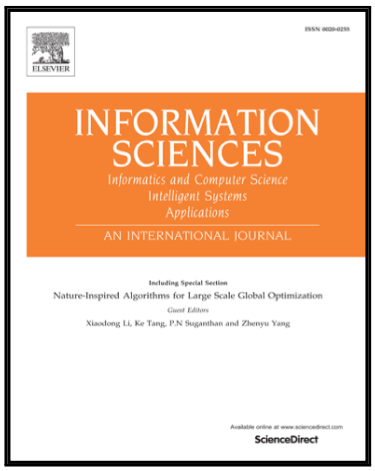

SSIR: Secure Similarity Image Retrieval in IoT

Hongyang Yan, Zhe Chen, Chunfu Jia

PII: S0020-0255(18)30932-0
DOI: https://doi.org/10.1016/j.ins.2018.11.046
Reference: INS 14090

To appear in: *Information Sciences*

Received date: 15 July 2018
Revised date: 4 November 2018
Accepted date: 17 November 2018

Please cite this article as: Hongyang Yan, Zhe Chen, Chunfu Jia, SSIR: Secure Similarity Image Retrieval in IoT, *Information Sciences* (2018), doi: https://doi.org/10.1016/j.ins.2018.11.046

Highlights

- We propose a novel secure similarity image retrieval system by using SGX technology based on CBIR, which can protect the privacy of features and image contents from cloud server.
- The SSIR scheme enables the resource-constrained clients to move the process of preprocessing images to cloud sever, and perform searching in cloud server. This will reduce the cost of client.
- We implemented secure similar images retrieval function on real SGX platform and analyzed the experimental results.

SSIR: Secure Similarity Image Retrieval in IoT

Hongyang Yan, Zhe Chen, Chunfu Jia*

College of Computer and Control Engineering, Nankai University, Tianjiin, 300000, China

Abstract

With the development of the Internet of Things (IoT) technology, we are entering a new era of computing technology. This emerging technology allows connectivity for everyone and everything. Thus, IoT encapsulates some intelligence in Internet-connected objects to communicate, exchange information, sharing multimedia data, take a decision, invoke various actions and provide amazing services through smart devices. A huge amount of sensitive information and multimedia data such as images and videos are sharing which generates traffic in the network. Moreover, multimedia data contains high dimension property, which affects image processing including storage and retrieval in IoT environment. Additionally, limited storage capabilities and computing power are drawbacks of smart devices which makes the situation more complicated. To overcome this problem, users prefer to store their multimedia data on a cloud server to make local storage and computation flexible in smart devices, but still security and privacy concerns. To get rid of this challenges, the emergence of Intel Software Guard Extension (SGX) provide a new solution. In this paper, a novel secure similarity image retrieval (SSIR) scheme based on the primitive of content-based image retrieval (CBIR) is proposed to protect the images search. In addition, the proposed SSIR scheme enables the resource-constrained clients to move the process of images as well as the outsource searching operations to the cloud server which reduce the cost. Furthermore, the security analysis shows

*Corresponding author.

Email addresses: hyang.yan@foxmail.com (Hongyang Yan), chenzhe501@foxmail.com (Zhe Chen), cfjia@nankai.edu.cn (Chunfu Jia)

our scheme is secure in the proposed model. Experiment results illustrate that our scheme is well fitting for images retrieval in practical applications.

Keywords: Content-based image retrieval, SGX, IoT, Security privacy

1. Introduction

With the rapid development of the Internet of Things, smart devices have been widely used in our daily life, which attracts people to share multimedia data such as images or videos. Thus, a large amount of image data are flooding on the Internet [39]. Although smart devices bring a lot of convenience for people, due to the disadvantages of smart devices such as limited storage capability and computing power, users on the mobile device side cannot perform complex processing, especially image data with a high dimension. Therefore, in order to save the storage space and reduce the computation overhead of the client side, users usually outsource their images to the cloud server.

This situation leads to the image search operated by the cloud server. Currently, a lot of companies and research institutes are working on developing the image retrieval systems [35, 36, 40]. The most popular image search systems include Google Similar Images and Baidu Shitu. But the security and privacy issues are still concerned because these systems are searching based on the original images. For example, when a client attends to retrieve some similarity images, he needs to upload the query image to the cloud server. Then the image content and his interests will are known by the cloud server. This will result in a privacy leak, especially the image content relates to the private photos or medical images.

Encryption is a general solution to protect the image privacy, image owners encrypt their images before uploading to the cloud server. Users can exploit the cloud server to share [7], search [34] or control access [31, 41, 16] to their image data. However, it also brings a new challenge when searching over the ciphertexts. Some existing works have tried to present a secure image retrieval system. They used technologies such as order-preserving encryption (OPE) [2],

homomorphic encryption (HE) [27], comparable encryption [42] to keep privacy-preserving. All previous works on privacy-preserving image search impose either a heavy workload or complex processing for image owners. These schemes are difficult to be implemented on resource-constrained devices.

The release of SGX [21, 1] technology provides a new way of secure image retrieval. It can isolate a completely trusted space for original image search. SGX is an extension of the Intel System to enhance the security of software. This method does not identify the malware on the platform, instead, it seals the security operations of legitimate software in an enclave, protecting it from malware, any non-privileged software cannot access the enclave. In other words, once the software or data are loaded into the enclave, anyone cannot affect the code and data even the operating system. Utilizing the SGX technology, during the image retrieval process, the encrypted image can be loaded into the enclave for decryption and then search over the plaintext image. Furthermore, there can be multiple enclaves running in parallel in the SGX.

1.1. Our contribution

In order to reduce the computing cost on the client side, we propose a novel secure similarity image retrieval (SSIR) scheme based on the primitive of CBIR to protect the privacy during a search by using SGX technology. Our proposed scheme provides a new solution for secure image retrieval. Compared with the existing works, our scheme has the following contributions:

- We propose a novel secure similarity image retrieval system by using SGX technology based on CBIR, which can protect the privacy of features and image contents from the cloud server.
- The SSIR scheme enables the resource-constrained clients to move the process of images to the cloud server, and outsource searching operations in the cloud server, which reduces the cost at the client side.
- We implemented secure similar images retrieval functions on real SGX platform and analyzed the experimental results. The experimental results

show that the proposed SSIR scheme has advantages in practical application.

1.2. Organization

The rest of paper is organized as follows: the related works are introduced in section 2. The preliminaries are given in section 3. Section 4 describes the basic system model. The concrete scheme is presented in section 5. Section 6 gives security analysis about our scheme and Section 7 shows the experimental evaluation. Finally, conclusions are made in section 8.

2. Related work

Content-based image retrieval has been studied for several years [8], and some image retrieval systems have been put into application, such as Google Similar Images and Baidu Shitu. However, these works focus on efficiency and performance, security and privacy issues are neglected. Thus, researchers are paying more attention to study the secure image retrieval scheme.

To the best of our knowledge, there are the following main techniques to construct secure image search schemes. Zou et al. [26] proposed a SecSIFT scheme by using scale-invariant feature transform (SIFT) [18] algorithm to extract features and order-preserving encryption (OPE) [5] to encrypt feature vector. Their scheme guarantees the privacy requirement when the user outsourced SIFT computation between two independent servers. Similarly, Wang et al. [32] proposed a practical privacy-preserving outsourced image search model. They

Scheme	Technique	Model	Search over
SecSIFT [26]	SIFT, OPE	Two cloud servers	Encrypted images
Wang et al. [32]	SURF, SHE	Two cloud servers	Encrypted images
Lu et al. [19]	SIFT, HE	A single server	Encrypted images
Our SSIR	SURF, SGX	A single server	Original images

Table 1: The main secure image retrieval schemes

extracted feature points and compared by leveraging speeded-up robust feature (SURF) and somewhat homomorphic encryption (SHE) [6] respectively. Lu et al. [19] presented a secure SIFT feature detection system with homomorphic encryption [10]. They detected feature points by investigating a quantization-like comparison strategy.

Table 1 gives some classic schemes of secure image retrieval. From Table 1, the most used encryption techniques include OPE, HE. Order-preserving encryption is used to guarantee the sequence is consistent with the plaintext in the case of ciphertext. But this will lead to the sequence information leak. Homomorphic encryption technology is also used to construct secure image search scheme, however, these schemes usually need complex computations. They cannot be applied in the computing-restricted environment. All the mentioned works are searching images over ciphertext, that is to say, they cost the precision of their schemes to achieve the security. Some other related works focus on the interesting fields such as face recognition [22, 27, 33], privacy-preserving classification of electrocardiogram (ECG) signals [3], privacy-preserving fingercode authentication [9]

3. Preliminaries

3.1. Speeded-up robust features (SURF)

The method of feature extraction is significant in context-based image retrieval. The common feature extraction methods include color feature [13, 14, 23, 29], texture feature [11, 30], shape feature [24, 25, 20] and local invariant feature [28, 37]. Comparing to other methods, both SURF algorithm and SIFT algorithm have a better robustness and distinguishable for the scale and rotation of images than other algorithms. But SURF algorithm is faster than SIFT algorithm, thus we use the SURF algorithm to extract image feature in our experiment.

SURF algorithm was first presented by Herbert Bay in 2006 [12], and published in 2008 [4]. SURF algorithm is an improvement of the SIFT algorithm,

which was proposed by David Lowe in 1999 [17], and finished perfectly in 2004 [18]. The major stages of computation used to generate the set of image features as follows:

a. Constructing scale-space For an image $I(x, y)$, in order to generate the image's stable edge points, it first needs to construct a Hessian matrix as follows:

$$H(I(x,y)) = \begin{bmatrix} \frac{\partial^2 I}{\partial x^2} & \frac{\partial^2 I}{\partial x \partial y} \\ \frac{\partial^2 I}{\partial x \partial y} & \frac{\partial^2 I}{\partial y^2} \end{bmatrix} \tag{1}$$

For each point $I(x, y)$, the Hessian's determinant is computed as

$$det(H) = D_{xx} \cdot D_{yy} - (0.9D_{xy})^2 \tag{2}$$

where D_{xx}, D_{yy} and D_{xy} are the second order Gaussian derivatives in x, y and xy direction repectively. The weighting factor 0.9 is used to balance the error which is caused by the use of approximation box filters.

b. Interest point localizaion Each point, processed by the Hessian matrix is compared with its 26 neighbors in the image space. If it is larger or smaller than its neighbors, this point will be selected as an interest point.

c. Orientation assignment For each interest point, the harr wavelet feature in its circular neighborhood is counted. That is, in the circular neighborhood of the feature points, the sum of the horizontal and vertical harr wavelet features of all points in the $\frac{\pi}{3}$ sector is counted, and then the fan shape is rotated at intervals of 0.2 radians and repeat this process. Finally, the direction of the sector with the largest value is taken as the main direction of the feature point.

d. Keypoint descriptor Select 4×4 square around the interest point, and count the harr wavelet feature in horizontal and vertical direction. Thus, this harr wavelet feature is denoted as $(\sum d_x, \sum d_y, \sum |d_x|, \sum |d_y|)$, and an interest point feature vector is 64-dimension.

3.2. Intel software guard extensions (SGX)

Intel Software Guard Extensions (SGX) [21, 1] is an extension of the Intel System to enhance the security of software. It provides an *enclave* to isolate execution environment, which is a trusted space. SGX mainly has three functions: *isolation*, *sealing*, and *attestation*.

- Isolation: Once programs and data are loaded into the enclave, no one cannot read or modified the content, even the operating system.
- Sealing: Every SGX processor has a hardware-resident key which is called the Root Seal Key. When an enclave is created, it can derive a key from the Root Seal Key called the Seal Key, and the key is used to encrypt or authenticate data and store it in untrusted memory.
- Attestation: It includes two forms of attestation: local attestation and remote attestation. When two enclaves on the same platform, they use local attestation. When two enclaves on the different platform, they use remote attestation.

SGX provides a secure computing environment during the search process. It loads the required calculation into the enclaves, which ensure the security of the calculation process.

4. System Model

In this section, we introduce the basic system model including *participants*, *threat model* and *design goals*.

4.1. Participants

In our system, we have three participants: *image owner*, *search client* and *a cloud server*.

- Image owner: Image owner has a large scale of images which can build an image library. The image owner extracts image features, and encrypt images and feature vectors, then sends the ciphertext to the cloud server.

- Client: A search client usually provides a query image, aiming to search for the similarity images. Because of the search client has a resource-constrained power, the process of extracting image features and searching have to be performed in a cloud server.

- Cloud server: A cloud server provides a powerful storage service and computing power. The encrypted images and index are stored in the server. It helps the client search the similarity images and returns the result to the client side.

4.2. Threat model

We suppose that the cloud server is "honest-but-curious". It follows our protocol honestly but always tries to learn additional information during the search process. In this paper, we consider the threat model as the following one [38]. The cloud server has the ability to access the encrypted images and feature vectors. It can access the encrypted query image and feature vector.

4.3. Design goals

In our system, we design to achieve the following several aspects:

- Privacy of image owner: The privacy of large images and feature vectors have to be protected, the adversary can not get any content information about images.

- Privacy of client: The query image information should be protected. The server and image owner cannot obtain the information about the query image. It guarantees the query privacy of the client.

- Unforgeability: Before searching, a client needs to authenticate to image owner firstly, a search client who is authorized by image owner can use search functions; otherwise, the program will terminate.

5. System Design

5.1. Overview

The SSIR system consists of three parts: *image owner, cloud server* and *client*. The first two platforms need SGX to be embedded, the last one does not need SGX embedded, it only needs to be able to do the encryption and decryption operations.

Protocol flow. First, image owner generates two pairs of keys: a public encryption key pair and a signature key pair. The public encryption key is used to encrypt the images and the feature vectors. The signature key is used to authorize the clients to perform the image search over the image set. Next, through remote attestation and local attestation, the secret key of image owner is transferred to the search enclave. The search enclave decrypts the encrypted query image, extracts the feature vectors of the query image and runs the search algorithm on the plaintext. Finally, it returns the result to the client.

5.2. Functions

5.2.1. Image owner

The image owner platform runs a secure enclave called the key manage enclave and has three main functions: *setup*, *search authorization*, and *decryption key provisioning*.

Setup. The key manage enclave generates a public/private key pair (pk_0, sk_0) which is used to encrypt the images and verification/signing key pair (vk_{sig}, sk_{sig}) which is used to authorize search function to clients. The keys pk_0 and vk_{sig} are published while the keys sk_0 and sk_{sig} are sealed with the key manage enclave's sealing key and kept in non-volatile storage.

Search authorization. When the image owner receives a request from a client, he determines whether or not to authorize search function to the client. If the image owner agrees, he provides a signature to the cloud server. The search function will be loaded into an enclave program called a *search enclave*. The image owner signs the MRENCLAVE value in the report of this enclave,

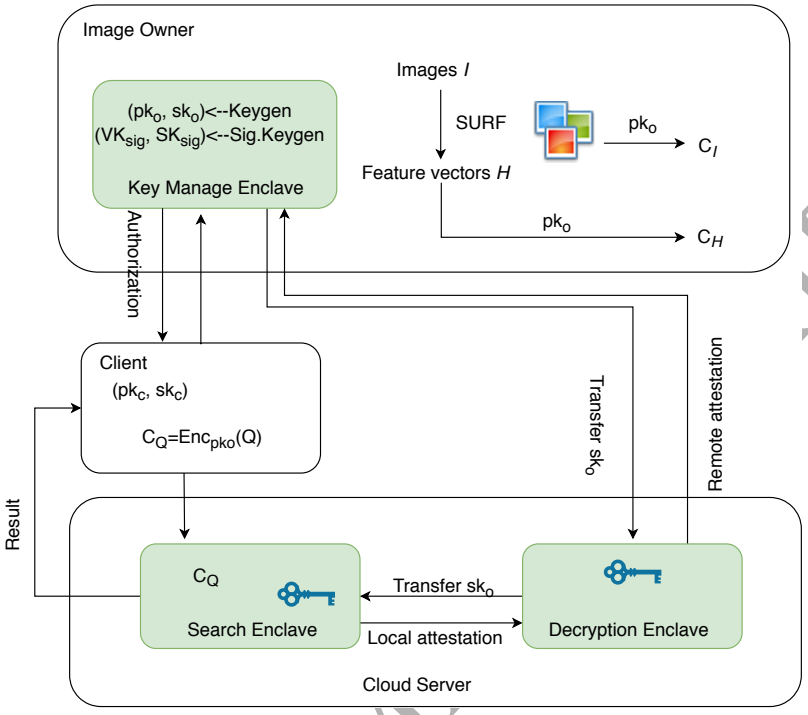

Figure 1: The system architecture and protocol flow

which identifies the code and static data that was loaded into the enclave upon initialization.

Decryption key provisioning. When the cloud server verifies the validity of the image owner's signature, the key manage enclave will receive a remote attestation from decryption enclave, and then transfer the image owner's secret key sk_o to decryption enclave. Then the decryption enclave transfers the secret key sk_o through local attestation sent from search enclave.

5.2.2. Client

Encryption. The search client provides a query image Q and intends to search similar images over the image set of the owner. Due to the resource-constrained, the client can not preprocess the image locally. The client encrypts the query image using the public key pk_0 and uploads to the server cloud.

Decryption. The client receives the search results from the cloud server and decrypts the encrypted images with private key sk_c.

5.2.3. Cloud server

Decryption enclave. When the cloud server verifies the validity of the image owner's signature, the decryption enclave sends a remote attestation to the key management enclave and obtains the image owner's private key sk_o through establishing a secure channel. Then the decryption enclave transfers the key to the search enclave after local attestation.

Search enclave. The search function is loaded in the search enclave. The client sends an encrypted query image to the search enclave, and the ciphertext will be decrypted with secret key sk_o. The feature vector of this query image is extracted in search enclave first, then the search algorithm is performed and returns the search results. The similar images are encrypted with the client's public key pk_c before they are output from search enclave. Therefore, the server cannot obtain the plaintext information and returns the ciphertexts to the client side at last.

5.3. The Concrete Scheme

We construct the concrete scheme in this part. Here, we suppose that the image owner has an image set $I = \{I_1, I_2, ..., I_n\}$, n is the number of images. For the image owner, there are two pairs of keys, one is public key pair (pk_o, sk_o), and another one is signature key pair (vk_{sig}, sk_{sig}). For a search client, there is a public key pair (pk_c, sk_c).

The secure similarity image retrieval scheme consists of the following steps:

Step 1: Image Preprocessing. Before uploading the image set to server, image owner needs to preprocess the images. This procedure includes two parts:

- Image encryption: Image owner needs to upload the image set $I = \{I_1, I_2, ..., I_n\}$ to the cloud server, where I_i denotes the i^{th} image. In order to protect the image content from the server, the image owner encrypts the

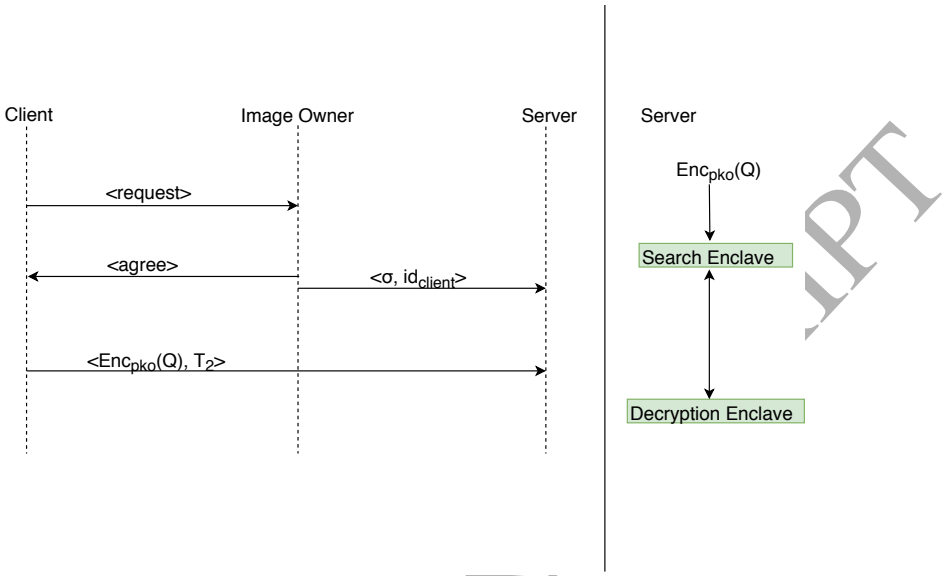

Figure 2: The search request protocol

image set I with the secret key sk_o, then obtains the encrypted images $C_1, C_2, ..., C_n$.

- Image index encryption: This part is to generate an image index according to the feature vectors which are extracted from images by using the SURF algorithm. The final feature vector is denoted as $\mathbf{h}_i$, where $1 \leq i \leq n$.

Step 2: Search Request. When a client needs to search a similar image in the owner's image set, the client has to ask the authorization from the image owner. If the image owner agrees the client's search request, he will send a message $< agree >$ to the client and a signature $\sigma < Sign_{sk_{sig}}(id_{client}, T_1) >$ by using the image owner's private signature key to the cloud server. The client once receives the *agree* message, he sends the encrypted query image $< Enc_{pk_o}(Q), T_2 >$ to the cloud server. The cloud server first verifies the time $T_2 - T_1 < \triangle T$, which $\triangle T$ denotes the valid time. Second, the cloud server verifies the signature by computing $Vrfy_{vk_{sig}}(Sign_{sk_{sig}}(id_{client}, T_1), id_{client})$. Then, the cloud server loads the encrypted query image $Enc_{pk_o}(Q)$ in search enclave.

Search enclave gets the secret key sk_o via local attestation from decryption enclave. Finally, the encrypted query image is decrypted in the search enclave, which is a trusted environment that the cloud server cannot obtain the image content.

Step 3: PreSearch. The query image Q will be first extracted feature by using the SURF algorithm, the feature vector is $\mathbf{h}_Q$.

Step 4: Search. This algorithm is performed in search enclave. It computes the distance between the query image Q and each image I_i in the image set. The detailed search algorithm is shown as Algorithm 1. $\mathbf{h}_Q, \mathbf{h}_i$ denotes the feature vector of query image and the i^{th} image respectively, suppose the dimension is m, the $dis(\mathbf{h}_Q, \mathbf{h}_i)$ denotes the distance between the two images. We use the Euclidean distance to measure the similarity between two images, the shorter the distance, the more similar the images. $\mathbf{h}_k$ denotes the similar images.

Algorithm 1 The search algorithm

Input $\mathbf{h}_Q$ and $\mathbf{h}_i$
Output $\mathbf{h}_k$
compute $dis(h_Q, h_i) = \sqrt{(\mathbf{h}_{Q_1} - \mathbf{h}_{i_1})^2 + ... + (\mathbf{h}_{Q_m} - \mathbf{h}_{i_m})^2}$
for $\{i = 1; 0 < i \leq n; i++\}$ **do**
    if $dis(\mathbf{h}_Q, \mathbf{h}_i) < dis_{match}$
        $\mathbf{h}_k = \mathbf{h}_i$
    end if
end for

Step 5: EncImage. The similar images are encrypted with the public key pk_c of the client in search enclave. The server can not get plaintext information. Then the server sends the ciphertext C_k to the client side.

Step 6: DecImage. The client receives the ciphertext C_k from the cloud server, then decrypts it by using his secret key sk_c. Finally, the client obtains the similar images.

6. Security Analysis

In this section, we present the security analysis of SSIR scheme from the following aspects:

Privacy: The SSIR scheme achieves both the privacy of the image owner and the client. Because image owner encrypts their images and feature vectors before uploading to the cloud server firstly, the cloud server cannot obtain any sensitive information about the image contents. Thus, the privacy of image owner is protected. Besides, when a search client intends to query an image, he encrypts the image and preprocesses it in the enclave on the cloud server. The similarity images are encrypted with the public key of the client in the enclave. Afterward, the cloud server returns the ciphertext of similar images to the client directly. Thus, image owner and cloud server do not get information about query image.

Unforgeability: Before searching, a client needs to authenticate to the image owner firstly. If the image owner agrees, the client sends the encrypted query image to the cloud server, the cloud server obtains the signature from the image owner, it verifies the validity of the signature. The program will go on formally in case of the signature is valid; otherwise, it will terminate.

7. Performance Evaluation

m	32 bits	64 bits	128 bits	256 bits	512 bits
$Enc_{enclave}$ (ms)	13	13	18	22	32
$Dec_{enclave}$(ms)	70	91	172	372	713

Table 2: The encryption and decryption time in enclave.

We implemented our scheme on a real SGX platform. We test the experimental evaluation and analyze the results in this section.

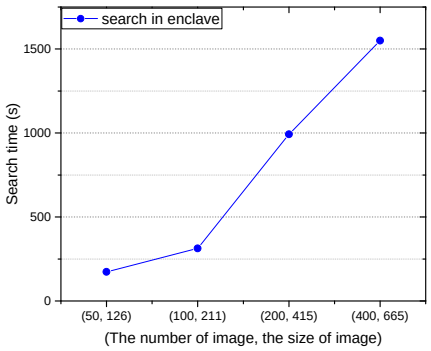

Figure 3: Impact of the number of images on search cost

We implement our scheme by using *C* language on the VS2010. The experiment is conducted on a computer with Intel(R) Core(TM) i9-8950 CPU running at 2.9GHz, 16G RAM. We test our experiment on the famous INRIA Holidays image set [15]. The holiday's image set is a set of images which mainly contains some holiday's photos, we randomly select 50, 100, 200, 400 images from the data set.

In our experiment, we mainly test the *search cost* and *search accuracy* to evaluate SSIR scheme.

- *Search cost:* We test the search time and the encryption/decryption time in the enclave. As shown in Figure 3, we test the query time by searching across different sized image sets. The image sets are (50, 126), (100, 211), (200, 415), (400, 665) respectively. The former represents the number of images, and the latter represents the size of the image set. The search time increase with the size of the image set. Table 2 illustrates the encryption/decryption time increase with the size of the plaintext.

- *Search accuracy:* In order to evaluate the accuracy of SSIR scheme, we use the well-known evaluation method: *recall* vs. *1-precision*.

$$recall = \frac{The\ number\ of\ correct\ matched\ images}{The\ total\ number\ of\ related\ images}$$

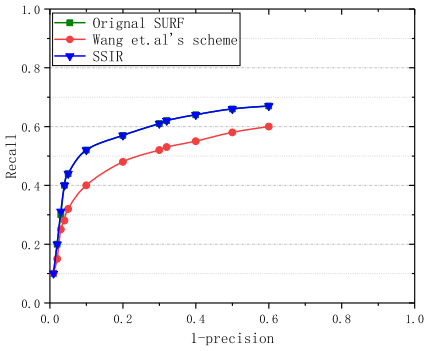

Figure 4: Recall vs. 1-precision

$$1 - precision = \frac{The\ number\ of\ correct\ matched\ images}{The\ totol\ number\ of\ all\ matched\ images}$$

Figure 4 shows the curve about recall vs. 1-precision. We compared our SSIR scheme with the original SURF [12] and Wang *et al.*'s scheme [32]. Because in both original scheme and SSIR scheme, the feature extraction and interesting points matching are conducted on plain images, their recall vs. 1-precision curves overlaps basically, while Wang et al.'s used two servers to extract feature points over the encrypted images, their recall and 1-precision lower than ours. We select two different images as the query images respectively. The search results are shown in Figure 5. When the number of same feature point between the two images is larger than t, where the t is the threshold value, the system returns the similar image.

Discussion. We also test the search time in a formal situation. Figure 6 illustrates the comparison of search time between a formal situation and enclave environment. It can be observed from the figure that as the image number increases, the time it takes for the search algorithm to run in the enclave is longer than the normal operation. The performance loss is indicated in Figure 7. We analyzed the reason of causing performance loss: read data and computing process. When the data is loaded into the enclave, the mapping table will be rewritten, switching from normal mode to enclave mode will result in a system

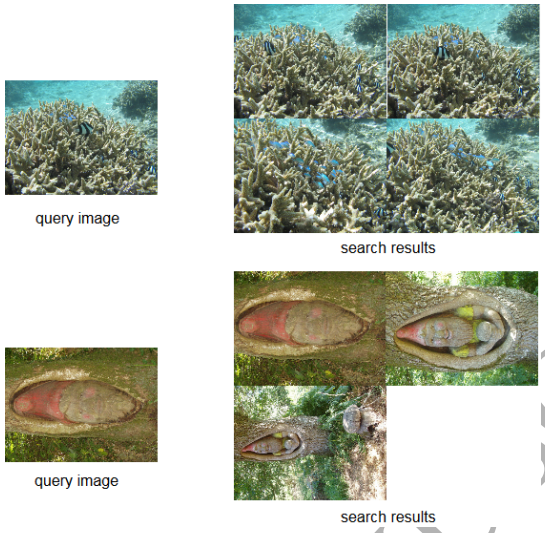

Figure 5: Search results

interrupt, which brings extra time. During the computing process, it also needs to be called from the outside to the enclave, thus it generates extra time.

8. Conclusion

In this paper, we proposed a novel secure similarity image retrieval (SSIR) scheme based on the primitive of CBIR to protect the privacy during the search. Our scheme uses SGX technology to ensure security during the matching process. It enables the resource-constrained clients to reduce the consumption of storage and computing power. Comparing to the existing solutions, our scheme can provide a new secure similarity image search solution.

Acknowledgments

This work is supported by National Key Basic Research Development Program (No.2013CB834204), National Natural Science Foundation of China (No.61772291), Tianjin Natural Science Foundation (No.17JCZDJC30500), Open Topic of China Civil Aviation University Information Security Evaluation Center (No.CA

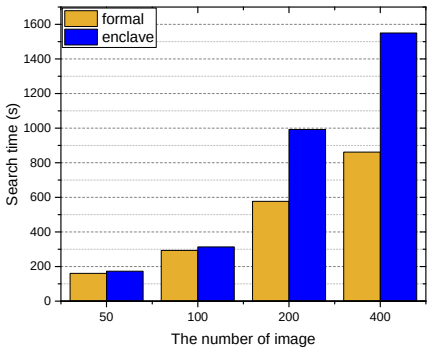

Figure 6: The comparison of search time between formal environment and enclave environment

AC-ISECCA-201702) and the Fundamental Research Funds for the Central Universities.

References

References

[1] Intel software guard extensions programming reference. *https://software.intel.com/en-us/sgx*, 2016.

[2] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. Order preserving encryption for numeric data. In *ACM SIGMOD International Conference on Management of Data*, pages 563–574, 2004.

[3] M. Barni, P. Failla, R. Lazzeretti, A. R. Sadeghi, and T. Schneider. Privacy-preserving ecg classification with branching programs and neural networks. *IEEE Transactions on Information Forensics and Security*, 6(2):452–468, 2011.

[4] Herbert Bay, Andreas Ess, Tinne Tuytelaars, and Luc Van Gool. Speeded-up robust features (surf). *Computer Vision and Image Understanding*, 110(3):346–359, 2008.

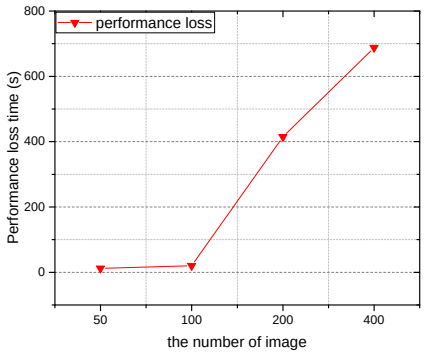

Figure 7: The performance loss of search cost in enclave environment

[5] Alexandra Boldyreva, Nathan Chenette, Younho Lee, and Adam Oneill. Order-preserving symmetric encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 224–241. Springer, 2009.

[6] Zvika Brakerski and Vinod Vaikuntanathan. Fully homomorphic encryption from ring-lwe and security for key dependent messages. In *Cryptology Conference*, pages 505–524, 2011.

[7] Xiaofeng Chen, Jin Li, Jian Weng, Jianfeng Ma, and Wenjing Lou. Verifiable computation over large database with incremental updates. *IEEE transactions on Computers*, 65(10):3184–3195, 2014.

[8] T. Dharani and I. Laurence Aroquiaraj. A survey on content based image retrieval. In *International Conference on Pattern Recognition, Informatics and Mobile Engineering*, pages 485–490, 2013.

[9] David Evans, Yan Huang, Jonathan Katz, and Lior Malka. Efficient privacy-preserving biometric identification. In *Proceedings of the 17th conference Network and Distributed System Security Symposium, NDSS*, 2011.

[10] Gentry and Craig. Fully homomorphic encryption using ideal lattices. *Stoc*, 9(4):169–178, 2009.

[11] R. M HARACLICK. Texture features for image classification. *IEEE Trans Smc*, 3(6):610–621, 1973.

[12] Bay Herbert, Tuytelaars Tinne, and Gool Luc Van. Surf: Speeded up robust features. *European Conference on Computer Vision*, pages 404–417, 2006.

[13] Zhongwen Hu, Zhaocong Wu, Qian Zhang, Qian Fan, and Jiahui Xu. A spatially-constrained colortexture model for hierarchical vhr image segmentation. *IEEE Geoscience and Remote Sensing Letters*, 10(1):120–124, 2013.

[14] Jing Huang, S. Ravi Kumar, Mandar Mitra, Wei Jing Zhu, and Ramin Zabih. Image indexing using color correlograms. In *1997 IEEE Computer Society Conference on Conference on Computer Vision and Pattern Recognition*, pages 762–768, 1997.

[15] Herv Jegou, Matthijs Douze, and Cordelia Schmid. Hamming embedding and weak geometry consistency for large scale image search. *Proc Eccv*, 5302:304–317, 2008.

[16] Kaitai Liang, Cheng Kang Chu, Xiao Tan, Duncan S. Wong, Chunming Tang, and Jianying Zhou. Chosen-ciphertext secure multi-hop identity-based conditional proxy re-encryption with constant-size ciphertexts. *Theoretical Computer Science*, 539(9):87–105, 2014.

[17] David G Lowe. Object recognition from local scale-invariant features. In *The proceedings of the seventh IEEE international conference on Computer vision*, volume 2, pages 1150–1157. IEEE, 1999.

[18] David G. Lowe and David G. Lowe. Distinctive image features from scale-invariant keypoints. *International Journal of Computer Vision*, 60(2):91–110, 2004.

[19] Chun Shien Lu. Homomorphic encryption-based secure sift for privacy-preserving feature extraction. *Proceedings of SPIE - The International Society for Optical Engineering*, 7880(2):788005, 2010.

[20] Xudong Lv and Z. Jane Wang. Perceptual image hashing based on shape contexts and local feature points. *IEEE Transactions on Information Forensics and Security*, 7(3):1081–1093, 2012.

[21] Frank McKeen, Ilya Alexandrovich, Alex Berenzon, Carlos V Rozas, Hisham Shafi, Vedvyas Shanbhogue, and Uday R Savagaonkar. Innovative instructions and software model for isolated execution. *HASP@ ISCA*, 10, 2013.

[22] Margarita Osadchy, Benny Pinkas, Ayman Jarrous, and Boaz Moskovich. Scifi-a system for secure face identification. In *2010 IEEE Symposium on Security and Privacy (SP)*, pages 239–254. IEEE, 2010.

[23] Greg Pass, Ramin Zabih, and Justin Miller. Comparing images using color coherence vectors. In *ACM International Conference on Multimedia*, pages 65–73, 1997.

[24] Eric Persoon and King Sun Fu. Shape discrimination using fourier descriptors. *Systems Man and Cybernetics IEEE Transactions on*, 7(3):170–179, 1977.

[25] Heng Qi, Keqiu Li, Yanming Shen, and Wenyu Qu. An effective solution for trademark image retrieval by combining shape description and feature matching. *Pattern Recognition*, 43(6):2017–2027, 2010.

[26] Zhan Qin, Jingbo Yan, Kui Ren, Chang Wen Chen, and Cong Wang. Towards efficient privacy-preserving image feature extraction in cloud computing. In *ACM International Conference on Multimedia*, pages 497–506, 2014.

[27] Ahmad Reza Sadeghi, Thomas Schneider, and Immo Wehrenberg. Efficient privacy-preserving face recognition. In *International Conference on Information Security and Cryptology*, pages 229–244, 2009.

[28] Baoming Shan and Fengying Cui. Image matching based on local invariant feature and histogram-based similar distance. *International Workshop on Education Technology and Computer Science*, pages 1030–1033, 2009.

[29] J. R. Smith and Shih Fu Chang. Single color extraction and image query. In *International Conference on Image Processing*, page 3528, 1995.

[30] Komal Vijay and Pratap Singh Patwal. Texture features for image retrieval. *Chief Patron National Advisory Board*, pages 313–344, 2002.

[31] Hao Wang, Zhihua Zheng, Lei Wu, and Ping Li. New directly revocable attribute-based encryption scheme and its application in cloud storage environment. *Cluster Computing*, 20(3):2385–2392, 2017.

[32] Qian Wang, Shengshan Hu, Jingjun Wang, and Kui Ren. Secure surfing: Privacy-preserving speeded-up robust feature extractor. In *IEEE International Conference on Distributed Computing Systems*, pages 700–710, 2016.

[33] Can Xiang, Chunming Tang, Yunlu Cai, and Qiuxia Xu. Privacy-preserving face recognition with outsourced computation. *Soft Computing*, 20(9):3735–3744, 2016.

[34] Hongyang Yan, Xuan Li, Yu Wang, and Chunfu Jia. Centralized duplicate removal video storage system with privacy preservation in iot. *Sensors*, 18(6):1814, 2018.

[35] Tingxin Yan, Vikas Kumar, and Deepak Ganesan. Crowdsearch:exploiting crowds for accurate real-time image search on mobile phones. pages 77–90, 2010.

[36] Tom Yeh, Kristen Grauman, Konrad Tollmar, and Trevor Darrell. A picture is worth a thousand keywords:image-based object search on a mobile platform. pages 2025–2028, 2005.

[37] Han Zu Yuan. Implementation of surf feature point extraction algorithm in pacs image processing. *Electro-Optic Technology Application*, (5):49–53, 2013.

[38] Jiawei Yuan, Shucheng Yu, and Linke Guo. Seisa: Secure and efficient encrypted image search with access control. In *Computer Communications*, pages 2083–2091, 2015.

[39] Saber Zerdoumi, Aznul Qalid Md Sabri, Amirrudin Kamsin, Ibrahim Abaker Targio Hashem, Abdullah Gani, Saqib Hakak, Mohammed Ali Al-Garadi, and Victor Chang. Image pattern recognition in big data: taxonomy and open challenges: survey. *Multimedia Tools and Applications*, (2):1–31, 2017.

[40] Wengang Zhou, Ming Yang, Houqiang Li, Xiaoyu Wang, Yuanqing Lin, and Qi Tian. Towards codebook-free: Scalable cascaded hashing for mobile image search. *IEEE Transactions on Multimedia*, 16(3):601–611, 2014.

[41] Hongfei Zhu, Yu-an Tan, Liehuang Zhu, Xianmin Wang, Quanxin Zhang, and Yuanzhang Li. An identity-based anti-quantum privacy-preserving blind authentication in wireless sensor networks. *Sensors*, 18(5):1663, 2018.

[42] Qin Zou, Jianfeng Wang, Jun Ye, Jian Shen, and Xiaofeng Chen. Efficient and secure encrypted image search in mobile cloud computing. *Soft Computing*, pages 1–11, 2016.