ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Content-Based Image Retrieval Scheme with a Privacy-Preserving and Copy-Deterrence in Cloud Computing

Mishal Anand[1], Kartik Sharma[2], Syeda Ayesha Unisa[3], Dr. K S Jagadeesh Gowda[4]

U.G. Student, Department of Computer Engineering, Sri Krishna Institute of Technology, Bengaluru, Karnataka India[1]

U.G. Student, Department of Computer Engineering, Sri Krishna Institute of Technology, Bengaluru, Karnataka India[2]

Assistant Professor, Department of Computer Engineering, Sri Krishna Institute Technology Bengaluru, Karnataka India[3]

Head of Department, Department of Computer Engineering, Sri Krishna Institute Technology Bengalurulu, India[4]

ABSTRACT: For privacy-preserving purposes, sensitive images, such as medical and personal images, need to be encrypted before outsourcing, which makes the CBIR technologies in plaintext domain to be unusable. weare introducing a scheme that supports CBIR over encrypted images without leaking the sensitive information to the cloud server. Firstly, feature vectors are extracted to represent the corresponding images. After that, the pre-filter tables are constructed by locality-sensitive hashing to increase search efficiency. Moreover, the feature vectors are protected by the secure kNN algorithm, and image pixels are encrypted by a standard stream cipher. In addition, considering the case that the authorized query users may illegally copy and distribute the retrieved images to someone unauthorized, we propose a watermark-based protocol to deter such illegal distributions. In our watermark-based protocol, a unique watermark is directly embedded into the encrypted images by the cloud server before images are sent to the query user.when an illegal image copy is found, the unlawful query user who distributed the image can be traced by the watermark extraction.

KEYWORDS: Searchable encryption, content-based image retrieval, secures kNN, copy deterrence, watermark.

I. INTRODUCTION

CBIR services typically incur high storage and computation complexities. Cloud computing offers a great opportunity for the on-demand access to ample computation and storage resources, which makes it an attractive choice for the image storage and CBIR outsourcing. Different from common watermarking techniques, the proposed protocol needs to embed the watermark directly into the encrypted images via the cloud server. After receiving the encrypted and watermarked images, the query user needs to decrypt the images directly. And the decryption should not affect the watermark in the images.we protects the privacy of image data in CBIR outsourcing applications against a curious cloud server and the dishonest query users.

An index of two layers is constructed. Four typical visual descriptors, which are defined in MPEG-7, are employed in our scheme. Meanwhile, the feature vectors are encrypted by the secure kNN algorithm.

The existing searchable encryption schemes usually con-sider that the query users are fully trustworthy. This is not necessarily true in real-world applications. To the best of our knowledge, this paper is the first work that proposes a searchable encryption scheme, considering the dishonest query users who may distribute the retrieved images to those who are unauthorized. A watermark-based protocol is designed for the copy-deterrence purpose. Specifically, after completing the search operation requested by an image user, a unique watermark associated with the image user is

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

imperceptibly embedded into the retrieved images. Then, the watermarked images are sent to the image user. When an illegal copy of the image is found, the unlawful query user who made the illegal distribution can be traced by the watermark extraction. This will help to deter the illegal distribution.

II.RELATED WORK

In the area of privacy-preserving CBIR schemes, Lu *etal*. Constructed the first privacy-preserving CBIR scheme over the encrypted images. The authors extracted the visual words to represent the images, and then calculated the Jaccard similarity between the two sets of visual words so as to evaluate the similarity between the two corresponding images. The order-preserving encryption and min-hash algorithm are employed to protect the information of the visual words. In another work, Lu *etal* .investigated three image feature protection techniques, i.e. the bitplane randomization, random projection, and randomized unary encoding. The features encrypted with the bit plane randomization and the randomized unary encoding can be used to calculate the Hamming distance in the encryption domain. The features encrypted with the random projection can be used to calculate the L1 distance in the encryption domain. Cheng *etal.* designed a CBIR system by combining the bit plane randomization and random projection. Xia *etal.* proposed a privacy-preserving CBIR scheme using local features and earth mover's distance (EMD). For the copy-deterrence purpose, we need to embed watermark into all the retrieved images for each query request. It requires high computational complexity and thus is expected to be completed by the cloud server. Therefore, we need to employ a watermarking method that is efficient and can embed the watermark directly in the encrypted image by the cloud server. After receiving the encrypted and watermarked images, the query user should be able to directly decrypt the watermarked im-ages with the predefined secret keys. After the decryption, the watermark is still contained in the image.

III.METHODOLOGY

Watermark certification authority (WCA) is a trusted agency who takes the responsibilities to generate watermarks for the authorized query users and execute the arbitration through the watermark extraction algorithm.

OVERVIEW OF ZHANG'S ALGORITHM

$C \leftarrow$ ImgEnc(K, M)

1. For each grayscale image $m \in M$,

1) Generate the secret key with a one-way pseudorandom number generator as StreamKey $\leftarrow$ $P\ RN\ G(k_{img}$, ID(m)). The size of*StreamKey*is the same as the image m, and the numbers in *StreamKey* are integers in the range of [0,255] as the pixels in grayscale images.

2. For each pixel in m,

a) Denote the pixel value at position (i, j) as $p_{i;j}$, and the bits of $p_{i;j}$ are computed as $p_{i;j;k} = \lfloor p_{i;j}/2^k \rfloor \bmod 2$, $k = 0, 1, ..., 7$. Similarly, denote the value of *StreamKey*at position(i, j)as$b_{i;j}$, and the bits of $bi;j$ are computed as $b_{i;j;k} = \lfloor b_{i;j}/2^k \rfloor \bmod 2$, $k = 0, 1, ..., 7$.

b) Encrypt the pixel value as $e_{i;j;k} = p_{i;j;k} \otimes b_{i;j;k}$, for

3. Output the encrypted image collection C.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

$M_q \leftarrow \text{ImgDec}(K, R')$

1. For each image $m' \in R'$,

1) Obtain the secret key as $StreamKey \leftarrow PRNG(k_{img}, \text{ID}(m'))$.

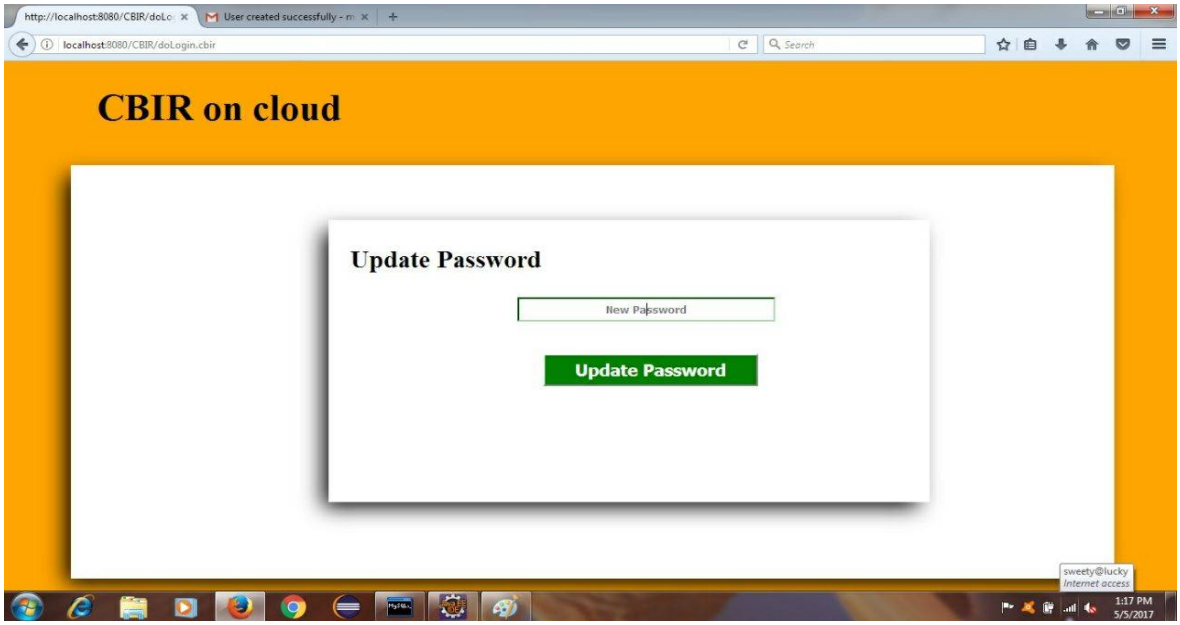
2) For each pixel in m',

a) Denote the pixel value of m' at position (i, j) as $e_{i;j}'$, and the bits of $e_{i;j}'$ are computed as $e_{i;j;k}' = \lfloor e_{i;j}'/2^k \rfloor \bmod 2$, $k = 0, 1, ..., 7$. Similarly, denote thevalue of $StreamKey$ at position (i, j) as $b_{i;j}$, and the bits of $b_{i;j}$ are computed as $b_{i;j;k} = \lfloor b_{i;j}/2^k \rfloor \bmod 2$, $k = 0, 1, ..., 7$.

b) Decrypt the pixel value as $p'_{i;j;k} = e'_{i;j;k} \otimes b_{i;j;k}$, for $k = 0, 1, ..., 7$.

2. Output decrypted image collection M_q.

IV.EXPERIMENTAL RESULTS



ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

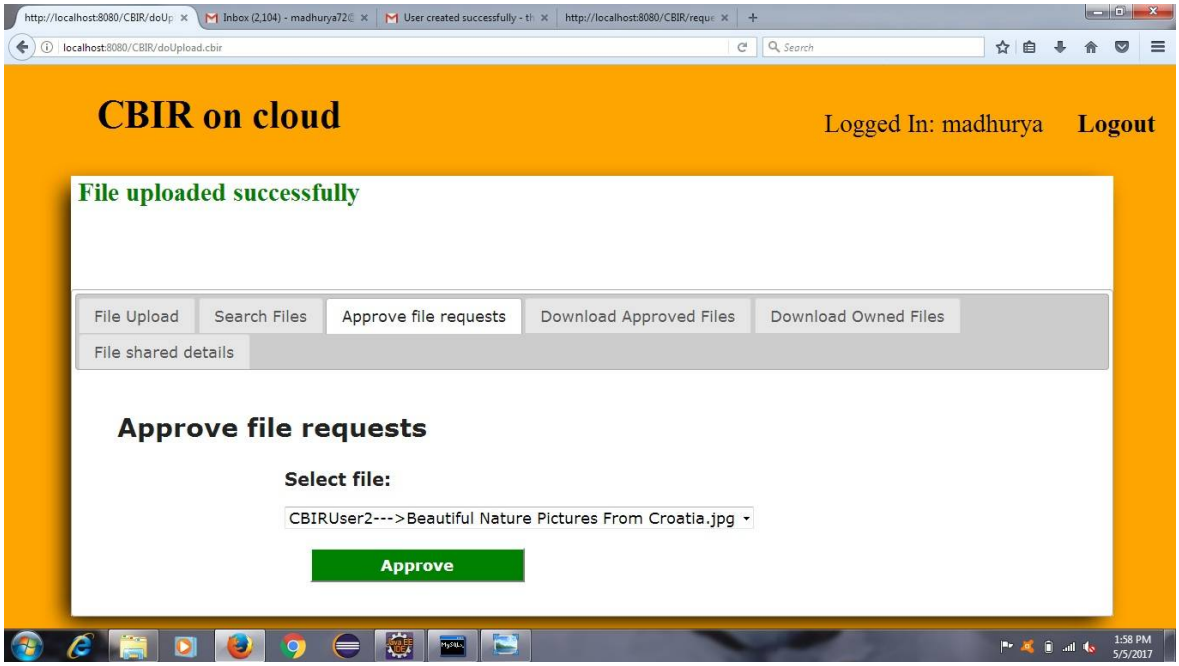
An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India



V. CONCLUSION

For the first time, we consider the dishonest users in SE schemes and propose a watermark-based protocol to deter the illegal distribution of images. Overall, the image features are secure against Ciphertext-only Attack model, the image contents are secure against Chosen-plaintext Attack model, and the search efficiency is improved from O(n) to O(n′). As future works, there still are some aspects could be improved. Firstly, the proposed watermarking method cannot be regarded as a very robust one. Secondly, a small parameter α will cause a limited number of available watermarks. In the future, we will make more efforts to design watermarking algorithm with better robustness and embedding capacity.

REFERENCES

[1]. S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," in *Financial Cryptography and Data Security*. Springer, 2013, pp. 258–274.
[2]. D. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner, "Dynamic searchable encryption in very large databases: Data structures and implementation," in *Proc. of Network and DistributedSystem Security Symposium*, vol. 14, 2014.
[3]. Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, "Mutual verifiable provable data auditing in public cloud storage," *Journal of Internet Technology*, vol. 16, no. 2, pp. 317–323, 2015.
[4]. J. Shashank, P. Kowshik, K. Srinathan, and C. Jawahar, "Private content based image retrieval," in *Proc. of IEEE Conference on Computer Vision*
[5]. P. Zheng and J. Huang, "An efficient image homomorphic encryption scheme with small ciphertext expansion," in *Proc. of 21st ACM international conference on Multimedia*. ACM, 2013, pp. 803–812.
[6]. Z. Qin, J. Yan, K. Ren, C. W. Chen, and C. Wang, "Towards efficient privacy-preserving image feature extraction in cloud computing," in *ACM International Conference on Multimedia*. ACM, 2014, pp. 497–506.
[7]. Z Xia, X. Wang, X. Sun, and B. Wang, "Steganalysis of least significant bit matching using multi-order differences," *Security and Communication Networks*, vol. 7, no. 8, pp. 1283–1291, 2014.
[8]. W. Lu, A. Swaminathan, A. L. Varna, and M. Wu, "Enabling search over encrypted multimedia databases," in *Proc. of IS&T/SPIE ElectronicImaging*. International Society for Optics and Photonics, 2009, pp.725 418–725 418.