|| Volume 6 || Issue 5 || May 2021 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

CONTENT BASED IMAGE RETRIEVAL FOR ENCRYPTED IMAGES IN CLOUD COMPUTING

Mr. Ajitkumar Kadam[1], Prof. Vandana Navale[2]
PG Student, Computer Engineering, Dhole Patil College of Engineering, Pune, India[1]
Faculty, Computer Engineering, Dhole Patil College of Engineering, Pune, India[2]
ajitkumar.kadam@gmail.com[1], vandananavale@dpcoepune.edu.in[2]

Abstract: - In today's world, cloud computing is crucial for data storage and cost reduction for businesses. The storage needs for visual data have grown in recent years as a result of the proliferation of interactive multimedia services and apps for mobile devices in both personal and commercial settings. This is a critical consideration when deciding whether to use cloud-based data outsourcing services. However, our decision to store data on the cloud creates additional security issues that must be properly handled. A safe system for storing and retrieving subcontracted privacy measures in huge collections of shared photos is proposed. Our approach is based on IES-CBIR, a novel image encryption technique with content-based picture recovery capabilities. This architecture provides for both secured storage and discovery using content-based picture retrieval queries, all while retaining anonymity from trustworthy yet curious cloud administrators. We provided a framework that was examined and evaluated in terms of security, as well as performance and retrieval accuracy. Our results show that IES-CBIR is probably safer, allowing existing proposals to be handled more efficiently in both time and space complexity and paving the way for new scenarios of practical application.

Keywords: - *Encrypted Data Processing; Searchable Encryption; Content-Based Image Retrieval, Cloud Storage.*

I INTRODUCTION

Image retrieval based on content is often referred to as image retrieval with content. Visual information based on content retrieval Artificial vision is being used to help in recuperation. Shape, a massive digital picture search database, has a big picture retrieval database. The term "content-based" refers to study that examines the image's actual content. Time is of the essence. Color, shape, texture, and any other information that may be gleaned from the image itself is referred to as "material" in this context. Image content should be dependent on searches if you don't have the capacity to inspect it. Titles and keywords are examples of metadata. A person must develop and store this info. Each and every image in the database A retrieval of images to match user demand, returns a sequence of photographs from the system's collection Images in database With similarity ratings such as image material similarity, border form, color similarity, and so forth. To access, study, and retrieve a sequence of comparable photos in real time, use an image retrieval system. It is now feasible to create a larger and more complete digital picture library as a consequence of recent improvements in digital storage technology. There might be millions of photographs and Terabytes of data in the collection.

It is vital to build Effective Research Methods in order to match the users' advantages of these databases. Prior to the use of automatic indexing methods, picture databases were indexed and inserted based on the keyword of a human classifier. Unfortunately, there are two major downsides to this method. First and foremost, as a database grows in size, the labor required to index each image becomes increasingly difficult. Second, the same photographs can be indexed inconsistently by two different persons, or even the same person on two separate days. Inability generates a search result. Isn't the best for the system's end users.

The fact that a computer can generate CBIR indexes based on the scheme. Fix any sequencing issues that are caused by humans. Because a computer can process a large number of photos at a high rate without becoming overburdened, to get best outcomes, each CBIR in the system, for example, must be changed in order of its specific application. Poor mechanism for recovering tropical satellite photos Designed a recovery system Medical X-ray pictures would certainly be one to consult South American forests. Algorithms, too, the essence that is now being utilized cannot be removed indefinitely. Emotional Feedback, for example, is a feature of visuals.

Various catch-up strategies have been developed. Image characteristics are determined via direct computation of the image's content. The characteristics of an image are produced immediately. by a compressed data sequence that is particular The decoding procedure is completed with no block or semitone truncation encoding. There are two parts to this picture recovery plan: sequencing and searching for a collection of related photographs in the database. The sequencing stage eliminates all picture features from the database, which is then saved as a

feature vector in the database. Retrieves during the search phase.

II RELATED WORK

"Pop: Privacy-preserving outsourced photo sharing and searching for mobile devices,"

They present POP, a framework that allows privacy-conscious mobile device users to safely outsource cumbersome photo sharing and searches to untrusted servers. Unauthorized parties do not have access to photographs or search queries, including the server. This is accomplished through a carefully planned architecture and unique non- interactive privacy-preserving picture comparison methods. [1]

"**Real-time semantic search using approximate methodology for large-scale storage systems,"**

They propose FAST, a semantic queries-based approach that is near-real-time and cost- effective. The concept behind FAST is to use correlation-aware hashing and managed flat-structured addressing to investigate and exploit semantic correlation inside and among datasets in order to dramatically reduce processing time without incurring a tolerable loss of data-search accuracy. [2]

"Securing sift: Privacy-preserving outsourcing computation of feature extractions over encrypted image data,"

They describe a new technique that meets efficiency and security criteria while preserving essential features by randomly partitioning the original picture data, creating two unique efficient protocols for safe multiplication and comparison, and carefully spreading the feature extraction computations across two different cloud servers. [3]

"A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing,"

They presented a method for implementing CBIR over encrypted photos without exposing sensitive data to the cloud server. To begin, feature vectors representing the matching photos are retrieved. To improve search efficiency, the pre-filter tables are then built using locality-sensitive hashing.[4]

III PROPOSED METHODOLOGY

In a large collection of shared photos, we present a safe architecture for storing and recovering subcontracted privacy protection. Based on CBIR, Picture offers a new encryption technique that presents image retrieval features based on content. The system enables for encrypted storage as well as search utilizing a content-based picture retrieval query, all while maintaining privacy against an honest but curious Cloud Administrator. The suggested framework was officially studied and evaluated once we created a prototype of it.

It was evaluated experimentally for its safety qualities. Recovery accuracy and performance. Our findings show that CBIR is most likely safe, allowing for more efficient operation of the existing plan, both in terms of time and space complexity, and paving the way for new scenarios of practical use.

A.Benefits of the proposed system

•The proposed technique promotes the protection of picture data privacy

•The suggested approach will produce more accurate results by employing the shape-based invariant texture index (SITI) Descriptor.

•In the suggested method, data is encrypted before being saved. The format will have a high level of security.

•Access control will be used to preserve security.

•Additionally, the user's image Pre-Shared Key will be used to preserve security.

B.Proposed system architecture

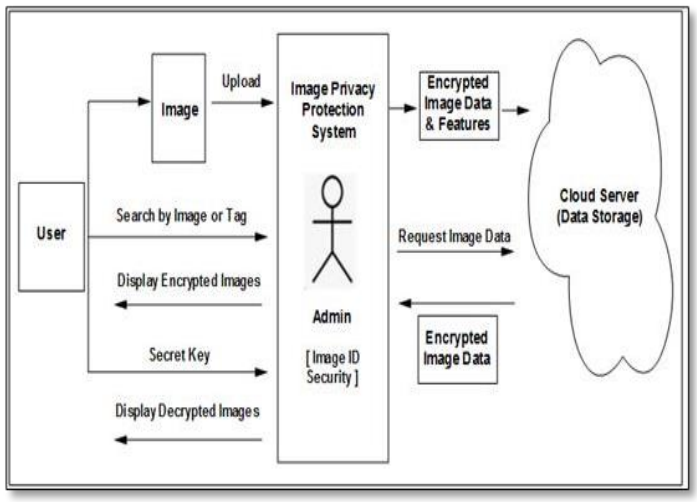

Fig. 1. Architecture

C. Algorithms

I.AES Algorithm

It is a symmetric algorithm. It used to convert plain text In cipher text. Need to come with this ego Weakness in DES / RSA. DES does not have a 56 bit key Long-term protection against attacks based on the entire key Also consider searches and 64-bit blocks as weak. Blowfish was to be used with 128-bit blocks 128-bit keys.

Input:

128 bit / 192 bit / 256-bit input (0, 1) secret key (128.) Bit) + plain text (128 bit).

process:

10/12/14-round for 128 bit / 192 bit / 256-bit input Xor State Block (i / p)

Final Round: 10,12,14

Each round includes: sub byte, shift byte, mix column, Add round key. Output: Cipher Text (128 bit)

2. Size-based invariant texture index (SITI) feature Extraction Image Content Identification.

Steps:

1.One of the most often utilized visualizations is the color feature. Picture retrieval features, as well as their variations in image scaling, rotation, and translation A picture is separated into four blocks of equal size in this work. And a similar-sized concentrated picture. A 9-D color moment is generated for each Block, resulting in a color annotation dimension of 65 for each picture. The mean, standard deviation, and value of The skewness of each channel in the HSV color space are utilized to calculate the 9-D color moments of the picture segment.

2.Edge Detection: The majority of the size data in Animation is contained within edges. So, initially, we use these filters to detect the edges of a picture, and then we go on to the next step. The image sharpness and clarity will improve by increasing the sections of the image that involve edges.

II.Shape-based invariant texture index (SITI) for feature extraction

Feature extraction image content identification. Steps:

1.Because of its irreversibility in respect to picture scaling, rotation, and translation, the color feature is one of the most extensively employed visual characteristics in image retrieval. A picture is separated into four equal-sized blocks in this work, and one main picture is also separated into four equal-sized chunks. A 9-D color moment is generated for each block, resulting in a color annotation amplitude of 45 for each picture. The picture segment's 9-D color moment is employed, which includes the mean, standard deviation, and asymmetry values for each. HSV color space channel

2.Edge detection: The majority of an image's shape information is contained inside its edges. So, we first identify these edges in a picture, and then we use these filters to boost the sharpness and clarity of the picture by increasing the portions of the picture that contain edges.

Canny Edge Detection:

A helpful removal approach is canny edge detection. Structural data from a variety of visual objects is used to drastically minimize the quantity of data processed. It's been used in a variety of computer vision systems. Requirements for edge detection application have been discovered by Canny.

Various vision systems have a lot in common. As a result, one edge detection method that fulfil these requirements is available. It may be used in a variety of scenarios. The following are some common edge detection criteria:

a.Low-error edge detection, which means Booking must accurately store as much of the image's edges as possible.

b.The edge point identified by the operator must be correctly localized at the edge's center.

c.Only the image's provided edge should be noted. The image should not be noisy if at all feasible. Make a set of artificial edges.

IV RESULT AND DISCUSSION

The accuracy of the present Algorithm (global color) and the suggested system Algorithm is shown in this section (SITI algorithm). As a result, it functions better. The findings of content-based picture retrieval were compared to those of the current approach.

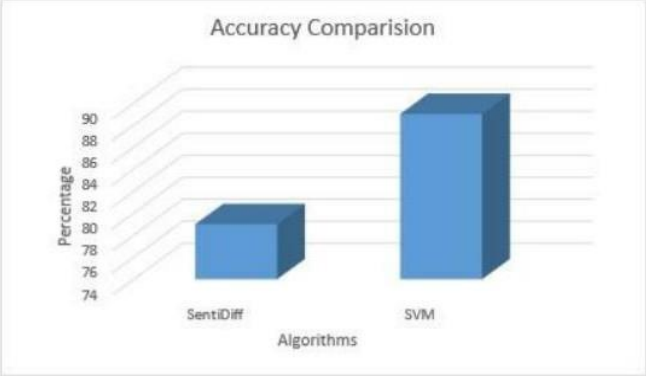

Fig. 2. Accuracy Graph

	Existing System	Proposed System
Accuracy	79.32	89.77

We utilized an image dataset and in these studies. Analyze theperformance of our system without using image compression. The graph below compares existing methodologies to experimental results for the search campaign. The displayed results are for a search Picture dataset with a random image from the Collection as the query (results represent averages 100 random runs each).

Image that has been encrypted and Local processing is represented by the encrypted picture feature. The user runs the query, while the cloud column is created automatically. Transmitting not only indicates network time spent querying and receiving results, but also time spent processing and calculating those results by the server.

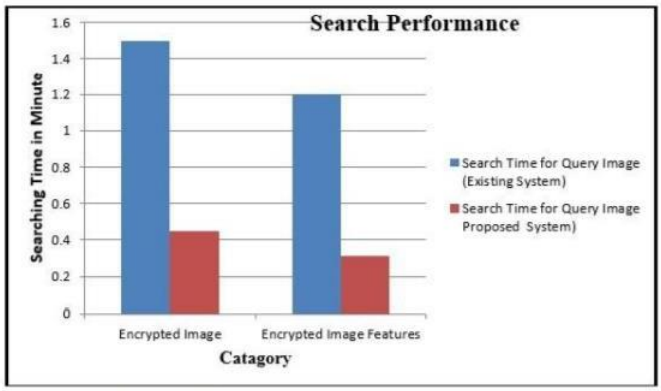

Fig. 3. Search Performance Graph

	Existing System	Proposed System
Encrypted Image	1.5min	0.45min
Encrypted Image Features	1.2min	0.43min

V CONCLUSION

We've developed a new approach for content-based search on large-scale photos that preserves privacy.

Most computationally difficult picture matching operations are outsourced to the cloud in a non-interactive manner, yet picture and query privacy is protected, thanks to our meticulous design.

To speed up the search process even further, the technology will allow the cloud to save the image ID, which serves as the index structure, and parallelize the search process without having to learn anything.

The shape-based invariant texture index will be used in the suggested system (SITI). As a result, the image content matching accuracy will be greater than it is now.

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.

[14]C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 8, pp. 1467–1479, Aug.2012.