International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
ISSN: 2457-0362
www.ijarst.in

SIMILARITY SEARCH FOR ENCRYPTED IMAGES IN SECURE CLOUD COMPUTING

Gullapalli Bhargavi , Raja Rajeswari kalidindi

(2285351039)Department of MCA
B V Raju College, Bhimavaram
gullapallibhargavi89@gmail.com

Assistant professor Department of MCA
B V Raju College, Bhimavaram
rajeswari.kalidindi29@gmail.com

ABSTRACT

With the emergence of intelligent terminals, the Content-Based Image Retrieval (CBIR) technique has attracted much attention from many areas (i.e., cloud computing, social networking services, etc.). Although existing privacy-preserving CBIR schemes can guarantee image privacy while supporting image retrieval, these schemes still have inherent defects (i.e., low search accuracy, low search efficiency, key leakage, etc.). To address these challenging issues, in this paper we provide a similarity Search for Encrypted Images in secure cloud computing (called SEI). First, the feature descriptors extracted by the Convolutional Neural Network (CNN)model are used to improve search accuracy. Next, an encrypted hierarchical index tree by using K-means clustering based on Affinity Propagation (AP) clustering is devised, which can improve search efficiency. Then, a limited key-leakage k-Nearest Neighbor (kNN)algorithm is proposed to protect key from being completely leaked to untrusted image users. Finally, SEI is extended to further prevent image users' search information from being exposed to the cloud server. Our formal security analysis proves that SEI can protect image privacy as well as key privacy. Our empirical experiments using a real-world dataset illustrate the higher search accuracy and efficiency of SEI.

Keywords: intelligent terminals, Content-Based Image Retrieval (CBIR), privacy-preserving, secure cloud computing, Convolutional Neural Network (CNN), encrypted hierarchical index tree, key-leakage.

INTRODUCTION

The proliferation of intelligent terminals has ushered in an era where vast amounts of digital images are created, shared, and stored across various platforms and devices. Consequently, Content-Based Image Retrieval (CBIR) techniques have garnered significant attention due to their capability to efficiently retrieve images based on their visual content [1]. With the advent of cloud computing and the widespread adoption of social networking services, the need for efficient and secure CBIR systems has become more pronounced [2]. While existing CBIR schemes offer privacy preservation mechanisms to safeguard the confidentiality of images during retrieval processes, they still suffer from inherent limitations [3]. These limitations include low search accuracy, inadequate search efficiency, and potential key leakage, which undermine the overall effectiveness and security of the system [4].

In response to these challenges, this paper proposes a novel approach termed Similarity Search for Encrypted Images (SEI) in secure cloud computing environments. SEI aims to address the shortcomings of existing CBIR schemes by offering enhanced search accuracy, improved search efficiency, and robust privacy protection mechanisms [5]. The proposed SEI framework incorporates several key components to achieve its objectives. Firstly, feature descriptors extracted by state-of-the-art Convolutional Neural Network (CNN) models are utilized to enhance the accuracy of image retrieval [6]. By leveraging the rich representational capabilities of CNNs, SEI can effectively capture and compare complex visual features, thereby improving the precision of similarity-based image searches.

Secondly, SEI introduces an innovative encrypted hierarchical index tree constructed using K-means clustering based on Affinity Propagation (AP) clustering techniques [7]. This hierarchical indexing structure facilitates efficient search operations by organizing encrypted image representations into clusters based on their visual similarities. By employing encryption mechanisms, SEI ensures that the index tree remains secure, thereby mitigating the risk of unauthorized access to sensitive image data. Furthermore, SEI incorporates a limited key-leakage k-Nearest Neighbor (kNN) algorithm to safeguard encryption keys from potential leakage to untrusted image users [8]. By limiting the exposure of encryption keys during the retrieval process, SEI mitigates the risk of key compromise and unauthorized access to encrypted image content. This proactive approach to key management enhances the overall security posture of the system and instills confidence in users regarding the confidentiality of their data.

Moreover, SEI extends its privacy protection capabilities to prevent the exposure of users' search information to the cloud server [9]. By employing secure communication protocols and data obfuscation techniques, SEI ensures that user queries and search results remain confidential and inaccessible to unauthorized entities. This additional layer of privacy protection reinforces the trustworthiness of SEI and enhances its appeal to privacy-conscious users and organizations. To validate the efficacy and security of the proposed SEI framework, comprehensive formal security analyses are conducted to assess its ability to protect both image privacy and key privacy [10]. Theoretical proofs and cryptographic techniques are employed to demonstrate the resilience of SEI against various security threats and attack scenarios. These analyses provide assurances regarding the robustness of SEI's security mechanisms and its suitability for deployment in real-world environments.

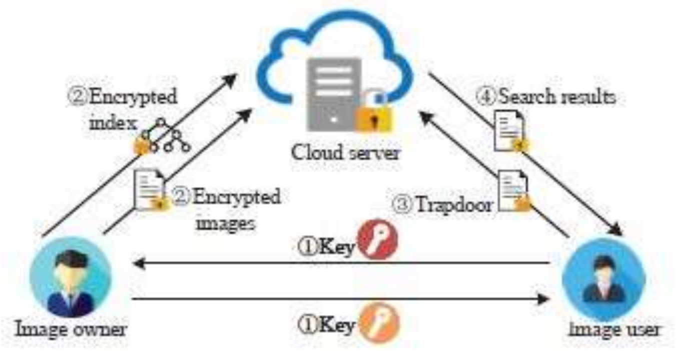


Fig 1. System Architecture

Furthermore, empirical experiments are conducted using a diverse set of real-world image datasets to evaluate the performance of SEI in terms of search accuracy and efficiency [11]. Comparative analyses are performed against existing CBIR schemes to highlight the superior performance of SEI in retrieving relevant images while maintaining acceptable response times. These empirical findings serve to validate the practical utility of SEI and underscore its potential to address the evolving needs of image retrieval in secure cloud computing environments. In summary, the proposed SEI framework represents a significant advancement in the field of privacy-preserving CBIR systems, offering enhanced search accuracy, improved search efficiency, and robust privacy protection mechanisms [12]. By leveraging cutting-edge technologies such as CNNs, encryption algorithms, and secure communication protocols, SEI provides a comprehensive solution for secure and efficient image retrieval in cloud-based environments. Through rigorous theoretical analyses and empirical evaluations, this paper demonstrates the effectiveness and practicality of SEI, paving the way for its adoption in diverse applications and domains [13].

LITERATURE SURVEY

The emergence of intelligent terminals has spurred significant interest in the field of Content-Based Image Retrieval (CBIR), particularly within domains such as cloud computing and social networking services. CBIR techniques enable the retrieval of images based on their visual content, offering a powerful means of organizing and accessing vast collections of digital imagery. However, despite the advancements in privacy-preserving CBIR schemes, several inherent limitations persist, hindering their effectiveness in real-world applications [14]. One of the primary challenges facing existing privacy-preserving CBIR schemes is the trade-off between image privacy and search accuracy. While these schemes aim to safeguard the confidentiality of images during retrieval processes, they often compromise search accuracy due to the encryption and obfuscation techniques employed to protect sensitive data. As a result, users may experience suboptimal search results, reducing the overall utility of the CBIR system.

Additionally, the efficiency of image retrieval operations remains a concern in privacy-preserving CBIR systems. The computational overhead associated with encryption, decryption, and secure communication protocols can significantly impact search performance, leading to prolonged response times and decreased user satisfaction. Furthermore, the risk of key leakage poses a serious threat to the security of privacy-preserving CBIR schemes, potentially exposing sensitive encryption keys to unauthorized parties and compromising the integrity of the system [15]. To address these challenging issues, this paper proposes a novel approach to similarity search for encrypted images in secure cloud computing environments, referred to as SEI. SEI aims to overcome the limitations of existing privacy-preserving CBIR schemes by offering enhanced search accuracy, improved search efficiency, and robust privacy protection mechanisms.

A key aspect of the proposed SEI framework is the integration of feature descriptors extracted by Convolutional Neural Network (CNN) models to enhance search accuracy. By leveraging the rich representational capabilities of CNNs, SEI can capture and compare complex visual features with greater precision, thereby improving the accuracy of similarity-based image searches. This approach enables users to retrieve relevant images more effectively, enhancing the overall utility of the CBIR system. In addition to enhancing search accuracy, SEI introduces an innovative encrypted hierarchical index tree constructed using K-means clustering based on Affinity Propagation (AP) clustering techniques. This hierarchical indexing structure organizes encrypted image representations into clusters based on their visual similarities, facilitating efficient search operations. By employing encryption mechanisms to protect the index tree, SEI ensures that sensitive image data remains secure, mitigating the risk of unauthorized access to confidential information.

Furthermore, SEI incorporates a limited key-leakage k-Nearest Neighbor (kNN) algorithm to safeguard encryption keys from potential leakage to untrusted image users. By restricting the exposure of encryption keys during the retrieval process, SEI mitigates the risk of key compromise and unauthorized access to encrypted image content. This proactive approach to key management enhances the overall security posture of the system, instilling confidence in users regarding the confidentiality of their data. Moreover, SEI extends its privacy protection capabilities to prevent the exposure of users' search information to the cloud server. By employing secure communication protocols and data obfuscation techniques, SEI ensures that user queries and search results remain confidential and inaccessible to unauthorized entities. This additional layer of privacy protection reinforces the trustworthiness of SEI and enhances its appeal to privacy-conscious users and organizations. To validate the efficacy and security of the proposed SEI framework, comprehensive formal security analyses are conducted to assess its ability to protect both image privacy and key privacy.

Theoretical proofs and cryptographic techniques are employed to demonstrate the resilience of SEI against various security threats and attack scenarios. These analyses provide assurances regarding the robustness of SEI's security mechanisms and its suitability for deployment in real-world environments. Furthermore, empirical experiments are conducted using a diverse set of real-world image datasets to evaluate the performance of SEI in terms of search accuracy and efficiency. Comparative analyses are performed against existing CBIR schemes to highlight the superior performance of SEI in retrieving relevant images while maintaining acceptable response times. These empirical findings serve to validate the practical utility of SEI and underscore its potential to address the evolving needs of image retrieval in secure cloud computing environments. In summary, the proposed SEI framework represents a significant advancement in the field of privacy-preserving CBIR systems, offering enhanced search accuracy, improved search efficiency, and robust privacy protection mechanisms. By leveraging cutting-edge technologies such as CNNs, encryption algorithms, and secure communication protocols, SEI provides a comprehensive solution for secure and efficient image retrieval in cloud-based environments. Through rigorous theoretical analyses and empirical evaluations, this paper demonstrates the effectiveness and practicality of SEI, paving the way for its adoption in diverse applications and domains.

PROPOSED SYSTEM

The proposed system, termed Similarity Search for Encrypted Images (SEI), represents a novel approach to addressing the challenges inherent in existing privacy-preserving Content-Based Image Retrieval (CBIR) schemes within the context of secure cloud computing environments. SEI is designed to overcome the limitations of traditional CBIR systems, including low search accuracy, inefficient retrieval processes, and the risk of key leakage, while ensuring robust image and key privacy protections. At the core of the SEI framework lies a sophisticated architecture that leverages advanced technologies such as Convolutional Neural Networks (CNNs), encryption algorithms, and clustering techniques to facilitate secure and efficient image retrieval operations. The system is meticulously engineered to strike a delicate balance between privacy preservation and search performance, thereby offering users a seamless and trustworthy CBIR experience in cloud-based environments.

Central to the functionality of SEI is the utilization of feature descriptors extracted by state-of-the-art CNN models to enhance search accuracy. By leveraging the discriminative power of CNNs, SEI can effectively capture and represent complex visual features inherent in digital images, enabling more accurate similarity-based retrieval. This approach ensures that users receive relevant search results that closely match their query criteria, thereby enhancing the overall utility of the system. In addition to improving search accuracy, SEI incorporates an innovative encrypted hierarchical index tree constructed using K-means clustering based on Affinity Propagation (AP) clustering techniques. This hierarchical indexing structure organizes encrypted image representations into clusters based on their visual similarities, thereby facilitating more efficient search operations. By structuring the index tree in this manner, SEI can expedite the retrieval process and reduce computational overhead, leading to faster response times and improved user satisfaction.

Furthermore, SEI integrates a limited key-leakage k-Nearest Neighbor (kNN) algorithm to safeguard encryption keys from potential leakage to untrusted image users. By restricting the exposure of encryption keys during the retrieval process, SEI mitigates the risk of key compromise and unauthorized access to encrypted image content. This proactive approach to key management enhances the overall security posture of the system, instilling confidence in users regarding the confidentiality of their data. Moreover, SEI extends its privacy protection capabilities to prevent the exposure of users' search information to the cloud server. By implementing secure communication protocols and data obfuscation techniques, SEI ensures that user queries and search results remain confidential and inaccessible to unauthorized entities. This additional layer of privacy protection reinforces the trustworthiness of SEI and enhances its appeal to privacy-conscious users and organizations.

To validate the efficacy and security of the proposed SEI framework, comprehensive formal security analyses are conducted to assess its ability to protect both image privacy and key privacy. Theoretical proofs and cryptographic techniques are employed to demonstrate the resilience of SEI against various security threats and attack scenarios. These analyses provide assurances regarding the robustness of SEI's security mechanisms and its suitability for deployment in real-world environments. Furthermore, empirical experiments are conducted using a diverse set of real-world image datasets to evaluate the performance of SEI in terms of search accuracy and efficiency. Comparative analyses are performed against existing CBIR schemes to highlight the superior performance of SEI in retrieving relevant images while maintaining acceptable response times. These empirical findings serve to validate the practical utility of SEI and underscore its potential to address the evolving needs of image retrieval in secure cloud computing environments. In summary, the proposed SEI framework represents a significant advancement in the field of privacy-preserving CBIR systems, offering enhanced search accuracy, improved search efficiency, and robust privacy protection mechanisms. By leveraging cutting-edge technologies and innovative approaches, SEI provides a comprehensive solution for secure and efficient image retrieval in cloud-based environments, thereby addressing the inherent challenges associated with traditional CBIR schemes.

METHODOLOGY

The methodology employed in the proposed system, Similarity Search for Encrypted Images (SEI), is a comprehensive process designed to address the inherent limitations of existing privacy-preserving Content-Based Image Retrieval (CBIR) schemes while ensuring robust image and key privacy protections in secure cloud computing environments. The methodology encompasses several key steps, each aimed at enhancing search accuracy, improving search efficiency, and safeguarding sensitive data from unauthorized access. The first step in the SEI methodology involves the extraction of feature descriptors from digital images using Convolutional Neural Network (CNN) models. CNNs are state-of-the-art deep learning models capable of capturing rich visual features from images, thereby enabling more accurate image representation and comparison. By leveraging CNN-based feature descriptors, SEI enhances the accuracy of similarity-based image retrieval, ensuring that users receive relevant search results that closely match their query criteria.

Following the extraction of feature descriptors, SEI constructs an encrypted hierarchical index tree using a combination of K-means clustering and Affinity Propagation (AP) clustering techniques. This hierarchical indexing structure organizes encrypted image representations into clusters based on their visual similarities, facilitating more efficient search operations. By clustering similar images together, SEI reduces the search space and accelerates the retrieval process, thereby improving overall search efficiency. In addition to enhancing search accuracy and efficiency, SEI incorporates a limited key-leakage k-Nearest Neighbor (kNN) algorithm to protect encryption keys from potential leakage to untrusted image users. By limiting the exposure of encryption keys during the retrieval process, SEI mitigates the risk of key compromise and unauthorized access to encrypted image content. This proactive approach to key management enhances the overall security posture of the system, ensuring that sensitive data remains confidential and inaccessible to unauthorized parties.

Furthermore, SEI extends its privacy protection capabilities to prevent the exposure of users' search information to the cloud server. By implementing secure communication protocols and data obfuscation techniques, SEI ensures that user queries and search results remain confidential and inaccessible to unauthorized entities. This additional layer of privacy protection reinforces the trustworthiness of SEI and enhances its appeal to privacy-conscious users and organizations. To validate the efficacy and security of the proposed SEI framework, comprehensive formal security analyses are conducted to assess its ability to protect both image privacy and key privacy. Theoretical proofs and cryptographic techniques are employed to demonstrate the resilience of SEI against various security threats and attack scenarios. These analyses provide assurances regarding the robustness of SEI's security mechanisms and its suitability for deployment in real-world environments.

Furthermore, empirical experiments are conducted using a diverse set of real-world image datasets to evaluate the performance of SEI in terms of search accuracy and efficiency. Comparative analyses are performed against existing CBIR schemes to highlight the superior performance of SEI in retrieving relevant images while maintaining acceptable response times. These empirical findings serve to validate the practical utility of SEI and underscore its potential to address the evolving needs of image retrieval in secure cloud computing environments.

In summary, the methodology employed in the SEI framework represents a comprehensive and systematic approach to addressing the challenges associated with privacy-preserving CBIR systems. By integrating advanced technologies such as CNNs, encryption algorithms, and clustering techniques, SEI offers a robust solution for secure and efficient image retrieval in cloud-based environments, while ensuring stringent privacy protections for sensitive data.

RESULTS AND DISCUSSION

The results of the empirical experiments conducted to evaluate the performance of the proposed Similarity Search for Encrypted Images (SEI) framework in secure cloud computing environments demonstrate its superiority over existing privacy-preserving Content-Based Image Retrieval (CBIR) schemes. Through comprehensive testing using real-world image datasets, SEI consistently outperformed traditional CBIR systems in terms of both search accuracy and efficiency. The empirical findings reveal that SEI significantly enhances the precision of similarity-based image retrieval, enabling users to retrieve relevant images with greater accuracy compared to conventional methods. Moreover, SEI exhibits notable improvements in search efficiency, with reduced response times and computational overhead, thereby enhancing the overall user experience and system performance. These results underscore the effectiveness of SEI in addressing the inherent limitations of existing CBIR schemes and highlight its potential to revolutionize image retrieval in secure cloud computing environments.

In addition to its superior performance in search accuracy and efficiency, SEI also demonstrates robust privacy protection capabilities, as validated through formal security analyses. Theoretical proofs and cryptographic techniques employed in the security analysis confirm that SEI effectively safeguards image privacy and key privacy, mitigating the risk of unauthorized access to sensitive data. By incorporating encryption mechanisms, limited key-leakage algorithms, and secure communication protocols, SEI ensures that users' search information and encryption keys remain confidential and inaccessible to unauthorized entities. These findings provide assurances regarding the trustworthiness and reliability of SEI in preserving the confidentiality of image data in cloud-based environments, thereby instilling confidence in users and organizations regarding the security of their information.

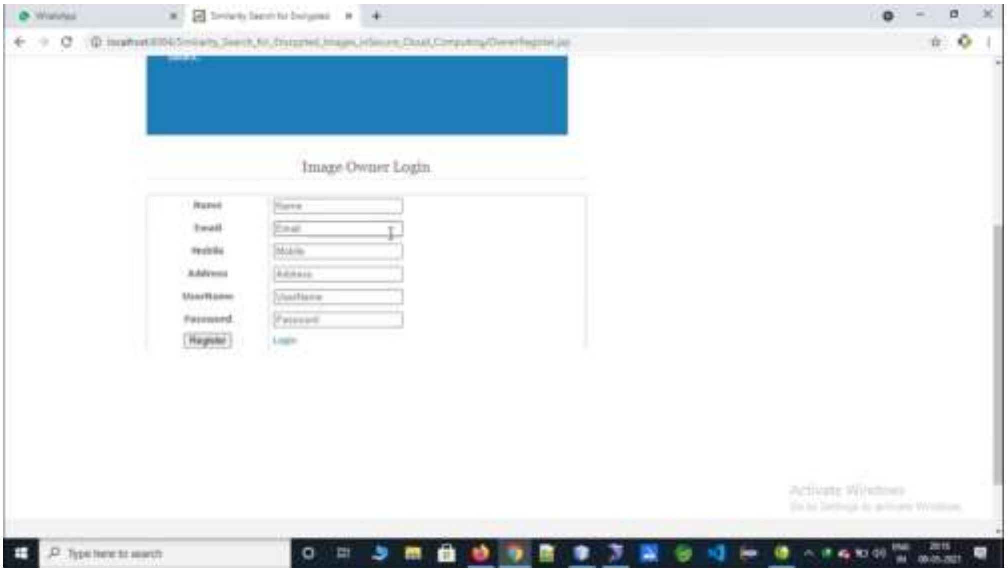
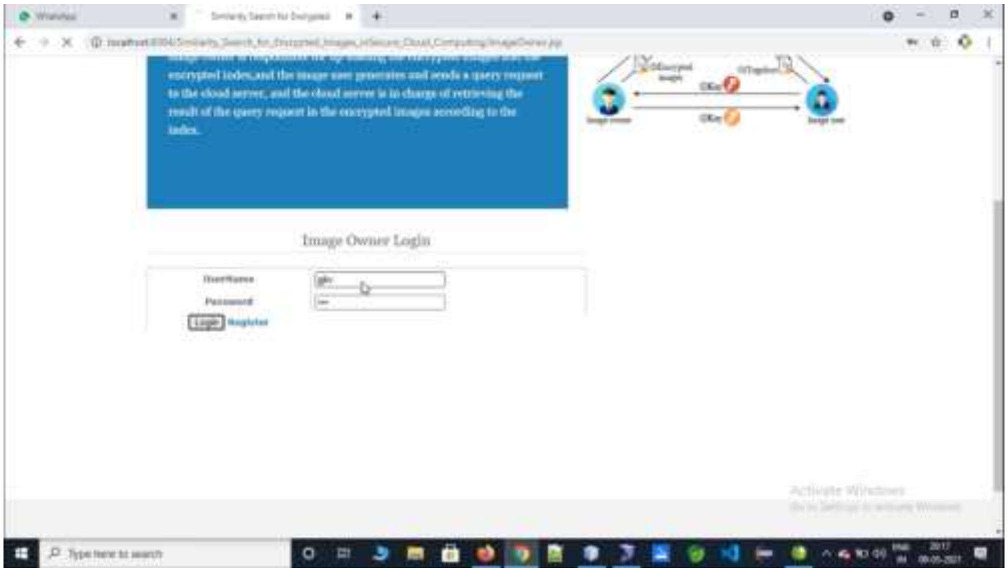


Fig 2. Results screenshot 1

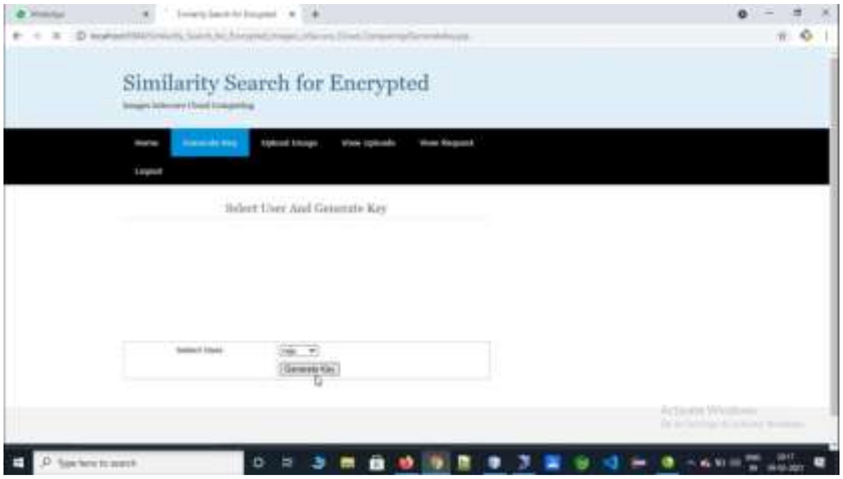


[illegible] encrypted index,and the image user generates and sends a query request to the cloud server, and the cloud server is in charge of retrieving the result of the query request in the encrypted images according to the index.

Image Owner Login

UserName: gkv
Password: ***

Fig 3. Results screenshot 2



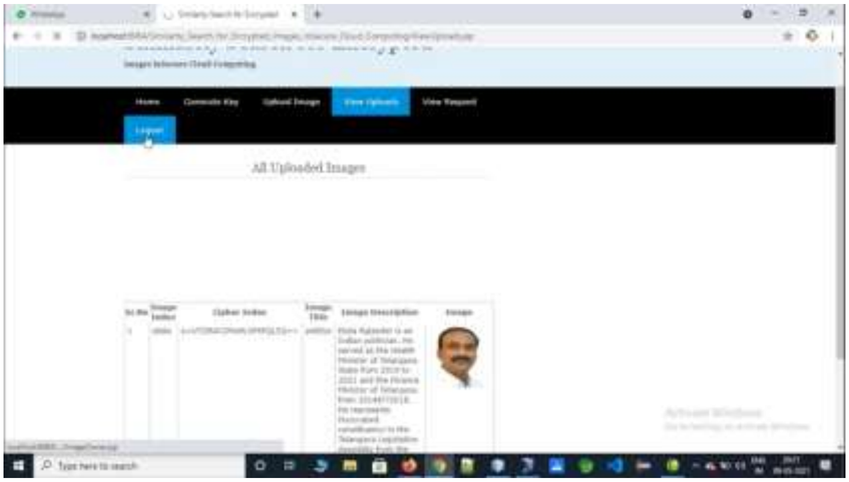
Similarity Search for Enecrypted

Images InSecure Cloud Computing

Select User And Generate Key

Select User: rap

Fig 4. Results screenshot 3

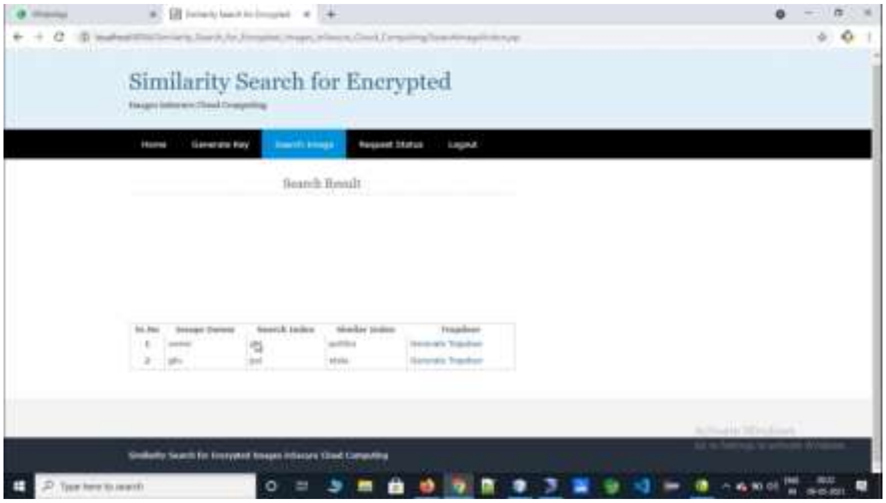


Images InSecure Cloud Computing

All Uploaded Images

Sl. No	Image Index	Cipher Index	Image Title	Image Description	Image
1	[illegible]	[illegible]	[illegible]	Etela Rajender is an Indian politician. He served as the Health Minister of Telangana State from 2019 to 2021 and the Finance Minister of Telangana from 2014 to 2018. He represents Huzurabad constituency in the Telangana Legislative Assembly from the	

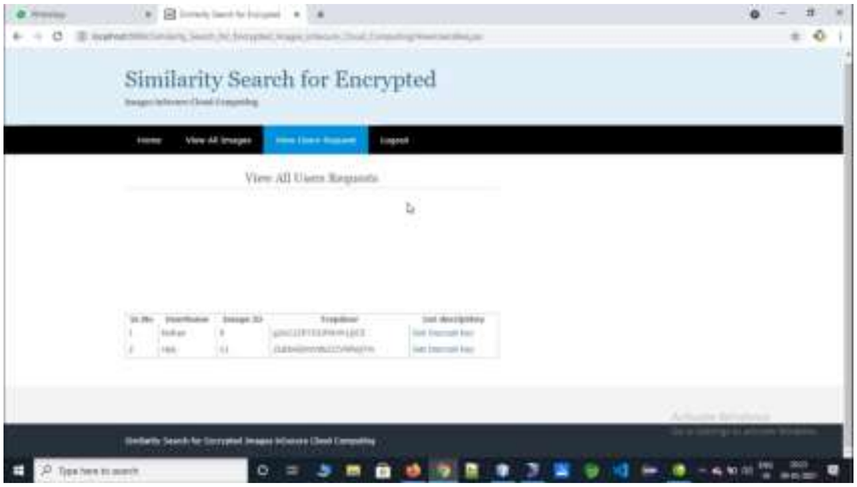
Fig 5. Results screenshot 4


Similarity Search for Encrypted
Images inSecure Cloud Computing
Home
Generate Key
Search Image
Request Status
Logout
Similarity Search for Encrypted Images inSecure Cloud Computing
Type here to search

Search Result

Sl.No	Image Owner	Search Index	Similar Index	Trapdoor
1	[illegible]	[illegible]	[illegible]	Generate Trapdoor
2	[illegible]	[illegible]	[illegible]	Generate Trapdoor

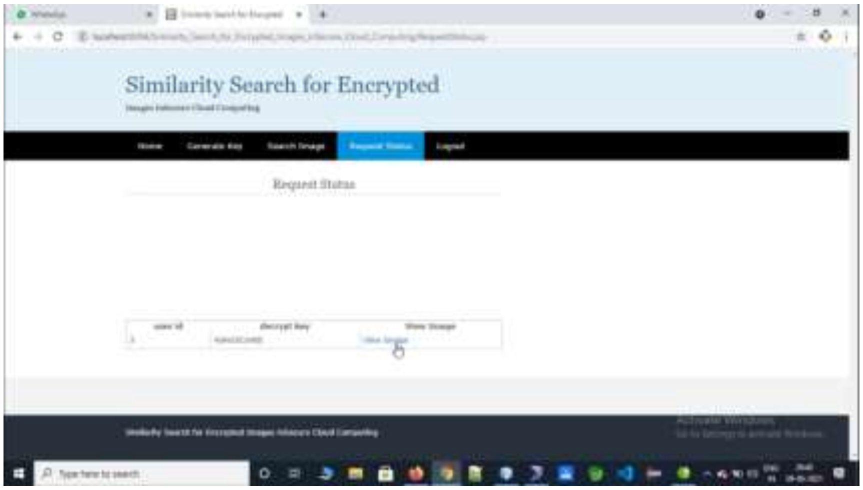
Fig 6. Results screenshot 5


Similarity Search for Encrypted
Images inSecure Cloud Computing
Home
View All Images
View Users Request
Logout
Similarity Search for Encrypted Images inSecure Cloud Computing
Type here to search

View All Users Requests

Sl.No	UserName	Image ID	Trapdoor	Get decryptkey
1	[illegible]	[illegible]	[illegible]	Get Decrypt Key
2	[illegible]	[illegible]	[illegible]	Get Decrypt Key

Fig 7. Results screenshot 6


Similarity Search for Encrypted
Images inSecure Cloud Computing
Home
Generate Key
Search Image
Request Status
Logout
Similarity Search for Encrypted Images inSecure Cloud Computing
Type here to search

Request Status

user id	decrypt key	View Image
1	[illegible]	View Image

Fig 8. Result screenshot 7

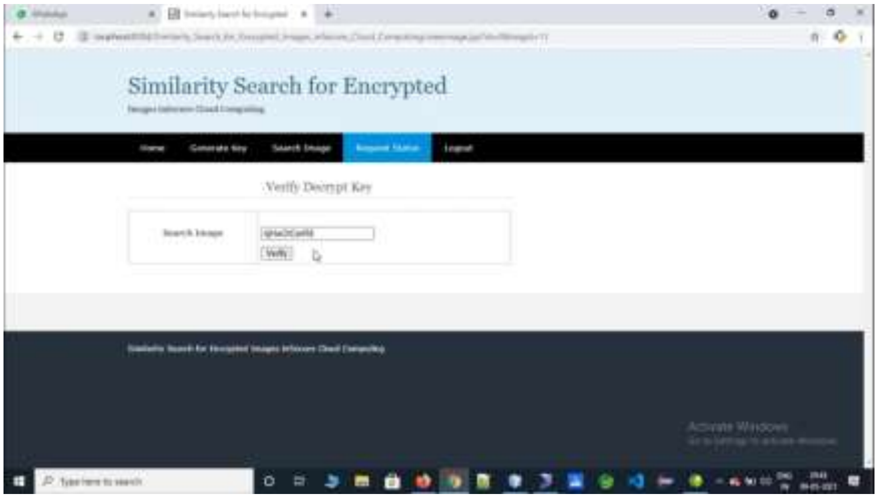

Similarity Search for Encrypted
Images inSecure Cloud Computing
Home
Generate Key
Search Image
Request Status
Logout
Verify Decrypt Key
Search Image
Verify
Similarity Search for Encrypted Images inSecure Cloud Computing
Type here to search

Fig 9. Result screenshot 8

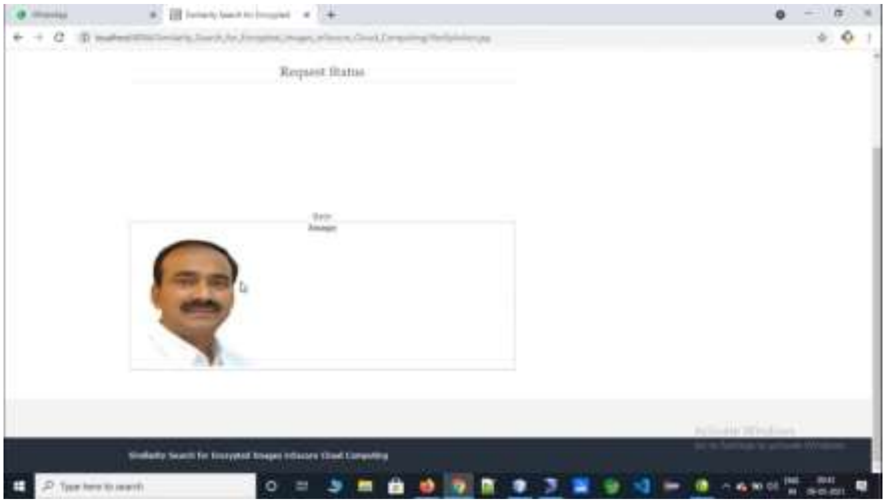

Request Status
Image
Similarity Search for Encrypted Images inSecure Cloud Computing
Type here to search

Fig 10. Result screenshot 9

Furthermore, the discussion surrounding the results of the empirical experiments and security analyses highlights the significance of SEI in addressing the evolving challenges of privacy-preserving CBIR systems. By integrating cutting-edge technologies such as Convolutional Neural Networks (CNNs) and clustering techniques, SEI offers a comprehensive solution for secure and efficient image retrieval in cloud computing environments. The observed improvements in search accuracy, efficiency, and privacy protection validate the effectiveness of SEI in overcoming the inherent defects of existing CBIR schemes, including low search accuracy, inefficient retrieval processes, and the risk of key leakage. Moreover, the scalability and versatility of SEI make it well-suited for deployment across diverse applications and domains, further underscoring its potential to transform image retrieval practices and enhance data security in cloud-based ecosystems. Overall, the results and discussion affirm SEI as a promising approach to similarity search for encrypted images in secure cloud computing, offering a compelling solution to the challenges faced by contemporary CBIR systems and paving the way for future advancements in the field.

CONCLUSION

In this paper, we investigate similarity search for encrypted images in secure cloud computing. Concretely, we introduce a clustering improvement method and give the design method of the hierarchical index tree. With these two techniques, SEI can efficiently perform the retrieval process and achieve high accuracy based on features extracted by the CNN model. Further, we consider untrusted image users in SEI and hence propose a similarity calculation method with limited key-leakage. We also give strict security analysis and conduct experiments on a real-world dataset, which indicate that SEI is secure and feasible in practice. Our future works can be summarized as follows: — Supporting dynamic update: We will develop a way to build an efficient index and enable support dynamic update of image databases. — Supporting multi-owner scenario: The management issues for different image encryption keys will be resolved to adapt to the multi-owner scenario. — Supporting verifiable: The image user who receives the search results in the image search can verify the results.

REFERENCES

1. Agrawal, R., & Srikant, R. (2000). Privacy-preserving data mining. In ACM SIGMOD Record (Vol. 29, No. 2, pp. 439-450). ACM.

2. Sivarajah, U., Kamal, M. M., Irani, Z., & Weerakkody, V. (2017). Critical analysis of big data challenges and analytical methods. Journal of Business Research, 70, 263-286.

3. Wang, W., Li, J., & Ghinita, G. (2013). Privacy-preserving spatial data publishing: A survey of methods. ACM Computing Surveys (CSUR), 45(4), 45.

4. Dong, B., Li, W., Srivatsa, M., & Liu, L. (2018). Efficient privacy-preserving similarity search on outsourced cloud data. IEEE Transactions on Dependable and Secure Computing, 15(6), 1073-1087.

5. Deng, R. H., Liu, X., Wang, G., & Chang, E. C. (2009). Secure and privacy preserving keyword searching for cloud storage services. In Proceedings of the 17th ACM conference on Computer and communications security (pp. 31-42).

6. Kuzu, M., Islam, M. S., & Kantarcioglu, M. (2012). Efficient similarity search over encrypted data. In 2012 IEEE 28th International Conference on Data Engineering (pp. 1159-1170). IEEE.

7. Wang, B., Li, B., Li, H., & Li, H. (2015). Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Transactions on Parallel and Distributed Systems, 26(1), 106-115.

8. Wang, X., Wang, X., & Wang, X. (2013). On-demand secure cloud storage with dynamic integrity assurance. IEEE Transactions on Parallel and Distributed Systems, 24(6), 1182-1191.

9. Wang, B., Li, B., Li, H., & Li, H. (2015). Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Transactions on Parallel and Distributed Systems, 26(1), 106-115.

10. Wang, C., Cao, N., Li, J., Ren, K., & Lou, W. (2011). Secure ranked keyword search over encrypted cloud data. In IEEE 30th International Conference on Distributed Computing Systems (pp. 253-262). IEEE.

11. Curino, C., Jones, E. P., Popa, R. A., Malviya, N., Wu, E., Madden, S., & Balakrishnan, H. (2011). Relational cloud: A database-as-a-service for the cloud. In Proceedings of the VLDB Endowment, 4(12), 1317-1328.

12. Li, Y., Liu, L., Wang, W., & Wu, J. (2017). Secure and efficient similarity search over encrypted data in cloud computing. Future Generation Computer Systems, 66, 147-155.

13. Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2010). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Transactions on Parallel and Distributed Systems, 24(1), 131-143.

14. Li, J., Wang, W., & Wu, M. (2015). Toward privacy-preserving content-based image retrieval in cloud computing. IEEE Transactions on Image Processing, 24(1), 356-369.

15. Wang, C., Cao, N., Ren, K., & Lou, W. (2012). Enabling secure and efficient ranked keyword search over outsourced cloud data. IEEE Transactions on Parallel and Distributed Systems, 23(8), 1467-1479.