 CMC, vol.58, no.1, pp.27-43, 2019

A Privacy-Preserving Image Retrieval Based on AC-Coefficients and Color Histograms in Cloud Environment

Zhihua Xia[1, *], Lihua Lu[1], Tong Qiu[1], H. J. Shim[1], Xianyi Chen[1] and Byeungwoo Jeon[2]

Abstract: Content based image retrieval (CBIR) techniques have been widely deployed in many applications for seeking the abundant information existed in images. Due to large amounts of storage and computational requirements of CBIR, outsourcing image search work to the cloud provider becomes a very attractive option for many owners with small devices. However, owing to the private content contained in images, directly outsourcing retrieval work to the cloud provider apparently bring about privacy problem, so the images should be protected carefully before outsourcing. This paper presents a secure retrieval scheme for the encrypted images in the YUV color space. With this scheme, the discrete cosine transform (DCT) is performed on the Y component. The resulting DC coefficients are encrypted with stream cipher technology and the resulting AC coefficients as well as other two color components are encrypted with value permutation and position scrambling. Then the image owner transmits the encrypted images to the cloud server. When receiving a query trapdoor form on query user, the server extracts AC-coefficients histogram from the encrypted Y component and extracts two color histograms from the other two color components. The similarity between query trapdoor and database image is measured by calculating the Manhattan distance of their respective histograms. Finally, the encrypted images closest to the query image are returned to the query user.

Keywords: Image retrieval, AC-coefficients histogram, color histogram, discrete cosine transform.

1 Introduction

With the rapid development of digital devices, a large number of images are generated and shared. Image data contain rich information and they have been explored in many fields, such as feature extraction [Hu, Wang, Wang et al. (2016)], information hiding [Cao, Zhou, Sun et al. (2018)] and image retrieval [Zhang, Liu, Dundar et al. (2015); Cavallaro, Lagendijk, Erkin et al. (2017)]. Searching an intended image from a huge dataset has raised increasing attention, and many advanced retrieval technologies have

[1] Jiangsu Engineering Centre of Network Monitoring, Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing, 210044, China.

[2] College of Information & Communication Engineering, Sungkyunkwan University, Korea.

[*] Corresponding Author: Zhihua Xia. Email: xia_zhihua@163.com.

been proposed [Liu, Shen, Xia et al. (2007); Akgül, Rubin, Napel et al. (2011); Abdulsada, li, Abdulabbat et al. (2013); Xia, Zhu, Sun et al. (2015)]. Nevertheless, huge storage space and complex computation requirements are needed to search one particular image from a large amount of images, which is almost impossible for users with lightweight devices (e.g. smart phones), so outsourcing image data to the cloud storage providers becomes one of the most convenient options because they provides enormous storage space and powerful computing ability.

However, outsourcing the image data with sensitive information (such as financial position, personal identification and healthy records) to the server often results in great challenges in terms of data control and privacy. To prevent unauthorized access, the image owners usually encrypt their image data before its transmission to the server, but the conventional encryption operations pose a threat to image retrieval. For effectively utilizing and managing image resources, the researchers have made great efforts and they have proposed many practical retrieval schemes in this field [Reynolds (2016); Parikesit (2017); Cui, Zhang, Cai et al. (2018); Cai, Wang, Zheng et al. (2013)]. In original scenarios [Rui, Huang, Ortega et al. (1998); Xia, Xiong, Vasilakos et al. (2017); Weng, Amsaled and Furon (2016); Xia, Wang, Zhang et al. (2017)], the image owners not only complete the task of index construction and encryption, but transmit the encrypted index to the server as well. Once receiving the query trapdoors, the server retrieves the intended images and returns them to the query users. These schemes provides feasible solutions and realize secure image retrieval in the encrypted domain, but the computation burden of index generation and encryption in the image client is really too heavy. To reduce the workload of image client and effectively implement retrieval work, some content-based image retrieval (CBIR) schemes have been put forward [Cheng, Wang, Wang et al. (2017); Xia, Xiong, Vasilakos et al. (2017); Cheng, Zhang, Yu et al. (2016)]. In this paper, we propose a secure retrieval scheme for encrypted images based on the combination of AC-coefficients and color histograms. The main contributions are as follows:

(1) In our scheme, the image owner only needs to encrypt the database images. The index construction and image retrieval work will be done by the cloud server.

(2) We propose to use the combination of AC-coefficients and color histograms for image retrieval in the encrypted domain. The search result shows that the combination of AC-coefficients and color histograms achieves better retrieval accuracy than either of them alone in the YUV color space.

The rest of our paper is organized as follows. In Section 2, we briefly review the methods of image encryption and index generation in previous woks. In Section 3, we introduce the design of our system model and security model. In Section 4, we describe the process of image encryption and index generation in proposed scheme. The Section 5 and Section 6 show the security analysis and retrieval performance respectively. In the final section, we draw a conclusion.

2 Related works

Previous searchable encryption schemes have more concentrated on retrieving text documents in the encrypted domain [Wang, Cao, Ren et al. (2012); Fu, Huang, Ren et al.

(2017)], where a data owner outsources text document to its server and is able to retrieve desired document with keyword search. Song et al. [Song, Wagner and Perrig (2000)] proposed the first retrieval scheme in data encryption, where the encryption and retrieval work is performed on a word-by-word basis, but this scheme is not efficient enough because of no-index mechanism. To improve efficiency, Curtmola et al. [Curtmola, Garay, Kamara et al. (2006)] constructed a secure reversed index for the encrypted text documents, where the computing cost is proportional to the amount of documents. They presented two encryption schemes, the first scheme is secure for the selective key attack, and the other scheme is secure for the dynamic selective key attack. Afterwards, the researchers improved the functions of encrypted algorithms for designing practical schemes, such as supporting fuzzy keyword search [Fu, Wu, Guan et al. (2017)], multi-keyword sorted search [Fu, Sun, Linge et al. (2014)] and dynamic search [Xia, Wang, Sun et al. (2016)].

An exploring work of image retrieval in the encrypted domain has attracted much attention, which aims at executing retrieval work on the server while ensuring images to be handled secretly. Lu et al. [Lu, Swaminathan, Varna et al. (2009)] proposed the solutions to realize image retrieval in the encrypted domain for the first time. They introduced two secure indexing schemes, in which the information of word frequency distribution is protected by order preserving encryption and Min-hash. In another work [Lu, Varna, Swaminathan et al. (2009)], they employed signal processing and cryptographic techniques to achieve secure distance calculation without divulging image content. They have compared three encryption algorithms, including plane randomization, random projection and randomized unary encoding. Their experimental results show that the first two algorithms support the ordered computation of Hamming distance and the third algorithm supports the approximate computation of L1 distance. Lu et al. [Lu, Varna and Wu (2014)] compared the homomorphic encryption with the proposed encryption scheme of work [Lu, Varna, Swaminathan et al. (2009)] in terms of retrieval accuracy, retrieval efficiency and storage overhead. The experimental results show that the homomorphic encryption is not advantageous in these aspects. In Abdulsada et al. [Abdulsada, Ali, Abdulabbat et al. (2013); Yuan, Wang, Wang et al. (2014); Yuan, Yu and Guo (2015)], tree index and local sensitive hashing (LSH) method are used to reduce retrieval time. In Abdulsada et al. [Abdulsada, Ali, Hashim et al. (2013)], Abdulsada et al. established a searchable index by using LSH method. Images are protected by using the advanced encryption standard (AES) encryption method and image feature is protected by a reversible matrix. In order to improve the retrieval efficiency further, Yuan et al. [Yuan, Wang, Wang et al. (2014)] proposed to combine LSH and Cuckoo hash to get faster and more efficient similarity search. Image features are extracted by using the Bag-of-words (BOW) model to generate visual word vectors. The image is protected by the encryption method based on attribute encryption, and its hash value is protected by a one-way function. In Yuan et al. [Yuan, Yu and Guo (2015)], secure k-nearest neighbors (kNN) algorithm is used to realize secure image retrieval and a tree index is constructed to improve search efficiency. In addition, Xia et al. [Xia, Zhu, Sun et al. (2013)] proposed a secure image retrieval scheme which uses invertible matrix to protect image feature vectors and achieves the order preserving calculation of Euclidean distance. Abduljabbar et al. [Abduljabbar, Jin, Ibrahim et al. (2017)] extracted local speeded up robust features

(SURF) to represent image feature and AES technology is used to protect images in the database. The similarity between query image and database image is measured by calculating the Euclidean distance of their responding feature vectors.

Although the previous outsourced CBIR schemes solve the privacy problem, the computational workload on user is still heavy, since it is image owner's task to deal with feature extraction and index generation that require numerous resources. Moreover, a large amount of computing resources and the problem of cipher expansion make homomorphic encryption impractical [Bellafqira, Coatrieux, Bouslimi et al. (2015); Zhang, Jung, Liu et al. (2017)]. A lot of work has been proposed to solve above problems. Cheng et al. [Cheng, Zhang, Yu et al. (2016)] introduced an encrypted JPEG image retrieval scheme using block feature comparison. AC-coefficient histogram in a block is used to form a local feature descriptor, and AC coefficients as well as DC coefficients are encrypted with permutation encryption and stream encryption respectively. The similarity between query image and database image is measured by comparing the distance of their corresponding local features. Cheng et al. [Cheng, Zhang, Yu et al. (2015)] proposed a retrieval scheme based on Markov process. The scheme uses stream cipher to encrypt coded data, and extracts Markov features from the encrypted data directly. The similarity between query image and database image is measured by calculating the distance of their corresponding Markov features. Bernardo et al. [Ferreira, Rodrigues, Leitao et al. (2017)] proposed an encrypted content-based image retrieval scheme. In this scheme, color information is protected by random permutation encryption and the rows and columns are disorganized to preserve texture information of images. Liu et al. [Liu, Shen, Xia et al. (2017)] proposed an image retrieval scheme based on difference histogram. In their scheme, two kinds of difference matrices (order difference and random order difference) are proposed, and the value replacement and location scrambling are utilized to encrypt the difference matrix. The difference histogram is extracted as image features by the server.

In the above schemes, the cloud server undertakes the workload of feature extraction and image search, so the image owners only need to encrypt images. Inspired by those outsourced CBIR schemes, we propose a secure retrieval scheme with the combination of AC-coefficients and color histograms in the encrypted domain. The retrieval result shows that the combination of them outperforms individual utilization, and our retrieval accuracy is six percent higher than the proposed scheme in Liu et al. [Liu, Shen, Xia et al. (2017)].

3 Program design and security model

3.1 System model

Our scheme mainly consists of three entities, i.e. the image owner, query user and cloud server, as shown in Fig. 1. The following are the assigned tasks of these three entities.

Image owner: The image owner possesses a huge image dataset including large numbers of images, and the dataset is denoted as $\mathcal{I} = \{I_i\}_{i=1}^{n}$ with a corresponding identity number set $\mathcal{ID} = \{ID_i\}_{i=1}^{n}$. The image owner outsources the images to the server for cost saving and flexible utilization, and the outsourced images are encrypted to prevent the disclosure of privacy. The generated encrypted image set is denoted as $\mathcal{C} = \{C_i\}_{i=1}^{n}$. The image owner only needs to encrypt images and upload encrypted images to the server.

Cloud server: The server stores the encrypted images from the image owner and undertakes the task of index generation and image search. Once receiving a search request, the server finds the most similar encrypted images from the encrypted image database and returns them to the query user.

Query user: The query user wants to search the intended image from the encrypted image database. In order to protect the query image, the query user encrypts the query image to generate a query trapdoor and transmits the trapdoor to the server. The encryption process of query image is consistent with the database images'.

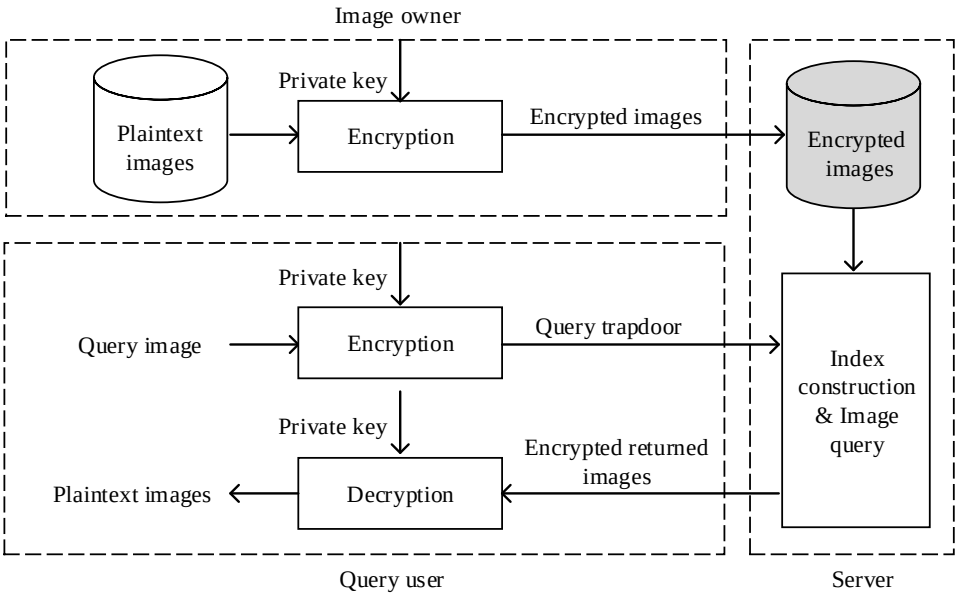


Figure 1: System model

3.2 Security models and assumptions

As pointed out in the previous works [Kuzu, Islam and Kantarcioglu (2012); Ferreira, Rodrigues, Leitao (2017)], we believe that the cloud server is an honest but curious one. In other words, the server can accomplish tasks in accordance with the protocol, but it may analyze and speculate about the image data. In our scheme, the query users are believed to be trustworthy, so they will not disclose any private information of the images to the server during their communication process. The images to which the cloud has access are the encrypted ones, and the security strength of the encrypted images will be discussed in the Section 5.

4 The proposed scheme

4.1 Discrete cosine transform (DCT)

Discrete cosine transform is an efficient transform which presents the texture information of an image in frequency domain. Typically, DCT is performed for each 8×8 size sub-block. For an image with the size of $M \times N$, the value $f(i,j)$ represents the pixel value at

the position (i, j) in the original image block. The transformation process can be formulated as:

$$A(u,v) = c(u)c(v)\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} f(i,j)\, cos\left[\frac{(i+0.5)\pi u}{M}\right] cos\left[\frac{(j+0.5)\pi v}{N}\right] \quad (1)$$

where $A(u,v)$ is the DCT coefficient at position (u,v), $c(u) = \begin{cases}\sqrt{\frac{1}{M}}, u = 0\\ \sqrt{\frac{2}{M}}, u \neq 0\end{cases}, c(v) = \begin{cases}\sqrt{\frac{1}{N}}, v = 0\\ \sqrt{\frac{2}{N}}, v \neq 0\end{cases}$, and $u = 0,1,\cdots,M-1, v = 0,1,\cdots,N-1$. The resulting $A(u,v)$ denotes DC coefficient when $u = 0$ and $v = 0$, and the resulting $A(u,v)$ denotes AC coefficient when $u \neq 0$ and $v \neq 0$.

Each DCT sub-block consists of one DC coefficient and 63 AC coefficients. The DC coefficient is the average energy value of sub-block and contains main content of sub-block. The remaining AC coefficients can be divided into three different categories according to their frequency. Most of energy in each block is concentrated in low frequency and middle frequency coefficients (i.e. in the upper left corner of the block), and most of high frequency coefficients in the lower right corner are equal to zero. The previous study [Fang, Cheng, Lin et al. (2012)] shows that AC coefficients can represent texture information of sub-block. The DC coefficients contain important image information, i.e., its histogram is important statistical information. In the proposed scheme, we do not utilize DC coefficient for image retrieval and encrypt them with the stream encryption technology. However, the AC coefficients contain rich edge and texture information of the image. We extract features from AC coefficients after encryption.

4.2 Quantization and truncation operation

The dynamic range of AC coefficients is one important factor. Our experiment with all database images shows that AC coefficients of Y component can vary in a large range $[-682, 683]$. In order to achieve a certain level of efficiency, we need to truncate the coefficients into a limited range. Accordingly, truncation causes unrecoverable quality degradation and it certainly is a tradeoff between efficiency and quality. In fact, truncation does not influence image recovery much, which will be discussed in Section 6. In the process of AC coefficients encryption, AC coefficients are firstly quantized as:

$$A(u,v) \leftarrow [A(u,v)/Q] \quad (2)$$

where Q is a quantization factor and equal to 1, the symbol $A(u,v)$ denotes one AC coefficient value which locates at (u,v) in an image block of Y component. Quantization causes image information loss, however, the main content of image is trivially influenced.

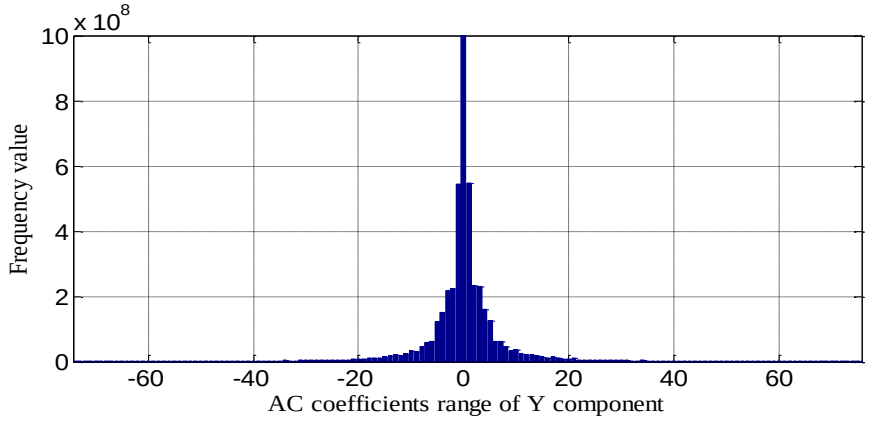


Figure 2: The distribution of AC coefficients in Y component

Although AC coefficients vary in a large range, most of them locate around zero value, as is shown in Fig. 2. From the statistical histogram of AC coefficients, we can observe that AC coefficients are mostly within the range of $[-20, 20]$. For efficiency, we truncate AC coefficients in a small interval $[-d, d]$ without losing a lot of useful information. Tab. 1 presents the percentages of AC coefficients in different ranges, which shows that more than 90% of AC coefficients are contained in a truncated range especially when d is greater than 9. Therefore, the boundary coefficient d is chosen to be greater than 9 in the following experiment. The truncation operation is defined as:

$$A(u,v) \leftarrow trunc_d\big(A(u,v)\big) \tag{3}$$

where if $A(u,v) > d, trunc_d\big(A(u,v)\big) = d$; if $A(u,v) < -d, trunc_d\big(A(u,v)\big) = -d$; if $A(u,v) \in [-d,d]$, $trunc_d\big(A(u,v)\big) = A(u,v)$.

Table 1: The proportions of different range AC-coefficients

Range $[-d, d]$	9	20	40	60	80	100
Proportions (%)	90.77	96.12	98.47	99.22	99.55	99.72

4.3 Image encryption

For encryption, we divide image data into three classes, i.e. DC coefficients in Y component, AC coefficients in Y component, and U and V color components. The encryption process is shown in Fig. 3. Above all, the discrete cosine transform is performed on the Y component, and the AC coefficients are quantized and truncated. Then, the image owner encrypts AC coefficients with value replacement and position scrambling and encrypts DC coefficients with stream cipher. The U and V color components are encrypted with the same encryption method but different keys as the encryption method of AC coefficients. We denote all keys in the whole encryption process as the symbol $\mathcal{K}$, and $\mathcal{K} = \{k_j,\ key_{AC}, \{key_{val*}\}_{*\in\{U,V\}},\ \{key_{pos*}\}_{*\in\{AC,U,V\}}\}$.

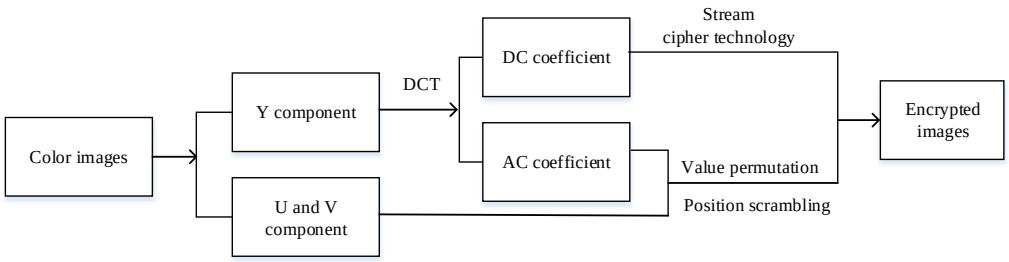


Figure 3: Flow chart of encryption process

4.3.1 Encryption of DC coefficients

First, the DC coefficients of all images are converted to binary numbers. Second, all the binary numbers are combined together to generate a binary stream d_j, where $d_j = (d_1, d_2, \cdots, d_m)$ and m is the length of the binary stream. Lastly, the DC coefficients are encrypted through exclusive or operation as:

$$D' = d_j \oplus k_j \tag{4}$$

where D' denotes the encrypted DC coefficients and the private key $k_j = (k_1, k_2, \cdots, k_m)$ has the same length as d_j.

4.3.2 Encryption of AC coefficients and U and V components

The private key key_{AC} is used to encrypt AC coefficients $A(u, v)$ in the Y component. The value of the private key is in the range of $[-d, d]$. Let $A'(u, v)$ denotes the corresponding encrypted coefficient in the encrypted Y component. The encryption process is described as:

$$A'(u, v) \leftarrow key_{AC}\big(A(u, v)\big) \tag{5}$$

The private key $\{key_{val*}\}_{*\in\{U,V\}}$ is used to encrypt color values in the U and V components. The value of the private key is in the range of $[0, 255]$. We denote one original pixel value as p and the corresponding encrypted pixel value as p'. The encryption process is described as:

$$p'_* \leftarrow key_{val*}(p_*), *\in \{U, V\} \tag{6}$$

The private key $\{key_{pos*}\}_{*\in\{AC,U,V\}}$ is used to scramble the position of AC coefficients and color values. The value of the private key is in the range of $[1, imgsize]$, where the $imgsize$ is the size of the image in the database.

After above two encryption steps, the image owner gets the encrypted image set $\mathcal{C} = \{C_i\}_{i=1}^n$ and sends it together with $\mathcal{ID} = \{ID_i\}_{i=1}^n$ to the server. It is worth noting that the frequency information of each value in the image is not changed after encryption.

4.4 Index generation and search operation

Once receiving the encrypted image set, the cloud server extracts feature vectors from the encrypted images. In our proposed scheme, the server provides index construction and image query services, which greatly reduces computational burden of image owner. The

following describes the index generation and search process.

4.4.1 Index generation

In the YUV color space, U and V channels represent Chrominance information and their AC coefficients provide texture information of a few. Therefore, two different histograms are considered in our scheme, which include the AC-coefficients histogram extracted from Y component and two color histograms extracted from U and V channels. These three histograms are combined into one feature vector to represent the image.

First, AC-coefficients histogram is extracted from Y channel and the range of AC coefficients is $[-d, d]$ as mentioned in Section 4.2. We denote AC-coefficients histogram as F_{AC} and its length as $len_{F_{AC}} = 2d + 1$. Then, the color histogram features are extracted from the encrypted U and V channels and the range of the pixel values is $[0, 255]$. We denote color histograms as $F_{*\{*\in(U,V)\}}$ and its length as $\{ len_{F_*}\}_{*\in(U,V)} = 256$. Finally, the final encrypted feature vector can be expressed as $F_i = \{F_{AC}, F_U, F_V\} = \left(F_{i1}, \cdots, F_{ik}, \cdots, F_{ilen_F}\right)$ and its length is expressed as $len_F = len_{F_{AC}} + len_{F_U} + len_{F_V}$, where $i \in (1,2, \cdots, n)$ and n is the total number of images in the database. In order to achieve better performance of following retrieval work, the cloud server establishes one-to-one mapping relation between the encrypted database image and their corresponding feature vector as shown in Tab. 2.

Table 2: Index construction

Cipher images	Feature vectors
C_1	$F_1 = \left(F_{11}, \cdots, F_{1k}, \cdots, F_{1len_F}\right)$
…	…
C_i	$F_i = \left(F_{i1}, \cdots, F_{ik}, \cdots, F_{ilen_F}\right)$
…	…
C_n	$F_n = \left(F_{n1}, \cdots, F_{nk}, \cdots, F_{nlen_F}\right)$

4.4.2 Search operation

Before sending a query image to the server, the query user needs to encrypt the query image as the image owner does to generate a query trapdoor $\mathcal{Q}$. Once a query trapdoor is received from one query user, the cloud extracts a query image feature from the trapdoor, which is denoted as $Q_f = \left(Q_{f1}, \cdots, Q_{fk}, \cdots, Q_{flen_F}\right)$. The similarity between the encrypted database image and the query image is measured by calculating the Manhattan distance between their respective feature vectors. Finally, the server returns the most similar images to the query user. The Manhattan distance d_{QF} is calculated as:

$$d_{QF_i} = \sum_{k=1}^{len_F} | Q_{fk} - F_{ik} | \tag{7}$$

5 Security analysis

It is well known that the cloud server is an honest-but-curious model. In addition to executing and completing our designated tasks, the cloud server may maliciously analyze

and count the uploaded image data. The security strength of our scheme is analyzed under the cipher-text-only attack (COA) and brute-force attack.

We summarize the functionality $\mathcal{F}$ and corresponding leaked information of proposed scheme under COA model in Fig. 4. In the real environment, the interaction in our scheme involves three kinds of participants, including the image client, cloud server and query user. The honest-but-curious cloud server is considered as a potential attacker $\mathcal{A}$ in our scheme. In the ideal environment, we define a simulator $\mathcal{S}$ that can simulate the information leakages from the view of attacker $\mathcal{A}$ by using the functionality $\mathcal{F}$. Our proposed scheme can be proved secure if the difference of the two environments can be ignored. For security analysis, we expose three kinds of information to the cloud server (i.e. the encrypted images, features and query images). Therefore, the security analysis is performed based on these three aspects. On the basics of the existing encryption algorithms, we can conceive that it is computationally difficult for the server to gain plaintext images without knowing the private keys.

The functionality $\mathcal{F}$ of proposed scheme as well as leaked information.

1. $\mathcal{F}$.StoreImg($\mathcal{I}, \mathcal{ID}, \mathcal{K}$):

· **Functionality.** Image client encrypts all database images in $\mathcal{I}$, and then sends the encrypted image set $\mathcal{C}$ and corresponding identity set $\mathcal{ID}$ to the cloud server.

· **Storage leakage.** The leaked information includes $\mathcal{C}$, $\mathcal{ID}$, each image size and the total number of images.

2. $\mathcal{F}$.Feature ($\mathcal{C}$):

· **Functionality.** Cloud server extracts AC-coefficients and color histograms from each encrypted image in $\mathcal{C}$ as an image feature vector.

· **Feature leakage.** The leaked information includes the encrypted feature vectors, and the similarities between the feature vector and the frequent distribution information of the histogram.

3. $\mathcal{F}$.QueryImg($\mathcal{Q}$):

· **Functionality.** Query user encrypts query image and sends the encrypted query image as a query trapdoor $\mathcal{Q}$ to the cloud server. After completing retrieval work, the server returns the encrypted images closest to the query trapdoor.

· **Query leakage.** The leaked information includes the query trapdoor and similarity between the database image and query trapdoor.

Figure 4: The functionality $\mathcal{F}$ and information leakages in our scheme

5.1 Security of image content

The simulator $\mathcal{S}$ knows the size of image database and each image size in it. Therefore, the simulator $\mathcal{S}$ can simulate a fictitious image database $\mathcal{I}^{\mathcal{S}}$ which resembles the real image database $\mathcal{I}$. However, the simulator $\mathcal{S}$ can only rig the whole image up through many different random sequences. As described in Section 4, the discrete cosine transform is performed in the images, and the resulting DC coefficient is encrypted by the stream cipher technology. Therefore, if the simulator $\mathcal{S}$ wants to obtain the original image,

it needs to solve some random sequences. The simulator $\mathcal{S}$ needs to solve n random sequences for discrete cosine transform and 2^m random sequences for stream cipher technology. The color value and position information is protected by value permutation and position scrambling respectively, and different keys are used in three components. Therefore, the simulator $\mathcal{S}$ needs to solve $(2d+1)! \times (256!)^2$ random sequences for value permutation encryption. The security strength of the position information depends on the size of image, so the security strength of the position information is $(imgsize!)^3$. The key space for database image can be expressed as Sec_{Img}, $Sec_{Img} = 2^m \times n \times (2d+1)! \times (256!)^2 \times (imgsize!)^3$.

5.2 Security of image features

The image features in proposed scheme are the combination of AC-coefficients histograms in the Y component and color histograms in the U and V component. The simulator $\mathcal{S}$ can extract the histograms from the fictitious image database $\mathcal{I}^{\mathcal{S}}$ similarly, and the security strength of image feature depends on the value permutation. The key space for image features can be expressed as $(2d+1)! \times (256!)^2$.

5.3 Security of trapdoor

The encryption method of the query image and database images are same, so the security strength of encrypted image is similar to the encrypted database image. The key space for query image is equal to Sec_{Img}. Apparently, the key space is large enough to withstand the brute-force attack.

6 Experimental results

The scheme is implemented by MatLabR2012b and the experiments are performed on the computer with the Intel Pentium CPU 3.3 GHz and 4 GB memory. The database we use is INRIA Holidays database [Chen and Shi (2008)]. The database is composed of 1491 images which are divided into 500 categories, and the first image in each category is used as a query image. To examine whether the truncation and quantization processes affect the image recovery process or not, we calculate the peak signal to noise ratio (PSNR) values between the original image and recovery image. The PSNR values in Tab. 3 show that the truncation and quantization operation is acceptable and the encrypted images can be restored after decryption.

Table 3: PSNR values in different coefficient ranges

Range $[-d, d]$	20	40	60	80	100
PSNR (dB)	31.6182	33.8712	35.8070	37.5708	39.2274

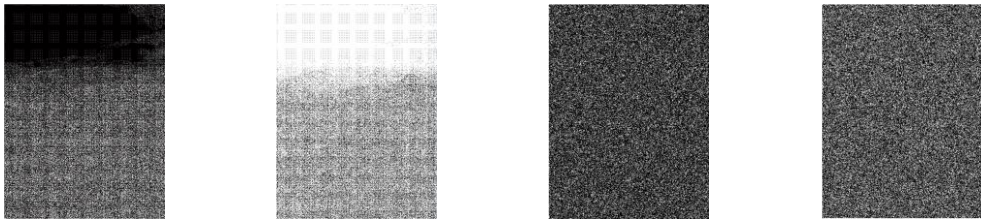
6.1 Encryption effect

We use the first image in the INRIA Holidays database to show our encryption effect. The Fig. 5 shows the original image and the YUV color components of it.

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

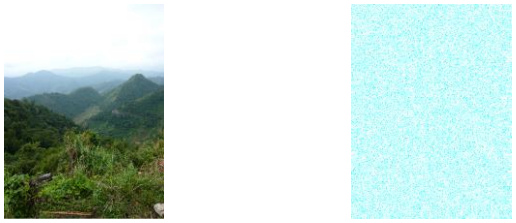
Figure 5: The Y, U and V component of a color image. (a) Original image. (b) Y color component. (c) U color component. (d) V color component

In proposed scheme, the discrete cosine transform is performed on the Y component. The encryption algorithm of U and V components are same as the AC coefficients of Y component, so we take Y component as an example to show the encryption effect presented in Fig. 6. The Fig. 7 shows the original image and its final encrypted form.



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

Figure 6: Encryption effect of Y component. (a) Y component after discrete cosine transform. (b) Value permutation. (c) Position scrambling. (d) Encrypted Y component



(a) (b)

Figure 7: Original image and final encrypted image

6.2 Retrieval accuracy

The mean average precision (mAP) value is used to measure retrieval performance of the proposed scheme. For mAP calculation, the retrieval precision is defined as the number of retrieved relevant images divided by the total number of retrieved images. Similarly, the recall rate is defined as the number of retrieved relevant images divided by the total number of relevant images in the image database. Finally, the mAP value is the mean value between the precision and the recall rate, which solves the single limitation

problem. We use an evaluation package of Inria Holidays Database in python environment to figure out the mAP of our scheme.

6.2.1 Retrieval accuracy in different AC-coefficient ranges

AC coefficients in different intervals are selected to perform experiment as shown in Tab. 4. The best retrieval accuracy is 52.938 when the range of AC coefficient is $[-60, 60]$. We can also observe that the different intervals have no great influence on the retrieval accuracy. The reason is that the coefficient intervals chosen to contain more than 90% of AC coefficients and they can represent most of image information.

Table 4: The mAP in different coefficient ranges

Range $[-d, d]$	20	40	60	80	100
mAP (%)	52.916	52.929	52.938	52.929	52.920

6.2.2 Retrieval accuracy comparison

We have compared the retrieval accuracy of our scheme with Lu's scheme [Lu, Swaminathan, Varna et al. (2009)], Ferreira's scheme [Ferreira, Rodrigues, Leitao et al. (2017)] and Liu's scheme [Liu, Shen, Xia et al. (2017)], the comparison result is shown in Tab. 5. We have realized Ferreira's and Liu's scheme. The image features in Ferreira's scheme are all normalized and then compute the outcome. The mAP in Liu's scheme is calculated through an evaluation package of Inria Holidays Database in python environment. Comparing with previous typical schemes, our scheme can achieve better retrieval performance.

Table 5: Comparison of previous schemes

Schemes	Lu's scheme	Ferreira's scheme	Liu's scheme	our scheme
mAP (%)	49.075	50.383	46.436	52.938

6.2.3 Retrieval accuracies of our schemes

We have also calculated the retrieval accuracies for three different types of feature set and the results are shown in Tab. 6. The first feature set is denoted as AC_YUV. We extract AC-coefficients histograms from YUV color components. Furthermore, we give the retrieval accuracy of AC-coefficients histogram extracted from each component, and those are denoted as AC_Y, AC_U and AC_V. The second feature set is denoted as color_YUV, where color histograms are extracted from YUV color components. The third feature set is denoted as ACCH, where AC-coefficients histogram is extracted from Y component and color histograms are extracted from the other two color components.

Finally, we summarize some observations from above experiments. Tab. 6 shows that the retrieval accuracy of Y component (AC_Y) is better than other components (AC_U, AC_V) and is close to three components together (AC_YUV). The retrieval accuracy of the AC-coefficients and color histograms (ACCH) combination is better than color histogram only (color_YUV) or AC-coefficients histogram only (AC_YUV). Obviously, the Y component contains texture information more, and the U and V components contain color

information more. This is why the retrieval accuracy of the third set (ACCH) is higher than the first two sets' (AC_YUV and color_YUV).

Table 6: The mAP of three feature sets

Feature sets	AC_Y	AC_U	AC_V	AC_YUV	color_YUV	ACCH
mAP (%)	38.022	36.101	35.838	41.462	46.663	52.938

6.3 Retrieval efficiency

Efficiency is an important indicator to measure the usability of proposed scheme. In our scheme, the retrieval efficiency contains the time consumption of image encryption, index construction and image searching. The time consumption for image encryption contains value permutation and position scrambling. The time for index construction contains feature extraction and indexing. When receiving an encrypted query image, the server searches the index for similar images. A liner index is built in our scheme, so the search time is relevant to the length of feature vectors. Tab. 7 lists the time consumption of three mentioned experiments.

Table 7: Time consumption of three experiments

	AC_YUV	color_YUV	ACCH
Time consumption in encryption (s)	608	1237	1068
Time consumption in index construction (s)	66	206	149
Time consumption in image searching (s)	6	6	6
Total time consumption (s)	680	1449	1223

7 Conclusion

This paper proposes a secure image retrieval scheme with the combination of the AC-coefficients and color histograms. The proposed scheme consists of three operations: i.e. image encryption, index construction and image search. Except the image encryption operation, other operations are outsourced to the cloud server. The images are protected by using stream encryption technology, values replacement and position scrambling encryption algorithms. The security strength of exposed information is computationally analyzed. We further examined and compared the retrieval accuracy of three feature sets. The comparison result shows that the combination of AC-coefficients and color histograms achieves the highest retrieval accuracy. In the future work, we will consider the combination of color feature from DC coefficient and texture feature from AC coefficients to achieve higher retrieval accuracy.

Acknowledgement: This work is supported in part by the National Natural Science Foundation of China under grant numbers 61672294, 61502242, 61702276, U1536206, U1405254, 61772283, 61602253, 61601236 and 61572258, in part by Six peak talent project of Jiangsu Province (R2016L13), in part by National Key R&D Program of China under grant 2018YFB1003205, in part by NRF-2016R1D1A1B03933294, in part by the

Jiangsu Basic Research Programs-Natural Science Foundation under grant numbers BK20150925 and BK20151530, in part by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) fund, in part by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) fund, China. Zhihua Xia is supported by BK21+ program from the Ministry of Education of Korea.

References

Abduljabbar, Z.; Jin, H.; Ibrahim, A.; Hussien, Z.; Hussain, M. et al. (2017): Privacy-preserving image retrieval in IoT-Cloud. *Trustcom/Bigdatase/Ispa*, pp. 799-806.

Abdulsada, A.; Ali, A.; Abduljabbar, Z.; Hashim, H. (2013): Secure image retrieval over untrusted cloud servers. *International Journal of Engineering and Advanced Technology*.

Akgül, C.; Rubin, D.; Napel, S.; Beaulieu, C.; Greenspan, H. et al. (2011): Content-based image retrieval in radiology: current status and future directions. *Journal of Digital Imaging*, vol. 24, no. 2, pp. 208-222.

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

Cai, Z.; Wang, Z.; Zheng, K.; Cao, J. (2013): A distributed TCAM coprocessor architecture for integrated longest prefix matching. *IEEE Transactions on Medical Computers*, vol. 62, no. 3, pp. 417-427.

Cao, Y.; Zhou, Z.; Sun, X.; Gao, C. (2018): Coverless information hiding based on the molecular structure images of material. *Computers, Materials & Continua*, vol. 54, No. 2, pp. 197-207.

Cavallaro, A.; Lagendijk, R.; Erkin, Z.; Kwasinski, A.; Barni, M. (2017): Encrypted signal processing for privacy protection. *IEEE Signal Process*, vol. 30, no. 1, pp. 82-105.

Cheng, H.; Wang, J.; Wang, M.; Zhong, S. (2017): Toward privacy-preserving JPEG image retrieval. *Journal of Electronic Imaging*, vol. 26, no. 4.

Cheng, H.; Zhang, X.; Yu, J. (2016): AC-coefficient histogram-based retrieval for encrypted JPEG images. *Multimedia Tools & Applications*, vol. 75, no. 21, pp. 13791-13803.

Cheng, H.; Zhang, X.; Yu, J.; Li, F. (2015): Markov process-based retrieval for encrypted JPEG images. *International Conference on Availability, Reliability and Security*, pp. 417-421.

Cheng, H.; Zhang, X.; Yu, J.; Zhang, Y. (2016): Encrypted JPEG image retrieval using block-wise feature comparison. *Journal of Visual Communication & Image Repre*sentation, vol. 40, pp. 111-117.

Cui, J.; Zhang, Y.; Cai, Z.; Liu, A.; Li, Y. (2018): Securing display path for security-sensitive applications on mobile devices. *Computers, Materials & Continua*, vol. 55, no. 1, pp. 17-35.

Curtmola, R.; Garay, J.; Kamara, S.; Ostrovsky, R. (2006): Searchable symmetric encryption: Improved definitions and efficient constructions. *ACM Conference on*

Computer and Communications Security, vol. 19, no. 5, pp. 895-934.

Fang, Y.; Chen, Z.; Lin, W.; Lin, C. (2012): Saliency detection in the compressed domain for adaptive image retargeting. *IEEE Transactions on Image Processing*, vol. 21, no. 9, pp. 3888-3901.

Ferreira, B.; Rodrigues, J.; Leitao, J.; Domingos, H. (2017): Practical privacy-preserving content-based retrieval in cloud image repositories. *IEEE Transactions on Cloud Computing.*

Fu, Z.; Huang, F.; Ren, K.; Weng, J.; Wang, C. (2017): Privacy-preserving smart semantic search based on conceptual graphs over encrypted outsourced data. *IEEE Transactions on Information Forensics & Security*, vol. 12, no. 8, pp. 1874-1884.

Fu, Z.; Sun, X.; Linge, N.; Zhou, L. (2014): Achieving effective cloud search services: Multi-keyword ranked search over encrypted cloud data supporting synonym query. *IEEE Transactions on Consumer Electronics*, vol. 60, no. 1, pp. 164-172.

Fu, Z.; Wu, X.; Guan, C.; Sun, X.; Ren, K. (2017): Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement. *IEEE Transactions on Information Forensics & Security*, vol. 11, no. 12, pp. 2706-2716.

Hu, S.; Wang, Q.; Wang, J.; Qin, Z.; Ren, K. (2016): Securing SIFT: Privacy-preserving outsourcing computation of feature extractions over encrypted image data. *IEEE Transactions on Image Processing*, vol. 25, no. 7, pp. 3411-3415.

Jegou, H.; Douze, M.; Schmid, C. (2008): Hamming embedding and weak geometric consistency for large scale image search. *European Conference on Computer Vision*, pp. 304-317.

Kuzu, M.; Islam, M.; Kantarcioglu, M. (2012): Efficient similarity search over encrypted data. *IEEE International Conference on Data Engineering*, pp. 1156-1167.

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

Liu, Y.; Zhang D.; Lu, G.; Ma, W. (2007): A survey of content-based image retrieval with high-level semantics. *Pattern Recognition*, vol. 40, no. 1, pp. 262-282.

Lu, W.; Swaminathan, A.; Varna, V. (2009): Enabling search over encrypted multimedia databases. *Media Forensics and Security I.*

Lu, W.; Varna, V.; Swaminathan, A. (2009): Secure image retrieval through feature protection. *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1533-1536.

Lu, W.; Varna, V.; Wu, M. (2014): Confidentiality-preserving image search: A comparative study between homomorphic encryption and distance-preserving randomization. *IEEE Access*, vol. 2, pp. 125-141.

Parikesit, G. (2017): Quantitative image analysis of Tintin comics. *International Journal of Arts & Technology*, vol. 10, no. 3, pp. 231-240.

Reynolds, C. (2016): Evolving textures from high level descriptions. *International Journal of Arts & Technology*, vol. 9, no. 1, pp. 26-38.

Rui, Y.; Huang, T. S.; Ortega, M.; Mehrotra, S. (1998): Relevance feedback: A power tool for interactive content-based image retrieval. *IEEE Transactions on Circuits & Systems for Video Technology*, vol. 8, no. 5, pp. 644-655.

Song, D.; Wagner, D.; Perrig, A. (2000): Practical techniques for searches on encrypted data. *IEEE Symposium on Security and Privacy*, pp. 44-55.

Wang, C.; Cao, N.; Ren, K.; Lou, W. (2012): Enabling secure and efficient ranked keyword search over outsourced cloud data. *IEEE Transactions on Parallel & Distributed Systems*, vol. 23, no. 8, pp. 1467-1479.

Weng, L.; Amsaleg, L.; Furon, T. (2016): Privacy-preserving outsourced media search. *IEEE Transactions on Knowledge & Data Engineering*, vol. 28, no. 10, pp. 2738-2751.

Xia, Z.; Wang, X.; Sun, X.; Wang, Q. (2016): A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. *IEEE Transactions on Parallel & Distributed Systems*, vol. 27, no. 2, pp. 340-352.

Xia, Z.; Wang, X.; Zhang, L.; Qin, Z.; Sun, X. et al. (2017): A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. *IEEE Transactions on Information Forensics & Security*, vol. 11, no. 11, pp. 2594-2608.

Xia, Z.; Xiong, N.; Vasilakos, A. V.; Sun, X. (2017): Epcbir: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing. *Information Sciences*, vol. 387, pp. 195-204.

Xia, Z.; Zhu, Y.; Sun, X.; Qin, Z.; Ren, K. (2015): Towards privacy-preserving content-based image retrieval in cloud computing. *IEEE Transactions on Cloud Computing*, vol. 6, no. 1, pp. 276-286.

Xia, Z.; Zhu, Y.; Sun, X.; Wang, J. (2013): A similarity search scheme over encrypted cloud images based on secure transformation. *International Journal of Future Generation Communication & Networking*, vol. 6, no. 6, pp. 71-80.

Yuan, J.; Yu, S.; Guo, L. (2015): Seisa: secure and efficient encrypted image search with access control. *Computer Communications*, pp. 2083-2091.

Yuan, X.; Wang, X.; Wang, C.; Squicciarini, A.; Ren, K. (2014): Enabling privacy-preserving image-centric social discovery. *IEEE International Conference on Distributed Computing Systems*, pp. 198-207.

Zhang, L.; Jung, T.; Liu, K.; Li, X.; Ding, X. et al. (2017): PIC: enable large-scale privacy preserving content-based image search on cloud. *IEEE Transactions on Parallel & Distributed Systems*, vol. 28, no. 11, pp. 3258-3271.

Zhang, X.; Liu, W.; Dundar, 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.