IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 2, 2019, accepted January 14, 2019, date of publication January 31, 2019, date of current version March 7, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2894673

An Encrypted Image Retrieval Method Based on Harris Corner Optimization and LSH in Cloud Computing

JIAOHUA QIN[1], HAO LI[1], XUYU XIANG[1], YUN TAN[1], WENYAN PAN[1], WENTAO MA[1], AND NEAL N. XIONG[2]

[1]College of Computer Science and Information Technology, Central South University of Forestry and Technology, Changsha 410004, China
[2]Department of Mathematics and Computer Science, Northeastern State University, Tahlequah, OK 74464, USA

Corresponding author: Xuyu Xiang (xyuxiang@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61772561, in part by the Key Research and Development Plan of Hunan Province under Grant 2018NK2012, in part by the Postgraduate Research and Innovation Project of Hunan Province under Grant CX2018B447, in part by the Postgraduate Science and Technology Innovation Foundation of the Central South University of Forestry and Technology under Grant 20183034 and Grant 20183027, and in part by the Key Laboratory for Digital Dongting Lake Basin of Hunan Province.

ABSTRACT The encrypted image retrieval in cloud computing is a key technology to realize the massive images of storage and management and images safety. In this paper, a novel feature extraction method for encrypted image retrieval is proposed. First, the improved Harris algorithm is used to extract the image features. Next, the Speeded-Up Robust Features algorithm and the Bag of Words model are applied to generate the feature vectors of each image. Then, Local Sensitive Hash algorithm is applied to construct the searchable index for the feature vectors. The chaotic encryption scheme is utilized to protect images and indexes security. Finally, secure similarity search is executed on the cloud server. The experimental results show that compared with the existing encryption retrieval schemes, the proposed retrieval scheme not only reduces the time consumption but also improves the image retrieval accuracy.

INDEX TERMS Cloud computing, image retrieval, Harris corner detection, local sensitive hash.

I. INTRODUCTION

With the rapid development of imaging sensors and handheld electronic devices, multimedia data such as images play an increasingly important role in medicine, advertising, education, entertainment and other industries, and they have shown an explosive growth trend.

Cloud computing provides users with on-demand, paid computing and storage services [1], which has become the primary choice of image storage and image search outsourcing. Encrypted image retrieval in cloud computing is a key technology to realize the massive images storage & management and ensure the images safety.

The existing encrypted retrieval schemes mainly focus on text retrieval. A plenty of methods are proposed based on different threat models to achieve various search functionalities, such as searchable encryption [2], similarity search [3], [4], multi-keyword ranked search [5]–[9], dynamic search [10], [11], index construction [12], [13], etc. However, there are few schemes for encrypted image retrieval. Xiang and Luo [14] proposed a reversible data hiding scheme for encrypted images based on the public key cryptosystems with homomorphic and probabilistic properties. This scheme not only completed the embedding of extra data in the homomorphic encryption domain while keeping the quantity of data unchanged, but also improved the efficiency of information embedding and extraction. Yuan *et al.* [15] proposed a novel coverless image steganography scheme based on scale-invariant feature transform and bag of feature. The scheme ensured data security without modifying the information of the original carrier. Mishra *et al.* [16] proposed a new digital image encryption algorithm based on chaotic mapping. The algorithm could not only guarantee the security of the key, but also resist a variety of brute force or statistical attacks. Parvaz and Zarebnia [17] proposed an image encryption algorithm based on a new chaotic system. The algorithm could effectively resist the attacks of difference, statistics, noise and data etc. and thus

The associate editor coordinating the review of this manuscript and approving it for publication was Chin-Feng Lai.

ensure the security of data effectively. The above image encrypted schemes have achieved good performance, and also provided security technology support for encrypted retrieval. However, an efficient encrypted image retrieval algorithm need not only ensure data security, but also consider the similarity search of encrypted images.

Huang *et al.* [18] proposed an encryption scheme. The scheme converted the image into the feature vectors, and used the similarity matching algorithm in the text encrypted neighborhood to retrieve the target image. Liu and Go [19] proposed a privacy-enhanced scheme for image similarity search in cloud image database. Although the security of encrypted image retrieval was improved in this scheme, the search efficiency was not optimal. Zhou *et al.* [20] proposed the Overlapping Region-based Global Context Descriptor (OR-GCD) for the verification of these matches to filter false matches. This scheme used a random validation method for similarity retrieval. Hazra *et al.* [21] designed a secure encryption retrieval system. The system used HSV histogram as image feature, and combined KNN and SVM algorithm to query similar images, which could achieve high retrieval accuracy.

The above several encrypted image retrieval schemes could not only ensure the security of the image, but also retrieve the similar images. However, these schemes didn't construct the searchable indexes for images, and the search efficiency was low. Therefore, choosing a reasonable index construction algorithm is the key point to improve retrieval efficiency.

Abduljabbar *et al.* [22] proposed an encrypted retrieval scheme. In this scheme, SURF algorithm was applied to extract the image features, and LSH algorithm was utilized to construct the index. This scheme could not only realize similarity search, but also guarantee the data security. However, this scheme had no optimization for the local sensitive algorithm. Xia *et al.* [23] proposed an encrypted image retrieval scheme based on local features in cloud environment. This scheme extracted image features by SIFT algorithm. EMD method was applied to evaluate the similarity of images and local sensitive hashing algorithm was applied to construct a hash table. With the cost of more time on extracting image features, SIFT algorithm improved the search efficiency of this algorithm. Xia *et al.* [24] proposed a privacy -preserving image retrieval scheme. LSH algorithm and K nearest neighbor algorithm were utilized to improve search efficiency and ensure data security. But the scheme did not optimize the hash functions and the hash tables.

This paper proposed an encrypted image retrieval algorithm based on Harris corner selection and p-stable LSH. Firstly, the Harris corners are selected and optimized by the 8-neighborhood similar pixel analysis method and Forstner algorithm [25]. Secondly, the SURF algorithm and the BOW model are applied on cluster image features to form feature vectors that effectively represent the image, LSH algorithm builds the indexes. Finally, the encryption scheme [24] encrypts the data. Thus the similarity of the feature vectors is calculated by the Euclidean distance.

II. SYSTEM MODEL AND RELATED PRELIMINARIES

A. SYSTEM MODEL

This paper uses a similar model as the one of Xia [24]. There are three modules: image owners, image users, and cloud server.

Cloud server provides content-based encrypted image retrieval. The authorized user generates and submits a search request to the cloud service. The cloud service responses search results to image users.

Image users have the authorization of data owner, and extract the feature set$\{G_i'\}_{i=1}^n$ from the query image $M_q = \{m_1, m_2, \cdots, m_{n_q}\}$, and generate query vectors $\{f_{qi}\}_{i=1}^{n_q}$, where n_q denotes the number of images in the query image databaseM_q. Then, build the trapdoor TD. Finally, decrypt the query result $\mathcal{R}$.

Image owners outsource the image set $M = \{m_1, m_2, \cdots, m_n\}$ to the cloud server and maintain the search capability, where n denotes the number of images m in the image library M. Image owners firstly extract the image feature set $\{G_i\}_{i=1}^n$ from the image library M, and generate feature vectors $\{f_i\}_{i=1}^n$ and build searchable indexes I. Then encryption $\{f_i\}_{i=1}^n$, M and I are sent to the cloud. To facilitate the authorized users to access the data, image owners need to send a series of key information to the query user to decrypt the data.

B. RELATED PRELIMINARIES

In our proposed scheme, the improved Harris algorithm [26] is applied to extract image features, and an optimized LSH algorithm is used to construct the index of image features. In this section, Harris algorithm and LSH algorithm are introduced.

1) HARRIS CORNER OPTIMIZATION BASED ON ADAPTIVE THRESHOLD AND FORSTNER

The content-based encrypted image retrieval scheme usually extracts the local features of the image, including SIFT features, corner features etc. Although the SIFT feature has good robustness, the time cost of the algorithmis more. Compared with SIFT algorithm, the Harris algorithm takes less time. Therefore, the Harris algorithm is used. However, there are many other problems in the Harris algorithm, such as low detection efficiency, non-maximum value, *et al.* Thus, we use the improved Harris algorithm [26] to extract the image features. The steps are described in detail as follows.

Step 1: The candidate set C is determined by 8 neighborhood similar pixel analysis. Specific process is as follows: 1) For the target pixel (x, y), calculate the absolute value Δ of the pixel gray level difference between the target pixel and the 8 neighborhood. 2) Determine whether the target pixel is similar to the surrounding 8 points by comparison with the set threshold t', $N(x, y)$ denotes the number of similar points, which is shown in Eq.(1):

$$N(x, y) = \sum_{ij} \chi(x+i, y+j) \times (-1 \leq i \leq 1, -1 \leq j \leq 1, i \neq 0, j \neq 0) \tag{1}$$

$$\chi(x+i, y+j) = \begin{cases} 1, & \Delta(x+i, y+j) \leq t' \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

if $2 \leq N(x, y) \leq 6$, the point is considered as a candidate, and C is the set of candidate points.

Step 2: The angle response function CRF of each candidate point is obtained, the threshold $\mathcal{T}$ is defined as ρ times of the maximum CRF value, as shown in Eq.(3). The candidate point is filtered by the maximum corner response function T. The total number of extracted pre-filtered feature points is c_1, and the pre-screening feature is set as C_1. Specific details are explored in literature [26].

$$\mathcal{T} = \rho * CRF_{max} \tag{3}$$

Step 3: The Froster algorithm [25] is applied to determine the total number of best candidate points c_2. Firstly, the $3 * 3$ window is built with the arbitrary feature points (x_i, y_i) of C_2 as the center, and the covariance matrix cov of each point within the window is calculated, it is described in Eq.(4):

$$cov = \begin{bmatrix} \sum \mathcal{I}'^2_x & \sum \mathcal{I}'_x \mathcal{I}'_y \\ \sum \mathcal{I}'_x \mathcal{I}'_y & \sum \mathcal{I}'^2_y \end{bmatrix} \tag{4}$$

where $\mathcal{I}'_x$, $\mathcal{I}'_y$ is Robert's gradient operator, $\mathcal{I}'_x = f(x+1, y+1) - f(x, y)$, $\mathcal{I}'_y = f(x+1, y) - f(x, y+1)$, $f(x+1, y+1)$ denote the pixel gray level of $(x+1, y+1)$. Secondly, the weight ω and the roundness τ of the feature points are calculated, which are shown in Eq.(5) and (6).

$$\omega = \frac{det(cov)}{trace(cov)} \tag{5}$$

$$\tau = \frac{4det(cov)}{(trace(cov))^2} \tag{6}$$

The determinant of the covariance matrix cov is $det(cov)$, the trace of the covariance matrix cov is $trace(cov)$. Then, ω and τ are compared with the given thresholds $\mathcal{T}_\omega$ and $\mathcal{T}_\tau$ to determine the alternate point feature set C_2. Finally, the total number of the best candidate point c_2 is determined by the weight in a certain window, the feature points set: the feature points set: $G = \{(x_i, y_i)\}_{i=1}^{c_2}$. Specific details are explored in literature [26].

2) LOCAL SENSITIVE HASH ALGORITHM

Local Sensitive Hash is member of hash functions, in which two adjacent data points in the original data space have a large probability to hash into the same bucket. This property can be applied in approximate queries [27]. A hash function family $\mathcal{H} = \{h : \mathcal{S} \to U\}$ is regarded to be $(w, c * w, p_1, p_2\ )$ local-sensitive for any $(x, y) \in \mathcal{S}$ if

$$\begin{cases} P_w\{h(x) = h(y)\} \geq p_1 & d(x, y) \leq w \\ P_w\{h(x) = h(y)\} \leq p_2 & d(x, y) \geq c * w \end{cases} \tag{7}$$

where $d(x, y)$ denotes the distance between x and y, the constant $c > 1$ probabilitiy $p_1 > p_2$, w is the parameter. Increasing the hash function can enlarge the gap between p_1 and p_2, to obtain efficient retrieval.

The p-stable LSH function family is a kind of local sensitive hash function. p-stable LSH function $h_{a,b} : \mathfrak{R}^l \to Z$ can map, l-dimensional vector v to an integer [27], as shown in Eq.(8)

$$h_{a,b}(v) = \left\lfloor \frac{a \cdot +b}{w} \right\rfloor \tag{8}$$

where a is a l-dimensional random vector with the entries following a p-stable distribution, $b \in [0, w]$.

III. AN ENCRYPTED IMAGE RETRIEVAL SCHEME BASED ON HARRIS CORNER OPTIMIZATION AND LSH

This paper aims at reducing the feature extraction time consuming and improving the efficiency of image retrieval. First, the improved Harris algorithm is used to extract the image features [26]. Second, SURF algorithm is applied to form the feature vectors of each image. Then, the optimized LSH algorithm builds the index. Finally, the traditional encryption scheme encrypts the data, and cloud service executes similarity search. The system model of encrypted image retrieval is shown in Figure 1.

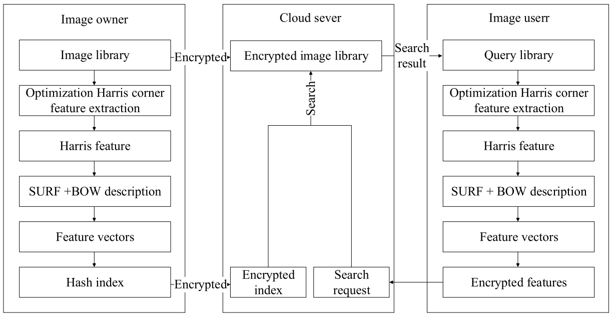


FIGURE 1. The system model of encrypted image retrieval.

A. FEATURE DESCRIPTION COMBINED WITH SURF AND BOW MODEL

In order to improve the image representation ability of Harris feature points and improve the accuracy and efficiency of image retrieval, this paper combines the SURF algorithm [28] to describe the image features, and uses the BOW model to generate the image feature vectors.

Harris features description algorithm based on SURF is described as follows:

Step 1: Establish scale space of Harris feature point.

Step 2: Select the main direction for the Harris feature point. 1) Construct 60° sector domain is with a radius of $60s$

centered on each feature point (x_i, y_i) in G, in which s denotes the scale of the point. 2) Calculate the sum of the Haar wavelet responses in the horizontal and vertical directions of the feature points in this sector domain, as $\sum \aleph_i$, in which $\aleph_i$ denotes the sum of the Haar wavelet responses of one of the feature points. Here the edge length of Haar wavelet is $4s$. 3) Rotat the sector is at regular intervals, and the direction of the fan at the maximum value $\sum \aleph_i$ is selected as the main direction of the feature.

Step 3: A square of $20s$ side length is divided into 16 small square windows. The formula (9) is to calculate the characteristic sub-vector $\mathcal{V}$ in each window.

$$\mathcal{V} = (\sum d_x, \sum d_y, \sum |d_x|, \sum |d_y|) \tag{9}$$

where $\sum d_x$ denotes the horizontal direction sum of Haar wavelet features,$\sum d_y$ denotes the vertical direction sum of Haar wavelet features, $\sum |d_x|$ denotes the sum of the horizontal absolute values of Harr wavelet features, $|\sum d_y|$ denotes the sum of the vertical absolute values of Harr wavelet features.

The eigenvectors of the image is generated by BOW model as shown in the following steps:

Step 1: Apply the k-means algorithm [29] on clusters local features $\{\mathcal{C}_i\}_{i=1}^{c2}$ to form a visual word, $\{\mathcal{C}_i\}_{i=1}^{c2}$ denotes $\{(x_i, y_i)\}_{i=1}^{c2}$. k-mean clustering process: Firstly, $\mathcal{K}$ points$\{\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_\mathcal{K}\}$ are regarded as cluster centers, which are randomly selected. Secondly, calculate the distance d' from each data point to the $\mathcal{K}$ center by Eq.(10). The data points are distributed to the nearest center to form $\mathcal{K}$ clusters $\mathcal{U} = \{\mathcal{U}_i\}_{i=1}^{\mathcal{K}}$.

$$d' = \sum_{i}^{c_2} \sum_{j}^{\mathcal{K}} \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \tag{10}$$

In Eq.(10), $(x_i, y_i) \in G$, $(x_j, y_j) \in \mathcal{C}_\mathcal{K}$.

Then, calculate the average $\bar{\mathcal{U}}_j$ of the clusters by Eq.(11). $\mathfrak{u}$ becomes the new cluster centers and form the visual words $\mathfrak{u} = \{\mathfrak{u}_1, \mathfrak{u}_2, \cdots, \mathfrak{u}_\mathcal{K}\}$.

$$\bar{\mathcal{U}}_j = \frac{1}{|\mathcal{U}|} \sum_{j=1}^{\mathcal{K}} \mathcal{U}_j \tag{11}$$

$\bar{\mathcal{U}}_j$ denotes the average value of the j word $\mathcal{U}_j$, $|\mathcal{U}|$ denotes the size of the set $\mathcal{U}$.

Finally, the values of the cluster centers are calculated by repeating the above steps until MSE converges. Visual words are denoted as $\mathfrak{u}' = \{\mathfrak{u}'_1, \mathfrak{u}'_2, \cdots, \mathfrak{u}'_\mathcal{K}\}$.

$$MSE = \sum_{j=1}^{\mathcal{K}} \sum_{\mathcal{U}_i \in \mathcal{U}} |\mathcal{U}_i - \bar{\mathcal{U}}_j|^2 \tag{12}$$

Step 2: The Eq.(13) maps the local feature $\mathcal{C}_i$ to the visual word. The image feature vector f_i can be calculated by counting the frequency of visual words in the entire image. The feature vectors of all images are denoted as $\{f_i\}_{i=1}^{n}$.

$$\mathcal{C}_i = \omega' = \{\omega_1, \omega_2, \cdots, \omega_\mathcal{K}\} \tag{13}$$

$\{\omega_1, \omega_2, \cdots, \omega_\mathcal{K}\}$ is denoted as the weight of $\mathcal{C}_i$ corresponding to the visual word $\mathfrak{u}'$. Specific details are explored in Algorithm 1:

Algorithm 1 : The Feature Description Algorithm of SURF and the BOW Model

```
Require: $G = \{(x_i, y_i)\}_{i=1}^{c2}$, $\mathcal{K}$, images set $M$
Ensure: $f_i$
Initialization $\mathcal{U} \leftarrow \emptyset, f_i \leftarrow \emptyset, \mathfrak{u} = 0, sum = 0, \mathcal{C}' \leftarrow \emptyset$
Establishment of Scale Space
for $i = 1, \cdots, c_2$ do
    Calculate $\sum sum_i$ by Step2 of the SURF algorithm, select the main direction of the feature
    Generate description vectors $\{\mathcal{C}_i\}_{i=1}^{c2}$ by Step3 of the SURF algorithm
end for
for $i = 1, \cdots, c_2$ do
    $\mathcal{K}$ points$\{\mathcal{C}_1, \mathcal{C}_2$, ą, $\mathcal{C}_\mathcal{K}\}$ are used as cluster centers
    Calculate $d'$ by formula (10), generate $\mathcal{K}$ clusters $\mathcal{U} \leftarrow \mathcal{U} \cup \mathcal{U}_i$
    for $j = 1, \cdots, \mathcal{K}$ do
        Calculate the average value of each cluster by Eq.(11),update cluster center, $\mathfrak{u} \leftarrow \mathfrak{u} \cup \mathfrak{u}_j$
        Calculate $MSE$ by Eq.(12)
        Repeat Step1 of the BOW model until $MSE$ converges, visual words can denote $\mathfrak{u}' \leftarrow \mathfrak{u}' \cup \mathfrak{u}'_j$
        Use the Step2 of the BOW model to generate the feature vector of the image,$f_i = f_i \cup f_{i,j}$
    end for
end for
```

Since the extracted feature vectors are used directly to retrieve the similarity, the algorithm efficiency cannot be obtained. Therefore, a more reasonable algorithm should be proposed to achieve the purpose of efficient retrieval.

B. HASH INDEX CONSTRUCTION

In order to improve the retrieval efficiency, this paper proposes a pre-processing index table to pre-filter similar images. Compared with the existing methods, which mostly adopted the LSH algorithm to build indexes, this paper adopts the p-stable LSH family of functions to construct the searchable index. Since p-stable LSH has the local sensitivity characteristics of LSH algorithm, this paper optimizes the algorithm by increasing the number of LSH function families and the number of hash tables. In specific, the image owners randomly choose L LSH functions $\{h_1, h_2, \cdots, h_L\}$and apply $g(f_i) = (h_1(f_i), \cdots, h_L(f_i))$ to all features in $\{f_i\}_{i=1}^{n}$. To improve accuracy, this process is repeated λ times to generate λ pre-filter tables. The set of buckets is denoted as $\{D_{i,j}\}$, $(i \in [1, \lambda], j \in [1, N_i])$, in which N_i refers to the total number of buckets in the ith pre-filter table. $ID(m_t)$ means

TABLE 1. The *i*th table of encrypted hash.

$\phi : (k'', D_{i,1})$	$D(m_1), ID(m_4), ID(m_7), ID(m_{11}) \cdots$
$\phi : (k'', D_{i,2})$	$D(m_9), ID(m_{12}), ID(m_{15}), ID(m_{18}) \cdots$
$\cdots$	$\cdots$
$\phi : (k'', D_{i,N_i})$	$D(m_{13}), ID(m_{16}), ID(m_{19}), ID(m_{22}) \cdots$

that the image m_t is mapped into$\{D_{i,j}\}$, as shown in Table1. The key k'' is generated using the scheme of literature [24]. To enhance the security, the bucket values are protected by a one-way hash function ϕ.

The hash index table can save similar images in the same bucket. Thus the users can shorten the query time while searching. However, there are still dissimilar images in the search results, which cannot meet the needs. In order to improve the retrieval accuracy, this paper adopts the Euclidean distance to measure similar images that have been searched. In summary, this article intends to design a safer encrypted image retrieval scheme with less feature extraction time.

C. ANALYSIS OF ENCRYPTED IMAGE RETRIEVAL SCHEME BASED ON HARRIS CORNER OPTIMIZATION AND LSH

This proposed scheme is consisted of three modules: image owners, image users, and cloud service. Each modules has its own task. They form the entire encrypted image retrieval system.

Image owners: Firstly, $Gen_{Harris}(Harris, M)$ algorithm generates the feature set$\{G_i\}_{i=1}^{n}$. Secondly $Gen_{feature}$ $(\{G_i\}_{i=1}^{n})$ algorithm calculates the feature vector $\{f_i\}_{i=1}^{n}$, then, $Build_{index}(\{f_i\}_{i=1}^{n})$ algorithm generates index I. Then, $Enc_{data}(\{f_i\}_{i=1}^{n}, M, I)$ algorithm generates the encrypted feature vectors $\{f_i'\}_{i=1}^{n}$, encrypted image set M' and the encrypted index I'. Finally, $\{f_i'\}_{i=1}^{n}$, M' and I' are sent to cloud server, and the encryption key K is sent to image users. The key K is generated using the scheme of literature [24]. The eigenvectors and indexes are encrypted in the same way as in reference [24].

Image users: Firstly, $Gen_{Harris}(Harris, M_q)$ algorithm calculates the feature set $\{G_i'\}_{i=1}^{n_q}$. Secondly, $Gen_{feature}(\{G_i'\}_{i=1}^{n_q})$ algorithm generates the feature vector $\{f_{q_i}\}_{i=1}^{n_q}$. Thirdly, TD is generated by $Gen_{TD}(K, \{f_{q_i}\}_{i=1}^{n_q})$ algorithm. Then, TD is sent to the cloud server. Finally, $Dec_{data}(K, \mathcal{R})$ algorithm decrypts the similar images set $\mathcal{R}$.

Cloud server: $Search(I, M', \{f_i'\}_{i=1}^{n}, TD)$ is applied to retrieve and return similar images $\mathcal{R}$. The specific details are explored in Algorithm 2:

Algorithm 2 :The Algorithm of the Encrypted Image Retrieval.

Image owners

1: **Step 1:**$(\{G_i\}_{i=1}^{n}) \leftarrow Gen_{Harris}(Harris, M)$, improved Harris algorithm extracts features $\{G_i\}_{i=1}^{n}$ from image set M.

2: **Step 2:** $\{f_{qi}\}_{i=1}^{n_q} \leftarrow Gen_{Harris}(\{G_i\}_{i=1}^{n})$, combine SURF algorithm and BOW model generates feature vectors $\{f_i\}_{i=1}^{n}$.

3: **Step 3:** $I \leftarrow Build_{index}$ $(\{f_i\}_{i=1}^{n})$, optimized p-stable LSH algorithm builds an index.

4: **Step 4:** I', M', $\{f_i'\}_{i=1}^{n} \leftarrow Enc_{data}(\{f_i\}_{i=1}^{n}, M, I)$, this paper adopts $Chao_{data}(M)$ algorithm to encrypt the image set M. The encrypted images is M'. Encrypted eigenvectors and encrypted indexes are I', $\{f_i'\}_{i=1}^{n}$.

Image users

5: **Step1:**$\{G_i'\}_{i=1}^{n_q} \leftarrow Gen_{Harris}(M_q)$, improved Harris algorithm extracts features $\{ G_i' \}_{i=1}^{n_q}$ from image set M_q.

6: **Step2:**$\{f_{qi}\}_{i=1}^{n_q} \leftarrow Gen_{feature}(\{G_i'\}_{i=1}^{n_q})$, combine SURF with BOW algorithm to generates feature vectors $\{f_{q_i}\}_{i=1}^{n_q}$.

7: **Step3:**$TD \leftarrow Gen_{TD}$ $(K, \{ f_{q_i}\}_{i=1}^{n_q})$, the key K encrypts the query vector to generate trapdoor TD.

8: **Step4:** $\mathcal{R} \leftarrow Dec_{data}$ $(K, \mathcal{R})$, the key K decrypts image set $\mathcal{R}$.

Cloud server

9: **Step1:**$\mathcal{R} \leftarrow Search(I, M', \{f_i'\}_{i=1}^{n}, TD)$ secures the similarity retrieval on the cloud server, and returns the image user the query result $\mathcal{R}$.

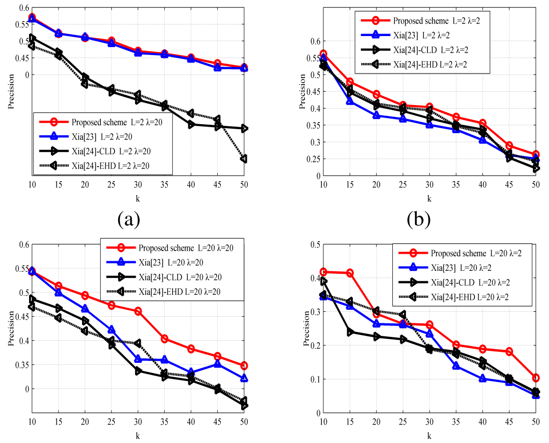
IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experiments of this scheme used MatlabR2014a and vs2008 C++ in Dell-14R-5421 laptop, with Windows 10 and CPU for Intel (R) Core (TM) i5-3337U 1.80GHz to evaluate the performance. The image database is Corel test set [30], which includes 10 categories and 100 JPG similar images for each category in the size of 256 × 384 or 384 × 256. This paper optimizes the encrypted image retrieval in Harris algorithm, L and λ, L is the number of the jointed LSH functions in the construction of pre-filter table. The parameters of the experiment are set as $w = 4$, $\mathcal{K} = 128$.

A. RETRIEVAL PRECISION

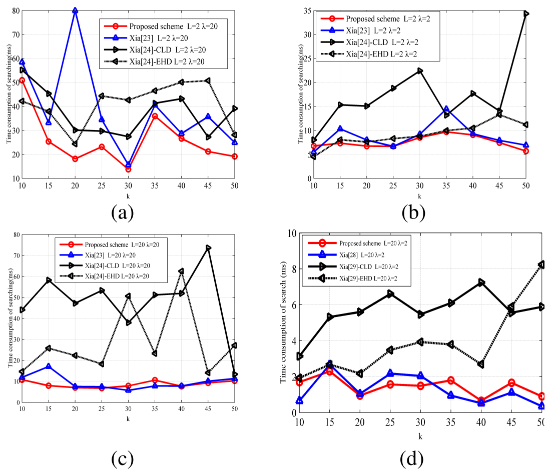
The retrieval precision in this paper is settled as $P_k = \frac{k'}{k}$, which k' is the number of real similar images in the k retrieved images. In the experiments, two images are randomly selected in the 10 different types of images to form a query library. Then, it is to test the retrieval accuracy of the retrieval schemes when $k = 10, 20, 25, 30, 35, 40, 45, 50$ respectively, the accuracy results are compared with the one of Xia's scheme [23] and Xia's scheme [24]. For the sake of better understanding, in the below statements, the scheme I denotes Xia's scheme [23], the scheme II denotes Xia's scheme [24]-CLD and Xia's scheme [24]-EHD.

Figure 2 shows the efficiency of search, when L and λ take different parameters, the retrieval efficiency decreases with the increasement of k. As shown in Figure 2(a), when $L = 2$, $\lambda = 20$, the retrieval efficiency of the proposed scheme is higher than 40% on average, while the retrieval accuracy of the scheme II is less than 35%, but when $k \leq 20$, the retrieval efficiency of the proposed scheme is the same with the scheme I; while $k > 20$, the retrieval efficiency of the proposed scheme is slightly higher than the scheme I. When L is unchanged and λ is increased, although the retrieval



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

FIGURE 2. Search precision.



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

FIGURE 3. Time consumption of search.

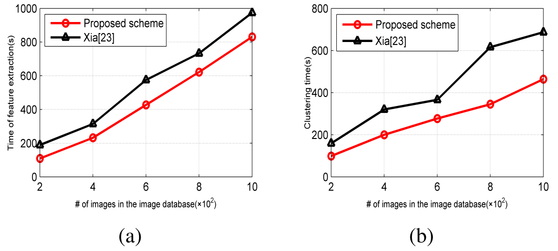
efficiency of three schemes reduced, the overall retrieval efficiency of the proposed scheme is still higher than the other two scheme, as shown in Figure 2(b). Next, when λ is unchanged and L is increased, the overall retrieval efficiency of the proposed scheme is more efficient than that of the scheme II, when $k = 10$, the retrieval efficiency of the proposed scheme and the scheme I is 54.3%, while $k > 10$, the proposed scheme is better than that of the scheme I, as shown in Figure 2(c). Finally, when λ is decreased and L is increased, the retrieval efficiency of the proposed scheme is higher than I scheme, but when $20 \leq k \leq 25$, the retrieval efficiency of the proposed scheme is lower than that of the scheme II; when $k < 20$ and $k > 25$, the proposed scheme is more efficient than that of the scheme I, as shown in Figure 2(d). The experimental results prove that the retrieval efficiency of the proposed method is better than the scheme I and the scheme II.

B. RETRIEVAL TIME

This paper investigates the retrieval time in three aspects: the searching, the index and the trapdoor.

1) SEARCHING TIME CONSUMPTION

Figure 3 shows the searching time of two schemes. When $L = 2$, $\lambda = 20$, compared with the scheme I and the scheme II, the proposed scheme spends less search time, as shown in Figure 3(a). Firstly, when L is unchanged and λ is increased, although the search time of the three scheme is much less than the original search time, the overall retrieval time of the proposed scheme is lower than that of the scheme I and the scheme II, as shown in Figure 3(b). Next, keeping λ is unchanged and L is increased, the search time is reduced. The proposed scheme spends less search time than the scheme II, but when $25 < k \leq 40$, the scheme I performs slightly better than the proposed scheme; when $k \leq 25$ and $k > 40$, the search time of the proposed scheme is lower than the scheme I, as shown in Figure 3(c). Finally, when λ is decreased and L is increased, the search time of the proposed scheme is less than the scheme II, and when $k \leq 30$, the search time of the proposed scheme is lower than the scheme I; when $k > 30$, the scheme I performs slightly better the proposed one, as shown in Figure 3(d). According to the entire search time analysis, the proposed scheme is less than the scheme I and the scheme II on searching time consumption.



(a) (b)

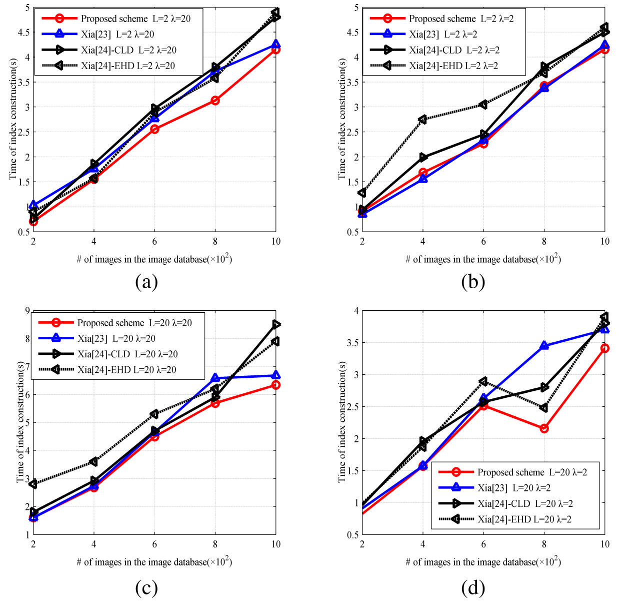
FIGURE 4. Time consumption of feature extraction and clustering.

2) INDEX CONSTRUCTION TIME CONSUMPTION

Before constructing an index with a p-stable LSH algorithm, image features should be extracted. The BOW model is applied to cluster and generate feature vectors. The index construction time consumption can be divided into three parts: feature extraction time, clustering time, and index construction time.

Figure 4(a) and 4(b) show the time consumption of feature extraction and clustering in the two schemes. It can be seen that the time consumption of both the feature extraction and the clustering in the proposed scheme is less than that of the scheme I.

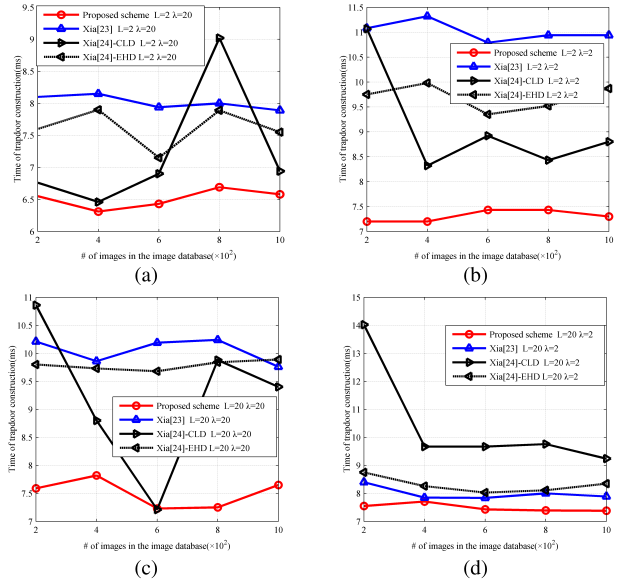
Figure 5 shows the index construction time consumption for different image set sizes. It can be seen that the index construction time is proportional to the size of the image set. When $L = 2$ and $\lambda = 20$, the index construction time of the proposed scheme is lower than the scheme I and the scheme II, as shown in Figure 5(b). When keep L is unchanged and λ is increased, the index construction time of the scheme I and the proposed scheme is flat, but the index construction time of the proposed scheme is shorter



(a) (b)

(c) (d)

FIGURE 5. Time consumption of index construction.



(a) (b)

(c) (d)

FIGURE 6. Time consumption of trapdoor construction.

than the scheme II, as shown in Figure 5(b). When keep λ is unchanged and L is increased, the index construction time has increased obviously, but the index construction time of the proposed scheme is less than the scheme I and the scheme II, as shown in Figure 5(c). Finally, when λ is decreased and L is increased, the proposed scheme spends less index construction time than the scheme I and the scheme II, as shown in Figure 5(d). The entire index construction time analysis shows that the proposed scheme is more efficient than the scheme I and the scheme II on index construction.

3) TRAPDOOR CONSTRUCTION

Figure 6 shows the trapdoor construction time consumption of three schemes. When $L = 2$ and $\lambda = 20$, the trapdoor time of the proposed scheme is less than the scheme I and the scheme II, as shown in Figure 6(a). When L is unchanged and λ is decreased, the trapdoor construction time of the proposed scheme is shorter than the scheme I and the scheme II, as shown in Figure 6(b). When λ is unchanged and L is increased, although the trapdoor time of three schemes increases, the proposed scheme takes less time than the scheme I and the scheme II, as shown in Figure 6(c). When λ is decreased and L is increased, the proposed scheme spends less time than the scheme II. Although the scheme I decreases, the proposed scheme time still takes less time than the scheme I, as shown in Figure 6(d). According to the time cost analysis of the entire trapdoor, it can be seen that the proposed scheme takes shorter time to construct trapdoors than the scheme I and the scheme II.

V. CONCLUSION

This paper proposes a novel encrypted image retrieval scheme based on Harris corner preference and LSH optimization in cloud computing. Firstly, we use the improved Harris algorithm to extract the image features. Secondly, in order to retrieve on the cloud server more sufficiently, SURF algorithm is combined with BOW model to generate the feature vectors of each image. Then, aims at improving the retrieval efficiency, the parameters of LSH algorithm are optimized and applied to construct the searchable index. Finally, the encrypted similar images can be searched successfully by the cloud server. The next step will be extracting the features of the encrypted image, and design a more secure encryption scheme and support similarity retrieval.

REFERENCES

[1] K. Djemame, D. Armstrong, J. Guitart, and M. Macias, "A risk assessment framework for cloud computing," *IEEE Trans. Cloud Comput.*, vol. 34, no. 3, pp. 265–278, Sep. 2016.

[2] J. Li, C. Jia, Z. Liu, J. Li, and M. Li, "Survey on the searchable encryption," *J. Softw.*, vol. 26, no. 1, pp. 109–128, Jan. 2015.

[3] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 451–459.

[4] Z. Xia, Y. Zhu, X. Sun, and L. Chen, "Secure semantic expansion based search over encrypted cloud data supporting similarity ranking," *J. Cloud Comput.*, vol. 3, no. 1, pp. 1–11, Jul. 2014.

[5] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," *IEICE Trans. Commun.*, vol. 98, no. 1, pp. 190–200, Feb. 2015.

[6] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2706–2716, Dec. 2017.

[7] H. Li, D. Liu, Y. Dai, T. H. Luan, and X. S. Shen, "Enabling efficient multi-keyword ranked search over encrypted mobile cloud data through blind storage," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 1, pp. 127–138, Mar. 2015.

[8] Y. Yang and M. Ma, "Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 4, pp. 746–759, Apr. 2017.

[9] Y. Zheng, B. Jeon, D. Xu, Q. Wu, and H. Zhang, "Image segmentation by generalized hierarchical fuzzy C-means algorithm," *J. Intell. Fuzzy Syst.*, vol. 28, no. 2, pp. 4024–4028, Feb. 2015.

[10] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, Apr. 2013, pp. 258–274.

[11] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 340–352, Feb. 2016.

[12] Z. Wei, Y. Lin, S. Xiao, J. Wu, and S. Zhou, "Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing," *IEEE Trans. Comput.*, vol. 65, no. 5, pp. 1566–1577, May 2016.

[13] C. Orencik, M. Kantarcioglu, and E. Savas, "A practical and secure multi-keyword search method over encrypted cloud data," in *Proc. IEEE 6th Int. Conf. Cloud Comput.*, Jun. 2013, pp. 390–397.

[14] S. J. Xiang and X. R. Luo, "Reversible data hiding in encrypted image based on homomorphic public key cryptosystem," *J. Softw.*, vol. 27, no. 6, pp. 1592–1601, Jan. 2016.

[15] C. Yuan, Z. Xia, and X. Sun, "Coverless image steganography based on SIFT and BOF," *J. Internet Technol.*, vol. 18, no. 2, pp. 435–442, Mar. 2017.

[16] K. Mishra, R. Saharan, and B. Rathor, "A new cryptographic method for image encryption," *J. Intell. Fuzzy Syst.*, vol. 32, no. 4, pp. 2885–2892, Jul. 2017.

[17] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Opt. Laser Technol.*, vol. 101, pp. 30–41, May 2018.

[18] D. Huang, X. Geng, L. Wei, and C. Su, "A secure query scheme on encrypted remote sensing images based on Henon mapping," *J. Softw.*, vol. 27, no. 7, pp. 1729–1740, Jul. 2016.

[19] H. Liu and H. Go, "Privacy-enhanced similarity search scheme for cloud image databases," *IEICE Trans. Inf. Syst.*, vol. E99-D, no. 12, pp. 3188–3191, Dec. 2016.

[20] Z. Zhou, Y. Wang, J. Wu, C.-N. Yang, and X. Sun, "Effective and efficient global context verification for image copy detection," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 48–63, Jan. 2017.

[21] T. K. Hazra, S. R. Chowdhury, and A. K. Chakraborty, "Encrypted image retrieval system: A machine learning approach," in *Proc. IEEE Electron. Mobile Commun. Conf.*, Oct. 2016, pp. 1–6.

[22] Z. A. Abduljabbar *et al.*, "Privacy-preserving image retrieval in IoT-cloud," in *Proc. Trustcom/Bigdatase/ISPA*, Aug. 2017, pp. 799–806.

[23] Z. Xia, Y. Zhu, X. Sun, Z. Qin, and K. Ren, "Towards Privacy-preserving content-based image retrieval in cloud computing," *IEEE Trans. Cloud Comput.*, vol. 6, no. 1, pp. 276–286, Oct. 2015.

[24] Z. Xia, N. N. Xiong, A. V. Vasilakos, and X. Sun, "EPCBIR: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing," *Inf. Sci.*, vol. 387, pp. 195–204, Dec. 2017.

[25] W. Forstner and E. Gülch, "A fast operator for detection and precise location of distinct points, corners circular features," in *Proc. ISPRS Intercommission Workshop Interlaken*, Jan. 1987, pp. 281–305.

[26] H. Li, J. Qin, X. Xiang, L. Pan, W. Ma, and N. N. Xiong, "An efficient image matching algorithm based on adaptive threshold and RANSAC," *IEEE Access*, vol. 6, pp. 66963–66971, Nov. 2018.

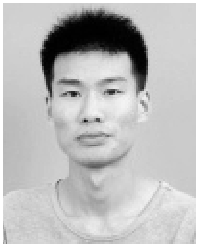
[27] M. Datar, N. Immorlica, P. Indyk, and V. S. Mirrokni, "Locality-sensitive hashing scheme based on p-stable distributions," in *Proc. 12th Symp. Comput. Geometry*, Jan. 2004, pp. 253–262.

[28] H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, "Speeded-up robust features (SURF)," *Comput. Vis. Image Understand.*, vol. 110, no. 3, pp. 346–359, Jun. 2008.

[29] X. Liu *et al.*, "Late fusion incomplete multi-view clustering," *IEEE Trans. Pattern Anal. Mach. Intell.*, to be published. doi: 10.1109/TPAMI.2018.2879108l.

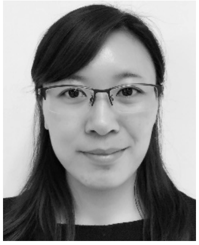
[30] J. Wang, J. Li, and G. Wiederhold, "SIMPLIcity: Semantics-sensitive integrated matching for picture libraries," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 23, no. 9, pp. 947–963, Sep. 2001.

JIAOHUA QIN received the B.S. degree in mathematics from the Hunan University of Science and Technology, China, in 1996, the M.S. degree in computer science and technology from the National University of Defense Technology, China, in 2001, and the Ph.D. degree in computing science from Hunan University, China, in 2009. She is currently a Professor with the Central South University of Forestry and Technology, China. Her research interests include information security and artificial intelligence.



HAO LI received the B.S. degree in computer science and technology from Zhengzhou University, China, in 2015. He is currently pursuing the M.S. degree in computer application technology with the College of Computer Science and Information Technology, Central South University of Forestry and Technology, China. His research interests include information security and image processing.

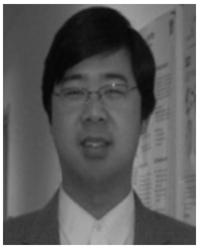
XUYU XIANG received the B.S. degree in mathematics from Hunan Normal University, China, in 1996, the M.S. degree in computer science and technology from the National University of Defense Technology, China, in 2003, and the Ph.D. degree in computing science from Hunan University, China, in 2010. He is currently a Professor with the Central South University of Forestry and Technology, China. His research interests include network and information security, image processing, and the Internet of Things.



YUN TAN received the M.S. and Ph.D. degrees from the Beijing University of Posts and Telecommunications, China, in 2004 and 2016, respectively. She is currently a Lecturer with the College of Computer Science and Information Technology, Central South University of Forestry and Technology. Her research interests include image security, compressive sensing, and signal processing.

WENYAN PAN received the B.S. degree in electronic and information engineering from Hunan City University, China, in 2017. He is currently pursuing the M.S. degree in computer technology with the College of Computer Science and Information Technology, Central South University of Forestry and Technology, China. His research interests include machine learning and image processing.

WENTAO MA received the B.S. degree in electronic science and technology from the Mingde College, Northwestern Polytechnical University, China, in 2017. He is currently pursuing the M.S. degree in information and communication engineering with the College of Computer Science and Information Technology, Central South University of Forestry and Technology, China. His research interests include pattern recognition and image processing.



NEAL N. XIONG received the Ph.D. degree in sensor system engineering from Wuhan University and the Ph.D. degree in dependable sensor networks from the Japan Advanced Institute of Science and Technology. Before he attends Northeastern State University, he was with Georgia State University, Wentworth Technology Institution, and Colorado Technical University for about 10 years. He is current an Associate Professor (third year) with the Department of Mathematics and Computer Science, Northeastern State University, OK, USA. His research interests include cloud computing, security and dependability, parallel and distributed computing, networks, and optimization theory.