iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** II **Month of publication:** February 2020

DOI: http://doi.org/10.22214/ijraset.2020.2114

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 8 Issue II Feb 2020- Available at www.ijraset.com

Survey on Secure and Efficient Content-Based Retrieval in Cloud Image Repositories

Yelapure Shital S.[1], Prof. Shah H.P.[2]
[1]*PG Student, Computer Science And Engineering, Dr.Babasaheb Ambedkar Technological University, lonere.*
[2]*Faculty, MS Bidve College Of Engineering*

Abstract: ***Many cloud stages ascend to meet sincere prerequisites for broad volume of individual picture store, sharing and search. Truth be told the vast majority of those pictures contain delicate secure information (e.g., Human, territory and any event) and people's insurance concerns ruin their venture into untrusted administrations, the present cloud stages give little help to picture security confirmation that is security assurance. Confronting extensive scale images from numerous clients i.e. user's, it is extremely challenging for the cloud to keep up the record structure and schedule parallel calculation without learning up anything about the image contents and indices. In this work, present a novel that is Privacy-protecting Content based Image Search framework on Cloud, or, in other words towards possible cloud services which give secure content based extensive scale image search with fine-grained access control using Shape-Based Invariant Texture Index (SITI). Users can search on others' images on the off chance that they are approved by the image owners. Larger part of the computationally serious part is handled by the cloud, and a querier can now simply send the query and get the search outcome. Specially, to manage enormous images, will designed our framework suitable for distributed and parallel calculation and introduce several optimizations with further facilitate the search procedure. Our security examination and model system assessment results will exhibit that this work adequately verifies the picture assurance expecting practically no exertion of computation and correspondence.***
Keywords: Privacy protection, Content-based, Cloud, Image Encryption, SITI, Feature Extraction;

I. INTRODUCTION

Content based image search center usefulness for different picture applications, e.g., individual picture the board, criminal examination utilizing publicly supported photographs. Previous image search systems typically extract distinctive feature descriptors (high-dimension feature vectors) from interest points of images to measure their content similarity. One image is usually described by hundreds of feature vectors, and millions of photos uploaded to the cloud imply billions of feature vectors. Therefore, it is necessary to introduce optimization techniques such as indexing or distributed computing to accelerate the search process. But most previous efforts did not support image privacy protection or assumed that feature vectors do not reveal content of images. However, recent researches show that an image can be approximately reconstructed based on the output of a black box feature descriptor software such as those classically used for image indexing. The image reconstructed using SITI feature vectors appears quite similar as the original image, and it shows a good match with the original one. Those methods are entirely automatic and much better reconstruction may be achieved with user interaction. The reconstruction allows clear interpretation of the semantic image content, which arouses great concerns on the image privacy in the image indexing and search systems. As a result, large-scale outsourced personal images need efficient yet private content-based search urgently. To implement a desired privacy-friendly image search platform, need to address several conflicted critical challenges. First, all feature vectors should be encrypted, the search process should be completed in a non-interactive way, and all storage and majority of computation should be outsourced to the cloud, while the cloud cannot learn the images, feature vectors and search results. Second, a user should be able to search freely on all his/her authorized images on the cloud, which could be encrypted by keys from multiple owners. Third, facing large image sets, the cloud should leverage the power of indexing and parallel computing using encrypted data.

II. RELATED WORK

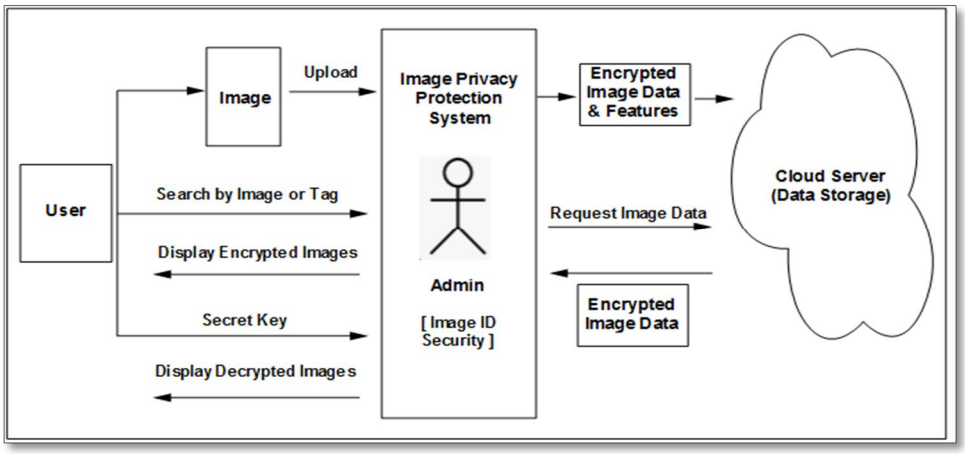
In this work, they introduce a framework POP, which enables privacy-seeking mobile device users to outsource burdensome photo sharing and searching safely to untrusted servers. Unauthorized interrupter, including the server, learns nothing about photos or search queries. This is achieved by carefully designed architecture and novel non-interactive privacy-preserving protocols for image similarity computation. This framework allows users to define personalized private content by a simple check-box configuration and then enjoy the sharing and searching services as usual [1]. They propose a near-real-time and cost-effective semantic queries based methodology, called FAST. The aim behind FAST is to explore and feat the semantic correlation within and among datasets via

correlation-aware hashing and manageable flat-structured addressing to significantly reduce the processing waiting, while incurring acceptably small loss of data-search accuracy**.** FAST is designed to exploit the correlation property of data by using correlation-aware hashing and manageable flat-structured addressing. This enables FAST to significantly reduce processing latency of correlated file detection with acceptably small loss of accuracy. This system only worked on data storage not content based image retrieval [2]. They present a new scheme design that achieves efficiency and security requirements simultaneously with the preservation of its key characteristics, by randomly splitting the original image data, designing two efficient protocols for secure multiplication and comparison, and carefully distributing the feature extraction estimation onto two independent cloud servers. This solution is practically secure, outperforms the state-of-the art, and performs comparably to the original SIFT. They proposed a scheme that supports CBIR over encrypted images without leaking the sensitive information to the cloud server. In this work, feature vectors are extracted to represent the corresponding images. Then the pre-filter tables are building by locality-sensitive hashing to increase search efficiency. The feature vectors are protected by the secure KNN algorithm, and image pixels are encrypted by a standard stream cipher but Low embedding capacity [4]. In this work they define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE). They set up a set of strict privacy requirements for such a secure cloud storage utilization system. In various multi-keyword definition, they choose the efficient similarity measure of "coordinate matching," i.e., as many matches as possible, to capture the relevance of data documents to the search query. Proposed work present low overhead on both computation and communication. This system only worked on data storage not content based image retrieval and image encryption [5]. In this work they propose a secure framework for outsourced privacy-preserving storage and retrieval in large image repositories. This proposal is based on IES-CBIR scheme, is an Image Encryption Scheme that displays Content-Based Image Retrieval properties. This solution enables both encrypted storage and searching using CBIR queries while preserving privacy. Encrypted data storage and searching using CBIR queries while preserving privacy but there have key sharing, user access control, and reliability issues [6]. In this work, they 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 original content of the database to the cloud server. The local features are handled to represent the images, and earth mover's distance is working to evaluate the similarity of images. The EMD computation is basically a linear programming (LP) issue. The proposed work transforms the EMD issue in such a way that the cloud server can solve it without learning the sensitive information. This system not works on image encryption [7]. In this work they propose a secure framework for outsourced privacy-preserving storage and retrieval in large shared image repositories. This proposal is based on IES-CBIR, a novel Image Encryption Scheme that exhibits Content-Based Image Retrieval properties. The framework works on both encrypted storage and searching using Content-Based Image Retrieval queries while preserving privacy against honest-but-curious cloud administrators. This system not work on colour and texture features for image retrieval [8]. This work is the first to target the importance of privacy-preserving SIFT (PPSIFT) and to address the problem of secure SIFT feature extraction and representation in the encrypted domain. The operations in SIFT must be moved to the encrypted domain, they propose a privacy-preserving realization of the SIFT method based on homomorphic encryption method. This work show through the security analysis based on the discrete logarithm problem and RSA that PPSIFT is secure against cipher text only attack and known plaintext attack. This system not work on colour and texture features for image retrieval [9]. In light of the observation, in this work proposed privacy-preserving social discovery service architecture based on encrypted images. As the core of such social discovery is to compare and quantify similar images, they first accepts the effective Bag-of-Words model to extract the "visual similarity content" of users' images into image profile vectors, and then process the issue as similarity retrieval of encrypted high-dimensional image profiles. To support fast and scalable similarity search over hundreds of thousands of encrypted images, they proposed a secure and efficient indexing structure. The advantage of this work is social discovery results are of high quality and related with human idea. This system did not work on image tag concept [10].

III.PROPOSED SYSTEM

In this proposed work is a Privacy-protecting Image Search framework on Cloud, or, in other words towards possible cloud services which give secure content based extensive scale image search with fine-grained access control using Shape-Based Invariant Texture Index (SITI) for global feature extraction. In this system, the authenticated user's can store the images on cloud with image features, encrypted image copy, secret key and particular image id. Also user can give the access permission like public, private and only me at the time of image stored on cloud server. Users can search on others' images and firstly get image encrypted copy in search result. Users can get original image result only if they are approved by the image owners using particular image secret key. Image download history will be also stored in database which is extra advantage of this propose work. Users can search using image tag also.

A. System Architecture



B. Proposed System Advantages

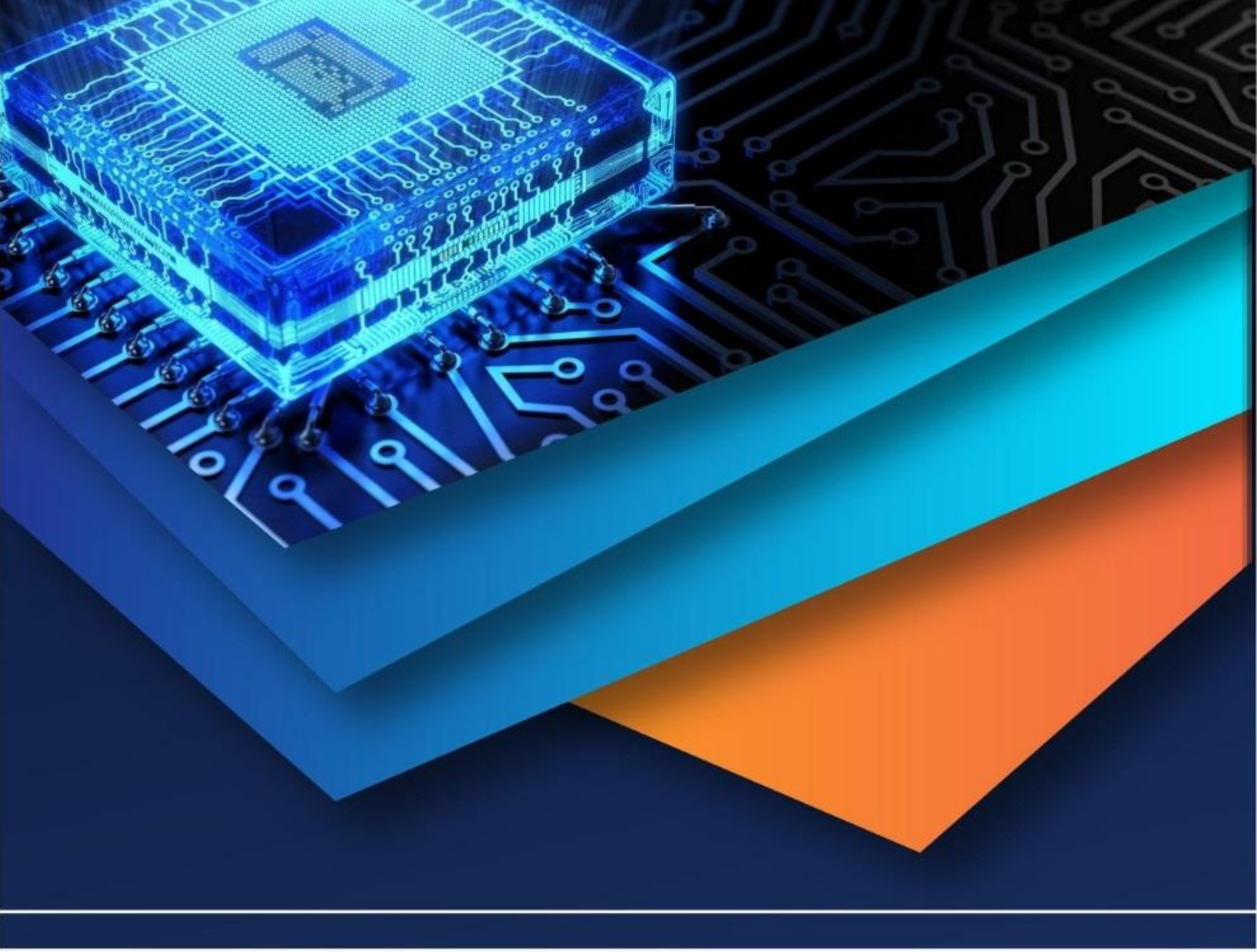
1) This proposed approach support image data privacy protection
2) Using Shape-Based Invariant Texture Index (SITI), proposed work will get more accurate result.
3) In proposed approach, data stored in encrypted format so more security will be provided.
4) Security will be maintained using access control.
5) Also security will be maintained using users image secret key.

IV. CONCLUSIONS

We will have presented a novel system towards privacy preserving content-based search on large-scale images. With our careful design, the majority of the computationally intensive image matching jobs are outsourced to the cloud in a non-interactive way, but the image and query privacy is preserved. To further expedite the search process, this system will enable the cloud to maintain the image id that is index structure and parallelize the search process without learning anything. Proposed system will use Shape-Based Invariant Texture Index (SITI). So that the image content matching accuracy will be more as compare to existing system.

REFERENCES

[1] 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 ICDCS. IEEE, 2015.
[2] Y. Hua, H. Jiang, and D. Feng, "Real-time semantic search using approximate methodology for large-scale storage systems," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 4, pp. 1212–1225, 2016.
[3] [S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, "Securing sift: Privacy-preserving outsourcing computation of feature extractions over encrypted image data," IEEE Transactions on Image Processing, vol. 25, no. 7, pp. 3411–3425, 2016.
[4] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Transactions on
Information Forensics and Security, vol. 11, no. 11, pp. 2594–2608, Nov 2016.
[5] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacypreserving multi-keyword ranked search over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222–233, Jan 2014.
[6] Bernardo Ferreira, Jo˜ao Rodrigues, Jo˜ao Leit˜ao, Henrique Domingos, "Privacy Preserving Content-Based Image Retrieval in the Cloud". 2015 IEEE 34th Symposium on Reliable Distributed Systems
[7] Zhihua Xia, Yi Zhu, Xingming Sun, Zhan Qin, Kui Ren, "Towards Privacy preserving Content-based Image Retrieval in Cloud Computing". IEEE TRANSACTIONS ON COMPUTER COMPUTING, VOL. *, NO. *, SEPTEMBER 2015
[8] Bernardo Ferreira, Joao Rodrigues, Joao Leitao, Henrique Domingos, "Practical Privacy-Preserving Content-Based Retrieval in Cloud Image Repositories". IEEE Transactions on Cloud Computing, Year: 2017, Volume: PP, Issue: 99
[9] C.-Y. Hsu, C.-S. Lu and S.-c. Pei, "Image Feature Extraction in Encrypted Domain With Privacy-Preserving SIFT," IEEE Trans. Image Process., vol. 21, no. 11, pp. 4593–4607, 2012.
[10] X. Yuan, X.Wang, C.Wang, A. Squicciarini, and K. Ren, "Enabling Privacy-preserving Image-centric Social Discovery," in ICDCS'14. IEEE, 2014.
[11] L. Zhang, X.-Y. Li, Y. Liu, and T. Jung, "Verifiable private multiparty computation: Ranging and ranking," in IEEE INFOCOM, 2013.
[12] T. Jung, X.-Y. Li, and M. Wan, "Collusion-tolerable privacy preserving sum and product calculation without secure channel". In IEEE TDSC, 2014.
[13] 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. 27, no. 2, pp. 340–352, Feb 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY