Privacy-Preserving Content-Based Retrieval in Cloud Image Repositories

Ashwini Prakash Nikam

ME Students, Department of Information Technology

Sinhgad College of Engineering, Pune

Mrs. Bharati P. Vasgi

Professor, Department of Information Technology

Sinhgad College of Engineering, Pune.

Abstract **- Now days, Cloud computing it is been playing a crucial role in terms of data storing and reducing the overall cost to entrepreneurs. Requirement of storage have increased in recent years for visual data, following the appearance of many interactive multimedia services and applications for mobile devices in personal and business scenarios. This was a key a determining factor for the adoption of cloud-based data outsourcing solutions. However, even the outsourcing of data storage in the cloud leads to new security challenges that must be carefully addressed. We propose a secure framework for the storage and recovery of the subcontracted privacy protection in large archives of shared images. Our proposal is based on IES-CBIR, a novel Encryption scheme of the image that presents image recovery properties based on content. The framework user to store image in database. The framework also allows to search image in large database. We have built a prototype of the proposed framework, formally analyzed and tested its safety properties, and experimentally assessed its performance and accuracy of recovery. IES-CBIR is probably safe, allowing more efficient operations that the existing proposals.**

Keywords −Encrypted Data Processing; Searchable Encryption; Content-Based Image Retrieval, Storage

I. INTRODUCTION

Content-based image retrieval (CBIR) is also known as image content retrieval and content-based visual information retrieval is the use of artificial vision for the problem of image retrieval of large digital image search database size. Contentmeans features that are used to retrieve the image from database like color,texture and shape. The term "content" in this context may refer to colours, shapes, textures or any other information that may be derived from the image itself. Without the ability to examine the image content, searches should be based on metadata such as titles or keywords. These metadata must be generated by a human being and stored exactly every image in the database. An image retrieval system returns a series of images from a collection of images in the database to meet the demand of users with a similarity rating like the similarity of the image content, the similarity of the border motif, the similarity of the color, etc. The image recovery system provides an effective way to access, explore and recover a series of similar images in real-time applications. As a result of recent advances in digital storage technology, it is now possible to create large and extensive digital image databases. These collections can contain millions of images and terabytes of data. In order for users to take full advantage of these databases, it is necessary to design effective research methods. Before the automatic indexing methods, the image databases were indexed based on the keywords that a human classifier had decided and inserted. Unfortunately, this practice has two serious shortcomings. First of all, because a database becomes bigger and bigger, the work required to index each image becomes less practical. Secondly, two different people, or even the same person on two different days, can index similar images in an inconsistent way. The result of these inefficiencies is a search result that is not optimal for the end user of the system. The fact that a computer performs indexing based on a CBIR scheme tries to solve the human-based indexing deficiencies. Because a computer is able to process images at a much higher rate, without ever getting tired. For example, each CBIR system must be adjusted for its particular use in order to achieve optimal results. A recovery system designed to consult medical X-ray images will probably be a poor system for recovering satellite images of tropical forests in South America. Furthermore, the algorithms currently used cannot consistently extract the abstract features from the images, such as the emotional response, which would be relatively easy to observe for a human being.

Various approaches have been developed to capture the image content information by directly calculating the image characteristics of an image. The characteristics of the image are constructed directly from the typical compressed data sequence based on block or semitone truncation encoding without executing the decoding procedure. These image recovery schemes include two phases, indexing and searching, to retrieve a set of similar images from the database. The indexing phase extracts the image characteristics of all images in the database, which is then stored in the database as a feature vector. In the search phase, the recovery system derives the characteristics of the image of an image sent by a user (as a query image).

II. Related Work

Literature survey is the most important step in any kind of research. We need to evaluate the papers related with our domain. On the basis of study we can predict or generate the drawback and start working with the reference of previous papers.

In this section, we briefly review the related work on Image search and their different techniques.

In this paper [1], a new multimedia retrieval paradigm proposed to innovate large-scale search of heterogeneous multimedia data. It is return results of different media types from heterogeneous data sources.
Advantages: Implement using a query image to retrieve relevant text documents or images from different data sources.
Disadvantages: Time complexity is high because of Heterogeneous Data Sources.

This paper [2] mainly focuses on two typical types of media data, i.e. image and audio. First, it builds multimodal representation via statistical canonical correlation between image and audio feature matrices and define cross-media distance metric for similarity measure; then it proposes optimization strategy by considering relevance feedback, which fuses short-term learning results and long-term accumulated knowledge into the objective function.
Advantages: In this paper, a new cross-media retrieval method based on short-term and long-term relevance feedback is used. and they worked in image and audio.
Disadvantages: Not worked on text

The former aims [3] to create a latent subspace with the ability in comparing information from the original incomparable views (i.e., textual and visual views), while the latter explores the largely available and freely accessible click-through data (i.e., "crowdsourced" human intelligence) for understanding query.
Advantages: This paper worked on 1) the surrounding texts are often noisy or too few to accurately describe the image content, and 2) The human annotations are resourcefully expensive and thus cannot be scaled up.
Disadvantages This paper consider color feature only.

In this paper [4], addresses problems of learning hash functions in the context of multimodal data for cross-view similarity search. In this paper a novel hashing method, which is referred to Collective Matrix Factorization Hashing (CMFH) is used.
Advantages: 1. CMFH learns unified hash codes by collective matrix factorization with latent factor model from different modalities of one instance, which can not only support cross-view search but also increases the search accuracy by merging multiple view information sources.
Disadvantages: Only worked on nearest neighbor search methods

This paper [5] addresses the problem of learning similarity-preserving binary codes for efficient similarity search in large-scale image collections. This problem is formulated in terms of finding a rotation of zero-centered data so as to minimize the quantization error of mapping this data to the vertices of a zero-centered binary hypercube and propose a simple and efficient alternating minimization algorithm to accomplish this task.
Advantages: 1. This technique can be used with both with unsupervised data embeddings such as PCA and supervised embeddings such as canonical correlation analysis (CCA). 2. This paper worked on large scale image search
Disadvantages: 1.This paper worked on 32 bit binary image search 2.Accuracy is low

In this paper [6], HFL in the context of multimodal data for cross-view similarity search is used. This paper presents a novel multimodal HFL method, called Parametric Local Multimodal Hashing (PLMH), which learns a set of hash functions to locally adapt to the data structure of each modality.
Advantages: 1. This paper implement hashing for efficient large-scale similarity search. 2. PLMH achieves higher empirical query accuracy than global-based ones
Disadvantages: Not explore more efficient optimization algorithms to improve the scalability of PLMH.

This paper [7] addresses the problem of large-scale image search. Three constraints have to be taken into account: search accuracy, efficiency, and memory usage. It first present and

evaluate different ways of aggregating local image descriptors into a vector and show that the Fisher kernel achieves better performance than the reference bag-of-visual words approach for any given vector dimension.

Advantages: 1. This paper addresses the problem of large-scale image search. 2. This paper implement bag-of-visual words implementation.

Disadvantages: Required Expensive hardware.

In DCDH [8], the coupled dictionary for each modality is learned with side information (e.g., categories). As a result, the coupled dictionaries not only preserve the intra-similarity and inter-correlation among multi-modal data, but also contain dictionary atoms that are semantically discriminative (i.e., the data from the same category is reconstructed by the similar dictionary atoms).

Advantages: 1.This paper underlying semantic information of the multi-modal data 2. The coupled dictionaries not only preserve the intra-similarity and inter-correlation among multi-modal data, but also contain dictionary atoms that are semantically discriminative

Disadvantages: Coupled dictionary accuracy is low.

This approach [9] leverages datasets of images and their sentence descriptions to learn about the inter-modal correspondences between language and visual data. Our alignment model is based on a novel combination of Convolution Neural Networks over image regions, bidirectional Recurrent Neural Networks over sentences, and a structured objective that aligns the two modalities through a multimodal embedding.

Advantages: They present a model that generates natural language descriptions of images and their regions.

Disadvantages: Accuracy is low.

In this paper [10], a novel Latent Semantic Sparse Hashing is used to perform cross-modal similarity search by employing Sparse Coding and Matrix Factorization. In particular, LSSH uses Sparse Coding to capture the salient structures of images, and Matrix Factorization to learn the latent concepts from text

Advantages: This paper can efficiently worked on cross-modal retrieval with massive data.

Disadvantages: They check only similarity search that's why accuracy is low.

III. PROPOSED METHODOLOGY:-

IES-CBIR propose a secure framework for the storage and recovery of the subcontracted privacy protection in large archives of shared images. Our proposal is based on CBIR, a novel Encryption scheme of the image that presents image recovery properties based on content. The framework allows both encrypted storage and search using content-based image retrieval queries while preserving privacy against honest but curious cloud administrators. We have built a prototype of the proposed framework, formally analysed and tested its safety properties, and experimentally assessed its performance and accuracy of recovery. Our results show that IES-CBIR is probably safe, allowing more efficient operations that the existing proposals, both in terms of complexity of time and space, and opens the way to new scenarios of practical application.

Cloud and user are the two importantant entities in this model. Images are stored in the database and database is stored on cloud. For preserving security, images are stored in the cloud in encrypted format. Images are encrypted by using repository key(rkR). Repository key is generated by performing permutation operation. Permutation operation takes pixel's color value as an input and generates repository key. Repository key is used for encryption. Repository key is also used for decrypting image.

Whenever user has to perform search operation, user has to upload query image(Q). Query image is encrypted by using repository key. Global color algorithm extracts the features of encrypted query image. Features of encrypted query image are mapped with features of encrypted images which are already stored on the cloud. If match is found, then that relevant image is extracted from database and display to the end user.

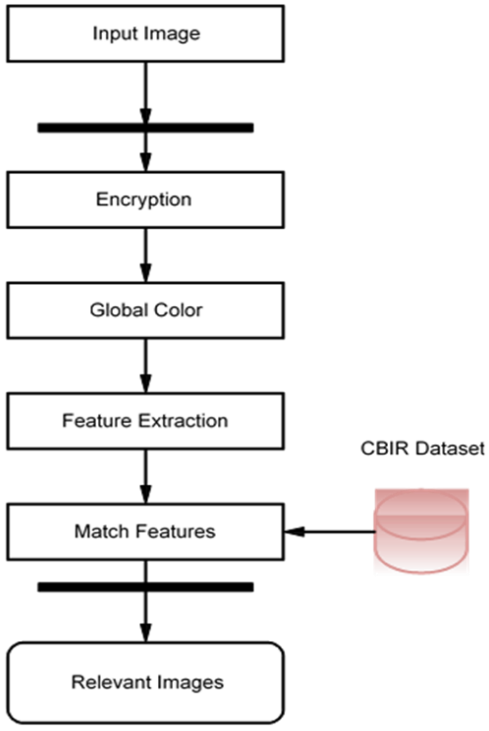


Fig 1. System Architecture

Algorithms:

1. AES Encryption Algorithm

AES (advanced encryption standard).It is symmetric algorithm. AES algorithm is used to perform encryption and decryption. It used to convert plain text into cipher text .The need for coming with this algorithm is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider as weak. AES was to be used128-bit block with128-bit keys.

Rijendeal was founder. In this drop we are using it to encrypt the data owner file. AES algorithm takes query image(Q) and repository key(rkR) as an input and generates ciphertext as an output. Repository key is used for encryption. Repository key is also used for decryption.

Input:

128_bit /192 bit/256-bit input

Secret key (128_bit) +plain text (128_bit).

Process:

10/12/14-rounds for-128_bit /192 bit/256-bit input

Output:

Cipher text (128 bit)

2. Global Color Algorithms

Different images in database may share similar information like color, shape and texture at different regions in image. This information plays important role during image matching process. Global color algorithm is used to extract the features of images. Features of image are color, texture, shape etc.

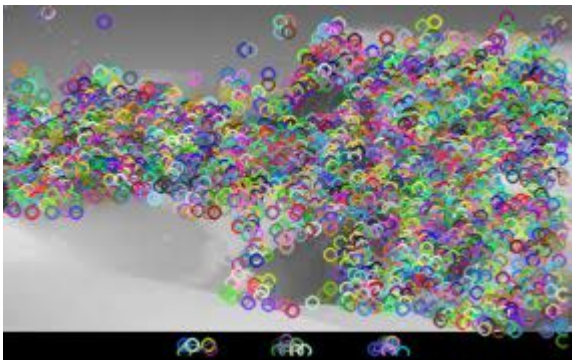
Steps:

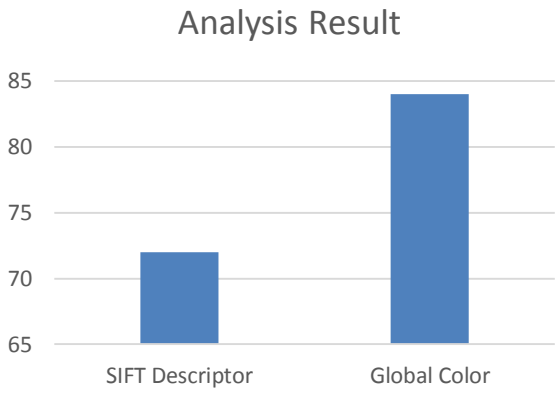
1. The opration to search relevant image in a database takes query image(Q),repository key(rkR) as an input.
2. AES algorithm generates ciphertext as an output.
3. Ciphertext is sent to cloud server.
4. Global color algorithm extract the features of encrypted query image
5. Features of encrypted query image is mapped with features of encrypted images in the CBIR dataset.
6. The cloud starts by extracting CQ's feature-vector.
7. Finally, the cloud sorts this set by descending score and returns the results to user.

IV.RESULT: -

Input:

Output:





Comparison table

Algorithm	IES-CBIR	SIFT
Accuracy Percentage	84 to 87%	72%

Conclusion

IES-CBIR is a new framework for the external storage of privacy protection, research and recovery of large-scale dynamic image archives, where the reduction of the general expenses of the customer is central appearance. At the base of our framework there is a new cryptography scheme, specifically designed for images, called content based image retrieval. The key to its design is the observation that in the images, color information can be separated from the plot information, allowing the use of different cryptographic techniques with different properties for each and allowing to preserve privacy Image recovery based on the content that will be created from unreliable third-party cloud servers. We formally analyze the safety of our proposals and further experiments the evaluation of the implemented prototypes revealed that our approach reaches an interesting exchange between precision and I remember in the CBIR, while exhibiting high performances and scalability compared to alternative solutions.

REFERENCES

[1] Y. Gong, S. Lazebnik, A. Gordo, and F. Perronnin, "Iterative quantization: A procrustean approach to learning binary codes for large-scale image retrieval," IEEE Trans. Pattern Anal. Mach. Intel., vol. 35, no. 12, pp. 2916–2929, Dec. 2013.

[2] Y. Pan, T. Yao, T. Mei, H. Li, C.-W. Ngo, and Y. Rui, "Clickthrough-based cross-view learning for image search," in Proc. 37th Int.ACMSIGIR Conf. Res. Develop. Inf. Retrieval, 2014, pp. 717–726.

[3] D. Zhai, H. Chang, Y. Zhen, X. Liu, X. Chen, and W. Gao, "Parametric local multimodal hashing for cross-view similarity search," in Proc. 23rd Int. Joint Conf. Artif. Intel., 2013, pp. 2754–2760.

[4] G. Ding, Y. Guo, and J. Zhou, "Collective matrix factorization hashing for multimodal data," in Proc. IEEE Conf. Comput. Vis. Pattern Recog., 2014, pp. 2083–2090.

[5] H. J_egou, F. Perronnin, M. Douze, J. S_anchez, P. P_erez, and C. Schmid, "Aggregating local image descriptors into compact codes," IEEE Trans. Pattern Anal. Mach. Intel., vol. 34, no. 9, pp. 1704–1716, Sep. 2011.

[6] J. Zhou, G. Ding, and Y. Guo, "Latent semantic sparse hashing for cross-modal similarity search," in Proc. 37th Int. ACM SIGIR Conf. Res. Develop. Inf. Retrieval, 2014, pp. 415–424.

[7] Z. Yu, F. Wu, Y. Yang, Q. Tian, J. Luo, and Y. Zhuang, "Discriminative coupled dictionary hashing for fast cross-media retrieval," in Proc. 37th Int. ACM SIGIR Conf. Res. Develop. Inf. Retrieval, 2014, pp. 395–404.

[8] H. Zhang, J. Yuan, X. Gao, and Z. Chen, "Boosting cross-media retrieval via visual-auditory feature analysis and relevance feedback," in Proc. ACM Int. Conf. Multimedia, 2014, pp. 953–956.

[9] A. Karpathy and L. Fei-Fei, "Deep visual-semantic alignments for generating image descriptions," in Proc. IEEE Conf. Compute. Vis. Pattern Recog., Boston, MA, USA, Jun. 2015, pp. 3128–3137.

[10] J. Song, Y. Yang, Y. Yang, Z. Huang, and H. T. Shen, "Inter-media hashing for large-scale retrieval from heterogeneous data sources," in Proc. Int. Conf. Manage. Data, 2013, pp. 785–796.