IRAQI Academic Scientific Journals
العراقية المجلات الأكاديمية العلمية
Kut University Journal
ISSN (E): 2616 - 7808 II ISSN (P): 2414 - 7419
www.kutcollegejournal.alkutcollege.edu.iq
k.u.c.j.sci@alkutcollege.edu.iq
Vol. 10 , Issue 1 , June 2025

A Comprehensive Survey of Privacy-Preserving Techniques for Cloud-Based Image Retrieval

Shaimaa Miteb Sadoon [1] , Ziyad Tariq Mustafa Al-Ta'i [2]

Abstract

"Content-Based Image Retrieval" (CBIR) refers to searching for and retrieving images without relying on metadata or user comments. As cloud services are increasingly in demand, CBIR has emerged as an efficient and effective solution for image storage systems; however, the problem of users' right to privacy poses significant obstacles to consumer adoption. To address this challenge, CBIR systems that safeguard users' privacy have been developed. These methods ensure the secure recovery of images and protect any sensitive information contained within them. This all-encompassing review delves into various strategies for retrieving images from the cloud while preserving users' privacy. We scrutinize methods that rely on encryption, secure multi-party computation, and potential future breakthroughs in this field. Our goal is to provide researchers with a comprehensive understanding of privacy protection in cloud-based image retrieval by assessing the pros and cons of each strategy. As a result, we examine the benefits and drawbacks of each strategy. Consequently, our survey results prove to be an indispensable resource for accelerating innovation and devising efficient strategies to protect users' privacy.

Keywords: Content-Based Image Retrieval (CBIR), Privacy, Cloud

Affiliation of Authors

[1,2] College of Science, University of Diyala, Iraq, Diyala, 32000

[1] scicompms2212@uodiyala.edu.iq
[2] ziyad1964tariq@uodiyala.edu.iq

[1] **Corresponding Author**

Paper Info.
Published: Jun. 2025

مسح شامل لتقنيات الحفاظ على الخصوصية لاسترجاع الصور القائمة على السحابة

شيماء متعب سعدون [1] ، زياد طارق مصطفى الطائي [2]

المستخلص

يشير مصطلح "استرداد الصور المستند إلى المحتوى" (CBIR) إلى تقنية البحث عن الصور واستردادها دون الاعتماد على البيانات الوصفية أو تعليقات المستخدم. مع تزايد الطلب على الخدمات السحابية ، برز CBIR كحل فعال وكفوء لأنظمة تخزين الصور ؛ ومع ذلك ، فإن مشكلة حق المستخدمين في الخصوصية تشكل عقبات كبيرة أمام تبني المستهلك. لمواجهة هذا التحدي ، تم تطوير أنظمة CBIR التي تحمي خصوصية المستخدمين. تضمن هذه الأساليب الاسترداد الآمن للصور وحماية أي معلومات حساسة واردة بداخلها. تتعمق هذه المراجعة الشاملة في استراتيجيات مختلفة لاسترداد الصور من السحابة مع الحفاظ على خصوصية المستخدمين. نقوم بفحص الطرق التي تعتمد على التشفير والحساب الآمن متعدد الأطراف والاختراقات المستقبلية المحتملة في هذا المجال. هدفنا هو تزويد الباحثين بفهم شامل لحماية الخصوصية في استرداد الصور المستند إلى السحابة من خلال تقييم إيجابيات وسلبيات كل إستراتيجية. نتيجة لذلك ، نقوم بفحص مزايا وعيوب كل استراتيجية. وبالتالي ، أثبتت نتائج استطلاعنا أنها مورد لا غنى عنه لتسريع الابتكار واستنباط استراتيجيات فعالة لحماية خصوصية المستخدمين.

الكلمات المفتاحية: استرجاع الصور المستند الى المحتوى، الخصوصية، الحوسبة

انتساب الباحثين

[1، 2] كلية العلوم، جامعة، العراق، ديالى، 32000

[1] scicompms2212@uodiyala.edu.iq
[2] ziyad1964tariq@uodiyala.edu.iq

[1] **المؤلف المراسل**

معلومات البحث
تأريخ النشر : حزيران 2025

1. Introduction

Over the past two decades, there has been a significant increase in the volume of multimedia. Data is generated, primarily driven by advancements in consumer electronics, particularly

smartphones. This data is frequently shared among individuals and on various social media platforms. For instance, Facebook and Instagram alone witnessed approximately 250 billion and 40 billion image shares in a single year, highlighting the exponential growth in multimedia data usage[1]. However, with such massive amounts of data, retrieving specific images from vast repositories poses a significant challenge. In response to this challenge, cloud services have emerged as a convenient and cost-effective solution for storing and sharing images. Users can transfer their data to cloud servers, which act as third-party entities responsible for storing, managing, and facilitating future data retrieval [2].

CBIR services can be resource-intensive in terms of storage and computation. However, cloud platforms offer the scalability and computing power required for large-scale CBIR systems, making data outsourcing feasible. By offloading CBIR functionalities to the cloud, data owners can alleviate the burden of maintaining a local image database and meeting user and application requirements. Nevertheless, cloud platforms introduce security concerns regarding the storage, transmission, and retrieval of images.[3], especially considering the sensitive personal or business information within them. A reliable cloud service must provide secure mechanisms for transferring, sharing, and accessing data. For example, a patient may need to share medical images with their doctor in the healthcare domain. However, there is a risk of data leakage or unauthorized access due to potential malicious actions by the cloud service provider (CSP) or security breaches. To mitigate these risks, a common practice is to encrypt users' images before uploading them to the cloud server. These encrypted images are subsequently retrieved using queries. In a healthcare setting, a hospital may store many medical images on remote cloud servers, enabling doctors to review similar cases for better analysis and treatment of patients. Doctors can generate queries based on medical features to retrieve similar cases. If the CBIR service provided by the CSP is effective, it may return correct images, leading to accurate diagnoses. Users encrypt their images before transferring them to the cloud to ensure security. Image retrieval is then performed based on the encrypted features of these images. Initially, image retrieval relied on manual annotation, which varied from person to person based on visual perception. However, with a large number of images, manual annotation becomes impractical. Content-based image retrieval (CBIR)[4][5] Offers a practical solution to retrieve similar images from a large dataset. In CBIR systems, image features, such as color[6], texture[7], and shape[8], play a crucial role in retrieval.

This has led to a critical need for secure and efficient mechanisms to manage large-scale images in the context of cloud-based image retrieval (CBIR) technology[9][10]. In this comprehensive survey, we delve into privacy-preserving techniques for CBIR. We explore the various approaches and methodologies developed to address the challenges of ensuring privacy while achieving accurate and efficient image retrieval. By examining recent research and advancements in the field, we aim to thoroughly analyze the state-of-the-art privacy-preserving techniques employed in cloud-based image retrieval. Throughout this survey, we will discuss the practical implications and considerations associated with privacy-preserving techniques,

highlighting their benefits and limitations.

Additionally, we will present key findings from relevant studies and highlight the significance of privacy preservation in the context of CBIR. We hope to illuminate this dynamic field's significant challenges and future directions by doing so. This survey is a comprehensive guide for researchers, practitioners, and stakeholders interested in understanding and implementing privacy-preserving techniques for cloud-based image retrieval. By gaining insights into the current landscape and emerging trends, we can foster the development of secure and efficient solutions that safeguard privacy while facilitating effective image retrieval in the cloud.

2. An Overview of the CBIR Flowchart

The initial framework of the CBIR (Content-Based Image Retrieval) system consists of two main subsystems: offline and online. In the offline subsystem, each image undergoes coding, where its feature vector is extracted and used as an index in the retrieval database. Moving to the online subsystem, when a query image is input, its feature vector is extracted using the same methodology employed for the images in the retrieval dataset. Subsequently, this feature vector calculates similarity scores between the query image and all possible images in the database. Images that surpass a predefined threshold in similarity score are then selected for further refinement, aiming to enhance the visual context compared to the original query. Finally, these refined images are presented as the retrieval system's probability-ordered results, arranged in descending order based on the rerank score. Within this framework, the cornerstone of the CBIR system lies in feature-based image representation, which is crucial for dataset indexing with a specific similarity measure. From a technological standpoint, the CBIR system relies on advancing image representation techniques and efficient database search algorithms. Therefore, in our survey of CBIR research, we explore the developments in image representation and database search.

Individually, recognizing their significance in advancing the field. [11]**.** These subsystems are depicted as shown in Figure (1).

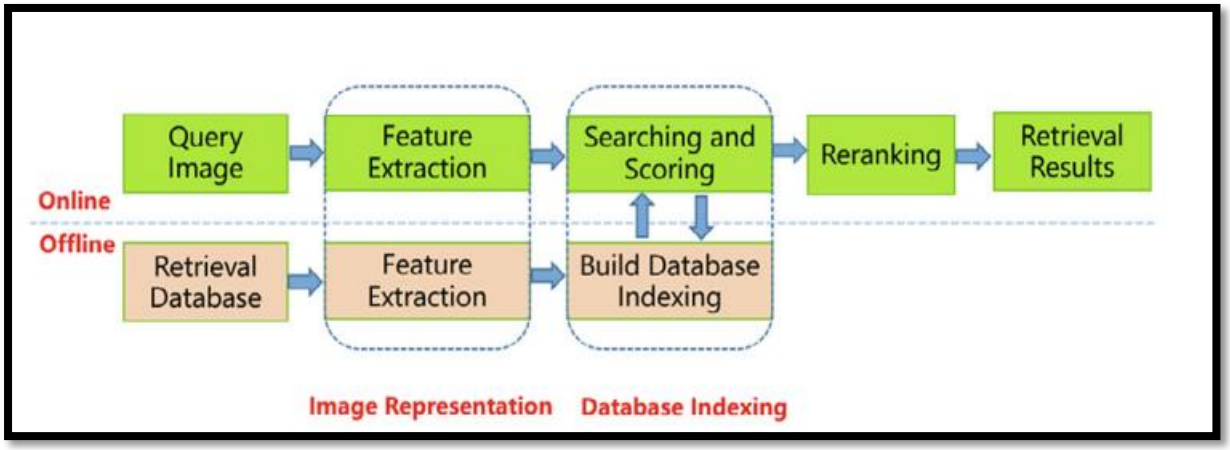

Figure (1): Structure of CBIR[11]

2. Image representation

Image representation is a crucial process in CBIR (Content-Based Image Retrieval) as it extracts critical features from an image and transforms them into a fixed-size vector known as a feature vector. Any content-based image retrieval method

must begin with the extraction of visual features. Features refer to textual information (keywords or comments) or visual information (color, texture, shape, etc.). Features can be further broken down into low-level and high-level categories within the visual feature scope. One of the crucial elements of a CBIR system is the use of characteristics to represent a picture. Due to the subjective nature of seeing and the intricate nature of visual data, there is no perfect depiction of any visual characteristic. Each of these visual characteristics has been established in several ways, each of which provides a unique characterization of the feature.[12].

4. Content-Based Image Retrieval (CBIR) based on Deep learning

The primary purpose of content-based image retrieval, often known as CBIR approaches, is to locate and display all images that share visual content that is comparable to a specified query image[13]. Three distinct eras can be distinguished by how they exported the numerous low-level features that represent the visual content of an image.[14]. The figure shows that 2. In 2015, image retrieval entered a new era. Deep learning (DL) techniques are increasingly used in scientific investigations. In many computer vision tasks, DL methods have surpassed the performance of more conventional low-level-based algorithms,garnering much interest.[13], as shown in Figure (2).

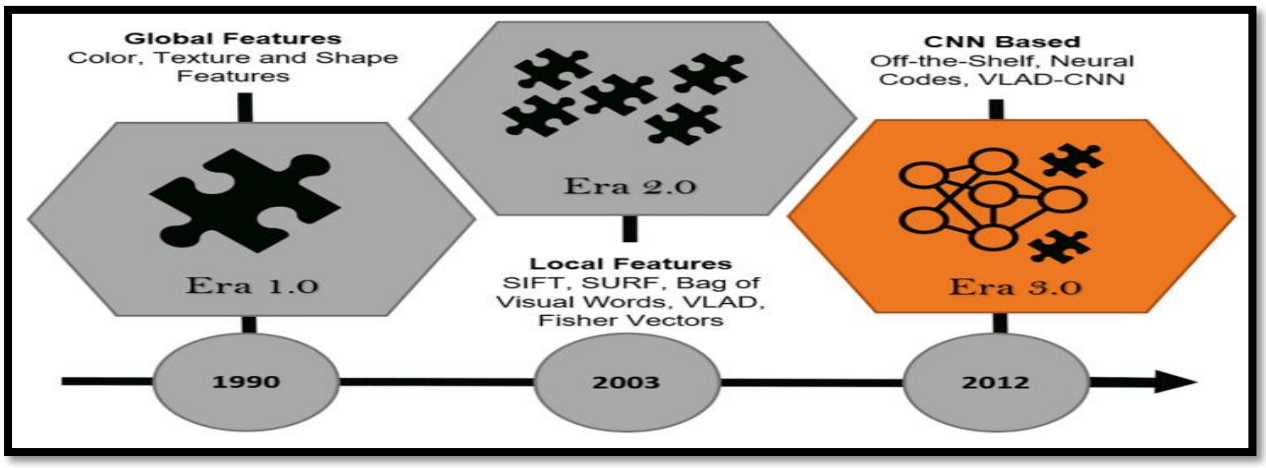

Figure (2) : Illustration of Content-Based Image Retrieval Eras[13]

4.1 Deep learning

A subset of machine learning methods[15] , that use multiple layers of nonlinear information processing for both supervised and unsupervised feature extraction and transformation, as well as pattern analysis and classification[16]. These neural networks are made up of neurons that are arranged in layers. The network is called deep because it comprises multiple layers stacked on top of each other. This is referred to as deep learning. When the layers of a deep learning network fire, they communicate with one another by sending signals. When the output of a layer cannot be seen directly, it is said to be hidden[17], as shown in Figure (3).

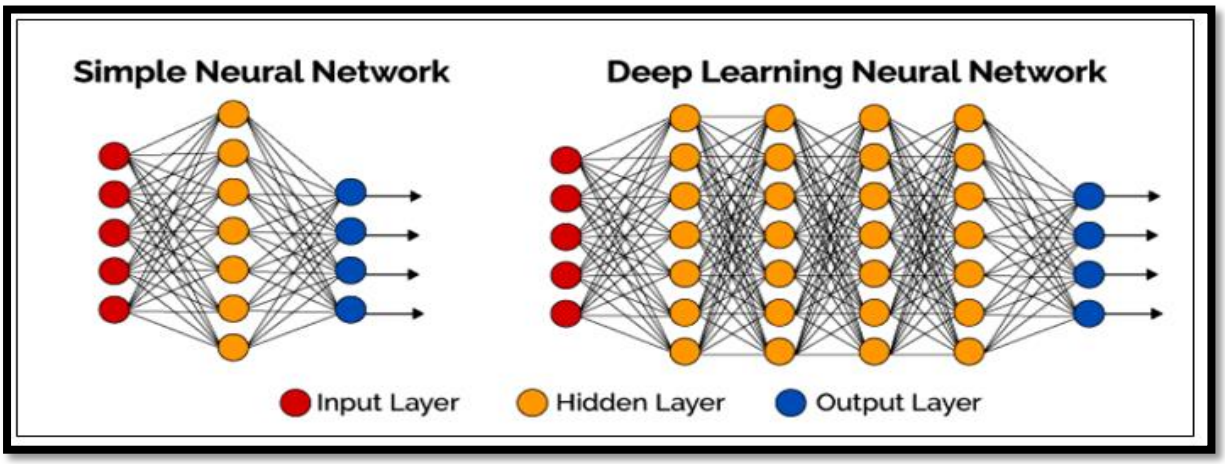

Figure (3): Neural Network Architecture[17]

5. A Privacy-Preserving Image Retrieval Method

Existing privacy-preserving CBIR techniques may be broken down into two groups: feature-encryption-based methods and image-encryption-based methods:-

5.1 Schemes that use CBIR features for encryption

In these techniques, the initial step is for the image's owner to extract visual features from the plaintext image. The photos are then encrypted using ordinary cryptographic methods, and the extracted features require additional encryption using methods developed to facilitate similarity computing. Effective photo feature descriptors have been proven in a large body of research to boost retrieval rates. In 2015, a suggestion was made by Xia et al. [18], for a Scale-Invariant Feature Transformation (SIFT) and Earth Mover's Distance (EMD)-based CBIR that ensured users' anonymity. The utilization of SIFT for image feature representation and empirical mode decomposition for similarity measurement was employed. The calculation of EMD was necessary to solve the linear programming problem. A linear transformation was used to shield the sensitive parameters of the problem. Xia et al. [19] suggested CBIR on encrypted photos in 2016. Extracting feature vectors represents images. This method employs MPEG-7's SCD, CSD, CLD, and EHD visual descriptors. Secure kNN encrypts features. Locality-sensitive hashing (LSH) pre-filter tables and stream cipher-encrypted image pixels sped up the search; Figure 2 shows that. In 2019, a surveillance video privacy-preserving method based on personal Re-identification (Re-ID) was suggested by Cheng et al. [20]. The technique includes incorporating the CNN model, which employs binary representation to convey highly accurate and effective visual information. The ideal connection between the dimension of the feature index and the number of cloud servers is disregarded by this method, resulting in a significant diminishment of the user experience, and safe person re-identification is not deemed very effective in a real-world setting. In 2019, a Speeded-Up Robust Feature (SURF) was extracted from photos by Qin et al. [21], who also developed chaotic encryption to preserve features and utilized Locality Sensitive Hashing (LSH) to enhance retrieval efficiency. In 2019, Qin et al. [22]used deep learning and adaptive weighted fusion for picture retrieval. Start by extracting low-level

characteristics like EHD (edge histogram descriptor), BOW (bag of words), CLD (Color layout descriptor), and high-level semantic features (CNN) of photos. Second, a principal component analysis (PCA) reduced the dimension of a 1024-dimensional high-level semantic feature, and then each of the three features was binarized. This sort of element is then adaptively merged.

The final stage is creating a prefilter table for fusion features using locality-sensitive hashing (LSH) to improve search performance. KNN and logistic encryption were employed to protect the fused features and photos. In 2020, Li et al. [23], introduced a method for similarity search of encrypted photos in secure cloud computing. This technique incorporates feature descriptors from the CNN model and employs K-means clustering based on affinity propagation to improve search efficiency and accuracy. Furthermore, a restricted key-leakage k-Nearest Neighbour is implemented to safeguard image privacy simultaneously, as shown in Figure (4).

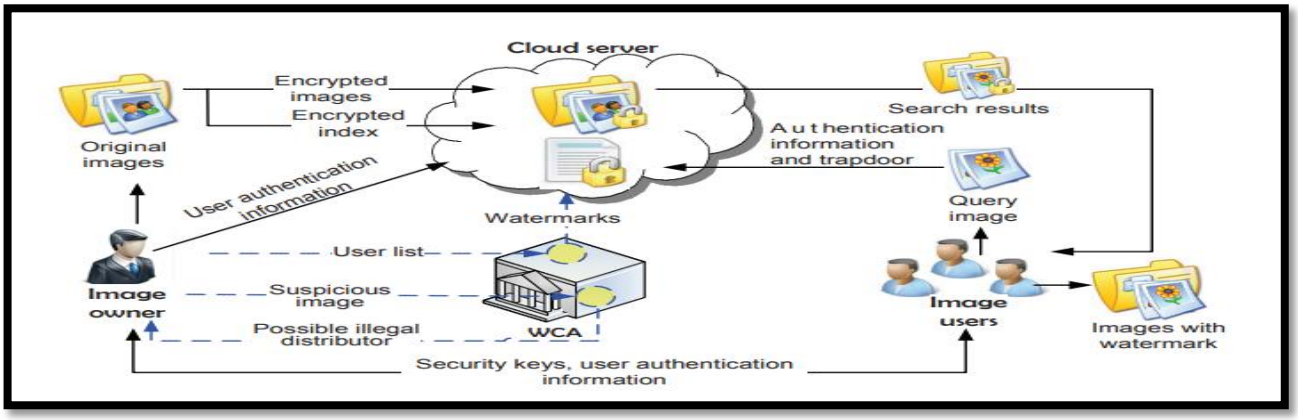

Figure (4): The System proposed in [19]

5.2 Schemes for image encryption based on CBIR

The abovementioned strategies effectively retrieve images while protecting users' privacy. However, the picture owner is responsible for completing the computation-intensive chores of extracting features and building the index, which was the case in previous efforts. Researchers presented numerous image-encryption-based privacy-preserving CBIR techniques to alleviate the responsibilities of picture owners further. Owners of the photographs need merely encrypt them for use in such systems. Outsourcing to the cloud is an option for doing feature extractions, index building, and CBIR services. In 2017, Xia et al. examined a method.[24], that enables encrypted photos to be used for CBIR without revealing any private data to the cloud server. This technique incorporates secure k-nearest neighbors to protect the picture feature representation vector and employs position-sensitive hashing to enhance the effectiveness of its searches. In 2018, Shen et al. [25] suggested an MIPP-secure CBIR mechanism. A secure multi-party computing approach lets picture owners encrypt image features using their keys. This allows efficient picture retrieval from many sources without compromising image privacy. They also developed a novel picture similarity measuring approach that avoids cloud disclosure. In 2019, Ferreira et al.[26] Proposed the IES-CBIR, which offers encrypted image storage and CBIR service while providing defense

against an Honest-But-Curious (HBC) cloud server. In a cloud environment, the HSV feature descriptors of the encrypted pictures are retrieved, and a similarity-matching search is performed based on the Hamming distance between the feature representations. The IES-CBIR enables picture owners to significantly reduce their computational requirements by offloading the computation burden to the cloud server. Gu et al. [27], 2020. This study explored MSPPIR's problems. Using the JPEG picture as an example, they proposed JES-MSIR—a unique JPEG image encryption approach for Multi-Source content-based picture retrieval. JES-MSIR can meet MSPPIR's demands by securely retrieving information continuously from various sources and combining sources for better retrieval services. They used randomized encryption to increase efficiency, accuracy, and security. The image was secured by the bit xor, permutation, and Bag-of-words model (BOW). Pan et al. [10] proposed a CNN-based hashing method for encrypted picture retrieval in 2021. The picture size was increased to increase the CNN's representation capacity, and a lightweight module was created to replace sections of the modules to decrease the CNN's parameters and computing cost. Finally, a hash layer created a tiny binary hash code. Ma et al. [28] presented a CNN-based picture retrieval system that preserves users' privacy in 2022. This system evaluated data sensitivity during cloud computing preparation, storage, and searchability. They created ChannelEnc, SequenceEnc, and PositionEnc hybrid encryption. This approach protects photographs' color and texture information, preventing unauthorized cloud servers from releasing essential data. An updated DenseNet model lets the cloud server extract semantic characteristics from encrypted pictures. It then used feature similarity matching to retrieve all results with those extracted features. They suggested an MIPP-secure CBIR mechanism. A secure multi-party computing approach lets picture owners encrypt image features using their keys. This allows efficient picture retrieval from many sources without compromising image privacy. They also developed a novel picture similarity measuring approach that avoids cloud disclosure as shown Figure (5).

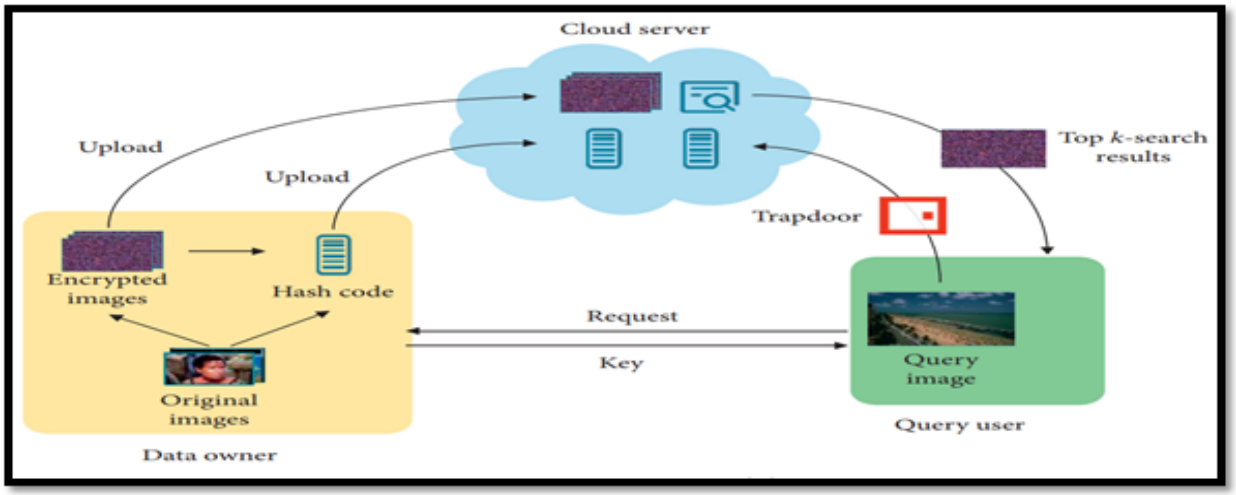

Figure (5): The model proposed in [10]

6. Performance Analysis and Discussion

6.1 Retrieval Performance

The evaluation metric of retrieval performance is Average Precision [29] (AP) which is widely used in many retrieval tasks. When returning top-*K* results, mAP and the equation of the data is given by equation (1) and (2).

$$AP@K(q) = \frac{1}{R_q} \sum_{k=1}^{K} P_q(k)\, rel_q(k) \quad (1)$$

$$mAP@K = \frac{1}{Q} \sum_{QQ=1}^{Q} AP@K\,(q) \quad (2)$$

Comparison of average search precision with different encryption techniques on the Corel10k dataset. As shown in Table (1) and shown in Figure (6).

Table (1): Comparison of average search precision with different encryption techniques

		AP@K (%)				
NO.	**Author(s)**	**Top-20**	**Top-40**	**Top-60**	**Top-80**	**Top-100**
1	**Xia et al. [19],2016**	**CSD 36.67**	**29.74**	**25.33**	**22.63**	**20.38**
		SCD 23.44	**17.05**	**14.53**	**12.46**	**11.29**
		CLD 20.16	**15.43**	**12.76**	**11.83**	**10.65**
		EHD 19.13	**14.82**	**12.66**	**11.37**	**10.19**
2	**Xia et al. [24],2017**	**CLD 20**	**15.43**	**12.74**	**11.87**	**10.67**
		EHD 19.16	**14.77**	**12.57**	**11.33**	**10.17**
3	**Shen. Et al.[25]2018**	**25.92**	**24.71**	**23.98**	**23.47**	**22.64**
4	**Qin et al.[22],2019**	**69.5**	**61.94**	**56.42**	**51.06**	**46.9**
5	**Gu et al. [27],2020**	**32.44**	**25.57**	**21.92**	**19.51**	**17.62**
6	**Pan et al. [10], 2021**	**86.23**	**86.21**	**86.15**	**86.08**	**69.91**
7	**Ma et al. [28], 2022**	**68.26**	**65.39**	**59.78**	**50.92**	**44.06**

Reference: Results of the program [19] [24] [25] [22] [27] [10] [28].

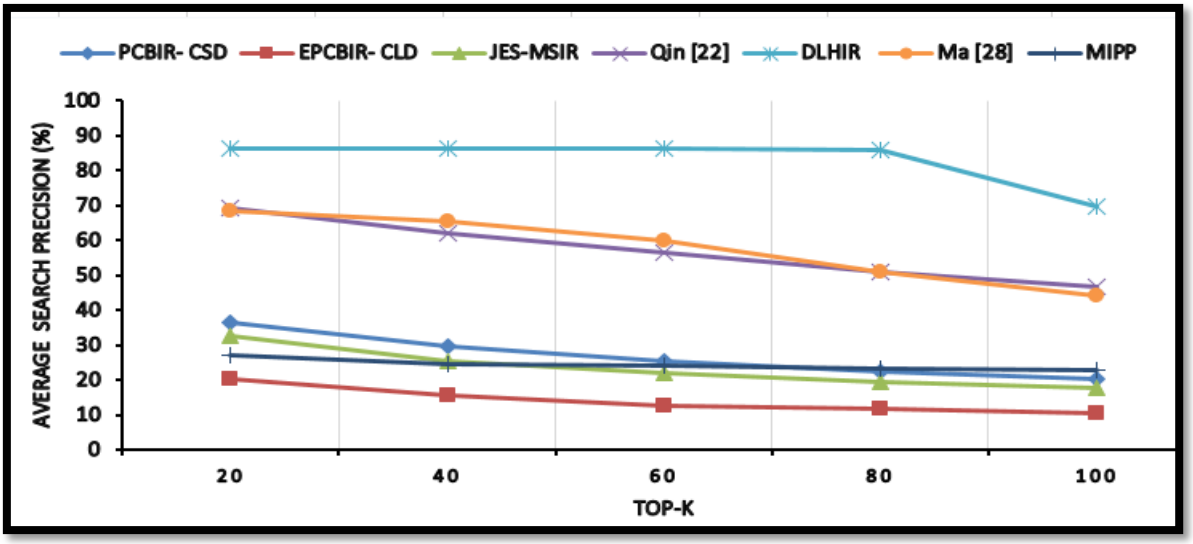

Figure (6): Comparison of average search precision for different models

6.2 Search efficiency

In this section, the efficiency of methods will be demonstrated by image encryption, feature extraction, index construction, search time, and image decryption. As shown in Tables (2), Table (2) and Figure (7).

Table (2): Comparison of average search time with different encryption techniques on the Corel10k dataset

No.	Author(s)	Average search time No. of image collection ($\times 10^3$)				
		2	4	6	8	10
1	Xia et al. [19],2016	CSD 8.45ms SCD 7.51ms CLD 7.64ms EHD 6.17ms	14.41ms 13.47ms 13.53ms 11.12ms	20.15ms 18.27ms 18.79ms 15.65ms	25.69ms 23.70ms 23.01ms 19.86ms	30.28ms 29.45ms 30.28ms 23.76ms
2	Xia et al. [24], 2017	CLD 7.68ms EHD 6.17ms	13.42ms 11.16ms	18.74ms 15.57ms	23.06ms 19.89ms	28.39ms 23.63ms
3	Shen. et al.[25]2018	29ms	37ms	38ms	44ms	50ms
4	Qin et al.[22], 2019	CNN 3.72ms	6.69ms	9.85ms	13.70ms	16.17ms
5	Gu et al. [27],2020	0.11s for retrieval(Top-50)				
6	Pan et al. [10], 2021	0.58ms	0.742ms	0.908ms	1.073ms	1.249ms
7	Ma et al. [28]	14.77ms	20.14ms	24.89ms	29.95ms	34.19ms

Reference: Results of the program [19] [24] [25] [22] [27] [10] [28].

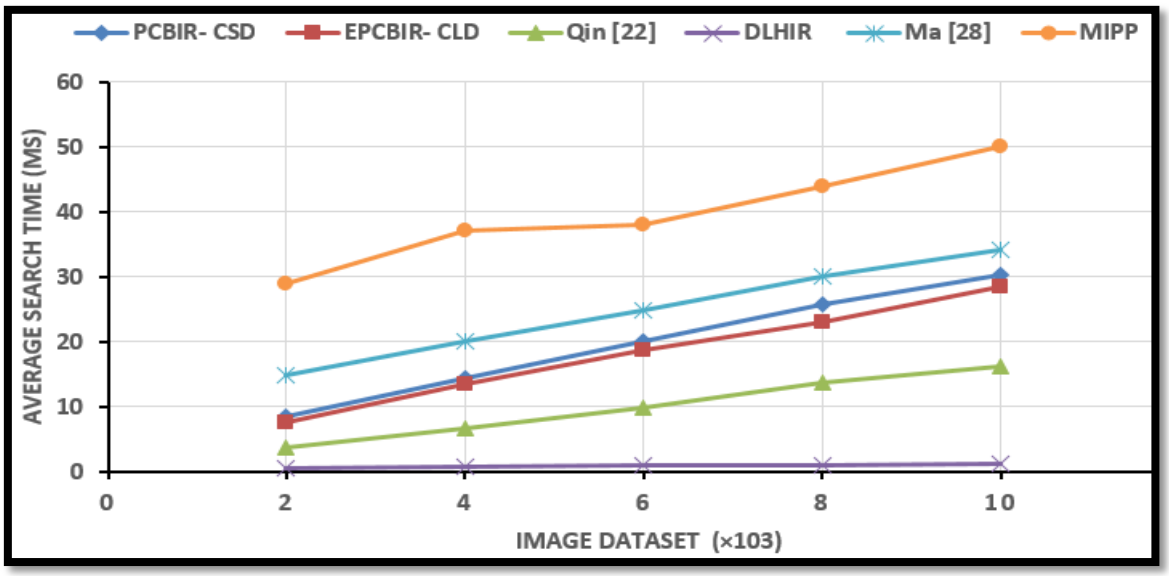

Figure (7): Comparison of average search time for different models on the Corel 10K dataset

Table (3): Comparison of the time consumption of index construction and the time of trapdoor with different encryption techniques

N0.	Author(s)	Time consumption of index construction No. of image collection ($\times 10^3$)					Time of Trapdoor generation
		2	4	6	8	10	
1	Xia et al. [19],2016	CSD 615.41ms SCD 572.97ms CLD 562.33ms EHD 392.57ms	1254.64ms 1201.59ms 986.73ms 572.94ms	1872.6ms 1671.10ms 1517.24ms 848.80ms	2533.14ms 2299.72ms 1920.42ms 1262.59ms	3140.58ms 2801.03ms 2514.58ms 1496.02ms	4ms 4ms 3.5ms 1.3ms
2	Xia et al. [24], 2017	CLD 552.63ms EHD 403.50ms	982.45ms 578.94ms	18.74ms 842.105ms	1912.28ms 1263.15ms	2508.77ms 1482.45ms	3.558ms 1.27ms
3	Shen. et al.[25]2018	83.307 s	169.804s	244.847s	328.108s	419.724s	
4	Qin et al.[22], 2019	759.40ms	1496.72ms	2181.001ms	2918.31ms	3655.60ms	10.48ms
5	Gu et al. [27],2020	Total time consumption 4.63s Decryption 4.43s					0.09s
6	Pan et al. [10], 2021	Time of feature extraction: 128.25s					8.86ms
7	Ma et al. [28]	Time of feature extraction: 67.2s					1.5s

Reference: Results of the program [19] [24] [25] [22] [27] [10] [28].

The provided results show the retrieval accuracy (AP@K) and retrieval time for different authors and their methods. We can observe variations among the different authors and methods in retrieval accuracy. For example, Xia et al. [57] achieved AP@Top-20 of 36.67% for the CSD method, 23.44% for the SCD method, 20.16% for the CLD method, and 19.13% for the EHD method. Similarly, other authors such as Qin et al. [59], Gu et al. [60], Pan et al. [9], and Ma et al. [61] also achieved varying levels of retrieval accuracy across different values of K. On the other hand, the retrieval time also varies across the different methods. Xia et al. [57] reported average search times ranging from 6.17 ms to 30.28 ms, depending on the number of images in the collection. Xia et al. [54] achieved an average search time of 7.68 ms. Shen et al. [58] reported a retrieval time of 29 ms. Qin et al. [59] performed a retrieval time of 7.8 ms for their CNN-based

method. Gu et al. [60] reported a retrieval time of 0.11 seconds for retrieving the top 50 results. Pan et al. [9] achieved a retrieval time of 0.58 ms. Ma et al. [61] reported a retrieval time of 14.77ms.

Overall, there is no clear correlation between retrieval accuracy and retrieval time among the authors and methods. Some methods may achieve higher accuracy but require more time for retrieval, while others may have lower accuracy but faster retrieval times. The plan choice would depend on the specific requirements and trade-offs of the application.

7. Similarity Measurement

Finding appropriate similarity measures to compare images based on their features is a complex task in content-based image retrieval (CBIR). The goal is to efficiently retrieve images from a database similar to a user-specified query image. Similarity measurement involves determining the degree of similarity or dissimilarity between the query image and the images in the database based on their respective features. The database images are then sorted in ascending order of their distance to the query image, and images are retrieved accordingly. Various distance measures can be employed to assess the similarity between two images based on their features.[30]. The choice of a specific measure can significantly impact the retrieval performance, depending on the measures' characteristics and the retrieval application's requirements. Some commonly used measures include:

I. Minkowski-Form Distance

The Minkowski-Form distance is a widely utilized metric in image retrieval. It is commonly employed to compare two feature vectors, f1 and f2, each consisting of N bins, and the equation of the data is given by equation (3).

$$\boldsymbol{D(f_1, f_2) = (\sum_1^N | f_1(i) - f_2(i)|^p)^{1/p}} \qquad \textbf{(3)}$$

In this measure, each dimension of the image feature vector is independent and equally important. The parameter 'p' determines the type of distance. When p = 1, the Minkowski-Form corresponds to the Manhattan Distance (or city-block) (L1). When p = 2, it represents the Euclidean Distance (L2). Lastly, when p = ∞, it is referred to as the Chebyshev Distance (L∞).

II. Euclidean Distance

Many content-based picture retrieval methods employ the Euclidean distance to measure vector distance. It works when all picture feature vector components are equally relevant and independent. Euclidean distance is the usual distance between two values. It is the square root of the vector components' squared differences. The Euclidean distance for feature vectors P=(p1,p2,p3,……pn) and Q=(q1,q2,q3,…..qn) and the equation of the data is given by equation (4).

$$\boldsymbol{D = \sqrt{\sum_{k=1}^{n} (p_k - q_k)^2}} \qquad \textbf{(4)}$$

Where n is the feature vector length, and D is the distance between the vectors. The Euclidean distance is a basic, low-complex way to estimate feature vector distance. Thus, feature vector comparisons are widespread. Commercial CBIR systems use Euclidean distance. MARS[31] Calculates texture feature similarity using Euclidean distance. Blobworld[32] uses Euclidean distance for texture, while Netra [33]Uses it for color and form.

III. Manhattan Distance

If the Euclidean distance can be considered the straight-line distance between points, then the Manhattan distance can be seen as the approach of moving along the sides of a square. This distinction gives the Manhattan distance its name, as the layout of Manhattan is organized in city blocks, requiring you to travel two sides of a square to reach a destination. The Manhattan distance between feature vectors P = (p1, p2, ..., pn) and Q = (q1, q2, ..., qn) and the equation of the data is given by equation (5).

$$\boldsymbol{D = \sum_{k=1}^{n} |p_k - q_k|} \quad \textbf{(5)}$$

Where n is the length of the feature vector, and D represents the distance between the two vectors.

8. Applications of Content-Based Image Retrieval

A Diverse Range of Fields. The applications of CBIR technology encompass a wide array of fields, each utilizing its capabilities to address specific challenges and enhance various processes. Here are some important applications:

a) Investigations: CBIR finds application in face recognition systems, aiding in identity verification and crime investigations. It also assists in identifying copyright infringements on the Internet.
b) Shapes Identification: CBIR plays a vital role in industrial automation by enabling the identification of defects and faults in manufacturing processes.
c) Medical Diagnosis: CBIR contributes to medical imaging by facilitating tumor detection, improving the accuracy of MRI and CT scans, and aiding in interpreting medical images.
d) Journalism, Advertising, Media, Fashion, and Graphic Design: CBIR technology finds utility in these fields for content retrieval, image matching, and generating visual recommendations.
e) Remote Sensing: CBIR is instrumental in information systems, weather forecasting, and the analysis of satellite images for environmental monitoring and disaster management.
f) Trademark Databases, Art Galleries, Museums, and Archaeology: CBIR assists in managing and searching large databases of trademarks, cataloging art collections, preserving historical artifacts, and aiding archaeological research.
g) Architectural and Engineering Designs: CBIR aids architects and engineers in retrieving relevant design inspirations, analyzing existing structures, and exploring similar projects for reference.
h) Cartography: CBIR techniques are applied to map-making processes, such as synthesizing weather maps from photographs and creating composite maps for geographical analysis.
i) Digital Forensics: CBIR plays a crucial role in digital forensics, particularly in fingerprint matching for crime detection and evidence analysis.
j) Radar Engineering: CBIR techniques are employed in radar systems for target detection and identification, aiding military applications and surveillance.

These examples highlight CBIR technology's versatility and broad applicability across numerous domains, showcasing its potential to revolutionize various industries and disciplines.[12].

9. Conclusion

Cloud computing emerges as a highly efficient and effective solution for modernizing the photo storage system, allowing users to conveniently access their data whenever and wherever needed. However, the increasing demand for cloud-based image retrieval services is accompanied by concerns regarding users' privacy rights, presenting significant obstacles to widespread consumer adoption. To address this issue, researchers and developers have been working on the development of privacy protection systems that safeguard sensitive information while enabling secure photo recovery. This comprehensive review has explored various strategies, including encryption and secure multi-party computation, as well as potential future breakthroughs in this field. By analyzing the advantages and disadvantages of each approach, our objective has been to provide researchers and practitioners with a comprehensive understanding of privacy protection in cloud-based image retrieval. The insights gained from this survey can serve as a valuable resource, facilitating the acceleration of innovation and the creation of efficient strategies to ensure the preservation of users' privacy in the digital age.

References

[1] K. Smith, “Incredible Facebook statistics and facts,” Retrieved Febr., vol. 2, p. 2020, 53AD.

[2] P. Mell and T. Grance, “Draft NIST working definition of cloud computing,‖ Referenced on June. 3rd, 2009 Online at http://csrc. nist. gov/groups,” SNS/cloud-computing/index. html, 2009.

[3] S. Belguith, N. Kaaniche, M. Hammoudeh, and T. Dargahi, “Proud: Verifiable privacy-preserving outsourced attribute-based signcryption supporting access policy update for cloud-assisted IoT applications,” Futur. Gener. Comput. Syst., vol. 111, pp. 899–918, 2020.

[4] S. Kumar, J. Pradhan, and A. K. Pal, “A CBIR scheme using GLCM features in DCT domain,” in 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2017, pp. 1–7.

[5] S. Kumar, J. Pradhan, and A. K. Pal, “A CBIR technique based on the combination of shape and color features,” in Advanced Computational and Communication Paradigms: Proceedings of International Conference on ICACCP 2017, Volume 2, 2018, pp. 737–744.

[6] J. Huang, S. R. Kumar, M. Mitra, W.-J. Zhu, and R. Zabih, “Image indexing using color correlograms,” in Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 1997, pp. 762–768.

[7] J. Pradhan, A. Ajad, A. K. Pal, and H. Banka, “Multi-level colored directional motif histograms for content-based image retrieval,” Vis. Comput., vol. 36, no. 9, pp. 1847–1868, 2020.

[8] D. Zhang and G. Lu, “Review of shape representation and description techniques,” Pattern Recognit., vol. 37, no. 1, pp. 1–19, 2004.

[9] Y. Xu, J. Gong, L. Xiong, Z. Xu, J. Wang, and Y. qing Shi, “A privacy-preserving content-based image retrieval method in cloud environment,” J. Vis. Commun. Image

Represent., vol. 43, pp. 164–172, 2017, doi: 10.1016/j.jvcir.2017.01.006.

[10] W. Pan, M. Wang, J. Qin, and Z. Zhou, "Improved CNN-Based Hashing for Encrypted Image Retrieval," Secur. Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/5556634.

[11] X. Li, J. Yang, and J. Ma, "Recent developments of content-based image retrieval (CBIR)," Neurocomputing, vol. 452, pp. 675–689, 2021, doi: 10.1016/j.neucom.2020.07.139.

[12] A. K. Yadav, R. R. Vaishali, and A. P. Kumar, "Survey on Content-based Image Retrieval and Texture Analysis with Applications," Int. J. Signal Process. Image Process. Pattern Recognit., vol. 7, no. 6, pp. 41–50, 2014, doi: 10.14257/ijsip.2014.7.6.04.

[13] S. Gkelios, A. Sophokleous, S. Plakias, Y. Boutalis, and S. A. Chatzichristofis, "Deep convolutional features for image retrieval," Expert Syst. Appl., vol. 177, no. March 2020, p. 114940, 2021, doi: 10.1016/j.eswa.2021.114940.

[14] L. Zheng, Y. Yang, and Q. Tian, "SIFT Meets CNN: A Decade Survey of Instance Retrieval," IEEE Trans. Pattern Anal. Mach. Intell., vol. 40, no. 5, pp. 1224–1244, 2018, doi: 10.1109/TPAMI.2017.2709749.

[15] Y. Zhao, B. Hu, Y. Wang, X. Yin, Y. Jiang, and X. Zhu, "Identification of gastric cancer with convolutional neural networks: a systematic review," Multimed. Tools Appl., vol. 81, no. 8, pp. 11717–11736, 2022, doi: 10.1007/s11042-022-12258-8.

[16] L. Deng and D. Yu, "Deep learning: methods and applications," Found. trends® signal Process., vol. 7, no. 3–4, pp. 197–387, 2014.

[17] P. Mulders, "Using Semantic Roles to Improve Inference Systems".

[18] Z. Xia, Y. Zhu, X. Sun, Z. Qin, and K. Ren, "Towards privacy-preserving content-based image retrieval in cloud computing," IEEE Trans. Cloud Comput., vol. 6, no. 1, pp. 276–286, 2015.

[19] 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 Trans. Inf. Forensics Secur., vol. 11, no. 11, pp. 2594–2608, 2016, doi: 10.1109/TIFS.2016.2590944.

[20] H. Cheng, H. Wang, X. Liu, Y. Fang, M. Wang, and X. Zhang, "Person re-identification over encrypted outsourced surveillance videos," IEEE Trans. Dependable Secur. Comput., vol. 18, no. 3, pp. 1456–1473, 2019.

[21] J. Qin et al., "An Encrypted Image Retrieval Method Based on Harris Corner Optimization and LSH in Cloud Computing," IEEE Access, vol. 7, pp. 24626–24633, 2019, doi: 10.1109/ACCESS.2019.2894673.

[22] J. Qin, J. Chen, X. Xiang, Y. Tan, W. Ma, and J. Wang, "A privacy-preserving image retrieval method based on deep learning and adaptive weighted fusion," J. Real-Time Image Process., vol. 17, no. 1, pp. 161–173, 2020, doi: 10.1007/s11554-019-00909-3.

[23] Y. Li, J. Ma, Y. Miao, Y. Wang, X. Liu, and K. K. R. Choo, "Similarity Search for Encrypted Images in Secure Cloud Computing," IEEE Trans. Cloud Comput., vol.

10, no. 2, pp. 1142–1155, 2022, doi: 10.1109/TCC.2020.2989923.

[24] 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," Inf. Sci. (Ny)., vol. 387, pp. 195–204, 2017, doi: 10.1016/j.ins.2016.12.030.

[25] M. Shen, G. Cheng, L. Zhu, X. Du, and J. Hu, "Content-based multi-source encrypted image retrieval in clouds with privacy preservation," Futur. Gener. Comput. Syst., vol. 109, pp. 621–632, 2020, doi: 10.1016/j.future.2018.04.089.

[26] B. Ferreira, J. Rodrigues, J. Leitao, and H. Domingos, "Practical privacy-preserving content-based retrieval in cloud image repositories," IEEE Trans. Cloud Comput., vol. 7, no. 3, pp. 784–798, 2017.

[27] Q. Gu, Z. Xia, and X. Sun, "MSPPIR: Multi-Source Privacy-Preserving Image Retrieval in cloud computing," Futur. Gener. Comput. Syst., vol. 134, pp. 78–92, 2022, doi: 10.1016/j.future.2022.03.040.

[28] W. Ma, T. Zhou, J. Qin, X. Xiang, Y. Tan, and Z. Cai, "A privacy-preserving content-based image retrieval method based on deep learning in cloud computing," Expert Syst. Appl., vol. 203, no. November 2021, p. 117508, 2022, doi: 10.1016/j.eswa.2022.117508.

[29] Q. Feng et al., "EViT: Privacy-Preserving Image Retrieval via Encrypted Vision Transformer in Cloud Computing," vol. 1, no. 1, pp. 1–26, 2022, [Online]. Available: http://arxiv.org/abs/2208.14657

[30] F. Long, H. Zhang, and D. D. Feng, "Fundamentals of content-based image retrieval," Multimed. Inf. Retr. Manag. Technol. Fundam. Appl., pp. 1–26, 2003.

[31] Y. Rui, T. S. Huang, and S. Mehrotra, "Content-based image retrieval with relevance feedback in MARS," in Proceedings of international conference on image processing, 1997, vol. 2, pp. 815–818.

[32] C. Carson, M. Thomas, S. Belongie, J. M. Hellerstein, and J. Malik, "Blobworld: A system for region-based image indexing and retrieval," in Visual Information and Information Systems: Third International Conference, VISUAL'99 Amsterdam, The Netherlands, June 2–4, 1999 Proceedings 3, 1999, pp. 509–517.

[33] W.-Y. Ma and B. S. Manjunath, "Netra: A toolbox for navigating large image databases," Multimed. Syst., vol. 7, pp. 184–198, 1999.