Secure and efficient image retrieval based on global features

Aqeel A Yaseen\textsuperscript{1*}, Murtad Hussein Sabri\textsuperscript{1}, and Haitham Ali Hussain\textsuperscript{2}

\textsuperscript{1}Department of Technical Computer Engineering, Faculty of Engineering, Al Kunooze University College, Basrah, Iraq.

\textsuperscript{2}Accountant Techniques Department, Management Technical College of Basrah, Southern Technical University, Basra, Iraq

*Corresponding author e-mail: aay.ali80@gmail.com

Abstract. A few years ago, an image retrieval needs have been increased enormously. Therefore, a need for an efficiency and accurate image retrieval scheme has become desired accordingly. In fact, the images require high storage space; for this reason, cloud computing considers the best selective to outsource images. Many outsourcing images to the cloud server such as medical, police investigation, and personal images that require to encrypt before being outsourced to the cloud servers. However, in this paper a robust scheme has been presented which provides Content Based Image Retrieval (CBIR) over the encrypted images without declassing the important information to the cloud server side. Additionally, the information is exchanging in the strong secure manner among entities. The proposed scheme consists of two phases: setup phase and retrieve phase. The first phase based on build secure dictionary based on global features (intensity of histogram) and images decryption while the second phase utilizes secure query to retrieve the queried image. This scheme is a robust to measure the Euclidean Distance similarity between two queries without decryption. The security and efficiency of the proposed scheme are proofed by security analysis and experiments.

Keywords: Cloud Computing, CBIR, histogram, Diffie-Hellman, n-gram, and Euclidian Distance.

1. Introduction

The cloud computing architecture has ability to store big data and application software depended on minimal management effort and supports on demand services to customers through the internet. Unfortunately, cloud service provider (CSP) does not responsible about security issues or leak data. It offers some levels of security to customer while the other levels of security relies on customers themselves to protect their sensitive data against malicious attacks. The main security issues faced cloud’s data storage existed in privacy, integrity, access control, availability, and confidentiality [9,12,15]. The most important issues are the how to manage the storage, retrieval, extract and invocation the vast amount of data to the cloud servers efficiently; especially with the increasing of the utilization and the development of internet and multimedia. Cloud service provides perfect solution to outsourcing images according to its great benefits such as cost savings, rapid resource elasticity, collaboration efficiency, flexibility of work practices, access to automatic updates and transference of risk [4,20].

The presence of images in cloud servers is very important due its features as previously mentioned. However, the methods of transferring and retrieval images need to take into account many sensitive aspects such as the cost and time complexity of retrieval. In way such retrieve whole image, for example Alice intends to retrieve an image from Bob database which have been already raised to the cloud servers. The query method considers an efficiency when Alice tries to retrieve image from Bob based on whole image. Whereas the retrieval of query image from the database costs time complexity and it is not efficiency especially with the large number of files. CBIR is the effective
method to manage such a retrieval method [11,15,17]. Another technology of image retrieval is the text annotation (specifies the image with notes as a keyword). Although it is a fairly good method, but practically it has some drawbacks and limitations. Two main problems could be determined as per following: (1) a huge amount of images consume the time in order to mark up the text annotation to the images overall the database. (2) The human perception and inaccuracy of some people can cause mistakes, for example the same image could be marked up by different text annotations on the contrary the same text annotation could use in different images. For the mentioned reasons above, the CBIR technology has been presented to overcome the text annotation image retrieval drawbacks [4, 6].

Recently, content-based image retrieval (CBIR) has become one of the most significant field of image retrieval topic. A lot of approaches have been presented to support and analyze an interesting view. In 2008, Yu Xiaohong presented a scheme to describe the basic features of CBIR system, and these features are color, shape, texture, and semantic. Actually, the mentioned components have been described earliest; in 2001 Manjunath et al., utilized texture and color descriptors for the evaluations and developments. The color descriptor contains color structure descriptor (CSD) and callable color descriptor. The texture descriptor includes an edge histogram descriptor (EHD) and a homogeneous texture descriptor (HTD) [1,4,5,6,11].

In 2008, Tamane and Sharvari proposed a scheme for image retrieval using high-level features based on the compounding of low-level features such as color, shape and texture features and converse them into high-level semantic features using fuzzy production rules. The aim of their work is to lead a view toward retrieval using high-level semantic features based on low-level features [6]. In 2013, Bae-Muu Chang et al., presented a method using CBIR depending on the visual features and the compound the features of color, texture, and shape. It is also called CBIRVP. Moreover, for the search optimization of CBIRVP method they used particle swarm optimization (PSO) algorithm. To provide an efficient search method between the query image and the others in database a series of distance measurements have been utilized in order to calculate the similarity between the features and their corresponding similarity measurements [3,11].

The most image retrieval methods that based on feature vectors utilize ether global features like histogram or the local features such Scale Invariant Feature Transform (SIFT) and Speeded Up Robust Features (SURF) descriptors. The global descriptor has the ability to describe the visual content of an entire object with single vector. While the local features describe navigate inside the image (test a small group of pixels) [6,13]. In 2015 Mohammed Alkhawlani et al, proposed CBIR method using local features descriptor Bag-of-Visual Words (BoVW), they utilized SIFT and SURF techniques as local descriptors in order to create image signatures that are invariant to rotation and scale [14].

In 2015 Jaykrishna Joshi and Dattatray Bade, proposed CBIR depending on global features descriptor. A feature extraction is performed for the query image depending on the Global Descriptor Attributes (GDA), they used color features (color moment and color histogram) and texture. Then the normalization is performed in order to fix the image dimension, so it allows comparisons between the query image and the others in database. To retrieve the query image all, the global features convert to the vector of features. Eventually, the matching of features (similarity) between the GDA of the query image and those of the images in the database are then calculated [15].

In 2016, Zhihua et al. proposed an image retrieval scheme that utilizes CBIR over the encrypted image without disclosing the important and sensitive information for the images’ database in the cloud server. The features vectors are constructed to the required image (query image). To protect the features vectors, they use kNN algorithm [18].

In 2017, Ahmad et al. proposed CBIR system using the convolutional neural networks (CNNs). Their idea to build a new CNN-based learning model depending on the context of CBIR. Where he utilizes a deep learning for two parallel CNNs as feature extractors [22]. This paper discusses an efficient and secure method of CBIR depending on the global features for the images that outsourcing to the cloud server. The main contributions are summarized as follows: The environment of our proposed scheme consists of three parts:

- Data owner (DO) who poses the original images which’s been already raised up to the CSP after the encryption step. CSP is the part side which responses to outsource DO’s encrypted images. Users are
the beneficiary people who need to retrieve the images for the scientific researches, medicine, GPS, and others.

Our proposed scheme retrieves any image from cloud servers in secure manner without needing to reveal any information from the original image by using decryption method. Our scheme depends on constructing a secure index in the setup phase which is raised up to CSP by DO. Each of users and DO send a secure query to CSP for retrieving images utilizing from potential of mentioned secure index. The experimental results refer to the accuracy, efficiency, flexibility of our proposed scheme comprising with related works.

The remaining part of this paper is organized as follows: Section 2 review the main concepts that are using in our proposed scheme; Section 3 presents the proposed scheme based on Homomorphic cipher[9,10], Euclidian distance vector, and secure index; Section 4 demonstrates and discusses the experiments carried out on several standard image retrieval datasets and security analysis; and Section 5 concludes this work. Section 2 Concepts and main tools (Image Histogram, Diffie-Hellman, n-gram, and Euclidian distance vector).

2. Concepts and Main Tools
In this paper, section two discusses the main concepts and tools which have already been employed in this paper; and these are image histogram, Diffie-Hellman, and Euclidian distance vector.

2.1. Image Histogram
A global feature descriptor is the feature vector which’s a set of features. It constitutes the representation of image (features such as color, shape, texture etc. are used to describe the content of image) [15]. Image Histogram is Image color representation as graph showing the number of pixels in an image at each different intensity value found in that image. The histogram can represent grayscale images and also color image, for example an 8-bit grayscale image there are 256 different possible intensities, and so the histogram will show the distribution of pixels amongst those grayscale values. Figure 1 shows an image, grayscale image histogram, and RGB image histogram.

The histogram is very useful and helpful in many search arias especially in security field, where it is considered a measurement for the quality and accuracy in computer visualization field. For example, it can use with image steganography to find the convergence percentage between the cover image and the secret image after extraction process; also, it is used with image cryptography to know the validity of image usage after decrypt process.

2.2. Diffie-Hellman Key Exchange
In order to generate, exchange, and share a secret key, Diffie-hellman key exchange algorithm has been used to generate the secret key then exchange it between the DO and users. The DO and users choose two large numbers let say p and g; where:

\[ g \mod p, g^{2} \mod p, ..., g^{p-1} \mod p \]
generate all numbers \([1...p - 1]\)
The two large mentioned above represent the public key. To generate the public key, they choose the private key separately, then use the below formula to generate the public key (PUk):

\[ PU_K = g^{PR_k} \mod p \]

Both PUk of user and DO exchange over secure channel. The last step they use the PUk to generate the shared secret key using below formula [19]:

\[ K = PU_K^{PR_k} \mod p \]

### 2.3. N-gram

N-gram is an adjacent sequence of items such as words, numbers, and characters which are used for a given text or speech. A Latin numerical prefixes n-gram represents the size of contiguous items, for example size of 1 n-gram refers to unigrams (one word, one letter or one character), table-1 shows the different size of n-gram for the sentence “I love my father” [12].

| Size of n-gram | Vernacular name | Order of resulting | Results                  |
|----------------|----------------|--------------------|-------------------------|
| 1              | Unigram        | 0                  | I, love, my, father     |
| 2              | Digram         | 1                  | I love, love my, my father |
| 3              | Trigram        | 2                  | I love my, love my father |

N-gram could be used with the letter, another example for letters n-gram using the same sentence above. Suppose size of n-gram 2, the result of n-gram appears as per below:

“II”, “lo”, “ov”, “ve”, “em”, “my”, “yl”, “fa”, “at”, “th”, “he”, “er”

Actually, the most important utilizing of n-gram is the probability and smoothing process of words and letters in the linguistic fields, analysis fields. Also, it uses in the cryptanalysis fields; where it is used to analysis and predict the ciphertext [18]. In current work, the n-gram has been used in the smoothing process for the histogram vectors, the n-gram size is 2 and the smoothing process and vector reduction perfumed according to the equation (2).

### 2.4. Euclidean Distance

The most important and commonly used metric is the Euclidean distance metric for the similarity measurement, it is widely used in image retrieval. It measures the distance between two vectors of images by calculating the square root of the sum of the squared absolute differences. The distance calculating using the equation below [20]:

\[ d = \sqrt{\sum_{i=1}^{n} (|Q_i - D_i|)^2} \]  

(1)

Where Qi and Di are the feature vectors of query image and images in database. The Euclidean distance has been used in our proposed scheme after the smoothing process to measure the distance between image histogram of query image and the histograms of images in the database of SCP.

### 3. Proposed Scheme

In this part, we proposed an efficient image retrieval scheme, which achieves a strong security and preserves privacy of image in the cloud side. Our work composes of two phases, namely, setup phase and image retrieval phase. The proposed scheme depends on the measure entities represented by the cloud service provider (CSP), data owner (DO), and users (Ui). Both of user and DO need to agree about the key in order to encrypt and decrypt the images based on Diffie Hillman exchange key method and homomorphic Cipher [9,10]. The user needs to send his image query to the CSP then the CPS checks whether the query image can be found; if it does not exist then the CSP informs the user...
failed query. Otherwise, the CSP sends sets of encrypted images. Our work utilizes the notation proposed in table 2 below. Additionally, figure 2 explains the proposed scheme.

**Table 2.** Notation of proposed scheme

| Symbol | Definition |
|--------|------------|
| CBIR   | Content Based Image Retrieval |
| kNN    | k-Nearest Neighbor |
| CSP    | Cloud Service Provider |
| CSD    | Color Structure Descriptor |
| EHD    | Edge Histogram Descriptor |
| HTD    | Homogeneous Texture Descriptor |
| PSO    | Particle Swarm Optimization |
| SIFT   | Scale Invariant Feature Transform |
| SURF   | Speeded Up Robust Features descriptors |
| BoVW   | Bag-of-Visual Words |
| GDA    | Global Descriptor Attributes |
| CNNs   | convolutional neural networks |
| DO     | Data owner |
| PR_k   | Private Key |
| PU_k   | Public Key |
| U_i    | Users |
| SPDO   | Smooth Process of Data Owner |
| SIF    | Secure Index File |
| SPU    | Smooth Process of User |

3.1. **Setup phase**

The DO and U_i should be agreed to generate a shared key (SK_e Z_n; where n is a random integer number) used to encrypt/decrypt images. The phase is organized as per below:

**Step S1.** The DO →CSP: encrypted images
- Encrypt each DO’s image based on homomorphic cipher \( E_i = Enc_{SK_e}(img_i) \).
- Sends the encrypted image \( E_i \) to CSP

**Step S2.** The DO →CSP:SIF
- Extract global feature based on histogram function from each DO’s image
  \( Feature_i = Imghist(img_i) \)
- Apply smoothing process by using the following equation:

\[
SPDO = \sum_{i=1}^{\text{length}(Feature_i)-n} Feature_i
\]  

(2)

Where \( n = 2 \) is the n-gram size.
- Create secure index file \( (SIF) \) that consists of index of DO’s images, \( SPDO, E_i \) and then raising up \( SIF \) and Encrypted images to CSP.
3.2. Image Retrieval Phase

The user $U_i$ wishes to send an image query in order to retrieve all similar images in the CSP. The response of $U_i$’s query either restores a set of images or no image. The CSP performs image retrieval in secure way. The following steps explain the mechanism of retrieval phase working:

3.2.1. Step I1. The $U_i \rightarrow$ CSP: Query$_i$ (Target$_i$ img$_i$, result)
- Select Target img$_i$, proceed Feature$_i'$=Imghist(Target$_i$img$_i$), and calculate SPU based on equation (2) and Feature$_i'$.
- Send SPU to CSP.

3.2.2. Step I2. Up on receiving the information of user’s request, CSP applies the following steps:
- Check the target image (Target$_i$ img$_i$); if found or no inside the SIF based on SPU and Euclidian distance vector. Where Euclidian distance vector (SPDO, SPU).
- The result of Euclidean distance gets back to the user with a set of encrypted images or nothing.
- Send the result (encrypted images ($E_1, ..., E_n$)) to the user.

Step I3. When up receiving the result ($E_1, ..., E_n$) from CSP. $U_i$ decrypts the result based on:
- img$_i$ =Enc$_{SK_i}$($E_i$), for all encrypted images ($E_1, ..., E_n$) by using homomorphic cipher. As a result, $U_i$ obtains all required images from CSP in securely way.

3.3. Key Exchange

It is the last step between users and DO. The DO and users shared the secret key for this reason. Therefore, they need to exchange the secret key at the end of each session; the key exchange method depends on Diffie-Hellman key exchange algorithm as mentioned above.

Figure 2. Demonstrating the proposed scheme
4. Experimental Results and Analysis

Our proposed scheme was evaluated by using a standard general image database from COREL Database for CBRI. The database contains 10,000 images; we utilized only 1000 image in our experimental. Figure 3 shows some sample training images. The experiments are implemented by using MATLAB ver. 9.2.0.538062 (R2017a) running on Windows 10 with an Intel Core i7 processor, 8 GB RAM and 2.4 GHz CPU. The proposed scheme was divided into three phases: setup, image retrieval, and key exchange.

4.1. Setup Phase

In this phase the index file is built, it has three fields: image index which represents the name of image, image histogram after applying the smoothing process and the encrypted image. Figure 3 shows how the index file appears.

![Original image](image1.png)  ![Image Histogram](image2.png)  ![Encrypted Image](image3.png)

**Figure 3. Setup phase**

4.2. Image Retrieval:

A query image is requested by the user, an extraction of global feature (histogram) of query image must be done with images inside CS, so the SPU performs previously, then Euclidian distance vector algorithm applies in order to calculate the similarity ratio to get the required image. A set of images retrieve once retrieval phase finished. The amount of retrieved images depends on the gradient and color density of the query image and the images stored in the CSP database. To increase the accuracy of retrieved images, we supposed a threshold to limit the number of image retrieval. According to our practical experiments, we suggested the value 11.99 as threshold to get the similarity ratio (distance). The last step in this phase is the images decryption, so the end use can check the required images after retrieving phase. Figure 4 shows the results of retrieval phase.
| Image          | Score 0 | Score 1 | Score 2 | Score 3 | Score 4 |
|---------------|---------|---------|---------|---------|---------|
| Elk #122      | 0       | 3.9278  | 4.0321  | 4.3464  | 4.5809  | 4.9389  |
| Shrimp #472   | 0       | 6.4153  | 6.8003  | 6.9522  | 7.0503  | 7.1396  |
| Lab #649      | 0       | 6.1833  | 7.4405  | 7.5987  | 7.7838  | 8.0245  |
| Water Flow #850 | 0     | 5.4239  | 3.7654  | 5.1308  | 5.6273  | 5.9766  |

**Figure 4.** Image retrieval result

5. Conclusion
A huge development in information technology, multimedia, social networks, and cloud computing era, provides an enormous prospect for users. Therefore, user can access to his data from anytime/
anywhere. With this widely and quick development in the information technology, the image retrieval is considered an active research topic. However, many image retrieval researches presented approaches of image retrieval using local and global features extraction. This paper presented secure image retrieval using global feature extraction through image histogram and retrieve the encrypted images with no need to decrypt images before the retrieving process. Our proposed scheme consists of two phases: setup and retrieval. In the setup phase, the data owner has ability to rise up his images in cloud service provider based on index file which consists of image name, image histogram, and encrypted image using homomorphic cipher. Continuously, in the second phase DO requests a query image in order to get the similarity between the query image and images in CSP database using Euclidean Distance vector. The experiments demonstrated a satisfied result and shows the flexibility, efficiency, scalability, and effectiveness.

References
[1] Manjunath, B S, Ohm J-R, Vasudevan and V V Yamada, Lu T C and Chang 2001. Color and texture descriptors, IEEE Transactions on Circuits and Systems for Video Technology 11, 703–715.
[2] J Weinman, A Hanson and A McCallum 2004. Sign detection in natural images with conditional random fields, In IEEE International Workshop on Machine Learning for Signal Processing, pages 549–558.
[3] Dimitri A Lisin, Marwan A Mattar, Matthew B Blaschko, Mark C Benfield and Erik G Learned-Miller 2006. Combining Local and Global Image Features for Object Class Recognition. IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp. 1 - 8.
[4] Lu T C and Chang 2007. Color image retrieval techniques based on color features and image bitmap, Information Processing and Management, 43,461–472.
[5] Yu Xiaohong and Xu Jinhua 2008. The Related Techniques of Content-based Image Retrieval, International Symposium on Computer Science and Computational Technology, PP. 154-158.
[6] Tamane and Sharvari 2008. Content Based Image Retrieval Using High level semantic features, Proceedings of the 2nd National Conference.
[7] P Mell and T Grance 2009. The NIST Cloud Computing Definition, Information Technology Laboratory, Special Publication 800-145.
[8] A C-F Chan 2009. Symmetric-Key Homomorphic Encryption for Encrypted Data Processing, Proc. of the IEEE International Conference on Communications (ICC’09), Dresden, Germany, pp.774-778.
[9] A A Yassin, H Jin, A Ibrahim, W Qiang and D Zou 2012. Efficient password-based two factors authentication in cloud computing, International Journal of Security and Its Applications, volumes 6 (2), 143-148.
[10] Ali A Yassin, Hai Jin, Ayad Ibrahim, Weizhong Qiang and Deqing Zou 2012. A practical privacy-preserving password authentication scheme for cloud computing, IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum.
[11] Bae-Muu Chang, Hung-Hsu Tsai and Wen-Ling Chou 2013. Using visual features to design a content-based image retrieval method optimized by particle swarm optimization algorithm, Engineering Applications of Artificial Intelligence 26, 2372–2382.
[12] Sidorov and Grigori 2013. Syntactic Dependency-Based n-grams in Rule Based Automatic English as Second Language Grammar Correction, International Journal of Computational Linguistics and Applications, 4 (2): 169–188.
[13] A. Abbas, K Bilal, L Zhang and S U Khan 2014. A cloud-based health insurance plan recommendation system: a user centered approach, Future Generation Computer Systems, Vol. 43–44.
[14] Mohammed Alkhawlani, Mohammed Elmogy and Hazem Elbakry 2015. Content-Based Image Retrieval using Local Features Descriptors and Bag-of-Visual Words, (IJACSA) International Journal of Advanced Computer Science and Applications, 6(9).
[15] Jaykrishna Joshi and Dattatray Bade 2015. Global Descriptor Attributes Based Content Based Image Retrieval of Query Images. *Journal of Engineering Research and Applications*, Vol 5.

[16] Naresh Vurukonda1 and B Thirumala Rao 2016. A Study on Data Storage Security Issues in Cloud Computing. *In: Proc. International Conference on Intelligent Computing, Communication & Convergence, Procedia Computer Science* 92, 128 – 135, Bhubaneswar, Odisha, India.

[17] K Guo, R Zhang, Z Zhou, Y Tang and L Kuang 2016. Approach for internet image retrieval. *Inf. Sci.* 358 151–163.

[18] Zhihua Xia, Neal N Xiong, Athanasios V Vasilakos and Xingming Sun 2016. EPCBIR An efficient and privacy-preserving content-based image retrieval scheme in cloud computing, *Information Sciences* 1–10.

[19] William Stallings 2016 *Cryptography and Network Security Principles and Practices*, Fourth Edition, ISBN-13: 978-0-13-44428-4.

[20] Sun Xiaoming, Zhang Ning, Wu Haibin, Yu Xiaoyang, Wu Xue and Yu Shuang 2016. Medical Image Retrieval Approach by Texture FeaturesFusion Based on Hausdorff Distance, *Mathematical Problems in Engineering*, Volume 2018, Article ID 7308328.

[21] Yanyan Xu, Jiaying Gong, Lizhi Xiong, Zhengquan Xu, Jinwei Wang and Yunqing Shi 2017. A Privacy-Preserving Content-based Image Retrieval Method in Cloud Environment, *Journal of Visual Communication and Image Representation*, Vol. 43, 164-172.

[22] Ahmad AlzuObi, Abbes Amira and Naeem Ramzan 2017. Content-Based Image Retrieval with Compact Deep Convolutional Features, *Neurocomputing, NEUCOM* 18305, S0925-2312(17)30618-5.