M. Mohanedova *et al*, International Journal of Advances in Agricultural Science & Technology,
Vol.11 Issue.4, April 2024, pg. 1-9

ISSN: 2348-1358

Impact Factor: 6.901

**NAAS Rating: 3.77**

# Securing Image Retrieval: A Blockchain-Based Encrypted Approach

Mr.K.Shamsri[1] ,Guttula Naga Bhavya Sri[2], Gunipe Abhinav[3],Adipudi Kamala Gayatri Satwika[4], Jatla Vinay Babu[5], Dhruv Parekh[6] , [1]Assistant Professor, [2,3,4,5, 6] B.tech Students Department of Computer Science Engineering, Pragati Engineering College, Surampalem , Andhra Pradesh, India
Email: shamsri.k@pragati.ac.in

**Abstract:**

Malicious cloud servers can pose a hazard to encrypted picture retrieval, leading to incomplete or incorrect results. The majority of current systems do not verify the completeness of search results, instead concentrating on retrieval performance and accuracy. We explore properties of blockchains including decentralization and tamper-proofing to achieve transparency and dependability in search results, and we suggest a blockchain-based encrypted picture retrieval system. Using the blockchain consensus process and the smart contract's search function, this method maintains the encrypted index on the Ethereum blockchain, guarantees the accuracy and integrity of search results. It then uses a cloud server to host the corresponding encrypted images in order to save storage costs. Finally, it creates a double-layer index structure by utilizing a simhash and a bag of visual word model in the image similarity index process. Experiments demonstrate that the scheme's accuracy, high retrieval efficiency, and dependability also have a positive impact on privacy protection.

**Keywords:**encrypted image retrieval, blockchain, searchableencryption, locality-sensitive hashing, attribute-based encryption

## I. Introduction

More and more enterprises and individuals use cloud computingplatform [1] to outsource a large number of images to cloud service centres (such as Amazon EC2) to reduce localstorage costs and computing resource consumption. However,the cloud service centre has lost user data due to internalreasons and external attacks in recent years. Therefore, toensure image security and prevent privacy leakage, usersencrypt the data before outsourcing them to the cloud server.However, the encrypted images lose the plaintext feature, andthe user cannot efficiently retrieve the images and affect themanagement of the images.Searchable encryption [2] [3] supports the simultaneousrealization of image confidentiality and search of encryptedimages, which ensures the security and availability of images,and realizes the search of encrypted data without disclosing theprivacy of user data. However, most image retrieval schemes

based on searchable encryption [4] [5] do not pay enoughattention to the problem of the malicious cloud server, which

may return error results. Although some related research workproposed verification schemes to let data owners verify theintegrity of search results, these schemes were highly dependenton the unique index structure and did not support fine-grainedaccess control for users' search rights. It is difficultto construct a general authentication structure to

ISSN: 2348-1358

Impact Factor: 6.901

**NAAS Rating: 3.77**

verify thesimilarity calculation process of images, the verification of.encrypted image retrieval results is faced with great challenges.

Besides, there is still a problem as shown in Fig. 1. Whenusers need to query the information of a car as shown in theleft of Fig. 1, and the background is a desert environment, theyhope to get more images of similar cars to understand theirinformation, such as car brand and model. However, as shownin the right of Fig. 1, the results of similar images retrievedare only desert and mound images related to the background,which cannot well reflect the users' real goals and interests.So how to narrow the gap between image semantics and itsfeature descriptors, and better capture the user's interest is alsoa considerable challenge.

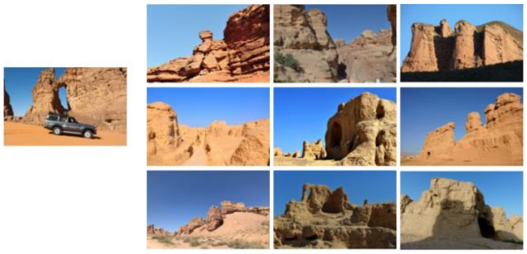


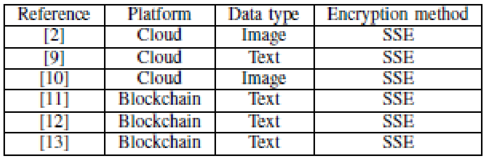
**Fig 1.Illustrative Example**

## II. LITERATURESURVEY

The related work of this paper can be divided into two parts:

1)encrypted image retrieval: This paper mainly introduces thedevelopment of related technologies to protect image privacyin the process of image retrieval; 2) symmetric searchableencryption and blockchain: This paper mainly introduces thecurrent work on how to better solve the problem of imageprivacy.A. Encrypted Image RetrievalIn 2015, Yuan et al. proposed an encryption domainimage retrieval algorithm with access control function, whichcan manage the user's access rights to the image, and realizethe access of different user roles to the image. Xia et al.propose a scheme that supports CBIR over encrypted images.They extracted feature vectors to represent the correspondingimages, and the pre-filter tables are constructed by locality sensitivehashing to increase search efficiency. In 2019, Qinet al. The Speeded-Up Robust Features technique and the Bag of Words model are used to create the feature vectors for each image, and the enhanced Harris algorithm is used to extract the image features. Next, the feature vectors' searchable index is created using the Local Sensitive Hash technique. Before sending an image to a cloud server, encryption is frequently carried out to safeguard its privacy. You can utilize a variety of encryption technologies, such RSA or AES. While encryption guarantees the security of the data content, it frequently complicates the index construction process.B.SSE and BlockchainCryptologists have proposed symmetric searchable encryption(SSE) to support the sublinear search of encrypteddata. Wang et al. designed an SSE scheme for image sby using local sensitive hashing (LSH), which does not relyon homomorphic encryption, but has the problem of linearsearch complexity on the dataset. Cui et al. also designeda scheme based on LSH. However, due to the complex processof building search credentials, the overall efficiency of thescheme is still very low.Reference showed that the technology can not only beused for the precise search of text data but also similaritysearch of images. As shown in Table I, referencesproposed encrypted image retrieval solutions on the cloudplatform, in which encrypted images and indexes are storedin cloud servers. References has proposed tointegrate blockchain into searchable encryption to realize adecentralized, reliable, and verifiable retrieval scheme. References used smart contracts to store security index andperform a search to solve the problem that the cloud serverreturns incorrect results but does not support the similarity.

TABLE I
SSE-BASED ENCRYPTED RETRIEVAL SCHEME



| Reference | Platform | Data type | Encryption method |
|---|---|---|---|
| [2] | Cloud | Image | SSE |
| [9] | Cloud | Text | SSE |
| [10] | Cloud | Image | SSE |
| [11] | Blockchain | Text | SSE |
| [12] | Blockchain | Text | SSE |
| [13] | Blockchain | Text | SSE |

search. Reference [13] stored both ciphertext database andencrypted index in the smart contract, which greatly increasesthe storage cost and causes unnecessary waste.In the above-related work, encrypted image retrieval still has some problems, such as complex index building process,low retrieval efficiency, and retrieval accuracy, a s well a s thethreat of malicious cloud servers. We propose a blockchain basedencrypted image retrieval service scheme BEIR to solvethem.

## III.SYSTEM ANALYSIS

### A. EXISTING SYSTEM

The existing system for encrypted image retrieval faces challenges, primarily centered around the potential compromise of results by malicious cloud servers. While current solutions emphasize retrieval efficiency and accuracy, they often lack a robust verification mechanism for ensuring the completeness of search results. To address this limitation, the proposed "Blockchain-Based Encrypted Image Retrieval Scheme" explores the decentralized and tamper-proof features of blockchain technology. In this existing system, the encrypted index is stored on the Ethereum blockchain, leveraging the blockchain's consensus mechanism and smart contract functionality for secure and transparent search operations. The scheme employs a double-layer index structure, combining the bag of visual word model and simhash for image similarity indexing. This not only enhances retrieval efficiency and precision but also contributes to the privacy protection of user data. Furthermore, the system optimizes storage costs by outsourcing corresponding encrypted images to a cloud server. Experimental results demonstrate the reliability, high retrieval efficiency, precision, and privacy protection efficacy of the existing system.

### DISADVANTAGES OF THE EXISTING SYSTEM

**Blockchain Scalability**: Blockchain networks, particularly Ethereum, may face scalability issues as the volume of transactions and data increases. This could impact the speed and efficiency of image retrieval operations.

**Transaction Costs**: The use of blockchain involves transaction fees, and in the case of Ethereum, gas fees. These costs can become significant, especially when performing frequent image retrieval operations or uploading large amounts of data to the blockchain.

ISSN: 2348-1358

Impact Factor: 6.901

**NAAS Rating: 3.77**

**Latency in Search Operations**: The decentralized nature of blockchain introduces some latency in search operations due to the consensus mechanisms and communication between nodes. In scenarios where low-latency retrieval is crucial, this delay could be a limitation.

**Blockchain Security Considerations**: While blockchain provides tamper-proofing, the security of the overall system is still dependent on the robustness of the chosen blockchain network. Vulnerabilities or attacks on the underlying blockchain infrastructure could compromise the security of the encrypted image retrieval scheme.

**Smart Contract Vulnerabilities**:Smart contracts, being integral to the proposed system, may be susceptible to vulnerabilities such as bugs or exploits. Security audits and rigorous testing are essential to minimize these risks.

## B. PROPOSED SYSTEM

The proposed system, "Blockchain-Based Encrypted Image Retrieval Scheme," builds upon the identified limitations of the existing system to introduce innovative enhancements for improved performance, security, and functionality. In the proposed system, efforts are directed towards mitigating the scalability concerns of blockchain networks by exploring potential solutions or adopting alternative blockchain platforms with improved scalability features.

To address transaction costs associated with blockchain operations, optimization strategies are proposed, such as batch processing or the utilization of layer 2 solutions, to reduce the overall cost of executing image retrieval transactions on the blockchain. Additionally, mechanisms are implemented to minimize latency in search operations, potentially through the optimization of consensus algorithms or the integration of caching mechanisms to enhance the speed of query processing.

Security measures are further strengthened in the proposed system by conducting thorough security audits of smart contracts and implementing additional safeguards to protect against potential vulnerabilities or exploits. The integration of advanced encryption techniques and secure key management practices ensures the privacy and integrity of both the encrypted index on the blockchain and the outsourced encrypted images on cloud servers.

Moreover, the proposed system aims to address the limitations in handling complex queries by introducing improvements in query processing capabilities, allowing for more versatile and sophisticated image retrieval tasks. The dependency on cloud servers is carefully managed by selecting reputable and secure service providers, implementing redundancy measures, and enhancing the overall robustness of the system against potential cloud-related risks.

## ADVANTAGES OF THE PROPOSED SYSTEM

The proposed "Blockchain-Based Encrypted Image Retrieval Scheme" offers several advantages over the existing system, addressing key limitations and introducing innovative features. Some of the notable advantages of the proposed system include:

**Enhanced Scalability**:

The proposed system incorporates solutions to improve the scalability of blockchain networks, ensuring efficient handling of a growing volume of transactions and data. This enhancement enables the system to scale more effectively as the demand for image retrieval operations increases.

**Cost Optimization**:

Optimization strategies are implemented to address transaction costs associated with blockchain operations. Batch processing and the exploration of layer 2 solutions contribute to reducing overall transaction costs, making the system more cost-effective and sustainable.

**Reduced Latency**:

Latency in search operations is minimized through the introduction of optimization techniques, such as enhanced consensus algorithms and caching mechanisms. This results in faster query processing, making the image retrieval system more responsive and user-friendly.

**Improved Security Measures**:

Thorough security audits of smart contracts and the implementation of additional safeguards contribute to a more secure system. Advanced encryption techniques and secure key management practices enhance the overall security of both the encrypted index on the blockchain and the outsourced encrypted images on cloud servers.

## IV.SYSTEM DESIGN

### SYSTEM ARCHITECTURE

Below diagram depicts the whole system architecture.

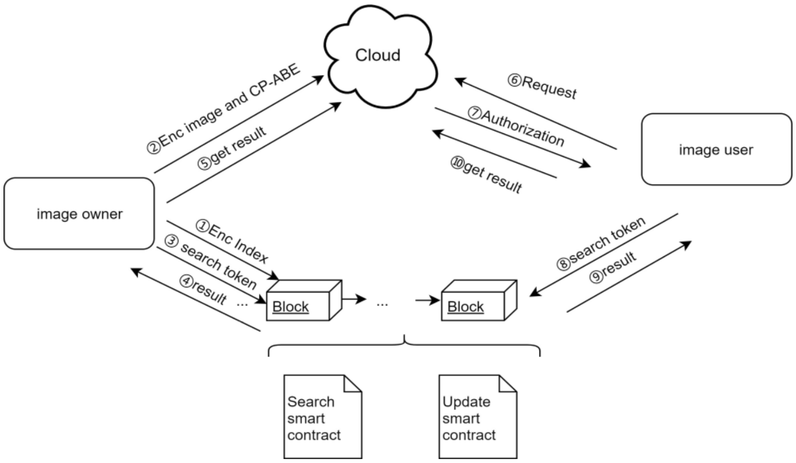


**Fig 2. Methodology followed for proposed model**

## V. SYSTEM IMPLEMENTATION

### MODULES

**Blockchain Integration Module**:

This module focuses on the integration of blockchain technology, particularly Ethereum, into the system. It includes functionalities for storing the encrypted index on the blockchain, managing transactions, and leveraging the consensus mechanism for ensuring the integrity and tamper-proof nature of the data.

**Smart Contract and Search Module**:

ISSN: 2348-1358

Impact Factor: 6.901

**NAAS Rating: 3.77**

The smart contract and search module are dedicated to the implementation of smart contracts for handling search operations. It involves the development of functions within the smart contract that facilitate secure and transparent image retrieval, ensuring the correctness of search results through blockchain-based verification.

**Image Similarity Indexing Module**:

This module is responsible for creating a robust image similarity index. It incorporates a double-layer index structure that utilizes both the bag of visual word model and simhash. The module involves the design and implementation of algorithms to efficiently process and index encrypted images, enhancing retrieval efficiency and precision.

**Cloud Server Interaction Module**:

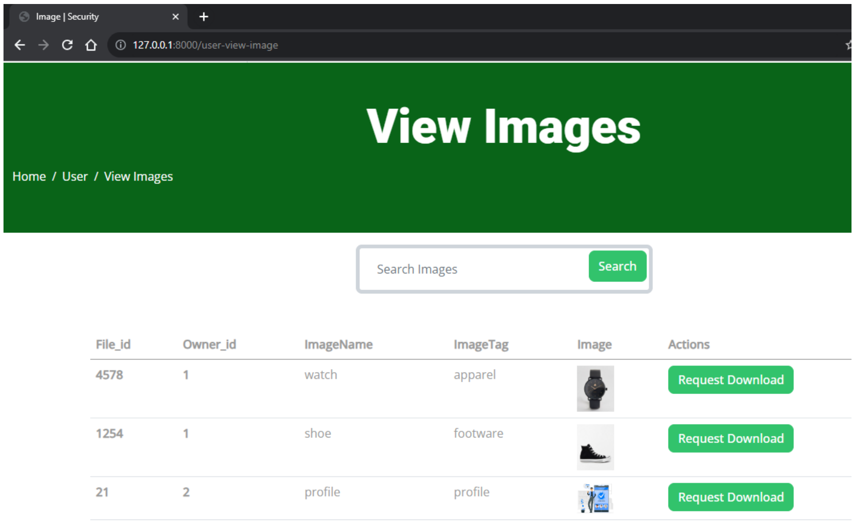
The cloud server interaction module manages the outsourcing of encrypted images to cloud servers. It includes functionalities for securely transmitting and storing encrypted images on the cloud, optimizing storage costs, and implementing measures to ensure the reliability and privacy of outsourced data.

**Privacy Protection and Security Module**:

This module is dedicated to privacy protection and security measures throughout the system. It encompasses advanced encryption techniques for securing both the index on the blockchain and the outsourced images. Additionally, it includes security audits of smart contracts, secure key management practices, and measures to address privacy concerns associated with cloud outsourcing.

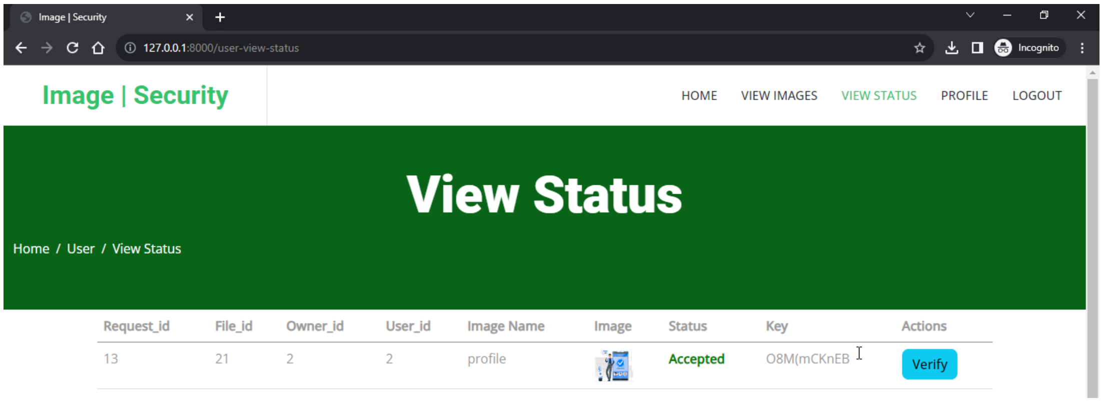
## VI .RESULTS AND DISCUSSION

Experimental configuration: 8GB memory Intel (R) Core(TM) i7-7700 3.20hz, and the operating system is MicrosoftWindows 10 64bit. We conduct the encryption index processof the image service provider on this computer and test thetime consumption of storage, search, and update on the smartcontract to evaluate our design scheme. To evaluate the actualperformance of the scheme more accurately, we used threefamous real data sets, namely holiday, Oxford 5K, and UKbench. The first data set is about 1491 pictures taken duringpersonal holidays, mainly landscape. In the second data set,there are 5062 maps for 11 different landmarks, and eachlandmark is represented by five possible queries. The thirddata set is 10200 graphs in 2550 different scenarios.



| File_id | Owner_id | ImageName | ImageTag | Image | Actions |
|---|---|---|---|---|---|
| 4578 | 1 | watch | apparel | | Request Download |
| 1254 | 1 | shoe | footware | | Request Download |
| 21 | 2 | profile | profile | | Request Download |

Fig 3. Viewing Searched Images



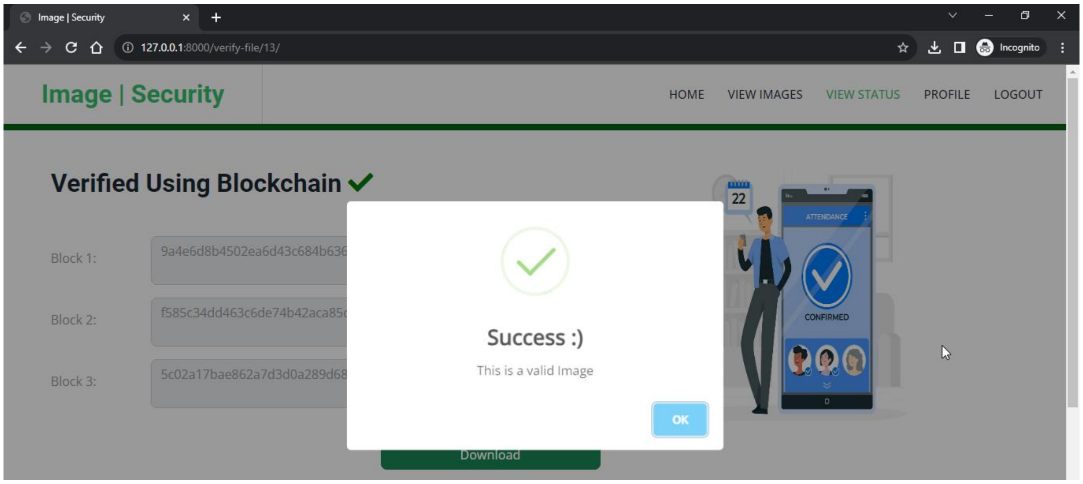
| Request_id | File_id | Owner_id | User_id | Image Name | Image | Status | Key | Actions |
|---|---|---|---|---|---|---|---|---|
| 13 | 21 | 2 | 2 | profile | | Accepted | O8M(mCKnEB | Verify |

Fig 4. Verifying Retrieved Images

ISSN: 2348-1358

Impact Factor: 6.901

**NAAS Rating: 3.77**



Verified Using Blockchain ✓

Block 1: 9a4e6d8b4502ea6d43c684b636

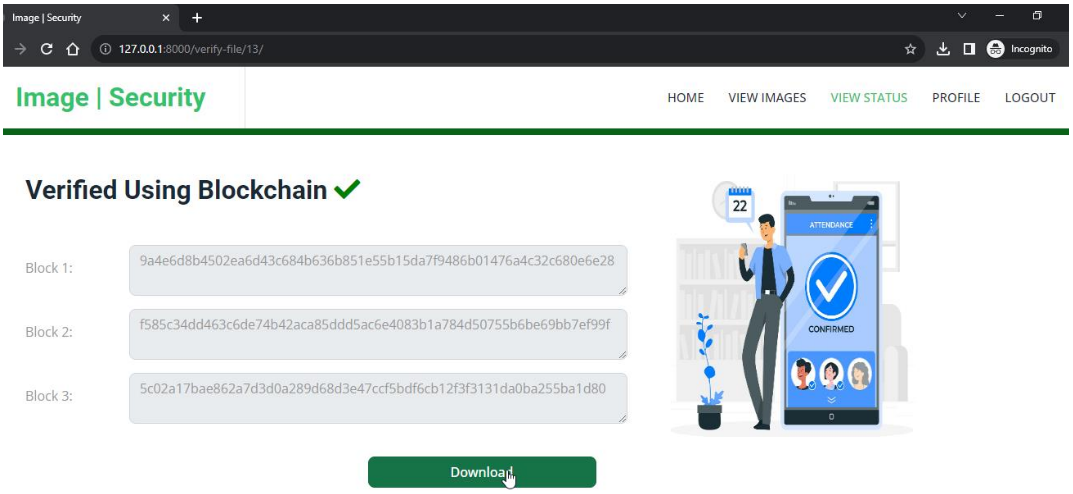
Block 2: f585c34dd463c6de74b42aca85c

Block 3: 5c02a17bae862a7d3d0a289d68

Success :)

This is a valid Image

Fig 5. Successfully verified the Retrieved Image



Verified Using Blockchain ✓

Block 1: 9a4e6d8b4502ea6d43c684b636b851e55b15da7f9486b01476a4c32c680e6e28

Block 2: f585c34dd463c6de74b42aca85ddd5ac6e4083b1a784d50755b6be69bb7ef99f

Block 3: 5c02a17bae862a7d3d0a289d68d3e47ccf5bdf6cb12f3f3131da0ba255ba1d80

**Fig 6.Verification Using Blockchain**

## VI I.CONCLUSION AD FUTURE WORK

In this paper, we propose an encrypted image retrieval scheme based on blockchain, which can solve the problem that the malicious cloud server returns wrong or incomplete search results by searching on the smart contract. Besides, we also design an index structure using bag of visual word (BOVW) model and simhash to improve the efficiency and accuracy of image retrieval, and the index generation process of this scheme can also be modularized into other searchable encryption schemes. We just hope that more researchers can use blockchain to solve the trust problems encountered in the process of encrypted image search, and spend more energy exploring faster and more accurate encrypted image retrieval schemes, and finally realize encrypted image retrieval on the blockchain. At present, the cost of our privacy protection works on blockchain, such as the retrieval of the encrypted index, is still not very ideal compared with the traditional cloud server. In our future work, we will also try to include trusted execution

ISSN: 2348-1358

Impact Factor: 6.901

**NAAS Rating: 3.77**

environment tee, homomorphic encryption, secure multi-party computing (SMC), and zero-knowledge proof, to further reduce the cost without disclosing image privacy. At the same time, we explore the feature fusion based on convolutional neural network and principal component analysis in the process of index establishment, which has achieved better similarity matching effect.

## REFERENCES :

[1] Rittinghouse, John, and James Ransome. Cloud Computing: Implementation, Management, and Security. 2009.

[2] Li, Minghui, et al. “InstantCryptoGram: Secure Image Retrieval Service.” IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, 2018, pp. 2222–2230.

[3] Wang, Qian, et al. “Searchable Encryption over Feature-Rich Data.” IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 3, 2018, pp. 496–510.

[4] Jarecki, Stanislaw, et al. “Outsourced Symmetric Private Information Retrieval.” IACR Cryptology EPrint Archive, vol. 2013, 2013, p. 720.

[5] Wang, Qian, et al. “SecGDB: Graph Encryption for Exact Shortest Distance Queries with Efficient Updates.” International Conference on Financial Cryptography and Data Security, 2017, pp. 79–97.

[6] Yuan, Jiawei, et al. “SEISA: Secure and Efficient Encrypted Image Search with Access Control.” 2015 IEEE Conference on Computer Communications (INFOCOM), 2015, pp. 2083–2091.

[7] Xia, Zhihua, et al. “A Privacy-Preserving and Copy-Deterrence ContentBased Image Retrieval Scheme in Cloud Computing.” IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, 2016, pp. 2594–2608.

[8] Qin, Jiaohua, et al. “An Encrypted Image Retrieval Method Based on Harris Corner Optimization and LSH in Cloud Computing.” IEEE Access, vol. 7, 2019, pp. 24626–24633.

[9] Kamara, Seny, et al. “Dynamic Searchable Symmetric Encryption.” IACR Cryptology EPrint Archive, vol. 2012, 2012, p. 530.

[10] Cui, Helei, et al. “Harnessing Encrypted Data in Cloud for Secure and Efficient Mobile Image Sharing.” IEEE Transactions on Mobile Computing, vol. 16, no. 5, 2017, pp. 1315–1329.

[11] Wang, Shangping, et al. “A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems.” IEEE Access, vol. 6, 2018, pp. 38437–38450.

[12] Hu, Shengshan, et al. “Searching an Encrypted Cloud Meets Blockchain: A Decentralized, Reliable and Fair Realization.” IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, 2018, pp. 792–800.

[13] Chen, Lanxiang, et al. “Blockchain Based Searchable Encryption for Electronic Health Record Sharing.” Future Generation Computer Systems, vol. 95, 2019, pp. 420–429.

[14] Shen, Meng, et al. “Privacy-Preserving Image Retrieval for Medical IoT Systems: A Blockchain-Based Approach.” IEEE Network, vol. 33, no. 5, 2019, pp. 27–33.