agriculture

MDPI

Article

Research on Blockchain-Based Cereal and Oil Video Surveillance Abnormal Data Storage

Yuan Zhang [1,2,3], Guangyuan Cui [1,2,3], Hongyi Ge [1,2,3,*], Yuying Jiang [1,2,4], Xuyang Wu [1,2,3], Zhenyu Sun [1,2,3] and Zhiyuan Jia [1,2,3]

[1] Key Laboratory of Grain Information Processing & Control, Ministry of Education, Henan University of Technology, Zhengzhou 450001, China; zhangyuan@haut.edu.cn (Y.Z.); cuiguangyuan@stu.haut.edu.cn (G.C.); yyjiang@haut.edu.cn (Y.J.); wuxuyang@stu.haut.edu.cn (X.W.); sunzhenyu@stu.haut.edu.cn (Z.S.); jiazhiyuan@stu.haut.edu.cn (Z.J.)
[2] Henan Provincial Key Laboratory of Grain Photoelectric Detection and Control, Zhengzhou 450001, China
[3] College of Information Science and Engineering, Henan University of Technology, Zhengzhou 450001, China
[4] School of Artificial Intelligence and Big Data, Henan University of Technology, Zhengzhou 450001, China
* Correspondence: gehongyi@haut.edu.cn

Abstract: Cereal and oil video surveillance data play a vital role in food traceability, which not only helps to ensure the quality and safety of food, but also helps to improve the efficiency and transparency of the supply chain. Traditional video surveillance systems mainly adopt a centralized storage mode, which is characterized by the deployment of multiple monitoring nodes and a large amount of data storage. It is difficult to guarantee the data security, and there is an urgent need for a solution that can achieve the safe and efficient storage of cereal and oil video surveillance data. This study proposes a blockchain-based abnormal data storage model for cereal and oil video surveillance. The model introduces a deep learning algorithm to process the cereal and oil video surveillance data, obtaining images with abnormal behavior from the monitoring data. The data are stored on a blockchain after hash operation, and InterPlanetary File System (IPFS) is used as a secondary database to store video data and alleviate the storage pressure on the blockchain. The experimental results show that the model achieves the safe and efficient storage of cereal and oil video surveillance data, providing strong support for the sustainable development of the cereal and oil industry.

Keywords: blockchain; cereal and oil; storage; traceability; deep learning; video surveillance

Citation: Zhang, Y.; Cui, G.; Ge, H.; Jiang, Y.; Wu, X.; Sun, Z.; Jia, Z. Research on Blockchain-Based Cereal and Oil Video Surveillance Abnormal Data Storage. *Agriculture* **2024**, *14*, 23. https://doi.org/10.3390/agriculture14010023

Academic Editors: Kristina Kljak, Klaudija Carović-Stanko, Darija Lemić, Jernej Jakše, Kurt A. Rosentrater, Arup Kumar Goswami and Craig Sturrock

Received: 27 October 2023
Revised: 19 December 2023
Accepted: 21 December 2023
Published: 22 December 2023

1. Introduction

Cereal and oil are necessities of human life and, therefore, it is important to ensure their quality and safety [1]. The large production scale of cereal and oil and their extended temporal and spatial span from cultivation to sale make it difficult to implement effective regulations [2]. Cereal and oil reserves are a key link in the supply chain, and the implementation of a national cereal and oil security strategy requires that the granary be well-guarded and -managed [3]. At present, most grain depots are equipped with omnidirectional video surveillance cameras. Through the remote monitoring of key areas and key grain depots, the information of depots can be viewed at any time to achieve visual supervision.

The grain depot video monitoring system has many monitoring nodes, large video storage, and contains a large amount of detected information [4,5]. Currently, the main problems are as follows: First, most grain depots store data in a centralized way, which forms an information island between different departments and grain depots, making it difficult to effectively share information. Second, cases of tampering, falsification, deletion, etc. can occur during the process of entering the information into the local database,

which makes it difficult to ensure the data's integrity. Third, the massive amount of video surveillance data occupies a large amount of storage space, which can very easily cause a wastage of resources [6,7]. Blockchain technology can effectively solve the aforementioned problems, and research on the storage of video data on a blockchain has become a current hot topic.

Blockchain is a new type of distributed database with the underlying use of hash encryption algorithms, consensus mechanisms, smart contracts, peer-to-peer networks and other core technologies. Consequently, the data uploaded to the blockchain have the characteristics of openness and transparency, tamper resistance, traceability, permanent preservation, etc. [8]. In recent years, many researchers have combined blockchain technology with the food industry [9–14]. The use of blockchain to store data can not only ensure data security, but also promote information interaction between nodes on the blockchain and solve the trust problem caused by centralization. However, the highly redundant storage mechanism of blockchain will cause problems such as a low throughput rate and difficulty in scaling [15–17], which will restrict its development. At present, researchers mainly study the storage scalability of blockchain from two aspects: on-chain capacity expansion [18–20] and off-chain capacity expansion [21–24]. It has been shown that the model incorporating the latter storage scheme enhances the scaling effect of the blockchain more than the former scheme.

Therefore, this paper proposes a blockchain-based cereal and oil video surveillance abnormal data storage model to ensure the security, traceability and anti-tamper robustness of video surveillance data storage. First, a dual storage model based on blockchain and InterPlanetary File System (IPFS) is designed to ensure the safe storage of data and relieve the storage pressure in the blockchain. Second, we study the target detection algorithm based on YOLOv7 [25], and design and implement the anomaly detection model for the video surveillance data of the grain depot. We extract and store the frames with abnormal behaviors in the video, and quickly obtain the video summary while reducing the data redundancy. Last, the FISCO BCOS [26] is deployed and relevant data are uploaded to the chain.

2. Materials and Methods

2.1. Blockchain

Blockchain is a chained data structure that sequentially combines data blocks in a chronological order. Each block is composed of a block header and a block body [27], as shown in Figure 1. Each block header contains the hash value of the previous block, and it is connected to the current block from the genesis block to form a chained data storage structure. The block body includes the number of transactions in the current block and all transaction records generated during the block creation process. These records undergo the Merkel tree hash process to generate a unique Merkel root and are stored in the block header, which ensures that each block is connected chronologically and the transaction data cannot be easily tampered with.

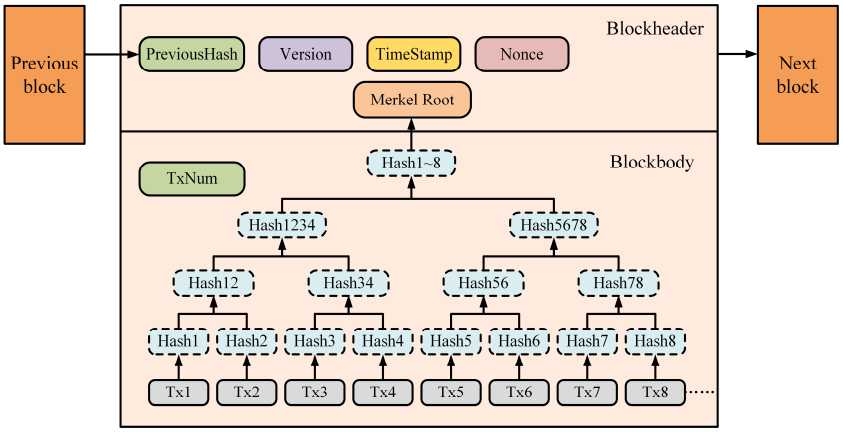

Figure 1. Structure of blocks.

Blockchain is essentially a decentralized database. It is a new application model of computer technology such as distributed data storage, peer-to-peer transmission, consensus mechanism, encryption algorithm and so on. It can ensure the safe storage, transmission and sharing of data, and solve the problems of data silos and information barriers. Currently, there are three main types of blockchains: public, private and consortium blockchain [28]. Table 1 shows the differences between them. Among them, the consortium blockchain is widely used as it is more private and secure compared to the public blockchain, and data sharing is more efficient compared to the private blockchain [29]. In this study, FISCO BCOS consortium blockchain technology is used as the basis for model design and development.

Table 1. Classification of blockchain.

	Public Blockchain	Consortium Blockchain	Private Blockchain
Participant	Anyone	Alliance members	Inside individual organizations
Degree of centralization	Totally decentralized	Partially decentralized	Centralized
Performance	Slow	Fast	Fast
Transaction efficiency	Low	Higher	High
Consensus algorithm	POW, POS	Raft, PBFT	Paxos
Representative Examples	Bitcoin, Ethereum	Hyperledger Fabric, FISCO BCOS	ConsenSys

2.2. IPFS

IPFS [30] is a new hypermedia transport protocol based on content addressing. It generates a corresponding hash fingerprint based on the file contents, which serves as a unique identifier for the file and provides the file storage location. The IPFS has the feature of automatic de-duplication, which considerably reduces the data storage cost. As the IPFS network has servers over many geographic locations, the failure of some servers can be overcome using the backup files of other nodes and, therefore, permanent storage can be achieved.

The files in IPFS use the form of objects to store data, where each object contains data items and link arrays, and the data size is no more than 256 KB [31]. If the data size exceeds 256 KB, it will be split into multiple objects, and subsequently, an upper-level object will be established to summarize the split objects and form a link, as shown in Figure 2.

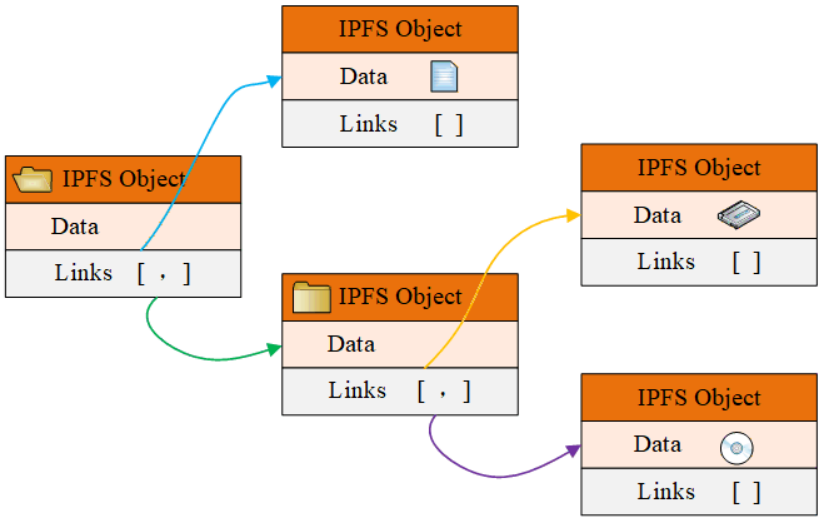

Figure 2. Storage structure of IPFS.

2.3. Inter-Frame Difference

Motion target detection is a very important research direction in video sequence analysis, and also plays an important role in intelligent video surveillance. Various researchers have conducted extensive research on motion target detection methods, and the commonly used methods include inter-frame difference, background subtraction and optical flow analysis [32–34]. Table 2 shows the differences between these algorithms.

Table 2. Comparison of methods for object detection.

Algorithm	Inter-Frame Difference	Background Subtraction	Optical Flow Analysis
Result of the operation	Outer contour of the moving target	Entire area of the movement target	Entire area of the movement target
Complexity of operation	Small	Determined by algorithm complexity	Big
Scope of use	Fixed camera	Fixed camera	Fixed or moving camera
Robustness	Good	Common	Bad

Inter-frame difference method selects two or more adjacent frames in a video image sequence and performs a difference operation to obtain the contour of a moving target. It achieves target detection by utilizing the results of the difference operation of pixels at the corresponding positions in different images [35]. Figure 3 shows the main workflow.

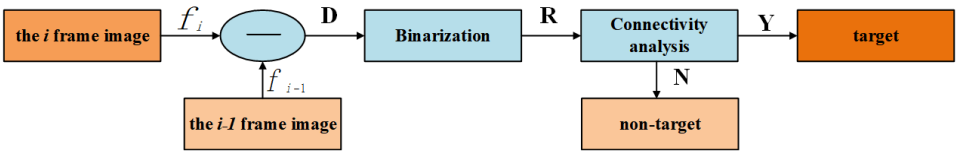

Figure 3. Flowchart of inter-frame difference.

In Figure 3, $f_i(x,y)$ and $f_{i-1}(x,y)$ are the two images collected at time i and time i − 1, respectively. The difference image can be obtained as the following:

$$D_i(x,y) = |f_i(x,y) - f_{i-1}(x,y)| \quad (1)$$

The binarization formula of D_i (x,y) is as follows:

$$R_i(x,y) = \begin{cases} 255, D_i(x,y) < Th \\ 0, D_i(x,y) \geq Th \end{cases} \quad (2)$$

where the points with a gray value of 255 and 0 are the foreground and background points, respectively, and Th is the threshold value. The inter-frame difference method is simple in calculation, fast in detection, has good adaptability to the dynamic environment, and detects distant moving targets effectively in real-time.

2.4. YOLOv7

YOLO is the most typical representation of one-stage target detection algorithms, which uses deep neural networks for object recognition and localization, and runs fast enough to be used in real-time systems [36]. YOLOv7 is the more advanced algorithm of the YOLO series, surpassing the previous YOLO versions in terms of accuracy and speed. The YOLOv7 algorithm framework is mainly composed of input, backbone and head [37], and its structure is shown in Figure 4. At the input, different preprocessing operations such as mosaic data enhancement, adaptive anchor frame computation and image scaling are performed on the input image. The backbone network consists of several CBS modules, ELAN modules and MP modules [38]. The CBS module consists of a Conv layer, BN layer and SiLU layer, and its purpose is to extract features from the image.

The ELAN module consists of several convolutional modules and can learn more features by controlling the shortest and longest gradient paths. The MP module has two branches that perform downsampling. It utilizes max pooling operations to reduce the spatial dimension of the feature maps, effectively capturing essential information at different scales, improving the feature extraction ability of the network. The SPPCSPC structure is composed of spatial pyramid pooling (SPP) and contextual spatial pyramid convolution (CSPC). It divides the features into two parts, one of which is processed by the conventional CBS module, the other part is processed by CBS and max pooling. Finally, these two parts are merged together, which can obtain a higher precision. The head network performs feature processing on the image output from the backbone network. It also uses a path aggregation pyramid network to pass the bottom level information to the higher level along a bottom-up path to efficiently fuse features at different levels [39]. Finally, the number of channels is adjusted by the RepConv structure for features of different scales, providing results of three different sizes.

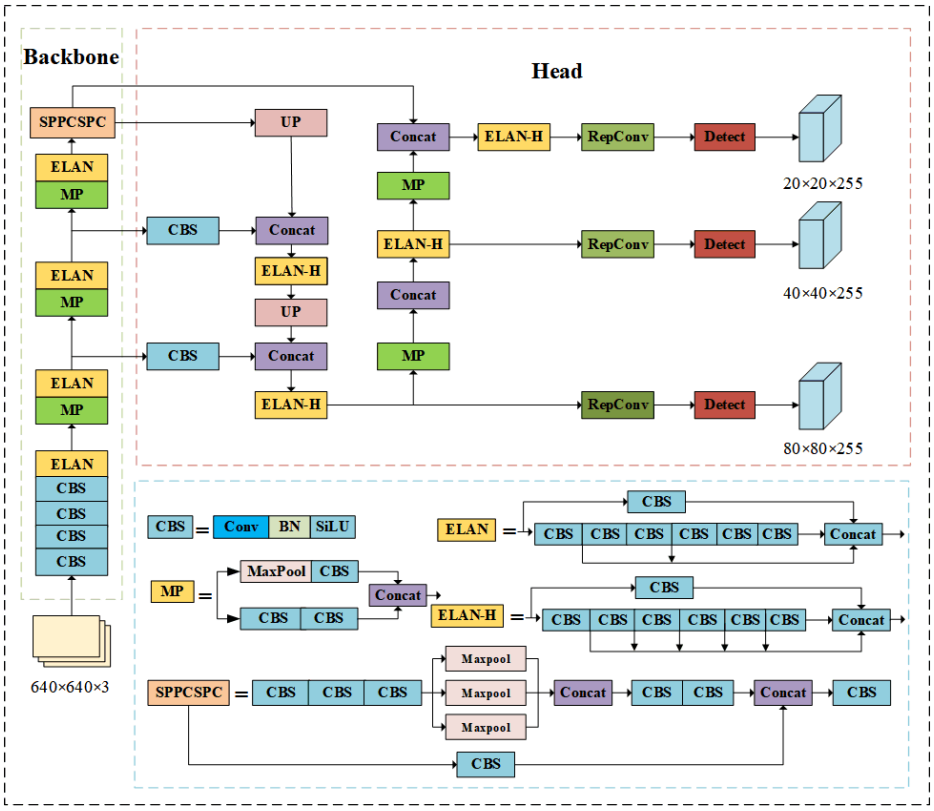

Figure 4. Overall network architecture of YOLOv7.

2.5. Cereal and Oil Video Surveillance Abnormal Data Storage Scheme Based on Blockchain

In this section, a cereal and oil video monitoring abnormal data storage scheme based on blockchain is proposed. The scheme studies the granary video monitoring data in the cereal and oil supply chain. It includes the model construction, target detection model based on the improved YOLOv7, and the dual storage model based on blockchain and IPFS. Table 3 illustrates the symbols used in the scheme and their respective meanings.

Table 3. List of symbols and their meanings.

Symbol	Meaning of Symbol
GVSD	Grain video surveillance data
KF	KeyFrames of video
DU	Data user

SD	Supervision department
IPFS	InterPlanetary File System
CID	Unique identifier of the file returned by IPFS
ID	Identity of block
Hash(.)	Hash value of data
PK(.)	Public key
SK(.)	Private key
Sign_SK(.)	Sign with the private key

As Figure 5 shows, the model consists of five entities: the monitoring device, the data user, the FISCO BCOS, the IPFS and the regulator. The surveillance device consists of a wireless self-organizing local area network of camera sensor nodes, which transmit the video stream to the data client. The data user represents the person within each depot who manages the video surveillance data of the grain depot. The FISCO BCOS and IPFS provide a decentralized storage platform for data users. The supervision department has the right to view the video monitoring data of each library point in the case of emergencies.

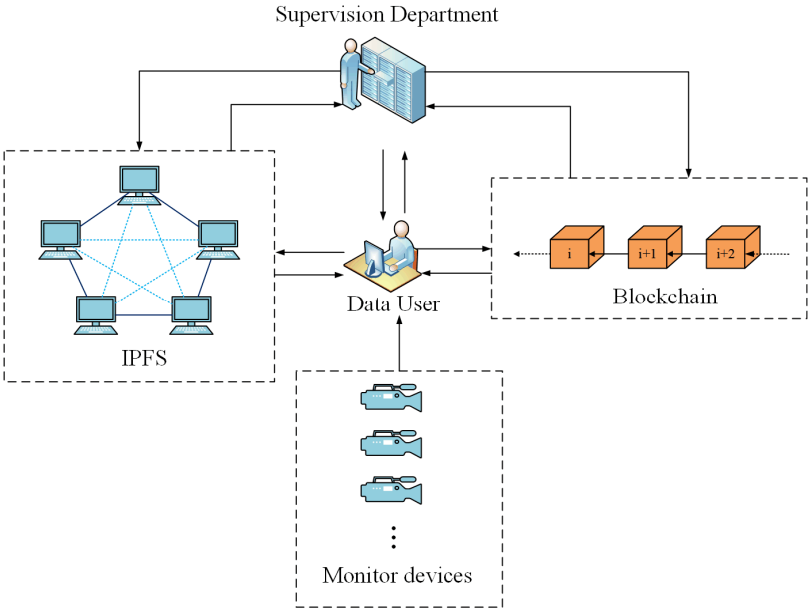

Figure 5. Model structure.

There are a variety of abnormal behaviors in grain depots such as not wearing a safety helmet, unauthorized personnel entering and exiting, and the unsafe operation of equipment. Hazards such as unstable grain accumulation and operation of machinery and equipment may cause accidental injuries to operators. As head protection equipment, safety helmets can effectively protect workers from falling objects, splashing debris and other injuries, reduce or avoid potential safety hazards to the workers' safety, and help to maintain the safe operation of grain depots. Thus, this paper takes the abnormal behaviors of not wearing safety helmets as the research object. This scheme uses the improved YOLOv7 algorithm to process the video surveillance data. It extracts and encrypts the video frames with abnormal behavior, i.e., without safety helmet, without tooling, etc., and stores the encrypted summarized information on the blockchain without storing the all the video data, which can effectively reduce the storage pressure on the block. The IPFS system stores the original video data and ensures its security. The proposed scheme achieves the safe and efficient storage of video surveillance data in the grain depot through a variety of technologies, which can effectively assist the supervisory authorities in investigating and handling emergencies.

2.5.1. Target Detection Model Based on Improved YOLOv7 Algorithm

Figure 6 shows the basic flow of the model. The data user first extracts the key frames in the grain depot video surveillance data using the inter-frame difference method. Subsequently, it uses the improved YOLOv7 algorithm to construct a target detection model, through which the images of personnel without helmets in the surveillance video are obtained.

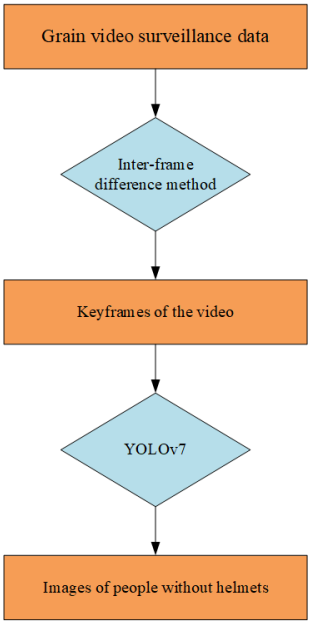

Figure 6. Process of extracting video summaries.

Due to the existence of a large amount of redundant information in video surveillance, this experiment uses the target detection method based on inter-frame difference to extract the key frames in the video, which improves the detection efficiency. There are three methods for threshold selection in the inter-frame difference, which are the maximum value of the difference intensity, the preset difference intensity, and the local maximum value of the difference intensity.

In order to intuitively compare the extraction performance of the above methods, some of the detected images are selected for comparison, as shown in Figures 7–9. The threshold selection methods are used to extract video data with a length of 32 min and 8 s, and the corresponding times are 26.91 s, 32.83 s and 23.63 s. Figure 9 shows that the extraction results obtained using the differential intensity local maxima as the threshold are the best: They are evenly dispersed in the video, and are representative to a certain extent. Therefore, in this paper, the frame with an average inter-frame differential intensity local maximum is selected as the key video frame.

Figure 7. The extraction performance of using differential intensity maxima.

Figure 8. The extraction performance of using preset differential intensity.

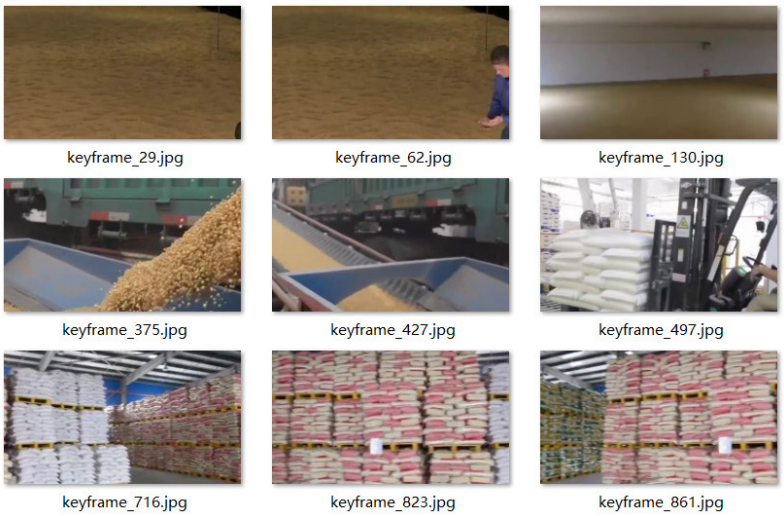

Figure 9. The extraction performance of using differential intensity local maxima.

In this study, the personnel without safety helmets in the grain depot are considered as the research target. A target detection model based on the improved YOLOv7 algorithm

is proposed to meet the real-time requirements and improve the detection accuracy. The YOLOv7 loss function contains the classification loss, the confidence loss and the localization loss. Out of these, the classification loss and confidence loss adopt the binary cross-entropy loss function, and the localization loss adopts the CIoU loss function, which is defined in (3) and (4).

$$\mathrm{CIoU} = \mathrm{IoU} - \frac{\rho^2(\mathrm{b},\mathrm{b}^{\mathrm{gt}})}{\mathrm{c}^2} - \alpha\mathrm{v} \tag{3}$$

$$\mathrm{Loss}_{\mathrm{CIoU}} = 1 - \mathrm{IoU} + \frac{\rho^2(\mathrm{b},\mathrm{b}^{\mathrm{gt}})}{2} + \alpha\mathrm{v} \tag{4}$$

where $\frac{\rho^2(\mathrm{b},\mathrm{b}^{\mathrm{gt}})}{\mathrm{c}^2}$ is the penalty term, b and b^{gt} represent the center point of the prediction box and the real box, respectively, ρ represents the Euclidean distance between the two points, and c represents the diagonal distance of the minimum external matrix formed by the prediction box and the real box. Furthermore, α is a balance parameter, and v is used to measure the consistency of the width-to-height ratio. These parameters are defined as follows:

$$\alpha = \frac{\mathrm{v}}{1-\mathrm{IoU}+\mathrm{v}} \tag{5}$$

$$\mathrm{v} = \frac{4}{\pi^2}\left(\arctan\frac{\mathrm{w}^{\mathrm{gt}}}{\mathrm{h}^{\mathrm{gt}}} - \arctan\frac{\mathrm{w}}{\mathrm{h}}\right)^2 \tag{6}$$

It can be gathered from (6) that when the difference between the aspect ratio of the predicted box and the real box is not large, the CIoU loss function cannot express the penalty term of the aspect ratio in a stable manner. At the same time, the model has a slower convergence speed because the CIoU loss function only considers the distance between the real box and the predicted box, overlapping area and aspect ratio, and ignores the angle between the real box and the predicted box. In YOLO, the commonly used loss functions also include SIoU, DIoU, GIoU and EIoU. Among them, EIOU replaces the aspect ratio by calculating the difference value of the width and height, respectively, on the basis of CIOU, which solves the fuzzy definition of aspect ratio. Therefore, in this study, the EIoU loss function is used instead of the CIoU loss function as the localization loss function of the YOLOv7 algorithm, which is defined as the following:

$$\mathrm{Loss}_{\mathrm{EIoU}} = 1 - \mathrm{IOU} + \frac{\rho^2(\mathrm{b},\mathrm{b}^{\mathrm{gt}})}{(\mathrm{w}^{\mathrm{c}})^2+(\mathrm{h}^{\mathrm{c}})^2} + \frac{\rho^2(\mathrm{w},\mathrm{w}^{\mathrm{gt}})}{(\mathrm{w}^{\mathrm{c}})^2} + \frac{\rho^2(\mathrm{h},\mathrm{h}^{\mathrm{gt}})}{(\mathrm{h}^{\mathrm{c}})^2} \tag{7}$$

The EIoU loss function includes the IoU loss, distance loss and position loss. On the basis of CIoU, the width and height influence factors of the prediction and real boxes are split and calculated separately, which minimizes the difference between their widths and heights. This improves the regression performance, the convergence speed and positioning. It also introduces the focal loss to reduce the imbalance of positive and negative samples, and the imbalance of difficult and easy samples.

2.5.2. Time-Division Storage of Cereal and Oil Video Surveillance Data Based on Blockchain

Considering grain depot video surveillance data (GVSD) as the research object, the acquired GVSD are processed in segments of two hours, and stored on the blockchain in batches in order to improve the storage access efficiency. The specific steps are as follows:

Step 1: The data user uploads the original GVSD data and the image data of the personnel without helmets together in a file to the IPFS. The IPFS generates a unique hash value based on the file content and returns the CID, which can be used by the CID to find the corresponding file in the IPFS.

Step 2: The data user uses the SHA256 hash function to encrypt the image data (KF) of the personnel without wearing helmets, and obtain the hash value h_{KF}, i.e., hash(KF)→h_{KF}.

Step 3: The data user uses the private key SK_d to sign the CID and the hash value h_{KF} of the image data obtained in step 2 as S_{IK}, i.e., S_{IK} = Sign_SK_d(CID, h_{KF}). Subsequently, S_{IK} is recorded in the consortium blockchain and broadcasted in the form of a transaction, and the blockchain will return the transaction receipt storing the data.

Step 4: The regulator needs to view the GVSD data for a certain time period, and obtain the corresponding S_{IK} record from the blockchain based on the index of the string containing the video time.

Step 5: The regulator performs the first decryption using the data user's public key PK_d to confirm that the S_{IK} record was uploaded by the same data user, i.e., Decrypt(PK_d, S_{IK})→(CID, h_{KF}).

Step 6: The regulator locates the storage node for the video surveillance data by content addressing in the IPFS based on the hash address CID, and downloads the original GVSD record and the image data of personnel without helmets.

Step 7: In the last step, hash operation is performed on the images of personnel without helmets and the corresponding calculation results are compared with h_{KF} on the chain. This completes the process of storing and the management of GVSD on the chain.

3. Results and Discussion

The operating systems of the experiments presented in this paper are Windows and Ubuntu. The deep learning framework Pytorch is utilized to build, train and test the target detection model, and the improved YOLOv7 algorithm is used to carry out the detection on the cereal and oil video surveillance data. The simulation deployment of alliance chain nodes is achieved on the virtual machine to construct the blockchain network based on FISCO BCOS. Table 4 shows the specific operating environment of this system.

Table 4. System operating environment.

Experimental Environment	Version
Virtual machine	VMware Workstation 16.2.1 build-18811642
Operating system	Windows10 64 bit, Ubuntu-16.04.7
CPU	11th Gen Intel(R) Core(TM) i7-11800H
GPU	NVIDIA GeForce RTX 3060 Laptop
Memory	32 GB
Python	v3.8.2
Deep learning framework	Pytorch 1.12.1 CUDA 10.2
FISCO BCOS	v2.9.1
Go-ipfs	v0.4.14
OpenSSL	V1.0.2

3.1. Target Detection Based on Improved YOLOv7 Algorithm

In this study, the personnel in the grain depot without helmets are considered the research target, and the YOLOv7 algorithm is chosen to construct the target detection model. The helmet datasets used in this paper are obtained from the web via Python scripts. A total of 2800 personnel samples are screened, and the images are labeled using Labelimg and saved in YOLO format. The datasets are randomly divided into the training set, the test set and the validation set, according to the ratio of 8:1:1. The datasets consist of two categories: one without a helmet and the other with a helmet. The initial learning rate during training is 0.01, momentum is 0.937 and batch size is set to 8. The training image sizes are all set to 640 × 640 pixels, and training is carried out over 100 epochs.

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \tag{8}$$

$$\text{mAP} = \frac{1}{\text{m}}\sum_{\text{i=1}}^{\text{m}} \text{AP}_\text{i} \tag{9}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \tag{10}$$

$$\text{AP} = \sum_{i=1}^{n-1}(r_{i+1} - r_i)p(r_{i+1}) \tag{11}$$

The performance of different loss functions is analyzed by replacing the loss function CIoU of the original YOLOv7 with SIoU, DIoU, GIoU and EIoU. Table 5 compares the performance of the above five loss functions applied to YOLOv7.

Table 5. Performance of five loss functions.

Loss	mAP/%	Precision/%	Recall/%	Training Time/hr
CIoU	93	90.8	86.6	2.99
SIoU	94.4	93.5	89.3	2.71
DIoU	92.9	90.6	87.0	2.81
GIoU	79.2	85.2	72.0	2.69
EIoU (ours)	94.5	93.7	90.0	2.67

It can be gathered based on Table 5 that compared with CIoU, the mAP, Precision and Recall of the EIoU loss function model are 1.5%, 2.9% and 3.4% higher, respectively, and the training time is shortened by 0.32 hr. Compared with SIoU, the mAP, Precision and Recall of EIoU loss function model are 0.1%, 0.2% and 0.7% higher, respectively, and the training time is 0.04 h less. Compared with DIoU, the mAP, Precision and Recall of EIoU loss function model are 1.6%, 3.1% and 3% higher, respectively, and the training time is shortened by 0.14 h. Compared with GIoU, the mAP, Precision and Recall of EIoU loss function model are 15.3%, 8.5% and 18% higher, respectively, and the training time is decreased by 0.02 hr. The above analysis shows that the comprehensive advantages of the EIoU loss function for model training are more obvious and the detection precision is the highest.

In order to objectively evaluate the performance of the improved YOLOv7 model for helmet detection in this study, the same number of training sets is used under the same configuration conditions. Comparative experiments are carried out using several popular target detection networks: YOLOv3-Tiny, YOLOv5s and YOLOv7. The experimental results are evaluated using Recall, Precision and mAP and FPS, which are shown in Table 6.

Table 6. Experimental results comparison of five algorithms.

Model	mAP@0.5/%	Precision/%	Recall/%
YOLOv3-Tiny	83.7	90.1	74.6
YOLOv5s	91.9	94.6	85.2
YOLOv7	93	90.8	86.6
Ours	94.5	93.7	90.0

Table 6 shows that YOLOv7 outperforms the YOLOv3 and YOLOv5 models in terms of the mAP and Recall rate, which has certain advantages. Compared with the basic YOLOv7 model, the mAP, Precision and Recall are increased by 1.5%, 2.9% and 0.4%, respectively. Therefore, the improved algorithm proposed in this study can increase the precision of helmet wearing inspection.

In order to better verify the algorithm proposed in this paper, some frames of the video monitoring data of the grain depot are selected for testing, and the detection performance of the benchmark model YOLOv7 before and after the proposed improvement is compared and analyzed, as shown in Figure 10. Figure 10a, c and e show the detection results with the reference model. Figure 10b, d and f show the detection results with the proposed algorithm. In the environment with dense intersection, false detection occurs in

Figure 10a,c. In the environment with weak light, false detection also occurs in Figure 10e. In Figure 10b,d,f, each target is accurately detected and has a higher detection accuracy. Therefore, the improved YOLOv7 model has good robustness in a more complex environment, showing better performance and higher detection accuracy.

Figure 10. Comparison of detection results.

3.2. Surveillance Video Data Storage Based on FISCO BCOS

This experiment builds an IPFS and deploys a blockchain network using the FISCO BCOS platform. The visualization WeBASE platform is used to complete the development, deployment and invocation of data storage smart contracts and other operations, as shown in Figures 11 and 12.

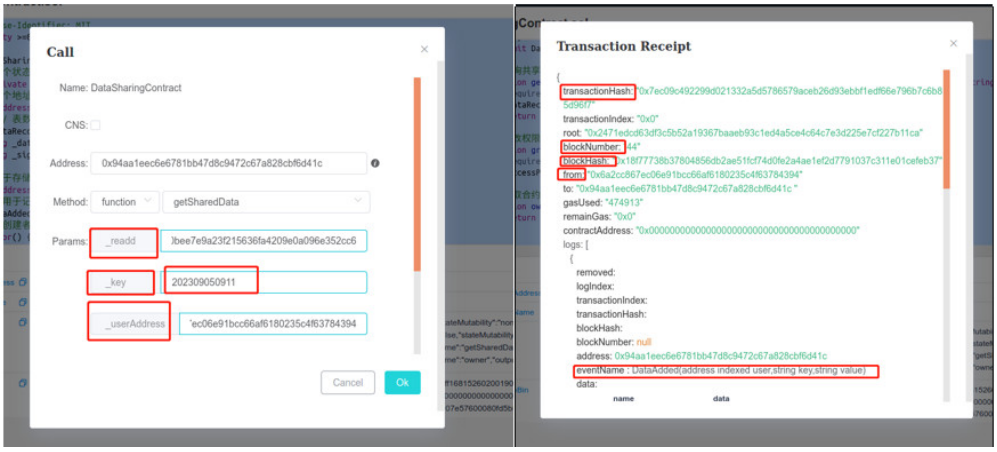

Figure 11. Process of writing data on-chain.

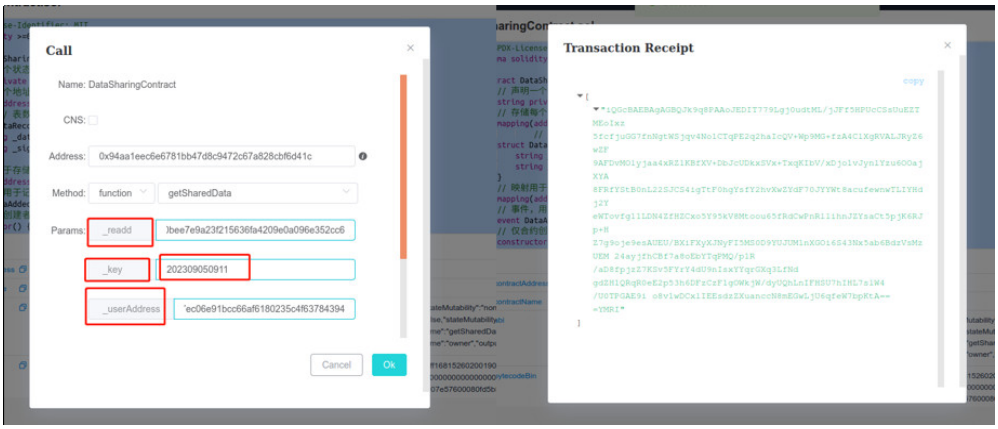

Figure 12. Process of reading data on-chain.

In this study, the SHA256 algorithm is used to encrypt the frames of the grain depot video where personnel are without helmets. The contract deployer has the right to call the function of setting the shared data, and sign the encrypted picture abstract h_{KF} and the video data storage address CID in IPFS with its own private key to obtain the data. Subsequently, the deployed contract uploads the data to the chain. Algorithm 1 shows the data upload algorithm.

Algorithm 1. Algorithm for setSharedData

Input: _wusr(address),_key(time of video),_value(data)

```
function setSharedData
    if hasAccess(_wusr)= =True
        _value=Sign _SK_wusr（data）
    if bytes(_key).length>0 and bytes(_value).length >0
        dataMap[_wusr] [_key] = DataRecord(_date: _key,_signdata: _value)
      emit DataAdded(_wusr, _key, _value)
```

When the regulator wants to view the video data in a certain period of time, they call the Get Shared Data function in the contract, and enters their own address and video index. If it has access rights, the system will return the corresponding block information. Algorithm 2 shows the data access algorithm.

Algorithm 2. Algorithm for getSharedData

Input: _rusr(address),_key(time of video), _wusr(address)

```
function getSharedData
    if hasAccess(_rusr)= =True
        DataRecord storage record = dataMap[_userAddress][_key]
    return record._signdata
```

Next, we test the stability of video files with different sizes. When the size of the stored video file is less than or equal to 5 GB, this system can complete a data-sending transaction in 5 s and return the block ID. When the uploaded file is larger than 10 GB, it is still able to complete the sending of a transaction at a faster speed. Considering the video file with a size of 3.2 GB as an example, 248 frames of key information are finally obtained using the target detection algorithm. Out of these frames, 34 abnormal images where personnel are not wearing helmets are extracted. The total size of these abnormal images is about 1.1 MB, which is considerably smaller than that of the original video file, and the whole process can be completed within 10 s. This analysis from the perspective of distributed storage shows that the way of storing data in this study improves the system scalability.

4. Conclusions

In this study, a dual storage model of "Blockchain + IPFS" was designed to address the problems of the reliability, security and resource wastage of traditional cereal and oil video surveillance data storage. The use of IPFS in this model was not only suitable for the decentralized characteristics of blockchain, but also mitigated the problem of the insufficient storage capacity of blockchain. The improved YOLOv7 algorithm exhibited a 1.5%, 2.9% and 3.4% higher mAP, Recall and Precision, respectively, than the original YOLOv7 model. Thus, it could obtain the abnormal information in the cereal and oil video surveillance data from the complex grain storage environment more accurately. This study replaced the complete video data with video summaries for on-chain storage, which effectively reduced the storage burden on the blockchain while ensuring the integrity and security of the cereal and oil video surveillance data storage, and significantly improved the query efficiency of the on-chain data. The model proposed in this paper is of great significance for ensuring cereal and oil safety, which is a fundamental issue linked to the survival of human beings.

Author Contributions: Conceptualization, H.G. and G.C.; methodology, H.G. and G.C.; software, Y.J.; validation, H.G., G.C. and Y.J.; formal analysis, Z.S. and Z.J.; investigation, Z.J. and G.C.; resources, Y.Z.; data curation, H.G. and X.W.; writing—original draft preparation, H.G.; writing—review and editing, Y.J. and Y.Z.; visualization, X.W.; supervision, Y.Z.; project administration, Y.Z.; funding acquisition, H.G., X.W., Y.J., Z.S., Z.J., Z.J., G.C. and Y.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (Grant No. 62271191, No. 61975053), Natural Science Foundation of Henan (No. 222300420040); The Innovative Funds Plan of Henan University of Technology (No. 2021ZKCJ04); Key Science and Technology Program of Henan Province (No. 222102110246, No. 222103810072); the Program for Science & Technology Innovation Talents in Universities of Henan Province (No. 23HASTIT024, No. 22HASTIT017), the Open Fund Project of Key Laboratory of Grain Information Processing & Control, Ministry of Education, Henan University of Technology (No. KFJJ2020103, No. KFJJ2021102), the Cultivation Programme for Young Backbone Teachers in Henan University of Technology. The authors declare no conflicts of interest.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Xu, Y.; Li, X.; Zeng, X.; Cao, J.; Jiang, W. Application of blockchain technology in food safety control: Current trends and future prospects. *Crit. Rev. Food Sci. Nutr.* **2020**, *62*, 2800–2819.
2. Lei, M.; Xu, L.; Liu, T.; Liu, S.; Sun, C. Integration of Privacy Protection and Blockchain-Based Food Safety Traceability: Potential and Challenges. *Foods* **2022**, *11*, 2262.
3. Chen, G.; Hou, J.; Liu, C. A Scientometric Review of Grain Storage Technology in the Past 15 Years (2007–2022) Based on Knowledge Graph and Visualization. *Foods* **2022**, *11*, 3836.
4. Khan, S.; Alsuwaidan, L. Agricultural monitoring system in video surveillance object detection using feature extraction and classification by deep learning techniques. *Comput. Electr. Eng.* **2022**, *102*, 108201.
5. Patil, P.W.; Dudhane, A.; Chaudhary, S.; Murala, S. Multi-frame based adversarial learning approach for video surveillance. *Pattern Recognit.* **2022**, *122*, 108350.
6. Feng, H.; Wang, X.; Duan, Y.; Zhang, J.; Zhang, X. Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges. *J. Clean. Prod.* **2020**, *260*, 121031.
7. Peng, X.; Zhao, Z.; Wang, X.; Li, H.; Xu, J.; Zhang, X. A review on blockchain smart contracts in the agri-food industry: Current state, application challenges and future trends. *Comput. Electron. Agric.* **2023**, *208*, 107776.
8. Zhu, Q.; Bai, C.; Sarkis, J. Blockchain technology and supply chains: The paradox of the atheoretical research discourse. *Transp. Res. Part E Logist. Transp. Rev.* **2022**, *164*, 102824.
9. Patelli, N.; Mandrioli, M. Blockchain technology and traceability in the agrifood industry. *J. Food Sci.* **2020**, *85*, 3670–3678.
10. Majdalawieh, M.; Nizamuddin, N.; Alaraj, M.; Khan, S.; Bani-Hani, A. Blockchain-based solution for Secure and Transparent Food Supply Chain Network. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 3831–3850.
11. Kechagias, E.P.; Gayialis, S.P.; Papadopoulos, G.A.; Papoutsis, G. An Ethereum-Based Distributed Application for Enhancing Food Supply Chain Traceability. *Foods* **2023**, *12*, 1220.
12. Wu, H.; Jiang, S.; Cao, J. High-Efficiency Blockchain-Based Supply Chain Traceability. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 3748–3758.
13. Zhang, X.; Li, Y.; Peng, X.; Zhao, Z.; Han, J.; Xu, J. Information Traceability Model for the Grain and Oil Food Supply Chain Based on Trusted Identification and Trusted Blockchain. *Int. J. Environ. Res. Public Health* **2022**, *19*, 6594.
14. Treiblmaier, H.; Garaus, M. Using blockchain to signal quality in the food supply chain: The impact on consumer purchase intentions and the moderating effect of brand familiarity. *Int. J. Inf. Manag.* **2023**, *68*, 102514.
15. Wang, J.; Chen, J.; Ren, Y.; Sharma, P.K.; Alfarraj, O.; Tolba, A. Data security storage mechanism based on blockchain industrial Internet of Things. *Comput. Ind. Eng.* **2022**, *164*, 107903.
16. Fan, X.; Niu, B.; Liu, Z. Scalable blockchain storage systems: Research progress and models. *Computing* **2022**, *104*, 1497–1524.
17. Sanka, A.I.; Cheung, R.C.C. A systematic review of blockchain scalability: Issues, solutions, analysis and future research. *J. Netw. Comput. Appl.* **2021**, *195*, 103232.
18. Ge, C.; Liu, Z.; Fang, L. A blockchain based decentralized data security mechanism for the Internet of Things. *J. Parallel Distrib. Comput.* **2020**, *141*, 1–9.
19. Li, L.; Huang, D.; Zhang, C. An Efficient DAG Blockchain Architecture for IoT. *IEEE Internet Things J.* **2023**, *10*, 1286–1296.
20. Wang, Y.; Wang, W.; Zeng, Y.; Yang, T. GradingShard: A new sharding protocol to improve blockchain throughput. *Peer-to-Peer Netw. Appl.* **2023**, *16*, 1327–1339.
21. Dorsala, M.R.; Sastry, V.N.; Chapram, S. Blockchain-based solutions for cloud computing: A survey. *J. Netw. Comput. Appl.* **2021**, *196*, 103246.
22. Li, Z.; Su, W.; Xu, M.; Yu, R.; Niyato, D.; Xie, S. Compact Learning Model for Dynamic Off-Chain Routing in Blockchain-Based IoT. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 3615–3630.
23. Zou, J.; He, D.; Zeadally, S.; Kumar, N.; Wang, H.; Choo, K.R. Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges. *ACM Comput. Surv.* **2021**, *54*, 1–36.
24. Chen, L.; Zhang, X.; Sun, Z. Scalable Blockchain Storage Model Based on DHT and IPFS. *KSII Trans. Internet Inf. Syst.* **2022**, *16*, 2286–2304.
25. Meng, X.; Li, C.; Li, J.; Li, X.; Guo, F.; Xiao, Z. YOLOv7-MA: Improved YOLOv7-Based Wheat Head Detection and Counting. *Remote Sens.* **2023**, *15*, 3770.
26. Tan, L.; Shi, N.; Yu, K.; Aloqaily, M.; Jararweh, Y. A Blockchain-empowered Access Control Framework for Smart Devices in Green Internet of Things. *ACM Trans. Internet Technol.* **2021**, *21*, 1–20.
27. Ma, F.; Ren, M.; Fu, Y.; Wang, M.; Li, H.; Song, H.; Jiang, Y. Security reinforcement for Ethereum virtual machine. *Inf. Process. Manag.* **2021**, *58*, 102565.
28. Chen, R.; Wu, X.; Liu, X. RSETP: A Reliable Security Education and Training Platform Based on the Alliance Blockchain. *Electronics* **2023**, *12*, 1427.

29. Yang, R.; Wakefield, R.; Lyu, S.; Jayasuriya, S.; Han, F.; Yi, X.; Yang, X.; Amarasinghe, G.; Chen, S. Public and private blockchain in construction business process and information integration. *Automation in construction* **2020**, *118*, *103276*.
30. Antony Saviour, M.; Samiappan, D. IPFS based file storage access control and authentication model for secure data transfer using block chain technique. *Concurr. Comput. Pract. Exp.* **2022**, *35*, e7485.
31. Doan, T.V.; Psaras, Y.; Ott, J.; Bajpai, V. Toward Decentralized Cloud Storage With IPFS: Opportunities, Challenges, and Future Considerations. *IEEE Internet Comput.* **2022**, *26*, 7–15.
32. Liu, N.; Liu, P. Goaling recognition based on intelligent analysis of real-time basketball image of Internet of Things. *J. Supercomput.* **2021**, *78*, 123–143.
33. Wang, J.; Zeng, C.; Wang, Z.; Jiang, K. An improved smart key frame extraction algorithm for vehicle target recognition. *Comput. Electr. Eng.* **2022**, *97*, 107540.
34. Yuan, J.; Zhang, G.; Li, F.; Liu, J.; Xu, L.; Wu, S.; Jiang, T.; Guo, D.; Xie, Y. Independent Moving Object Detection Based on a Vehicle Mounted Binocular Camera. *IEEE Sens. J.* **2021**, *21*, 11522–11531.
35. Niu, J.; Jiang, Y.; Fu, Y.; Zhang, T.; Masini, N. Image Deblurring of Video Surveillance System in Rainy Environment. *Comput. Mater. Contin.* **2020**, *65*, 807–816.
36. Gündüz M, Ş.; Işık, G. A new YOLO-based method for real-time crowd detection from video and performance analysis of YOLO models. *J. Real-Time Image Process.* **2023**, *20*, 5.
37. Gallo, I.; Rehman, A.U.; Dehkordi, R.H.; Landro, N.; La Grassa, R.; Boschetti, M. Deep Object Detection of Crop Weeds: Performance of YOLOv7 on a Real Case Dataset from UAV Images. *Remote Sens.* **2023**, *15*, 539.
38. Chen, X.; Xie, Q.; Liguori, R. Safety Helmet-Wearing Detection System for Manufacturing Workshop Based on Improved YOLOv7. *J. Sens.* **2023**, *2023*, 7230463.
39. Yu, C.; Feng, Z.; Wu, Z.; Wei, R.; Song, B.; Cao, C. HB-YOLO: An Improved YOLOv7 Algorithm for Dim-Object Tracking in Satellite Remote Sensing Videos. *Remote Sens.* **2023**, *15*, 3551.