symmetry

MDPI

Article

A Privacy-Protected Image Retrieval Scheme for Fast and Secure Image Search

Anyu Du [1,*], Liejun Wang [1,*], Shuli Cheng [1] and Naixiang Ao [2]

[1] College of Information Science and Engineering, Xinjiang University, Urumqi 830046, China; cslxjuedu@126.com

[2] Xinjiang Lianhai INA-INT Information Technology Ltd., Urumqi 830000, China; aonaixiang@sina.com

* Correspondence: dayxjuedu@126.com (A.D.); wljxju@xju.edu.cn (L.W.); Tel.: +86-139-9981-6618 (L.W.)

Received: 16 January 2020; Accepted: 6 February 2020; Published: 14 February 2020

Abstract: With the development of multimedia technology, the secure image retrieval scheme has become a hot research topic. However, how to further improve algorithm performance in the ciphertext needs to be further explored. In this paper, we propose a secure image retrieval scheme based on a deep hash algorithm for index encryption and an improved 4-Dimensional(4-D)hyperchaotic system. The main contributions of this paper are as follows: (1) A novel secure retrieval scheme is proposed to control data transmission. (2) An improved 4-D hyperchaotic system is proposed to preserve privacy. (3) We propose an improved deep pairwise-supervised hashing (DPSH) algorithm and secure kNN to perform index encryption and propose an improved loss function to train the network model. (4) A secure access control scheme is shown, which aims to achieve secure access for users. The experimental results show that the proposed scheme has better retrieval efficiency and better security.

Keywords: multimedia; hyperchaotic; privacy protection; deep hashing

1. Introduction

Based on the development of big data and the increasing awareness of privacy protection, the construction of a secure index becomes the key technology of ciphertext domain image retrieval [1]. On the one hand, users query the information of interest in massive data. On the other hand, the privacy of the image is easily leaked during the storage and retrieval of images by the user. Cloud computing has a good advantage depending on its powerful computing power. This has led many researchers to study the image search scheme under the ciphertext domain. In previous cloud computing image retrieval schemes, the data owner lost direct control of the image when passing data to the cloud server. This will cause the image data information to leak. How to ensure the validity and reliability of ciphertext domain image retrieval has been widely concerned by researchers.

In ciphertext domain research, many schemes are proposed to protect data privacy. Ferreira et al. [2] proposed the practical content-based image retrieval (CBIR) scheme in an image repository. Xia et al. [3] proposed an efficient CBIR scheme in cloud computing. Zhu et al. [4] proposed a secure method to implement data management. In order to improve the ciphertext domain retrieval performance, approximate search and chaotic encryption algorithms are proposed in the cloud computing scheme [5,6]. For the application of the ciphertext domain scheme, Xia et al. [7] proposed a copyright detection retrieval scheme. In summary, in the ciphertext domain retrieval scheme, there are three key technologies (image encryption, index encryption, and data control) that need to be addressed.

Unlike traditional encryption methods, hyperchaotic systems are very suitable for image encryption because of their key sensitivity. The chaotic systems are characterized by randomness, ergodicity,

and sensitivity. In order to preserve privacy, some encryption algorithms are proposed [8–10]. At present, chaotic encryption systems are the current research hotspots, and many researchers are engaged in chaotic system related research [11–13]. For color image encryption, DNA sequence manipulation [14], scrambling [15], and chaotic mapping [16] are presented. These algorithms are very sensitive.

Image data have much inherent feature information such as shape, color, texture, etc., and there is a correlation between image pixels. Index encryption is a key technology for ciphertext retrieval. In order to improve retrieval efficiency, the hash algorithm becomes the mainstream algorithm for retrieval. The locality-sensitive hashing (LSH) [17] algorithm and traditional feature extraction methods are widely used in most ciphertext searches. To improve CBIR service quality, convolutional neural network hashing (CNNH) [18] was proposed in 2014 to fit mainly binary hash codes. In the traditional hash algorithm, supervised discrete hashing (SDH) [19] is proposed to learn binary hash codes directly. Some hashing algorithms (DPSH [20], deep supervised discrete hashing (DSDH) [21], deep joint semantic-embedding hashing (DSEH) [22], deep discrete supervised hashing (DDSH) [23]) based on supervision and quantization are proposed to evaluate the quality of hash code learning. At the same time, these algorithms are also the baseline of this paper.

Our main contributions are as follows: (1) A novel ciphertext domain retrieval scheme is proposed to ensure data control authority during data transmission. (2) In the proposed scheme, the 4-D hyperchaotic system is proposed to perform image encryption. (3) We propose an improved DPSH algorithm to perform index encryption and propose an improved loss function to train the network model. (4) A secure access control scheme is shown, which aims to achieve secure access for users. The algorithm used is AES based on output-feedback (OFB) mode. (5) The experimental results fully demonstrate that the proposed scheme has better retrieval efficiency and better security.

The remaining sections of this paper are organized as follows: Section 2 describes related work; Section 3 shows the image privacy protection scheme; Section 4 presents the experimental results and analysis; Section 5 summarizes.

2. Related Works

2.1. Privacy Protection Image Retrieval Scheme

In previous cloud computing image retrieval schemes, the data owner lost direct control of the image when passing data to the cloud server. This will cause the image data information to leak. How to ensure the validity and reliability of ciphertext domain image retrieval has become a focus of attention. In the ciphertext domain research, many schemes are proposed to protect data privacy. Ferreira et al. [2] proposed a practical CBIR scheme in an image repository. Xia et al. [3] proposed an efficient CBIR scheme in cloud computing. Zhu et al. [4] proposed a secure scheme to implement data management. Based on [2–4], this paper uses the blocked 4-D hyperchaotic system combined with the DNA operation to encrypt the image. Compared with the 2-D hyperchaotic system, the proposed algorithm has a larger range of chaotic states.

2.2. Explanation of Key Technologies in the Scheme

In the current research, the AES algorithm, DPSH algorithm, and 4-D hyperchaotic system are proposed. In the field of image retrieval, there are some hot topics that need to be further improved. The current research on image retrieval is mainly manifested in the following aspects: (1) In privacy protection image retrieval schemes, the LSH algorithm is currently used to construct the index. The DPSH algorithm has been the scientific frontier of deep hashing in recent years, and the DPSH algorithm has not been used in previous image retrieval schemes. (2) In privacy protection image retrieval schemes, low-dimensional hyperchaotic algorithms (one-dimensional hyperchaotic system and two-dimensional hyperchaotic system) are currently used to encrypt data. The high-dimensional hyperchaotic algorithm has been the scientific frontier in the field of image encryption in recent years,

and the high-dimensional hyperchaotic algorithm has not been used in previous image retrieval schemes. In the current research, 4-D and 5-D hyperchaotic systems are cutting-edge work in image encryption, but 5-D hyperchaotic systems have higher computational complexity, and low-dimensional hyperchaotic system algorithms have lower key sensitivity. In order to further ensure the security of the algorithm and reduce the computational complexity of the algorithm, this paper uses a block 4-D hyperchaotic system to complete the data encryption. (3) In the research of ciphertext image retrieval schemes, although AES has been proposed by scholars, it has not been used by scholars to protect retrieval scheme keys. In this paper, in order to further ensure data privacy and prevent third parties from obtaining unauthorized 4-D hyperchaotic system keys, we use AES to re-encrypt the key of the 4-D hyperchaotic system. This method can further ensure data privacy during data transmission. (4) For privacy-protected image retrieval schemes, index extraction is the most critical factor in the scheme, which also affects the retrieval accuracy of the entire scheme to a certain extent. Therefore, this paper proposes an improved DPSH algorithm to construct an image data index. The proposed method mainly improves the network model and loss function.

2.2.1. 4-D Hyperchaotic System

In this paper, we give the four-dimensional hyperchaotic system to encrypt images. The equation is [24]:

$$\begin{cases} y_1 = a(y - x) + w \\ y_2 = dx - xz + cy \\ y_3 = xy - bz \\ y_4 = yz + ew \end{cases} \tag{1}$$

Here, a, b, c, and d respectively represent the control parameters of this system. If the parameters are set to $a = 35$, $b = 3$, $c = 12$, $d = 7$, and $e = 0.2$, then the four-dimensional chaotic system is hyperchaotic, and the system can generate four hyperchaotic sequences.

2.2.2. Advanced Encryption Standard

AES is a block encryption algorithm, and its block length is 128 bits. Its secret key length is divided into three, which is 128, 192, and 256 bits [25]. AES encryption takes a short time, and the encryption speed is fast. Since the number of keys generated by the encryption sequence is small, the AES algorithm is used for encryption, which is fast.

In the encryption process, each round of the AES encryption loop consists of four steps, which are: Addroundkey transform, SubBytes transform, ShiftRows transform, and mixed column transform [26]. Before looping through the four steps, we initialize the Addroundkey. In the last encryption loop, we will omit the mixed column transform and replace it with another Addroundkey.

2.2.3. Privacy Protection and Retrieval

The DNA sequence consists of four letters, which are A, T, C, and G, which express the four nucleotides: adenine, thymine, cytosine, and guanine. Among them, each letter represents a base, and two bases form a base pair. Let us talk about the base pairing rules: A-T, C-G. This is also called the Watson–Crick base pairing rule [27]. In this paper, we map these four letters to the binary system. We will match every two letters, and there are eight rules.

In image encryption, this article will use some operations in DNA, such as addition and the XOR algorithm, and we will introduce the two operations [28].

The DNA complementation rules are defined [29] as follows,

$$\begin{cases} x \neq B(x) \neq B(B(x)) \neq B(B(B(x))) \\ x = B(B(B(B(x)))) \end{cases} \tag{2}$$

where B(x) is the base pair of x. According to Formula (2), the DNA complementation rules are given below:

Rule 1: (AT) (TC) (CG) (GA), Rule 2: (AT) (TG) (GC) (CA)
Rule 3: (AC) (CT) (TG) (GA), Rule 4: (AC) (CG) (GT) (TA)
Rule 5: (AG) (GT) (TC) (CA), Rule 6: (AG) (GC) (CT) (TA)

kNN means that each sample in the system can be represented by its neighboring k samples. It means a sample in the feature space that has k adjacent pixels. If these pixels belong to the same category, then this sample also belongs to this category, and they have the same characteristics [30].

Secure kNN is a secure and reliable ciphertext calculation method [31]. In ciphertext retrieval, both the homomorphic encryption algorithm and secure kNN algorithm have better ciphertext computing ability to evaluate ciphertext domain similarity. However, the secure kNN algorithm has lower computational complexity and is well suited for ciphertext image retrieval based on hash indexing. In addition, the kNN algorithm based on secret key encryption has been widely used in ciphertext domain image retrieval in recent years, and the algorithm is called secure kNN [32].

To improve CBIR service quality, CNNH [18] was proposed in 2014 to mainly fit binary hash codes. In the traditional hash algorithm, SDH [19] is proposed to learn binary hash codes directly. Some hashing algorithms (DPSH [20], DSDH [21], DSEH [22], DDSH [23]) based on supervision and quantization are proposed to evaluate the quality of hash code learning. At the same time, these algorithms are also the baseline of this paper.

In order to improve the retrieval efficiency of large-scale images, we use a deep hash algorithm (improved DPSH algorithm) to build indexes efficiently. In order to ensure a safe searchable index, this paper also uses the secure kNN to encrypt the index. In terms of security control, we use the AES algorithm to encrypt the key of the encrypted image again. The security and privacy of the key during the sharing process are guaranteed.

3. The Proposed Method

In the ciphertext domain research, many schemes are proposed to protect data privacy. Ferreira et al. [2] proposed a practical CBIR scheme in an image repository. Xia et al. [3] proposed an efficient CBIR scheme in cloud computing. Zhu et al. [4] proposed a secure scheme to implement data management. Based on [2–4], this paper uses the blocked 4-D hyperchaotic system combined with the DNA operation to encrypt the image. Compared with the 2-D hyperchaotic system, the proposed algorithm has a larger range of chaotic states.

In order to improve the retrieval efficiency of large-scale images, we used a deep hash algorithm (improved DPSH algorithm) to build indexes efficiently. In order to ensure a safe searchable index, this paper also uses the secure kNN to encrypt the index. In terms of security control, we used the AES algorithm to encrypt the key of the encrypted image again. The security and privacy of the key during the sharing process was guaranteed. The main contributions of this paper are as follows: (1) A novel secure retrieval scheme is proposed to control data transmission. (2) Improved 4-D hyperchaotic system is proposed to preserve privacy. (3) We propose an improved DPSH algorithm and secure kNN to perform index encryption and propose an improved loss function to train the network model. (4) A secure access control scheme is shown, which aims to achieve secure access for users.

3.1. Privacy Protection Scheme

The works in [2–4] presented a ciphertext domain search scheme, and researchers conducted related research on the ciphertext search scheme, image encryption module, and index encryption module. In these schemes, the data owner's control authority was not considered in the scheme of [2,3], and the work in [4] considered the data owner's control authority. As shown in Figure 1, in this paper, the privacy protection scheme is novel. The specific process is as follows.

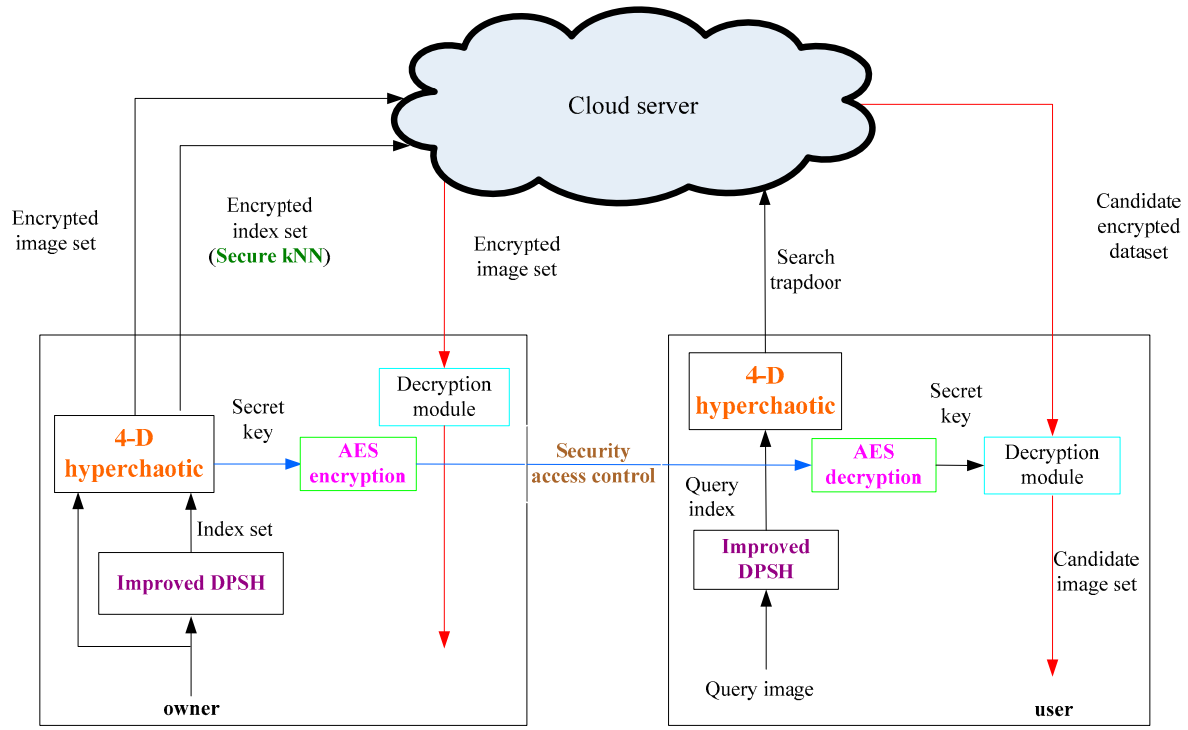


Figure 1. Novel privacy protection scheme.

The image owner stores the encrypted data in a cloud server, where the encrypted data include an encrypted image dataset C = $\{c_1, c_2, c_3, \cdots, c_n\}$ and the encrypted index set. The image encryption algorithm uses the 4-D hyperchaotic system and DNA sequence manipulation scheme, while enabling the function of searching for the encrypted image. The owner extracts features based on improved DPSH, which is F = $\{f_1, f_2, f_3, \cdots, f_n\}$ from M, and then to guarantee the confidentiality of the index. M is the original image dataset. This paper uses a secure kNN to encrypt the index to form a secure searchable index. Then, the image owner stores the encrypted image dataset and the encrypted index set in cloud server [31–33]. Additionally, in order to enable authorized legitimate users to decrypt the encrypted images that have been searched, the image owner shares the secret key of the encrypted image with the image user. However, in this process, the secret key may be stolen by an illegal user, causing the leakage of image information. Therefore, before sharing with the image user, we encrypt the key with AES and then share the encrypted secret key with the image user.

The image user retrieves an image similar to the sample. In order to search for images in the cloud server, first, the image user produces a trapdoor (TD). We generate a TD by key encryption of the eigenvector of the query image and search for images in the cloud server through TD. When the image is searched, the image user decrypts the encrypted secret key by the AES decryption algorithm, and then, the image user uses the secret key to decrypt the searched image and finally obtains the plaintext image.

The cloud server stores the encrypted image set and the encrypted index set generated by the image owner. At the same time, when the image user issues a query request, the cloud server also needs to process it.

3.2. *Image Encryption*

In this paper, the image is encrypted using a block 4-D hyperchaotic system and DNA sequence operations. The 4-D hyperchaotic system can reduce the computational complexity, while the block will affect the encryption effect. The proposed scheme is shown in Figure 2. It contains the following 6 steps: (1) Perform block processing on the image, denoted as B_1, B_2,..., B_k, where k is the number of

blocks. (2) Generate a random matrix of the same size as a normal image by logistic chaotic mapping. The random matrix is expressed as R. (3) A random chaotic sequence is generated by a 4-D hyperchaotic system. According to Formula 1, the four hyperchaotic sequences are y_1, y_2, y_3, y_4. (4) Select a DNA encoding and decoding method for each sub-block of the plain image and random matrix based on sequence y_3. (5) Select the DNA calculation method between the two sub-blocks based on sequence y_1 and sequence y_2. (6) Combine all the encrypted sub-blocks together to form an encrypted image based on sequence y_4. The process of image encryption and decryption is reversed.

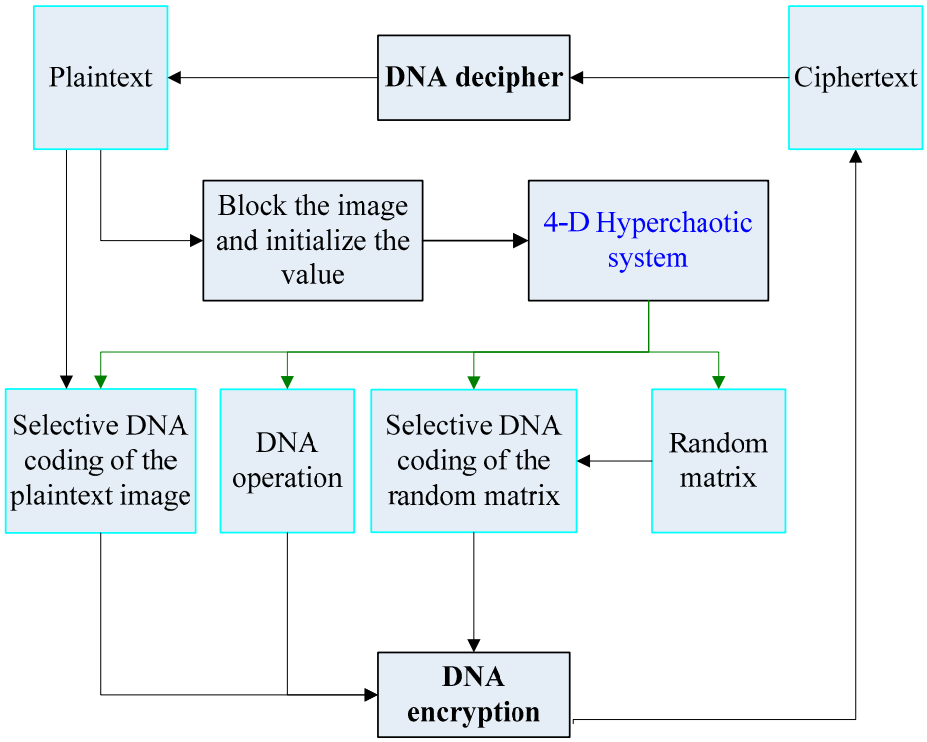


Figure 2. The encryption and decryption process.

3.3. Index Encryption

In most schemes, the index encryption module uses the LSH algorithm. Some hashing algorithms [20–23] based on supervision and quantization are proposed to evaluate the quality of hash code learning. These hash algorithms are optimized primarily from the perspective of network structure and the loss function. The goal is to improve the efficiency of large-scale image retrieval. In this paper, we use the improved DPSH algorithm to construct a database image index. The index construction process is shown in Figure 3.

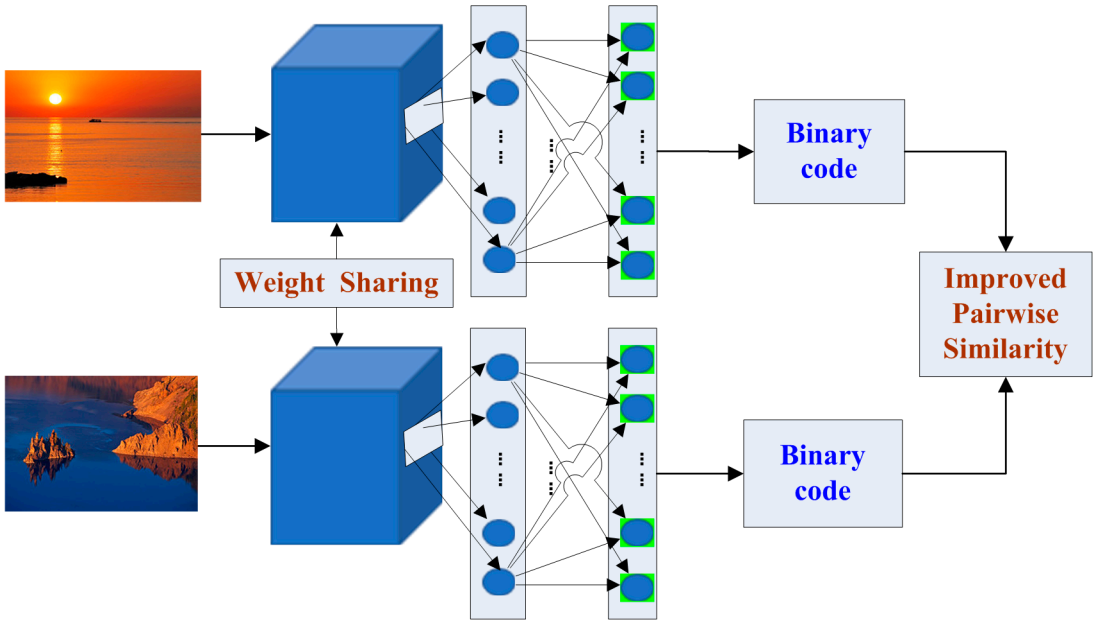


Figure 3. The index construction process.

The loss function is fundamental to network training. The loss function of the original DPSH algorithm is shown in Equation (3):

$$\min_{B,U} J(B,U) = -\sum_{s_{ij}\in S}\left(s_{ij}\Theta_{ij} - \log\left(1+e^{\Theta_{ij}}\right)\right) + \gamma\sum_{i=1}^{n} \parallel b_i - u_i \parallel_2^2 \tag{3}$$

where B is a binary hash code, U is the output of the network, S is a similar matrix, $\Theta_{ij} = \frac{1}{2}u_i^T u_j$, and γ is a regular term.

In order to further improve the retrieval accuracy, we improved the corresponding loss function to train better parameters. Our loss function included semantic loss, classification loss, and quantization loss. The specific description is as shown in Equation (4):

$$\begin{aligned} \min_{B,U} J(B,U) \quad &= -\sum_{s_{ij}\in S}\left(s_{ij}\Theta_{ij} - \log\left(1+e^{\Theta_{ij}}\right)\right) \\ &+ \gamma\textstyle\sum_{i=1}^{n} \parallel b_i - u_i \parallel_2^2 \\ &+ \frac{\sum_{i=1}^{n}|u_i-1|^2+\sum_{i=1}^{n}|b_i-1|^2}{n} \\ &- \textstyle\sum_{i=1}^{n} y_i * log(y_i') \end{aligned} \tag{4}$$

where B is a binary hash code, U is the output of the network, S is a similar matrix, $\Theta_{ij} = \frac{1}{2}u_i^T u_j$, and γ is a regular term. y_i is the real classification label for category I, and y_i' is the prediction classification label for category i. The backbone network we selected was the ResNet network.

In this paper, we extract the index based on the improved DPSH algorithm, whose goal is to improve retrieval efficiency. Encrypted image feature vectors make it impossible for an attacker to obtain private information. However, it is important to note that legitimate authorized users can use the encrypted index vectors for similarity calculations and can sort them. Because the algorithm has less computational complexity, we utilized the secure kNN algorithm to perform ciphertext indexing. The basic steps of index encryption mainly include: (1) extracting image features and establishing indexes; (2) encrypting indexes by using secure kNN.

In order to encrypt images and store the encrypted image set in the cloud server, the image owner needs to get the private key from the image. In the process of sharing the key with the legitimate image user by the image owner, unauthorized users and attackers can easily steal the key of the

algorithm. Therefore, this article uses AES to encrypt the key. Secure access control through AES prevents unauthorized personnel and attackers from stealing the algorithm's secret key.

4. Experimental Evaluation

In this section, we mainly analyze the performance of the solution from three aspects (ciphertext domain retrieval scheme comparison, image encryption performance analysis, index encryption performance analysis). Our main improvements are also given in the following three parts.

4.1. Search Scheme Comparison

In the ciphertext domain research, many schemes have been proposed to protect data privacy. Ferreira et al. [2] proposed a practical CBIR scheme in an image repository. Xia et al. [3] proposed an efficient CBIR scheme in cloud computing. Zhu et al. [4] proposed a secure scheme to implement data management.

These schemes [2,3] lacked control over the data, so when the data owner transmitted data to the cloud server, it lost control of the data. The scheme proposed by Zhu et al. [4] considered the power of data control, but the overall performance of the scheme still needs to be improved. In addition, these solutions used the traditional indexing method, so the performance of image encryption and index encryption schemes needs to be further improved.

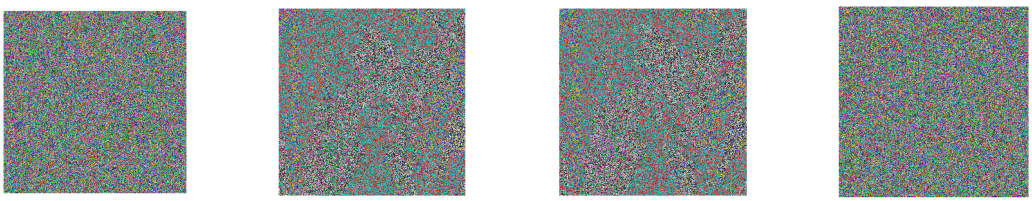
In summary, this paper proposes a new scheme that combines the advantages of the schemes of [2–4]. The scheme proposed in this paper can further improve the security of ciphertext domain retrieval. The proposed scheme is shown in Figure 1.

4.2. Encryption Performance Analysis

Some studies have shown that large key spaces have higher security. If you want to get more security, the encryption key is sensitive to any minor changes. The key space size of the proposed algorithm is $10^{15} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^{16} = 10^{95} \approx 2^{315}$. If the key space is greater than a certain threshold, this algorithm can effectively avoid violent attacks. After verification, the proposed method is robust.

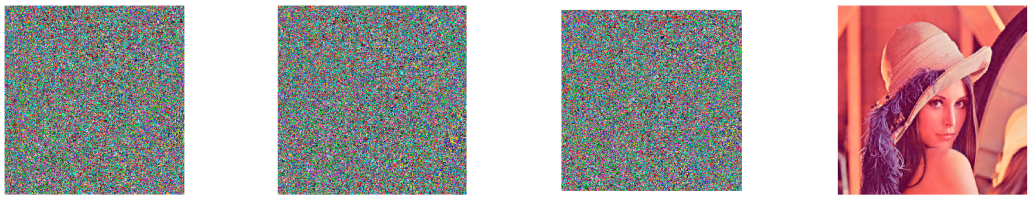
4.2.1. Sensitivity Analysis

We first selected an image from the public image library to detect the sensitivity of the algorithm. Because the encryption algorithm had the same sensitivity as the decryption algorithm, we could get the sensitivity of the encryption algorithm very intuitively from the decrypted image. We made minor changes to the six sets of encryption keys. Then, the changed key was used for the decrypt operation of the encrypted image. Finally, we decrypted the image with the original key compared to the previous result. Figure 4 illustrates the algorithm's key sensitivity analysis.



(**a**) (**b**) (**c**) (**d**)

Figure 4. *Cont.*

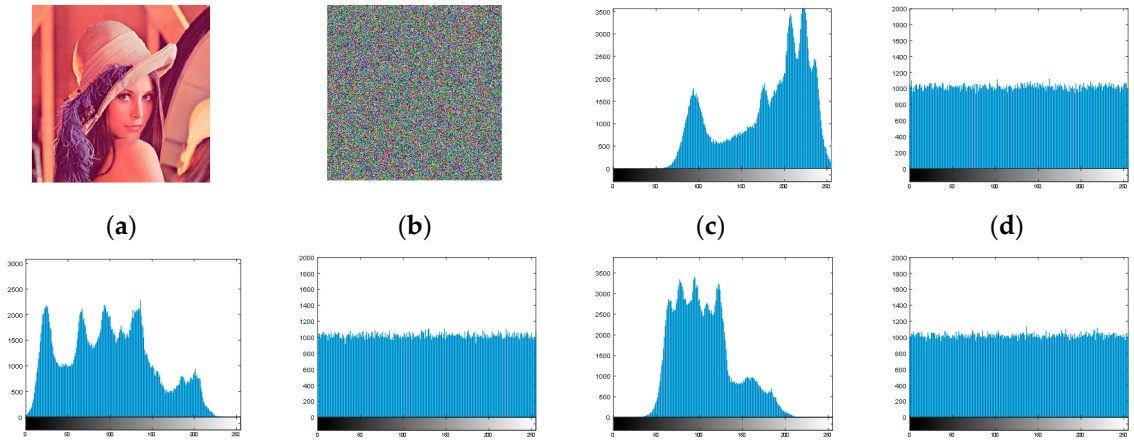


(**e**) (**f**) (**g**) (**h**)

Figure 4. Key sensitivity analysis. (**a**) Encrypted image. (**b**) Fine-tuning the private key 1. (**c**) Fine-tuning the private key 2. (**d**) Fine-tuning the private key 3. (**e**) Fine-tuning the private key 4. (**f**) Fine-tuning the private key 5. (**g**) Fine-tuning the private key 6. (**h**) Original private key decryption.

4.2.2. Histogram Analysis

The histogram showed the image statistical properties. It mainly showed the pixel value distribution in the image, that is it counted the pixel number. When the all the image histogram's pixel value numbers were almost equal, the histogram was flat. This showed that it was very resistant to statistical attacks. In this experiment, we chose the Lena image for testing. Figure 5 discusses the histograms in the plaintext and ciphertext fields. By comparison, we can see that the pixel values were mainly concentrated in the middle of the histogram, and in the ciphertext image, the pixel values were evenly distributed. This experiment could show that the ciphertext image could be well concealed to hide the gray value distribution in the original image.



(**a**) (**b**) (**c**) (**d**)

(**e**) (**f**) (**g**) (**h**)

Figure 5. Histogram analysis. (**a**) Plaintext. (**b**) Ciphertext. (**c**) Plaintext R-channel histogram. (**d**) Ciphertext R-channel histogram. (**e**) Plaintext G-channel histogram. (**f**) Ciphertext G-channel histogram. (**g**) Plaintext B-channel histogram. (**h**) Ciphertext B-channel histogram.

4.2.3. Correlation Analysis

Image correlation is an indicator for evaluating the randomness of an image. The plaintext image's adjacent pixels had a strong correlation. When we encrypted the plaintext image, we could increase the randomness between the pixels. This paper uses the Lena image to detect the correlation. The function is as follows:

$$\rho_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)D(y)}} \tag{5}$$

$$cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{6}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{7}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \tag{8}$$

where x and y represent two adjacent pixel values randomly selected in three directions of horizontal, vertical, and diagonal. In Figure 6, the correlation between the plaintext image pixels and the secret image is exhibited. Through the figures, we can know that in the original image of the three channels R, G, and B, all points were almost concentrated on the diagonal of the coordinate system. For the encrypted image in the three channels R, G, and B, its points were distributed throughout the coordinate system. This meant that there was almost no correlation between the encrypted image's two adjacent pixels. Therefore, the experimental results showed that the proposed scheme was random.

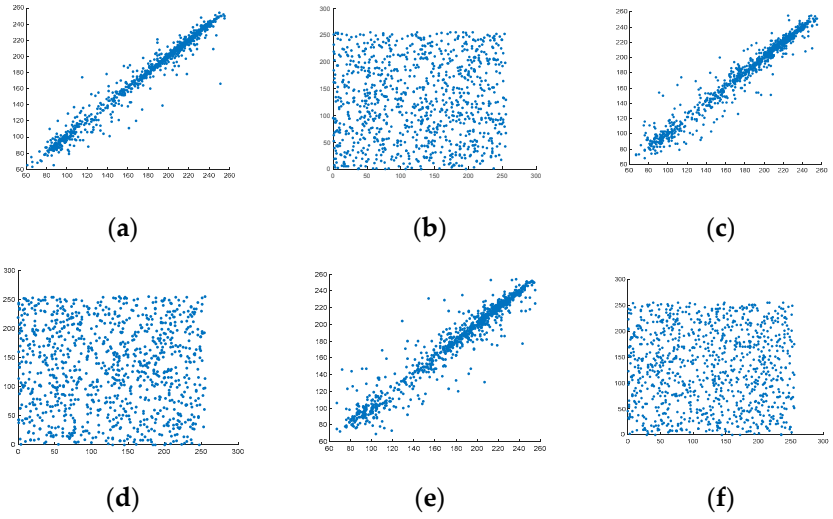


Figure 6. Correlation of images. (**a**) R channel in original image. (**b**) R channel in encrypted image. (**c**) G channel in original image. (**d**) G channel in encrypted image. (**e**) B channel in original image. (**f**) B channel in encrypted image.

4.2.4. Blocking Attack Analysis

During image transmission and storage in a cloud server, digital images are susceptible to blocking attacks and lose the original image information. Next, the article analyzes the algorithm's anti-blocking attack performance. We first encrypted the plaintext image, then blocked the encrypted image to different degrees, and finally decrypted the plaintext image. The experimental results are shown below. As can be known from Figure 7, there was a limited degree of blocking attack, and we could still see most of the information of the original image in the decrypted image. Therefore, the encryption algorithm we proposed could effectively resist blocking attacks.

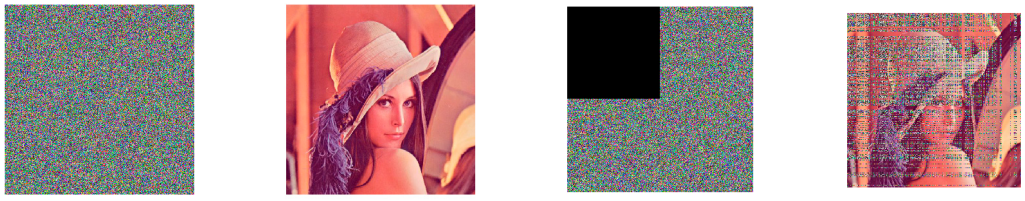


Figure 7. *Cont.*

(**e**) (**f**) (**g**) (**h**)

Figure 7. Blocking attack. (**a**) Encrypted image. (**b**) Decrypted image. (**c**) A 1/4 degree blocking of the encrypted image. (**d**) A 1/4 degree blocking of the decrypted image. (**e**) A 1/2 degree blocking of the decrypted image. (**f**) A 1/2 degree blocking of the encrypted image. (**g**) Blocking encrypted image by 3/4. (**h**) A 3/4 degree blocking of the decrypted image.

4.2.5. Differential Attack Analysis

A differential attack is when an attacker or an unauthorized user makes a small change in an area of the plaintext image, encrypts the plaintext image without change and the changed image separately, and then, tries to find the contact between the two encrypted images. We attacked cryptographic algorithm through encrypted changes. We used the number of pixels change rate (NPCR) and unified average changing intensity (UACI) to analyze differential attacks.

In order to analyze whether the scheme in this paper could resist differential attacks, we encrypted the Lena image using our algorithm and the scheme proposed in [11,13–16]. We performed a 1 bit change on the original plaintext image and tested the impact on the corresponding encrypted image by calculating the values of NPCR and UACI. Table 1 gives the results of these two indicators. It can be seen from the table that the proposed algorithm's NPCR was 99.63%, and its UACI was 33.45%. Compared with [11,13–16], the proposed algorithm was more resistant to differential attacks. From the overall analysis, the proposed algorithm performed better than the baseline. Table 1 shows the NPCR and UACI properties.

Table 1. The performance of the number of pixels change rate (NPCR) and unified average changing intensity (UACI).

Algorithm	NPCR (%)	UACI (%)	Key Space
Ours	99.63	33.45	2298
Ref. [14]	99.52	33.36	256
Ref. [11]	99.61	33.41	2138
Ref. [13]	99.62	33.51	2210
Ref. [15]	99.63	33.59	2240
Ref. [16]	99.41	33.26	2256

4.2.6. Statistical Analysis

Information entropy and correlation are important test methods for statistical analysis. Table 2 shows the results of the statistical analysis. The algorithm proposed by us was the same as the information entropy proposed by [15], but the correlation of our algorithm was smaller than that of [15]. However, for other comparisons, the image encrypted by the algorithm had the largest entropy value. In Table 2, the security of our algorithm was greater than other algorithms.

Table 2. Statistical analysis of plaintext and ciphertext.

Algorithm	Horizontal	Vertical	Diagonal	Entropy
Plaintext	0.9708	0.9863	0.9596	7.2682
Ours	−0.0021	0.0015	−0.0018	7.9994
Ref. [14]	−0.0219	0.0326	−0.0098	7.9914
Ref. [11]	−0.0036	−0.0026	0.0017	7.9931
Ref. [13]	−0.0231	−0.0019	−0.0034	7.9974
Ref. [15]	0.0021	0.0017	0.0011	7.9994
Ref. [16]	0.0031	−0.0024	−0.0034	7.9976

It can be seen from Tables 1 and 2 that the proposed algorithm was robust to both differential and statistical attacks. Therefore, the algorithm proposed in this paper could resist the common types of attacks encountered during image transmission. Cloud computing-based CBIR services require not only better security, but also better retrieval performance. Next is the retrieval evaluation index of the paper's verification scheme.

4.3. Retrieval Performance Comparison

In index encryption, we optimized the network model selection and loss function construction. We optimized the performance of the algorithm based on the pre-trained ResNet34 network and improved the loss function. The improved DPSH was performed on the CIFAR-10 dataset. In the experiment, 5000 images were used to train the improved DPSH algorithm, and 1000 images were used to test the improved DPSH algorithm. Figure 8 shows the precision recall rate curve of the improved DPSH algorithm.

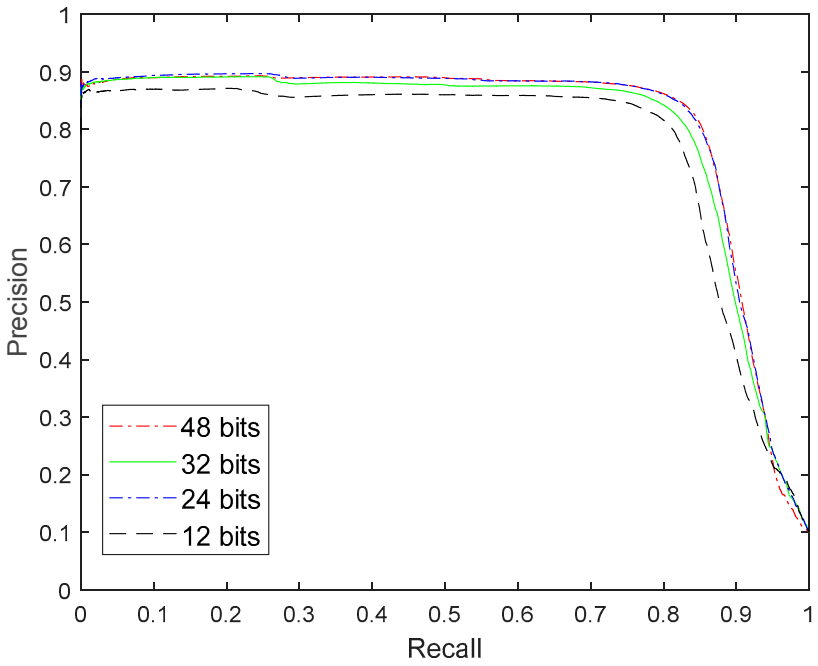


Figure 8. The precision recall curve of our algorithm.

MAP is an indicator to measure retrieval efficiency, which is the most widely used indicator in image retrieval. Figure 9 shows the MAP results of the improved DPSH algorithm. In Figure 9, the proposed algorithm achieved the best results. Our optimal result was 0.8931, when the number of bits in the hash code was 24.

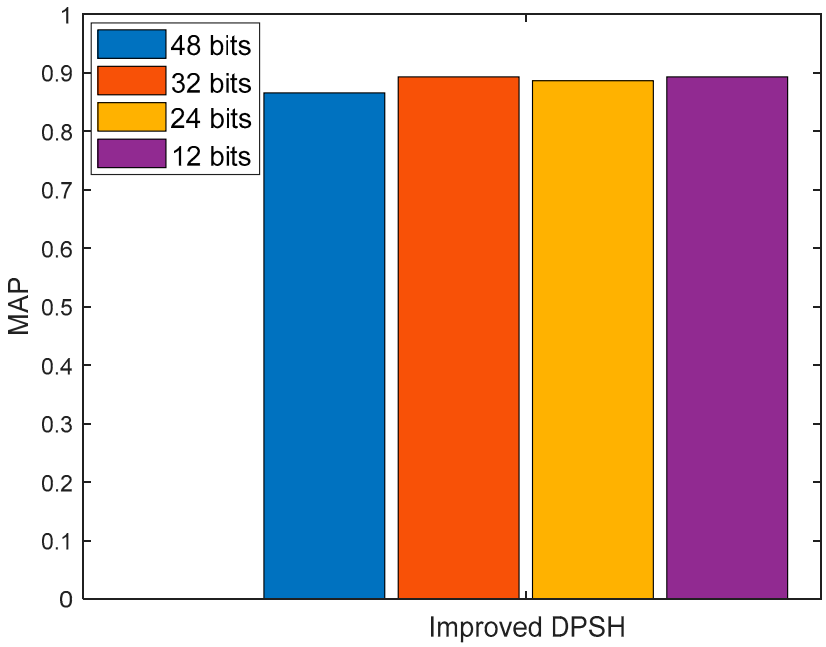


Figure 9. The MAP result of improved DPSH algorithm.

The selection of the backbone network affected the overall performance of the algorithm. In the experiment, we used AlexNet, ResNet18, ResNet34, and ResNet50 as the main networks and used the improved loss function to train these networks to find the optimal parameters. Our loss function construct is shown in Equation (6). The experimental results under different network models are shown in Figure 10. Figure 10 shows that the proposed algorithm could obtain the optimal experimental results. The optimal experimental result was 0.8931, where the number of hash code bits was 24. In the proposed model, the selected network model was ResNet34, and the loss function is shown in Equation (4).

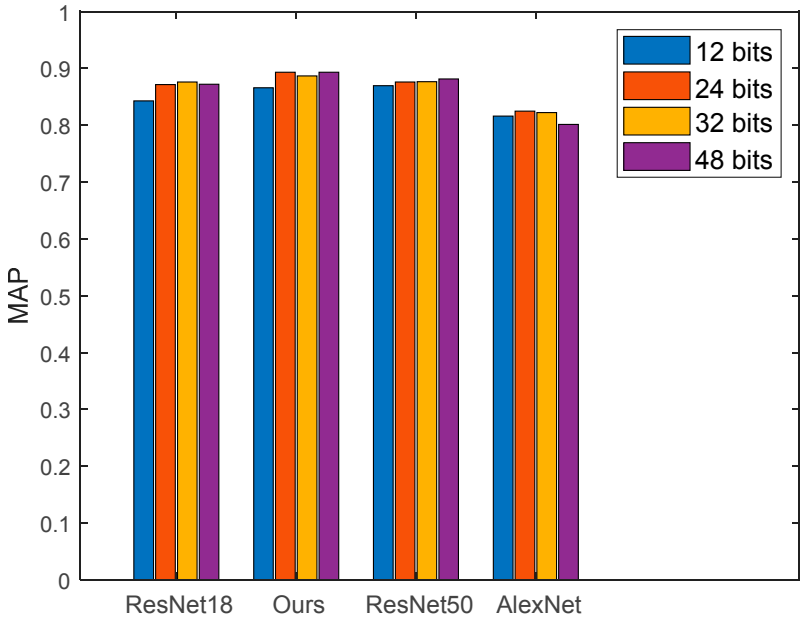
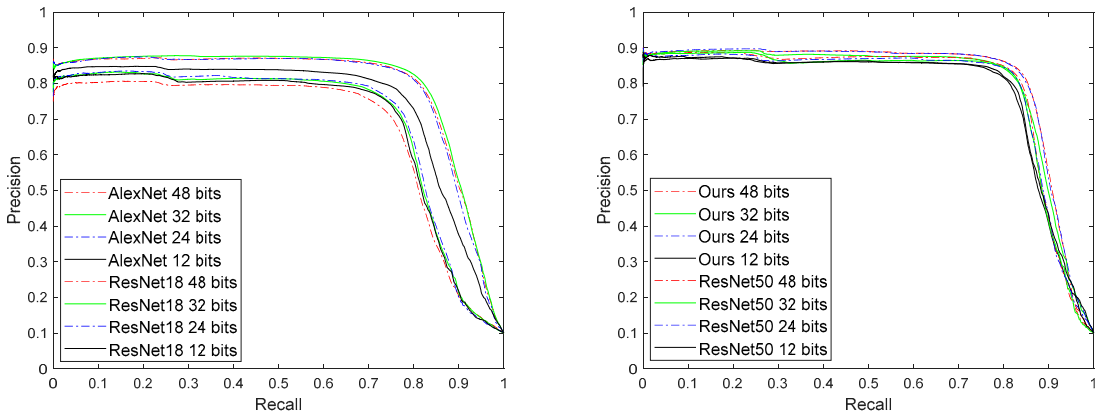


Figure 10. The MAP result of different algorithms.

The precision recall rate is another performance indicator for image retrieval. In our experiments, we plotted the precision recall curves of AlexNet, ResNet18, ResNet50, and the proposed algorithm. Figure 11a shows the precision recall curve for AlexNet and ResNet18 with different bits. Figure 11b shows the precision recall curve of the proposed algorithm and ResNet50 under different bits. The best performing curve in Figure 11 is the precision recall rate curve for the proposed algorithm.



(**a**) (**b**)

Figure 11. The precision recall curve of the algorithms. (**a**) the precision recall curve for AlexNet and ResNet18 with different bits. (**b**) the precision recall curve of the proposed algorithm and ResNet50 under different bits.

To better improve the quality of CBIR services, CNNH [18] was proposed in 2014 to mainly fit binary hash codes. In the traditional hash algorithm, SDH [19] was proposed to learn binary hash codes directly. Some hashing algorithms (DPSH [20], DSDH [21], DSEH [22], DDSH [23]) based on supervision and quantization were proposed to evaluate the quality of hash code learning. At the same time, these algorithms were also the baseline of this paper.

The comparison algorithm was tested on the public data set Cifar10, and the experimental results are shown in Figure 12. From the comparison experiment, we can see that the proposed algorithm had the best retrieval effect in the secure retrieval scheme. As can be seen from Figure 12, when the hash code length was 24, the security retrieval scheme proposed in this paper had the best retrieval performance, and the result was 0.8931.

In summary, we introduced the comparison and analysis of the ciphertext domain scheme, the effect and analysis of the image encryption algorithm, the index encryption effect and analysis, and the effect and analysis of the comparison algorithm. The experimental results showed that the proposed scheme had better security under the premise of ensuring retrieval accuracy.

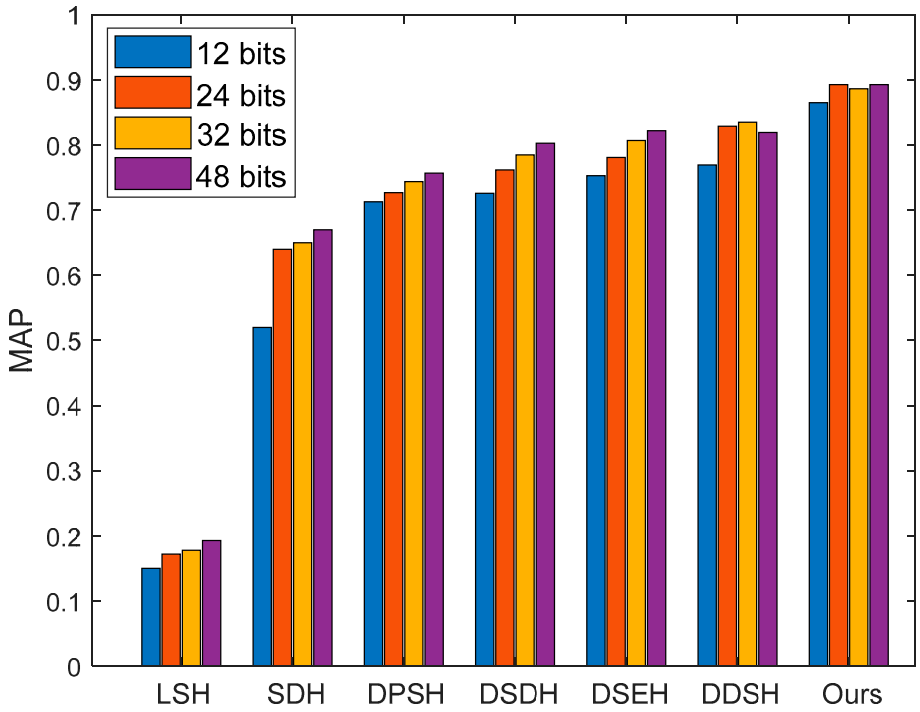


Figure 12. Scheme retrieval performance analysis.

5. Conclusions

This paper presented a new privacy-protected image retrieval scheme. The goal was to improve the effectiveness and reliability of the scheme. The main contributions of this paper are as follows: (1) A novel secure retrieval scheme was proposed to ensure data control authority during data transmission. (2) In the proposed scheme, the 4-D hyperchaotic system was proposed to perform image encryption. (3) We proposed an improved DPSH algorithm and secure kNN to perform index encryption and proposed an improved loss function to train the network model. (4) A secure access control scheme was shown, which aimed to achieve secure access for users. The experimental results showed that the proposed scheme had better retrieval efficiency and better security. Moreover, the existing algorithm ignored the security of the access control, so that the attacker stole the key, resulting in leakage of data privacy. In our scheme, the algorithm had better encryption performance to protect data privacy.

Moreover, the existing algorithm ignored the security of the access control, so that the attacker stole the key, resulting in leakage of data privacy. In our scheme, the algorithm had better encryption performance to protect data privacy. The study of multi-modal technology can comprehensively utilize information to a certain extent. In future research, we will introduce a multi-mode hash algorithm to further improve the retrieval accuracy of the scheme.

Author Contributions: Conceptualization, S.C. and L.W.; methodology, A.D.; software, S.C.; validation, S.C., A.D. and L.W.; formal analysis, N.A.; writing, original draft preparation, A.D.; writing, review and editing, A.D.; visualization, S.C. All authors read and agreed to the published version of the manuscript.

Funding: This research was funded by the Natural Science Foundation of Xinjiang Uygur Autonomous Region, Grant Number 2019D01C033", in part by the National Science Foundation of China under Grants 61771416 and U1903213, in part by the CERNET Innovation Project under Grant NGII20180201, and in part by the Creative Research Groups of Higher Education of Xinjiang Uygur Autonomous Region under Grant XJEDU2017T002.

Conflicts of Interest: The authors declare that no competing interests exist.

References

1. Cheng, B.; Zhuo, L.; Bai, Y. Secure Index Construction for Privacy-Preserving Large-Scale Image Retrieval. In Proceedings of the 2014 IEEE Fourth International Conference on Big Data and Cloud Computing, Sydney, NSW, Australia, 4 December 2014; pp. 116–120.
2. Ferreira, B.; Rodrigues, J.; Leitao, J.; Domingos, H. Practical Privacy-Preserving Content-Based Retrieval in Cloud Image Repositories. *IEEE Trans. Cloud Comput.* **2019**, *7*, 784–798. [CrossRef]
3. Xia, Z.; Xiong, N.N.; Vasilakos, A.V.; Sun, X. EPCBIR: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing. *Inf. Sci.* **2017**, *387*, 195–204. [CrossRef]
4. Zhu, X.; Li, H.; Guo, Z. Privacy-preserving query over the encrypted image in cloud computing. *J. XiDian Univ.* **2014**, *41*, 151–158.
5. Ibrahim, A.; Jin, H.; Yassin, A.A.; Zou, D.; Xu, P. Towards Efficient Yet Privacy-Preserving Approximate Search in Cloud Computing. *Comput. J.* **2014**, *57*, 241–254. [CrossRef]
6. Fan, K.; Wang, X.; Suto, K.; Li, H.; Yang, Y. Secure and Efficient Privacy-Preserving Ciphertext Retrieval in Connected Vehicular Cloud Computing. *IEEE Netw.* **2018**, *32*, 52–57. [CrossRef]
7. Xia, Z.; Wang, X.; Zhang, L.; Qin, Z.; Sun, X.; Ren, K. A Privacy-Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2594–2608. [CrossRef]
8. Feng, W.; He, Y. Cryptanalysis and Improvement of the Hyper-Chaotic Image Encryption Scheme Based on DNA Encoding and Scrambling. *IEEE Photon. J.* **2018**, *10*, 1–15. [CrossRef]
9. Zhu, Z.-L.; Zhang, W.; Wong, K.-W.; Yu, H. A chaos-based symmetric image encryption scheme using a bit-level permutation. *Inf. Sci.* **2011**, *181*, 1171–1186. [CrossRef]
10. Ravichandran, D.; Praveenkumar, P.; Rayappan, J.B.B.; Amirtharajan, R. Chaos based crossover and mutation for securing DICOM image. *Comput. Boil. Med.* **2016**, *72*, 170–184. [CrossRef]
11. Chen, J.-X.; Zhu, Z.-L.; Fu, C.; Yu, H.; Zhang, L.-B. A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. *Commun. Nonlinear Sci. Numer. Simul.* **2015**, *20*, 846–860. [CrossRef]
12. Chai, X.; Chen, Y.; Broyde, L. A novel chaos-based image encryption algorithm using DNA sequence operations. *Opt. Lasers Eng.* **2017**, *88*, 197–213. [CrossRef]
13. Xu, L.; Li, Z.; Li, J.; Hua, W. A novel bit-level image encryption algorithm based on chaotic maps. *Opt. Lasers Eng.* **2016**, *78*, 17–25. [CrossRef]
14. Wang, J.; Long, F. CNN-based color image encryption algorithm using DNA sequence operations. In Proceedings of the 2017 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC), Shenzhen, China, 15–17 December 2017; pp. 730–736.
15. Enayatifar, R.; Abdullah, A.H.; Isnin, I.F.; Altameem, A.; Lee, M. Image encryption using a synchronous permutation-diffusion technique. *Opt. Lasers Eng.* **2017**, *90*, 146–154. [CrossRef]
16. Liu, W.; Sun, K.; Zhu, C. A fast image encryption algorithm based on chaotic map. *Opt. Lasers Eng.* **2016**, *84*, 26–36. [CrossRef]
17. Datar, M.; Immorlica, N.; Indyk, P.; Mirrokni, V.S. Locality-sensitive hashing scheme based on p-stable distributions. In Proceedings of the 20th Annual Symposium on Computational Geometry, Brooklyn, NY, USA, 9–11 June 2004; pp. 253–262.
18. Xia, P.; Pan, Y.; Lai, H.; Liu, C.; Yan, S. Supervised hashing for image retrieval via image representation learning. In Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence(AAAI), Québec City, QC, USA, 27–31 July 2014; pp. 2156–2162.
19. Shen, F.; Shen, C.; Liu, W.; Shen, H.T. Supervised Discrete Hashing. In Proceedings of the 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, 7–12 June 2015; pp. 37–45.
20. Li, W.-J.; Wang, S.; Kang, W.-C. *Feature Learning Based Deep Supervised Hashing with Pairwise Labels*; IJCAI: New York, NY, USA, 2016; pp. 3270–3278.
21. Li, Q.; Sun, Z.; He, R.; Tan, T. Deep supervised discrete hashing. In *Advances in Neural Information Processing Systems*; NIPS: Long Beach, CA, USA, 2017; pp. 2482–2491.
22. Li, N.; Li, C.; Deng, C.; Liu, X.; Gao, G. Deep joint semantic-embedding hashing. In Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence (IJCAI-18), Stockholm, Sweden, 13–19 July 2018; pp. 2397–2403.

23. Jiang, Q.; Cui, X.; Li, W. Deep Discrete Supervised Hashing. *IEEE Trans. Image Process.* **2018**, *27*, 5996–6009. [CrossRef] [PubMed]
24. Nazarimehr, F.; Rajagopal, K.; Kengne, J.; Jafari, S.; Pham, V.T. A new four-dimensional system containing chaotic or hyper-chaotic attractors with no equilibrium, a line of equilibria and unstable equilibria. *Chaos Solitons Fractals* **2018**, *111*, 108–118. [CrossRef]
25. Zhang, Y.; Zhang, Q.; Liao, H.; Wu, W.; Li, X.; Niu, H. A Fast Image Encryption Scheme Based on Public Image and Chaos. In Proceedings of the 2017 International Conference on Computing Intelligence and Information System (CIIS), Nanjing, China, 21–23 April 2017; pp. 270–276.
26. Deshmukh, P.; Kolhe, V. Modified AES based algorithm for MPEG video encryption. In Proceedings of the International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, India, 27–28 February 2014; pp. 1–5.
27. Cisse, I.I.; Kim, H.; Ha, T. A rule of seven in Watson-Crick base-pairing of mismatched sequences. *Nat. Struct. Mol. Biol.* **2012**, *19*, 623–627. [CrossRef]
28. Zhang, X.Q.; Wang, X.S. Multiple-image encryption algorithm based on DNA encoding and chaotic system. *Multimed. Tools Appl.* **2018**, *77*, 1–29. [CrossRef]
29. Wang, X.Y.; Zhang, Y.Q.; Bao, X.M. A novel chaotic image encryption scheme using DNA sequence operations. *Opt. Lasers Eng.* **2015**, *73*, 53–61. [CrossRef]
30. Murat, H.; Zhang, S.; Yan, C. Classification of Xinjiang Uygur medicine image based on KNN Classifier. *J. Xinjiang Med. Univ.* **2015**, *38*, 800–804.
31. Rong, H.; Wang, H.; Liu, J.; Wu, W.; Xian, M. Efficient Integrity Verification of Secure Outsourced kNN Computation in Cloud Environments. In Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 23–26 August 2016; pp. 236–243.
32. Wong, W.K.; Cheung, D.W.-L.; Kao, B.; Mamoulis, N. Secure kNN computation on encrypted databases. In Proceedings of the ACM SIGMOD International Conference on Management of Data, SIGMOD 2009, Providence, RI, USA, June 29–July 2 2009.
33. Choi, S.; Ghinita, G.; Lim, H.; Bertino, E. Secure kNN Query Processing in Untrusted Cloud Environments. *IEEE Trans. Knowl. Data Eng.* **2014**, *26*, 2818–2831. [CrossRef]