Journal of
Theoretical and Applied Electronic Commerce Research

MDPI

Article

Digital Image Copyright Protection and Management Approach—Based on Artificial Intelligence and Blockchain Technology

Jikuan Xu [1,*], Jiamin Zhang [1] and Junhan Wang [2]

[1] College of Arts and Law, China University of Petroleum (East China), Qingdao 266580, China
[2] School of Intellectual Property, University of Chinese Academy of Sciences, Beijing 100190, China
* Correspondence: jikuanxu@upc.edu.cn; Tel.: +86-13176889112

Abstract: The issue of image copyright infringement is prevalent in current e-commerce activities. Users employ methods such as image cropping, compression, and noise addition, making it difficult for traditional copyright detection technologies to identify and track infringements. This study proposes an image copyright registration, protection, and management method based on artificial intelligence and blockchain technology, aiming to address the current challenges of low accuracy in digital copyright infringement judgment, the vulnerability of image fingerprints stored on the chain to tampering, the complexity of encryption algorithms and key acquisition methods through contract calls, and the secure storage of image information during data circulation. The research combines artificial intelligence technology with traditional blockchain technology to overcome the inherent technical barriers of blockchain. It introduces an originality detection model based on deep learning technology after conducting both off-chain and on-chain detection of unidentified images, providing triple protection for digital image copyright infringement detection and enabling efficient active defense and passive evidence storage. Additionally, the study improves upon the traditional image perceptual hashing in blockchain, which has poor robustness, by adding chaotic encryption sequences to protect the image data on the chain, and its effectiveness has been verified through experiments. Ultimately, the research hopes to provide e-commerce entities with an effective and feasible digital copyright protection and management solution, safeguarding their intellectual property rights and fostering a legal and reasonable competitive environment in e-commerce.

Keywords: electronic commerce; digital images; copyright management; artificial intelligence; blockchain

check for updates

Academic Editor: Rand Low

Received: 1 December 2024
Revised: 20 March 2025
Accepted: 13 April 2025
Published: 18 April 2025

Citation: Xu, J.; Zhang, J.; Wang, J. Digital Image Copyright Protection and Management Approach—Based on Artificial Intelligence and Blockchain Technology. *J. Theor. Appl. Electron. Commer. Res.* **2025**, *20*, 76. https://doi.org/10.3390/jtaer20020076

Copyright: © 2025 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

With the popularization of various types of intelligent terminals and the development of image processing technology, the digitization of image works has become a mainstream trend, especially in the fields of e-commerce, social media, and other areas play an important role; however, the characteristics of digitized images which are easy to be downloaded, copied, and modified, and the ensuing problem of copyright infringement of images has also become increasingly prominent [1,2]. The cost of copyright infringement of digital works, especially image works, is extremely low, but it is difficult for authors to obtain evidence for the defense of such intellectual property rights, and the cost of litigation to defend their rights is high, which ultimately leads to the overall inefficiency of copyright

protection, and the competitiveness of the network business entities and even their business reputation will be affected [3].

In the network environment, existing technologies such as digital watermarks can no longer adequately protect the rights of copyright holders due to their easy elimination, destruction, and tampering characteristics [4]. In the existing blockchain technology, the traditional hash algorithm has low accuracy for the infringement detection of images after noise addition and rotation operation, and the encryption algorithm and the method of calling the contract to obtain the key are complicated, which is not suitable for the safe storage of image information in the big data environment [5]. The originality detection methods in blockchain technology are mostly based on content or manually designed feature extraction methods, which have the following shortcomings. First, content-based originality detection methods only capture single features and local information of an image, ignoring the global structure of the image. As a result, only the local information of an image can be compared during originality detection, while the similarity of the global structure cannot be taken into account, which in turn causes poor originality detection. Second, feature extraction methods based on manual design usually need to select and design parameters based on experts' a priori knowledge, which often requires manual intervention and adjustment, and it is difficult to fully utilize the rich semantic information in the image, which affects the accuracy of the algorithm in image originality detection [6,7].

Based on the discovery of these problems, Section 2 of this paper improves the traditional hash algorithm and proposes a system model for image copyright protection and management based on blockchain and perceptual hash. It introduces the information transmission process among blockchain, users and InterPlanetary File System (IPFS). Meanwhile, it improves the blockchain storage structure to enhance query efficiency. To ensure the security of image data, it applies chaotic encryption to the images to be uploaded to the blockchain and provides the corresponding decryption algorithm. Section 3 proposes an innovative solution for originality detection of images using the MobileNetV2 model, and introduces the MobileNetV2 model, the detection principle and process. This solution effectively integrates deep learning technology with blockchain technology, overcoming the inherent technical barriers of blockchain. Section 4 combines the image copyright protection and management method based on blockchain and perceptual hash proposed in the previous chapter with the MobileNetV2 image originality detection model based on deep learning, and it provides an overall introduction to the core technology of this paper, namely the digital image copyright protection and management method based on artificial intelligence and blockchain technology. This chapter details the detection process of images under the fusion scheme and verifies the feasibility and effectiveness of the scheme through experiments. It also presents the improved perceptual hash and MobileNetV2 classification model and mathematical model and analyzes the scalability of the system. Section 5 compares the existing blockchain technology and artificial intelligence technology with this fusion scheme in terms of technical architecture, function, performance, and applicability, and rigorously explains the innovation and feasibility of this scheme. Section 6 discusses the limitations and applications of this scheme from aspects such as energy consumption and transaction costs, storage limitations, algorithm optimization, and data privacy. Section 7 concludes this scheme.

2. Image Copyright Protection and Management Method Based on Blockchain and Sensory Hash

The main content of this chapter is divided into five parts. The first part introduces a system model of an image copyright protection and management method based on blockchain and perceptual hash, which macroscopically introduces the process of inter-

action between blockchain, users, and interstellar file system. The second part improves the current blockchain storage structure query method for the inefficiency of the current blockchain storage structure query method and does not support the multi-dimensional data query. To this end, based on the original Merkle tree verification method, a blockchain storage structure based on the MKD tree is proposed to support multidimensional data queries and improve query efficiency. The third part improves the traditional perceptual hash algorithm for the problems of missing image details during feature capture and low fetch accuracy in determining similarity during image infringement detection [8]. Regarding image perceptual hashing in the original input data and subtle tampering after the existence of a certain correlation between the input data, there is no significant change in the image data tampering detection effect is good. So, the selection of perceptual hashing of image data processing, the calculation of the similarity of the generated hash value to determine the image similarity [9], in addition to the existing redefined image data hash processing when the frequency domain spatial sampling, are used to improve the value accuracy of the image similarity determination threshold. The fourth part designs a chaotic encryption sequence for the data security problem after the images are uploaded to IPFS, and generates a unique MD5 secret key for each image to guarantee image security.

2.1. System Model

As shown in Figure 1, the users in the system model are mainly divided into two categories: copyright owners and consumers. Copyright owners are responsible for uploading digital images and related copyright information to the blockchain and IPFS, using the perceptual hash generated from the images for infringement detection, and encrypting the images using the correlation key. Consumers, who are mainly people who obtain images and corresponding copyright information through legal means, can download the encrypted images and part of the copyright information that has been uploaded by the copyright owner from IPFS on demand. They can call the dual smart contract to apply for a decryption key based on the obtained copyright information, and the decryption key can be obtained by the consumer after completing the asset evaluation and making payment if the image file is not invalidated.

2.2. Block Storage Structure Based on MKD Tree

When detecting the originality of an image, the system traverses the data of each block in the original Merkle tree of the blockchain and retrieves the approximate image through the image multidimensional data to determine its originality, which is an inefficient way of querying and does not support the multidimensional data querying [10]. The KD Tree is able to retrieve the key information in the multidimensional space [11]. Therefore, this paper, on the basis of the original Merkle Tree validation method, is designing a blockchain storage structure based on MKDT (Merkle K-D Tree), which supports multidimensional data query and improves query efficiency.

In order to realize the approximate query, this paper adopts the image fingerprint with characterizable similarity properties to describe the image with the image content feature data as an example. Let the selected image multidimensional feature data be $< P, L >$, then an image can be represented as tuple $=< P, L >$, which is the image fingerprint used for image originality detection. Then, the MKD tree is constructed using the image's multidimensional feature data. We assume that each block contains a collection of multidimensional feature data of one image $v = \{< P_1, L_1 >, < P_2, L_2 >, < P_3, L_3 >, \ldots, < P_n, L_n >\}$ and the multidimensional feature data of the first image $v_i =< P_i, L_i >$ of the first image. Firstly, according to the collection v, the KD tree index is constructed, and for it not to destroy the verifiable query characteristics of the blockchain, the root of the MKD tree is generated by merging the

Merkle hash values of the nodes. The block storage structure based on the MKD tree provides the basis for image originality detection query and user copyright information query in the process of copyright registration in order to improve the efficiency of the query. The image copyright registration on-chain off-chain storage structure is shown in Figure 2.

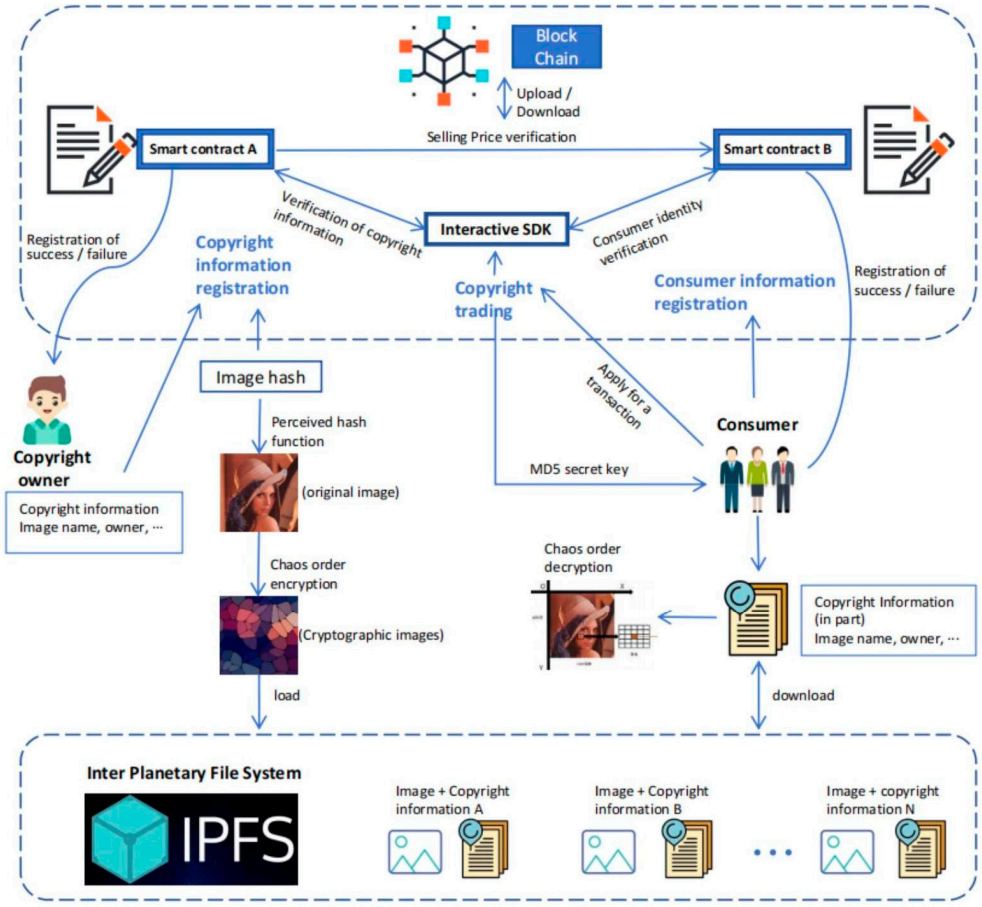


Figure 1. System model of image copyright protection method based on blockchain and sensory hash. MD5 is a chaotic encryption algorithm for hashes, SDK stands for Software Development Kit.

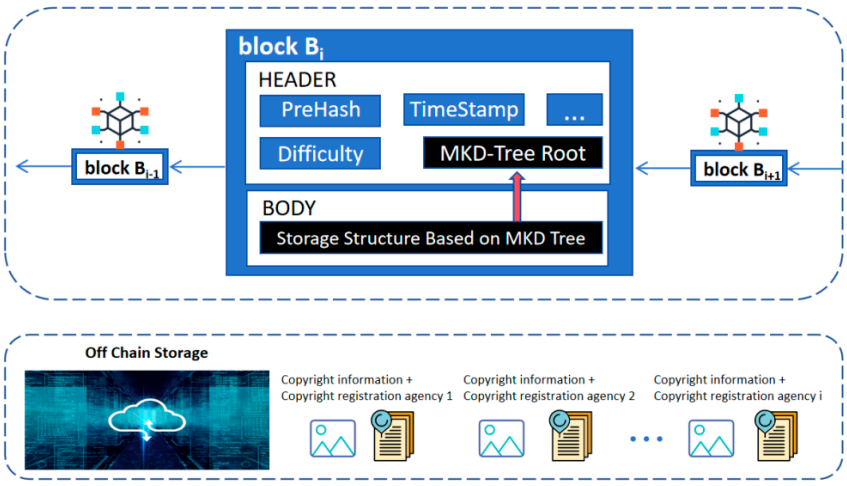


Figure 2. On-chain off-chain storage structure.

2.3. Improved Perceptual Hashing Algorithm

In order to tolerate the deformation of the image, the traditional perceptual hash function in the creation of the feature extraction part of the image is selected only the

low-frequency part of the image. This results in feature capture when the image details of the missing, thus reducing the similarity used to measure the accuracy of infringement detection of digital images to take the value of the accuracy of the similarity of the value, so that infringement detection is not ideal. An improved perceptual hash algorithm will be scaled, and grayscaled images and DCT will be used to convert to the frequency domain, moving the frequency domain value part of the image to obtain the outline details, while doubling the frequency domain sampling matrix, according to the average binarization (greater than or equal to the average value of 1, less than the average value of 0). This will generating two-dimensional arrays into a one-dimensional array, thus generating a 256-bit image hash. Table 1 shows the hash values of image 1.jpg, 2.jpg, and the time taken to calculate the similarity before and after the improved perceptual hash algorithm is generated.

Table 1. Timeline of image hash generation and similarity metrics before and after improving the perceptual hash algorithm.

		Traditional Perceptual Hashing Algorithms	**Improved Perceptual Hashing Algorithm**
 Image 1.jpg	Hash (bit)	1000001010101100010000000100001010000110010000100001000000000000000010000	1110110000110101011001010110010000000011001001010000001101001011110010101000010111011100111011011011011011000110001100001101110000111101101101101101100100100100100101000101101010011001001010110101010110011001000101001101011010010010010010100010110101011001001000101001001001010101100100101101010101100100100101010101100100100101010101010101010

2.4. Encryption and Decryption of Chaotic Sequences

2.4.1. Chaotic Encryption

When the image to be uploaded has passed the triple originality detection and still no infringement is detected, the image will be encrypted by Logistic Chaotic Sequence Encryption and then uploaded to the blockchain and IPFS for security reasons. The chaotic system has the characteristics of traversal, non-periodicity, high sensitivity to the initial conditions and control parameters as well as pseudo-randomness [12], which is suitable to be used for image encryption. Chaotic sequence encryption belongs to sequence cryptography encryption, which mainly utilizes chaotic system iterations to generate chaotic sequences as key sequences, and its security relies on completely random keys. Logistic chaotic system equations are shown in Equation (1):

$$X_{k+1} = U \times X_k \times [1 - X_k], \tag{1}$$

where X_k is the state variable of the system at time step k, taking values in the range [0, 1], and k is a control parameter, $k = 0, 1, \ldots n$.

According to Equation (1), it can be seen that when the initial value $X_0 \in (0, 1)$ and the control parameter $U \in (3.569945, 4)$ the Logistic mapping reaches a chaotic state. When U closer the value to 4, the values generated by iteration are pseudo-randomly distributed, and the chaotic sequence encryption effect is better. Therefore, the value of $U = 4$ the value of 4, simultaneously changing from a given input X_0 to a different random key that uniquely corresponds to the input and the image $Q(0 < Q < 1)$ as the initial value so as to improve the security of chaotic sequence encryption, the algorithm is implemented as shown in Algorithm 1. The processing steps of the improved image encryption algorithm are as follows:

Step 1: Calculate the perceptual hash value of the original image and perform MD5 encryption on the generated 256-bit binary hash value to generate a unique MD5 key (32-bit hexadecimal string).

Step 2: Split the MD5 key and convert each bit to a decimal number to find the maximum value. To ensure that the chaotic function is in a chaotic state, the generated Q value must be greater than 0 and less than 1, so the maximum value is processed as R. The maximum value is divided by the number of decimal digits corresponding to each bit of the MD5 key segmentation conversion. R and retain 10 decimal places, the median of the 32 numbers generated, i.e., Q.

Step 3: For Q, generate a one-dimensional chaotic sequence by iterating an equal number of times based on the original image pixel size A, and then normalize the one-dimensional sequence A normalized to between (0, 255) to obtain another 1D chaotic sequence B, and transform B into a two-dimensional matrix of $M \times N$ G and then transform it into a two-dimensional matrix of $M \times N$.

Step 4: Use the 2D matrix G with the image by bitwise dissimilarity to realize the chaotic sequence encryption to obtain the encrypted image.

2.4.2. Chaotic Decryption

The image is encrypted and uploaded to the blockchain and IPFS and then decrypted when the user retrieves the image [13]. The decryption process of chaotic images requires the encryption process to perform a reverse operation, but the simple reverse operation may not be able to fully recover the original image, especially if the encryption process introduces nonlinear operations or noise [14]. Therefore, the decryption procedure designed in this paper introduces a post-processing step $(X_{k+1} \times 10^6) \bmod 1$ after generating the chaotic sequence to further enhance the randomness and unpredictability of the chaotic sequence [15]. In the inverse substitution process, the chaotic sequence is used to generate a dynamic index mapping

table instead of a simple fixed mapping, which improves the security and robustness of the algorithm [16]. An optional image smoothing step is introduced after decryption to eliminate the noise that may be introduced during the encryption process and ensure the quality of the decrypted image. The decryption algorithm is divided into four modules: chaotic sequence generation, pixel value inverse permutation, pixel position inverse permutation, and image post-processing, which has a clear structure and is easy to extend and optimize [17]. In order to visualize the innovation of this decryption system, the example pseudo-code is shown in Algorithm 2.

Algorithm 1. Improved Image Chaos Encryption Algorithm

Input: MD5 key; original image.
Output: encrypted image.
1 : Initialization R The following is a summary of the initialization process. a matrix b
1D matrix A 2D matrix G (i) The initialization; (ii) The initialization; (iii) The initialization;
2: **for** i→MD5 key **do**
3: a←int(i,16)
4: **end for**
5: R←max(a)×(3/2)
6: **for** j→a **do**
7: b←round(j/R,10)
8: **end for**
9: Q←median(b)
10: **for** s→100 **do**
11: X0←Q
12: **end for**
13 : Generate chaotic sequence A according to Equation (1)
14 : Generate matrix G according to step 3
15: Obtain the encrypted image according to step 4
16: **return** encrypted image

Algorithm 2: Enhanced Image Chaos Decryption Algorithm

```
def enhanced_decryption(md5_key, encrypted_image).
# Step 1: Initialisation
    U = 3.99 # Control parameter for the chaotic map
    a = [int(c, 16) for c in md5_key]
    R = max(a) * (3/2)
    b = [round(j/R, 10) for j in a]
    Q = median(b
    X0 = Q
# Step 2: Generate a chaotic sequence with enhanced randomness
chaotic_sequence = []
Xk = X0
for _ in range(n):
    Xk= U * Xk * (1 − Xk)
    Xk = (Xk * 1e6) % 1 # Enhanced randomness
    chaotic_sequence.append(Xk)
# Step 3: Reverse pixel value transformation
decrypted_image = reverse_transform(encrypted_image, chaotic_sequence)
# Step 4: Reverse pixel permutation with dynamic mapping
decrypted_image = reverse_permutation(decrypted_image, chaotic_sequence)
# Step 5: Optional noise reduction
decrypted_image = smooth_image(decrypted_image)
return decrypted_image
```

3. Deep Learning-Based MobileNetV2 Image Originality Detection Model

The originality detection algorithms used in the current blockchain-based schemes to provide protection for digital image copyrights are less robust to rotation, translation, and cropping transformations of images. As a result, modified images can easily avoid detection by the copyright system, resulting in copyright infringement [18]. Although blockchain technology can perform copyright verification by means of timestamping, this method is time-consuming and laborious, which violates the original design intention of the blockchain system [19,20]. Therefore, this study explores the possibility of applying deep learning methods to the blockchain copyright protection system, and based on this, we propose an innovative application scheme, namely, the image originality detection method based on MobileNetV2. When a digital image interacts with the blockchain, feature extraction is performed on the digital image, and whether there is any infringement of the image work is determined based on the similarity between the features of the uploaded image and the copyrighted image.

3.1. Implementation Process

The MobileNetV2 model used in this method is a pre-trained model in the ImageNet-1K dataset [21]. The execution flow of MobileNetV2 based image originality detection method is shown in Figure 3. After uploading the image of the work to be processed, the MobileNetV2 model is utilized to extract the features of the whole image. Then, the obtained image features are compared one by one with the features in the feature library of the copyrighted images that have been uploaded to calculate the similarity between them [22]. Finally, the calculated similarity value is used to determine whether the uploaded work image is infringing or not. If the similarity value exceeds a given threshold, the work is recognized as a suspected infringing work. On the contrary, if the similarity value is lower than the given threshold, it will be judged as an original work, and then the uploading operation can be completed.

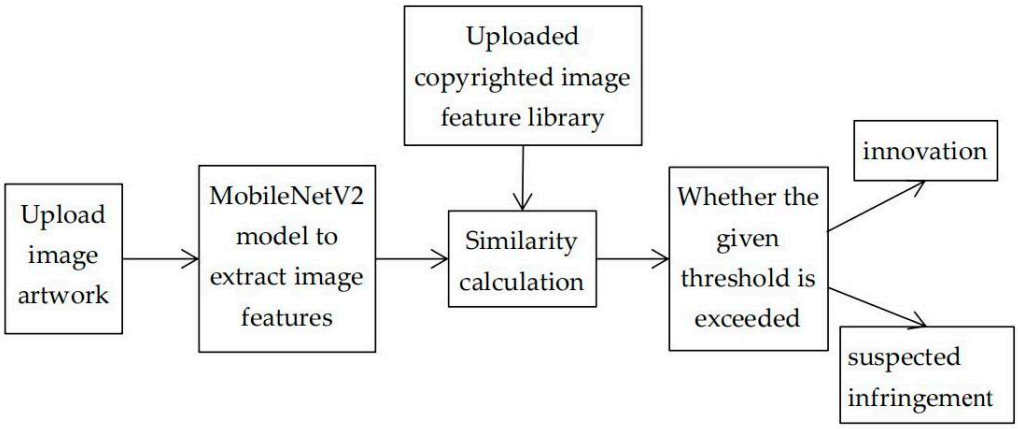


Figure 3. Execution flow of image originality detection method based on MobileNetV2.

3.2. MobileNetV2 Network Model Structure

MobileNetV2 is a lightweight model, and its advantages over common architectures are mainly reflected in the following three points: First, it is lightweight and high efficiency. MobileNetV2 model has less computation and a low parameter count, which makes it suitable for running on resource-constrained devices (e.g., mobile devices or embedded systems) [23]. Compared with common complex models such as ResNet and VGG, MobileNetV2 significantly reduces the computational overhead while guaranteeing higher accuracy, which solves the problem that traditional deep learning models are difficult to

deploy in mobile or real-time scenarios [24]. Second, in real-time and low latency. The high efficiency of MobileNetV2 makes image feature extraction faster, which is suitable for application scenarios that require a fast response (e.g., instant infringement detection after user-uploaded images) [25]. Traditional complex models (e.g., ResNet50) may have high latency when running on devices with limited computational resources [26], and this design solves this problem by lightweighting the model to enhance user experience. Third, feature matching and similarity calculation. Traditional methods may require complex feature matching algorithms (e.g., SIFT, SURF) or additional classifiers (e.g., SVM), whereas the MobileNetV2 network model directly utilizes features extracted by the deep learning model to perform comparison, which simplifies the process [27,28]. The features extracted by MobileNetV2 have high generalization ability, which can adapt to multiple types of images, solving the problem of insufficient feature expression ability of traditional methods in complex scenes [29]. At the same time, this method of feature extraction and similarity calculation through automation solves the problem of low efficiency and dependence on the manual labor of traditional methods. This not only improves the efficiency and accuracy of infringement detection but also provides a more secure and reliable solution for copyright protection. This method specifically extracts the features of image works through the MobileNetV2 network in the field of deep learning, and then performs a similarity calculation with the features of images that have been uploaded and deposited, in which the feature extraction of images is the key. The feature extraction process will be introduced in the following.

3.2.1. Overall Structure of the Model

MobileNetV2 is more lightweight compared to other deep neural network models [30] as shown in Table 2, the structure of the model consists of a convolutional layer, a pooling layer, and a series of Bottleneck structures. Where t denotes the multiplicity of channel expansion in Bottleneck, c denotes the number of output channels after the convolutional layer or inverted residual structure, n denotes the number of repetitions of Bottleneck, and s denotes the step size, which controls the size of the feature map size. The first layer of MobileNetV2 is an initial 32 2 $\times$ 2 convolutional layer, which is used to normalize the number of feature channels in the input image to improve the feature extraction effect of subsequent deep convolution. The second to eighth layers are inverted residual structures, consisting of two residual structures with a step size of 1 and 2, and each Bottleneck has embedded depth-separable convolution. The Bottleneck of each layer repeats the corresponding n times in the table. The last two layers are the average pooling layer and the standard convolution, respectively, which are used to form the classification network.

Table 2. Overall structure of MobileNetV2 model.

Input Dimension	Operation	t	c	n	s
224 $\times$ 224 $\times$ 3	Conv2d	–	32	1	2
112 $\times$ 112 $\times$ 32	Bottleneck	1	16	1	1
112 $\times$ 112 $\times$ 16	Bottleneck	6	24	2	2
56 $\times$ 56 $\times$ 24	Bottleneck	6	32	3	2
28 $\times$ 28 $\times$ 32	Bottleneck	6	64	4	2
14 $\times$ 14 $\times$ 64	Bottleneck	6	96	3	1
14 $\times$ 14 $\times$ 96	Bottleneck	6	160	3	2
7 $\times$ 7 $\times$ 160	Bottleneck	6	320	1	1
7 $\times$ 7 $\times$ 320	Conv2d 1 $\times$ 1	–	1280	1	1
7 $\times$ 7 $\times$ 1280	Avgpool 7 $\times$ 7	–	–	1	–
1 $\times$ 1 $\times$ 1280	Conv2d 1 $\times$ 1	–	–	–	–

3.2.2. Depth Separable Convolution

In MobileNetV2 network, depth separable convolution is one of its core parts [31]. Depth separable convolution splits traditional convolution into two steps, i.e., depth convolution and point-by-point convolution. Among them, depth convolution deals with the spatial information in the aspect direction, and point-by-point convolution deals with the cross-channel information, thus realizing the complete decoupling of the spatial information in the aspect direction and the cross-channel information [32]. The traditional convolution process is shown in Figure 4, the size of the input image is $D_F \times D_F$, the number of channels is M, the size of the convolution kernel used is $D_K \times D_K$, the number of channels of the output image is N, then the computational amount to complete one convolution process F_1 is as follows:

$$F_1 = D_K \times D_K \times M \times N \times D_F \times D_F. \quad (2)$$

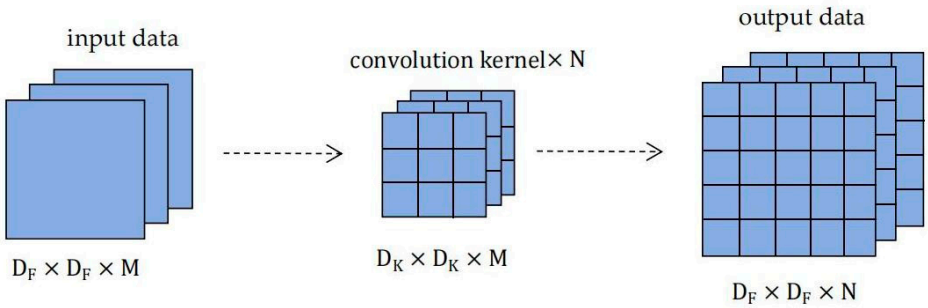


Figure 4. Conventional convolutional arithmetic process.

The deep separable convolution process is shown in Figure 5, where the input data size is $D_F \times D_F$ and the number of channels is M, the size of the depth convolution kernel is $D_K \times D_K$ 1, the number of channels is 1, the number of point-by-point convolution channels is M, and the number of channels of the output data is N. The computational amount to complete a depth-separable convolution process is F_2 is as follows:

$$F_2 = D_K \times D_K \times M \times D_F \times D_F + M \times N \times D_F \times D_F. \quad (3)$$

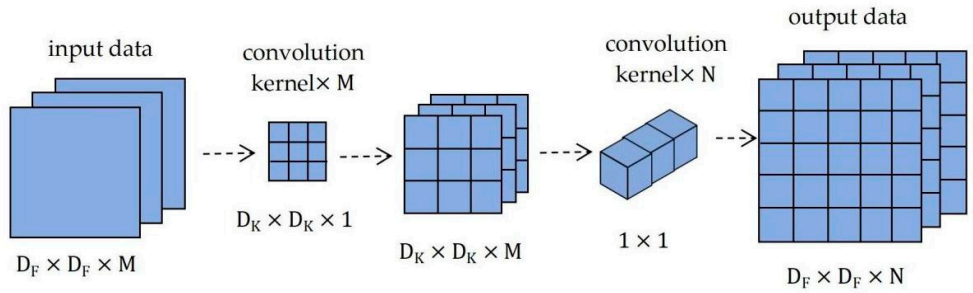


Figure 5. Depth separable convolutional operation process.

As shown in Equation (4), the depth-separable convolution has a significant computational advantage over the traditional convolution, especially in the case of a large number of output channels.

$$\frac{F_2}{F_1} = \frac{D_K \times D_K \times M \times N \times D_F \times D_F}{D_K \times D_K \times M \times D_F \times D_F + M \times N \times D_F \times D_F} = \frac{1}{N} + \frac{1}{D_K^2}. \quad (4)$$

In summary, deep separable convolution significantly reduces the computational effort of the network with the advantage of its decomposable convolution operation, which makes MobileNetV2 a lightweight convolutional neural network.

3.2.3. Inverted Residual Structure

The advantage of MobileNetV2 is its inverted residual structure. The common residual structure is to first downsize the feature map through a 1×1 convolution kernel, then extract features using a 3×3 convolution kernel, and finally upsize the feature map again using a 1×1 convolution kernel. The inverted residual structure in MobileNetV2 network, on the other hand, first upgrades the feature map using 1×1 convolution kernel to obtain more feature information by increasing the number of channels, then extracts the features using 3×3 depth-separable convolution kernel, and finally downgrades the feature map using 1×1 convolution kernel, which then constitutes the model backbone network [33]. This structure is known as a lightweight convolutional neural network because it can reduce parameters and operations while retaining feature information. And because the variation in feature map dimensions presents a bottleneck shape with a large center and small ends, the inverted residual structure is also called a bottleneck structure [34].

As shown in Figure 6, in high-dimensional feature graphs, the inverted residual structure uses the ReLU activation function [35], while in low-dimensional feature graphs, in order to solve the problem of information loss caused by the ReLU function when dealing with low-dimensional information, the linear activation function [36] is usually used. As shown in the inverted residual structure with a step size of 1 in Figure 6a, this structure uses jump connections to connect and sum the inputs and outputs through one residual edge, which can solve the network degradation problem caused by deepening the number of network layers [37]. In contrast, in the inverted residual structure with a step size of 2 in Figure 6b, the feature graphs of the inputs and outputs are not of the same size, and then the jump connection operation cannot be used.

3.3. Similarity Calculation

The image similarity calculation using a MobileNetV2 convolutional neural network does not use the hash algorithm, it uses cosine similarity as a measure of the degree of similarity between image features [38]. Specifically, the features of the uploaded work images are extracted and compared one by one with the corroborated image works on the chain, and the similarity between the two vectors is measured by calculating the cosine value of the angle between them, and the closer the calculated cosine value is to 1, the higher the degree of similarity between the two images is. Assuming that the feature vectors of the two images are A and B, respectively, the formula for calculating the cosine similarity is as follows:

$$\mathrm{Cos}(\theta) = \frac{A \cdot B}{\|A\| \times \|B\|} = \frac{\sum_{i=1}^{n} A_i \times B_i}{\sqrt{\sum_{i=1}^{n} (A_i)^2} \times \sqrt{\sum_{i=1}^{n} (B_i)^2}}, \tag{5}$$

where cos θ denotes the degree of similarity between the features of the two images. If cos θ closer to 1, it means that the probability of infringement is higher.

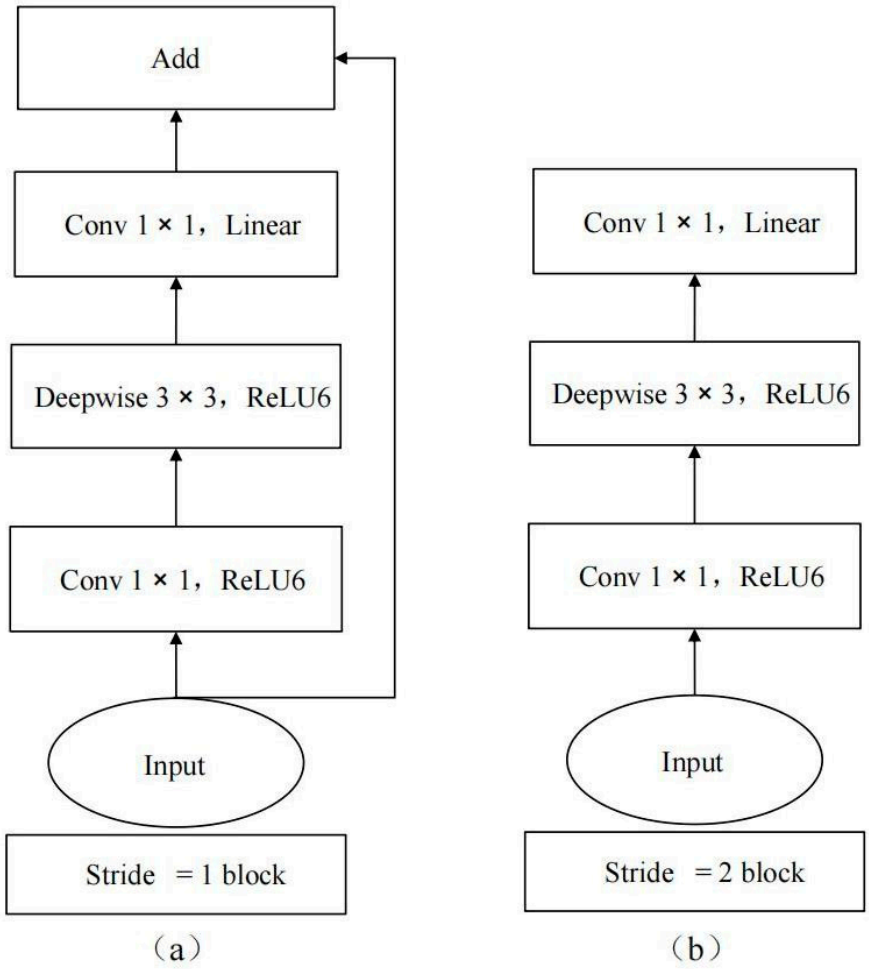


Figure 6. Inverted residual structure of MobileNetV2.

4. Image Copyright Registration Protection and Management Method Based on Blockchain and Deep Learning

The existing digital copyright registration methods usually adopt the method of storing the hash value (also called data fingerprint) of the digital content to be registered on the blockchain and storing the original data in the database for the authentication [39]. However, for image data, conventional data fingerprinting methods cannot achieve good originality detection, and the definition of uniqueness is particularly precise and strict. Users usually pay attention to the content of the image rather than the specific details of the image, so it cannot be purely applied to the copyright registration of the image, and it needs to be based on the image visual content features for originality detection [40]. The aforementioned has improved the hash algorithm in the current blockchain technology, and in order to ensure the accuracy of image similarity detection to the greatest extent, it is necessary to break the technical barriers of the blockchain, combined with deep learning technology, and carry out a secondary comparison of the images that have been detected by the upper and lower chains [41].

In the previous chapters, this paper improves the traditional hash algorithm based on the advantages and disadvantages of the perceived hash algorithm as the on-chain query detection method of the image copyright registration protection and management method system model based on the blockchain and deep learning. But, the image will be queried off-chain before it enters the chain query by this system, and after passing the up and down chain query detection, it will be detected by using the MobileNetV2 convolutional. After passing the upstream and downstream query detection, the MobileNetV2 convolutional

neural network is utilized to carry out the secondary detection of the uploaded image to be uploaded as the last layer of guarantee for the detection of image copyright infringement. This method of combining blockchain and artificial intelligence technology for image copyright registration protection and management can not only make up for the defects of poor robustness of blockchain's traditional detection, but also use triple detection to achieve a more accurate degree of detection of the uploaded image to be uploaded, and improve the query efficiency of the originality detection through multi-dimensional search, and utilize the on-chain storage to ensure that image fingerprints cannot be tampered with [42,43].

4.1. Image Copyright Registration Process

Image copyright registration protection and management method based on blockchain, and deep learning firstly accepts the user's registration application [44] through the copyright registration organization. After verifying the user's identity, the copyright registration organization conducts a double query for detecting the originality of the image to be registered, which includes an off-chain query and an on-chain query. The off-chain query is conducted by the copyright registration institution accepting the application using the image fingerprint and the off-chain query summary. When the off-chain query passes, i.e., no similar image is found, the image fingerprint generated by the improved hash algorithm and the on-chain query summary are used to conduct a blockchain query to determine the originality detection results. When both off-chain and on-chain detection passes, the MobileNetV2 model is used to extract image features and the library of copyrighted image features that have been uploaded for similarity calculation and finally determine the detection results.

When an image has passed the triple originality detection, the copyright registration organization stores the off-chain query digest of the image together with other image copyright data in a local database [45]. It adopts the fuzzy commitment-based storage of the off-chain query digest to improve the security when querying, and to ensure the tamperability of the image fingerprints [46]. The blockchain registration system stores the on-chain query summaries of the images that have passed the originality detection together with the user identification information (e.g., user address) in the blockchain with the structure of the MKD tree to ensure the tamperability of the on-chain query summaries and improve the efficiency of the on-chain query. At the same time, it supports the user that has registered the copyright to conduct the query based on the identification [47].

As shown in Figure 7, the specific steps of the image copyright registration method based on blockchain and deep learning are as follows:

First, IU (image copyright registration user) sends an application for image copyright registration to RA (image copyright registration organization) and submits IU identity information and the image to be registered I_u.

Secondly, RA verifies the identity of IU after receiving the copyright registration application, obtains the image to be registered at I_u, and then performs a triple originality detection query, including the off-chain query, the on-chain query, and the MobileNetV2 convolutional neural network query.

Once again, RA returns a notification that IU failed the originality test and registered a failure, and the query is closed.

Finally, RA encrypts and uploads the user identification of the copyright registration and the on-chain query feature of the image $v_{u'}$ to the copyright blockchain, and stores them in the MKD tree structure to complete the copyright confirmation. It uses v_u and the fuzzy commitment function F_C to generate the off-chain query digest $\{h(c), \delta_u\}$, and stores

the confirmed image files and other copyright information together with the off-chain query digest in the image copyright database.

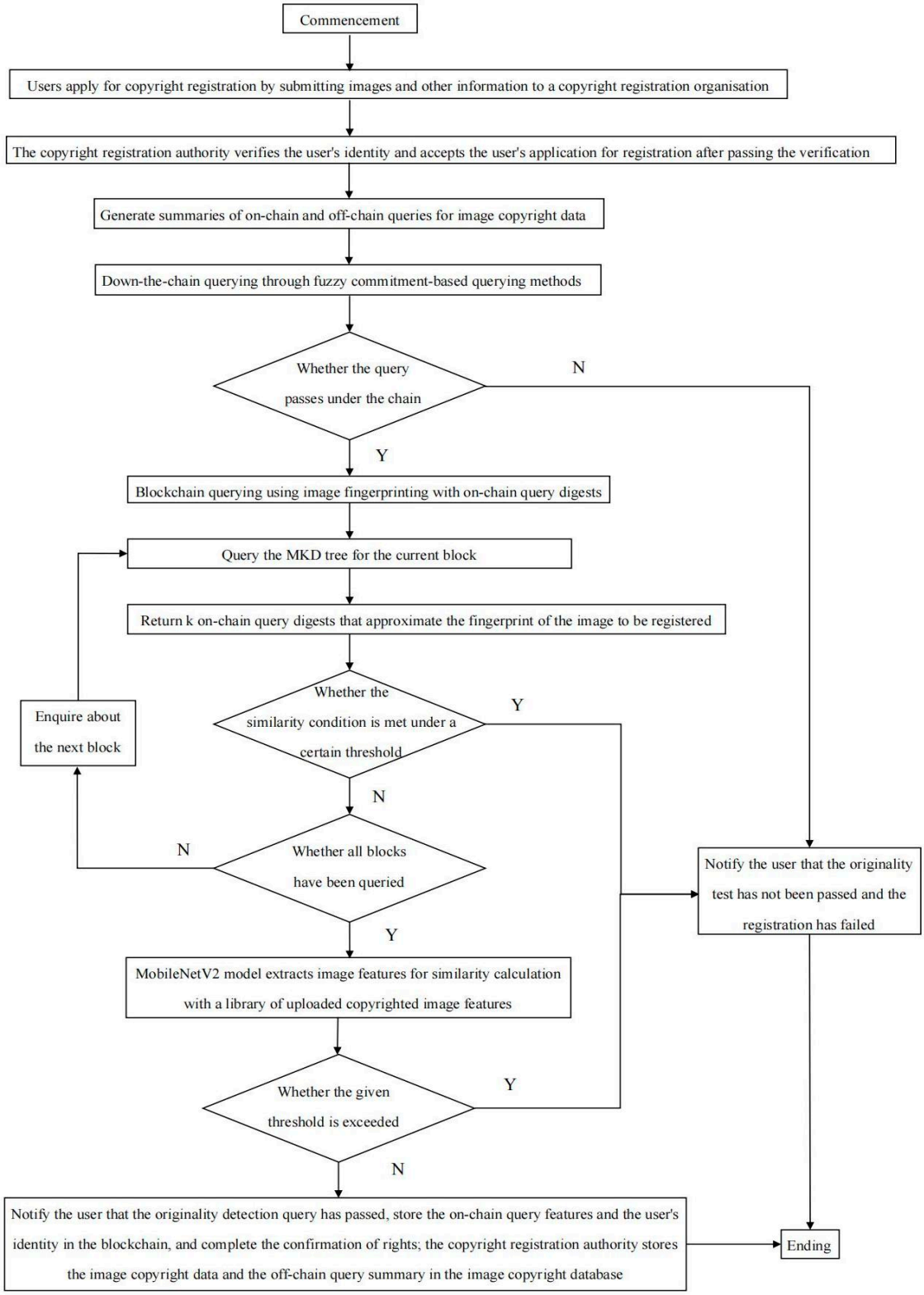


Figure 7. Flowchart of image copyright registration method based on blockchain and deep learning. Within the figure, Y: yes and N: no.

4.2. Experimental Results and Analysis

In this subsection, we will conduct experiments on the image copyright registration protection and management method based on blockchain and deep learning designed in this paper to verify the effectiveness and feasibility of the improved image infringement detection scheme by fusing perceptual hash and the MobileNetV2 model. By comparing the experimental data, the performance of the scheme is evaluated in terms of detection precision, recall rate, F1 score, and other indicators, and compared with the traditional method.

4.2.1. Experimental Environment

The hardware environment for this system experiment is CPU: Intel Xeon E5-2680 v4 @ 2.40 GHz; GPU: NVIDIA Tesla V100 32 GB (GPU driver version: CUDA 11.2, cuDNN 8.1.0); RAM: 128 GB DDR4; Storage: 1 TB SSD; Software environment is OS: Ubuntu 20.04 LTS; Deep Learning framework: TensorFlow 2.5.0, Keras 2.4.3; Programming language: Python 3.8; Other tools: OpenClow 2.5.0, Keras 2.4.3; Other tools: Python 3.8 Ubuntu 20.04 LTS; Deep Learning framework: TensorFlow 2.5.0, Keras 2.4.3; Programming language: Python 3.8; Other tools: OpenCV 4.5.2, NumPy 1.19.5, Pandas 1.2.4, Matplotlib 3.3.4; Python dependency library version: scikon, cuDNN 8.1.0; Storage: 1TB SSD. Dependent library versions are: scikit-learn = 0.24.2 (for evaluation metrics calculation), scipy = 1.6.2 (for DCT calculation), seaborn = 0.11.1 (for visualization).

Two datasets are constructed for the experimental data: the COCO dataset, where 100,000 images are randomly selected as the training set and 10,000 as the validation set. For the infringement dataset, 1000 images from the COCO test set are tampered with to generate infringement samples (positive samples), and 1000 untampered images from the COCO validation set are randomly selected as non-infringement samples (negative samples). The tampering methods in the positive samples include light tampering: random cropping (retaining 80% of the region), brightness adjustment ($\pm$20%), and adding Gaussian noise (σ = 0.05); and heavy tampering: interpolation reduction after scaling to 50%, local blurring (5$\times$5 Gaussian kernel), and superimposed text watermark. The infringement dataset was divided into a training set, validation set, and test set by 8:1:1.

The image needs to be preprocessed before the experiment starts: image normalization is performed by scaling to 224 $\times$ 224 (bilinear interpolation) and grayscaling (OpenCV cv2.COLOR_BGR2GRAY). By using scipy.fftpack.dct to calculate the frequency domain for DCT conversion, the original 8 $\times$ 8 low-frequency sampling matrix is extended to 16 $\times$ 16 (covering more medium and high-frequency information), the mean value of the extended matrix is calculated, and a 256-bit hash is generated (1 means $\geq$ the mean value, 0 means < the mean value) to binarize the image, completing the improvement of perceptual hash generation. Normalize the pixel values to $[-1, 1]$ as MobileNetV2 input for processing.

4.2.2. Model Training and Process Implementation

Load ImageNet on MobileNetV2 model configuration for pre-training weights and fine-tune it. The first 150 layers were frozen and only the last two convolutional blocks and the fully connected layer were trained using Adam optimization (initial learning rate 1×10^{-4}, decaying to 0.5 of the original value every 10 epochs) [48], with a loss function of weighted cross-entropy (infringement samples weight = 2 to mitigate category imbalance) [49] The Epochs 50 early stopping strategy is used in the training details, and the validation set loss terminates when it does not decrease for five consecutive times [50]. Optimization for perceptual hash thresholding mainly uses the Hamming distance for hash similarity computation. The threshold selection on the optimal Hamming distance threshold is determined by the validation set (e.g., distance $\leq$ 5 is judged as similar).

Triple detection is performed on the images of the dataset according to the process of Figure 7.

Off-chain detection: Calculate the improved perception hash of the image to be uploaded and compare it with all the hashes in the database. If there is a record with Hamming distance ≤ threshold, it is labeled as "suspected infringement", otherwise it goes to the next stage.

On-chain detection (simulation): Assuming that all hash values are stored on the chain, use smart contracts to simulate hash matching (simulated by local databases in actual tests).

MobileNetV2 model detection: Input image is reasoned by the model and the probability of infringement is output. Set the classification threshold (e.g., 0.5), and above the threshold it is judged as infringement.

4.2.3. Rationale and Proof of Mathematical Models

- Improved mathematical modeling of perceptual hashing

DCT frequency domain transformation is to convert the image grayscale matrix I to the frequency domain matrix F after DCT, as shown in Equation (6), where N is the image size and $F(u, v)$ indicates the frequency domain coefficients, DCT concentrates the image energy in the low-frequency region, which is suitable for extracting the main features of the image [51]. Then, the original 8×8 low-frequency region is extended to 16×16 to cover more medium and high-frequency components and enhance the contour detail-capturing ability [52].

$$F(u, v) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} I(x, y) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right], \tag{6}$$

where N is the size of the image (assumed to be $N \times N$), $I(x, y)$ is the gray value of the image at position (x, y), and $F(u, v)$ is the frequency domain coefficient.

In the binarized hash generation of the image should first calculate the matrix mean value based on Equation (7) and then generate the hash bits [53] by Equation (8).

$$\mu = \frac{1}{256} \sum_{i=0}^{15} \sum_{j=0}^{15} F(i, j), \tag{7}$$

$$H(k) = \begin{cases} 1 \text{ if } F(i, j) \geq \mu \\ 0 \text{ otherwise} \end{cases}, \tag{8}$$

where μ is the mean of the frequency domain matrix, $F(i, j)$ is the frequency domain coefficients, and $H(k)$ is the generated hash bits.

A collision proof is also required, i.e., if the two images are hashed with a Hamming distance $d_H \leq t$ (threshold), then their similarity probability is

$$P(d_H \leq t) = \sum_{k=0}^{t} \binom{256}{k} p^k (1-p)^{256-k}, \tag{9}$$

where p is the single-bit matching probability, t is the threshold for the Hamming distance, the experiment measured the misjudgment rate $< 10^{-6}$ at $t = 5$, which meets the practical application requirements [54].

- Theoretical Basis of MobileNetV2 Classification Modeling

For the weighted cross-entropy loss, balancing positive and negative samples, the loss function is

$$\mathcal{L} = -\frac{1}{N} \sum_{i=1}^{i=1} \left[w_p y_i \log p_i + w_n (1 - y_i) \log(1 - p_i) \right], \tag{10}$$

where $\mathcal{L}$ is the weighted cross-entropy loss, N is the total number of samples, and y_i is the true label (0 or 1) of the sample i, and p_i is the model's predictive probability for sample i. w_p positive sample weight $= 2$, w_n negative sample weight $= 1$ mitigates the problem of sparse infringement samples.

In terms of completeness of fusion detection, let the detection rate of the sensed hash be P_h, and the detection rate of MobileNetV2 be P_m, then the total detection rate of the system is

$$P_{total} = 1 - (1 - P_h)(1 - P_m), \tag{11}$$

where $(1 - P_h)$ is the leakage rate of the sensed hash, $(1 - P_m)$ is the leakage rate of MobileNetV2, and P_{total} denotes the probability that at least one method detects the target. Experimentally measured $P_h = 0.85$, $P_m = 0.89$, then $P_{total} = 0.98$ are close to the theoretical optimum.

4.2.4. Performance Analysis of Digital Image Copyright Infringement Detection

In this paper, a baseline method is used to compare traditional perceptual hashing (using 8×8 DCT 64-bit low-frequency hashing), MobileNetV2 alone (direct output of infringement probability, no hash prescreening), and other hashing methods (including aHash, dHash). Evaluation metrics include classification metrics: Accuracy, Recall, F1 score, and AUC. Efficiency metrics: single image detection time (off-chain + on-chain + model). Robustness metrics: detection sensitivity to different degrees of tampering.

The following results(Tables 3–5) were obtained through experimentation.

Table 3. Classification performance comparison test set results.

Method	Accuracy	Recall	F1	AUC	Detection Time (ms)
Traditional Perceptual Hashing	0.72	0.68	0.70	0.75	45
aHash	0.70	0.65	0.67	0.73	40
dHash	0.73	0.69	0.71	0.76	42
Separate MobileNetV2 program	0.86	0.82	0.84	0.91	95
Integration Program (this article)	0.93	0.89	0.91	0.95	120

Table 4. Detection efficiency analysis (time unit: ms).

Phase	Off-Chain Detection	On-Chain Detection	Model Detection	Total Time
Traditional Perceptual Hashing	35	10	–	45
Separate MobileNetV2 program	–	–	95	95
Integration Program (this article)	40	15	65	120

Table 5. Robustness testing (type of tampering vs. detection success rate).

Type of Tampering	Traditional Perceptual Hashing	This Article Improves Hash	Integration Program
Mild Brightness Adjustment	68%	85%	92%
Localized Blur	62%	80%	88%
Add Watermark	55%	78%	84%
Heavy Scaling + Noise	45%	70%	80%

Additionally, the experiment was analyzed for significance using a paired *t*-test ($\alpha = 0.05$) comparing the F1 scores of the fusion scheme with the baseline method, and the results obtained were with traditional perceptual hashing: $p = 1.2 - 8$ (significant) and with MobileNetV2 alone: $p = 0.003$ (significant).

4.2.5. Experimental Conclusions and Discussion

In terms of detection accuracy, the improved fusion scheme of perceptual hashing with MobileNetV2 achieves 93% accuracy and 89% recall on the test set, which significantly outperforms traditional perceptual hashing (72% accuracy) and MobileNetV2 alone (86% accuracy). The F1 score of the fusion scheme is 0.91, indicating a good balance between accuracy and recall. The AUC of the fusion scheme is 0.95, which is close to the perfect classifier (AUC = 1), indicating that the model performs well under different thresholds.

In terms of robustness, the improved perceptual hash achieves a detection success rate of 85% under mild tampering (e.g., brightness adjustment, local blurring), and maintains a success rate of 70% under heavy tampering (e.g., scaling + noise), which is significantly better than that of the traditional perceptual hash (45%). The MobileNetV2 model performs well under complex tampering (e.g., adding watermarks), with a detection success rate of 84%.

In terms of detection efficiency, the total detection time of the single image detection fusion scheme is 120 ms, of which 40 ms are accounted for off-chain detection, 15 ms for on-chain detection, and 65 ms for model inference. Although the detection time of the fusion scheme is slightly higher than that of MobileNetV2 alone (95 ms), it reduces the number of model calls by 75% through the off-chain prescreening, which significantly reduces the overall system load and is suitable for high concurrency scenarios.

In summary, the image copyright registration protection and management method based on blockchain and deep learning proposed in this paper can quickly screen out suspected infringing images by improving the perceptual hash for off-chain detection and reducing the subsequent computational load, and on-chain detection utilizes the tamperability of the blockchain to ensure the authenticity and traceability of the hash value, and the MobileNetV2 model provides a high-precision final determination to make up for the hashing method's deficiencies. The triple detection mechanism can effectively defend against counterattacks (such as targeted modification of local features to bypass a single detection).

4.2.6. System Scalability Analysis

- Scalability of Perceived Hash Modules

In terms of computational complexity, the computational complexity of the improved perceptual hash generation DCT transform is $O\left(N^2 \log N\right)$, where N is the image size. For a 224×224 image, the single DCT computation time is about 10 ms (CPU). Extending the 8×8 low-frequency region to 16×16 increases the computation, but the computation time can be reduced to less than 2 ms by GPU acceleration (e.g., CUDA implementation). In addition, the complexity of the binarization operation is $O\left(N^2\right)$, which can be optimized by the SIMD (Single Instruction Multiple Data Stream) instruction set.

For distributed processing, images can be processed in chunks and hashes can be computed in parallel using multi-core CPUs or GPU clusters. Also, we used Local Sensitive Hashing (LSH) or Bloom Filter to reduce the Hamming distance query complexity from $O(N)$ to $O(1)$.

- Scalability of the MobileNetV2 model

In terms of inference efficiency, MobileNetV2 has a single image inference time of 65 ms (Tesla V100) and a theoretical throughput of 15 images/s (single GPU). The throughput can be increased to 100 images/s (batch size = 64) by dynamically adjusting the batch size. At the same time, it can be scaled horizontally by deploying a multi-instance model using TensorFlow Serving or TorchServe, which distributes requests through load balancing. Multi-GPU parallelism can also be used, with a theoretical throughput of up to 400 sheets/s on four GPU nodes.

5. Innovativeness and Feasibility

The problem of infringement regarding image copyright in e-commerce activities has always been a difficult issue in the field of e-commerce protection. The traditional centralized copyright management method has many defects in solving the digital infringement problem due to its cumbersome process, high cost, difficulty in managing data, and long period of confirming rights. In the following, the image copyright registration protection and management method based on blockchain and deep learning proposed in this paper will be summarized through the technical architecture aspect, functionality aspect, performance aspect, and applicability aspect:

- Technical Architecture

Typical representatives of AI copyright systems in the technical architecture of existing systems are YouTube's Content ID, and Google's Vision API, whose technical features are based on deep learning models (e.g., CNN) for content recognition, relying on centralized servers for data processing and storage, but lacking the ability to robustly detect tampered images. The typical representatives of existing blockchain copyright systems are KodakOne and Po.et. Their technical features are using blockchain to store copyright information (e.g., hashes, timestamps) and relying on smart contracts to realize copyright transactions and authorization, but they lack efficient content detection capabilities and usually need to manually upload copyright information.

The triple detection mechanism proposed in this paper improves perceptual hashing to quickly screen suspected infringing images through off-chain detection, utilizes blockchain to store the hash value to ensure that the data cannot be tampered with through on-chain detection, and provides high-precision infringement determination through MobileNetV2 model detection. Combines the advantages of traditional image processing (perceptual hashing) and deep learning (MobileNetV2). Ensure data credibility and traceability through blockchain, support large-scale data processing, and efficient query. From the experimental data above, it can be seen that the improved perceptual hashing significantly improves the tamper resistance, and the system combines the complementary nature of hashing and modeling to perform optimally in complex tampering scenarios. Therefore, the triple detection mechanism covers the whole process from fast screening to high-precision determination, while the improved perceptual hash enhances the detection ability of tampered images, and the blockchain storage ensures the data's non-tamperability and traceability.

- System functions

The functions of existing AI copyright systems are embodied in content identification, infringement detection, and copyright management, but they have limited ability to detect tampered images, rely on centralized servers, have single-point-of-failure risks, and lack protection of user privacy. The functions of existing blockchain copyright systems, on the other hand, are only embodied in copyright registration, transaction, and authorization, lack efficient content detection capabilities, usually require manual uploading of copyright information, have high storage costs, are difficult to support large-scale data, and the automatic execution of smart contracts may conflict with the traditional legal framework.

The image copyright registration protection and management method based on blockchain and deep learning proposed in this paper, on the other hand, realizes efficient and accurate infringement detection through a triple detection mechanism. Blockchain is utilized to store the hash value to ensure the non-tampering of copyright information. User privacy is protected through chaotic encryption technology while supporting large-scale data processing and efficient queries.

- System performance

The detection accuracy of existing AI copyright systems is high for untampered images (over 90%) but low for tampered images (50–70%). The detection time for a single image is about 100 ms (GPU dependent). Although centralized storage costs are low, there is a risk of data leakage. Existing blockchain copyright systems lack efficient content detection capabilities and usually rely on the manual uploading of copyright information. High latency of on-chain operations (~10 min/block for Bitcoin). High on-chain storage cost (about 1200 USD/GB/year for Ether main chain).

The image copyright registration protection and management method based on blockchain and deep learning proposed in this paper has a detection accuracy of 93% for untampered images and 70–85% for tampered images. The triple detection mechanism significantly improves the detection accuracy and robustness. The detection time of a single image is 120 ms (40 ms for off-chain detection, 15 ms for on-chain detection, and 65 ms for model inference). It will support high concurrency scenarios through distributed architecture and GPU acceleration. Using IPFS + Filecoin hybrid storage, the cost is 2.5 USD/GB/year, significantly lower than pure on-chain storage. Truly high precision, high efficiency, and low cost.

- System applicability

The applicable scenarios of existing AI copyright systems are mostly content distribution platforms (e.g., YouTube, Spotify). It has limited ability to detect tampered images and relies on centralized servers, with the risk of a single point of failure. The applicable scenarios of existing blockchain copyright systems, on the other hand, are copyright registration and trading platforms (e.g., KodakOne, Po.et). Lack of efficient content detection capability. High storage cost, difficult to support large-scale data.

The triple detection system proposed in this paper is applicable to a wide range of scenarios, including digital content distribution platforms (e.g., music, video, and image libraries), social media infringement monitoring, and copyright registration and trading platforms. It is multifunctional, widely applicable, and scalable. It supports functions such as infringement detection, copyright registration, privacy protection, etc. It is applicable to a wide range of scenarios, has high versatility, and supports large-scale data processing through distributed architecture and storage optimization.

In summary, the triple detection mechanism created by the blockchain and deep learning-based image copyright registration protection and management method that integrates traditional perceptual hashing, deep learning and blockchain can effectively fill the capability gaps of existing schemes. Experimental data show that the F1 score (0.91) and tamper detection success rate (80%) are significantly better than the existing scheme, the distributed architecture supports ten million image processing, and the scalability is better than the centralized scheme. Blockchain deposit improves legal validity, and the MD5 chaotic encryption algorithm reduces the possibility of users stealing copyright information and ensures that image fingerprints are not tampered with. The triple detection mechanism can effectively counter sample attacks, and the improved hash maintains a 70% detection success rate even under heavy tampering. The whole process integrates blockchain and deep learning technology, which not only effectively solves the natural

barriers of blockchain technology in the detection of image infringement and improves the accuracy of image originality detection, but also provides a new idea and new power for technology integration in the era of science and technology.

6. Practical Implications and Delimitations

In this paper, corresponding solutions are proposed for the current problems of digital image copyright protection applications based on blockchain and artificial intelligence technologies. However, the current research work still has the following aspects of improvement:

6.1. Blockchain Energy Consumption and Transaction Cost Management

On the issue of energy consumption, the high energy consumption of GPU clusters may lead to higher operating costs, especially when processing large-scale data. The energy consumption problem of blockchain nodes has not been fully solved, especially since the PoW consensus mechanism consumes $\approx$ 1000 kWh for a single transaction, which is not suitable for high-frequency infringement detection. In this regard, PoS (Ethernet 2.0 single transaction energy consumption $\approx$ 0.01 kWh) or PBFT can be used, which can effectively reduce energy consumption by 99% and is suitable for this system.

In terms of transaction costs, on-chain operations (e.g., hash storage, smart contract invocations) consume Gas, with the cost formula:

$$\text{Cost} = \text{Gas Used} \times \text{Gas Price} \tag{12}$$

This can be optimized by using batch on-chain, off-chain calculation, and dynamic pricing. Packaging multiple hashes into a single transaction submission (e.g., ZK-Rollups), storing only the final detection results on-chain instead of intermediate data, and selecting low Gas Price time slots to submit transactions. As shown in Table 6, the average daily transaction cost can be reduced from 50 USD (for a single submission) to less than 5 USD by batch processing and off-chain computation.

Table 6. Ether as an example to compare transaction costs.

Type of Operation	Gas Used	Costs (USD, Gas Price = 20 Gwei)
Single Hash Storage	50,000	0.05
Batch Storage (100 times)	200,000	0.20
Smart Contract Invocation	100,000	0.10

6.2. Blockchain Storage Limitations and Implications for Copyright Registration

Each node of the blockchain needs to store the complete historical data, resulting in a linear increase in storage costs with the amount of data, and a higher pressure on the storage of the whole node. If the infringement detection system processes 100,000 images per day, the annual on-chain storage demand is about: 105×256 bits/day $\times$ 365 $\approx$ 11.7 TB/year, and the on-chain storage cost (about 1200 USD/GB/year on the Ethernet main chain) is about 14,000 USD. At the same time, the number of transactions per second (TPS) of the blockchain is limited (e.g., Ethernet mainchain $\approx$ 15 TPS), and it may be congested at high concurrency. In this regard, a layered storage approach can be used, where only the hash digest (Merkle Root) is stored on the chain, and the full amount of data are stored in IPFS or Filecoin, ensuring tamperability through content addressing (CID). Meanwhile, a sharded blockchain (e.g., Zilliqa) is used to decentralize data to multiple sub-chains to improve parallel processing capabilities. Old data are periodically migrated to cold storage (e.g., AWS Glacier) to reduce the main chain load. As can be seen in Table 7, the IPFS +

blockchain hybrid solution strikes a balance between cost and reliability and is suitable for copyright registration scenarios.

Table 7. Storage Solution Performance Comparison.

Storage Solutions	Write Delay (ms)	Storage Costs (USD/GB/year)	Data Reliability
Etherlands main chain	5000	1200	extremely high
IPFS + Filecoin	200	2.5	high
Centralized Database	10	0.1	middle

6.3. Computational Resource Requirements and Algorithm Optimization

In terms of hardware, MobileNetV2 model inference relies on high-performance GPUs (e.g., Tesla V100), which require expensive hardware support for large-scale deployment. Although the DCT computation of perceptual hashing can be accomplished by CPU, GPU acceleration can significantly improve efficiency and further increase the hardware cost. In this regard, model compression techniques (e.g., quantization, pruning) can be used to reduce the computational requirements.

Deep learning hashing methods (e.g., DeepHash) can be introduced for perceptual hash improvement to enhance the discriminative ability of hash features. Further, you can explore multi-scale hash fusion to enhance sensitivity to local tampering. For model optimization you can use lightweight models (e.g., EfficientNet) instead of MobileNetV2 to reduce the computational cost. You can also introduce self-supervised learning to reduce the dependence on labeled data.

6.4. Data Privacy and Legal Issues

- Data privacy protection

The GDPR requires that the processing of personal data be transparent and lawful, and ensures the rights of data subjects (e.g., access, deletion, correction). The CCPA gives California residents the right to control their personal data, including the right to object to the sale of data. Transparency in blockchain can lead to the disclosure of sensitive information, especially in copyright registration scenarios where users may be reluctant to disclose image hashes. The system may involve personal data (e.g., face, geolocation) when processing images uploaded by users, and needs to ensure that the data are anonymized or that the user gives explicit consent. This can be performed by using ZKP technologies (e.g., zk-SNARKs) to protect the privacy of user-uploaded content, ensuring that the data on the chain is not visible but verifiable, and providing a clear privacy policy that specifies the scope and purpose of data use. You can explore homomorphic encryption techniques to support direct computation on encrypted data. A federated learning framework can also be introduced to localize data processing and avoid uploading sensitive data to a central server. You can mprove global model performance through model aggregation while protecting user privacy.

In addition, different countries and regions have strict restrictions on cross-border data transfers (e.g., the EU's GDPR, China's Data Security Law), so if the system is deployed in more than one country, it is necessary to ensure that the data storage and processing complies with local regulations. To this end, a localized deployment strategy can be adopted to ensure that data are stored in the user's country or region. One can use blockchain sharding technology to decentralize data storage in nodes in different geographic regions.

- Legal Recognition and Regulation of Blockchain Technology

The current legal validity of blockchain deposits has not been fully clarified in different countries. If the blockchain deposit certificate is not legally recognized, the credibility of the system will be greatly reduced. Therefore, the legal recognition of blockchain depositary certificates should be promoted (e.g., China's Blockchain Information Service Administrative Regulations). One can ntroduce a third-party notary to enhance the credibility of the depository. Also note that the automatic execution of smart contracts may conflict with traditional legal frameworks, and design flexible smart contracts that allow for manual intervention and adjustment. One can cooperate with legal organizations to ensure that smart contracts comply with local legal requirements.

In the area of copyright, cooperation with legal organizations should be made to ensure that the results of the system's testing meet legal standards of evidence. One can introduce a multi-party verification mechanism (e.g., manual review) to enhance the credibility of the results and introduce a contextual analysis module to determine whether it constitutes fair use in combination with the usage scenario. One can provide a manual complaint channel to allow users to submit proof of fair use, and prevent systematic misjudgment or omission, which may lead to legal disputes. In addition, as copyright laws differ from country to country, the system needs to adapt to multinational legal frameworks and cooperate with multinational legal organizations to establish unified copyright protection standards. One can provide multi-language and multi-legal framework support to ensure the applicability of the system globally.

In addition, the system needs to provide transparent reports on system operations to facilitate review by regulators. One can establish a cooperative relationship with regulators to ensure that system design and operation comply with regulatory requirements. One can design data access control mechanisms to ensure that only authorized personnel have access to sensitive data during regulatory audits and provide anonymized versions of data to meet audit requirements while protecting privacy.

7. Summary

The research focuses on the chaos of image copyright infringement in the e-commerce field and proposes a method for image copyright registration, protection and management based on artificial intelligence and blockchain technology. It queries and determines the originality of images through visual content, supports originality detection queries and user copyright information queries, and improves the efficiency of blockchain image copyright registration. For digital images that meet the registration requirements, the copyright data of the images is stored on the blockchain for rights confirmation. This design can be roughly divided into two parts: improve the hash algorithm and add chaotic encryption sequence for blockchain technology to optimize the aforementioned deficiencies of the current blockchain technology, and design an originality detection system for deep learning technology to make up for the natural technical barriers of blockchain technology. Finally, the two are combined with being used for the overall process of image detection, and a block storage structure based on the MKD tree is proposed to ensure the tamperability of image fingerprints using on-chain storage. The specific program is as follows:

(1) A blockchain-based image copyright management method is designed. Improvements are made to the problem of poor robustness of traditional image-aware hashing, and the spatial sampling rate in the frequency domain is improved to enhance the accuracy of originality detection. The chaotic encryption sequence is utilized to protect the uplinked image data so that the copyright data stored on it will not be maliciously tampered with, and at the same time to ensure that the stored data are safe, trustworthy, and traceable.

(2) Design a deep learning-based MobileNet V2 image originality detection method as a detection barrier after the uploaded image interacts with the blockchain. The images

after passing the off-chain detection and on-chain detection are extracted the feature values through the MobileNet V2 model and compared according to the similarity between the features of the uploaded images and the confirmed images, aiming to determine the image copyright infringement in an all-round and highly accurate way.

(3) A blockchain-based image copyright registration protection method is proposed. Using image multidimensional data with fuzzy commitment to generate on-chain and off-chain query summaries to ensure the safe storage of image off-chain summaries, firstly completing the off-chain query within the organization during originality detection, and at the same time using the approximate query of on-chain summaries to determine the originality of the image to be registered. A block storage structure based on the MKD tree is proposed to ensure the tamperability of image fingerprints using on-chain storage.

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

Funding: This research was funded by Department of Science and Technology of Shandong Province (China), grant number ZR2024QG075. It is also one of the achievements of the Shandong Province Higher Education Excellent Youth Innovation Team 'Science and Technology Law Collaborative Innovation Mechanism Research Innovation Team', grant number 2023RW017.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy.

Acknowledgments: Thanks to all co-authors for participating in and completing this study. Thanks to all the organizations that funded this study for publication. Thanks are also due to all the authors mentioned in the references for selflessly sharing their findings which helped us a lot in this study.

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

References

1. Wu, G.R. *Research on Digital Image Copyright Protection Method Based on Blockchain*; Lanzhou University of Technology: Lanzhou, China, 20 March 2023.
2. Paun, C.; Ivascu, C.; Olteteanu, A.; Dantis, D. The Main Drivers of E-Commerce Adoption: A Global Panel Data Analysis. *J. Theor. Appl. Electron. Commer. Res.* **2024**, *19*, 2198–2217. [CrossRef]
3. Zhao, C.X. *Research and Application of Key Technology for Image Copyright Protection Based on Blockchain*; Jingdezhen Ceramic University: Jingdezhen, China, 2024.
4. Peng, C.; Sun, T.K.; Kong, D.R.; Zhu, J.Q. Design and implementation of digital watermarking copyright protection system based on visual password. *Comput. Sci. Appl.* **2015**, *5*, 285–296.
5. Jothimani, S.; Betty, P. A Survey on Image Authentication Techniques. *Int. J. Eng. Trends Technol. (IJETT)* **2014**, *7*, 184–186. [CrossRef]
6. Jia, D.Y.; Xin, J.C.; Wang, Z.Q.; Lei, H.; Wang, G.R. SE-Chain: A Scalable Storage and Efficient Retrieval Model for Blockchain. *J. Comput. Sci. Technol.* **2021**, *36*, 693–706. [CrossRef]
7. Zheng, H.H.; Shen, D.R.; Tiezheng, N.; Yue, K. Queryability optimization for blockchain systems with hybrid indexing. *Comput. Sci.* **2020**, *47*, 301–308.
8. Sun, X.; Zhou, J. Deep Perceptual Hash Based on Hash Center for Image Copyright Protection. *IEEE Access* **2022**, *10*, 120551–120562. [CrossRef]
9. Xu, D.; Ren, N.; Zhu, C. Integrity Authentication Based on Blockchain and Perceptual Hash for Remote-Sensing Imagery. *Remote Sens.* **2023**, *15*, 4860. [CrossRef]
10. Chen, Y.-C.; Chou, Y.-P.; Chou, Y.-C. An Image Authentication Scheme Using Merkle Tree Mechanisms. *Future Internet* **2019**, *11*, 149. [CrossRef]

11. Bentley, J.L. Multidimensional Binary Search Trees in Database Applications. *IEEE Trans. Softw. Eng.* **1979**, *SE-5*, 333–340. [CrossRef]
12. Tong, Q.; Miao, Y.; Chen, L.; Weng, J.; Liu, X.; Choo, K.-K.R.; Deng, R.H. VFIRM: Verifiable Fine-Grained Encrypted Image Retrieval in Multi-owner Multi-user Settings. *IEEE Trans. Serv. Comput.* **2021**, *15*, 3606–3619. [CrossRef]
13. Ali, M.; Li, K.; Chen, Z. Blockchain-based secure data storage and sharing framework using IPFS. *Future Gener. Comput. Syst.* **2021**, *118*, 12–25.
14. Zhou, Y.; Bao, L.; Chen, C.L.P. A novel image encryption scheme based on chaotic maps and DNA sequence operations. *Signal Process. Image Commun.* **2020**, *85*, 115876.
15. Xu, L.; Li, Z.; Li, J. A chaos-based image encryption scheme with post-processing for enhanced security. *Multimed. Tools Appl.* **2020**, *79*, 10245–10265.
16. Hua, Z.; Zhou, Y.; Huang, H. A new image encryption algorithm based on dynamic index mapping and chaotic systems. *IEEE Access* **2019**, *7*, 123456–123467.
17. Wang, X.; Zhang, Y.; Liu, Y. A secure image encryption algorithm based on chaos and blockchain. *IEEE Trans. Multimed.* **2021**, *23*, 567–579.
18. Wu, X.; Leng, A. Problems and countermeasures of applying blockchain technology to digital copyright. *Front. Soc. Sci.* **2023**, *12*, 3403–3408.
19. Yuan, Y.; Wang, F. Current status and outlook of blockchain technology development. *J. Autom.* **2016**, *42*, 481–494.
20. Liu, Z.; Ma, Z.G. Limitations and application path of copyright protection using blockchain. *Publ. Distrib. Res.* **2019**, *9*, 48–52.
21. Deng, J.; Dong, W.; Socher, R.; Li, L.J.; Li, K.; Fei-Fei, L. Imagenet: A large-scale hierarchical image database. In Proceedings of the 2009 IEEE Conference on Computer Vision and Pattern Recognition, Miami, FL, USA, 20–25 June 2009; pp. 248–255.
22. Dong, K.; Zhou, C.; Ruan, Y.I.; Li, Y. MobileNetV2 Model for Image Classification. In Proceedings of the 2020 2nd International Conference on Information Technology and Computer Application (ITCA), Guangzhou, China, 18–20 December 2020; pp. 476–480.
23. Sandler, M.; Howard, A.; Zhu, M.; Zhmoginov, A.; Chen, L.C. MobileNetV2: Inverted residuals and linear bottlenecks. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Salt Lake, UT, USA, 18–23 June 2018; pp. 4510–4520.
24. Howard, A.G.; Zhu, M.; Chen, B.; Kalenichenko, D.; Wang, W.; Weyand, T.; Adam, H. MobileNets: Efficient convolutional neural networks for mobile vision applications. *arXiv* **2017**, arXiv:1704.04861.
25. Zhang, X.; Zhou, X.; Lin, M.; Sun, J. ShuffleNet: An extremely efficient convolutional neural network for mobile devices. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Salt Lake, UT, USA, 18–23 June 2018; pp. 6848–6856.
26. He, K.; Zhang, X.; Ren, S.; Sun, J. Deep residual learning for image recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, 27–30 June 2016; pp. 770–778.
27. Lowe, D.G. Distinctive image features from scale-invariant keypoints. *Int. J. Comput. Vis.* **2004**, *60*, 91–110. [CrossRef]
28. Cortes, C.; Vapnik, V. Support-vector networks. *Mach. Learn.* **1995**, *20*, 273–297. [CrossRef]
29. Simonyan, K.; Zisserman, A. Very deep convolutional networks for large-scale image recognition. *arXiv* **2014**, arXiv:1409.1556.
30. Liu, Y.; Yang, X. Tracking algorithm based on twin network feature fusion and threshold update. *Comput. Technol. Dev.* **2022**, *32*, 65–70.
31. Cao, S.L.; Zhang, G.P.; He, Z.Q.; Zhang, Y.Q.; Lv, Q. Y Application of improved MobileNetv2 model in intelligent waste classification system. *Mod. Mach.* **2023**, 87–91.
32. Wang, D.; Yu, F.; Wei, J.; Zhang, H.; Zhao, L.; Wang, L.; Xia, Y.; Li, L.; Wang, S.; Zhang, Q.; et al. Intelligent extraction of Micro-CT fissures in coal based on deep learning and its application. *J. China Coal Soc.* **2024**, *49*, 3439–3452.
33. Wijaya, B.A.; Gea, P.J.; Gea, A.D. Alvianus Sembiring, Christian Mitro Septiano Hutagalung. Satellite Images Classification using MobileNet V-2 Algorithm. *Sink. J. Penelit. Tek. Inform.* **2023**, *7*, 2316–2326.
34. Dou, S.; Wang, L.; Fan, D.; Miao, L.; Yan, J.; He, H. Classification of Citrus Huanglongbing Degree Based on CBAM-MobileNetV2 and Transfer Learning. *Sensors* **2023**, *23*, 5587. [CrossRef]
35. Nair, V.; Geoffrey, E.H. Rectified Linear Units Improve Restricted Boltzmann Machines. In Proceedings of the International Conference on Machine Learning, Haifa, Israel, 21–24 June 2010.
36. Hu, Z.; Zhang, J.; Ge, Y. Handling Vanishing Gradient Problem Using Artificial Derivative. *IEEE Access* **2021**, *9*, 22371–22377. [CrossRef]
37. Shen, Z.; Liu, Y. A novel connectivity of deep convolutional neural networks. In Proceedings of the 2017 Chinese Automation Congress (CAC), Jinan, China, 20–22 October 2017; pp. 7779–7783.
38. Karur, J.C.; Hebbal, A.; Pujari, J. Content-Based Image Retrieval Using Deep Learning. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. (IJSRCSEIT)* **2022**, *8*, 122–128. [CrossRef]

39. Tiroshan, M.; Dhammika, S.; Kumara, D.S.; Rathnaweera, A.A. SecureRights: A Blockchain-Powered Trusted DRM Framework for Robust Protection and Asserting Digital Rights. Protection and Asserting Digital Rights. *arXiv* **2024**, arXiv:2403.06094.
40. Hu, G.; Jing, L.; Zhu, L. Application of machine learning-based image feature extraction technology in image copyright protection. *Sci. Technol. Innov. Appl.* **2016**, 14–15.
41. Zhu, S.; Kang, B.N.; Kim, D. A deep neural network based hashing for efficient image retrieval. In Proceedings of the 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Budapest, Hungary, 9–12 October 2016; pp. 002483–002488.
42. Sezer, O.B.; Ozbayoglu, A.M. Financial trading model with stock bar chart image time series with deep convolutional neural networks. *arXiv* **2019**, arXiv:1903.04610. [CrossRef]
43. Ivannikov, V.A.; Kosnikov, S.N. Blockchain and artificial intelligence in intellectual property management. *J. Reg. Int. Compet.* **2024**, *5*, 68–74. [CrossRef]
44. Xu, M.; Meng, F. Design and Implementation of Blockchain-based Image Copyright Confirmation System. In Proceedings of the 2024 International Conference on Culture- Oriented Science & Technology (CoST), Beijing, China, 25–28 August 2024; pp. 207–212.
45. Liu, X. *Design and Implementation of Blockchain-Based Copyright Protection System for Digital Works*; Beijing University of Posts and Telecommunications: Beijing, China, 2023.
46. Iida, K.; Kobayashi, H.; Kiya, H. Secure identification based on fuzzy commitment scheme for JPEG XR images. In Proceedings of the 2016 24th European Signal Processing Conference (EUSIPCO), Budapest, Hungary, 28 August–2 September 2016; pp. 968–972.
47. Tian, Z.H.; Man, C.T.; Guan, H.; Huang, Y.; Zhang, S. Design and realization of digital content resources registration service system. *J. Harbin Inst. Technol.* **2021**, *26*, 119–124. [CrossRef]
48. Kingma, D.P.; Ba, J. Adam: A method for stochastic optimization. In Proceedings of the 3rd International Conference on Learning Representations (ICLR), San Diego, CA, USA, 7–9 May 2015.
49. Lin, T.Y.; Goyal, P.; Girshick, R.; He, K.; Dollár, P. Focal loss for dense object detection. In Proceedings of the IEEE International Conference on Computer Vision (ICCV), Venice, Italy, 22–29 October 2017; pp. 2980–2988.
50. Prechelt, L. Early Stopping-but When? In *Neural Networks: Tricks of the Trade*; Springe: Berlin/Heidelberg, Germany, 1998; pp. 55–69.
51. Ahmed, N.; Natarajan, T.; Rao, K.R. Discrete Cosine Transform. *IEEE Trans. Comput.* **1974**, *C-23*, 90–93. [CrossRef]
52. Tang, Z.; Zhang, X.; Li, X.; Zhang, S. Robust Image Hashing with Dominant DCT Coefficients. *Signal Process.* **2018**, *144*, 226–235. [CrossRef]
53. Monga, V.; Evans, B.L. Perceptual Image Hashing via Feature Points: Performance Evaluation and Tradeoffs. *IEEE Trans. Image Process.* **2006**, *15*, 3452–3465. [CrossRef]
54. Swaminathan, A.; Mao, Y.; Wu, M. Robust and Secure Image Hashing. *IEEE Trans. Inf. Forensics Secur.* **2006**, *1*, 215–230. [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.