Volume 1, Issue 8, November 2016 ISSN: 2456-0006
International Journal of Science Technology Management and Research
Available online at: www.ijstmr.com

Survey on Increase Robustness and Privacy of Content-Based Image Retrieval in Cloud Computing using Watermark-Based Protocol

Sonal H. Kunte
Department of Computer
Gokhale Education Society's, R. H. Sapat College of Engineering, Management Studies and Research, Nashik (M.S.), INDIA

Shivaji R.Lahane
Department of Computer
Gokhale Education Society's, R. H. Sapat College of Engineering, Management Studies and Research, Nashik (M.S.), INDIA

Abstract: ***Content-based image retrieval (CBIR) are easy to manipulate and edit due to availability of powerful image processing and cloud computing environment. Searchable encryption (SE) scheme allows image users to search over encrypted data collection. Nowadays, it is possible to do retrieval with preserving privacy by encrypting it before outsourcing and with copy-deterrence so that unauthorized image users will not get access to it. Also tried to increase robustness of CBIR. Watermark certification authority (WCA) is a trusted agency who generate watermark-based protocol for copy deterrence to avoid illegal distribution. Generating a unique watermark and directly Embedding it into the encrypted images by the cloud server before images are sent to the query user is one of the critical challenge WCA. The image integrity verification as well as generating trapdoor for retrieval in this environment is now days becoming the challenging for image users. Secure kNN algorithm is used to protect feature vectors [2] (SCD,CSD,CLD,EHD) which are used to represent corresponding images. Recently hashing algorithm, auditing and alert generation are used at image users' side for verification purpose. Firstly, Zhangs' algorithm was used for encryption, decryption and generating watermark-based images. But now-a-days, watermark-based protocol is used, which improve robustness.***

Keywords: Content-based image retrieval, copy-deterrence, Watermark certification authority, trapdoor, Secure kNN, feature vectors, watermark.

I. INTRODUCTION

This paper describes the strategy followed by various techniques to retrieve required images. Several authors have been working in recent years on the efficient similarity search over encrypted data [5], preserving privacy [2] and copy deterrence [3] with the help of various visual descriptors [6] such as scalable color descriptor (SCD), Color structure descriptor (CSD), Color layout descriptor (CLD), Edge histogram descriptor (EHD). Indeed, it is well known that, given the different types of descriptors in practice, and availability of watermark-based algorithm, hashing algorithm and secure kNN algorithm [12], it becomes possible to obtain best result. Based on this consideration, we also used alert generation for verification. Unfortunately, the Zhangs' algorithm is not give guaranteed that each watermark bit can be correctly extracted. So, watermark-based protocol is used to improve Zhang's watermarking algorithm to increase the robustness.

A. System Model-:

Mainly, there are 6 types of entities are involved:

1. Image owner
2. Watermark certification authority (WCA)
3. Cloud server
4. Image users
5. Hashing algorithm and auditing
6. Alert generation

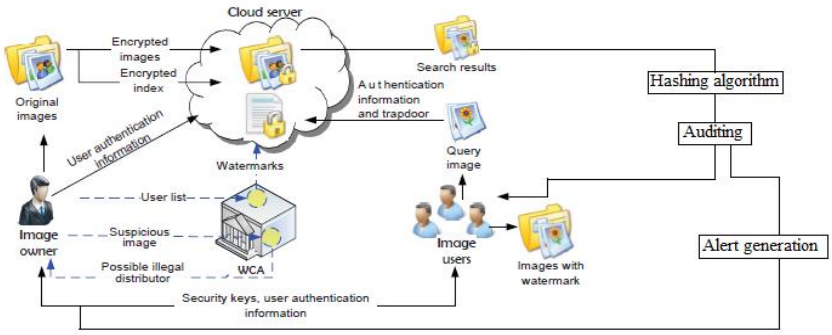

Fig. 1 Framework of the content-based image retrieval using watermark-based protocol.

1. Image owner encrypts original images, index and saves them on cloud server along with user authentication information.
2. Watermark certification authority (WCA) generate watermarks and send them on cloud server.
3. Cloud server embedded watermarks into encrypted images
4. Image users generate trapdoors and then fire required query. According to query, server reply with proper results.
5. Hashing algorithm and auditing is used for verification purpose.
6. If the results are satisfactory to image users, process terminates otherwise alert generation is sent back to image owner.

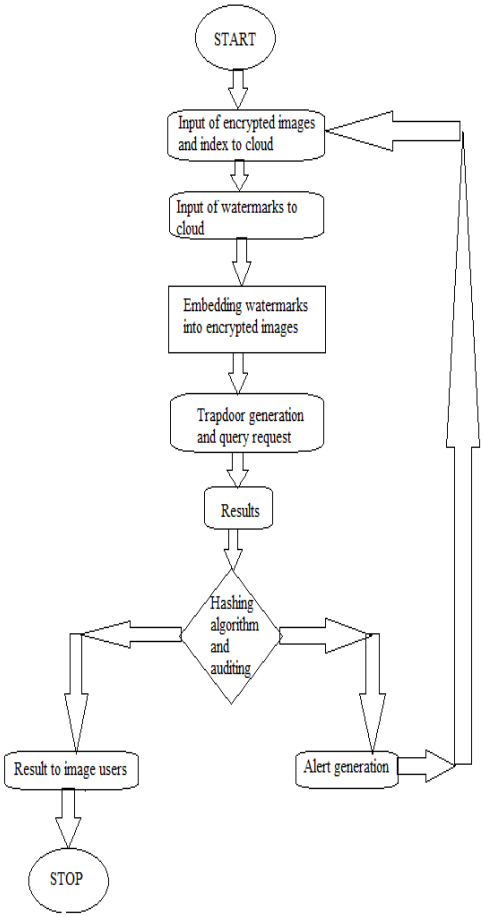

Fig. 2 Flowchart of the content-based image retrieval using watermark-based protocol.

Security keys and user authentication information is shared among image owner and image users. Using these keys and information, encryption and decryption is done at image owner and image users level. Robustness is considered while developing this system model.

We are performing strong literature survey which helps in developing robustness and privacy of content-based image retrieval using various algorithms, at the same time deal with the problems mentioned previously,

- Firstly, Searchable encryption scheme were used which have main focus on Boolean search and retrieval of text document [7].

- Secondly, Private CBIR scheme comes into account who protect privacy of query image [2], but it expose unencrypted image database to the server directly.
- Then, focus turns towards efficient similarity search over encrypted data [3] and Key techniques to privacy preserve of CBIR outsourcing [2].
  Different threat models have been proposed to achieve various search functionalities such as similarity search [8], dynamic search [9], multi-keyword ranked search [10], etc
- Finally, Privacy preserving and copy deterrence techniques are used with watermark-based protocol [4].
- In this paper, along with privacy preserving and copy deterrence, it has tried to increase robustness of CBIR in cloud computing.

II. LITERATURE SURVEY

Zhihua Xia, Member, IEEE, Yi Zhu, Xingming Sun, Senior Member, IEEE, Zhan Qin, Member, IEEE and Kui Ren, Senior Member, IEEE, all in their paper titled "Towards Privacy-preserving Content-based Image Retrieval in Cloud Computing" focused on Content-based image retrieval (CBIR) applications which are rapidly developed along with the increase in the quantity, availability and importance of images in our daily life. In this paper, we propose a privacy-preserving content-based image retrieval scheme, which allows the data owner to outsource the image database and CBIR service to the cloud, without revealing the actual content of the database to the cloud server [01].

Zhihua Xia, Xinhui Wang, Liangao Zhang, Zhan Qin, Xingming Sun, and Kui Ren, all in their paper titled "A Privacy-preserving and Copy-deterrence Content-based Image Retrieval Scheme in Cloud Computing" focused on Content-based Image Retrieval (CBIR) with preserving privacy and copy deterrence in cloud computing. 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. Moreover, the feature vectors are protected by the secure kNN algorithm, and image pixels are encrypted by a standard stream cipher [03].

K. Gopalakrishnan, Nasir Memon, Poorvi L. Vora, all in their paper titled "Protocols for Watermark Verification" focused on adding a watermark signal to the digital image that can later be extracted or detected to make an assertion about the image. Two types of watermarks exist: visible and invisible. Visible watermarks typically contain conspicuously visible messages or company logos indicating the ownership of the image. Invisible watermarks, on the other hand, are unobtrusive modifications to the image and the invisibly watermarked image visually appears similar to the original [04].

B. S. Manjunath, Jens-Rainer Ohm, Vinod V. Vasudevan and Akio Yamada all in their paper titled "Color and Texture Descriptors" focused on presenting an overview of color and texture descriptors that have been approved for the Final Committee Draft of the MPEG-7 standard. The color descriptors in the standard include a histogram descriptor that is coded using the Haar transform, a color structure histogram, a dominant color descriptor, and a color layout descriptor. The three texture descriptors include one that characterizes homogeneous texture regions and another that represents the local edge distribution [06].

Z. Xia, X. Wang, X. Sun, and Q. Wang all in their paper titled "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data " focused on a special tree-based index structure and propose a "Greedy Depth-first Search" algorithm to provide efficient multi-keyword ranked search. The secure kNN algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors [10].

S. Rane and P. T. Boufounos, all in their paper titled "Privacy-preserving nearest neighbor methods: comparing signals without revealing them," focused on the privacy-preserving NN (PPNN) method, in which the reader will find it convenient to divide it into two distinct problems: a method for privacy-preserving distance computation followed by a method for privacy-preserving minimum finding. The choice of mathematical tools used for PPNN as well as the structure and complexity of the resulting protocols are dictated by the privacy model under consideration. These models encapsulate assumptions such as the privacy requirements, the behavior of participating entities, and the possibility of information sharing among the participants [12].

CONCLUSION

In this paper, a through literature survey has been studied by collecting and analyzing 11-12 papers on image processing and cloud computing. Several techniques prefilter tables, descriptors, feature vectors, watermarking etc have been studied. Unlike zhangs' algorithm, which have been proved to be effective in encryption and decryption, my method is to retrieve appropriate images that are saved on cloud server by image owners.

.

ACKNOWLEDGMENT

I am thankful to my guide Prof. S.R.Lahane for his guidance and encouragement. Their expert suggestions and scholarly feedback had greatly enhanced the effectiveness of this work.I would like to express the deepest appreciation to authors Zhihua Xia, Xinhui Wang, Liangao Zhang, Zhan Qin, Xingming Sun, and Kui Ren for their beneficial information and knowledge.

REFERENCE

1. Z. Xia, Y. Zhu, X. Sun, Z. Qin, and K. Ren, "Towards privacy-preserving content-based image retrieval in cloud computing," IEEE Transactions on Cloud Computing, vol. PP, no. 99, pp. 1–1, 2015.
2. 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.
3. Zhihua Xia, Xinhui Wang, Liangao Zhang, Zhan Qin, Xingming Sun, and Kui Ren, "A Privacy-preserving and Copy-deterrence Content-based Image Retrieval Scheme in Cloud Computing", IEEE TRANSCATION ON INFORMATION FORENSIC AND SECURITY, VOL. , NO. , SEPTEMBER 2016.
4. K. Gopalakrishnan, N. Memon, and P. L. Vora, "Protocols for watermark verification," IEEE MultiMedia, no. 4, pp. 66–70, 2001.
5. M. Kuzu, M. S. Islam, and M. Kantarcioglu, "Efficient similarity search over encrypted data," in Proc. of 28th International Conference on Data Engineering. IEEE, 2012, pp. 1156–1167.
6. B. S. Manjunath, J.-R. Ohm, V. V. Vasudevan, and A. Yamada, "Color and texture descriptors," IEEE Transactions on Circuits and Systems for Video Technology, vol. 11, no. 6, pp. 703–715, 2001.
7. 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.
8. M. Kuzu, M. S. Islam, and M. Kantarcioglu, "Efficient similarity search over encrypted data," in Proc. of 28th International Conference on Data Engineering. IEEE, 2012, pp. 1156–1167.
9. Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. PP, no. 99, p. 1,2015.
10. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multikeyword ranked search over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222–233, 2014.
11. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. of 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88.
12. S. Rane and P. T. Boufounos, "Privacy-preserving nearest neighbor methods: comparing signals without revealing them," IEEE Signal Processing Magazine, vol. 30, no. 2, pp. 18–28, 2013.