IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 4, April 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304260 |

SEI: Similarity Search for Encrypted Images in Secure Cloud Computing

Rama Mrudula, Aitha Akhil, Ponugoti Sai Deekshith, Samudrala Srikanth

Assistant Professor, Dept. of CSE, Anurag University, Hyderabad, India

UG Student, Dept. of CSE, Anurag University, Hyderabad, India

UG Student, Dept. of CSE, Anurag University, Hyderabad, India

UG Student, Dept. of CSE, Anurag University, Hyderabad, India

ABSTRACT: The Content-Based Image Retrieval (CBIR) technique has garnered a lot of attention from various domains (such as cloud computing, social networking services, etc.) with the rise of intelligent terminals. Even though current privacy-preserving CBIR methods can allow image retrieval and ensure picture privacy, they nevertheless have intrinsic flaws (such as low search accuracy, low key leakage, search efficiency, etc.). To tackle these challenging issues, we introduce in this study a similarity search for encrypted pictures in secure cloud computing (called SEI). Initially, search accuracy is increased by using the feature descriptors that the Convolutional Neural Network (CNN) model extracted. The next step is to create an encrypted hierarchical index tree that can increase search performance using K-means clustering based on Affinity Propagation (AP) clustering. After that, a k-Nearest Neighbour (KNN) with limited key leaking.

KEYWORDS: Content-based image retrieval, hierarchical index tree, k-Nearest Neighbour, search accuracy, search efficiency.

I. INTRODUCTION

Since cloud computing has grown so quickly and become so popular, consumers have been able to take advantage of many advantages offered by cloud services, like online image storage. However, there will always be privacy issues if photos are immediately outsourced to the public cloud. There will be severe repercussions or needless difficulties once the vast photos (such as patient medical images) holding extremely sensitive information have been exposed to unauthorized parties. To some extent, the encryption method can allay worries about picture data security and privacy, but it also breaks the Content-Based picture Retrieval (CBIR) method over ciphertext and raises other issues that are illustrated in the example that follows.

Example: Alice uses the cloud server to handle the encrypted image C from the local image database M. Using the searchable key k, the authorized Bob creates an encrypted search request T based on the query picture q, supplied by Alice during his search for pictures that match q. After getting T, the cloud server then searches C and gives Bob the relevant search results, R. In the end, Bob uses Alice's picture encryption key, k, to decrypt the R.

For the sake of our encrypted image search, the cloud server is considered semi-trusted. Alice uses this cloud server to store her photos and gives it control over similarity search operations. In accordance with Alice's request, Bob will be able to access Alice's photographs on the cloud server and do searches. Bob's search experience will be significantly impacted by the effectiveness and accuracy of search services. If Bob is a physician who uses search engine results to determine a patient's condition, then inaccurate search results will result in an inaccurate diagnosis, putting the patient's health and maybe life in jeopardy. In addition, Bob's waiting period will be prolonged by the laborious search procedure. If Bob uses a mobile device to see images and needs.

II. RELATED WORK

Image feature extraction in encrypted domain: This method provides excellent efficiency and confidentiality by proposing a novel image retrieval scheme over encrypted cloud data. An index tree is frequently used in the image retrieval strategy to increase search performance. In the meantime, another crucial concern is the confidentiality of the

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304260 |

sensitive cloud data, including the query request, index tree, and outsourced photos.

Secure image retrieval with multiple keys: A secure picture retrieval strategy for multiuser scenarios is proposed in this article. According to this approach, the owner encrypts and uploads images to the cloud along with their related features first; the user then submits the encrypted feature of the query image to the cloud; the cloud then compares the encrypted features and provides the user with encrypted images that have similar content. An encryption with multiple keys is presented, in which each user's query feature is encrypted by a unique key, making it possible to locate the nearest neighbor in the encrypted features. In order to create numerous keys, global optimization and Gaussian distribution are used, respectively, to increase key security and space utilization.

Instant Crypto Gram: For social media platforms like Instagram to find related photographs and suggest users with similar interests, image retrieval is essential. However, encryption must be used before outsourcing the photographs due to privacy issues. We require a safe method of obtaining pictures from a server that we don't fully trust. A secure picture retrieval service called Instant Crypto Gram is proposed in this paper. First, it creates a novel data structure called sub-sim hash, which fits into the format of various searchable symmetric encryption algorithms that use an inverted index. This results in our modular approach that facilitates effective updating and similarity queries across encrypted photos.

Epcbir: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing: One of the most common services in cloud computing is the outsourcing of CBIR to the cloud servers. Sensitive photos, such private and medical photos, must be encrypted for privacy reasons before being outsourced. Failure to do so will render CBIR technologies in the plaintext domain useless. In this research, it presents a technique that allows CBIR over encrypted photos while keeping the cloud server unaware of any sensitive information. Initially, the relevant images are represented by the extracted feature vectors. To improve search efficiency, locality-sensitive hashing is then used in the construction of the pre-filter tables. Next, the secure k-nearest neighbour (KNN) technique is applied to safeguard the feature vectors. The suggested scheme's efficiency and security are demonstrated by the experiments and security analysis.

Content-based multi-source encrypted image retrieval in clouds with privacy preservation: This research presents a secure CBIR technique that allows for the protection of Multiple Image owners while maintaining privacy (MIPP). We employ a secure multi-party computation method to encrypt image features, enabling the owners of the images to do so using their own keys. This ensures that an individual picture owner's privacy is protected from being revealed to other image owners while enabling effective image retrieval over images collected from various sources. Additionally, we provide a fresh approach to picture similarity assessment that can prevent disclosing image similarity data to cloud services. MIPP maintains picture privacy while concurrently achieving retrieval efficiency and accuracy, as shown by theoretical analysis and experimental findings.

III. PROPOSED SYSTEM

To address the flaws in the CBIR techniques now in use:
High search precision: To reach a high level of search precision Convolutional Neural Network (CNN) model is used in similarity search for encrypted images to extract feature vectors.
High search efficiency: SEI classifies photos using the K-means clustering algorithm and builds a hierarchical index tree from the bottom up depending on the clustering findings. thereby shortens the search time and boosts effectiveness.
Restricted key leakage: To stop unauthorized image users from running queries, SEI offers a safe trapdoor creation mechanism with restricted key leakages.
The Convolutional Neural Network (CNN) model can extract features from encrypted photos without the need to decrypt them since it is trained to extract high-level features from the images, capturing its visual information.
Based on the characteristics that were extracted from the photos, a hierarchical k-means tree is built, which hierarchically divides the feature vectors into clusters and guarantees great search efficiency.
The following are some benefits of the suggested approach:
1. Search accuracy is increased by using the feature descriptors that the Convolutional Neural Network (CNN) model extracts.
2. Next, utilizing K-means clustering based on Affinity Propagation (AP) clustering, an encrypted hierarchical index tree is created, which can enhance search efficiency.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304260 |

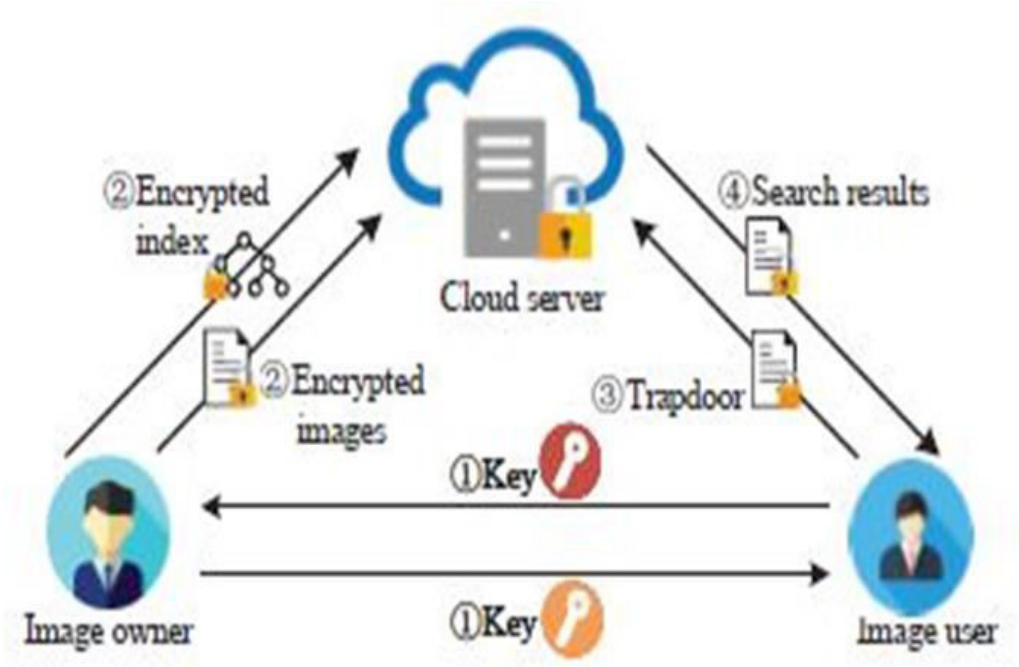


Figure 1 Architectural Diagram

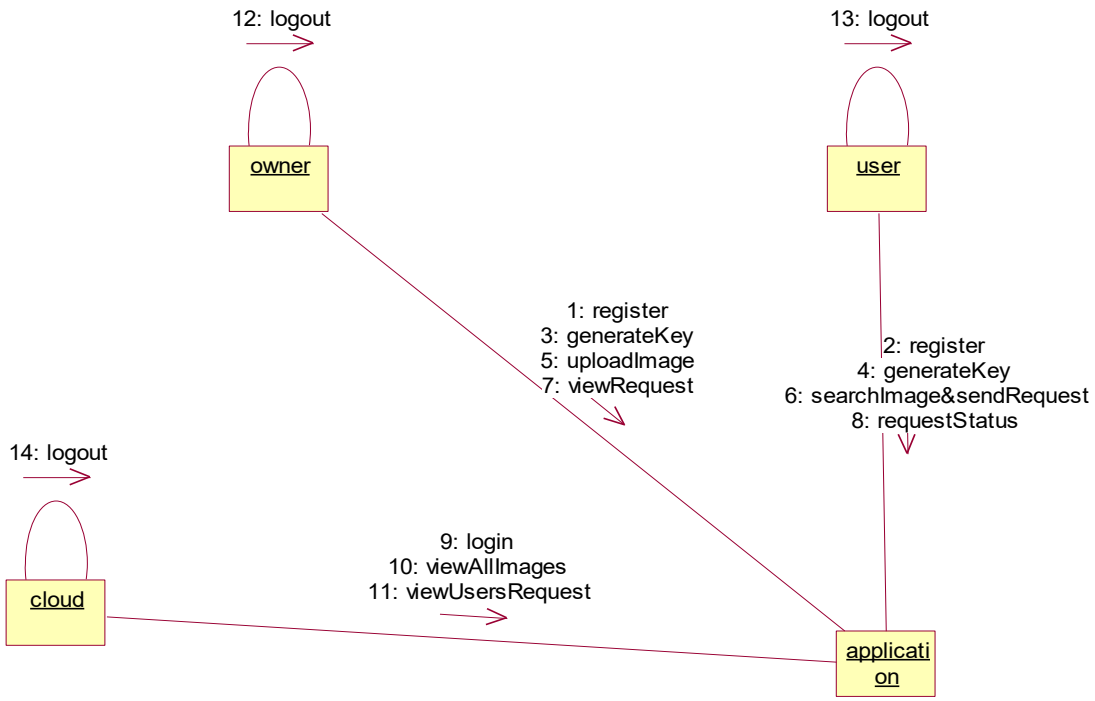


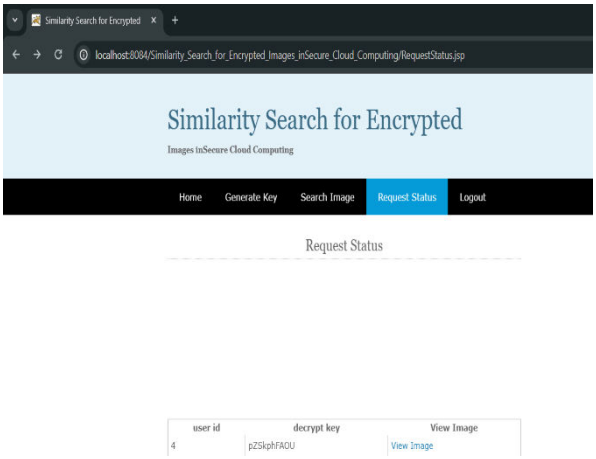
Figure 2 Dataflow Diagram

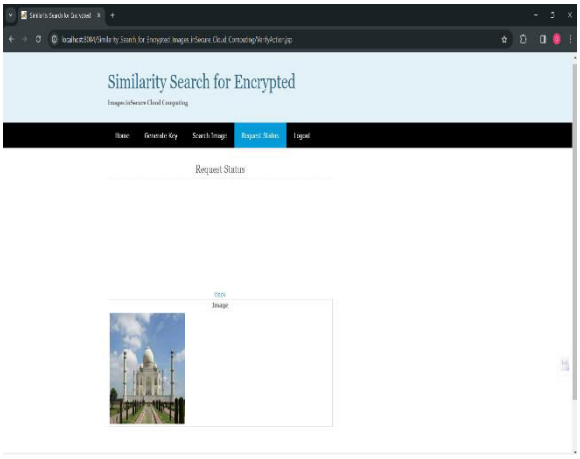
| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304260 |

IV. RESULTS





The Image user can view the image that he desired only when the cloud accepts the request made by the image user.

V. CONCLUSION

In conclusion, a major step toward accomplishing the twin objectives of data privacy and utility in cloud-based image processing applications is the invention of similarity search for encrypted images in secure cloud computing. We have tackled the fundamental problem of enabling accurate and efficient image retrieval while maintaining the privacy of sensitive data stored in the cloud with this research.

Through the application of sophisticated cryptographic methods, scalable algorithms, and creative strategies, we have proven that similarity search operations on encrypted image collections can be carried out without sacrificing security or privacy. While guaranteeing that the underlying data is secured and unavailable to unwanted parties, such as the cloud service provider, our system lets users search for comparable photographs.

We have determined the main obstacles to be overcome and the areas that still need investigation and improvement. To further improve the security, privacy, and functionality of similarity search systems in the cloud, these include investigating quantum-safe cryptography, differential privacy methods, federated learning techniques, secure hardware enclaves, hybrid encryption schemes, and blockchain integration.

We can open up new avenues for secure and private image analysis in the cloud by keeping up with innovation and cross-disciplinary collaboration. This will allow businesses to obtain insightful information from their encrypted datasets while complying with industry standards and strict data protection laws.

REFERENCES

[1]. Y. Rubner, C. Tomasi, and L. J. Guibas, “The earth mover’s distance as a metric for image retrieval,” International Journal of Computer Vision, vol. 40, no. 2, (2000), pp. 99–121.
[2]. H. Ling and K. Okada, “An efficient earth mover’s distance algorithm for robust histogram comparison,” Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 29, no. 5, (2007), pp. 840–853.
[3]. E. Levina and P. Bickel, “The earth mover’s distance is the mallows distance: some insights from statistics”, in Computer Vision, 2001, ICCV 2001, Proceedings, Eighth IEEE International Conference on, vol. 2. IEEE, (2001), pp. 251–256.
[4]. P. Indyk and R. Motwani, “Approximate nearest neighbors: towards removing the curse of dimensionality”, in Proceedings of the thirtieth annual ACM symposium on Theory of computing, ACM, (1998), pp. 604–613.
[5]. A. Gionis, P. Indyk and R. Motwani, “Similarity search in high dimensions via hashing”, in VLDB, vol. 99, (1999), pp. 518–529.
[6]. M. Datar, N. Immorlica, P. Indyk, and V. S. Mirrokni, “Locality-sensitive hashing scheme based on pstable distributions”, in Proceedings of the twentieth annual symposium on Computational geometry. ACM, (2004), pp. 253–262.
[7]. A. Rajaraman and J. D. Ullman, “Mining of massive datasets”, Cambridge University Press, (2011).

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details