International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Novel Security Aware Approach in Content Based Image Retrieval System using Trapdoor Verification for Cloud Environment

Pushpanjali M. Chouragade[1], Premchand Bhagwan Ambhore[2]

Submitted: 22/05/2023 **Revised**: 08/07/2023 **Accepted**: 27/07/2023

Abstract- Despite the fact that internet technology has accelerated the revolution in how images are distributed, it has also greatly increased the prevalence of illegally copying and using images. Numerous issues exist, including a protracted audit cycle, a lack of in-depth examination, a difficulty with the evidence, excessive costs, centralized storage, and more. It also raises privacy concerns since images often include sensitive personal information that may be immediately outsourced to the cloud utilizing image datasets. Encrypting the sensitive data before transferring or uploading it to the cloud is one approach to sort these things out. Once the data has been uploaded, the use will request particular target image data from the cloud server. At this time, content-based image retrieval (CBIR) is the method utilized to search for the target data. However, this approach lacks the capacity to search encrypted image data, hence this system attempts to address the issue of searching encrypted image.

Keywords*: Content Based Image Retrieval, Information Sharing, Privacy Preservation, Cloud Environment.*

1. Introduction

Nowadays, images-based data are very important in various means. Previously the text-based data were having the highest priority because it was used for identification, for recognition of the person's identity, but as we are moving towards the digital applications, the image based data is going ahead with highest priorityas we are using it for own identification such as while unlocking our mobile, we are using face recognition, again for disease detection and for object detection or recognition, the image based data is used mostly. But however, the image-based data requires more space for storage as compared to text-based data. That's why there is the urgent need of storage space for image-based data to get stored. Currently, the primary problem is that we utilize cloud storage services for the protection of our personal data due to the quick, widespread growth of cloud services. Furthermore, searching over encrypted datasets and cloud storage has emerged as crucial issues. When it comes to privacy leaks, image-based data like identity cards and driver's licenses are being utilized to leak data.

As a result of the fact that the picture often includes sensitive personal information and that this information may be directly outsourced by uploading the image dataset to the cloud, privacy concerns are raised. Encrypting the sensitive data before transferring or uploading it to the cloud is one approach to sort these things out. Once the data has been uploaded, the user will request particular target picture data from the cloud server. At this time, CBIR is the method utilized to search for the target data. However, this method is unable to search the encrypted picture data; as a result, this research aims to address the issue of searching encrypted images.

To accomplish this, the ASPE (asymmetric scalar-product-preserving encryption) and HE (homomorphic encryption) combination of two encryption techniques will be employed. Although ASPE has the ability to encrypt data and determine how similar ciphertexts are, it isn't a realistic method since it relies on the idea that users are totally reliant on the outside world and may also have key leakage issues. HE, in contrast to ASPE, has the ability to perform addition and multiplication inside of an encrypted region while also resolving the key leaking issue.

The other entities in this system are regarded as semi-trusted entities engaged in picture retrieval, therefore the data owner is not required to provide a secret key to the authorized users. The user must request permission and create a trapdoor for every search since only the data owner has the secret key to perform the searching procedure. Data leaking might result from the user's habit of searching. The key leakage issue will be resolved in this work, and the data owner will be forbidden from collecting user search data when the user is submitting a search request. Without knowing anything about the query picture, the trapdoor may be safely generated by the data owner. To prevent the attacker from posing as the search trapdoor and to get rid of the unauthorized

[1]*PhD Research Scholar and Assistant Professor in Computer Science and Engineering Department, Government College of Engineering, Amravati, Maharashtra, India.*
[2]*Assistant Professor in Information Technology Department, Government College of Engineering, Amravati, Maharashtra, India.*
pushpanjalic3@gmail.com, pbambhore@gmail.com

trapdoor when the cloud server acquires it, we also recommended straightforward trapdoor verification.

Summary of the work:

i. Since encrypted images prevent others from accessing the content, the data owner may safely outsource the images to the cloud server.
ii. Our solution makes sure that the trapdoor and the secure index are worthless for the cloud server, despite the fact that it attempts to get knowledge about the search index by examining the data gathered during the picture retrieval phase.
iii. Additionally, we take into account the cloud server's cooperation with harmful users. Because the data owner maintains the secret key's confidentiality in our system, it is still difficult to break our system.
iv. By integrating the ASPE and HE methods, our method may offer more secure encryption while looking for the picture data.

2. Literature Review

A client and a server may share information without revealing more information than is necessary thanks to a safe and effective approach Emillano et al. [1] developed for the exchange of highly classified data while protecting privacy. Guarantees of privacy are explicitly stated and achieved with verifiable security. They initiated two Privacy-Preserving Sharing of Sensitive Information (PPSSI) different forms: one is intended for small to medium-sized data collections, while the other lowers transmission costs and liability worries for datasets with large sizes. In the latter, a non-colluding, untrusted party called the Isolated Box is shown that may be employed as robust device hardware. They have proven that their PPSSI procedures are effective enough to be applied in practical applications in the final experimental results.

Markov chain extraction of encoded JPEG pictures was suggested by Cheng, et al. [2]. This method encrypts the picture data, allowing the Markov properties to be directly retrieved from the ciphertexts. We develop a retrieval method for encrypted JPEG pictures using a Markov process. This technique, which protects the content secrecy of JPEG pictures using a combination of the stream cypher and permutation encryption, encrypts discrete cosine transform (DCT) coefficients. The JPEG pictures that were encrypted and transferred to a database server are finally made available to the content owner. The effectiveness of the search is still the main issue. Since the strategy relies on hiding the DCT coefficients' true values, it may be difficult to spot small differences among close DCT coefficients in this region. This indicates that things could turn out poorly. Additional examination is required on the image retrieval approaches for more highly precise efficiency with authenticated securely systems.

A safe and effective access-controlled image search technique, called SEISA, was introduced by Yuan et al. [3]. In terms of performance and precision, it is comparable to normal text image ways of searching without protecting privacy. Additionally, they developed a secure k-means deploying approach that enables data holders to handle enormous datasets by safely delegating the bulk of computing tasks during the system setup process to public clouds. This decreased the expense for data owners under SEISA. A compact polynomial-based search authorization method was also developed, allowing data owners to demonstrate flexible search access rules for each image without impairing SEISA's index formulating and search capabilities. Additionally, their safe k-means deploying algorithm and search access control method may be applied independently in other relevant disciplines including secure keyword search and privacy-preserving data mining. To demonstrate the security and effectiveness of SEISA, they offered a comprehensive study. In comparison to other image search approaches for plaintexts, they demonstrate SEISA's concept fulfilment on a large image data set, demonstrating that it maintains accuracy while achieving the same an instant image search complexity.

A Private Relevance Feedback - Content Based Image Retrieval (PRF-CBIR) approach was put out by Huang et al. [4] to protect the user's search intent while maximizing the benefits of input on importance. unique inquiry, unique reaction, and differentiated recovery are the three core components of this method. The search term, outcome, and observation attacks that occur in RF-CBIR may be defended against using PRF-CBIR. The privacy protection of the new system is presented a theoretical analysis. It was shown that the suggested method effectively reduces privacy leaks while also significantly reducing the chance of an attack succeeding. A contemporary image resource was also the subject of several investigations. The findings demonstrate that the PRF confidentially CBIR outperforms the RFCBIR while maintaining a reasonable retrieval latency tradeoff. While processing the data, one might make advantage of the image's colour and texture.

A reliable encryption retrieval device was created by K. Hazra et al. [5]. The HSV histogram utilized by the computer as an image aspect, and it compared images using KNN and SVM sets of instructions, which may lead to extremely accurate retrieval. In addition to ensuring the reliability of the image, the aforementioned many encrypted image retrieval systems may now also retrieve the identical images. The efficacy of the hunt was, however, diminished since these methods were unable to provide navigable indexes for images. In order

to improve retrieval speed, it is crucial to choose a cheap set of index building rules.

Using anonymity substance image retrieval technique created by Xia Z et al. [6], a database owner can deliver an image dataset and the CBIR service to the cloud without disclosing the relevant database information. The Earth Mover's Distance (EMD) is utilized to assess image likeness once input characteristics are gathered to examine the images. The EMD issue may be resolved using linear programming (LP). The EMD issue has generated to the point where a web server can fix it despite having access to classified data. To boost retrieval how they perform, a two-stage structure built on LSH is created. To reduce the scope of the search, dissimilar images are filtered away using preload clean sets in the first step. The rest of the images are compared one at a time in the subsequent phase to provide more accurate outcomes of searches using the EMD scale. Security analysis and testing were used to show the recommended scheme's effectiveness and security. Although it is not mentioned that the research's settings are the ideal ones, they may typically improve detection performance even if search reliability cannot be guaranteed. The EMD assessment and regional variables cannot always convey the highest retrieval accuracy. The local delicate hash aids in removing certain distinct. images in which the EMD metric incorrectly believes to be the identical as the query image. In this method, the request's user spends the most of their time retrieving specific elements.

A privacy-more appealing method for picture similarity search in cloud image databases was put out by Liu et al. [7]. It provides a method for picture similarity searches in cloud image databases that is more private. Although the security of encrypted picture retrieval improved under this technique, the performance of the search degraded. The system's security should be increased while the time complexity might be decreased. It should be experimental in performance.

The constraints of current privacy-aware large scale picture retrieval techniques are addressed by Li et al.'s [8] proposal for CASHEIRS, an effective and secure image retrieval system. The CASHEIRS has four main characteristics, including (i) The adaptability allows for efficient query processing by allowing searches to be conducted over subsets of sets rather than the whole collection. A distinct cluster is formed by connecting related clusters together using a hierarchical index tree that is created by our CASHEIRS. (ii) High accuracy: To increase the accuracy of picture retrieval, Convolutional Neural Network (CNN) features are applied. (iii) The proper storage and communication costs: High broad CNN image elements are translated into condensed digital codes to reduce storage and communication expenses. (iv) Privacy-conscious: An efficient encryption technique is advised to protect the private information of the search terms and the classified information of saved photographs. The Caltech256 and INRIA Holiday datasets have undergone extensive reviews. According to experimental findings, CASHEIRS outperforms other current systems in terms of matching picture accuracy while using less storage and transmission resources.

In a cloud computing environment, Xia et al. [9] suggestion for a content-driven image retrieval method that protects confidentiality was provided. The secure KNN technique was employed by the authors to encrypt the visual features once they had extracted characteristics to represent the related pictures. The cloud server can rank the obtained results without the need for extra connection by immediately calculating the similarity scores and using encrypted characteristics. To prevent the distribution of illegal images, they developed an encryption-domain watermarking strategy, and to improve the efficiency of extraction, they used a locality-sensitive hash technique. Overall, the picture characteristics are resistant against attacks using solely ciphertext. In addition, it should be noted that feature extraction techniques and the security lever of image features have improved to ensure CBIR outsourcing.

An encrypted picture retrieval system based entirely on neighborhood functions in a cloud setting was suggested by Xia et al. [10]. Through the use of a set of SIFT rules, this technique derived picture functionalities. EMD method was used to determine how similar two images were, and neighborhood touchy hashing rules were used to create a hash table. The SIFT set of rules improved the hunt performance at the cost of more time spent extracting picture functions.

Gong et al. [11] proposed an improved Bag of Visual Words (BoVW) model-based method for cloud computing image retrieval. to offer cloud-based image retrieval while protecting privacy. An upgraded BOVW technique based on Hamming integration and orthogonal transformation are coupled to provide binary signatures for improving visual terms. When performing an identical transformation, the image's features are separated into a few distinct regions using identical decomposition, for which distance comparison and encoding are applied separately, and what results from these various kinds of operations merge in the outcome vector using orthogonal composition. As a result, without jeopardising the user's privacy, the cloud server quickly acquired components from protected functionality and compared their distance to those of the query image.

A similar new edge-assisted with a confidentiality figuring technique was published by Xuan Li et al. [12]. Both the minor shield and high-level protective

components of the data shield work. Lightweight permutation-substitution authentication is used in low-level mitigation, whereas homomorphic encryption is used in high-level security. These two privacy-related tasks are assigned to the edge node and the terminal device, respectively. By shifting challenging cryptographic computations to the edge node, the suggested architecture lightens the strain on the terminal device. Under the edge-assisted framework, an image retrieval strategy that protects privacy is suggested. The method addresses the issue of retrieving images while protecting privacy via a similarity analysis of the encrypted form. For privacy-preserving searches, the terminal device just has to conduct effective low-level security on the images.

A innovative content-based retrieval method that protects privacy was also put out by Ferreira et al. [13]. Additionally, under their plan, deterministic encryption methods are used to encode colour information. This may allow for picture retrieval while protecting privacy. Additionally, they make it possible for texture data to be protected using probabilistic encryption techniques for increased security. Therefore, it is evident from the preceding scheme that a more secure, privacy-preserving content-based retrieval strategy may be created to strengthen the existing deficiency.

To guarantee that the original picture creators are duly acknowledged and given credit for their contributions, Mehta et al. [14] set out to address the important problem of precise image identification for images shared on interpersonal image sharing networks and generic image portals. In the suggested design, images and hashes are stored using IPFS, a decentralized collaborative interactive network for distribution. In order to reduce network redundancy and provide blocks inside files a unique fingerprint, IPFS utilizes cryptographic hashes. It is content addressable and leverages these distinctive hashes for information retrieval. The IPFS system is used to store pictures and perceptual hashes, greatly reducing the size of the Ethereum test chain. Any accepted encryption method, including MD5, SHA, and perceptual hashing, may be used to encrypt data saved on IPFS. For retrieval, the dissimilarity is determined by calculating the hamming distance between the hashes that are so acquired, which is referred to as normalizing this hamming distance. Only the right buyer will get the encryption keys through a smart contract. This strategy is used in implementation and is scaleable. Berkeley Segmentation Data Set, a dataset of 500 real images, is used for testing.

Meng Shen et al. [15] propose a blockchain technology method for reliably accessing imaging data. They launched by describing typical professional image retrieval scenarios and summing the pertinent system layout constraints. Future blockchain systems are used to define the layered structure and vulnerability scenario for the proposed system. Physical level, Transaction level, Service level, and Application level are the four tiers of the architecture. Five categories are present in the physical layer, such as Hospital, Third, Regulatory Authority, Miner, and Rehabilitation Service. The structure of the transaction layer has been modified to meet the requirements of the medical image. Image matching is computed at the service layer. Smart contracts help to facilitate the recovery process. Appropriate parameters may be extended into future data modelling at the application layer. Through the use of digital imaging or illness predicting software, this piece incorporates textual elements that will be used in future data modelling. As a way to accommodate large-size images with storage-constrained wipes and protect the privacy of medical images and their characteristics, a meticulously analyzed feature vector from each imaging specimen is obtained, and a special interaction form is devised.

H. A brand-new picture retrieval method that protects privacy was put out by Wang et al. [16]. Images are encrypted using block permutation and AES. AES-encrypted pictures' characteristics are retrieved using random mapping and bag-of-words techniques. The known-plaintext approach cannot break the encrypted pictures. The studies show that the suggested approach can retrieve somewhat comparable images. Some essential characteristics were taken from AES-encrypted images for similarity analysis. The trials did show, however, that the randomly generated attributes are helpful when looking for images that are comparable.

A content-based, multi-supplier, encrypted picture retrieval technique in clouds with privacy protection has been presented by Meng Shen et al. [17]. Using the reliable multi-party 820 computation, we were able to encrypt picture functionality while allowing image owners to do so using their own private keys. We also put out a fresh method for determining how similar two images are that, to a certain extent, may prevent disclosing picture similarity information to the cloud. Theoretical analysis and practical findings demonstrated 825 that our approach allowed for the accurate and environmentally friendly retrieval of images from a variety of sources while also providing privacy assurances. We will further improve the effectiveness of picture retrieval in future studies.

L. Jiang et al. [18] published a powerful and beneficial scale-invariant function transform (SIFT) method for protected images. It employs balanced homomorphic authentication, which is completely centered around new encoding methods, new homomorphic assessment, and division and consequence encrypted data. Their system

may identify increased processing efficiency, significantly reduce verbal exchange costs and interactive server-client interactions, and perform accurate function factor identification, accurate function factor description, and accurate picture matching.

The work offers a new privacy policy, according to Anyu Duet al. [19]. The system's effectiveness and dependability had to be increased. The following are the primary contributions of this paper: A safe retrieval mechanism for the novel was suggested in order to guarantee data control authority during data transmission. A 4-D hyperchaotic system was suggested for the proposed system to conduct picture encryption. It advises utilizing a sophisticated loss function to train the network architecture and provides an effective DPSH and kNN secure approach in order to protect the code.

Zhang Zongye et. al. [20],in this research, a content retrieval and content-based protection programme has been suggested and implemented. It may be utilised for helpful suggestions in social multimedia applications. They used the image's visual characteristics to assess how similar the two were. use of eLSH to condense the images and find visual feature similarities. To expedite the search, a cuckoo hashing index has been created. Based on private sharing, this method removed more key management and access control compared to previous methods by allowing the user to independently query and restore images.

SensIR is a novel privacy-sensitive image retrieval system that looks for similar images in an external image database, according to Hu, et al.'s [21] introduction. To prevent certain picture regions from being revealed, they used the confidential area recognition algorithm PRDet. They proposed the use of a partial CNN (PCNN) to decrease the impact of the encrypted pseudorandom pixels. They developed a means to speed up PCNN-based picture recognition in large anonymity sectors as well as consistent hash encapsulation. When a region's pixels have a grey level greater than the threshold, the region is said to have saliency zones, which are classified as private spaces. However, given the diversity of the visual content, disturbances in the foreground maps could have an impact. There are two smaller areas that are similarly thought of being private yet are not. Contradicting the results are the uneven shapes of the private zones created by the threshold.

C Zhang et al. [22] talked about a new deep hashing-based securely image acquisition tactics (TDHPPIR) based on triplet deep CNN hashing to improve the velocity of image retrieval in the cloud with respect to security. To boost hash code comprehension, a triplet deep CNN model is proposed for acquiring graphical illustrations and hash codes simultaneously. In addition, to speed up hashing-based image search, the authors established the H2S-Tree, a unique structured bit-scalable hash code-based S-Tree. Additionally, authors presented TDHPPIR's primary scheme and methods. The suggested technique clearly outperformed state-of-the-arts, which included deep, non-deep, and non-hashing approaches, in terms of both accuracy and efficiency.

A completely new stable, responsible privacy-maintaining system was put out by Youcef Imine et al. [23]. Their response enables anonymous and responsible public fact sharing in facts sharing architectures based on name-of-game sharing and randomization approaches. Their plan involves sharing anonymous token data together with the symptoms of each speaking entity. Then, without using the registration authority or any other 1/3 party, they could be able to proportion facts using the externalization servers. The token is used by externalization servers to authenticate the entity without violating its privacy. Despite the anonymity of the provided signature, anomaly detection grants authorization demonstrating any interacting with others object in the system's network. They want to deal with the issue of conditional revocation in the future by providing ways to partially or entirely stop dishonest users from disseminating public information. Additionally, they acknowledge that it will be fascinating to demonstrate that their system is stable under a more preferable version than the random oracle. Some problems that need to be handled include the annoyance of conditional revocation and the absence of security concerns with regard to sharing and externalization servers.

Iida et al. [24] established a technique that supports both direct image retrieval from intrinsically protected images and EtC format images that can be compressed using JPEG configuration. The suggested retrieval method makes applying the weighted searching on images involving specialized characterizations permitted by MPEG-7, such as scaled colour descriptors (SCD) or colour and edge directivity descriptors (CEDD). To remove the effects of picture encoding, CEDD has been modified and the weighted SIMPLE descriptors have been increased. The suggested strategy has been shown to have nearly no loss in recovery results when compared to existing material separation techniques that employ raw pictures. Furthermore, the new system outperforms conventional confidentiality CBIR approaches, including existing ones, based on mean average accuracy (mAP) ratings. Recycling characteristics obtained by the decoder in unauthorized picture retrieval is useless. EtC picture file sizes have been somewhat increased (recommended) and are up 7.91% from vulnerable JPEG images. The suggested system does not support an asymmetric encryption.

A ground-breaking content-based picture retrieval method was presented by Iida et al. [25] and enabled the simultaneous use of encrypted and plain images. The suggested method employs block-scrambling, a technique created for encryption-then-compression (EtC) systems, to encrypt images. JPEG may be used to compress both simple pictures and images that have been encoded. The recommended retrieval employs picture descriptors designed to get around image encryption. As a result, the recovery of both encoded and decoded pictures is made possible by the use of EtC images and descriptors. The proposed system is shown to work with plain images using conventional retrieval techniques, even when plain images and EtC images are mixed together. The accuracy of the retrieval may be increased by applying recovery strategies for mixed pictures.

A secrecy and spy detection material for picture retrieval technology in cloud computing was provided by Wang et al. [26]. In this method, statistical properties are reinforced using the DenseNet network. For the protection of copyright and the identity of users, however, just one hash method and the XOR operation are employed, and a reversible information concealing strategy are employed for traitor tracking. The method is used, among other things, to ciphertext picture retrieval, digital rights and confidentiality, and traitor surveillance. In comparison to earlier leak tracking systems, it promises to give improved retrieval accuracy, efficiency, and a more straightforward architecture. Changes to the watermark embedding technique are extremely straightforward. Picture attacks are not taken into consideration since the method may be swiftly updated in response to technological improvements and real-world applications.

Iida et al. [27] suggested a unique content-based image retrieval method for encryption-then-compression (EtC) images. The conventional extraction models for EtC images used the JPEG compression standard even though EtC images may be encoded using both JPEG and lossless compression methods like JPEG-LS. On the other hand, both lossless and lossy compression approaches are enabled to be applied with the suggested retrieval approach. The recommended method maintains a satisfactory retrieval performance even while employing both lossless and lossy-compressed EtC pictures. Web setups run the danger of security lapses and unauthorized usage since cloud servers are not always protected. In theory, CEDD cannot effectively obstruct both movement and abstraction.

Wang L. et al. [28] implied an adequate navigable image retrieval tactics with accurate retrieval authentication to address a challenge of data integrity. ECC (elliptic curve cryptography) was used to determine the substance. To increase retrieval speed, updated lists may be created using local sensitive hash algorithms. The findings suggested that entity IDs could be properly recognized in the system and statistical information from picture data could be correctly kept. Since the establishment of the updated list, image retrieval has shown to be more successful than traditional retrieval. A changed list may modify the retrieval reliability. However, compared to the RSA method, the ECC approach is more intricate and difficult to develop, which lowers the likelihood of execution faults.

An encoded feature vector is used in the indicated CBIR located in the cloud image retrieval method in a try to preserve simultaneously the spectrum of features and the real images over spreading, as described by Kumar et al. [29]. To protect the security of the image material, users often cypher pictures before transferring them to the cloud. It illustrates the difficulties of effectively determining images out of unethical cloud environment. With the intention to produce an image feature vector, images are defined in regard to their various properties. The feature vector is then secured using asymmetric scalar-product-preserving encryption (ASPE). Prior to transmission to a data center, images are encoded. On several Corel picture databases as well as a medical image database, the recommended method has been tested. The recommended technique exceeds the most effective CBIR methodologies in the industry, according to performance evaluation. On cloud systems, image transmission, storage, and retrieval present security vulnerabilities. Inaccurate pictures might be returned by the CSP CBIR if its service is subpar, leading to misleading diagnoses. Classification will just increase the complexity of the process with no apparent benefits.

In an encrypted layout, Janani T et al. [30] introduced Strong SEcure Similar Image Matching (SESIM). Comparing the proposed SESIM protocol to the current secure distance metrics, the computation cost of the described standard is higher. Image analysis and protected image asset derivation are accomplished via two useful detachment servers. The recommended method provides query protection by encoding request picture features prior to sending them to the cloud. Performance evaluations show that the method, when coupled with an encrypted cloud server, is efficient and secure. Additionally, there isn't an infrastructure in place for an effective search in a scattered context that integrates actual image retrieval. The suggested approach cannot provide protection from all threats.

Research Gap Analysis:

Following a thorough review of the literature on secure content-based image retrieval strategies, it is important to highlight that the study findings all depend on particular encryption techniques, which limits the research's

applicability. Different types of images are not employed, different image phases are not taken into account, the right characteristics needed to preserve image privacy are not used, and new approaches are not developed for safe and private cloud-based quick image retrieval. Due to their high absorbing and connectivity demands, some are inappropriate for large-scale systems and low-profile devices. For environments with extensive safety prerequisites, some are inappropriate. The retrieval accuracy is limited by the similarity measurement's high feature reliance.

In the proposed research endeavor, these shortcomings of current approaches will be addressed. Therefore, progress may be made on a universal encryption method. In addition, similarity measurement is used to decrease computational and time complexity while also increasing retrieval accuracy and efficiency. As a result, a more advanced, secure content-based image retrieval system may be used in a cloud context.

3. Problem Formulation

Statement of the research problem:

More storage capacity and safe exchange of highly confidential information in images are required because of the exponential expansion of digital image applications. Image usually contains both personal and confidential information, which can be directly outsourced to the cloud using the image dataset. This may provoke number of privacy issues. Therefore, before uploading images to the cloud, it is necessary to encrypt them to secure the important information contained in them. The user may ask the cloud server to look for specified target image data once the encrypted image data has been saved there. This method of finding specific information is known as content-based image retrieval. This approach, however, cannot be used to search encrypted image data.

The rapid expansion of cloud services with the need for individual confidentiality have boosted the relevance of secured cloud storage services and search through digitally encrypted data. In order to safeguard the privacy of information contained in images during image retrieval, it is necessary to find a solution to the issue of searching encrypted images.

Motivation:

The performance of the existing privacy preserving image retrieval schemes suffers from either higher computational complexity, low speed image searching or compromised accuracy of image retrieval, as well as they highly depend on specific encryption methods resulting to compromise between meeting higher security requirements and implementing on low profile devices. Only few efforts have been made to apply security awareness in cloud environment.

Proposed Flow:

The proposed model of our research work consists of 3 main modules i.e., image owner side, cloud server side and user side, as shown in below Fig.1.

- **Image owner side:** The owner of the image maintains an original image database. To encrypt the original image, the proprietor of the image must first provide the secret codes. The owner of the encrypted image then outsources it to a cloud environment.
- **Cloud server side:** After acquiring and decoding the classified images, the cloud server forms the index using the image properties it has discovered. The cloud server extracts a feature from the trapdoor upon getting a search request from the user and finds the most comparable features in the index. The user is shown with images that have the most comparable attributes.
- **User side:** In order to identify the required images, visitors encode the query image in interchangeable manner as the image owner. The encoded query image is published as a gateway to the cloud server. The user cracks corresponding images that the web-based source gave using secret access codes.

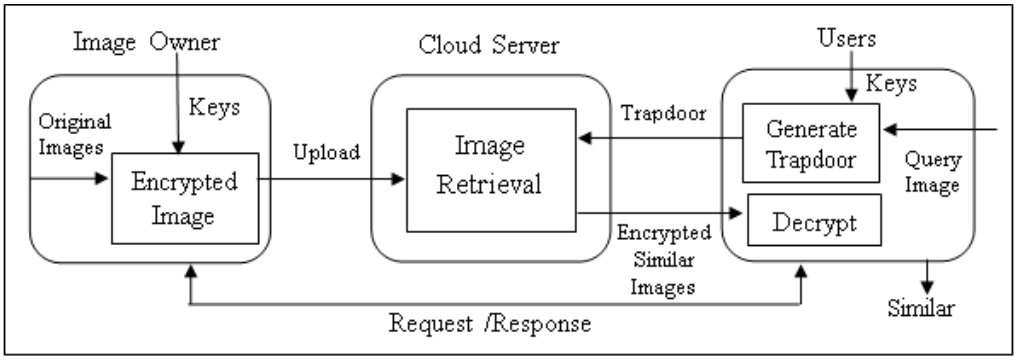

Fig. 1: Proposed model of our research work

Proposed Methodology

Development of imaging technology, resulted in gathering of huge amount of visual data. So, image privacy comes to a top concern, as images may contain all kinds of personal and private information of users. In view of this, information security brings a challenge for image retrieval as encrypted image may be unsuitable. To efficiently retrieve the required information Secure Content based Image Retrieval over encrypted domain can be used. These schemes are mainly divided into two categories:

- Feature Encryption Based which provides more security and accuracy
- Image Encryption Based which provides less computational time and storage space

Some shortcomings identified in the existing schemes of secure content-based image retrieval are image security, retrieval accuracy, computational time and storage space.

The goal of our study is to provide a secure environment. Without authorization, the unauthorized person

cannot access the information. Some regions need a more secure setting since today's photographs include both critical and personal information. For instance, a high degree of safety should be maintained in the banking industry, the health care sector, and so on. Millions of images in these industries need to be kept, yet they are often ignored as personal secrets. We do not want any personal information, user information, or search information to be made available to anybody except the authorized user. The image retrieval system typically consists of three main modules: users, cloud server, and picture data owner.

Further such system will be divided into four phases as given below:

1. Configuration and key creation
2. Secure index construction and encryption of picture data
3. a search query
4. Image Recovery

1) Configuration and key creation

Data points operator must specify the precautionary approach during the configuration stages in order to handle the information properly. And in Key generation phase, the randomly generated invertible matrix by the data owner will consider it as a secret key for ASPE.

2) Secure index construction and encryption of picture data

First initially obtain the metadata from the image repository before applying the VLAD set of rules to represent each image during the secure index generation phase. Throughout the image's information encoding equilibrium, the search query label will be transformed into amplified by a hidden code and interpreted using a confidential way to retrieve the encrypted image.

3) Search Query

Once data sets proprietor transmits the image over the preserve index to the cloud server, the infrastructure gets ready to deliver a content-oriented image lookup tool.

4) Image Recovery

Because the returned data are ciphertexts, in the ultimate phase of the platform, an individual needs to approach the information proprietor for the image key. Upon downloading those appropriate images, the cloud server will first decide if the entry point was created by the information proprietor or not. When a fake gateway is detected, the cloud server immediately shuts down the application.

4. Conclusion

According to the research analysis, particularly different types of photos are not employed, different image phases are not taken into account, the right characteristics needed to preserve image privacy are not used, and new approaches are not developed for safe and private cloud-based quick image retrieval. These limitations of existing methodologies would be addressed in further research work.

Distinguished cloud-based image acquisition strategies on a variety of images at different phases will be examined during the current endeavor, features required for privacy preservation of images will be identified, and methodology will be designed and developed for improving the performance of search time and to maintain the confidentiality by keeping the secret key. Image Processing based methodology will be designed and developed for security awareness and information sharing from extracted features (local and global features). As it turns out, enhanced confidentiality in cloud image retrieval is expected to be obtained with this pair of factors. The performance of proposed research system will be evaluated by utilizing various performance evaluation measures and metrics parameters. Hence, the expected result of this research would be a secure image retrieval scheme in cloud environment.

This proposed research work findings can be applied to image datasets from a variety of image processing-related applications, among them are those used for individual and professional images, money transfer, the

healthcare sector, the farming industry, authenticated safety equipment, the armed forces, legal forensic analysis cars, detached sensing imaging (satellite), commerce, among other uses.

References

[1] Emiliano De Cristofaro, Yanbin Lu, Gene Tsudik, "Efficient Techniques for Privacy Preserving Sharing of Sensitive Information", in Trust and Trustworthy Computing, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, Vol. 6740, pp.1-15, 2011, https://doi.org/10.1007/978-3-642-21599-5_18

[2] H. Cheng, X. Zhang, J. Yu, and F. Li, "Markov Process Based Retrieval for Encrypted JPEG Images", in Proceeding of IEEE 10th International Conference on Availability, Reliability and Security, 2015, pp. 417-421, doi: 10.1109/ARES.2015.18.

[3] J. Yuan, S. Yu, and L. Guo, "SEISA: Secure and efficient encrypted image search with access control", in Proceeding of IEEE Conference Computing Communication (INFOCOM), pp. 2083-2091, Apr. 2015, doi: 10.1109/INFOCOM.2015.7218593

[4] D. Huang, X. Geng, L. Wei, and C. Su, "A secure query scheme on encrypted remote sensing images based on Henon mapping", in Journal of Software, Research Gate, Vol. 27, no. 7, pp. 1729–1740, Jul. 2016, doi: 10.13328/j.cnki.jos.005039.

[5] T. K. Hazra, S. R. Chowdhury, and A. K. Chakraborty, "Encrypted Image Retrieval System: A machine learning approach", IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 1-6, Oct. 2016, doi: 10.1109/IEMCON.2016.7746351.

[6] Xia, Z., Wang, X., Zhang, L., Qin, Z., Sun, X. and Ren, K., "A Privacy-Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing", in IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2594-2608, Nov. 2016, doi: 10.1109/TIFS.2016.2590944.

[7] H. Liu and H. Go, "Privacy-Enhanced Similarity Search Scheme for Cloud ImageDatabases", IEICE Transaction on Information and System, Vol. E99-D, no. 12, pp. 188–3191, Dec. 2016, doi: 10.1587/transinf.2016EDL8141.

[8] X. Li, Q. Xue, and M. C. Chuah, "Casheirs: Cloud Assisted Scalable Hierarchical Encrypted Based Image Retrieval System", IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, pp. 1-9, 2017, doi: 10.1109/INFOCOM.2017.8056953. 8

[9] Z. Xia, N. N. Xiong, A. V. Vasilakos, and X. Sun, "EPCBIR: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing", InformationSciences, Vol. 387, pp. 195-204, Dec. 2017, https://doi.org/10.1016/j.ins.2016.12.030.

[10] Xia, Z., Zhu, Y., Sun, X., Qin, Z. and Ren, K., "Towards Privacy-Preserving Content-Based Image Retrieval in Cloud Computing", in IEEE Transactions on CloudComputing, vol. 6, no. 1, pp. 276-286, 1 Jan.- March 2018, doi:10.1109/TCC.2015.2491933

[11] J. Gong, Y. Xu, and X. Zhao, "A Privacy-preserving Image Retrieval Method Based onImproved BoVW Model in Cloud Environment", IETE Technical Review, Vol. 35, no.sup1, pp. 76-84, 2018, doi: 10.1080/02564602.2018.1526654

[12] Li, X., Li, J., Yiu, S. et al., "Privacy-preserving edge-assisted image retrieval andclassification in IoT", in Frontiers of Computer Science, Springer Nature, 13, pp.1136–1147, 2019, https://doi.org/10.1007/s11704-018-8067-z

[13] B. Ferreira, J. Rodrigues, J. Leitao, and H. Domingos, "Practical Privacy-PreservingContent-Based Retrieval in Cloud Image Repositories", in IEEE Transaction on CloudComputing, Vol. 7, no. 3, pp. 784-798, 1 July-Sept. 2019, doi: 10.1109/TCC.2017.2669999.

[14] R. Mehta, N. Kapoor, S. Sourav and R. Shorey, "Decentralised Image Sharing andCopyright Protection using Blockchain and Perceptual Hashes", 11th InternationalConference on Communication Systems & Networks (COMSNETS), Bengaluru, India,pp. 1-6, 2019, https://doi: 10.1109/COMSNETS.2019.8711440.

[15] Meng Shen, Yawen Deng, Liehuang Zhu, Xiaojiang Du, and Nadra Guizani, "Privacy-Preserving Image Retrieval for Medical IoT Systems: A Blockchain-Based Approach",in IEEE Network (Edge Intelligence for The Industrial Internet of Things), pp.27-33,Sept.-Oct. 2019, https://doi: 10.1109/MNET.001.180050

[16] H. Wang, Z. Xia, J. Fei and F. Xiao, "An AES-Based Secure Image Retrieval SchemeUsing Random Mapping and BOW in Cloud Computing", in IEEE Access, Vol. 8, pp.61138-61147, 2020, doi: 10.1109/ACCESS.2020.2983194.

[17] M. Shen, G. Cheng, L. Zhu, X. Du, J. Hu, "Content-based multi-source encrypted imageretrieval in clouds with privacy preservation", Future Generation Computer Systems,Vol. 109, pp. 621-632, 2020,https://doi.org/10.1016/j.future.2018.04.089

[18] L. Jiang, C. Xu, X. Wang, B. Luo, and H. Wang, "Secure outsourcing SIFT: Efficientand privacy-

preserving image feature extraction in the encrypted domain", in IEEETransactions on Dependable and Secure Computing, vol. 17, no. 1, pp. 179-193, 1 Jan.-Feb. 2020, doi: 10.1109/TDSC.2017.2751476.9

[19] Anyu Du 1, Liejun Wang, Shuli Cheng and NaixiangAo, "A Privacy-Protected ImageRetrieval Scheme for Fast and Secure Image Search", MDPI - Symmetry 2020, 12(2),282, Feb 2020, https://doi:10.3390/sym12020282

[20] Zongye Zhang, Fucai Zhou, Shiyue Qin, Qiang Jia and Zifeng Xu, "Privacy-PreservingImage Retrieval and Sharing in Social Multimedia Applications", inIEEE Access, Vol.8,pp. 66828-66838, Mar 2020,https://doi.org/10.1109/ACCESS.2020.2984916

[21] Hu, Lishuang& Xiang, Tao & Guo, Shangwei, "SensIR: Towards privacy-sensitiveimage retrieval in the cloud", Signal Processing: Image Communication, 84, 115837,Mar 2020,doi: 10.1016/j.image.2020.115837

[22] Chengyuan Zhang, Lei Zhu, Shichao Zhang, Weiren Yu, "TDHPPIR: An Efficient DeepHashing Based Privacy-Preserving Image Retrieval Method", Neurocomputing, Vol.406, pp. 386-398, April 2020,https://doi.org/10.1016/j.neucom.2019.11.11

[23] Youcef Imine, Ahmed Lounis, AbdelmadjidBouabdallah, "An accountable privacy-preserving scheme for public information sharing systems", Elsevier (Computers &Security), Vol. 93, 101786, 2020, https://doi.org/10.1016/j.cose.2020.101786

[24] K. Iida and H. Kiya, "Privacy-Preserving Content-Based Image Retrieval UsingCompressible Encrypted Images", in IEEE Access, vol. 8, pp. 200038-200050, Nov2020, doi: 10.1109/ACCESS.2020.3035563.

[25] K. Iida and H. Kiya, "A Privacy-Preserving Content-Based Image Retrieval SchemeAllowing Mixed Use of Encrypted and Plain Images", 2020 Asia-Pacific Signal andInformation Processing Association Annual Summit and Conference (APSIPA ASC), pp.1436-1441, Dec 2020.

[26] Wang, Z., Qin, J., Xiang, X. et al., "A privacy-preserving and traitor tracking content-based image retrieval scheme in cloud computing", in Multimedia Systems 27, pp.403–415, Jan 2021, https://doi.org/10.1007/s00530-02000734-w

[27] K. Iida and H. Kiya, "Privacy-preserving Image Retrieval Scheme Allowing Mixed Useof Lossless and JPEG Compressed Images", 2021 IEEE 3rd Global Conference on LifeSciences and Technologies (LifeTech), pp. 37-39, April 2021,doi:10.1109/LifeTech52111.2021.9391868.

[28] [28] L. Wang and H. Yu, "A Secure Searchable Image Retrieval Scheme with CorrectRetrieval Identity", 2021 IEEE International Conference on Acoustics, Speech andSignal Processing (ICASSP), pp. 8183-8187, May 2021,doi: 10.1109/ICASSP39728.2021.94140240

[29] Kumar, S., Pal, A.K., Islam, S. et al., "Secure and efficient image retrieval throughinvariant features selection in insecure cloud environments", in Neural Computing &Applications, June 2021, https://doi.org/10.1007/s00521-021-06054-y

[30] J. T and B. M, "SEcure Similar Image Matching (SESIM): An Improved PrivacyPreserving Image Retrieval Protocol over Encrypted Cloud Database", in IEEETransactions on Multimedia, August 2021, doi: 10.1109/TMM.2021.3107681.

[31] Khetani, V. ., Gandhi, Y. ., Bhattacharya, S. ., Ajani, S. N. ., & Limkar, S. . (2023). Cross-Domain Analysis of ML and DL: Evaluating their Impact in Diverse Domains. International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 253–262.

[32] R. Patil Rashmi, Y. Gandhi, V. Sarmalkar, P. Pund and V. Khetani, "RDPC: Secure Cloud Storage with Deduplication Technique," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 1280-1283, doi: 10.1109/I-SMAC49090.2020.9243442.

[33] Prof. Bhushan Thakre, Dr. R.M Thakre. (2017). Analysis of Modified Current Controller and its Implementation in Automotive LED. International Journal of New Practices in Management and Engineering, 6(04), 01 - 06. https://doi.org/10.17762/ijnpme.v6i04.60

[34] Smith, J., Ivanov, G., Petrović, M., Silva, J., & García, A. Detecting Fake News: A Machine Learning Approach. Kuwait Journal of Machine Learning, 1(3). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/142

[35] Dhingra, M., Dhabliya, D., Dubey, M. K., Gupta, A., & Reddy, D. H. (2022). A review oncomparison of machine learning algorithms for text classification. Paper presented at theProceedings of 5th International Conference on Contemporary Computing and Informatics, IC3I 2022, 1818-1823. doi:10.1109/IC3I56241.2022.10072502 Retrieved from www.scopus.com