IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023

DOI: 10.17148/IARJSET.2023.10790

Secure Image Retrieval in the Cloud: Leveraging Bag-of-Encrypted-Words (BOEW) Model

Merwyn D Almeida[1], Sandarsh Gowda M M[2]

Master of Computer Applications, Bangalore institute of technology, Bengaluru- 560004[1]

Master of Computer Applications, Bangalore institute of technology, Bengaluru- 560004[2]

Abstract: Content-based Image Recovery (CBIR) techniques have undergone substantial research given the development of digital photographs. CBIR services are often highly expensive in terms of computational and storage costs. Therefore, choosing to outsource CBIR service to a cloud server with a lot of resources is a wise decision. However, since the cloud server cannot be completely trusted, privacy protection becomes a significant issue.

In this study, we suggest a CBIR outsourcing strategy. based utilizing a brand-new bag-of-encrypted-words (BOEW) architecture. Through color value replacement, block permutation, and intra-block pixel combination, the picture is encoded. The cloud server then uses the encrypted information to generate local histograms. picture blocks.

The cluster centres are employed as the encrypted visual words, and all of the Regional graphs grouped together. The bag-of- Pattern for coded words (BOEW) constructed in this manner A characteristics vector format or a normalized histogram of the encrypted visual words, that represents each image. The distance at Manhattan between vectors of features on a remote platform may be used to directly evaluate picture similarity. The suggested scheme's safety and precision of searches are demonstrated based on research findings and safety analysis.

Keywords: BEOW, CBIR, Digital Images, encryption

1. INTRODUCTION

THE PLANET has seen a rapid advancement in imaging technology That includes mobile devices, cameras that are digital, and other devices with photographic capabilities. The outcome is the quantity of digital photos grows quickly. Many viable Techniques called Content-based Image Retrieval (CBIR) have been created to swiftly find comparable pictures from enormous amounts of photographs. However, a typical picture database is just too enormous, with millions of photographs, some wherein are greater than 40 gigabytes. The result is CBIR services often demand a big storage area and calculation. Such requirements make it appealing CBIR outsourcing functions to a cloud server. The result is the picture owner no longer has To keep the picture information and can quickly obtain the needed photos to a server in the distance.

Other than the numerous advantages under CBIR, the picture owner's primary concern is image privacy. The search for the photo as well as the database of photos must be appropriately safe guarded.

2. LITERATURE SURVEY

Customers can keep encrypted data in the cloud thanks to searchable cryptography (SE). while also supporting data search across the cipher-text domain. However, because many previous SE methods for reading creation documents, The first CBIR system that protects anonymity over a private key picture database was presented. The method used an assortment of visual terms to represent pictures. The Using the Jaccard's separation among groups of pictorial phrases, determine image similarity. To safeguard the Its min-hash algorithm, order-preserving encrypting it and visual words were used.

Another study [2] looked into three picture feature protection techniques: Stochastic portrayal, bitplane selection, and randomised unary encoding. Bitplane randomization and random unary encoding are used within the cryptography field. enable the determination of Hamming distance. An arbitrary translation allows for an approximation of L1 a separation in the decryption field. Lu et al. contrasted the three in approaches discussed above to homomorphic cryptography with found that homomorphic security required substantially greater assets for communications and processing.

To facilitate secure similarity search, Local sensitive hashing and Cuckoo Hashing were employed by Yuan and colleagues. safeguard the picture has. That social relationships between picture owners were discovered using this

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023

DOI: 10.17148/IARJSET.2023.10790

strategy. suggested a CBIR technique that preserves privacy using Scale-Invariant Feature Transform (SIFT) features and Earth Mover's Distance (EMD). The EMD calculation is, in reality, a linear programming issue. During the EMD problem solving procedure, It was an ordered change. used to secure the personal information. To increase search performance, we created Searching for encoded photos technique in accordance with the safe kNN (k-nearest Neighbors) method and a tree index. Over encrypted pictures, The Markov chainbased retrieval approach was presented. JPEG file encryption for the Schwarz list safeguarded the image content.

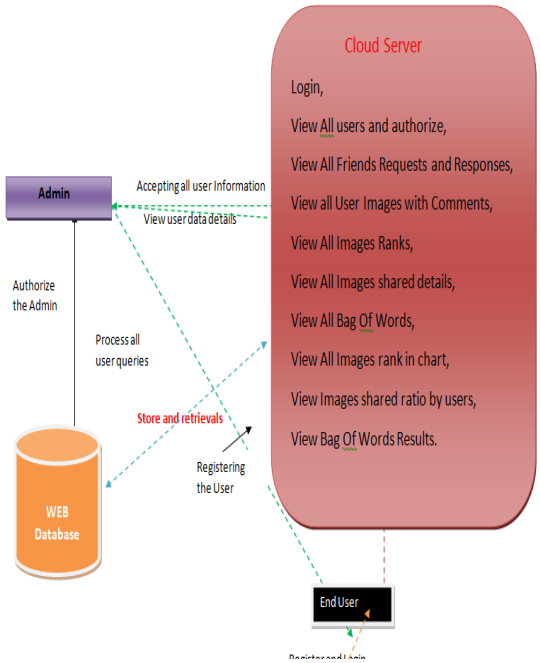

Fig. 1. Proposed Architecture

3. PROPOSED METHODOLOGY

In this work, the system presents an external CBIR approach with appropriately secured picture material. The following are the key contributions:

1) For CBIR outsourcing, In a BOEW approach, proposed. We suggest encrypting pictures in blocks and ensuring that secure and beneficial local characteristics may properly retrieved from the stored blocks. To construct K-mean clustering is employed to decode the encoded graphical words. Then, using the visual terms, generate the final feature vectors, including the encrypted ones. The similarity of the feature vectors may be determined directly using the Manhattan's or Euclid distance. The BOEW proposal model might be useful in encrypted picture processing.

2) As an example, we propose that a picture be encrypted using colour blocking arrangement, intra-block pixel permutations, and value exchange. encryptable local graphs may be retrieved directly from encrypted photos within the cloud servers using a specifically built encryption mechanism. The index can alternatively be completed through a virtual database. In comparison to the technique employing the safe worldwide histogram our method yields greater retrieval rate accuracy.

Advantages

The Ownership of the picture secures the inquiry picture and uploads as soon as the online server a query trapdoor. The internet server provides the most comparable photos to the photographer after searching the index.

The stolen material contains The table's photographs' resemblance to the decrypted query image and the and Searchable encryption.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023

DOI: 10.17148/IARJSET.2023.10790

4. IMPLEMENTATION

Cloud Server:

Computer within the Clouds must login in this module using a valid user name and password. He can do various actions after successfully logging in, such as Login, View and authorise all users, View All Requests and Responses from Friends, View all User Image Comments, View All Images Ranks, View All Images Shared Details, View All Bag Of Words, View All Images Rank in Chart, View Images Shared Ratio by Users, View All Images Shared Ratio by Users, View All Images Shared Ratio by View the results of Bag Of Words.

View and Authorize User:

The admin may view a list of all registered users in this module. The admin can examine the user's data such as user name, email, and address, and the admin can authorise the users.

End User

There are a n number of users in this module. Before doing any activities, the user must first register. When a user registers, their information is saved in the database. After successfully registering, he must login using his authorised user name and password.After successfully logging in, the user may do the following actions: Register and Login, View Profile, Search Friend and Friend Request, View All Friends, Upload Image, View All My Images, Search Images, View All My Friends Image.

5. CONCLUSIONS

A unique privacy-preserving CBIR technique is suggested in this research. A unique bag-of-encrypted-words (BOEW) algorithm's recovery efficiency is high. As an example, we use colour blocks the permutation, pixel rotation within a block, as well as value replacement to secure the picture content. As local characteristics, Regional graphs computed. To produce encrypted visual words, the k-means method is used. To illustrate the image, The graphical letters' gradient is computed. The Manhattan distance between feature vectors on a remote service may be used to directly evaluate picture similarity. Along with the looking process, the index creation in our method may be delegated A virtual server. The suggested strategy may be enhanced further. For starters, it may be a noteworthy future project.

REFERENCES

[1] J. M. Lewin, R. E. Hendrick, C. J. D'Orsi, P. K. Isaacs, L. J. Moss, A. Karellas, G. A. Sisney, C. C. Kuni, and G. R. Cutter, "Comparison of full-field digital mammography with screen-film mammography for cancer detection: results of 4,945 paired exam-inations." Radiology, vol. 218, no. 3, pp. 873–80, 2001.

[2] C. S. Lu, "Homomorphic encryption-based secure sift for privacy-preserving feature extraction," Proceedings of SPIE The International 2011's Society for Optical Engineering, volume 7880, issue 2, pages 788 005–17.

[3] J. Rodrigues, B. Ferreira, and J. Leit˜ao, and H. Domingos, "Privacy-preserving content-based image retrieval in the cloud," on Reliable Distributed Systems, the 34th IEEE Symposium. 2015 IEEE, pp. 11–20.

[4] J. Leitao, H. Domingos, B. Ferreira, J. Rodrigues,
"Practical privacy-preserving content-based retrieval in cloud image reposi-tories," IEEE Transactions on Cloud Computing, vol. PP, no. 99, pp.1–1, 2017.

[5] Y. Rui, T. S. Huang, M. Ortega, and S. Mehrotra, "Relevance feed-back: a power tool for interactive content-based image retrieval," IEEE Transactions on Circuits and Systems for Video Technology, vol. 8, no. 5, pp. 644–655, 1998.

[6] Y. Liu, D. Zhang, G. Lu, andW.-Y. Ma, "A survey of content-based image retrieval with high-level semantics," Pattern Recognition, vol. 40, no. 1, pp. 262–282, 2007.

[7] C. B. Akg¨ ul, D. L. Rubin, S. Napel, C. F. Beaulieu, H. Greenspan, and B. Acar, "Content-based image retrieval in radiology: current status and future directions," Journal of Digital Imaging, vol. 24, no. 2, pp. 208–222, 2011.

[8] X. Zhang, W. Liu, M. Dundar, S. Badve, and S. Zhang, "Towards large-scale histopathological image analysis: Hashing-based im-age retrieval," IEEE Transactions on Medical Imaging, vol. 34, no. 2, pp. 496–506, 2015.

[9] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient con-structions," Journal of Computer Security, vol. 19, no. 5, pp. 79–88,2011.

[10] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in 2010 Proceedings IEEE INFOCOM. IEEE, 2010, pp. 1–5.