Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

A National Conference On Spectrum Of Opportunities In Science & Engineering Technology
Volume 5, Special Issue 06, April-2018 (UGC Approved)

SECURE IMAGE SEARCHING FOR RETRIEVING DOCUMENTS

[1]Dipti D. Mehare, [2]Prof. A. V. Deorankar

[1]*P. G. Scholar, Department of Computer Science,*
Government college of Engineering, Amravati, Maharashtra, India

[2]*Associate Professor , Department of Computer Science,*
Government college of Engineering, Amravati, Maharashtra, India

Abstract:- *Encryption is the method, which provides security and privacy to an image. A number of methods have been devised for searching encrypted data. In this paper we describe the implementation methods of searchable image encryption. The main aim of image search is to retrieve the relevant image with respect to user query. We first discuss the homomorphic encryption and feature randomized technique that enable similarity comparison between features in the encrypted domain. The encrypted features with encrypted image can protect image privacy from malicious intruder. We proposed secure k-NN computation to display result of correct image to user, also active re-ranking is used. Few images are labelled by user in active re-ranking.*

Keywords: *k-NN algorithm, homomorphic encryption, Feature randomizes technique, Secure image retrieval.*

I. INTRODUCTION

Now, the commercial Web image search engines, e.g., Microsoft's Live Image Search and Google Image Search are based on query by keywords scenario. That means, user will enter query, one keyword will be extracted from that query and that keyword will provide by user to search data. **E.g. I like rose**. The rose keyword will extracted from this query. Then search engine will processed it and returned corresponding images associated with textual information. Here we use the image as the input and get the relevant document as the output. For some web pages the encryption is not needed but in certain organizations the encrypted image is needed because unauthorised user can hack the image. Therefore we use homomorphic encryption, this encryption method only encrypt the image. But in homomorphic encryption unauthorized user can not decrypt it because it required security key for decryption. This method is used to strengthen the security mechanism. After this we use feature randomized technique to increase the accuracy of the search. The documents related to the image are indexed by the index randomized technique. So at the next time it cannot need to compare all the documents to retrieve the result because already the indexing is done for the document. Then k-NN (K Nearest Neighbor) algorithm is use to retrieve the relevant document for the given images. It compares all the image in the database by using the features in the image then it retrieve the relevant document for the given image from the large database.

II. Related work

Related work for image searching is fall into number of categories: Exploiting Image content in web search, improve ranking.

Improving Document Search Using Images

In this paper they check the document search using the images. They use the Trec Million Query track bench mark to search the content using the image. It take the feature of the image and search the document related to the image. They compare the accuracy of the text-based search engines (UDMQ and Indri) to the different image based ranking models. We have shown that this yields a 33 percent relative improvement in accuracy over a state-of-the-art text-based retrieval baseline. All this is achieved at the small cost of a few additional hundred bytes of storage for each page.

Exploiting image content in web search

This paper proposes a new framework for Web search, which exploits image contents to help improve the search performance. In this framework, candidate images are retrieved at first by considering their associated text information. Then, images related to the query are identified by analyzing the density of the visual feature space. After that, an image-based rank of the Web pages is generated, which is combined with the traditional keyword-based search result to produce the final search result. It Improve the search performance. Lack of a mechanism to adaptively trade off the contributions of keyword-based and image-based ranks. But current process for analyzing the images is not fast enough.

Improve Ranking by Using Image Information

In determining the ranking of Web pages against a given query, most (if not all) modern Web search engines consider two kinds of factors: text information (including title, URL, body text, anchor text, etc) and static ranking. Although images have been widely used to help represent Web pages and carry valuable information, little work has been done to take advantage of them in computing the relevance score of a Web page given a query. We propose, in this paper, a framework to contain image information in ranking functions. But the online computation cost is too high.

III. PROPOSED SYSTEM

The main aim of searching of the image is the retrieving of relevant image with respect to query entered by user from large image database. So identification of the accurate image is the most challenging task. In this paper, we propose two categories of secure retrieval schemes, namely, homomorphic encryption based techniques and feature/index randomization-based techniques, for confidentiality-preserving image search. First we discuss feature extraction schemes that enable similarity comparison between features in the encrypted domain. The encrypted features can protect image content privacy against untrustworthy service providers and malicious intruders. The ability to generate encrypted indexes on the user side provides an alternative for secure retrieval with reduced communication overhead. We proposed secure k-NN computation that can determine which of using to display result of correct images to the user. In k-NN computation user intention is captured and used for re-ranking the images. Few images are labelled by user in active re-ranking.

K-NN Algorithm:

We presented a k-NN algorithm for improving the classification of large collection of documents. We extract the content and then search the index for the K-NN classifications.

KNN can be run in these steps:

1. Store the output values of the M nearest neighbors to query scenario q in vector $r=\{r^1,...r^M\}$ by repeating the following loop M times:

a. Go to the next scenario s^i in the data set, where is the current iteration within the domain {1,....,P}

b. If q is not set or $q<d(q,s^i)$:$q<-d(q,s^i)$, $t<-o^i$

c. Loop until we reach the end of the data set (i.e.i=P)

d. Store q into vector c and t into vector r

2. Calculate the arithmetic mean output across r as follows:

$$\bar{r}=\frac{1}{M}\sum_{i=1}^{M} r_i$$

3. Return $\bar{r}$ as the output value for the query scenario q.

Homomorphic Encryption:

A homomorphic encryption scheme is a crypto system that allows computations to be performed on data without decrypting it.

Additive Homomorphic Encryption:

A Homomorphic encryption is additive,
if: Enc $(x \oplus y)$ = Enc(x) $\otimes$ Enc(y)

$$\text{Enc}\left(\sum_{i=1}^{1} mi\right) = \prod_{i=1}^{1} \text{Enc}(mi)$$

Multiplicative Homomorphic Encryption:

A Homomorphic encryption is multiplicative, if:
Enc $(x \otimes y)$ = Enc(x) $\otimes$ Enc(y)

$$\text{Enc}\left(\prod_{i=1}^{1} mi\right) = \prod_{i=1}^{1} \text{Enc}(mi)$$

Feature/Indexed Randomized Technique:

This technique is used to find out the highest level of accuracy of matching content with optimal solution. Feature selection is used to identifying a content of the most relevant features in the context of images. We then choose a random neighbor of dataset and compute its accuracy.

III. SYSTEM IMPLEMENTATION

User Interface: This Module provides functionality to register viewers in order to get access to personalized content that the site using.
Data Pre-processing: This module first analyze the query and then pre-processing of the process takes place.
Query Analysis: This method finds out the meaning of the input data images. The semantic dataset is used, and it is compares with the input query, and results in the semantic data for the input data images.
Retrieving Result: It first extracts the web documents, and compares with the semantic relations. It uses the visual features for comparison and find out the relations between the web documents and the user query input data images.

IV. CONCLUSIONS

In this paper, we proposed secure image searching scheme for retrieving documents from cloud. We first discuss the homomorphic encryption and feature randomized technique that enable similarity comparison between features in the encrypted domain. Also we proposed secure k-NN computation to display result of correct image to user, also active re-ranking is used. While in this work we have focused on a re-ranking strategy, we believe that our framework is sufficiently efficient to support in the near future the application of a single joint search model over text and images in the Web collection.

V. REFERENCES

[1]. Abinaya S, Dr. R. Kalpana**," Secure and Dynamic Image Search for Retrieving Document"** **International Journal of Computer Science and Mobile Computing** Vol. 5, Issue. 3, March 2016, pg.157 – 162.

[2]. M.Aruna, J. Nulyn Punitha**," SECURE FILE KEY SHARING OVER SINGLE IMAGE ON CLOUD COMPUTING", IJCSMC, Vol. 5, Issue. 3, March 2016, pg.587 – 593.**

[3]. Ahmad Akmal Aminuddin Mohd Kamal, Keiichi Iwamura† and Hyunho Kang," Searchable Encryption of Image based on Secret Sharing Scheme" ,Proceedings of APSIPA Annual Summit and Conference 2017.

[4]. Mustafa A Al Sibahee, Songfeng Lu, Zaid Ameen Abduljabbar, Ayad Ibrahim, Zaid Alaa Hussien, Keyan Abdul-Aziz Mutlaq and Mohammed Abdulridha Hussain," Efficient encrypted image retrieval in IoT-cloud with multi-user Authentication", International Journal of Distributed Sensor Networks 2018, Vol. 14(2).

[5]. Shengshan Hu, Qian Wang, Member, IEEE, Jingjun Wang, Zhan Qin, and Kui Ren, Fellow, IEEE," Securing SIFT: Privacy-preserving Outsourcing Computation of Feature Extractions over Encrypted Image Data", Citation information: DOI 10.1109/TIP.2016.2568460, IEEE Transactions on Image Processing.