Impact Factor Value: 4.029 ISSN: 2349-7084
International Journal of Computer Engineering In Research Trends
Volume 4, Issue 6, June-2017, pp. 231-235 www.ijcert.org

Content-Based Image Retrieval in Cloud Using Watermark Protocol and Searchable Encryption

R.Santhi*[1], Dr.D.Yuvaraj[2]

*M.E (CSE) Final year, Computer Science and Engineering, M.I.E.T Engineering College, Trichy
Head and Professor, Computer Science and Engineering, M.I.E.T Engineering College, Trichy

[1] anandsanthi@rediffmail.com

[2] contactyuvraj199@gmail.com

Abstract :-With the development of the imaging devices, such as digital cameras, smartphones, and medical imaging equipments, our world has been witnessing a tremendous growth in quantity, availability, and importance of images. The needs of efficient image storage and retrieval services are reinforced by the increase of large-scale image databases among all kinds of areas. Compared with text documents, images consume much more storage space. Hence, its maintenance is considered to be a typical example for cloud storage outsourcing. 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. In order to secure the data in cloud, the proposed system 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, a watermark-based protocol is used to deter such illegal distributions. In 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. Hence, when an illegal image copy is found, the unlawful query user who distributed the image can be traced by the watermark extraction.

Keywords: CBIR (Content-Based Image Retrieval), kNN algorithm, watermark, encrypted image.

1. Introduction

With the development of the imaging devices, such as digital cameras, smartphones, and medical imaging equipment, our world has been witnessing a tremendous growth in quantity, availability, and the importance of images. The needs of efficient image storage and retrieval services are reinforced by the increase of large-scale image databases among all kinds of areas. Meanwhile, after more than twenty years of development, CBIR techniques show the potential of usefulness in many real-world applications. For example, clinicians can use CBIR to find similar cases of patients and facilitate clinical decision-making processes. However, a large image database usually consists of millions of images. Therefore, 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.

By outsourcing CBIR services to the cloud server, the data owner is relieved from maintaining local image database and interacting with database users online. Despite the tremendous benefits, image privacy becomes the main concern with CBIR outsourcing. For example, patients may not want to disclose their medical images to any others except to a specific doctor in medical CBIR applications. To formulate the problem, this paper considers two types of privacy threats. Firstly, a curious cloud server may look into the owner's database for additional information. Secondly, after receiving the retrieved images, the query user may illegally distribute these images to someone unauthorized for benefits.

2. Literature review

The privacy-preserving framework is used to outsourced storage, search, and retrieval of images in large-scale, dynamically updated repositories. This framework is composed of two main components: an image encryption component, executed on client devices;

and storage, indexing, and searching component (in the encrypted domain), implemented in the outsourcing server (e.g. a cloud provider). It is based on a new encryption scheme specifically designed for images, called IES-CBIR. IES-CBIR allows us to design outsourced image repository systems that support content-based image retrieval (CBIR) based on color features while protecting the privacy of both image owners and other users issuing queries. Figure 1 represents system architecture of the existing system.

Comparing with state-of-art, IES-CBIR shows comparable retrieval precision and higher computational performance than previous approaches as perceived by the clients, since it securely moves indexing computations to the cloud provider's infrastructure and avoids public-key and Homomorphic cryptography. IES-CBIR also minimizes ciphertext expansion and consequently bandwidth and outsourced space requirements, reinforcing the positive impact on user-perceived latency[2].

Limitations of Existing System

1. PCBIR scheme which protects the privacy of the query image, but exposing the unencrypted image database to the server directly.
2. High computation and storage burden Image retrieval accuracy is low.
3. None of these schemes consider the dishonest query users who may illegally distribute the retrieved images.

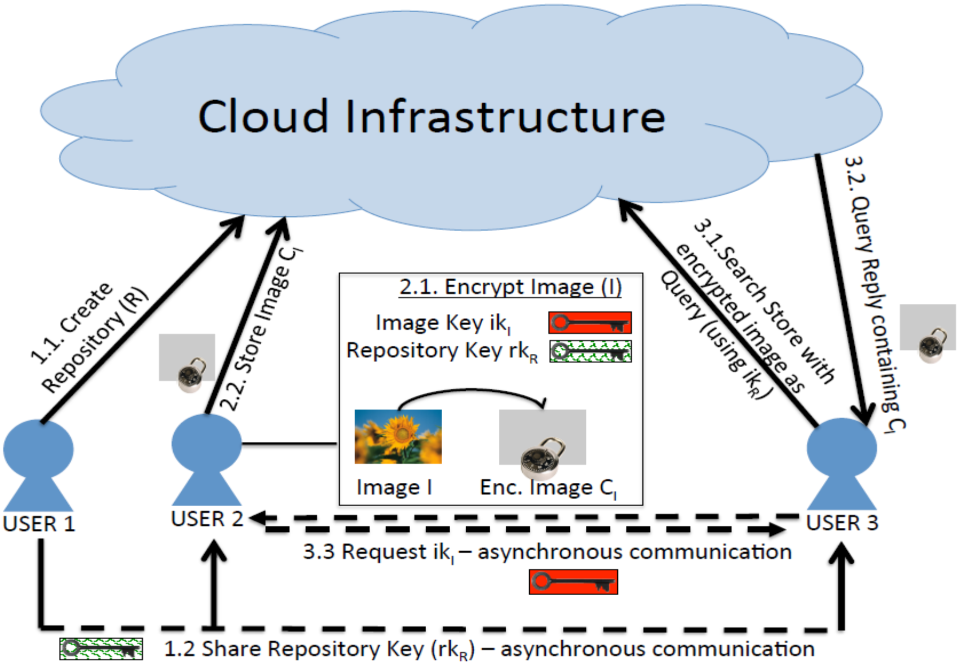
Cloud Infrastructure
1.1. Create Repository (R)
2.2. Store Image C_I
2.1. Encrypt Image (I)
Image Key ik_I
Repository Key rk_R
Image I
Enc. Image C_I
3.1.Search Store with encrypted image as Query (using ik_R)
3.2. Query Reply containing C_I
USER 1
USER 2
USER 3
3.3 Request ik_I – asynchronous communication
1.2 Share Repository Key (rk_R) – asynchronous communication

Figure 1: System Architecture of Existing System

3.Proposed Work

With the development of the imaging devices, such as digital cameras, smart phones, and medical imaging equipments, our world has been witnessing a tremendous growth in quantity, availability, and importance of images. The needs of efficient image storage and retrieval services are reinforced by the increase of large-scale image databases among all kinds of areas. Compared with text documents, images consume much more storage space. Hence, its maintenance is considered to be a typical example for cloud storage outsourcing. 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. In order to secure the data in cloud, the proposed system 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, a watermark-based protocol is used to deter such illegal distributions. In 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. Hence, when an illegal image copy is found, the unlawful query user who distributed the image can be traced by the watermark extraction[1]. The system model is sub divided into four different entities: the image owner, image user, cloud server and watermark certification authority (WCA).

Image owner outsource his local data, i.e., a collection of *n* images *M= {m*1,*m*2, ...,*mn}*, to the cloud server in the encrypted form *C* = *{c*1, *c*2, ..., *cn}*. Firstly, the image owner extracts the feature vectors *F* = *{f*1, *f*2, ..., *fn}* from *M*, and then constructs a secure searchable index *I* on *F*. Next, both the encrypted image collection *C* and index *I* are outsourced to the cloud server. The image owner also takes the responsibility to authorize image users through a certain secure method. The image owner sends the authentication information of authorized users to the cloud server who will take the responsibility to verify the identity of user in search requests. In addition, the image owner sends the identities of the authorized users to WCA for watermark generation. Only a single image owner is considered. However, if there are multiple image owners in our scheme and all the owners have the same set of users, the owners can encrypt the indexes under the same cryptosystem and secret keys so that the users can search images from all of these owners. But if the sets of authorized users are different for each of image owners, the owners need to encrypt their images and indexes with their particular keys. Accordingly, the user can only search from the corresponding owners. In addition, if some image owners share a part of users, one can resort to some sophisticated methods to efficiently manage the authorization of users. Attribute-based encryption methods could be a good choice.

Image users are the authorized ones to retrieve images from the cloud server. To request a search, the image user firstly generates a trapdoor *TD* for the query image, and then submits the trapdoor *TD* and his identity to the cloud server. After receiving the resulting images, the user can decrypt them with the secret key shared by the image owner.

Cloud server stores the encrypted image collection *C* and the index *I* for the image owner and processes the query requests from image users. Besides, in order to support copy deterrence, the cloud server takes the responsibility to embed the watermark into the retrieved images.

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. Figure 2 represents system architecture of proposed system.

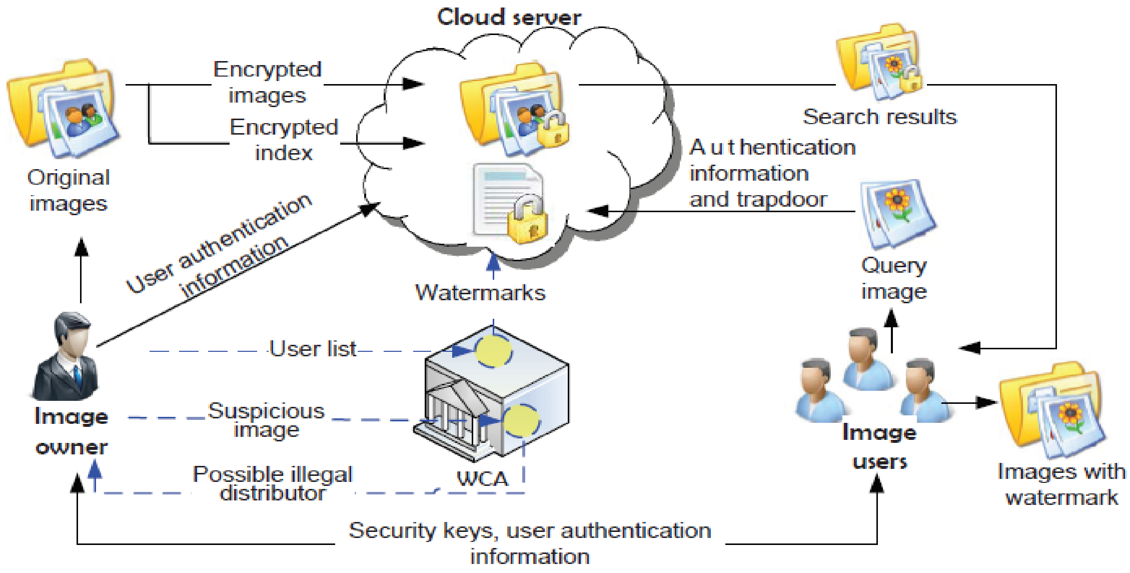

Figure 2: System Architecture of Proposed System

4.Conclusion

The proposed system 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, a watermark-based protocol is used to deter such illegal distributions. In 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. Hence, when an illegal image copy is found, the unlawful query user who distributed the image can be traced by the watermark extraction.

References

[1] Zhihua Xia, Xinhui Wang, Liangao Zhang, Zhan Qin, Xingming Sun, Kui Ren, "A Privacy-preserving and Copy-deterrence Content-based Image Retrieval Scheme in Cloud Computing" IEEE TRANSCATION ON INFORMATION FORENSIC AND SECURITY, VOL.11, NO. 11, NOVEMBER 2016.

[2] B. Ferreira, J. Rodrigues, J. Leit˜ao, and H. Domingos, "Privacypreserving content-based image retrieval in the cloud," arXiv preprint arXiv:1411.4862, 2014.

[3] A. Rial, M. Deng, T. Bianchi, A. Piva, and B. Preneel, "A provably secure anonymous buyer–seller watermarking protocol," Information Forensics and Security, IEEE Transactions on, vol. 5, no. 4, pp. 920– 931, 2010.

[4] Carson, C., Thomas, M., Belongie, S., Hellerstein, J. M. and Malik, J. 1999. Blobworld: A system for region-based image indexing and retrieval. In Proceedings of the Third International Conference on Visual Information and Information Systems, Springer-Verlag, London, UK. 509-516.

[5] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," in Proc. of INFOCOM. IEEE, 2012, pp. 451–459.

[6] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology-Eurocrypt. Springer, 2004, pp. 506–522.

[7] S. Anto, S. Chandramathi," An Expert System based on SVM and Hybrid GA-SA Optimization for Hepatitis Diagnosis,", International Journal of Computer Engineering In Research Trends, 2(7):437-443, 2015.

[8] F. Long, H. J. Zhang, and D. D. Feng, "Fundamentals of Content-based Image Retrieval," in Multimedia Information Retrieval and Management, D. Feng Eds,Springer, 2003.

[9] Shivangi Jindal, Harkiran Kaur, "Intensification of Resolution in the Realm of

[10] Digital Imaging," International Journal of Computer Engineering In Research Trends, 3(6):343-346,2016.

[11] J. C. Bezdek, "Pattern Recognition with Fuzzy Objective Function Algorithms", New York: Plenum Press, 1981.

[12] Ma, W. and Manjunath, B.S. (1999) NeTra: a toolbox for navigating large image databases. Multimedia Systems, Springer-Verlag, Berlin, Germany. 7(3), 184-198.

[13] Nbhan D. Salih , David Chek Ling Ngo, " A novel method for shape representation," GVIP 05 Conference, 19-21 December 2005.

[14] Ravichandran K. and Ananthi B., "Color Skin Segmentation Using K-Means Cluster, " International Journal of Computational and Applied Mathematics, vol.4, no.2, pp. 153-157 , 2009.

[15] Rui, Y., Huang, T. S. and Mehrotra, S. 1997. Content-based image retrieval with relevance feedback in MARS. In Proceedings of International Conference on Image Processing. 2, 815-818.

[16] S. Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative watermarking and encryption for media data," Optical Engineering, vol. 45, no. 8, pp. 080 510–080 510, 2006.

[17] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacypreserving multi-keyword text search in the cloud supporting similaritybased ranking," in Proc. of 8th ACM SIGSAC symposium on Information, computer and communications security.

[18] 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.

[19] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Transactions on Parallel & Distributed Systems, vol. PP, no. Online, pp. 1–1, 2015.