JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

An Efficient Blockchain Assisted Similarity Search on Cloud Images

[1]Sudha Devi. K, [2]Subhiksha.G.B, [3]Vagrasri.S, [4]Varshini.S

[1]Associate Professor, [2]Student, [3]Student, [4]Student
[1]Computer Science and Engineering,
[1]Paavai Engineering College, Namakkal , India

Abstract : Image retrieval is a fundamental task in computer vision and has numerous applications in various fields. This abstract presents a method for image retrieval using query image features, specifically focusing on the popular Scale-Invariant Feature Transform (SIFT) algorithm for feature extraction and distance calculation. The proposed approach begins with the extraction of SIFT features from a collection of images, creating a database of keypoints and descriptors. These features capture the distinctive characteristics of local image regions, allowing for robust matching and retrieval. Another big problem is the security of private cloud data, which includes query queries, the search tree, and outsourced photos. First, employ a feature extraction approach for integrated picture features, which consist of basic elements like colour and shape. Specifically, the suggested method can achieve logarithmic search time since it makes use of a balancing index tree. Second, the secure inner product is used to encrypt the image and query feature. Install a mechanism to identify duplicate image content as well. When a query image is provided, SIFT feature extraction is performed on the query image, generating key points and descriptors that represent its visual attributes. Subsequently, a distance calculation technique, such as Euclidean distance is employed to compare the query image features with the features of images in the database. This comparison quantifies the similarity between the query image and the images in the database. Based on the calculated distances, the retrieved images are ranked according to their similarity to the query image. Images with smaller distances are considered more similar and are presented as the top-ranked search results. The image retrieval system employing SIFT feature extraction and distance calculation offers a robust and efficient solution for finding visually similar images in large databases. It enables applications such as content-based image search, image recommendation systems, and image clustering, contributing to advancements in fields such as multimedia retrieval, visual analytics, and image understanding.

Index Terms **- Image Storage, SIFT Feature Extraction, Duplicate Detection, Manhattan Distance Calculation, Similarity Identification, Image Retrieval.**

I.INTRODUCTION

The process of finding images that visually resemble a particular image is known as similarity-based image search. This method has certain drawbacks even though it has shown to be helpful in a variety of situations. The quality of the feature extraction and similarity metrics employed determines how accurate similarity-based image search can be. Images that share a similar visual aspect may not always share the same meaning or content. The context of an image is irrelevant when using similarity-based image search. Images that share a similar visual appearance might not share the same message or intended purpose. It is inefficient in managing changes in orientation, illumination, colour, and scale. Images that differ in lighting, colour, scale, orientation, or other aspects but share a similar content may not be recognised as such.

The method of safely searching for photos saved in cloud-based storage systems is called similarity-based image search. Before the photos are uploaded to the cloud, they are encrypted to prevent anyone from accessing them without the right decryption keys. Using machine learning methods, the images are first transformed into feature vectors in this methodology. After that, these feature vectors are uploaded to the cloud and encrypted using a safe encryption procedure. The query image that the user submits to search for a certain image is likewise transformed into a feature vector and encrypted using the same process. The cloud server receives the encrypted query vector after which it compares it to the encrypted feature vectors of the cloud-stored images.

The cloud server uses a similarity metric to compare the encrypted query vector with the encrypted feature vectors of the images. The similarity metric is designed to preserve privacy by ensuring that the similarity between two encrypted feature vectors is not revealed. The cloud server returns the encrypted feature vectors of the images that are most similar to the encrypted query vector. The client-side application then decrypts the returned encrypted feature vectors to obtain the corresponding images. This technique is useful in scenarios where privacy is a major concern, such as in medical image search or national security applications. By encrypting the images and using similarity-based search, it is possible to ensure that sensitive images are protected while still enabling efficient search and retrieval.

Cloud computing is the supply of accounting services via the Internet. With cloud administrations, individuals and groups can use equipment and programming that is remotely managed by third parties. Examples of cloud services include webmail, online business applications, online record storage, and long-distance informal contact areas. Access to data and PC assets is made possible by the cloud computing concept from any location where a system association is available. A shared pool of resources, such as systems, PC preparation power, information storage space, and focused business and client apps, is provided by cloud computing. Cloud computing's features include asset pooling, rapid adaptability, on-demand self-administration, extensive system access, and anticipated benefit. On-demand self-administration means that those clients, who are usually associations, have the ability to request

and manage their own specific processing resources. Broad system access makes it possible to provide services via private or public networks or the Internet. Clients in distant server farms can choose which resources to use from a pool of processing resources. The number of services offered can be small or large; the use of each service is estimated, and clients are billed according to need. Cloud computing administration models that are delegable include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). In Software as a Service demonstration, the required programming, hardware, software, and framework are included along with a pre-made application. In PaaS, a working framework, hardware, and system are provided, and the client adds or creates its own custom programming and applications on top of these. Only the equipment and system are provided by the IaaS display; the client must introduce or develop its own unique working frameworks, programming, and applications. Benefits notwithstanding, security and safety issues also exist. Data is transferred across the Internet and stored in distant locations. Additionally, cloud providers frequently serve multiple clients concurrently. The majority of this could increase the presentation's size to potential breaks, both accidental and deliberate. Many have voiced worry that cloud computing may result in data being used by cloud providers in a "capacity crawl" manner—a use not intended at the time the data was gathered and often without authorization. Since storing data on the cloud is so inexpensive, there are more incentives to explore new uses for it than there are to remove it from the cloud.

These days, no presentation would be complete without multimedia. It has been used for anything from education to entertainment. The need for multimedia content has grown as a result of the internet's development. To inform or amuse the user, multimedia employs a variety of information content formats and their processing, such as text, audio, video, graphics, animation, and interactivity. Multimedia also refers to the use of electronic media for multimedia content storage and interaction. Multimedia is similar to traditional mixed media in fine art, although it may be used much more widely. "Rich media" is another term for interactive multimedia, which is used in current times for content retrieval and search. "The process of finding interesting patterns from the large media data such as text, image, audio, and video that are not ordinarily accessible by basic queries and associated results" is the definition of multimedia data retrieval. Since the suggested system has to do with data retrieval, multimedia data searching and retrieval is a novel field of study that calls for background expertise in both the multimedia processing and data searching domains. The steps involved in retrieving multimedia data are primarily

(1) Domain understanding

(2) Data selection

(3) Data pre-processing, (cleaning and transformation)

(4) Patterns Evaluation

(5) Interpretation and

(6) Reporting and Knowledge discovery.

II. Related Work

Gao, et.al,…[1] present a safe and effective plan to have the unreliable cloud server handle the item reputation on hyperspectral remote sensing photos. The input and output privacy of the computation can be protected by the suggested technique. Additionally, expand on the efficient verification method in this suggested scheme such that it has the best probability of discovering cloud server misconduct. We provide here the most popular item popularity outsourcing method for hyperspectral remote sensing photos, which enables resource-constrained devices to execute object reputation in a safe and effective manner. Specifically, by shifting the workload to a cloud server, picture recognition speed is improved while maintaining input and output privacy guarantee. In order to ensure the confidentiality of input and output, we here provide a single, fundamental, transformation-based approach. Assemble the verification procedure as well, so that the customer can find any instances of the cloud server misbehaving. Furthermore, the verification method won't increase the customer's computing load. Lastly, compare the suggested strategy using extensive theoretical research and experimental data. Analyse the suggested scheme's performance, safety, and accuracy theoretically. The suggested method protects the input and output of the computation's privacy by using simple rotation matrices. The customer in the suggested plan can use the cloud server to confirm that the lower back implications are accurate.

Shen, et.al,…[2] presented a privacy protection Multiple Image owners are assisted with privacy protection under the CBIR scheme (MIPP). Here, encrypt image capabilities using a simple multi-party computing method that lets picture owners encrypt their own keys for the photograph's features. This ensures that an individual image owner's privacy is protected from being disclosed to other image owners and enables effective photo retrieval over features collected from various sources. Additionally, provide a novel method for the picture similarity dimension that can prevent the cloud from learning the picture similarity statistics. MIPP functions in the same manner as current first-class schemes, which outsource encrypted images together with their encrypted picture functionalities to the cloud. To handle the challenging circumstances of assisting a few photo owners, this method encrypts images using a key rotation, encrypts the associated photo functions using the comfortable multi-birthday celebration computation technique, and then suggests a special method to assess the degree of picture similarity; this will help to prevent disclosing the image similarity records in cloud to a significant degree. Multiple picture owners are permitted to encrypt images and picture features in the proposed MIPP by using their own secret image encryption keys. This makes it possible to retrieve pictures from many sources quickly and efficiently, all the while providing assurances that the privacy of a character photo owner won't be revealed to other owners. As a result, the suggested MIPP can satisfy the requirements of real worldwide packages.

Wu, Tong, et.al,…[3] implement an RDIC scheme to allow the third party auditor (TPA) to concurrently validate the submitted data content and the length of data storage as indicated by an updateable timestamp. Additionally, the suggested plan

ensures indistinguishable privacy (IND-privacy) for each fact's content and timestamp towards TPA. Here, the authenticator is assembled using a randomizable shape-maintaining signature (SPS) in order to tie the data content and timestamp inside the authenticator and guide efficient timestamp replace. In addition, this method offers the IND-privacy and ensures the timestamp validity in the auditing part by utilising the Groth-Sahai evidence and variety evidence. A fully developed RDIC protocol aims to provide timestamp validation and record integrity at the same time in order to direct the aforementioned PAYG price version. Additionally, by updating the timestamp, it must facilitate the garage issuer's renewal in an efficient manner. Putting together an RDIC scheme that supports timestamp validation and updates while also improving the current RDIC systems is not simple. The key workaround is for the CSP to send the timestamp to a third-party verifier for verification. However, this solution has drawbacks in that the timestamp needs to be discovered by the verifier and isn't appropriate in the third-party auditing setting, where the TPA needs to stop looking at any data storage information along with the timestamp in order to prevent users from being subjected to inference attacks that can be carried out using the TPA's resource to infer the information content cloth. Furthermore, it is a challenging hassle to find a technique for the timestamp to be updated effectively in the event that the user wants to permit clients to continue using the garage. Computing new authenticators using the updated timestamp is a simple solution. It is not realistic for the client to download all the data in order to update the authenticators. It is also appropriate to permit the CSP to swap out the authenticators for the new timestamp in order to reduce the computational load on the part of the customer.

Fu, Anmin, et.al,…[4] present the NPP, a new privacy-conscious public auditing tool, for the shared cloud records with management of many organisations. The four entities in the proposed version are the institution clients, PKG, TPA, and cloud. The cloud offers services (such data storage, record sharing, and other things) to institution clients and boasts substantial computer and storage capacity. For the benefit of the organization's clients, the TPA is able to confirm the accuracy of the shared records. For institution customers, the PKG creates the group key pair and public parameters. GMs (Group Managers) and regular users are included in the group users. In contrast to existing practises, the GMs involve a number of participants who work together to develop common knowledge and share it with regular members via the cloud. As a result, the GMs take action since they are the equally equal and common owners of the unique facts. Any of the GMs has the authority to remove contributors from the group or add new ones in the interim. Furthermore, the shared documents in the cloud can be accessed, downloaded, and altered by a general manager (GM) or a regular member. Keep in mind that in reality, having a few managers in a collection may be rather typical. For example, multiple managers work together to build the common data of an assignment crew. Later on, each GM will have the authority to manage the institution's users and preserve the shared data. A certain number of managers can work together to trace the signer's true identity while tracing them, guaranteeing the process's equality. A collection consumer must first send an auditing request message to the TPA in order to verify the accuracy of the shared records. The TPA sends a request for auditing evidence to the cloud after receiving it. The cloud first authenticates the TPA after receiving the auditing mission. The auditing proof will be returned to the TPA by the cloud if it is authentic. If not, the request will be rejected by the cloud. Lastly, the TPA provides an auditing answer to the institution consumer after confirming the accuracy of the evidence.

Song, et.al,…[5] provide a novel deep hashing convolutional neural network (DHCNN) that can simultaneously retrieve the same images and categorise their semantic labels within a single application. Convolutional neural networks (CNNs) are employed in larger elements to extract high dimensional deep capabilities. The deep features are then converted into compact hash codes by precisely inserting a hash layer into the community. To create the class distribution, a fully linked layer with a softmax characteristic is applied to the hash layer as well. Lastly, a loss characteristic is carefully crafted to simultaneously recall each picture's label loss and the lack of similarity between feature pairs. In addition, in order to extract high-dimensional deep functions from unprocessed remote sensing images, here we first use a CNN. Subsequently, the high-dimensional deep functions are seamlessly encoded to low-dimensional hash codes by inserting a hash layer into the CNN. To construct the class distribution, a completely linked layer using a softmax function is applied to the hash layer as well. In order to enhance the function representation capability, a detailed layout of a loss characteristic is presented here, wherein the label data of each photo and the similarity facts of pairs of snap shots are taken into consideration at the same time. When DHCNN is sufficiently trained, it can produce a hash code for a given image by binarizing the hash layer's output. At that point, retrieval may be accomplished with ease using Hamming distance ranking. Furthermore, by putting the semantic properties of the snapshots—including the query image—into the softmax classifier, the semantic labels of the pictures may be determined.

III. BACKGROUND OF THE WORK

Images from huge databases can be retrieved using a well-known technique called content-based image retrieval. For many years, study on this difficult subject of image retrieval has been the main emphasis. Applications such as face recognition, fingerprint recognition, pattern matching, picture validation, and verification have shown how crucial this is. In large database systems, picture categorization is another name for image retrieval. The ability to store and retrieve a vast amount of photos has been made possible by the rapid advancement of database technology in recent years. The need for software systems that enable efficient and quick image retrieval from massive database systems is brought about by this requirement. Content-based image search and retrieval is necessary in the modern world due to the increasing demand and use of multimedia applications. Kato coined the term "content based image retrieval" (CBIR) in reference to his work retrieving photos from databases using criteria such as colour and shape. From that point on, the method of looking for and obtaining a desired image from a database collection using artificially generated attributes such as colour, texture, and shape is referred to as CBIR. A crucial piece of software in scientific fields is content-based whole picture retrieval, which enables radiologists to obtain images with similar functionalities for input photos that yield similar analyses. There must be a feature extraction module in every CBIR system. This module is used with both image queries and image databases. This module turns a photo into a binary form and displays its properties, such as shape, colour, and texture. It also includes another module called similarity matching, which compares the functions of the input photo with database pixel functions. The image is transformed into a binary matrix wavelet histogram in order to extract the characteristics. Because of this, there is a method known as the Haar Wavelet.

IV. BLOCKCHAIN ASSISTED SIMILARITY SEARCH ON CLOUD IMAGES

Sensitive data, including emails, personal health records, official papers, and more, is being consolidated into the cloud as cloud computing gains popularity. Data owners can benefit from high-quality, on-demand data storage without having to worry about

maintaining or keeping their data by putting it on the cloud. In cloud computing, data owners can share their outsourced data with a huge user base. Each user may select to retrieve only the specific data files that they are interested in during a given session. One of the most widely used methods is using image-based search to selectively recover files rather than trying to obtain every aspect of the data owner, which is utterly unfeasible in cloud computing environments. This type of image-based search method has been extensively used in plaintext search contexts and enables users to obtain files of interest selectively. The SIFT algorithm plays a crucial role in this process by detecting and describing invariant key points in images. These key points capture the unique characteristics of image regions, regardless of changes in scale, rotation, or illumination. Extracting SIFT features allows for robust matching and retrieval of similar images, even in the presence of transformations and variations. Then check the duplication of images using chunk similarity algorithm. The Manhattan distance, also known as the L1 distance, is utilized to measure the similarity between SIFT descriptors. It computes the absolute differences between corresponding feature vector elements, providing a reliable metric for image similarity assessment. And also implement deduplication concept into verify the duplicate images in data storage. By comparing the Manhattan distances between query image descriptors and those in the image database, the retrieval system ranks and retrieves images with the most similar visual content. It offers robustness to transformations and provides efficient retrieval capabilities.

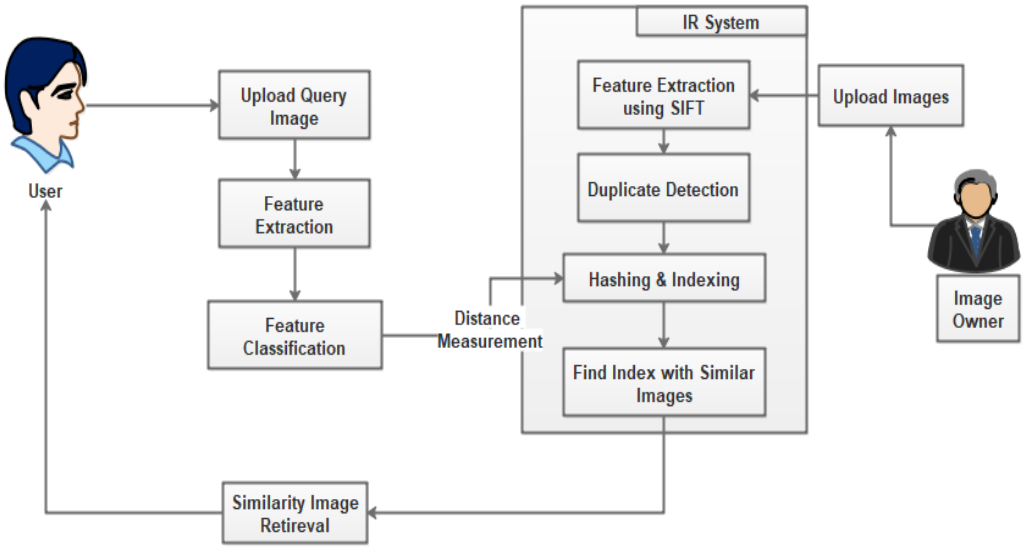

Fig.1 proposed system architecture

4.1 Framework Construction

Cloud computing is the on-demand provision of computer system resources, namely processing power and data storage (cloud storage), without the need for direct user management. In large clouds, functions are often distributed across multiple sites, each of which is a data centre. Resource sharing is necessary for coherence in the "pay as you go" model utilised by cloud computing, which can lower capital costs but potentially result in unforeseen operational costs for clients. Design the project's users', server's, and image owner's framework. The owner of the photograph owns a database with n images in it. After selecting an interesting image, an authorised photo user uploads the image, builds the corresponding trapdoor locally, and transmits it to the cloud server. The top k relevant photos are returned by the cloud server once it retrieves photos. Its processing and storage capacity are limitless.

4.2 Duplicate Detection

Data compression is a specific data compression method used in computing to get rid of duplicate copies of material that repeats. Single-instance (data) storage and intelligent (data) compression are words that are related and somewhat synonymous. This method can be used to decrease the amount of bytes that need to be delivered during network data transfers as well as to increase storage utilisation. Analysed during the compression process, distinct data segments, or byte patterns, are found and saved. As the analysis goes on, more chunks are compared to the stored copy. If a match is discovered, the unnecessary chunk is replaced with a brief reference pointing to the saved chunk. With the help of this module, we may validate photo files using their contents and file name. The Chunk Based Approach helps with image collection and indexing. First, preprocessing and feature extraction techniques are used to the photos. Following that, features are compared to previously recorded photos. The image won't be saved if its features are identical to those of an already-presented image.

4.3 Query Image Processing

Image processing is a technique wherein photographs are analysed and modified to improve their visual quality or extract useful information. Image processing is essential for comparing and matching photos based on their visual properties when getting similarity-based images from a cloud module. The image processing pipeline in a cloud module intended for similarity-based picture retrieval usually consists of multiple steps. Pre-processing is done on the input photographs to eliminate noise, adjust for lighting, and standardise their size and orientation. This stage guarantees that the photos are in a format that is consistent for additional examination.

4.4 Feature Extraction

The process of turning raw data into numerical features that may be handled while preserving the information in the original data set is known as feature extraction. The process of extracting features can be done manually or mechanically. The former entails

identifying and characterising the features relevant to a specific issue and implementing an extraction technique for those aspects. Making decisions can frequently benefit from having a thorough understanding of the field or background. Scientists and engineers have developed feature extraction techniques for text, photos, and signals during decades of research. One example of a basic feature of a signal is the mean of a window. By employing deep networks or specialised algorithms to automatically extract features from signals or images, automated feature extraction reduces the requirement for human engagement. When a user wants to quickly go from raw data to constructing SIFT algorithms, this technique can be quite helpful.

Step 1: Preparation: The filter method is used for image inversion, smoothing, and grayscale conversion during pre-processing.
Step 2: Shape Extraction: The SIFTS technique is used to extract shape characteristics based on the image's x and y coordinate representation.
Step 3: Colour Extraction: The R, G, and B Colour Coherence Vectors are examined using a histogram.

4.5 Index Detection

The Manhattan distance computation is an essential step in the similarity image retrieval process' index finding stage when comparing the feature vectors of query photos with the feature vectors that are stored in the index. Following the feature extraction process, a feature vector that captures the pertinent visual attributes of each image in the database is used to represent it. The feature vectors may contain elements pertaining to texture descriptors, colour histograms, or other relevant image attributes. To find photographs that are comparable to the query image, one calculates the Manhattan distance between the feature vectors of the stored photos and the query image. The Manhattan distance determines the total "distance" between two vectors by summing the absolute differences between each vector's matching elements. This distance metric is suitable for similarity comparisons because it considers both positive and negative differences between elements.

4.6 Similarity Image Retrieval

By calculating the Manhattan distance for each feature vector in the index, the system is able to rank the stored photos according to how similar they are to the query image. Pictures with closer Manhattan distances to the query image are regarded as more comparable, while pictures with farther distances are regarded as less similar. The Manhattan distance computation helps the retrieval system locate photos that are visually comparable to the query image quickly and effectively. It does this by providing a quantitative estimate of the dissimilarity of images. The system can efficiently identify and show the user the most relevant photos by integrating the Manhattan distance computation into the index finding stage, hence improving the user's overall image retrieval experience.

I. RESEARCH METHODOLOGY

Duplicate Checking
The Chunk Based Approach is used to assist gather and index images. First, pre-processing and feature extraction techniques are used to the images. Following that, features are compared to previously recorded images. Should an image's features match those of an already-presented image, it won't be saved.

The following are the steps of the algorithm:

- BlockTag(FileBlock): File block hash computation is done via BlockTag.
- Duplicate CheckReq(Token): which asks the storage server to check the file block twice.
- FileUploadReq(FileBlockID, FileBlock, Token): If the file block is unique, it uploads the file data to the storage server and modifies the stored file block token.
- FileBlock Encrypt (Fileblock) - This method uses convergent encryption to encrypt the file block, with the convergent key derived from the file block's blowfish.
- TokenGen(File Block, UserID): The process loads the user's associated privilege keys and generates a token
- FileBlockStore(FileBlockID, FileBlock, Token): This method updates the Mapping and saves the FileBlock on disc.

SIFT Feature Extraction

Processing Steps:

Step 1: Building a scale space: This is the first stage of preparation. To guarantee scale invariance, construct the original image's internal structure here.

Step 2: Estimating LoG: To locate important or interesting points in an image, utilise the Gaussian Laplacian.

Step 3: Locating the key points: Now try to identify the important points using the ultra-fast approximation. These are the maximum and minimum values found in step 2's computation of the Gaussian image difference.

Step 4: Eliminate problematic main points: Bad keypoints are regions with low contrast and edges. The method becomes reliable and efficient when these are removed.

Step 5: Giving the main points an orientation: Every important point has an orientation that is computed.

Step 6: Create SIFT functionalities: Lastly, a larger illustration is produced after ensuring rotation and scale invariance. This makes it possible to interpret things differently. That represented the algorithm's overall top level picture.

Distance Measurement

The technique of calculating the difference in features between a requested image from the server and a query image is known as distance measurement. After entering the query image, the user uploads an image and extracts its features. The recognizer improves the performance of server spot recognition. This strategy ought to offer a transformation technique that prevents the server from determining whether user-sent visual characteristics are the original or modified versions [3]. Image features are compared with dataset to get relevant information. Based on these details, system automatically extracts similar image owner detail. The distance measurement algorithm can be explained below,

The similarity measure is calculated as follows if I is the database image and I is the query image:

- Determine the database image's histogram vector (vI = [vI1, vI2, ….vIn]) and ccv vector (cI = [cI1, cI2, ….cIn]).
- Additionally, compute the vectors vI and cI for the query image.
- The similarity metric can then be determined by calculating the Manhattan distance between two feature vectors:
- The images match if d is less than the threshold, τ.
- Show the top 24 images as a result of all the matching images.

V. CONCLUSION

By integrating advanced computer vision techniques, this project has successfully created a system that empowers users to efficiently search and manage extensive image databases while ensuring optimal resource utilization. Similarity-based image retrieval in the cloud using query image processing, SIFT feature extraction, and Manhattan distance calculation provides an effective way to search and retrieve visually similar images. The combination of these techniques allows for efficient indexing and retrieval, making it possible to handle large-scale image databases. The incorporation of duplicate image detection not only ensures efficient resource management but also minimizes the risk of redundant data storage. This feature is especially valuable in scenarios where large image databases are maintained, reducing the storage footprint while preserving data integrity. As image collections continue to expand, similarity-based image retrieval in the cloud becomes an invaluable tool for various applications, including image search engines, content-based image retrieval systems, and visual recommendation systems.

.

REFERENCES

[1] Gao, Peng, Hanlin Zhang, Jia Yu, Jie Lin, Xiaopeng Wang, Ming Yang, and Fanyu Kong. "Secure cloud-aided object recognition on hyperspectral remote sensing images." IEEE Internet of Things Journal 8, no. 5 (2020): 3287-3299.

[2] Shen, Meng, Guohua Cheng, Liehuang Zhu, Xiaojiang Du, and Jiankun Hu. "Content-based multi-source encrypted image retrieval in clouds with privacy preservation." Future Generation Computer Systems 109 (2020): 621-632.

[3] Wu, Tong, Guomin Yang, Yi Mu, Rongmao Chen, and Shengmin Xu. "Privacy-enhanced remote data integrity checking with updatable timestamp." Information Sciences 527 (2020): 210-226.

[4] Fu, Anmin, Shui Yu, Yuqing Zhang, Huaqun Wang, and Chanying Huang. "NPP: A new privacy-aware public auditing scheme for cloud data sharing with group users." IEEE Transactions on Big Data 8, no. 1 (2017): 14-24.

[5] Song, Weiwei, Shutao Li, and Jón Atli Benediktsson. "Deep hashing learning for visual and semantic retrieval of remote sensing images." IEEE Transactions on Geoscience and Remote Sensing 59, no. 11 (2020): 9661-9672.

[6] Ravishankar, B., Prateek Kulkarni, and M. V. Vishnudas. "Blockchain-based database to ensure data integrity in cloud computing environments." In 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI), pp. 1-4. IEEE, 2020.

[7] Liu, Yishu, Conghui Chen, Zhengzhuo Han, Liwang Ding, and Yingbin Liu. "High-resolution remote sensing image retrieval based on classification-similarity networks and double fusion." IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing 13 (2020): 1119-1133.

[8] Shao, Zhenfeng, Weixun Zhou, Xueqing Deng, Maoding Zhang, and Qimin Cheng. "Multilabel remote sensing image retrieval based on fully convolutional network." IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing 13 (2020): 318-328.

[9] Li, Jiaxing, Jigang Wu, Guiyuan Jiang, and Thambipillai Srikanthan. "Blockchain-based public auditing for big data in cloud storage." Information Processing & Management 57, no. 6 (2020): 102382.

[10] Tong, Qiuyun, Yinbin Miao, Lei Chen, Jian Weng, Ximeng Liu, Kim-Kwang Raymond Choo, and Robert H. Deng. "Vfirm: Verifiable fine-grained encrypted image retrieval in multi-owner multi-user settings." IEEE Transactions on Services Computing 15, no. 6 (2021): 3606-3619.