recent years, deep learning-based object detection algorithms have achieved remarkable progress in plant disease recognition (Senthil Pandi et al., 2024; Ravì et al., 2017; Zhang et al., 2017). Lightweight models, particularly the YOLO series, have attracted considerable attention for their fast detection speeds and high accuracy (Zhang et al., 2024; He et al., 2024; Liu et al., 2022). Sangaiah et al. (2024) proposed T-YOLO-Rice, based on YOLOv4, to improve small-target detection such as rice leaf spots, outperforming YOLOv7 but remaining limited to a single task. To address diverse diseases and class imbalance, Roy and Bhaduri (2022) developed Dense-YOLOv4 by integrating DenseNet and an enhanced PANet, achieving 96.20% mAP and 93.61% F1-score for mango disease detection, and demonstrating generalization to grape and tomato diseases. Lin et al. (2023) built YOLO-Tobacco based on YOLOX-Tiny by adding HMU and CBAM modules, improving outdoor tobacco leaf detection (80.56% AP, 69 FPS), although its adaptability to multiple diseases remains limited. Building upon these advances, Li et al. (2023a) introduced MG-YOLO, integrating multi-head self-attention, BiFPN, and GhostCSP modules, achieving 98.3% accuracy at 0.009 seconds per image and surpassing YOLOv5 by 6.8% in complex environments. In addition to single-task detection, recent studies have explored joint detection and tracking paradigms (Li et al., 2023b, 2024), leveraging reinforcement learning to achieve object recognition and continuous tracking in dynamic environments. For example, Li et al. (2025) proposed a reinforcement learning-based joint detection and tracking paradigm for compact HFSWR target detection and tracking, which effectively improves detection probability and tracking performance.

In image tasks related to object detection, image enhancement has also emerged as an important research direction in recent years. For example, researchers have proposed a reinforcement learning-based human visual perception-driven image enhancement method (Luo, 2024). Liu et al. (2025a) introduced a framework that cascades an aerial image enhancement module with AC3Net, while Xiao et al. (2024) proposed a neuromorphic computing-based underwater image enhancement network (UIEN), which simulates visual system perception and employs unsupervised learning to address multiple types of underwater image degradation and validate its effectiveness. Despite these significant advances in image enhancement, most existing studies still overlook data privacy issues, as unencrypted images transmitted over networks are vulnerable to theft or misuse. This further highlights the necessity of integrating image encryption with recognition.

Therefore, with increasing emphasis on data privacy, researchers have begun integrating image encryption with disease detection to achieve end-to-end security without compromising performance. Qin et al. (2014) proposed SecSIFT, a method that performs SIFT feature extraction directly within the encrypted domain, effectively safeguarding sensitive image data while maintaining high detection accuracy and computational efficiency. Building on this idea, Man et al. (2021) integrated convolutional neural networks with chaotic encryption, enabling intelligent privacy protection for both image and text data, and laying the foundation for secure image processing in agriculture. Kumar et al. (2021) introduced SP2F, a privacy-preserving framework combining blockchain and deep learning, with a two-level privacy engine and stacked LSTM networks to improve UAV data authentication and resilience. Furthermore, Kethineni and Gera (2023) proposed an IoT security model that integrates sparse capsule autoencoders and attention-based GRUs for lightweight detection and data protection, achieving 99.9% accuracy and F1 score, highlighting its potential for agricultural data security.

Our work aims to develop a lightweight deep learning model for precise crop disease detection and robust image-level privacy protection. Optimized for resource-constrained edge devices, it ensures real-time, high-precision identification of various disease types. Additionally, to secure data transmission, we integrate a novel image encryption scheme based on a 3D chaotic cube, effectively preventing unauthorized access without compromising detection performance. Our model has been comprehensively evaluated on real-world datasets and outperforms existing methods in detection accuracy, computational overhead, and privacy protection. This solution offers a practical and secure pathway for smart agriculture applications. Our approach addresses two key challenges in plant disease detection: data privacy and detection accuracy.

Our main contributions are as follows:

- We propose an encryption model combining SHA-256, a 3D Logistic Map, pixel permutation, and XOR operations, ensuring both strong security and high efficiency. Compared to traditional Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman(RSA), our method offers a larger key space, enhanced attack resistance, and millisecond-level encryption speeds, making it well-suited for edge and mobile devices in agriculture. Security evaluations using entropy, Structural Similarity Index Measure(SSIM), Number of Pixel Change Rate(NPCR), and Unified Average Changing Intensity(UACI) confirm its balanced performance.
- We present a knowledge distillation framework with YOLOv12s as the teacher and YOLOv11n as the student. The distilled student model, YOLOv11n-12D, inherits enhanced detection capabilities while maintaining a lightweight structure. To address class imbalance and improve small lesion detection, Focal Loss and CIoU Loss are incorporated during training. Experimental results show that YOLOv11n-12D outperforms existing lightweight models in precision, recall, F1 score, and mAP, while achieving real-time inference speed.
- We develop an end-to-end system in which farmers encrypt images locally, transmit them wirelessly to a diagnostic

center, and receive encrypted detection results. This framework ensures data security and scalability across various crop scenarios, effectively integrating deep learning and encryption technologies. The overall architecture is shown in Figure 1.

The rest of this paper is organized as follows: Section 2 reviews related work. Section 3 details the encryption method. Section 4 introduces the detection model. Section 5 describes data processing and optimization. Section 6 presents experiments and analysis. Section 7 concludes the paper.Section 8 highlights the system's significance, practical value, and limitations.

2 Related work

Traditional encryption algorithms such as AES and DES are inadequate for real-time protection of agricultural images due to high dimensionality, redundancy, and computational overhead associated with such data. Although deep learning has achieved success in plant disease detection tasks, most existing studies overlook privacy concerns during image transmission and processing. To contextualize the proposed integrated system, this section reviews key image encryption techniques and plant disease detection approaches.

2.1 Data encryption techniques

In response to the need for secure image transmission in agriculture, several encryption techniques have been developed, each aiming to balance security and efficiency. Key representative methods are summarized below. Niyat et al. (2017) proposed an encryption scheme based on non-uniform cellular automata (CA) and hyper-chaotic mapping, enhancing key space and attack resistance. Kulalvaimozhi et al. (2020) introduced a method combining homomorphic encryption (NHE) and enhanced discrete wavelet transform (EDWT), improving both security and compression efficiency. Priyanka et al. (2024) employed 3D chaotic mapping and Huffman coding for medical image encryption. Sha et al. (2024) developed an IoT-oriented image encryption scheme utilizing graph data structures and logic gate mechanisms to strengthen attack protection. Ding et al. (2022) proposed a GAN-based key generation model, significantly improving key security.

Devi et al. (2024) proposed a DWT-SVD watermarking and PSMD symmetric encryption scheme to enhance UAV image security. While effective, its reliance on symmetric keys may pose challenges in key management and attack resistance. Zhou et al. (2024) applied compressed sensing and a two-dimensional hyperchaotic coupled Fourier oscillator system (2D-HCFOS) to improve encryption speed and security, achieving promising simulation results. Chen et al. Zhou et al. (2025) introduced a 2D super-attractor Logistic coupled chaotic model (2D-SALC), outperforming existing methods in chaos and security metrics. However, further validation, including integration with YOLO models and assessment of encryption impact on detection accuracy, remains needed.

2.2 Deep learning-based disease monitoring

Deep learning has shown strong results in plant disease detection Attri et al. (2023), with notable performance across crops like rice, wheat, tomato, and grape. Jia et al. (2023) improved YOLOv7 for rice pest detection by integrating MobileNetV3 and coordinate attention, achieving 92.3% accuracy and 93.7% mAP@0.5. However, its performance in complex

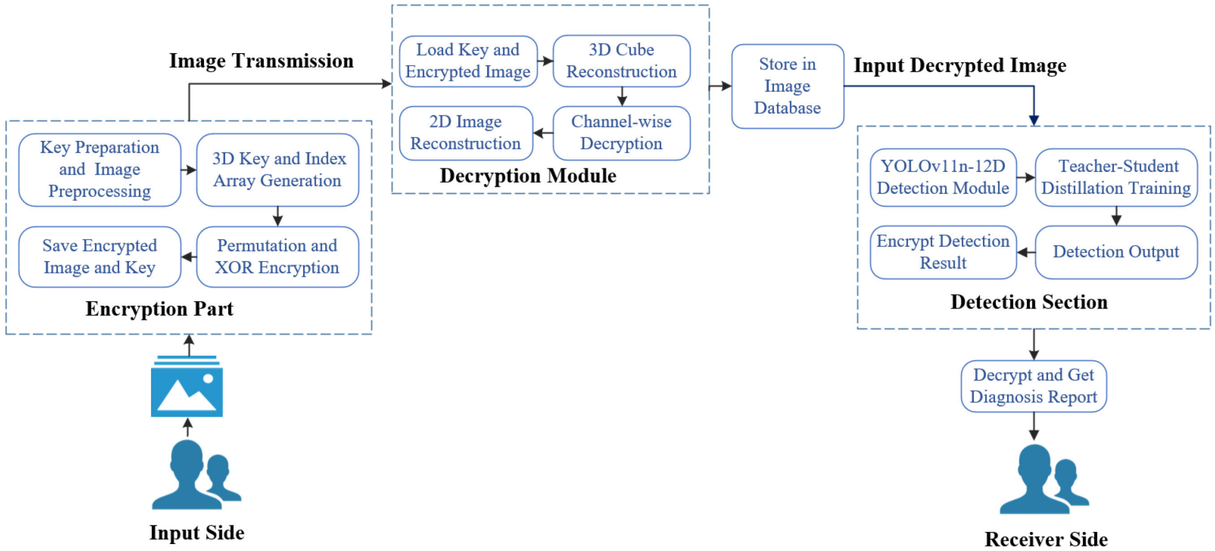
Image Transmission
Key Preparation and Image Preprocessing
3D Key and Index Array Generation
Save Encrypted Image and Key
Permutation and XOR Encryption
Encryption Part
Input Side
Load Key and Encrypted Image
3D Cube Reconstruction
2D Image Reconstruction
Channel-wise Decryption
Decryption Module
Store in Image Database
Input Decrypted Image
YOLOv11n-12D Detection Module
Teacher-Student Distillation Training
Encrypt Detection Result
Detection Output
Detection Section
Decrypt and Get Diagnosis Report
Receiver Side

FIGURE 1
Overview of the process.

backgrounds still faces challenges. To address this, Deng et al. (2023) enhanced YOLOv5s and YOLOv7-tiny models for better accuracy and speed, enabling mobile deployment. Liu and Wang (2020) optimized YOLOv3 with an image pyramid for better multi-scale detection in tomato disease recognition. Zhang et al. (2023) proposed RYWD and SSA networks for wheat Fusarium head blight detection, improving accuracy and precision by 11.8% and 10.7%. Wu et al. (2023) combined YOLOv5 with HRNet for grape stem localization, achieving 92% accuracy in bunch detection and 90.2% in stem recognition. While these methods show improvements, their performance under complex field conditions still requires further refinement.

For eggplant disease detection, Liu et al. (2025b) enhanced YOLOv8n with the YOLO-RDM model, improving accuracy and robustness. Huang et al. (2024) proposed YOLOv8-E, which enhanced detection accuracy and small target recognition while reducing computational complexity. MR et al. Haque and Sohel (2022) used a dual-stream architecture combining CNN-SVM and CNN-Softmax, outperforming traditional models. Despite these advances, challenges remain in achieving high accuracy, robustness, and data security.

Despite significant progress in image encryption and plant disease detection, several critical gaps remain. Most existing studies treat encryption and detection as separate processes, lacking a unified solution that simultaneously ensures privacy protection and detection accuracy. Moreover, few works consider the resource constraints of real-time processing on edge devices. Many YOLO-based methods either overlook the impact of encryption on feature extraction or employ models that are too heavy for mobile deployment. Therefore, there is a need for a unified lightweight framework that guarantees image security while enabling efficient disease detection. To address this gap, we propose an integrated system that combines 3D chaotic cube encryption with the YOLOv11n-12D detection model, aiming to enhance both detection performance and data security.

3 3D chaotic cube encryption scheme

In eggplant disease detection, image encryption is essential for data security by preventing unauthorized access, tampering, and maintaining integrity. Ciphertext transmission enhances system security and reduces the risk of cyberattacks. This section presents a novel image encryption method based on a 3D Chaotic Cube Encryption Scheme, which consists of four steps: preparation of the key and image, generation of 3D key and index array, permutation encryption and XOR operation, and save the encrypted image and key. Compared to frequency- and chaos-based methods (Jui-Cheng and Guo, 2000; Armand Eyebe Fouda et al., 2014; Jammula et al., 2022), the proposed scheme offers stronger resistance to attacks and superior performance. Figure 2 illustrates the encryption framework, and Figure 3 shows the original and encrypted eggplant images.

3.1 Preparation of the key and image

Prior to encryption, a 64-bit hexadecimal key and the target image are provided. The key is then processed using a hash function to generate the initial values for the chaotic system. The provided 64-bit hexadecimal string key hex is first converted into binary, and its SHA-256 hash value is computed: H_K=SHA-256(key_hex). Assume the original image *img* has a size of 128 × 128. Extract the R, G, and B channels separately as R(*i,j*), G(*i,j*), and B(*i,j*), where *i,j* ∈ {0,127}. The result is as shown in Equations 1–3. Then expand the image into a 128 × 128 × 128 3D cube and *K* ∈ {0,127}:

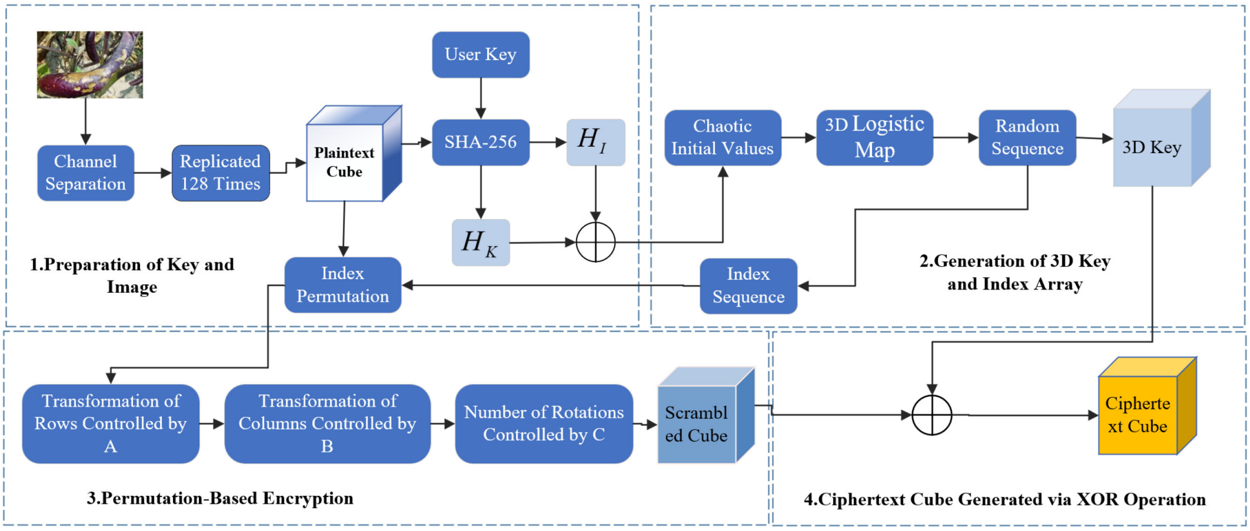
User Key
Channel Separation
Replicated 128 Times
Plaintext Cube
SHA-256
H_I
H_K
1.Preparation of Key and Image
Index Permutation
Chaotic Initial Values
3D Logistic Map
Random Sequence
3D Key
Index Sequence
2.Generation of 3D Key and Index Array
Transformation of Rows Controlled by A
Transformation of Columns Controlled by B
Number of Rotations Controlled by C
Scrambled Cube
3.Permutation-Based Encryption
Ciphertext Cube
4.Ciphertext Cube Generated via XOR Operation

FIGURE 2
Encryption flowchart.

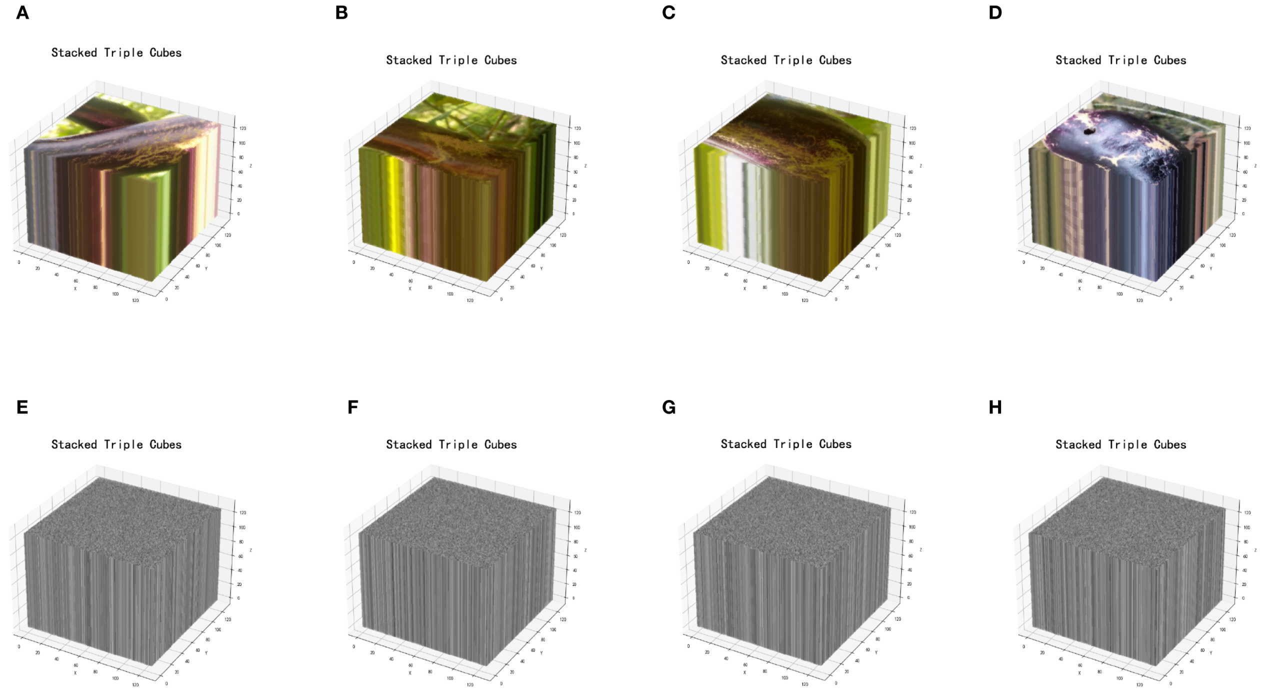

FIGURE 3
(A-D) show the original images, **(E-H)** display the encrypted images.

$$C_R(i,j,k) = R(i,j) \tag{1}$$

$$C_G(i,j,k) = G(i,j) \tag{2}$$

$$C_B(i,j,k) = B(i,j) \tag{3}$$

The three channel cubes are concatenated into a one-dimensional bitstream. The image hash is then computed as shown in Equation 4:

$$H_I = \text{SHA}-256(\text{img}) \tag{4}$$

To initialize the chaotic system, extract the first, middle, and last 64 bits from the bitstream, convert them into decimal values x_0,y_0,z_0, and normalize each to the range (0,1). These values are used as initial conditions for the chaotic system, x_0,y_0,z_0 as defined in Equations 5–7:

$$x_0 = \frac{\text{int}(H_K[0:16], 16)}{2^{64}} \tag{5}$$

$$y_0 = \frac{\text{int}(H_K[16:32], 16)}{2^{64}} \tag{6}$$

$$z_0 = \frac{\text{int}(H_K[48:64], 16)}{2^{64}} \tag{7}$$

3.2 Generation of 3D key and index array

- To generate chaotic sequences, the 3D Logistic Map is employed with the following initial conditions, as defined in Equations 8–10:

$$x_1 = r_x \cdot x_0 \cdot (1 - x_0) + \beta \cdot y_0 \cdot z_0 \tag{8}$$

$$y_1 = r_y \cdot y_0 \cdot (1 - y_0) + \gamma \cdot x_0 \cdot z_0 \tag{9}$$

$$z_1 = r_z \cdot z_0 \cdot (1 - z_0) + \alpha \cdot x_0 \cdot y_0 \tag{10}$$

Then use x_1, y_1, z_1 in the equations again to calculate the next values of x_2,y_2,z_2 repeat this process to generate a chaotic sequence array as shown in Equations 11–13:

$$x_{n+1} = r_x \cdot x_n \cdot (1 - x_n) + \beta \cdot y_n \cdot z_n \tag{11}$$

$$y_{n+1} = r_y \cdot y_n \cdot (1 - y_n) + \gamma \cdot x_n \cdot z_n \tag{12}$$

$$z_{n+1} = r_z \cdot z_n \cdot (1 - z_n) + \alpha \cdot x_n \cdot y_n \tag{13}$$

Here, r_x,r_y,r_z ∈ (3, 57, 4), Take the values from the chaotic interval. These α, β, γcontrol the coupling degree of the system. The 3D Logistic Map is iterated one million times, and the initial steps are discarded to eliminate transient effects. This process generates three long chaotic sequences. Figure 4 shows the resulting random sequences, chaotic sequences as defined in Equations 14–16:

$$X = \{x_1, x_2, \ldots, x_N\} \tag{14}$$

$$Y = \{y_1, y_2, \ldots, y_N\} \tag{15}$$

$$Z = \{z_1, z_2, \ldots, z_N\} \tag{16}$$

Map the values to the range [0, 255] to form the 3D key: $K(x,y,z) = [X(x,y,z) \times 256]$.

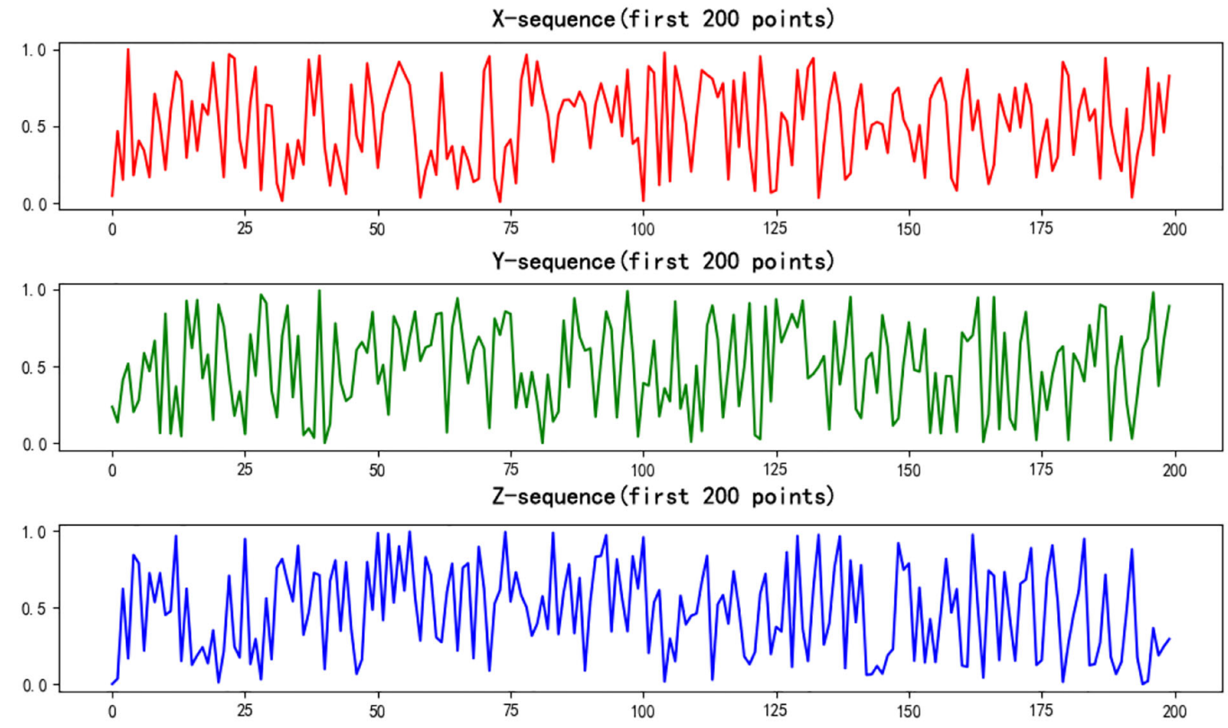

FIGURE 4
Random sequence numbers.

- To construct the index arrays, X is sorted to obtain A = argsort(X), and Y is sorted to obtain B = argsort(Y), Z is normalized to the range [0, 3], which is used for rotation: C = [Z × 4].

3.3 Permutation encryption and XOR operation

- First, apply index-based permutation to the 3D cube using arrays A and B to reorder rows and columns, respectively. Specifically, perform row permutation as: $C_R \rightarrow (:, A, :)$, $C_G \rightarrow (:, A, :)$, $C_B \rightarrow (:, A, :)$, and column permutation: $C_R \rightarrow (B, :, :)$, $C_G \rightarrow (B, :, :)$, $C_B \rightarrow (B, :, :)$. and rotation based on the value of C, rotate each layer $C(i, j)$ times 90°. The result as shown in Equations 17–19:

$$\mathbf{C}_R(:, :, i) = \mathrm{Rotate}(\mathbf{C}_R(:, :, i), \mathbf{C}(i, j)) \tag{17}$$

$$\mathbf{C}_G(:, :, i) = \mathrm{Rotate}(\mathbf{C}_G(:, :, i), \mathbf{C}(i, j)) \tag{18}$$

$$\mathbf{C}_B(:, :, i) = \mathrm{Rotate}(\mathbf{C}_B(:, :, i), \mathbf{C}(i, j)) \tag{19}$$

- Next, complete the encryption by performing a bitwise XOR operation between the permuted 3D cube and the 3D key: $C'_R = C_R \oplus K, \quad C'_G = C_G \oplus K, \quad C'_B = C_B \oplus K$

3.4 Save the encrypted image and key

The encrypted 3D cube is converted back into a 2D color image by mapping the corresponding values to the RGB channels as shown in Equations 20–22:

$$\mathrm{R}'(i, j) = \mathrm{C}'_R(i, j, 0), \tag{20}$$

$$\mathrm{G}'(i, j) = \mathrm{C}'_G(i, j, 0), \tag{21}$$

$$\mathrm{B}'(i, j) = \mathrm{C}'_B(i, j, 0) \tag{22}$$

These channels are combined to generate the final encrypted image enc_img, which is saved to a file. The index arrays A, B, C, along with the key file key_bin, are stored for decryption.

3.5 Decryption process

To enable proper visualization and subsequent detection, the encrypted image must be decrypted. The decryption process involves four steps: load the key and encrypted image, reconstruct the 3D cube, decrypt each channel, and rebuild the 2D image.

3.5.1 Load the key and encrypted image

The decryption process begins by loading the 3D key and index arrays (A, B, C) from the file system, along with the encrypted image file.

3.5.2 Reconstruct the 3D cube

Each color channel (R, G, B) of the image is reshaped into a 128 × 128 × 128 3D cube, where the first two dimensions represent pixel positions and the third dimension corresponds to the stacked image layers.

3.5.3 Decrypt each channel

For each color channel's 3D cube, two operations are applied:

- Bitwise XOR Restoration: The cube is first restored by applying a bitwise XOR operation with the original 3D key used during encryption.
- Reverse Rotation: Then, reverse rotations are performed based on the index arrays A and B. Array A controls the reversal along rows, and B controls the columns. The rotation direction is opposite to the encryption process. The number of 90° rotations is determined by the values in array C, applied in reverse order to maintain symmetry.

3.5.4 Rebuild the 2D image

The decrypted 3D cubes of the R, G, and B channels are converted back into 2D images. These channels are then merged to reconstruct the final color image, which is output as the decrypted result.

4 YOLOV11N-12D model

Deep learning-based object detection has demonstrated remarkable performance in disease recognition, with the YOLO series widely used for its speed and accuracy (Dai et al., 2022; Wang et al., 2024; Xie et al., 2024). However, traditional YOLO models struggle when dealing with small objects and class imbalance (Obu et al., 2023; A.N. and A.P., 2022). To address these issues, we propose an enhanced lightweight model, YOLOv11n-12D. As shown in Figure 5, the architecture consists of four components: Stem, Backbone, Neck, and Head. In our model, YOLOv11n serves as the student model, while YOLOv12s acts as the teacher. By leveraging knowledge distillation and detection loss, we enhance recall, reduce missed detections, and maintain efficiency, making it suitable for large-scale agricultural applications. The distillation process is detailed in Figure 6.

The following are the steps of the distillation process:

a. The pre-trained YOLOv11n is used as the student model, and YOLOv12s as the teacher. Z_*t* and Z_*s* are defined as shown in Equations 23, 24: Augmented samples are input into both models to compute their respective logits:

$$Z_t = \text{TeacherModel}(X) \tag{23}$$

$$Z_s = \text{StudentModel}(X) \tag{24}$$

Since logits vary significantly in magnitude, a temperature parameter $T = 4.0$ is applied to smooth them, stabilize gradients, and generate soft labels for distillation.

b. Temperature scaling ($T = 4.0$) is applied to smooth the logits and obtain softened probability distributions for effective knowledge transfer as shown in Equations 25, 26:

$$P_t = \text{softmax}\left(\frac{Z_t}{T}\right) \tag{25}$$

$$P_s = \text{softmax}\left(\frac{Z_s}{T}\right) \tag{26}$$

When $T = 1.0$, the distribution reduces to standard softmax, limiting the ability to learn from the teacher. We adopt Kullback-Leibler divergence as the distillation loss: Distillation Loss = $T^2 \times$ KL ($p_t \parallel p_s$). Here, T^2 offsets the gradient scaling effect caused by smoothing. A smaller KL value indicates better alignment between the student and teacher outputs, KL as defined in Equation 27:

$$\text{KL}(\mathbf{p}t \parallel \mathbf{p}s) = \sum i(\mathbf{p}t)_i \cdot \log\left(\frac{(\mathbf{p}t)i}{(\mathbf{p}s)i}\right) \tag{27}$$

c. The student model is trained to balance knowledge from the teacher and performance on the original task. To achieve this, the detection loss and distillation loss are combined with a weighted sum: TotalLoss = $(1 - \alpha) \times$ (Detection Loss) + $\alpha \times$ (Distillation Loss). Mixed precision training, learning rate scheduling, and early stopping strategies are employed to improve efficiency and convergence.

d. The detection loss consists of a weighted sum of classification loss (Focal Loss) and regression loss (CIoU Loss):Detection Loss=Focal Loss + CIoU Loss, A weight of $\alpha = 0.7$ is used to emphasize the distillation loss. The learning rate is adjusted using the OneCycleLR policy as shown in Equation 28:

$$\text{LR}(t) = \begin{cases} \text{LR}_{\max} \times \frac{t}{t_{up}} & \text{if } t \leq t_{\text{up}} \\ \text{LR}_{\max} \times \left(1 - \frac{t - t_{up}}{t_{down}}\right) & \text{if } t > t_{\text{up}} \end{cases} \tag{28}$$

e. Training is terminated using an early stopping strategy when the condition specified in Equation 29 is met.

$$\text{if Patience Count} \geq 10, \text{stop training} \tag{29}$$

After each epoch,the validation set is evaluated using mAP, Precision, and Recall to monitor the effectiveness of the distillation strategy on student model performance.

5 Materials preparation and optimization methods

To ensure high efficiency and accuracy in eggplant disease detection, a large-scale dataset was constructed, encompassing four categories: eggplant rot, fruit borer, healthy samples, and thrips. All images were annotated in YOLO format with

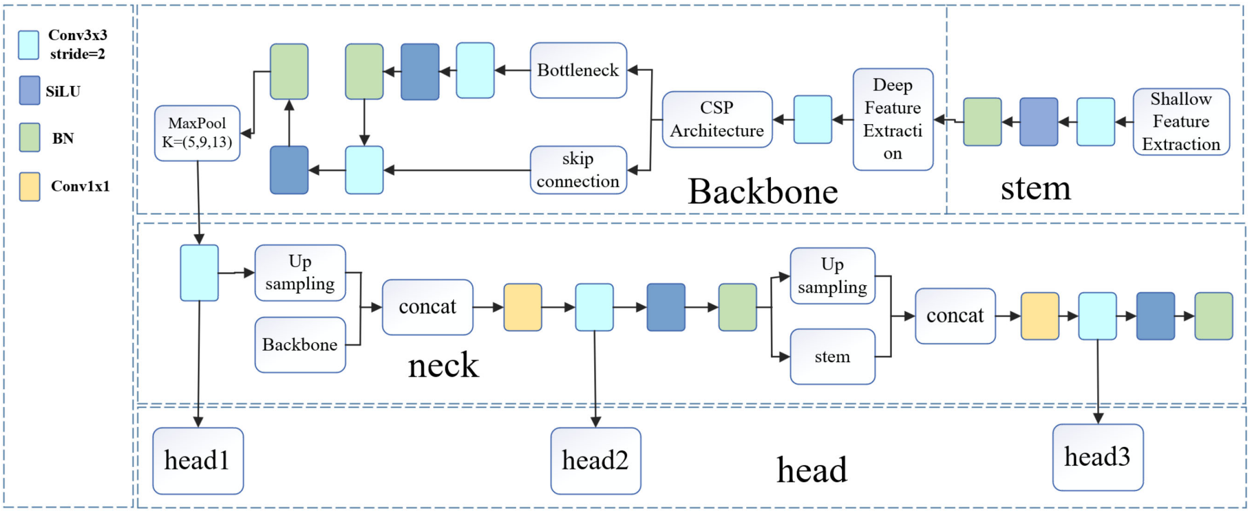

FIGURE 5
Detection model architecture.

standardized bounding boxes and precise class labels. The annotations were reviewed by agricultural experts to ensure high-quality and consistent labeling.The dataset was collected from multiple eggplant cultivation bases, encompassing various growth cycles, diverse lighting conditions, and all developmental stages of pest/disease infestation (from initial infection to characteristic symptom manifestation). Specifically, the test set comprises 745 representative images (containing 1516 annotated instances), while the remaining 7520 images were partitioned into training (5264 images) and validation (2256 images) sets at a 7:2:1 ratio. This scientifically designed partitioning scheme ensures both sufficient training data volume and reliable evaluation of model generalization capability. Sample differences between healthy and diseased eggplants are shown, highlighting the visual variability between categories (Figure 7). To address the limited quantity and variable quality of the collected raw images, we employed the Albumentations data augmentation library to enhance dataset diversity and improve model generalization and robustness (Buslaev et al., 2020; Korra et al., 2022). The overall workflow for material preparation and optimization is illustrated (Figure 8), and the specific data augmentation strategies are detailed as follows:

- Random Flip: Applies horizontal and vertical flips to simulate different viewing angles, enhancing feature recognition and robustness.
- Color Jitter: Alters brightness, contrast, and saturation to mimic various lighting conditions.
- Random Crop: Generates new samples by cropping image regions, helping reduce reliance on specific areas.

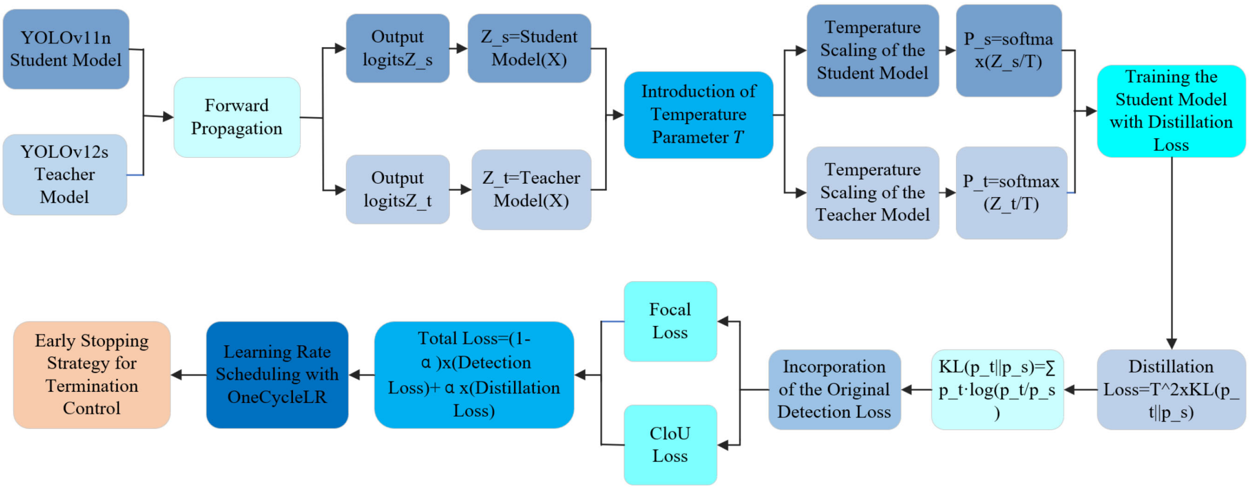
YOLOv11n Student Model
YOLOv12s Teacher Model
Forward Propagation
Output logitsZ_s
Z_s=Student Model(X)
Output logitsZ_t
Z_t=Teacher Model(X)
Introduction of Temperature Parameter T
Temperature Scaling of the Student Model
P_s=softma x(Z_s/T)
Temperature Scaling of the Teacher Model
P_t=softmax (Z_t/T)
Training the Student Model with Distillation Loss
Distillation Loss=T^2xKL(p_ t||p_s)
KL(p_t||p_s)=∑ p_t·log(p_t/p_s)
Incorporation of the Original Detection Loss
Focal Loss
CIoU Loss
Total Loss=(1- α)x(Detection Loss)+ α x(Distillation Loss)
Learning Rate Scheduling with OneCycleLR
Early Stopping Strategy for Termination Control

FIGURE 6
Knowledge distillation process flow.

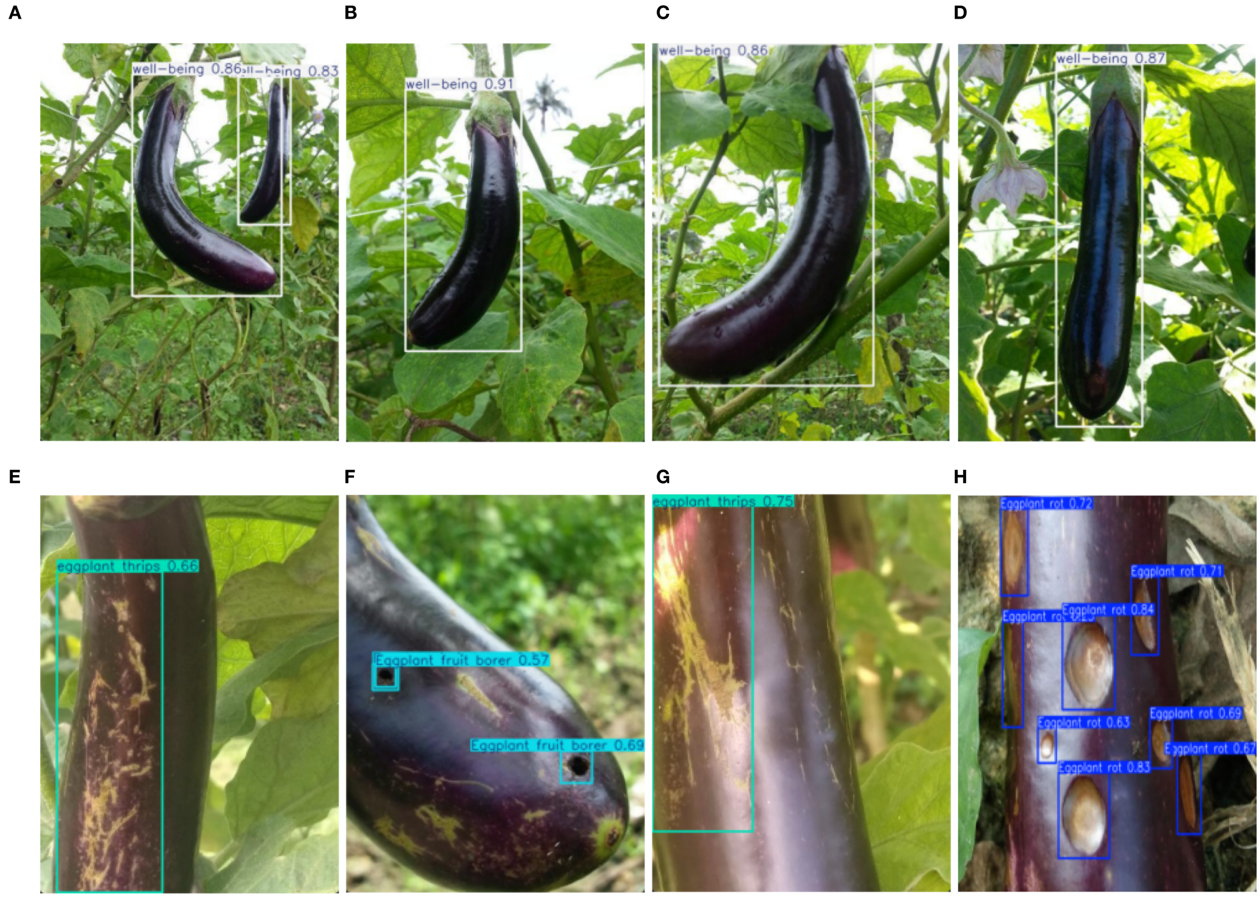

FIGURE 7
(A-D) are healthy eggplant images, **(E-H)** are diseased eggplant images.

- Random Rotation: Rotates images within ±30° to improve viewpoint diversity and reduce angle bias.
- Random Noise Addition: Introduces Gaussian or salt-and-pepper noise to improve performance under degraded image conditions.
- Mosaic Augmentation: Merges multiple images to enrich contextual and visual diversity in complex scenes.
- MixUp Augmentation: Blends two images and labels to promote smooth label transition and mitigate overfitting.

The applied augmentation techniques significantly enhance the model's robustness and generalization, allowing more reliable recognition of eggplant disease features under diverse conditions. Furthermore, the integration of Focal Loss and CIoU Loss improves detection accuracy, achieving a final accuracy of 99.1% and effectively reducing the miss detection rate, thereby improving applicability in real-world agricultural scenarios.

5.1 Focal loss

Focal Loss is designed to address class imbalance, especially in single-stage detectors like RetinaNet. Traditional cross-entropy is dominated by easy negatives, causing unstable training. Focal Loss introduces a modulation factor to focus learning on hard examples, improving detection of minority classes.The construction of this function is shown in part (a) of Figure 8. For a binary label: $y \in \{0,1\}$ (0 for positive class and 1 for negative class), the predicted probability pt is defined as Equation 30:

$$\mathrm{p}_t = \begin{cases} p & \text{if } y = 1 \\ 1 - p & \text{if } y = 0 \end{cases} \tag{30}$$

The standard cross-entropy loss is: $\mathrm{CE} = -\log(\mathrm{p}_t)$, Calculate the weight decay factor $(1 - \mathrm{p}_t)^{\gamma}$, $\gamma$is Hyperparameters, Typically takes values of 2 or 3, when p_t is small,the decay factor approaches 1 when p is small; otherwise, it approaches 0. A balancing factor is introduced to control the ratio of positive to negative samples. The final Focal Loss as presented in Equation 31:

$$\mathrm{FL} = -\alpha(1 - \mathrm{p}_t)^{\gamma} \log(\mathrm{p}_t) \tag{31}$$

To compute the average Focal Loss for all samples in a batch, the classification loss is: Focal Loss $= \frac{1}{N}\sum_{i=1}^{N} \mathrm{FL}(\mathrm{p}_t^{(i)})$

5.2 CIoU loss

CIoU Loss is primarily used for object bounding box regression, especially in the context of rotated object detection. It optimizes the

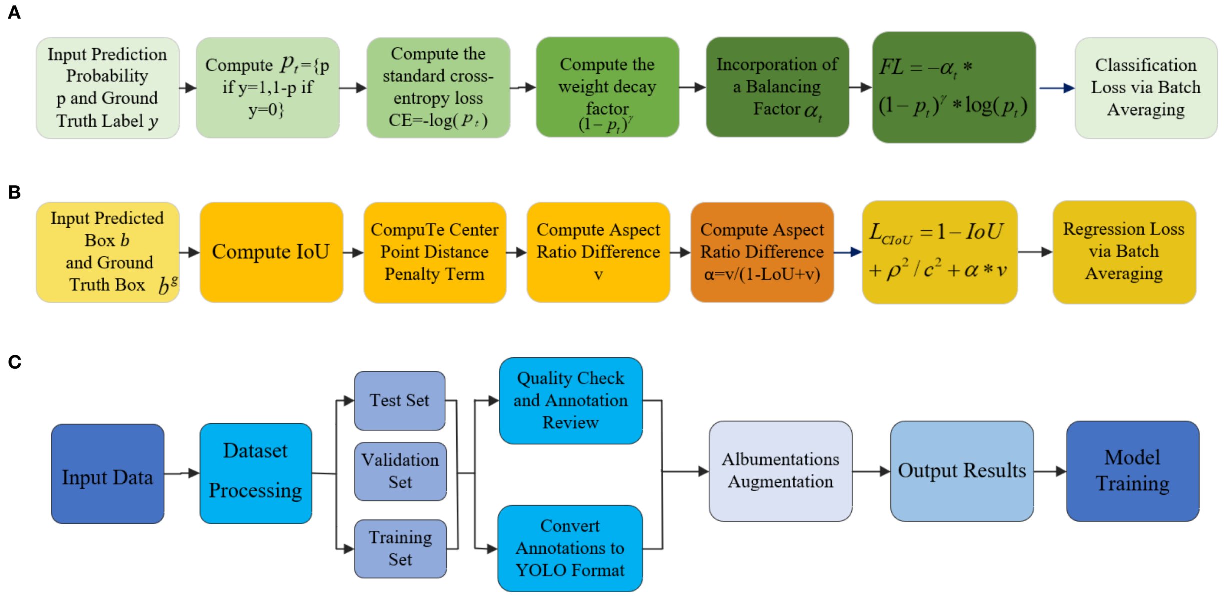
A
Input Prediction Probability p and Ground Truth Label y
Compute p_t={p if y=1,1-p if y=0}
Compute the standard cross-entropy loss CE=-log(p_t)
Compute the weight decay factor $(1-p_t)^\gamma$
Incorporation of a Balancing Factor α_t
$FL=-\alpha_t * (1-p_t)^\gamma * \log(p_t)$
Classification Loss via Batch Averaging
B
Input Predicted Box b and Ground Truth Box b^g
Compute IoU
CompuTe Center Point Distance Penalty Term
Compute Aspect Ratio Difference v
Compute Aspect Ratio Difference α=v/(1-LoU+v)
$L_{CIoU}=1-IoU+\rho^2/c^2+\alpha*v$
Regression Loss via Batch Averaging
C
Input Data
Dataset Processing
Test Set
Validation Set
Training Set
Quality Check and Annotation Review
Convert Annotations to YOLO Format
Albumentations Augmentation
Output Results
Model Training

FIGURE 8
Diagram of materials analysis and optimization. **(A)** Focal loss. **(B)** CIoU loss. **(C)** Material preparation and optimization.

accuracy of the bounding box's location, size, and angle. CIoU Loss was introduced to improve the detection accuracy of rotated objects, as traditional bounding box regression methods typically only consider rectangular boxes, while CloU Loss also accounts for the angle of the rotated boxes. CloU Loss optimizes the bounding box regression of object detection models by considering the center point error, size error (width and height), and rotation angle error. The construction of this function is shown in part (b) of Figure 8. Calculate the Intersection over Union (IoU) between the predicted box b and the ground truth box b^g. As shown in Equation 32:

$$\mathrm{IoU} = \frac{\text{Intersection Area}}{\text{Union Area}} \tag{32}$$

Calculate the Euclidean distance between the center of the predicted box and the center of the ground truth box, as defined in Equation 33:

$$\rho^2(b, b^g) = (x - x^g)^2 + (y - y^g)^2 \tag{33}$$

c can represent the diagonal distance of the smallest enclosing box that contains both the predicted box and the ground truth box as shown in Equation 34: Distance penalty term:

$$\frac{\rho^2(\mathrm{b}, \mathrm{b}^g)}{c^2} \tag{34}$$

Measure the difference in aspect ratio between the predicted box and the ground truth box, as defined in Equation 35:

$$V = \frac{4}{\pi^2}\left(\arctan\frac{w^g}{h^g} - \arctan\frac{w}{h}\right)^2 \tag{35}$$

Adaptive weight α is primarily used to balance the contribution of the aspect ratio loss term v in the overall CIoU loss. The result as shown in Equation 36:

$$\alpha = \frac{v}{(1 - \mathrm{IoU}) + v} \tag{36}$$

By combining IoU, center distance, and aspect ratio, the final CIoU Loss is obtained as shown in Equation 37:

$$\mathcal{L}_{\mathrm{CIoU}} = 1 - \mathrm{IoU} + \frac{\rho^2(\mathbf{b}, \mathbf{b}^g)}{c^2} + \alpha v \tag{37}$$

6 Performance analysis

This section presents the evaluation metrics used to assess the performance of the two core components of the proposed system: the 3D chaotic cube-based encryption scheme for image security, and the YOLOv11n-12D-based detection model for eggplant disease diagnosis.

6.1 Analysis of the proposed encryption scheme

To evaluate our encryption scheme, we developed a quantitative assessment system for image encryption security (Table 1). It uses seven key indicators: contrast and mean square error (positively correlated) indicate pixel perturbation; information entropy shows randomness; while structural similarity (SSIM), energy value, homogeneity, and structural content (negatively correlated) assess structural damage, pattern concealment, and pixel disorder. This framework is based on research by Gupta and Chauhan (2021); Rahman et al. (2025), and Karmakar et al. (2021).

TABLE 1 Evaluation parameters and their relation with image encryption security.

P.	M.E.	R.W.S.S.	V.E.
Contrast	$\text{Contrast} = \sum_{a,b} \lvert a-b \rvert^2 \, O(a,b)$	Contrast $\propto$ S.S	Higher contrast reduces predictability and enhances security.
SSIM	$SSIM = (2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)/(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)$	SSIM $\propto \frac{1}{\text{S . S}}$	Lower SSIM prevents structural leakage, improving security.
MSE	$MSE = \frac{1}{N}\sum_{i=1}^{N}(I_1(i) - I_2(i))^2$	MSE $\propto$ S.S	Higher MSE increases difference, making decryption harder.
Entropy	$\text{Entropy} = -\sum_{i=0}^{255} p_i \times \log_2(p_i)$	Entropy $\propto$ S.S	Higher entropy means more randomness, improving security.
Energy	$\text{Energy} = \sum_{a,b}[O(a,b)]^2$	Energy $\propto \frac{1}{\text{S . S}}$	Lower energy hides patterns, strengthening security.
Homogeneity	$\text{Homogeneity} = \sum_{a,b}\frac{O(a,b)}{1 + \lvert a-b \rvert}$	Homogeneity $\propto \frac{1}{\text{S . S}}$	Lower homogeneity increases pixel chaos, improving security.
SC	$\text{SC} = \frac{\sum(\text{original image}^2)}{\sum(\text{original} - \text{encrypted})^2}$	SC $\propto \frac{1}{\text{S . S}}$	Lower SC means less similarity to the original, enhancing security.

P, Parameter; M.E., Mathematical Equation; R.W.S.S., Relationship with Strong Security (S.S); V.E., Variable Explanation.

Table 2 shows that our method outperforms existing technologies (Huang et al., 2025; Xu et al., 2024; Ullah et al., 2025) in encryption quality, security, and efficiency. By integrating chaotic sequence generation, pixel permutation, and XOR encryption, our solution maintains consistent performance metrics for all test samples (both healthy and diseased eggplants). The entropy value is 7.6195 (close to the theoretical maximum of 8), and the pixel correlation coefficient is −0.0084 (close to 0). Our method achieves high image fidelity (40.26 dB) and fast encryption speed (0.0127 seconds), which is 23 times faster than the fastest comparative method. It also preserves key features for disease identification, meeting smart agriculture's requirements for real-time performance, security, and feature preservation.

6.2 Key space analysis

The key space, representing the total number of possible keys, is a critical factor in resisting brute-force attacks. In this scheme, the user key is a 64-character hexadecimal string, corresponding to 256 bits. As each hex character encodes 4 bits, the key space size is: $2^{256} \approx 1.16 \times 10^{77}$. Such a vast key space is computationally infeasible to exhaust. Even at 10^{18} keys per second, a brute-force search would take: $\frac{1.16\times10^{77}}{10^{18}\times60\times60\times24\times356} \approx 3.67 \times 10^{50}$ year. These results confirm that the proposed key space is computationally infeasible to exhaust via brute-force attacks.

6.3 Attack resistance analysis

6.3.1 Known-Plaintext attack

The proposed scheme uses a 3D Logistic Map, which exhibits strong sensitivity to initial conditions—tiny variations lead to drastically different outputs. The chaotic system evolves as shown in Equation 38:

$$x_{n+1} = \mathrm{r} \cdot x_n \cdot (1 - x_n) + \beta \cdot y_n \cdot z_n \tag{38}$$

Chaotic behavior is verified by the Lyapunov exponent, as defined in Equation 39:

$$\lambda = \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\ln\left|\frac{df(x_i)}{dx_i}\right| \tag{39}$$

A positive exponent $\lambda > 0$, indicates exponential divergence. In our experiments, $\lambda = 0.89$ confirms high sensitivity, making it extremely difficult to reverse-engineer the key, even with known plaintext–ciphertext pairs. This divergence is described as defined in Equation 40:

$$\Delta x_n = \Delta x_0 \cdot \mathrm{e}^{\lambda n} \tag{40}$$

To initialize the chaotic system, we apply the SHA-256 hash function to the user key. With its strong collision resistance and irreversibility, the probability of a successful brute-force match is negligible, as defined in Equation 41:

$$P = \frac{1}{2^{256}} \tag{41}$$

6.3.2 Differential attack: NPCR

NPCR evaluates how a minor change in the input affects the encrypted output. It is defined as: $\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W\times H} \times 100\,\%$. $D(i,j)$ as defined in Equation 42:

$$D(i,j) = \begin{cases} 1 \ \text{ if } \mathrm{C}_1(i,j) \neq \mathrm{C}_2(i,j) \\ 0 \ \text{ if } \mathrm{C}_1(i,j) = \mathrm{C}_2(i,j) \end{cases} \tag{42}$$

Here, $\mathrm{C}_1(i,j)$ and $\mathrm{C}_2(i,j)$ denote the pixel values of two encrypted images with slight input differences. The ideal NPCR approaches 100%.

6.3.3 Differential attack: UACI

UACI quantifies the average intensity difference between two encrypted images, as shown in Equation 43:

TABLE 2 Comparative performance analysis of eggplant image encryption methods.

Proposed work (encrypted images)							
Image type	Homogeneity	SC	Entropy	Correlation	Energy	Contrast	Execution time (s)
Healthy 1	0.0158	0.6381	7.6195	−0.0084	0.0001	4905.8639	0.0160
Healthy 2	0.0158	0.8239	7.6195	−0.0084	0.0001	4905.8639	0.0124
Healthy 3	0.0158	0.4249	7.6195	−0.0084	0.0001	4905.8639	0.0131
Healthy 4	0.0158	0.3750	7.6195	−0.0084	0.0001	4905.8639	0.0127
Diseased 1	0.0158	**0.9212**	7.6195	−0.0084	0.0001	4905.8639	**0.0111**
Diseased 2	0.0158	0.5680	7.6195	−0.0084	0.0001	4905.8639	0.0119
Diseased 3	0.0158	0.6245	7.6195	−0.0084	0.0001	4905.8639	0.0112
Diseased 4	0.0158	0.6458	7.6195	−0.0084	0.0001	4905.8639	0.0131
Mean	**0.0158**	**0.6277**	**7.6195**	**-0.0084**	**0.0001**	**4905.8639**	**0.0127**
Existing methods comparison							
Method	MSE	PSNR	Entropy	Correl.	Energy	Contrast	Execution Time (s)
15	5170.0723	10.9958	7.1346	−0.0707	0.0001	2706.7328	2.0395
41	8778.5593	8.6966	7.6232	0.2083	0.0001	3970.8332	0.2992
45	8256.4317	8.9629	**7.7475**	−0.0854	0.0000	**6158.4497**	0.8220
Ours	**0.158**	**40.2623**	7.6195	**-0.0084**	**0.0001**	4905.8639	**0.0127**

Bold values are representative or key results.

$$\mathrm{UACI} = \frac{1}{W \times H} \sum_{i,j} \frac{|\mathrm{C}_1(i,j) - \mathrm{C}_2(i,j)|}{255} \times 100\,\% \tag{43}$$

The ideal value should be close to 33%. Experimental results show: *NPCR* = 99.63%, *UACI* = 32.85%, These values confirm high resistance to differential attacks and strong sensitivity to input perturbations. Figure 9 compares the pixel distribution: the original image (left) shows structured patterns, while the encrypted image (right) displays uniform randomness, demonstrating visual and statistical security.

6.4 Statistical analysis

6.4.1 Histogram analysis

Figure 10 illustrates the grayscale distributions of the original and encrypted images. The original image shows a clear peak in pixel intensity, while the encrypted image exhibits a nearly uniform distribution with no apparent structure. This indicates that the encryption process effectively randomizes the statistical properties of the original image, eliminating pixel concentration and preventing histogram-based attacks.

6.4.2 Pixel autocorrelation analysis

The Pearson correlation coefficient measures the linear relationship between adjacent pixel values and defined as in Equation 44:

$$r = \frac{\sum (x_i - \mu_x)(y_i - \mu_y)}{\sqrt{\sum (x_i - \mu_x)^2 \sum (y_i - \mu_y)^2}} \tag{44}$$

Ideally, $r \approx 0$ indicates no correlation. In our experiment, r =0.005, confirming that the encrypted image lacks linear pixel dependencies, which enhances its resistance to statistical attacks.

6.5 Detection performance evaluation

This study evaluated the YOLOv11n-12D model using Tables 3, 4, confirming its innovative breakthroughs. Table 3 highlights the model's superior performance in detecting four eggplant diseases: rot (mAP@0.5=0.861), fruit borer (0.872), healthy plants (0.911), and notably thrips (0.753), a 6.5% improvement over the baseline. It achieves accuracy comparable to YOLOv12s (gap <2%) via knowledge distillation while remaining lightweight. Table 4 provides a comprehensive performance comparison. The model maintains near-teacher accuracy (1.2% mAP@0.5 difference) and achieves a 2.7ms inference speed—3.6× faster than YOLOv12s (9.6ms) and 3.2× faster than YOLOv8n (8.7ms). Its F1-Score (0.804) outperforms YOLOv10n (0.764) and YOLOv8n (0.785), with a 4.5% improvement in the stricter mAP@0.5:0.95 metric, demonstrating stability in multi-scale detection.

Comprehensive analysis of data from both tables demonstrates that YOLOv11n-12D, through the synergistic optimization of

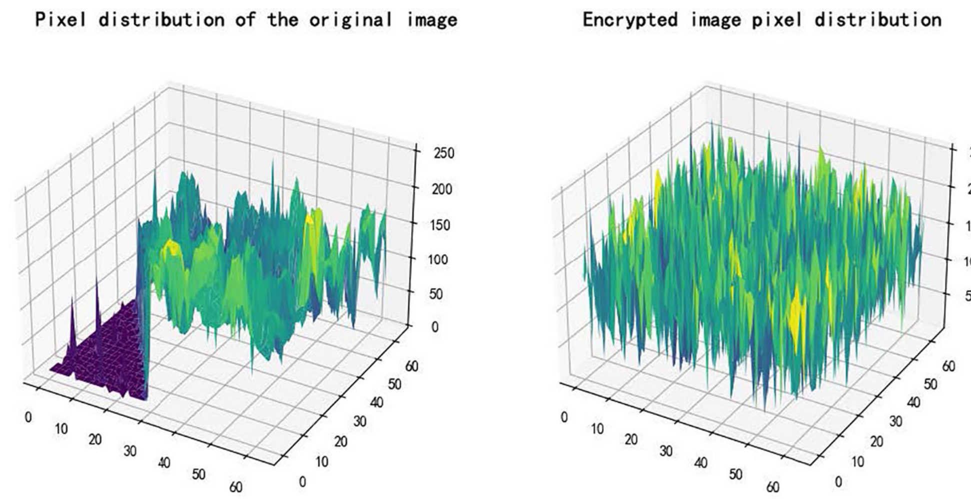

FIGURE 9
Pixel analysis diagram.

knowledge distillation and Focal Loss, successfully overcomes the traditional trade-off between accuracy and efficiency, achieving the innovative breakthrough of “teacher-level accuracy with edge-level efficiency” and providing reliable technical support for real-time disease detection in smart agriculture.

6.6 Information entropy analysis

The formula for information entropy as defined in Equation 45:

$$H(X) = -\sum_{i=0}^{255}\mathbf{p}(x_i)\log_2 p(x_i) \quad (\text{Information entropy (unit: bit)}) \tag{45}$$

The entropy of the original image ranges from 5 to 7, while the encrypted image’s entropy is close to 8 (theoretical maximum), showing a more uniform and random pixel distribution. Our calculated entropy value is 7.6195, indicating high information entropy, which helps prevent information leakage and statistical analysis attacks.

7 Conclusion

This paper proposes an integrated system for eggplant disease detection that combines image encryption and deep learning-based recognition. The system employs a lightweight encryption scheme based on 3D chaotic mapping and pixel permutation to secure image transmission with low computational overhead. It then utilizes an optimized YOLOv11n-12D model to process the decrypted images, achieving high detection accuracy and real-time performance. A teacher–student knowledge distillation

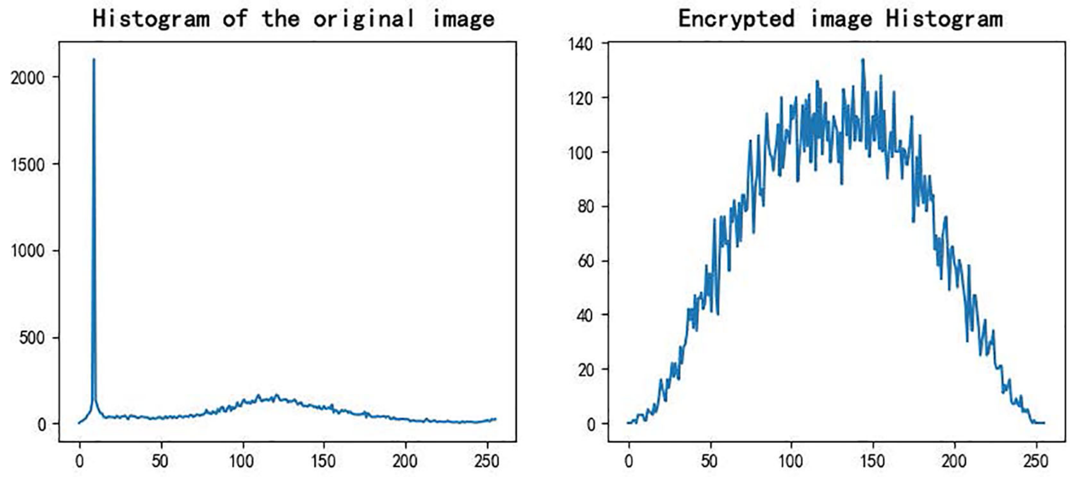

FIGURE 10
Image grayscale distribution.

TABLE 3 Performance comparison of YOLO models for eggplant disease detection.

Model	Category	Dataset		Performance metrics			
		Images	Instances	Precision	Recall	mAP@0.5	mAP@0.5:0.95
YOLOv11n-12D	Eggplant Rot	117	544	0.838	0.814	**0.861**	0.565
	Eggplant Fruit	237	323	**0.861**	0.819	**0.872**	0.407
	Healthy	216	331	0.871	0.886	**0.911**	0.725
	Eggplant Thrips	175	318	0.752	0.643	**0.753**	0.442
YOLOv11n-12D Unencrypted (Baseline)	Eggplant Rot	117	544	0.838	0.814	**0.861**	0.565
	Eggplant Fruit	237	323	0.861	0.819	**0.872**	0.407
	Healthy	216	331	0.871	0.886	**0.911**	0.725
	Eggplant Thrips	175	318	0.752	0.643	**0.753**	0.442
yolov11n	Eggplant Rot	117	544	0.838	0.724	0.822	0.552
	Eggplant Fruit	237	323	0.826	0.807	0.850	0.395
	Healthy	216	331	0.861	0.891	**0.924**	0.728
	Eggplant Thrips	175	318	0.810	0.575	0.707	0.411
yolov12s	Eggplant Rot	117	544	0.852	0.827	0.873	0.582
	Eggplant Fruit	237	323	0.879	0.831	0.884	0.418
	Healthy	216	331	**0.883**	0.901	0.922	**0.741**
	Eggplant Thrips	175	318	0.765	0.659	0.767	0.456
yolov10n	Eggplant Rot	117	544	0.805	0.706	0.781	0.502
	Eggplant Fruit	237	323	0.821	0.768	0.826	0.384
	Healthy	216	331	0.852	**0.904**	0.910	0.719
	Eggplant Thrips	175	318	0.770	0.505	0.672	0.397
yolov8n	Eggplant Rot	117	544	0.820	0.750	0.817	0.524
	Eggplant Fruit	237	323	0.859	0.794	0.857	0.408
	Healthy	216	331	0.815	**0.907**	0.917	0.717
	Eggplant Thrips	175	318	0.781	0.566	0.697	0.399

Bold values are representative or key results.

strategy is incorporated to further enhance model robustness. Experimental results demonstrate that the system not only safeguards data privacy but also outperforms existing methods in accuracy, speed, and stability, offering a reliable solution for smart agriculture. At the same time,our future research will focus on enabling disease detection directly on encrypted images to eliminate the risk of data leakage during decryption. This will involve exploring privacy-preserving techniques like homomorphic

TABLE 4 Comprehensive performance comparison.

Model version	Precision	Recall	mAP@0.5	mAP@0.5:0.95	F1-score	Inference speed (ms)
YOLOv11n-12D	0.831	0.791	0.849	0.535	0.804	**2.7**
YOLOv11n	0.834	0.749	0.826	0.522	0.789	3.3
YOLOv12s	**0.845**	**0.804**	**0.861**	**0.549**	**0.812**	9.6
YOLOv10n	0.812	0.721	0.797	0.501	0.764	3.1
YOLOv8n	0.819	0.754	0.822	0.512	0.785	8.7

Bold values are representative or key results.

encryption and designing lightweight models that can operate effectively in the encrypted domain.

8 Discussion

Our study proposes a framework that integrates image encryption with deep learning based object detection for real time, privacy-preserving crop disease monitoring. The designed 3D chaotic cube encryption scheme demonstrates strong security performance, achieving high entropy (7.6195), low pixel correlation (0.0084), and strong resistance to statistical and differential attacks (NPCR = 99.63%, UACI = 32.85%). Meanwhile, the YOLOv11n-12D model retains the detection performance of the teacher model while achieving fast inference speed (2.7 ms), with a notable mAP improvement of +6.5% in small-object detection such as eggplant thrips. This solution offers a promising approach for advancing smart agriculture in rural or resource limited areas. By encrypting images before transmission and decrypting them only during model inference, the framework strikes a practical balance between data security and operational efficiency. Its compatibility with edge devices further supports deployment in real world scenarios, where data privacy, bandwidth limitations, and low computing resources are common challenges. Despite the promising results, the current framework still requires decryption before detection, which introduces a temporary risk of data exposure. Future work will focus on privacy preserving deep learning techniques that support inference directly in the encrypted domain, such as homomorphic encryption or secure multi party computation. Further validation on larger and more diverse crop datasets is also needed to assess generalization. Enhancing the interpretability of both the detection model and the encryption process will help improve transparency and user trust in practical applications.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material. Further inquiries can be directed to the corresponding author.

Author contributions

JH: Writing – original draft, Funding acquisition, Methodology. ZW: Writing – original draft. YD: Writing – review & editing, Conceptualization. YG: Data curation, Writing – original draft. RF: Investigation, Writing – review & editing, Supervision.

Funding

The author(s) declare financial support was received for the research and/or publication of this article. This research was supported by the Weifang University of Science and Technology A-Class Doctoral Research Fund (Grant No. KJRC2024014), Shan dong Provincial Natural Science Foundation (Grant No. ZR2025QC649), and the Weifang University of Science and Technology A-Class Doctoral Research Fund (Grant No. KJRC2024006).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

A.N., A., and A.P., S. (2022). Lightweight and computationally faster hypermetropic convolutional neural network for small size object detection. *Image Vision Computing* 119, 104396. doi: 10.1016/j.imavis.2022.104396

Armand Eyebe Fouda, J., Yves Effa, J., Sabat, S. L., and Ali, M. (2014). A fast chaotic block cipher for image encryption. *Commun. Nonlinear Sci Numerical Simulation* 19, 578–588. doi: 10.1016/j.cnsns.2013.07.016

Attri, I., Awasthi, L. K., Sharma, T. P., and Rathee, P. (2023). A review of deep learning techniques used in agriculture. *Ecol. Inf.* 77, 102217. doi: 10.1016/j.ecoinf.2023.102217

Baldi, P., and La Porta, N. (2020). Molecular approaches for low-cost point-of-care pathogen detection in agriculture and forestry. *Front. Plant Sci* 11, 570862. doi: 10.3389/fpls.2020.570862

Buslaev, A., Iglovikov, V. I., Khvedchenya, E., Parinov, A., Druzhinin, M., and Kalinin, A. A. (2020). Albumentations: Fast and flexible image augmentations. *Information* 11, 125. doi: 10.3390/info11020125

Cornia, G. A. (1985). Farm size, land yields and the agricultural production function: An analysis for fifteen developing countries. *World Dev.* 13, 513–534. doi: 10.1016/0305-750X(85)90054-3

Dai, Y., Liu, W., Wang, H., Xie, W., and Long, K. (2022). Yolo-former: Marrying yolo and transformer for foreign object detection. *IEEE Trans. Instrumentation Measurement* 71, 1–14. doi: 10.1109/TIM.2022.3219468

Deng, J., Yang, C., Huang, K., Lei, L., Ye, J., Zeng, W., et al. (2023). Deep-learning-based rice disease and insect pest detection on a mobile phone. *Agronomy* 13, 2139. doi: 10.3390/agronomy13082139

Devi, K. J., Singh, P., Bilal, M., and Nayyar, A. (2024). Enabling secure image transmission in unmanned aerial vehicle using digital image watermarking with h-grey optimization. *Expert Syst. Appl.* 236, 121190. doi: 10.1016/j.eswa.2023.121190

Ding, Y., Tan, F., Qin, Z., Cao, M., Choo, K.-K. R., and Qin, Z. (2022). Deepkeygen: A deep learning-based stream cipher generator for medical image encryption and decryption. *IEEE Trans. Neural Networks Learn. Syst.* 33, 4915–4929. doi: 10.1109/tnnls.2021.3062754

Elijah, O., Rahman, T. A., Orikumhi, I., Leow, C. Y., and HIndia, M. N. (2018). An overview of internet of things (iot) and data analytics in agriculture: Benefits and challenges. *IEEE Internet Things J.* 5, 3758–3773. doi: 10.1109/JIOT.2018.2844296

Gupta, M. D., and Chauhan, R. (2021). Secure image encryption scheme using 4d-hyperchaotic systems based reconfigurable pseudo-random number generator and s-box. *Integration* 81, 137–159. doi: 10.1016/j.vlsi.2021.07.002

Haque, M. R., and Sohel, F. (2022). Deep network with score level fusion and inference-based transfer learning to recognize leaf blight and fruit rot diseases of eggplant. *Agriculture* 12, 1160. doi: 10.3390/agriculture12081160

He, M., Qin, L., Deng, X., and Liu, K. (2024). Mfi-yolo: Multi-fault insulator detection based on an improved yolov8. *IEEE Trans. Power Delivery* 39, 168–179. doi: 10.1109/TPWRD.2023.3328178

Huang, Y., Zhang, Q., and Zhao, Y. (2025). Color image encryption algorithm based on hybrid chaos and layered strategies. *J. Inf. Secur. Appl.* 89, 103921. doi: 10.1016/j.jisa.2024.103921

Huang, Y., Zhao, H., and Wang, J. (2024). Yolov8-e: An improved yolov8 algorithm for eggplant disease detection. *Appl. Sci. (2076-3417)* 14. doi: 10.3390/app14188403

Jammula, M., Vakamulla, V. M., and Kondoju, S. K. (2022). Retracted: Artificial intelligence framework-based ultra-lightweight communication protocol for prediction of attacks in internet of things environment. *Trans. Emerging Telecommunications Technol.* 34. doi: 10.1002/ett.4680

Jia, L., Wang, T., Chen, Y., Zang, Y., Li, X., Shi, H., et al. (2023). Mobilenet-ca-yolo: An improved yolov7 based on the mobilenetv3 and attention mechanism for rice pests and diseases detection. *Agriculture* 13, 1285. doi: 10.3390/agriculture13071285

Jui-Cheng,, and Guo, J.-I. (2000). "A new chaotic key-based design for image encryption and decryption," in *2000 IEEE International Symposium on Circuits and Systems (ISCAS).* Piscataway, NJ, USA: IEEE, Vol. 4. 49–52. doi: 10.1109/ISCAS.2000.858685

Karmakar, J., Pathak, A., Nandi, D., and Mandal, M. K. (2021). Sparse representation based compressive video encryption using hyper-chaos and dna coding. *Digital Signal Process.* 117, 103143. doi: 10.1016/j.dsp.2021.103143

Kethineni, K., and Gera, P. (2023). Iot-based privacy-preserving anomaly detection model for smart agriculture. *Systems* 11. doi: 10.3390/systems11060304

Korra, S., Mamidi, R., Soora, N. R., Kumar, K. V., and Kumar, N. C. S. (2022). Intracranial hemorrhage subtype classification using learned fully connected separable convolutional network. *Concurrency Computation: Pract. Exp.* 34. doi: 10.1002/cpe.7218

Kulalvaimozhi, V., Alex, M. G., and Peter, S. J. (2020). A novel homomorphic encryption and an enhanced dwt (nhe-edwt) compression of crop images in agriculture field. *Multidimensional Syst. Signal Process.* 31, 367–383. doi: 10.1007/s11045-019-00660-9

Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Gadekallu, T. R., and Srivastava, G. (2021). Sp2f: A secured privacy-preserving framework for smart agricultural unmanned aerial vehicles. *Comput. Networks* 187, 107819. doi: 10.1016/j.comnet.2021.107819

Li, K., Zhu, X., Qiao, C., Zhang, L., Gao, W., and Wang, Y. (2023a). The gray mold spore detection of cucumber based on microscopic image and deep learning. *Plant Phenomics* 5, 11. doi: 10.34133/plantphenomics.0011

Li, X., Sun, W., Ji, Y., Dai, Y., and Huang, W. (2023b). "Joint detection and tracking for compact hfswr," in *OCEANS 2023 - Limerick.* Piscataway, NJ, USA: IEEE. 1–4. doi: 10.1109/OCEANSLimerick52467.2023.10244275

Li, X., Sun, W., Ji, Y., Dai, Y., and Huang, W. (2024). "Reinforcement learning based joint detection and tracking of target for compact hfswr," in *OCEANS 2024 - Singapore.* Piscataway, NJ, USA: IEEE. doi: 10.1109/OCEANS51537.2024.10682213

Li, X., Sun, W., Ji, Y., and Huang, W. (2025). A joint detection and tracking paradigm based on reinforcement learning for compact hfswr. *IEEE J. Selected Topics Appl. Earth Observations Remote Sens.* 18, 1995–2009. doi: 10.1109/JSTARS.2024.3504813

Lin, J., Yu, D., Pan, R., Cai, J., Liu, J., Zhang, L., et al. (2023). Improved yolox-tiny network for detection of tobacco brown spot disease. *Front. Plant Sci* 14, 1135105. doi: 10.3389/fpls.2023.1135105

Liu, H., Ding, Y., Zeng, H., Pu, H., Luo, J., and Fan, B. (2025a). A cascaded multimodule image enhancement framework for underwater visual perception. *IEEE Trans. Neural Networks Learn. Syst.* 36, 6286–6298. doi: 10.1109/TNNLS.2024.3397886

Liu, J., and Wang, X. (2020). Tomato diseases and pests detection based on improved yolo v3 convolutional neural network. *Front. Plant Sci* 11. doi: 10.3389/fpls.2020.00898

Liu, Q., Zhou, Z., Xiong, L., Lu, M., and Ouyang, J. (2025b). Yolo-rdm: Innovative detection methods for eggplants and stems in complex natural environment. *IEEE Access* 13, 37656–37672. doi: 10.1109/ACCESS.2025.3545670

Liu, W., Quijano, K., and Crawford, M. M. (2022). Yolov5-tassel: Detecting tassels in rgb uav imagery with improved yolov5 based on transfer learning. *IEEE J. Selected Topics Appl. Earth Observations Remote Sens.* 15, 8085–8094. doi: 10.1109/JSTARS.2022.3206399

Luo, Y. (2024). "Research on interest region detection of images based on enhanced visual quality," in *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON).* Piscataway, NJ, USA: IEEE. 1–4. doi: 10.1109/NMITCON62075.2024.10699026

Man, Z., Li, J., Di, X., Sheng, Y., and Liu, Z. (2021). Double image encryption algorithm based on neural network and chaos. *Chaos Solitons Fractals* 152, 111318. doi: 10.1016/j.chaos.2021.111318

Niyat, A. Y., Moattar, M. H., and Torshiz, M. N. (2017). Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Optics Lasers Eng.* 90, 225–237. doi: 10.1016/j.optlaseng.2016.10.019

Obu, U., Ambekar, Y., Dhote, H., Wadbudhe, S., Khandelwal, S., and Dongre, S. (2023). "Crop disease detection using yolo v5 on raspberry pi," in *2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN).* Piscataway, NJ, USA: IEEE. 528–533. doi: 10.1109/ICPCSN58827.2023.00092

Priyanka,, Baranwal, N., Singh, K. N., and Singh, A. K. (2024). Yolo-based roi selection for joint encryption and compression of medical images with reconstruction through super-resolution network. *Future Generation Comput. Syst.* 150, 1–9. doi: 10.1016/j.future.2023.08.018

Qin, Z., Yan, J., Ren, K., Chen, C. W., and Wang, C. (2014). "Towards efficient privacy-preserving image feature extraction in cloud computing," in *Proceedings of the 22nd ACM international conference on Multimedia (ACM).* New York, NY, USA: ACM, Vol. 14. 497–506. doi: 10.1145/2647868.2654941

Rahman, S., Uddin, J., Hussain, H., Shah, S., Salam, A., Amin, F., et al. (2025). A novel and efficient digital image steganography technique using least significant bit substitution. *Sci. Rep.* 15. doi: 10.1038/s41598-024-83147-3

Ravì, D., Wong, C., Deligianni, F., Berthelot, M., Andreu-Perez, J., Lo, B., et al. (2017). Deep learning for health informatics. *IEEE J. Biomed. Health Inf.* 21, 4–21. doi: 10.1109/JBHI.2016.2636665

Roy, A. M., and Bhaduri, J. (2022). Real-time growth stage detection model for high degree of occultation using densenet-fused yolov4. *Comput. Electron. Agric.* 193, 106694. doi: 10.1016/j.compag.2022.106694

Sangaiah, A. K., Yu, F.-N., Lin, Y.-B., Shen, W.-C., and Sharma, A. (2024). Uav t-yolo-rice: An enhanced tiny yolo networks for rice leaves diseases detection in paddy agronomy. *IEEE Trans. Network Sci Eng.* 11, 5201–5216. doi: 10.1109/TNSE.2024.3350640

Senthil Pandi, S., Sooraj Nikam, P., Subeash, D., and Kannaiah, S. K. (2024). "Tomato leaf disease detection technique using vgg-19," in *2024 International Conference on Computational Intelligence for Green and Sustainable Technologies (ICCIGST).* Piscataway, NJ, USA: IEEE. 1–6. doi: 10.1109/ICCIGST60741.2024.10717462

Sha, Y., Mou, J., Banerjee, S., and Zhang, Y. (2024). Exploiting flexible and secure cryptographic technique for multidimensional image based on graph data structure and three-input majority gate. *IEEE Trans. Ind. Inf.* 20, 3835–3846. doi: 10.1109/tii.2023.3281659

Ullah, S., Liu, X., Waheed, A., and Zhang, S. (2025). S-box using fractional-order 4d hyperchaotic system and its application to rsa cryptosystem-based color image encryption. *Comput. Standards Interfaces* 93, 103980. doi: 10.1016/j.csi.2025.103980

Wang, L., Cai, J., Wang, T., Zhao, J., Gadekallu, T. R., and Fang, K. (2024). Detection of pine wilt disease using aav remote sensing with an improved yolo model. *IEEE J. Selected Topics Appl. Earth Observations Remote Sens.* 17, 19230–19242. doi: 10.1109/JSTARS.2024.3478333

Wu, Z., Xia, F., Zhou, S., and Xu, D. (2023). A method for identifying grape stems using keypoints. *Comput. Electron. Agric.* 209, 107825. doi: 10.1016/j.compag.2023.107825

Xiao, F., Liu, J., Huang, Y., Cheng, E., and Yuan, F. (2024). Neuromorphic computing network for underwater image enhancement and beyond. *IEEE Trans. Geosci. Remote Sens.* 62, 1–17. doi: 10.1109/TGRS.2024.3473020

Xie, S., Zhou, M., Wang, C., and Huang, S. (2024). Csppartial-yolo: A lightweight yolo-based method for typical objects detection in remote sensing images. *IEEE J. Selected Topics Appl. Earth Observations Remote Sens.* 17, 388–399. doi: 10.1109/jstars.2023.3329235

Xu, Y., Liu, J., You, Z., and Zhang, T. (2024). A novel color image encryption algorithm based on hybrid two-dimensional hyperchaos and genetic recombination. *Mathematics* 12. doi: 10.3390/math12223457

Zhang, D.-Y., Luo, H.-S., Cheng, T., Li, W.-F., Zhou, X.-G., Wei-Guo,, et al. (2023). Enhancing wheat fusarium head blight detection using rotation yolo wheat detection network and simple spatial attention network. *Comput. Electron. Agric.* 211, 107968. doi: 10.1016/j.compag.2023.107968

Zhang, K., Zuo, W., Chen, Y., Meng, D., and Zhang, L. (2017). Beyond a gaussian denoiser: Residual learning of deep cnn for image denoising. *IEEE Trans. Image Process.* 26, 3142–3155. doi: 10.1109/TIP.2017.2662206

Zhang, Y., Ye, M., Zhu, G., Liu, Y., Guo, P., and Yan, J. (2024). Ffca-yolo for small object detection in remote sensing images. *IEEE Trans. Geosci. Remote Sens.* 62, 1–15. doi: 10.1109/TGRS.2024.3363057

Zhou, L., Chen, H., Zhou, X., Yuan, Y., Zhu, W., and Zhou, M. (2025). A smart agriculture image protection scheme based on annealing algorithm and affine transformation is optimized for s-box generated by chaos. *Nonlinear Dynamics* 113, 12263–12287. doi: 10.1007/s11071-024-10677-w

Zhou, L., Xia, H., Lin, Q., Yang, X., Zhang, X., and Zhou, M. (2024). Two-dimensional hyperchaos-based encryption and compression algorithm for agricultural uav-captured planar images. *Sci. Rep.* 14. doi: 10.1038/s41598-024-73050-2