mathematics

MDPI

Article

SEAIS: Secure and Efficient Agricultural Image Storage Combining Blockchain and Satellite Networks

Haotian Yang [1,*], Pujie Jing [1], Zihan Wu [2], Lu Liu [3] and Pengyan Liu [4]

[1] School of Agricultural Engineering, Jiangsu University, Zhenjiang 212013, China; jingpujie914@gmail.com
[2] School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China; wzh042@seu.edu.cn
[3] Department of Computer Science, University of Leicester, Leicester LE1 7RH, UK; l.liu@leicester.ac.uk
[4] Institute of Food Safety and Nutrition, Jiangsu Academy of Agricultural Sciences, Nanjing 210014, China; lpy@jaas.ac.cn
* Correspondence: haotyang@gmail.com

Abstract: The image integrity of real-time monitoring is crucial for monitoring crop growth, helping farmers and researchers improve production efficiency and crop yields. Unfortunately, existing schemes just focus on ground equipment and drone imaging, neglecting satellite networks in remote or extreme environments. Given that satellite internet features wide area coverage, we propose SEAIS, a secure and efficient agricultural image storage scheme combining blockchain and satellite networks. SEAIS presents the mathematical model of image processing and transmission based on satellite networks. Moreover, to ensure the integrity and authenticity of image data during preprocessing such as denoising and enhancement, SEAIS includes a secure agricultural image storage and verification method based on blockchain, homomorphic encryption, and zero-knowledge proof. Specifically, images are stored via IPFS, with hash values and metadata recorded on the blockchain, ensuring immutability and transparency. The simulation results show that SEAIS exhibits more stable and efficient processing times in extreme environments. Also, it maintains low on-chain storage overhead, enhancing scalability.

Keywords: blockchain; satellite networks; image storage model; verifiability

MSC: 62P30; 94A60

check for updates

Citation: Yang, H.; Jing, P.; Wu, Z.; Liu, L.; Liu, P. SEAIS: Secure and Efficient Agricultural Image Storage Combining Blockchain and Satellite Networks. *Mathematics* **2024**, *12*, 2861. https://doi.org/10.3390/math12182861

Academic Editor: Andrea Scozzari

Received: 31 July 2024
Revised: 6 September 2024
Accepted: 12 September 2024
Published: 14 September 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Ensuring the integrity and authenticity of agricultural image data is important. In agriculture 4.0, the application of precision agriculture is becoming increasingly widespread [1]. These technologies rely on high-quality image data for their implementation [2–4]. Accurate images can help farmers and researchers monitor important factors, such as crop growth, pest and disease levels, soil moisture, nutrient content, and weather changes. These images assist farmers in making precise decisions in daily management and provide a substantial foundation for agricultural research [5,6]. In the production process, any tampering or loss of data can lead to incorrect decisions, resulting in agricultural production losses and potentially affecting food safety [7]. Therefore, to ensure agricultural production efficiency and sustainable development, a reliable image data storage and verification mechanism is crucial.

However, existing studies mainly focus on ground-based equipment and drone imaging [8,9]. Ground-based devices, such as sensors and smart devices, provide high-resolution and high-precision image data [10]. Drones can cover large farmland areas and flexibly capture images from different angles [11]. These devices are effective in many situations, but they face limitations in remote areas or extreme environments [12]. For example, in large farmlands, mountains, or during adverse weather, ground equipment and drones are

often impractical. Additionally, drones have limited flight time and altitude, making them inadequate for continuous monitoring over extensive areas [13].

Satellite imaging offers a viable solution due to its wide coverage, high frequency, and independence from ground conditions, providing continuous monitoring in large and extreme environments [14]. However, satellite imaging generates vast amounts of data, which are complex to process. The resolution may be lower than that of ground-based equipment and drones, increasing the difficulty of data management and verification [15]. Therefore, an effective scheme is needed to ensure the integrity and authenticity of this large and complex data. Blockchain, with its decentralized, tamper-proof, and transparent nature, is a reliable solution for addressing these challenges [16–18]. Thus, this paper proposes SEAIS, a secure and efficient agricultural image storage scheme combining blockchain and satellite networks. The contributions are as follows:

1. We propose a mathematical model for agricultural image processing and transmission based on satellite networks, specifically considering the use of satellite imaging in remote areas or extreme environments. The model ensures the effective acquisition and processing of agricultural image data in a variety of environments.
2. We design a secure agricultural image storage and verification method based on blockchain, homomorphic encryption, and zero-knowledge proof. The method guarantees data transparency and immutability while ensuring the integrity and authenticity of the image.
3. We implement the prototype for SEAIS on Hyperledger Fabric and NS-3. The simulation results show that SEAIS has stable encryption and decryption rates, with time overhead increasing as image size grows. Also, the transmission time of SEAIS for (1024×1024) images is about 21.3% of the traditional ground networks.

The remainder of the paper is organized as follows: Section 2 presents a review of related works. Section 3 outlines the system model, providing details about the components and architecture of SEAIS. Section 4 describes the design and methodology of the proposed scheme. Section 5 offers a thorough security analysis. Section 6 covers experimental evaluations, demonstrating the performance of SEAIS in terms of encryption and decryption times, transmission efficiency, and storage overheads. Finally, Section 7 concludes the paper.

2. Related Works

In agriculture 4.0, certain technologies play a crucial role. Existing research covers a range of advancements from ground equipment [19] to UAV imaging [20], significantly promoting the development of precision agriculture. Additionally, after obtaining image data, some studies utilize cloud-edge architecture for task offloading [21,22], which enables real-time analysis of the data. In such cases, farmers and researchers can manage crops better, thereby improving production efficiency and yield. However, existing research has not yet addressed the challenges of agricultural image acquisition and storage in remote areas or extreme environments. In these scenarios, field imaging is essential for accurate monitoring and management of agricultural production, ensuring data integrity and avoiding decision-making errors due to harsh environmental conditions [23].

2.1. Satellite Network-Based Imaging Technology

There is currently limited research on agricultural imaging based on satellite internet, and most of it focuses on data transmission and image matching. Burke et al. [24] reviewed the literature on using satellite imagery and machine learning to measure sustainable development outcomes, with a particular focus on the impact of data scarcity and noise on model performance. The research showed that satellite technology is better than traditional methods for predicting key sustainable development outcomes. Stratoulias et al. [25] proposed an automated workflow, which can process large volumes of high spatial resolution satellite imagery, to generate actionable information within the framework of smallholder farming. Mckinion et al. [26] studied the bottlenecks of multispectral imaging precision agriculture technology in U.S. cotton-growing regions. They successfully achieved fast

bidirectional data transfer between devices by implementing wireless LAN technology on experimental farms. Lin et al. [27] studied the satellite imaging data transmission scheduling problem and proposed a Specific Time-Evolving Graph (STEG) model that improves the efficiency of image data transmission. Saleem et al. [28] Booker studied image matching between satellite images and aerial photographs of agricultural land. They also evaluated the performance of multiple feature points under different times, perspectives, sensors, and altitudes.

Despite significant progress in predicting and understanding agricultural sustainability outcomes, enhancing data transmission efficiency, and improving image-matching techniques using satellite imagery and machine learning, existing research still falls short in ensuring data integrity, authenticity, and security.

2.2. Blockchain-Based Agricultural Data Storage Scheme

Blockchain is mostly used for trusted storage, deposit, and traceability of agricultural data. Liu et al. [29] proposed a storage method for agricultural monitoring data based on blockchain, which mainly focused on storage and privacy protection solutions. The scheme stored encrypted data in the cloud and stored hash value in the blockchain, which addresses the issue of insufficient local storage space caused by the increasing volume of monitoring data. Bhat et al. [30] proposed the Agri-SCM-BIoT architecture, which combines blockchain and IoT to optimize storage and scalability in the agricultural supply chain. This architecture addresses the interoperability, security, and privacy issues present in current single-chain agricultural supply chain systems. Dai et al. [31] explored the use of an aerial blockchain approach for storing images to ensure secure data transmission in Air-Ground Integrated Networks. Ren et al. [32] proposed a dual-blockchain scheme based on IPFS storage for agricultural IoT sampling data protection. The scheme combines IPFS networks and Ethereum, achieving efficient and secure data storage and retrieval. Zhu et al. [33] used blockchain to create a decentralized platform for storing image data in air-to-ground IoT heterogeneous networks, addressing security issues by ensuring data integrity and security.

In summary, blockchain is currently used more for agricultural data storage. The research focused on performance optimization, privacy protection, and supply chain management. However, there are no studies yet on the verifiable storage of images.

Table 1 compares the existing solutions, showing that existing agricultural image data acquisition primarily relies on ground-based equipment and UAVs, which provide high-precision images but are limited in remote areas or extreme environments. Satellite imaging, with its wide coverage and high frequency, can offer continuous monitoring of large farmlands. However, satellite image data is vast and complex, and current research lacks effective mechanisms to verify its integrity and authenticity. The decentralized and tamper-proof nature of blockchain offers a promising solution, but research on verifiable storage for agricultural images remains limited.

Table 1. Comparison of related works.

Related Works	Image Acquisition Method	Storage Method	Verifiable Storage	Scalability
[19]	Ground Equipment	Local Storage	×	Low
[20,22]	UAV Imaging	Cloud Storage	×	High
[31,33]	Ground Equipment + UAV Imaging	Blockchain	✓	Low
SEAIS	Ground Equipment + UAV + Satellite Imaging	IPFS + Blockchain	✓	High

3. System Model

As shown in Figure 1, this paper designs a comprehensive agricultural image storage scheme that combines blockchain and satellite networks. The system comprises the following five modules:

1. *Image Acquisition Module*. This module includes ground equipment imaging, drone imaging, and satellite imaging. Ground equipment imaging involves installing sensors and cameras in the fields to collect high-resolution close-up images, providing detailed field monitoring data. Drone imaging involves drones cruising over the fields to capture images from different angles and heights. Satellite imaging is used when the other two methods are not applicable, offering wide-area coverage and multispectral images suitable for field monitoring in remote areas or extreme environments.
2. *Image Preprocessing Module*. The module is deployed on cloud or local servers and is responsible for denoising and enhancing the image data. The server uses a median filter algorithm to denoise the images, reducing noise interference and improving image quality. It also uses histogram equalization to enhance the images, improving contrast and detail to ensure high-quality data input.
3. *Image Encryption Module*. This module is also deployed on cloud or local servers and handles encryption and verification processes. The preprocessed image data is encrypted using homomorphic encryption, allowing denoising and enhancement to be performed on the encrypted data, thereby ensuring security during transmission and storage. Zero-knowledge proof technology is also applied to verify the consistency between the encrypted image data and the original data, ensuring data integrity and authenticity during processing.
4. *Image Storage and Blockchain Module*. The storage module utilizes IPFS for decentralized storage and records the hash value of the image on the blockchain. Storing the encrypted image data on IPFS achieves efficient and reliable file storage. Additionally, blockchain storage ensures data immutability and transparency, thus providing long-term data security.
5. *Image Verification Module*. The verification module is deployed on user terminals or servers to handle data verification and access control. The module verifies the integrity and authenticity of the encrypted image using zero-knowledge proof. It combines this with the hash value on the blockchain for further verification. Meanwhile, the module ensures that only authorized users can access and verify relevant data, thus protecting sensitive information.

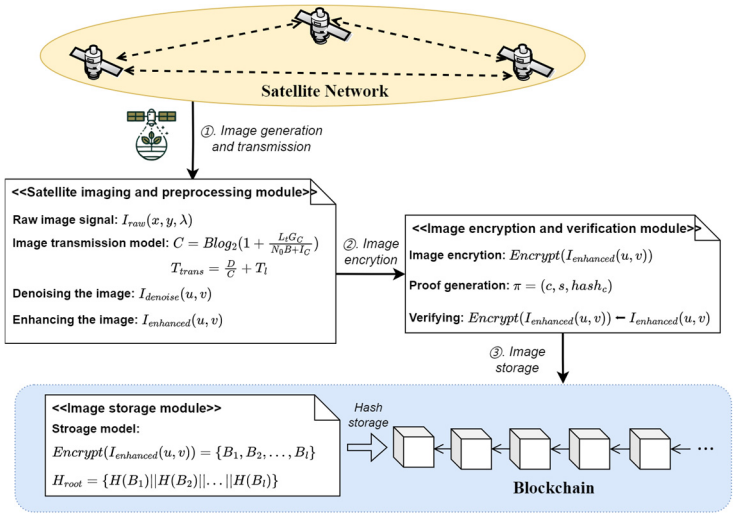

Figure 1. Agricultural image processing and storage model.

4. System Design and Methodology

In this section, we introduce the image storage and verification schemes in detail. SEAIS combines satellite network-based imaging and blockchain storage and ensures image data integrity and authenticity through homomorphic encryption and zero-knowledge proof.

4.1. Satellite Imaging and Pre-Processing

In remote farmland or extreme environments, traditional smart devices and drones often cannot effectively monitor fields and generate real-time images. The satellite network can regularly capture images of fields, providing a continuous data stream, as it has a wide coverage area and is unaffected by environmental factors. The transmitted image data includes raw image signals and various environmental noises. To ensure data integrity and reliability, we propose the following mathematical model and data processing scheme, as shown in Equation (1):

$$I_{raw}(x, y, \lambda) = R_{sat}(x, y, \lambda) + A(x, y, \lambda) + N(x, y, \lambda), \tag{1}$$

where $I_{raw}(x, y, \lambda)$ represents the raw image signal at pixel (x, y) and wavelength λ, $R_{sat}(x, y, \lambda)$ is the ground reflectance at pixel (x, y) and wavelength λ, $A(x, y, \lambda)$ is atmospheric noise and absorption effects, and $N(x, y, \lambda)$ represents the sensor noise. To simplify calculations, we combine atmospheric and sensor noise, as shown in Equations (2) and (3).

$$I_{raw}(x, y, \lambda) = R_{sat}(x, y, \lambda) + N'(x, y, \lambda), \tag{2}$$

$$N'(x, y, \lambda) = A(x, y, \lambda) + N(x, y, \lambda) \tag{3}$$

In this model, we assume that atmospheric noise, such as humidity, temperature fluctuations, and aerosol presence, remains relatively stable over the course of transmission. These environmental factors can impact noise estimation, particularly in dynamic or extreme conditions, but we assume their influence to be consistent in our modeling. Furthermore, the sensor noise $N(x, y, \lambda)$ is modeled under typical satellite sensor conditions, with minimal external interference such as radiation or equipment malfunctions. One limitation of this model is that it assumes a uniform distribution of noise across the entire image, without explicitly accounting for severe atmospheric disturbances like heavy rainfall or dust storms, which could cause localized variations in communication quality.

After capturing the images, they need to be transmitted to a local server or cloud server for preprocessing. We assume no channel interference between satellites and servers, and that the bandwidth B remains constant throughout the transmission process. Additionally, the model assumes that interference power I_c is minimal and stable, without considering potential atmospheric disturbances or signal disruptions caused by multipath effects. The transmission delay T_c is assumed to be fixed. Therefore, the image transmission model is idealized and does not consider more complex scenarios such as multi-satellite communications or changing environmental conditions. This introduces limitations in real-world applications, where factors like rain, snow, and dust storms could degrade communication quality. According to Shannon's formula, the data transmission model is given, with the channel capacity C expressed in Equation (4). Assuming that the raw image data volume is D, the transmission time T_{trans} is given in Equation (5).

$$C = B \log_2(1 + \frac{L_t G_c}{N_0 B + I_c}), \tag{4}$$

$$T_{trans} = \frac{D}{C} + T_l \tag{5}$$

In the above equations, B is the channel bandwidth, P_t is the transmission power of the device, G_c denotes the noise power spectral density, N_0 represents the average co-channel interference power, and T_c is the transmission delay. To ensure data transmission integrity, we use a cyclic redundancy check (CRC) to verify data packets. During transmission,

each data packet includes a checksum, and the receiver uses this checksum for integrity verification. Given the raw data sequence $M(d)$ and the generating polynomial $P(d)$, the data sequence with the appended checksum $S(d)$ is calculated from Equation (6), where n denotes the length of the checksum and $U(d)$ is the remainder and satisfies Equation (7). The raw image data is verified by computing $T'(d)$ mod $P(d)$ when receiving the sequence $T'(d)$; if the result is 0, the transmission is successful; otherwise, there is an error in the data.

$$S(d) = d^n M(d) + U(d), \tag{6}$$

$$U(d) = d^n M(d) \bmod P(d) \tag{7}$$

After the image is transmitted to the local farm server or cloud server, preprocessing operation is required, aiming to enhance image quality for further analysis and processing. The first step is denoising the image, for which we use a median filtering algorithm, as shown in Equation (8).

$$I_{denoise}(u, v) = median\{I_{raw}(u + i, v + j, \lambda) | (i, j) \in W\}, \tag{8}$$

where $I_{denoise}(u, v)$ is the denoised image signal, and W denotes the filtering window. After denoising, we enhance the image using histogram equalization to improve contrast and make details more visible, as shown in Equations (7), (10), and (11).

$$h(k) = \sum_{u=0}^{Y-1} \sum_{v=0}^{N-1} \delta(I_{denoise}(u, v) - k), \tag{9}$$

$$C_{cdf}(k) = \sum_{m=0}^{k} h_{hist}(m), \tag{10}$$

$$I_{enhanced}(u, v) = (\frac{E - 1}{Y \times N}) C_{cdf}(I_{denoise}(u, v)), \tag{11}$$

where $h_{hist}(k)$ represents the grayscale histogram, k is the grayscale level, $C_{cdf}(k)$ denotes the cumulative distribution function value at k, $I_{enhanced}(u, v)$ is the enhanced image signal, $Y \times N$ is the total number of pixels in the image, E represents the number of grayscale levels, and δ is the Dirac delta function, which equals 1 when $I_{denoise}(u, v) = k$ and 0 otherwise.

4.2. Image Encryption and Verification

After denoising and enhancing the image, we ensure data security and integrity using homomorphic encryption and zero-knowledge proof. First, we encrypt the denoised and enhanced image data with the Paillier homomorphic encryption algorithm. Given two large prime numbers p and q, compute $z = p \cdot q$ and $\gamma = lcm(p - 1, q - 1)$, and choose a random number $g \in \mathbb{Z}_{z^2}^*$ to satisfy Equation (12), where $f(\tau)$ is a function in the homomorphic encryption algorithm, denoted as $f(\tau) = \frac{\tau - 1}{z}$. Then, the server keys with the public key (z, g) and private key (γ, μ) are generated.

$$\mu = (f(g^\gamma \bmod z^2))^{-1} \bmod z \tag{12}$$

For the denoised and enhanced image data $I_{enhanced}(u, v)$, selective encryption strategies are applied to minimize the computational load. Let $Mask(u, v)$ represent a binary mask where sensitive data is marked as 1 and non-sensitive data as 0, as shown in Equation (13).

$$I_{selective}(u, v) = Mask(u, v) \cdot I_{enhanced}(u, v) \tag{13}$$

Thus, only pixels marked as sensitive by $Mask(u, v)$ are encrypted, reducing the number of pixels requiring encryption. Then, encrypt each pixel in $I_{selective}$ using the Paillier encryption scheme, as shown in Equation (14).

$$Encrypt(I_{selective}(u, v)) = g^{I_{selective}(u,v)} \cdot r \bmod z^2 \tag{14}$$

Next, the server needs to generate proof for the image receiver to verify. Assuming that we need to prove that the encrypted image data $Encrypt(I_{selective}(u,v))$ is indeed generated from the original denoised and enhanced image data $I_{selective}(u,v)$, we use non-interactive zero-knowledge proof to achieve this. To reduce computational costs, we optimized the traditional modular exponentiation used to generate the commitment value c. In the original implementation, $c = g^r \bmod q$, which can be computationally expensive for large-scale data. We applied precomputation and exponentiation decomposition techniques to optimize this process. We assume the random number r can be represented in binary form, see Equation (15). Thus, the commitment value $c = g^r \bmod q$ can be decomposed into φ smaller powers of g, as shown in Equation (16). Then, the hash value of the encrypted image $hash_d = H(Encrypt(I_{selective}(u,v)))$ is computed.

$$r = r_0 + 2r_1 + 2^2 r_2 + \ldots + 2^{\varphi} r_{\varphi}, \tag{15}$$

$$c = \prod_{\alpha=0}^{\varphi} g^{2^{\alpha} r_{\alpha}} \bmod q \tag{16}$$

After that, the server performs a hash calculation with the commitment value to obtain $hash_c = H(c||hash_d)$. Then, it computes the response value s, see Equation (17). Finally, to minimize transmission overhead, we applied compression techniques to the proof components c and s, while keeping the cryptographic integrity intact. Thus, the proof $\pi = (compress(c), compress(s), hash_c)$ is generated, where $compress()$ represents the compression function.

$$s = r + c \cdot I_{selective}(u,v) \bmod q \tag{17}$$

The final image receiver will verify the authenticity and integrity of the image data. First, the receiver extracts c, s, and $hash_c$ from the proof π. Then, the receiver computes the hash value of the encrypted image $hash'_d = H(Encrypt(I_{selective}(u,v)))$ and calculates c' using Equation (18), followed by computing $hash'_c = H(c'||hash'_d)$. If $hash'_c = hash_c$, it confirms that $Encrypt(I_{selective}(u,v))$ was indeed generated by $I_{selective}(u,v)$ and that the data maintained its integrity and authenticity during encryption and transmission.

$$c' = g^s \cdot (Encrypt(I_{selective}(u,v)))^{-hash_c} \bmod q \tag{18}$$

4.3. Image Storage and Blockchain Recording

After data encryption and verification, to ensure long-term storage and immutability, the encrypted image is stored in IPFS, and its hash value is recorded in the blockchain. IPFS stores and transmits data by dividing the encrypted image into l small blocks, typically 256 KB each, with each block denoted as B_i. The image data is represented by Equation (19).

$$Encrypt(I_{selective}(u,v)) = \{B_1, B_2, \ldots, B_l\} \tag{19}$$

Each data block generates a unique identifier $H(B_i)$ through a hash function. IPFS uses a Directed Acyclic Graph (DAG) to organize and manage these data blocks. The identifier of each image data block acts as a leaf node in the Merkle DAG. The hash values of higher-level nodes are computed layer by layer until the root node, whose hash value H_{root} serves as the unique identifier for the entire image file, as shown in Equation (20). The image data blocks and their corresponding hash values are then stored across multiple nodes in the IPFS network. When a retrieval request is made, it is based on the identifier H_{root}. The IPFS network locates the corresponding Merkle DAG using the Content Identifier (CID), resolves it layer by layer, downloads all data blocks, and reconstructs the original file.

$$H_{root} = \{H(B_1)||H(B_2)||\ldots||H(B_l)\} \tag{20}$$

To ensure data security and privacy, only authorized users can access and verify encrypted data stored in IPFS. IPFS creates an Access Control List (ACL) for each CID

and its stored data. Assuming that the CID is CID_d, and the corresponding ACL is ACL_d, it includes the public keys or identity identifiers of authorized user nodes. When a user requests access, they must provide their identity information and access proof, generating a timestamped access request as shown in Equation (21). The server receives the request, verifies the signature using the user's public key, and checks if the user is listed in the corresponding ACL, as shown in Equation (22). If verified, the user is granted access to download and decrypt the data; otherwise, the request is denied. This ensures that only authorized users can access and verify the encrypted data in IPFS, protecting data security and privacy.

$$\text{AccessRequest} = Sign_{sk_{user}}(CID_d || Timestamp), \tag{21}$$

$$Verify(AccessRequest, pk_{user}, ACL_d) \tag{22}$$

5. Security Analysis

To prove the security of the SEAIS, this section proves it through the reductive approach. We verify the security of each key component step by step, including homomorphic encryption, zero-knowledge proofs, and blockchain recording, and finally prove the security of the whole system.

Theorem 1. *The Paillier homomorphic encryption scheme is secure against chosen plaintext attacks (IND-CPA) in the random oracle model and possesses additive and scalar homomorphic properties, thereby ensuring data confidentiality and integrity.*

Proof of Theorem 1. Given $z = p \cdot q$, we assume the existence of an attacker A; if A can distinguish encrypted ciphertexts from random ciphertexts in polynomial time, this attacker can be used to factor z. However, this contradicts the difficulty of the large number decomposition problem. In the random oracle model, the attacker gains no information about p and q, thus making it impossible to factor z, which ensures data confidentiality. Meanwhile, Paillier homomorphic encryption has additive and scalar homomorphic properties. The additive homomorphism is as follows:

$$\begin{array}{l} Encrypt(I_1) \cdot Encrypt(I_2) = (g^{I_1} \cdot r_1^z) \cdot (g^{I_2} \cdot r_2^z) \bmod z^2 \\ = g^{I_1+I_2} \cdot (r_1 r_2)^z \bmod z^2 = Encrypt(I_1 + I_2) \end{array}, \tag{23}$$

$$Encrypt(I_1)^k = (g^{I_1} \cdot r_1^z)^k \bmod z^2 = g^{k \cdot I_1} \cdot (r_1^k)^z \bmod z^2 = Encrypt(k \cdot I_1) \tag{24}$$

These homomorphic properties allow specific operations on the encrypted data without decrypting it. By verifying the additive and scalar homomorphic properties, we ensure that the integrity of the encrypted data is maintained during processing. That is, any operations performed on the ciphertext correspond to equivalent operations on the plaintext, thus preserving the correctness of the data. □

Theorem 2. *Zero-knowledge-proof protocol ensures the authenticity and integrity of encrypted image data. It allows a verifier to confirm the validity of the data without revealing the data itself.*

Proof of Theorem 2. Assume there exists an adversary B that can produce a valid proof $\pi = (c, s, hash_c)$ for a statement that is false. Given a challenge to solve the discrete logarithm problem (DLP) for g and $y = g^x \bmod p$, where x is unknown, if B can generate a proof for a false statement, it must mean that B can find c, s, and $hash_c$, such that $c' = g^s \cdot (Encrypt(I_{enhanced}(u, v)))^{-hash_c} \bmod q$, which means B can solve the DLP by finding x in polynomial time. This contradicts the DLP assumption. Moreover, given a challenge to find a collision in the hash function H, if B can modify the ciphertext $Encrypt(I_{enhanced}(u, v))$ to $Encrypt(I'_{enhanced}(u, v))$ and produces a valid proof for $Encrypt(I'_{enhanced}(u, v))$, it must mean that B can find the two distinct inputs $(c, hash_d)$ and $(c', hash'_d)$ such that $H(c||hash_d) = H(c'||hash'_d)$, which directly contradicts the collision resistance of H. There-

fore, zero-knowledge proof ensures the authenticity and integrity of encrypted image data. □

Theorem 3. *Blockchain ensures the immutability and transparency of data records by using cryptographic hash functions and a distributed consensus mechanism.*

Proof of Theorem 3. Assume there exists an adversary $\mathbb{C}$ that can alter the data in a block without being detected. Let B_l be the l-th block in the blockchain and $H(B_l)$ be its hash. If $\mathbb{C}$ modifies the image data in B_l to B_l' and recomputes the hash $H(B_l')$ to match the hash stored in the next block B_{l+1}, this implies that $\mathbb{C}$ can break the cryptographic hash function or compromise the consensus protocol, both of which are assumed to be secure. This contradiction proves the immutability of blockchain records. In addition, controlling a majority of the network resources (51% attack) is computationally impractical due to the decentralized nature of blockchain networks and the significant resources required. Any attempt to create an alternate version of the blockchain would be visible to all honest participants, who would reject the tampered chain in favor of the valid chain. Thus, blockchain ensures the immutability and transparency of data records. □

6. Experimental Evaluation

In this section, a simulation experiment is provided concerning the processing and storage of agricultural images from satellite networks. The experiment is conducted on Hyperledger Fabric for blockchain storage and NS-3 for network simulation, deployed in a virtual machine with an AMD EPYC 7713 CPU @4.0 GHz, 8 GB RAM, and 40 GB of storage. We use open-source Sentinel-2 satellite images, obtained from the Copernicus Open Access Hub (https://scihub.copernicus.eu/) (accessed on 8 July 2024) [34], for encryption and decryption analysis. Sentinel-2 provides images for a wide range of agricultural applications, making it particularly relevant to the proposed scheme. The image transmission times were tested under various network conditions simulated in the NS-3 environment, including scenarios representing remote or extreme environments. This helped assess the robustness and performance of the proposed scheme under challenging conditions. We utilized images with pixels of (128×128), (256×256), (512×512), and (1024×1024). The dataset consisted of 50 images from Sentinel-2, with sizes ranging from 10 MB to 100 MB, depending on the image resolution and spectral bands used. Note that the final experimental data is the average of 50 experiments carried out.

We first text image encryption and decryption time based on satellite networks using the dataset from Copernicus Open Access Hub, analyzing the impact of independent variables, namely image size and quantity, on the time overhead for image encryption and decryption. In the experiment, we set the image sizes ranging from (128×128) to (1024×1024). In addition, the encryption algorithm used is the Paillier homomorphic encryption with a key length of 2048 bits to ensure adequate security. The bit error rate (BER) is set to 1×10^{-5}, simulating typical transmission errors in satellite communications. For comparative analysis, we also evaluated the performance of the scheme proposed by Alkhelaiwi et al. [35], which used a similar homomorphic encryption approach.

As shown in Figure 2a, the average encryption and decryption rates remain stable, regardless of the image size. However, as the image size increases, the encryption and decryption times gradually increase. The encryption and decryption times for (1024×1024) image are 63.95 times and 63.69 times those for the (128×128) image, respectively. Compared with the scheme proposed by Alkhelaiwi et al., our system shows better scalability, especially with larger image sizes. For the (1024×1024) image, encryption time of SEAIS is 1417.8 s compared to Alkhelaiwi's 1500 s, and the decryption time is 424 s versus 460 s. As shown in Figure 2b, we fix the image size to (256×256) because the throughput rate remains stable, and the time overhead grows linearly with the increase in the number of image blocks. Additionally, our system maintains higher throughput rates, especially for decryption. The strength of SEAIS is its ability to scale efficiently with larger datasets,

maintaining stable time overhead and throughput, unlike the comparison approach, which experiences higher overhead and reduced throughput as data size increases.

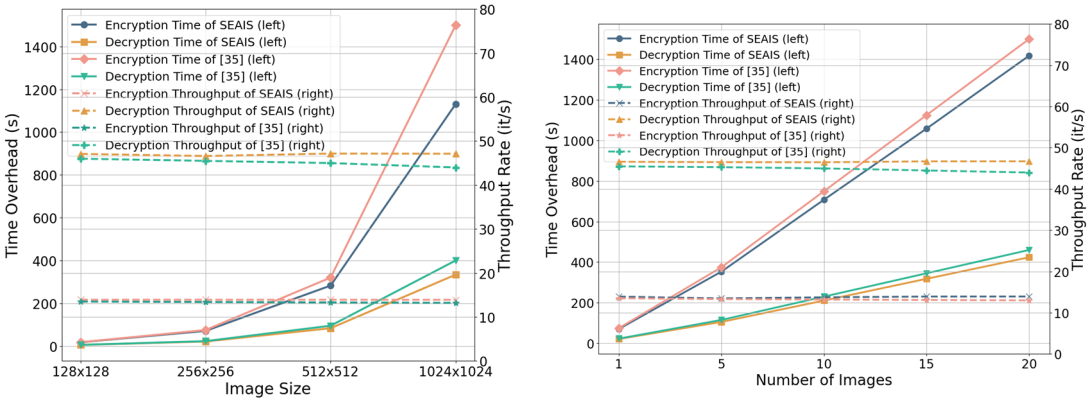

Figure 2. Time overhead of image encryption and decryption. (**a**) Impact of variations in the image size on time overhead; (**b**) impact of variations in the number of images on time overhead.

Moreover, we then simulate the image transmission time overhead in a data transmission model using the NS-3 environment. The communication rate is set to 50 Mbps to reflect typical satellite network bandwidth, which is generally lower than ground networks due to distance and cost constraints. The channel delay of 800 ms simulates the high latency common in satellite communications, reflecting the propagation delay over large distances. A signal-to-noise ratio (SNR) of 15.0 is chosen to represent moderate noise levels, simulating interference from environmental conditions and long transmission distances. The channel capacity is around 100 Mbps to 150 Mbps. These parameters are selected to assess the system's performance in realistic satellite-based agricultural applications. We compared this setup to the work of Andújar et al. [19], who transmitted images over ground networks.

From Figure 3, we can see that under normal conditions, satellite internet image transmission is slower than the scheme proposed by Andújar et al. This is true regardless of the image size or quantity. However, after simulating extreme environments, SEAIS using satellite internet proves more stable. For (1024×1024) image transmission, it takes only about 21.3% of the time compared to the traditional method. Additionally, for transmitting 20 images of (256×256), SEAIS takes only about 59.2% of the time of the traditional transmission scheme. At the same time, transmission time increases with larger image sizes or higher image quantities.

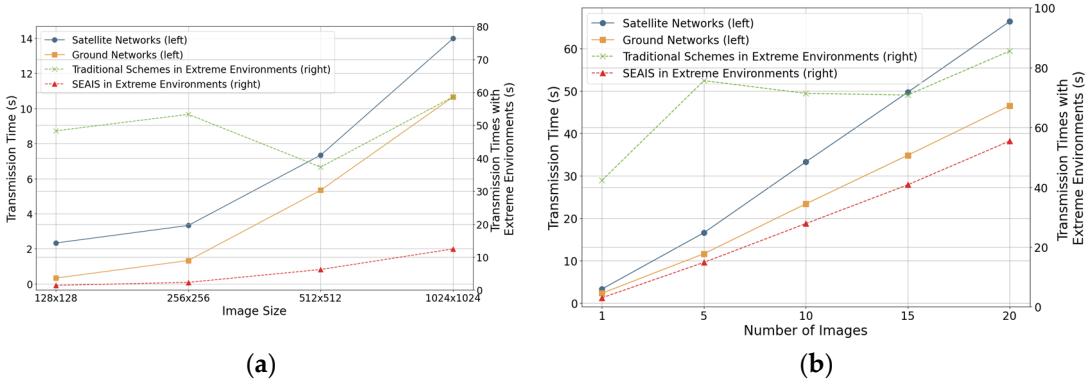

Figure 3. Transmission time comparison. (**a**) Impact of variations in the image size on transmission time; (**b**) impact of variations in the number of images on transmission time.

Finally, we experiment with agricultural image storage overheads, as shown in Figure 4. In the experiment, we utilize IPFS for distributed storage combined with blockchain to ensure

data integrity. Each image is divided into blocks of 256 KB. Also, we use the SHA-256 hashing algorithm to ensure the integrity of data during transmission and storage. To test the storage overhead, the total image data size ranges from 10 MB to 100 MB, and we compare scenarios involving 10 and 20 images.

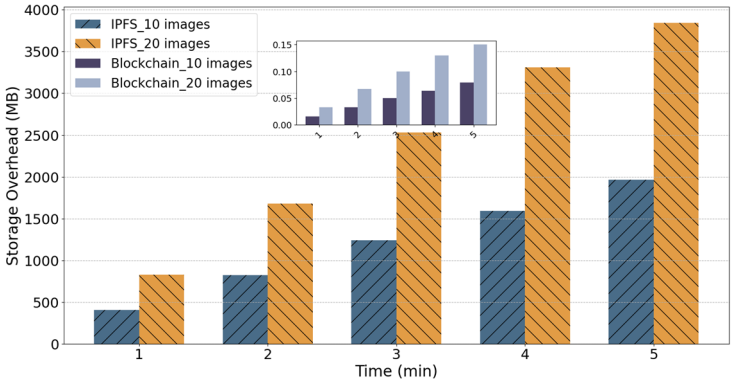

Figure 4. Agricultural image storage overhead.

The results indicate that blockchain stores the hash values of denoised and enhanced images using SHA-256, which reduces storage overhead and improves the scalability of blockchain. Additionally, when generating numerous images, the storage growth rate decreases over time due to the performance limitations of the simulation device.

7. Conclusions

In sum, this paper proposes SEAIS, a secure and efficient storage scheme for agricultural images combining blockchain and satellite networks. SEAIS can use satellite imaging in remote areas and extreme environments, based on imaging from drones and ground equipment. To ensure data integrity and authenticity during denoising and enhancement of images, we combine homomorphic encryption and zero-knowledge proofs. Image data is stored on IPFS, and its hash and raw images are recorded on the blockchain for immutability and transparency. In the experiments, we evaluate the encryption and decryption times, transmission time, and storage overhead. The results show that SEAIS has stable encryption and decryption rates, with time overhead increasing as image size grows. Also, the transmission time of SEAIS for (1024×1024) images is about 21.3% of the traditional ground networks. Meanwhile, the storage method combining IPFS and blockchain reduces blockchain storage costs and enhances scalability.

In future work, we will implement batch processing, data aggregation, edge computing, and IPFS sharding to enhance the scalability of SEAIS, enabling it to efficiently handle larger datasets and more frequent updates in real-time agricultural monitoring scenarios.

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

Funding: This work was funded by the National Key Research and Development Program of China, grant number 2022YFD2100605.

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

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

References

1. Ahmed, N.; De, D.; Hussain, I. Internet of Things (IoT) for Smart Precision Agriculture and Farming in Rural Areas. *IEEE Internet Things J.* **2018**, *5*, 4890–4899. [CrossRef]
2. Zhao, Z.; Liao, G. Imaging Hyperspectral Feature Fusion for Estimation of Rapeseed Pod's Water Content and Recognition of Pod's Maturity Level. *Mathematics* **2024**, *12*, 1693. [CrossRef]
3. Horng, G.J.; Liu, M.X.; Chen, C.C. The smart image recognition mechanism for crop harvesting system in intelligent agriculture. *IEEE Sens. J.* **2019**, *20*, 2766–2781. [CrossRef]
4. Sulistyo, S.B.; Wu, D.; Woo, W.L.; Dlay, S.S.; Gao, B. Computational deep intelligence vision sensing for nutrient content estimation in agricultural automation. *IEEE Trans. Autom. Sci. Eng.* **2017**, *15*, 1243–1257. [CrossRef]
5. Weyler, J.; Magistri, F.; Marks, E.; Chong, Y.L.; Sodano, M.; Roggiolani, G.; Chebrolu, N.; Stachniss, C.; Behley, J. PhenoBench: A Large Dataset and Benchmarks for Semantic Image Interpretation in the Agricultural Domain. *IEEE Trans. Pattern Anal. Mach. Intell.* **2024**, 1–12. [CrossRef]
6. Saranya, T.; Deisy, C.; Sridevi, S.; Anbananthen, K.S.M. A comparative study of deep learning and Internet of Things for precision agriculture. *Eng. Appl. Artif. Intell.* **2023**, *122*, 106034. [CrossRef]
7. Yang, X.; Shu, L.; Chen, J.; Ferrag, M.A.; Wu, J.; Nurellari, E.; Huang, K. A survey on smart agriculture: Development modes, technologies, and security and privacy challenges. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 273–302. [CrossRef]
8. Tarchi, D.; Oliveri, F.; Sammartino, P.F. MIMO radar and ground-based SAR imaging systems: Equivalent approaches for remote sensing. *IEEE Trans. Geosci. Remote Sens.* **2012**, *51*, 425–435. [CrossRef]
9. Gómez-Candón, D.; De Castro, A.I.; López-Granados, F. Assessing the accuracy of mosaics from unmanned aerial vehicle (UAV) imagery for precision agriculture purposes in wheat. *Precis. Agric.* **2014**, *15*, 44–56. [CrossRef]
10. Zahiri, Z.; Laefer, D.F.; Kurz, T.; Buckley, S.; Gowen, A. A comparison of ground-based hyperspectral imaging and red-edge multispectral imaging for façade material classification. *Autom. Constr.* **2022**, *136*, 104164. [CrossRef]
11. Jiang, Y.E.; Wang, L.; Chen, H.H.; Shen, X. Physical Layer Covert Communication in B5G Wireless Networks—Its Research, Applications, and Challenges. *Proc. IEEE* **2024**, *112*, 47–82. [CrossRef]
12. Von Bueren, S.K.; Burkart, A.; Hueni, A.; Rascher, U.; Tuohy, M.P.; Yule, I.J. Deploying four optical UAV-based sensors over grassland: Challenges and limitations. *Biogeosciences* **2015**, *12*, 163–175. [CrossRef]
13. Adão, T.; Hruška, J.; Pádua, L.; Bessa, J.; Peres, E.; Morais, R.; Sousa, J.J. Hyperspectral Imaging: A Review on UAV-Based Sensors, Data Processing and Applications for Agriculture and Forestry. *Remote Sens.* **2017**, *9*, 1110. [CrossRef]
14. Nguyen, T.T.; Hoang, T.D.; Pham, M.T.; Vu, T.T.; Nguyen, T.H.; Huynh, Q.T.; Jo, J. Monitoring agriculture areas with satellite images and deep learning. *Appl. Soft Comput.* **2020**, *95*, 106565. [CrossRef]
15. Gazzea, M.; Pacevicius, M.; Dammann, D.O.; Sapronova, A.; Lunde, T.M.; Arghandeh, R. Automated Power Lines Vegetation Monitoring Using High-Resolution Satellite Imagery. *IEEE Trans. Power Deliv.* **2022**, *37*, 308–316. [CrossRef]
16. Yang, H.; Zhang, X.; Wu, Z.; Wang, L.; Chen, X.; Liu, L. Co-Sharding: A Sharding Scheme for Large-Scale Internet of Things Application. *Distrib. Ledger Technol. Res. Pract.* **2024**, *3*, 1–16. [CrossRef]
17. Fan, W. Blockchain-Secured Task Offloading and Resource Allocation for Cloud-Edge-End Cooperative Networks. *IEEE Trans. Mob. Comput.* **2024**, *23*, 8092–9110. [CrossRef]
18. Bamakan, S.M.H.; Malekinejad, P.; Ziaeian, M. Towards blockchain-based hospital waste management systems; applications and future trends. *J. Clean. Prod.* **2022**, *349*, 131440. [CrossRef]
19. Andújar, D.; Moreno, H.; Bengochea-Guevara, J.M.; de Castro, A.; Ribeiro, A. Aerial imagery or on-ground detection? An economic analysis for vineyard crops. *Comput. Electron. Agric.* **2019**, *157*, 351–358. [CrossRef]
20. Cao, H.; Liu, Y.; Yue, X.; Zhu, W. Cloud-Assisted UAV Data Collection for Multiple Emerging Events in Distributed WSNs. *Sensors* **2017**, *17*, 1818. [CrossRef]
21. Li, D.; Jiang, Q.; Li, S.; Liu, X.; Liu, J. Networked Edge Intelligence for Autonomous Farm Vehicles. *IEEE Netw.* **2023**, *37*, 297–304. [CrossRef]
22. Bai, Z.; Lin, Y.; Cao, Y.; Wang, W. Delay-aware cooperative task offloading for multi-UAV enabled edge-cloud computing. *IEEE Trans. Mob. Comput.* **2022**, *23*, 1034–1049. [CrossRef]
23. Osinga, S.A.; Paudel, D.; Mouzakitis, S.A.; Athanasiadis, I.N. Big data in agriculture: Between opportunity and solution. *Agric. Syst.* **2022**, *195*, 103298. [CrossRef]
24. Burke, M.; Driscoll, A.; Lobell, D.B.; Ermon, S. Using satellite imagery to understand and promote sustainable development. *Science* **2021**, *371*, eabe8628. [CrossRef]
25. Stratoulias, D.; Tolpekin, V.; De By, R.A.; Zurita-Milla, R.; Retsios, V.; Bijker, W.; Hasan, M.A.; Vermote, E. A Workflow for Automated Satellite Image Processing: From Raw VHSR Data to Object-Based Spectral Information for Smallholder Agriculture. *Remote Sens.* **2017**, *9*, 1048. [CrossRef]
26. McKinion, J.M.; Turner, S.B.; Willers, J.L.; Read, J.J.; Jenkins, J.N.; McDade, J. Wireless technology and satellite internet access for high-speed whole farm connectivity in precision agriculture. *Agric. Syst.* **2004**, *81*, 201–212. [CrossRef]
27. Lin, X.; Chen, Y.; Xue, J.; Zhang, B.; He, L.; Chen, Y. Large-volume LEO satellite imaging data networked transmission scheduling problem: Model and algorithm. *Expert Syst. Appl.* **2024**, *249*, 123649. [CrossRef]
28. Saleem, S.; Bais, A.; Sablatnig, R. Towards feature points based image matching between satellite imagery and aerial photographs of agriculture land. *Comput. Electron. Agric.* **2016**, *126*, 12–20. [CrossRef]

29. Liu, Z.; Huang, W.; Wang, D. Functional agricultural monitoring data storage based on sustainable block chain technology. *J. Clean. Prod.* **2021**, *281*, 124078. [CrossRef]
30. Bhat, S.A.; Huang, N.-F.; Sofi, I.B.; Sultan, M. Agriculture-Food Supply Chain Management Based on Blockchain and IoT: A Narrative on Enterprise Blockchain Interoperability. *Agriculture* **2022**, *12*, 40. [CrossRef]
31. Dai, M.; Wang, T.; Li, Y.; Wu, Y.; Qian, L.; Su, Z. Digital twin envisioned secure air-ground integrated networks: A blockchain-based approach. *IEEE Internet Things Mag.* **2022**, *5*, 96–103. [CrossRef]
32. Ren, W.; Wan, X.; Gan, P. A double-blockchain solution for agricultural sampled data security in Internet of Things network. *Future Gener. Comput. Syst.* **2021**, *117*, 453–461. [CrossRef]
33. Zhu, Y.; Zheng, G.; Wong, K.K. Blockchain-empowered decentralized storage in air-to-ground industrial networks. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3593–3601. [CrossRef]
34. European Space Agency; Copernicus Open Access Hub. Available online: https://scihub.copernicus.eu/ (accessed on 8 July 2024).
35. Alkhelaiwi, M.; Boulila, W.; Ahmad, J.; Koubaa, A.; Driss, M. An Efficient Approach Based on Privacy-Preserving Deep Learning for Satellite Image Classification. *Remote Sens.* **2021**, *13*, 2221. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.