An Encrypted Image Retrieval Method Based on SimHash in Cloud Computing

Jiaohua Qin[1], Yusi Cao[1], Xuyu Xiang[1, *], Yun Tan[1], Lingyun Xiang[2] and Jianjun Zhang[3]

Abstract: With the massive growth of images data and the rise of cloud computing that can provide cheap storage space and convenient access, more and more users store data in cloud server. However, how to quickly query the expected data with privacy-preserving is still a challenging in the encryption image data retrieval. Towards this goal, this paper proposes a ciphertext image retrieval method based on SimHash in cloud computing. Firstly, we extract local feature of images, and then cluster the features by K-means. Based on it, the visual word codebook is introduced to represent feature information of images, which hashes the codebook to the corresponding fingerprint. Finally, the image feature vector is generated by SimHash searchable encryption feature algorithm for similarity retrieval. Extensive experiments on two public datasets validate the effectiveness of our method. Besides, the proposed method outperforms one popular searchable encryption, and the results are competitive to the state-of-the-art.

Keywords: Cloud computing, SimHash, encryption image retrieval, K-means.

1 Introduction

With the rapid popularity of cloud computing technology, more and more enterprises and individuals begin to outsource multimedia data, especially image to the cloud server [Vaquero, Roderomerino, Caceres et al. (2008)]. As one of the most common data, the image plays an important role in all walks of life. In medicine, entertainment and other fields, we need to store and manage the large image efficiently which has become an urgent problem.

However, with the popularization of cloud computing, its security issues have become a prominent bottleneck which restricts its development [Xia, Xiong, Vasilakos et al. (2017)]. Therefore, it is challenging to make the image owners to encrypt and store images in cloud computing and ensure that the authorized users can search images quickly.

[1] College of Computer Science and Information Technology, Central South University of Forestry & Technology, Changsha, 410004, China.

[2] School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha, 410114, China.

[3] College of Engineering and Design, Hunan Normal University, Changsha, 410012, China.

[*] Corresponding Author: Xuyu Xiang. Email: xyuxiang@163.com.

Received: 02 July 2019; Accepted: 11 July 2019.

CMC. doi:10.32604/cmc.2020.07819

The existing Searchable Encryption Scheme (SSE) enables image owners to store encryption data in cloud servers and support data search in ciphertext domains [Zhang, Liu, Dunder et al. (2015)]. Recently, many researchers have done a lot of research on encrypted image retrieval methods. Bellafqira et al. [Bellafqira, Coatrieux, Bouslimi et al. (2015); Bellafqira, Coatrieux, Bouslimi et al. (2016)] proposed two feature extraction methods of privacy-preserving in homomorphic encryption. However, the extracted features can't be used for image similarity retrieval. Hsu et al. [Hsu, Lu and Pei (2012)] proposed a homomorphic encryption-based privacy-preserving SIFT (PPSIFT) approach to settle the privacy-preserving problem encountered in a cloud computing. SIFT is generated in the encryption domain by homomorphic encryption and plaintext multiplication. Although the algorithm based on homomorphic encryption has high security, it takes a long time and increases the user's computation. Liu et al. [Liu, Wang, Zhang et al. (2017)] proposed a global and local structure retention framework for feature selection to obtain the best feature. Ma et al. [Ma, Qin, Xiang et al. (2019)] proposed an improved median filtering algorithm based on divide and conquer with good denoising, while the filtering efficiency is low. Ferreira et al. [Ferreira, Rodrigues, Lei et al. (2014)] proposed a secure image encryption algorithm for image retrieval, and processed image color information and texture information respectively. This scheme encrypts the texture information by a random encryption algorithm, and uses the deterministic encryption to protect the color information. The authors use color histograms as image features for image retrieval. Ferreira's scheme greatly reduces the computing burden on users. However, the color histogram does not include the texture information of the image. Liu et al. [Liu, Shen, Xia et al. (2017)] encrypted the image by difference matrix calculation, difference value replacement and difference position scrambling, and proposed an image retrieval scheme based on difference histogram to improve the retrieval accuracy.

In the above method, the image owner outsourcing the encrypted image to cloud server that can provide CBIR services.

Lu et al. [Lu, Swaminathan, Varna et al. (2009)] first proposed a ciphertext image retrieval scheme in 2009. The scheme extracts local features from the image datasets, which uses the clustering method to generate a visual word. Xia et al. [Xia, Zhu, Sun et al. (2018)] proposed a proprietary CBIR scheme based on local features and earth mobile distance (EMD). Linear transformation is used to protect sensitive information in EMD computation. In 2017, Xia et al. [Xia, Xiong, Vasilakos et al. (2017)] proposed the image with two MPEG descriptors and protected the image features through the secure k-nearest neighbor (KNN) algorithm. The proposed scheme uses the local sensitive hash to improve search efficiency. Li et al. [Li, Qin, Xiang et al. (2018)] proposed a Harris image matching method combining adaptive threshold and random sample consensus (RANSAC) for explosive image feature extraction, which improved the matching accuracy and saved the retrieval time. Shen et al. [Shen, Cheng, Zhu et al. (2018)] proposed a content-based multi-source encrypted image retrieval scheme. Xiang et al. [Xiang, Shen, Qin et al. (2019)] proposed the discrete multi-view hash to integrate multiple views and reduce the distortion errors in the quantization stage. But the retrieval precision applied to large-scale image is low. In 2019, Qin et al. [Qin, Li, Xiang et al. (2019)] improved Harris algorithm with LSH to build indexes to achieve encrypted retrieval. All the above-mentioned are representative outsourcing CBIR schemes.

However, these methods have common weaknesses: large data size, complex computational overhead, namely, image feature extraction and index construction are extremely time-consuming. In this paper, we propose a SimHash encryption image retrieval scheme with high retrieval accuracy and low storage overhead.

2 Related work

(1) Bag-of-words model (BOW): In CBIR, BOW model is used to describe the local descriptors of the area around the key points detected in the image. The 128-dimensional SIFT local feature descriptors have been proved to be a good feature to represent the key information of the image. However, if the SIFT local feature descriptors of the whole image are extracted, a lot of information will be generated. It becomes time-consuming when the query image searches for datasets. Therefore, the number of descriptors can be significantly reduced by quantifying local descriptors into "visual words". By this manner, each image can be regarded as a long and sparse vector of words.

(2) SimHash: SimHash is a "locally sensitive" hash method used to detect approximately duplicate documents [Buyrukbilen and Bakiras (2014)]. First, each document content corresponds to a signature S with a length of f initialized to 0, and the vector V with a dimension of f initialized to 0. Secondly, the document content is segmented by word segmentation datasets, and the redundant information is filtered out to transform the document content into a set of Feature words. The Weight of feature words is the frequency of the feature words appearing in the document. The Hash function is then used to map all the features to a signed Hash of length f, and each Hash bit is traversed. If the i-th bit of Hash is $1, 1 \leq \mathrm{i} \leq f$, the i-th bit of V is added to the weight of the feature, otherwise minus. Finally, V is traversed. If the i-th bit of $V > 0$, then i-th bit of Sign is 1; otherwise, it is 0. The resulting signature Sign is the SimHash signature for the document content.

3 Encryption image retrieval method based on SimHash

In the cloud computing, image retrieval based on SimHash is consisted of the data owner, query user and cloud server. The overall framework of the system is explained as follow.

3.1 System model

In Fig. 1, the system model overview of the proposed framework. The data owner should store the image set $\mathrm{M} = \{m_1, m_2, \cdots, m_N\}$ to the cloud server. In order to ensure the security of these data, encryption algorithm should be used to encrypt the image set M into ciphertext form before uploading. To enable query users to realize ciphertext retrieval, features extracted from image set M need to be clustered to generate visual word set $\mathrm{V} = \{v_1, v_2, \cdots, v_k\}$. Secondly, the key word fingerprint generation algorithm based on SimHash was used to generate the visual word fingerprint of each visual word $v_i \in V$, and then index I was constructed through the fingerprint. Finally, the encrypted image set and index I were jointly uploaded to cloud server.

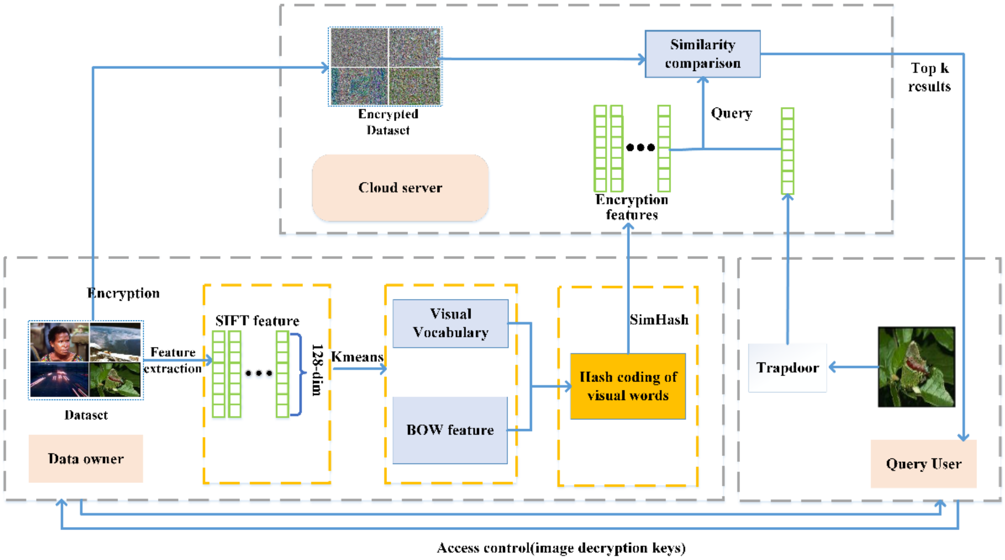

Figure 1: System model

Query users are authorized users to access the image datasets. Query users hope to efficiently search similar images to the query images by using the CBIR service in cloud server. To ensure the security of query image, the image trapdoor should be built before uploading to the cloud server. In our method, query users use the authorization key to extract the features of the query image and the trapdoor construction, then uploads the trapdoor to cloud server.

Cloud server needs to extract the features of query images, construct query trapdoor Q, similarity search and sort the results. The cloud server returns the most relevant top-k ciphertext images. Finally, the authorized query user decrypts the ciphertext image by the key.

3.2 Overview of the method

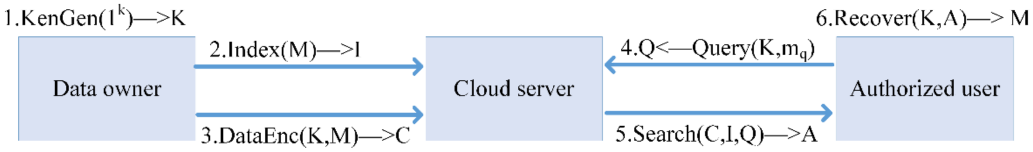

Figure 2: Pipeline of the proposed method

The search method based on SimHash is shown in Fig. 2. The main process of each algorithm is given here will be explained in detail:

(1) KenGen (*1^k*)→*K* is the key generation algorithm. The algorithm inputs the security parameter *k* and returns the key groups *K*.

(2) Index (M)→I is the feature encryption algorithm, which inputs key set *K* and image datasets M and outputs secure and searchable encryption features. In our method, the searchable feature encryption algorithm based on SimHash is proposed to search the

ciphertext image while privacy-preserving of the images. The algorithm includes feature extraction, codebook construction, searchable feature encryption, and other processes.

(3) $\mathrm{DataEnc}\,(K, \mathrm{M}) \rightarrow C$ is the image dataset encryption algorithm, which inputs the secret key K and image dataset M, and outputs the encryption image datasets C. The data owner uses the key K to encrypt the image datasets M and obtains the encryption image datasets C. The data owner sends the C, encryption signature datasets and secure searchable index to cloud service. The authorized query user searched similar encryption images from cloud server. To accomplish this, the data owner needs to authorize the key K to the query user.

(4) $Q \leftarrow \mathrm{Query}\,(K, m_q)$ is the search generation algorithm, which inputs the key set K, query image m_q, and outputs the transformed security search request.

(5) $\mathrm{Search}\,(C, I, Q) \rightarrow \mathrm{A}$ is the search algorithm, which inputs encryption image datasets C, security search index I, query request Q, outputs encryption image results set A. After receiving the search trapdoor Q sent by the authorized query user, the cloud service can calculate the hamming distance between trapdoor Q and index I. By the sorting of hamming distance, top-k encryption images are returned to the query user.

(6) $\mathrm{Recover}\,(K, \mathrm{A}) \rightarrow \mathrm{M}$ is the decryption algorithm, the algorithm inputs the key groups K, encryption image results set A, then outputs image result set M.

3.3 Encryption image retrieval algorithm based on SimHash

As can be seen from Fig. 1, the encryption image retrieval based on SimHash includes features extraction, visual words and codebook generation, visual word hash encoding, index construction of these steps, which are described as follows.

3.3.1 Feature extraction

SIFT is an effective image feature extraction method, which has strong robustness to image brightness change, deformation, scaling, rotation, and affine transformation. Based on these advantages, this paper extracts SIFT features for experiments.

3.3.2 Visual word and codebook generation

To facilitate image search of the SimHash, this section extracts visual words and codes to describe images through clustering SIFT features by *k*-means. The details are as follows:

(1) Partial image $\mathrm{T} = \{t_1, t_2, \cdots, t_n\}$ is selected from the image datasets $\mathrm{M} = \{m_1, m_2, \cdots, m_N\}$ as the training set, where N is the number of image datasets, n is the number of the training set, $n \leq N$.

(2) SIFT features $\mathrm{F} = \{f_1, f_2, \cdots, f_z\}$ of all images in training set T are extracted, where z is the number of SIFT features.

(3) Visual dictionary $\mathrm{V}=\{v_1, v_2, \cdots, v_q\}$ is derived from K-mean clustering SIFT feature, where q is the number of visual words, $v_i \in R^d$ is the column vector of d dimension, $1 \leq \mathrm{i} \leq q$. The visual dictionary is generated as shown in Algorithm 1.

(4) Calculate the distance from SIFT feature to the visual words q, and map it to the visual words (the word frequency of the visual word increases by 1). Thus, the image

can be represented by a q-dimension vector, and the BoW feature codebook is $L = \{l_1, l, \cdots, l_N\}$.

Algorithm 1: Visual dictionary generation algorithm

```
Input: Feature set $F$
Output: Visual dictionary $V$
Step 1: $q \in F$ SIFT features were randomly selected as the initial cluster center $u_i$, $1 \leq i \leq q$.
Step 2: SIFT features are allocated to any $u_i$ by the Euclidean distance, so all SIFT features form $q$ clusters. Calculate the mean value of each cluster and take the mean value as the new cluster center. Calculate the sum of error squares of each cluster, and then get the sum of error squares of $q$ clusters.
Step 3: Repeat Step 2 until the total sum of squared errors is less than the threshold, and the clustering center $u_i$ of $q$ clusters is used as the visual dictionary $V$.
```

3.3.3 Hash coding of visual words

In SimHash text retrieval method, feature words are mapped into signatures by the hash function, while in this paper, visual words generated by k-means clustering are hashed. The detailed description is as follows:

Calculate the locally sensitive hash code $\mathcal{L}_i$ for each visual word v_i, where $\mathcal{L}_i \in \{-1,1\}^k$, and k is the total number of encoding bits. k d-dimension column vectors r_j are randomly generated from the Gaussian distribution, where $r_j \in R^d$, $1 \leq \mathrm{j} \leq k$, and each bit of $\mathcal{L}_i$ is calculated by Eq. (1).

$$\mathcal{L}_{ij} = \begin{cases} -1 & r_j^T \bullet v_i < 0 \\ 1 & other \end{cases} \tag{1}$$

$\mathcal{L}_{ij}$ is the j-th bit of $\mathcal{L}_i$, $1 \leq \mathrm{j} \leq k$.

3.3.4 Searchable encryption feature algorithm based on SimHash

The existing encryption retrieval method needs to extract features from the image datasets, construct the search index and encrypt the search index, and image matching by the encryption search index. In this paper, the searchable encryption feature is generated by Simhash visual words, and then the generated searchable encryption feature is used for similarity comparison.

The weight W_i of each code word in the image codebook is calculated by using $TF\!-IDF_i$ (term frequency-inverse document frequency). Calculate as Eq. (2).

$$W_i = TF \bullet IDF_i \tag{2}$$

where $1 \leq \mathrm{i} \leq q$, TF_i is the word frequency of visual words v_i in the image m_i codebook, IDF_i is the inverse document frequency of visual words v_i in the BoW codebook L, in Eq. (3).

$$IDF_i = lg\frac{n}{n_i} \tag{3}$$

where $1 \leq \mathrm{i} \leq q$, n is the number of the training set, n_i is the number of images containing visual words v_i, and lg is the logarithm calculated at the base of 10.
The image local similar hash encoding method based on SimHash is implemented by Eq. (4).

$$H(m_t,j) = sign(\sum_{i=1}^{q} \mathcal{L}_{ij} W_i) \tag{4}$$

where $1 \leq \mathrm{i} \leq N$, $H(m_t,j)$ is the j-th bit of $H(m_t)$, m_t is the t-th image in the datasets M. The sign function satisfies the following properties:

$$\mathrm{sign(x)} = \begin{cases} 0 & \mathrm{x} < 0 \\ 1 & \mathrm{other} \end{cases} \tag{5}$$

Hash encoding of the image is performed by Algorithm 2:

Algorithm 2: Searchable Encryption Feature Algorithm Based on SimHash

```
Input: Locally sensitive hash code $\mathcal{L}_i$ for visual words $v_i$, codebook $L$.
Output: Hash code $H(m_t)$ of the image.
Step 1: The word frequency $TF_t$ of each visual word is calculated by the codebook $l_t$
        of image, $1 \leq t \leq q$.
Step 2: Calculate the $IDF_t$ of each visual word in the image codebook $L$ by Eq. (3).
Step 3: Calculate the weight $W_t$ of each visual word in the image codebook $L$ by Eq. (2).
Step 4: Calculate each hash code $H(m_t,j)$ of the image $m_t$ in datasets by Eq. (4).
Step 5: Repeat Step 4 until the hash code $H(m_t)$ for the image is $H(m_t)$.
```

3.3.5 Encryption image retrieval based on SimHash

The encryption feature generated by SimHash is binary vector, so hamming distance between the query image and all the images in the dataset is calculated. The smaller the hamming distance, the similar the image.

4 Experimental results and analysis

In this section, we demonstrate the experimental results of the proposed method on two public datasets and compare it with two state-of-the-art encryption image retrieval. The experiments are conducted with Acer's E1-571G notebook computer, Windows 10, Intel(R)Core(TM)i5-Intel 3230 M CPU @2.60 GHz, 12 G RAM, MatlabR2014a. The image data set used in the experiment is the Corel 1000 datasets and the Corel10k datasets, including 10 classes of images and 100 classes of images respectively, and each class has 100 similar images.

4.1 Retrieval accuracy

In order to evaluate the search precision of our method, precision was adopted as the performance measurement. The precision is defined as $\mathrm{R} = \check{N}/N$, where N represents the number of images in the datastes that are similar to the query image, and $\check{N}$ denotes the number of similar images in the first N images of the search results.

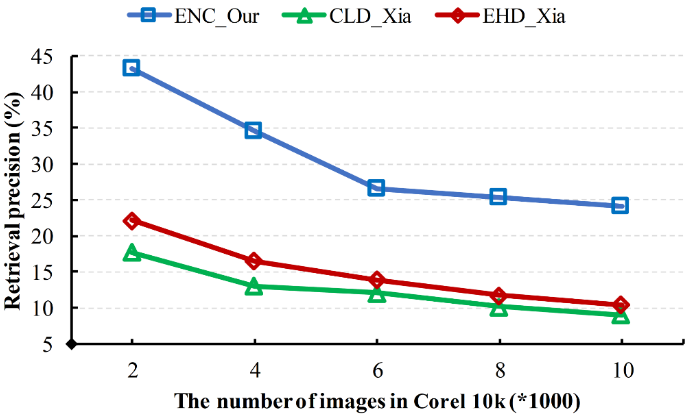

Figure 3: Comparison of the average retrieval precision with [Xia] on Corel10k

The retrieval precision of Corel10k datasets is shown in Fig. 3. ENC_Our represents our method, and EHD_Xia and CLD_Xia denote the method [Xia, Xiong, Vasilakos et al. (2017)]. It can be seen that our method is feasible and effective, and the retrieval precision increases 43.28% in top-20.

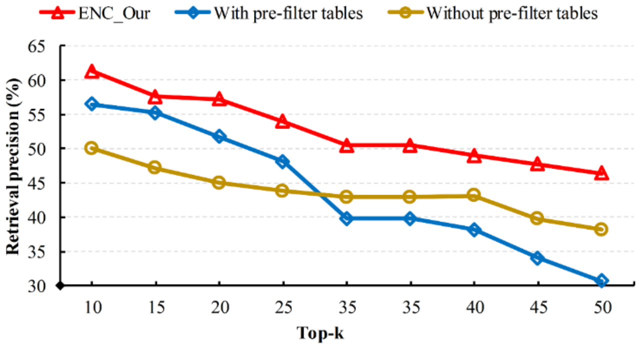

Figure 4: Comparison of the average retrieval precision with [Xia] on Corel1000

The retrieval precision of Corel 1000 datasets is shown in Fig. 4. ENC Our represents our method, and with pre-filter tables and without pre-filter tables denote the method [Xia, Zhu, Sun et al. (2018)]. It can be seen that the retrieval precision of the encryption image retrieval method proposed in this paper increases to 61.27% in top-10.

4.2 Search efficiency

Retrieval efficiency and system storage consumption are also important evaluation indicators for measuring a retrieval system. Based on this, this paper conducts experiments on retrieval time consumption and index storage consumption.

4.2.1 Time consumption of the search

The CBIR service is performed by the cloud server, which needs to calculate the hamming distance between the image datasets and the query image, and return the most similar k images to the authorized query user. Therefore, the time complexity of the SimHash-based encryption image retrieval scheme is $O(n)$. In Tab. 1, the retrieval time of our method is almost linear. Compared with the retrieval time of hashed pre-filtered table by Xia as an index, our method consumes less retrieval time when the datasets exceed 8k, which is more advantageous for large scale image datasets and retrieval time.

Table 1: Comparison of the retrieval time consumption with [Xia]

Method	2k	4k	6k	8k	10k
CLD_Xia	3.32	5.73	8.26	11.17	14.14
EHD_Xia	3.73	6.70	10.22	14.86	16.79
ENC_Our	**10.24**	**13.33**	**14.39**	**15.08**	**15.97**

4.2.2 Storage consumption of the index

In Tab. 2, the encryption feature of SimHash used in this paper and the storage cost of building indexes in Xia et al. [Xia, Xiong, Vasilakos et al. (2017)]. In our method, only one corresponding SimHash fingerprint is generated for each image. Through comparison, it is found that the index of [Xia, Xiong, Vasilakos et al. (2017)] scheme requires more storage space.

Table 2: Comparison of the index storage consumption with [Xia] on Corel 10k

Method	2k	4k	6k	8k	10k
CLD_Xia	712 kb	1410 kb	2110 kb	2810 kb	3520 kb
EHD_Xia	332 kb	667 kb	999 kb	1300 kb	1630 kb
ENC_Our	**1.8 kb**	**2.74 kb**	**3.54 kb**	**4.36 kb**	**5.21 kb**

It is shown in Fig. 3 that the encryption features of SimHash used in this paper and the storage overhead of using pre-filtered tables as indexes in Xia et al. [Xia, Zhu, Sun et al. (2018)]. By comparison, we can see that the storage consumption in this paper is far lower than that in the method [Xia, Zhu, Sun et al. (2018)], and the storage consumption in this paper can be negligible.

Table 3: Comparison of the index storage consumption with [Xia] on Corel 1000.

Method	200	400	600	800	1000
SIFT_Xia	356 kb	714 kb	1072 kb	1431 kb	1789 kb
ENC_Our	**0.48 kb**	**0.62 kb**	**0.73 kb**	**0.87 kb**	**1 kb**

5 Conclusion

By the existing encryption retrieval technology, this paper proposes an encryption image retrieval scheme based on SimHash to improve the retrieval accuracy and optimize the system performance. Specifically, visual words and image vectors are generated by BoW model, and then the visual words are hashed to generate the searchable encryption features by using SimHash. Finally, the image similarity is retrieved through searchable encryption features. And we proved that our method not only can improve the retrieval accuracy but also greatly reduce the memory cost of index construction than the state-of-the-art methods by a large number of experiments on public datasets. However, the retrieval time of the method in this paper is relatively large. Therefore, in the future work, we will further explore to optimize the retrieval efficiency.

Acknowledgment: This work is supported by the National Natural Science Foundation of China (No. 61772561), the Key Research & Development Plan of Hunan Province (No.2018NK2012), the Science Research Projects of Hunan Provincial Education Department (Nos. 18A174, 18C0262), the Science & Technology Innovation Platform and Talent Plan of Hunan Province (2017TP1022), and this work is implemented at the 2011 Collaborative Innovation Center for Development and Utilization of Finance and Economics Big Data Property, Universities of Hunan Province, Open project (No. 20181901CRP04).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Bellafqira, R.; Coatrieux, G.; Bouslimi, D.; Quellec, G. (2015): Content-based image retrieval in homomorphic encryption domain. *Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 2944-2947.

Bellafqira, R.; Coatrieux, G.; Bouslimi, D.; Quellec, G. (2016): An end to end secure CBIR over encrypted medical database. *Engineering in Medicine & Biology Society*, pp. 2537-2540.

Buyrukbilen, S.; Bakiras, S. (2014): Secure similar document detection with simhash. *Processdings of the 10th Very Larger Data Bases Workshop*, pp. 61-75.

Ferreira, B.; Rodrigues, J.; Leitao, J.; Domingos, H. (2014): Practical privacy-preserving content-based retrieval in cloud image repositories. *IEEE Transactions on Cloud Computing*, vol. 13, no. 9, pp. 1-14.

Hsu, C. Y.; Lu, C. S.; Pei, S. C. (2012): Image feature extraction in encrypted domain with privacy-preserving SIFT. *IEEE Transactions on Image Processing*, vol. 21, no. 11, pp. 4593-4607.

Li, H.; Qin, J. H.; Xiang, X. Y.; Pan, L. L.; Ma, W. T. et al. (2018): An efficient image matching algorithm based on adaptive threshold and RANSAC. *IEEE Access*, vol. 6, no. 1, pp. 66963-66971.

Liu, D. D.; Shen, J.; Xia, Z. H.; Sun, X. M. (2017): A content-based image retrieval scheme using an encrypted difference histogram in cloud computing. *Information*, vol. 8, no. 3, pp. 96.

Liu, X. W.; Wang, L.; Zhang, J.; Yin, J. P.; Liu, H. (2017): Global and local structure preservation for feature selection. *IEEE Transactions on Neural Networks and Learning Systems*, vol. 25, no. 6, pp. 1083-1095.

Lu, W. J.; Swaminathan, A.; Varna, A. L.; Wu, M. (2009): Enabling search over encrypted multimedia databases. *Media Forensics and Security*, pp. 1-11.

Ma, W. T.; Qin, J. H.; Xiang, X. Y.; Tan, Y.; Lou, Y. J. et al. (2019): Adaptive median filtering algorithm based on divide and conquer and its application in CAPTCHA recognition. *Computers, Materials & Continua*, vol. 58, no. 3, pp. 665-677.

Qin, J. H.; Li, H.; Xiang, X. Y.; Tan, Y.; Pan, W. Y. et al. (2019). An encrypted image retrieval method based on harris corner optimization and LSH in cloud computing. *IEEE Access*, vol. 7, no. 1, pp. 24626-24633.

Shen, M.; Cheng, G. H.; Zhu, L. H.; Du, X. J.; Hu, J. K. (2018): Content-based multi-source encrypted image retrieval in clouds with privacy preservation. *Future Generation Computer Systems*.

Vaquero, L. M.; Roderomerino, L.; Caceres, J.; Lindner, M. (2008): A break in the clouds: towards a cloud definition. *ACM Sigcomm Computer Communication Review*, vol. 39, no. 1, pp. 50-55.

Wang, B. W.; Gu, X. D.; Ma, L.; Yan, S. S. (2017): Temperature error correction based on bp neural network in meteorological wireless sensor network. *International Journal of Sensor Networks*, vol. 23, no. 4, pp. 265-278.

Xia, Z. H.; Xiong, N. N.; Vasilakos, A. V.; Sun, X. M. (2017): EPCBIR: an efficient and privacy-preserving content-based image retrieval scheme in cloud computing. *Information Sciences*, vol. 387, no. 2017, pp. 195-204.

Xia, Z. H.; Zhu, Y.; Sun, X. M.; Qin, Z. (2018): Towards privacy-preserving content-based image retrieval in cloud computing. *IEEE Transactions on Cloud Computing*, vol. 96, no. 13, pp. 276-286.

Xiang, L. Y.; Shen, X. B.; Qin, J. H.; Hao, W. (2019): Discrete multi-graph hashing for large-scale visual search. *Neural Processing Letters*, vol. 49, no. 3, pp. 1055-1069.

Zhang, X. F.; Liu, W.; Dunder, M.; Badve, S.; Zhang, S. (2015): Towards large-scale histopathological image analysis: hashing-based image retrieval. *IEEE Transactions on Medical Imaging*, vol. 34, no. 2, pp. 496-506.