An encrypted hierarchical index tree by K-means clustering based on Affinity Propagation

[1]A BHAGYA LAKSHMI, [2]B HEMA NAGA MANI

[1,2]Dept. of CSE, V. S. Lakshmi Engineering College for women, Matlapalem, Talarevu Mandal, E.G.dt, AP

ABSTRACT:

Existing security protecting CBIR plans can ensure image protection while supporting image retrieval, these plans actually have inherent defects (i.e., low search accuracy, low search efficiency, key leakage, etc.) To resolve these difficult issues, in this paper we give a comparability Search to Encrypted Images in secure distributed computing (called SEI). To start with, the element descriptors separated by the (CNN) model are utilized to further develop search exactness. Then, a scrambled various leveled record tree by utilizing K-means clustering dependent on (AP) clustering is formulated, which can further develop search proficiency. Then, at that point, a restricted key-leakage (kNN) algorithm is proposed to protect key from being totally leaked to untrusted image clients. At long last, SEI is stretched out to additionally prevent image clients' pursuit data from being presented to the cloud worker. Our formal security examination demonstrates that SEI can ensure image protection just as key protection.

KEYWORDS: Convolutional Neural Network (CNN), Search for Encrypted Images SEI, Affinity Propagation (AP), k-Nearest Neighbor (kNN)

1] INTRODUCTION:

With the quick turn of events and advocacy of cloud computing, individuals appreciate different accommodations brought by cloud administrations, like putting away images on the cloud. Nonetheless, directly outsourcing images to the public cloud definitely raises protection concerns. When the enormous images e.g., patients' medical images) containing profoundly delicate data have been leaked to unapproved substances, it will cause significant outcomes or pointless difficulty. The encryption system can reduce image information security and protection worries somewhat, however it refutes the Content-Based Image Retrieval (CBIR) method over ciphertext, and even causes different concerns examined in the accompanying model.

Example. Alice rethinks the encoded images C of the nearby image data set M to the cloud server. The verified Bob produces a scrambled inquiry demand T as indicated by question image mq by utilizing the accessible key sk shared by Alice when he inquiries images like mq. Then, at that point, the cloud server searchs through C in the wake of getting T and returns significant indexed lists R to Bob. At last, Bob decrypts the R with image encryption key kie from Alice.

2] LITERATURE SURVEY:

2.1] M. Li, M. Zhang, Q. Wang *et al*

Image retrieval is critical for web-based media sites, for example, Instagram to distinguish comparable images and make suggestions for clients who share comparable interests. To dispose of the capacity weight and calculation for image recovery, moving to a remote cloud is presently a pattern. However, security concerns order the utilization of encryption prior to re-appropriating the images. We need a solid way for recovering images from a not-completely confided in worker. This paper proposes Instant CryptoGram, a solid image recovery administration. We first plan another information structure called sub-simhash, which fits for the transformed list utilized by numerous accessible symmetric encryption plans. It prompts our secluded arrangement that upholds productive likeness inquiries and updates over encoded images.

2.2] C. Guo, S. Su, K.-K. R. Choo *et al*

We propose a protected and effective plan to track down the specific closest neighbor over encoded clinical images. Rather than working out the Euclidean distance, we reject competitors by registering the lower bound of the Euclidean distance that is identified with the mean and standard deviation of information. In contrast to most existing plans, our plan can get the specific closest neighbor as opposed to a rough outcome. We, then, at that point, assess our proposed way to deal with show its utility.

3] PROBLEM DEFINTION:

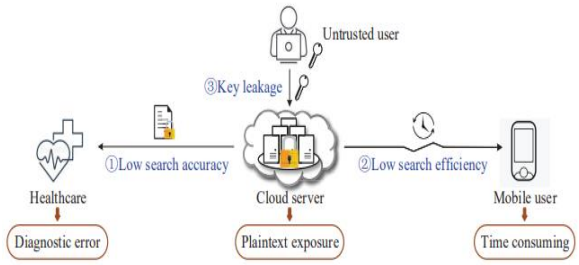
In this encrypted image search process, the cloud server is regarded as semi-trusted. Alice stores her images on this cloud server, and entrusts the cloud server to perform similarity search tasks. When Bob comes to query Alice's images, the cloud server will honestly provide Bob with search service under Alice's arrangement. The performance of search services, such as search accuracy and efficiency, will profoundly affect Bob's search experience. Assuming that Bob is a doctor who relies on search results to diagnose a certain patient's condition, the incorrect search results will lead to a wrong diagnose, which endangers the

patient's health and even life. Besides, the time-consuming search process will prolong the waiting time of the Bob. If Bob is a mobile image user who requires high real-time responses, such a long search time is hard to bear and easily makes search time lose timeliness. Moreover, the above search mechanism still requires Alice to share sk and kie with Bob, which cannot completely protect image privacy. This is because we cannot promise that Bob is fully trusted and does not share sk and kie with other unauthorized image users due to interest incentives in practice.

4] PROPOSED APPROACH:

As far as we know, no existing work is dedicated to solving the above three challenges simultaneously. Hence, in this paper we propose a similarity Search for Encrypted Images in secure cloud computing (SEI) to solve the above challenges. Specifically, we employ the CNN model to extract feature vectors to improve search accuracy, and then build a hierarchical index tree in a bottom-up manner based on the clustering algorithm to improve search efficiency. Besides, we design an optimized ASPE algorithm, which does not require the image owner to share sk with image users, to achieve limited key-leakage for untrusted image users.

5] SYSTEM ARCHITECTURE:



6] PROPOSED METHODOLOGY:

USER

In this application user is a module, here user should register with the application then login. After user successful login he can perform some operations such as generateKey, searchImages, requestStatus and logout

OWNER

In this application user is a module, here user should register with the application then login. After user successful login he can perform some operations such as generateKey, uploadImage, viewRequest and logout.

CLOUD

Here cloud can directly login with the application and after cloud successful login he can perform some operations such as view all images and view all users' requests and logout

7] ALGORITHM:

KNN

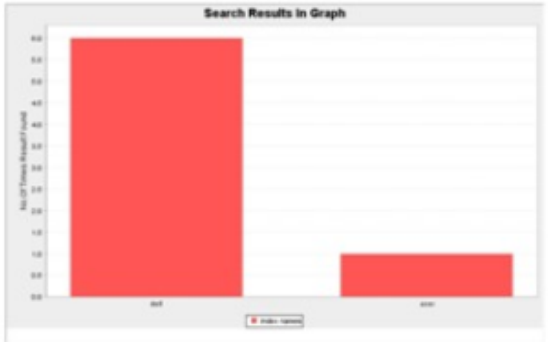
K-Nearest Neighbour is one of the simplest Machine Learning algorithms based on Supervised Learning technique.

K-NN algorithm assumes the similarity between the new case/data and available cases and put the new case into the category that is most similar to the available categories.

K-NN algorithm stores all the available data and classifies a new data point based on the similarity. This means when new data appears then it can be easily classified into a well suite category by using K- NN algorithm.

8] RESULTS:

Image database update



Search results for images index

9] CONCLUSION:

We examine similarity search for scrambled images in secure distributed computing. Solidly, we present a grouping improvement strategy and give the plan technique for the various leveled record tree. With these two methods, SEI can productively play out the recovery cycle and accomplish high exactness dependent on highlights removed by the CNN model. Further, we consider untrusted image clients in SEI and henceforth propose a similitude estimation technique with restricted key-spillage. We likewise give severe security examination and lead probes a genuine world dataset, which show that SEI is secure and feasible in practice.

10] EXTENSION WORK:

Supporting dynamic update: We will develop a way to build an efficient index and enable support dynamic update of image databases.

Supporting verifiable: The image user who receives the search results in the image search can verify the results.

11] REFERENCES:

[1] C.-Y. Hsu, C.-S. Lu, and S.-C. Pei, "Image feature extraction in encrypted domain with privacy-preserving sift," IEEE transactions on image processing, vol. 21, no. 11, pp. 4593–4607, 2012.

[2] M. Li, M. Zhang, Q. Wang, S. S. Chow, M. Du, Y. Chen, and C. Lit, "Instantcryptogram: Secure image retrieval service," in IEEE INFOCOM 2018-IEEE Conference on Computer Communications. IEEE, 2018, pp. 2222–2230.

[3] Z. Xia, N. N. Xiong, A. V. Vasilakos, and X. Sun, "Epcbir: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing," Information Sciences, vol. 387, pp. 195–204, 2017.

[4] M. Shen, G. Cheng, L. Zhu, X. Du, and J. Hu, "Content-based multi-source encrypted image retrieval in clouds with privacy preservation," Future Generation Computer Systems, 2018.

[5] C. Guo, S. Su, K.-K. R. Choo, and X. Tang, "A fast nearest neighbor search scheme over outsourced encrypted medical images," IEEE Transactions on Industrial Informatics, 2018.

[6] X. Wang, J. Ma, X. Liu, and Y. Miao, "Search in my way: Practical outsourced image retrieval framework supporting unshared key," in Proc. IEEE Conference on Computer Communications (INFOCOM'19). IEEE, 2019, pp. 2485–2493.

[7] H. Liang, X. Zhang, Q. Wei, and H. Cheng, "Secure image retrieval with multiple keys," Journal of Electronic Imaging, vol. 27, no. 2, p. 023032, 2018.

[8] 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. 6, no. 1, pp. 276–286, 2015.

[9] B. Cheng, L. Zhuo, Y. Bai, Y. Peng, and J. Zhang, "Secure index construction for privacy-preserving large-scale image retrieval," in 2014 IEEE Fourth International Conference on Big Data and Cloud Computing. IEEE, 2014, pp. 116–120.

[10] X. Li, Q. Xue, and M. C. Chuah, "Casheirs: Cloud assisted scalable hierarchical encrypted based image retrieval system," in IEEE INFOCOM 2017-IEEE Conference on Computer Communications. IEEE, 2017, pp. 1–9.

[11] W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure knn computation on

encrypted databases," in Proceedings of the 2009 ACM SIGMOD International Conference on Management of data. ACM, 2009, pp. 139–152.

[12] L. Zhang, T. Jung, C. Liu, X. Ding, X.-Y. Li, and Y. Liu, "Pop: Privacy-preserving outsourced photo sharing and searching for mobile devices," in 2015 IEEE 35th International Conference on Distributed Computing Systems. IEEE, 2015, pp. 308–317.

[13] J. Yuan, S. Yu, and L. Guo, "Seisa: Secure and efficient encrypted image search with access control," in Proc. IEEE conference on computer communications (INFOCOM'15). IEEE, 2015, pp. 2083– 2091.

[14] Y. Zhu, Z. Wang, and Y. Zhang, "Secure k-nn query on encrypted cloud data with limited key-disclosure and offline data owner," in Pacific-Asia Conference on Knowledge Discovery and Data Mining. Springer, 2016, pp. 401–414.

[15] L. Zhang, T. Jung, K. Liu, X.-Y. Li, X. Ding, J. Gu, and Y. Liu, "Pic: Enable large-scale privacy preserving content-based image search on cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 28, no. 11, pp. 3258–3271, 2017.

A BHAGYA LAKSHMI is a student of V. S. Lakshmi Engineering College for women, Matlapalem, Talarevu Mandal, E.G.dt, AP, India. Presently she is pursuing her M.Tech[Computer Science and Engineering] from this college. Her area of interest includes Cloud Computing, Data Mining.

B HEMA NAGA MANI, Assoc Professor, V. S. Lakshmi Engineering College for women, Matlapalem, Talarevu Mandal, E.G.dt, AP, India. She has 5 years of teaching experience. Her area of interest includes Software Engineering, Cloud Computing.