Research Paper
Volume : 5 | Issue : 8 | Special Issue August-2016 • ISSN No 2277 - 8179

Privacy Preserving Image Hashing for Content Based Information Retrieval

Engineering

KEYWORDS: Index Terms—image hashing, Multimedia database, indexing, data privacy, content based retrieval

S.Kavitha — Asso.Professor, Computer Science and Engineering Vedavyasa Institute of Technology Karad,Malappuram

Aswathi.N.V — PG Scholar, Computer Science and Engineering Vedavyasa Institute of Technology Calicut, Kerala

ABSTRACT

This paper propose a privacy preserving for content based image retrieval. For increasing privacy the proposed method relies on a robust hashing method. Two different robust hash algorithms are used.one is based on random projection and second one is based on discrete wavelet transform. After applying one of this algorithm on image client send a certain hash value to the server. The proposed method used two partial query for increasing the privacy of client and server. Due to the reduced information server can't realize client's interest. The server send possible candidate list into the client. The client select the best match in that list. The database undergo piece wise inverted indexing.

I. INTRODUCTION

Information retrieval is the obtaining information from a collection of stored data. Multimedia information differs from conventional text or numerical data because it require a large amount of memory and space for processing operations.

In recent years different techniques was used for information retrieval. But these techniques did not protect privacy of both client and server. Search engine, face book, flip kart's are the examples of CBIR. In search engine user send input image to the server. server send back similar images as the output to the client. System check the similar images of input image and produce the higher similarity output. Searching is based on content of object is called CBIR.

Multimedia object like image, video, song as input and system provide user required result. The content of the input query and database are sometimes privacy sensitive. CBIR is multi-party system, in which there are minimum 2 parties, user and information retrieval system. Both the parties consider unknown and untrusted to each other [12]. A privacy issue arises when an untrusted party wants to access the private information of another party, so the main challenge is that the search has to be performed without revealing the original query or database, This motivates the need for privacy preserving content based information system [11].

Recently, the one way privacy model for CBIR was developed [4]. One way privacy assume that the database is public and user want to keep the information safely. In public content based information retrieval system one has to deal with the authentication, sometimes database owner doesn't have trust on to the database servers, server may contain private information which is requested by unknown client in such case privacy preserving concept comes into focus. Some clarification are depends on the idea of signal processing in encrypted domain, many time called as (Speed). They normally rely on intense cryptographic calculation, like multiparity computation and homomorphic encryption [13].

Rest of the work is organized as follow. Section II is a brief literature review. Section III describes proposed framework. Section IV is a Experimental analysis. That is here cpmparing existing and proposed framework. Section V conclude the work.

II. RELATED WORK

There are number of application under privacy preserving data processing. The search is based on content based information retrieval M.S Lew and R. jain [1] describe the multimedia content based information retrieval, This survey review the recent articles on content based information retrieval. Some application of CBIR is related to biometric data [14], this is an article presents a tutorial overview of the application of techniques of secure two-party computation (also known as secure function evaluation) to biometric identification .Efficient privacy preserving face recognition [2] describe privacy preserving techniques inth face detection method using Eigenfaces recognition algorithm and a combination of known cryptographic techniques, in particular Homomorphic Encryption and Garbled Circuits.

The encryption of multimedia content is sequential and independent operation. Desirable to carry out signal processing operations directly on encrypted signal [3], The general cryptographic tools that allow to process encrypted signals are homomorphic cryptosystems since they allow performing linear computations on the encrypted data and take an application-oriented view on secure signal processing. Advantage of this sytem is the cryptographic encryption and disadvantage is they are expensive to use in practice, especially for low-profile devices and large-scale systems.

In the recent survey locality sensitive hashing (LSH) has been proposed to solve Approximate Nearest Neighbor (ANN) problem [4]. To achieve good performance LSH require large memory space this is the drawback. FBLSH does not use hash function which is generated by concatenating several functions chosen randomly from LSH family ,Compared with E2LSH, FBLSH achieving better search quality.

Fouad Khelifi, and Jianmin Jiang propose a new robust and secure perceptual image hashing technique based on virtual watermark detection [5]. Digital water marking is an hiding techniques, that is copy right protection in multimedia.

P.R Sabbu, Umadevi Ganugulay, Srinathan Kannan_ and Bruhadeshwar Bezawada introduce a An Oblivious Image Retrieval Protocol [6] are capable of ensuring the privacy of both the user and the server privacy at the same time. The goal of oblivious retrieval protocol is to achieve the user and database privacy.

J. Shashank, P. Kowshik, K. Srinathan, and C. V. Jawahar propose a private content based image retrieval [7] deals with retrieving similar images from an image database without revealing the content of the query image – not even to the database server and propose algorithm for PCBIR, when the database is indexed using hierarchical index structure or hash based indexing scheme. Due to high computational complexity the method is not applicable in small database.

G. Fanti, M. Finiasz, and K. Ramchandran, propose an One-way private media search on public databases: The role of signal processing which describe the one way privacy [8].

C.-Y. Hsu, C.-S. Lu, and S.-C. Pei propose an Image feature extraction in encrypted domain with privacy-preserving SIFT [9]. SIFT is a key

point detector.

S. Rane and P. T. Boufounos propose a Privacy-preserving nearest neighbor methods [10]. Nearest neighbor problem is described.

Li Weng, Member, IEEE, Laurent Amsaleg, April Morton, and Stéphane Marchand- Maillet, propose A Privacy-Preserving Framework for Large-Scale Content-Based Information Retrieval [11]. Here proposed for PCBIR with facility to adjust the level of privacy of both client and server. Figure 1 user send a partial query to server. Server produce a candidate list that send back to the client. Client perform a search within the candidate. To summarizing the existing framework following having shortcomings [11], Non scalability to large database, Expensive implementation, Between server and client have unbalanced load.

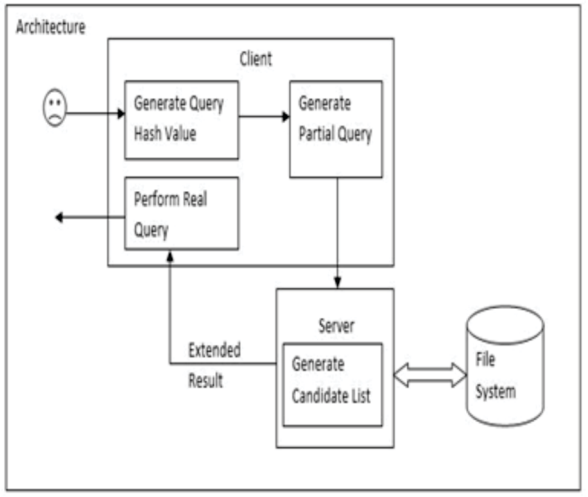


Figure 1. Existing approach in PCBIR

III. THE PROPOSED FRAMEWORK

A new PCBIR structure is developed. It is used for large scale database, provide different levels of security and non-expensive implementation. Robust hashing techniques is applied on images and produce the two partial query. Two different construction of robust hash algorithms are used. One is based on Random projection and other is discrete wave length transform. The database is based on Pease wise inverted indexing [11].

Li Weng, Member, IEEE, Laurent Amsaleg, April Morton, and Stéphane Marchand- Maillet, propose A Privacy-Preserving Framework for Large-Scale Content-Based Information Retrieval [11], this framework protect both client and server privacy. This framework work as

1) The client creates a partial query, and sends it to the server

2) The server generates an extended query list based on the partial query

3) The server performs a search with the extended query list, and sends back all matching items

4) The client performs a search within the received set of matching results using the original query

In the proposed framework using a two partial query instead one. In figure 2, client send two partial query to server. Server produce a candidate list. Candidate list contain set of matching item. That list send back to the client. Client perform a search within the candidate list based on the original query.

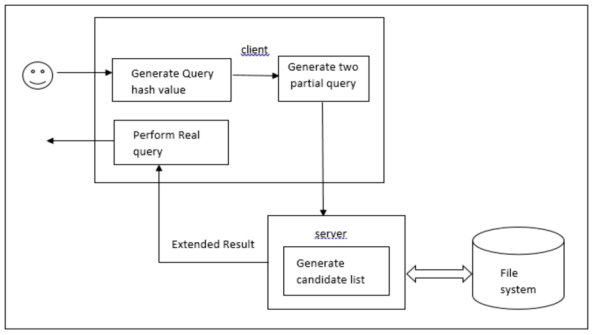


Figure 2. Proposed Framework

3.1 Robust hashing Algorithm

First algorithm is based on random projection. Generate GIST features [11] of image. Perform principle component analysis (PCA). In PCA convert possibly correlated variables in to set of uncorrelated variables. This features can be converted into hash value. Then convert this hash value into two partial query.

Second algorithm is Discrete Wavelet Transform (DWT) then processed by the discrete cosine transform (DCT) then extracted to form a hash value. Then generate two partial query from the hash value. These both algorithm gives better retrieval performance [11].

IV. EXPERIMENTAL RESULT

Figure 3 and Figure 4 shows in the proposed framework using two partial query and exiting framework using one partial query. For increasing the privacy using two partial query instead of one. First Take 10 dataset and select 5 images then count the total recognized images of each one. Second take 15 dataset and select 10 images then count the total recognized images of each one, So on.

Compared with previous techniques this techniques gives more privacy. That is using two partial query the privacy of client protected, also server produce candidate list that contain more images compared with exiting system so privacy of server protected.



Figure 3. Using two partial query

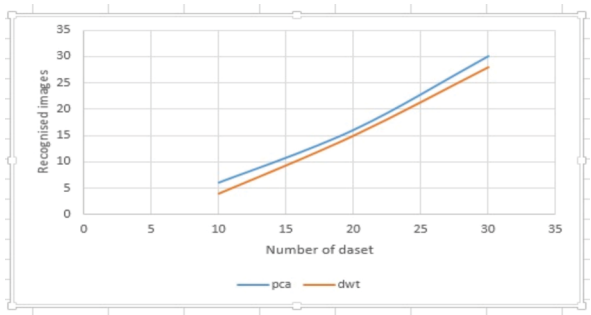


Figure 4. Using one partial query

V. CONCLUSION

In this work, propose a privacy preserving framework image hashing for content based information retrieval. This proposed framework is based on robust hashing and piece-wise inverted indexing. Two different construction of robust hash algorithms are one is based on Random projection and other is based on DWT. Both algorithm show better retrieval performance.

Proposed system requires both the server and the client to implement the same architecture, the same feature extraction, hash algorithms, indexing, etc. Although random projection and DWT can be applied to any feature, it is also seen in the existing systems [11]. The existing framework containing partial query generated from original content by applying robust hashing, In the proposed framework generate two partial query instead of one for increasing the privacy of both client and server

V. REFERENCES

[1.] M. S. Lew, N. Sebe, C. Djeraba, and R. Jain, "Content-based multimedia information retrieval: State of the art and challenges," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 2, no. 1, pp. 1–19, Feb. 2006.

[2.] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, "Privacy-preserving face recognition," in *Proc. 9th Int. Symp. Privacy Enhancing Technol. (PETS)*, 2009, pp. 235–253.

[3.] Z. Erkin *et al.*, "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing," *EURASIP J. Inf. Secur.*, vol. 2007, p. 20, Dec. 2007.

[4.] Kang Ling, Gangshan Wu "Frequency Based Locality Sensitive Hashing".

[5.] F. Khelifi and J. Jiang, "Perceptual image hashing based on virtual watermark detection," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 981–994, Apr. 2010.

[6.] P. R. Sabbu, U. Ganugula, S. Kannan, and B. Bezawada, "An oblivious image retrieval protocol," in *Proc. IEEE Int. Workshop Adv. Inf. Netw. Appl. (WAINA)*, Mar. 2011, pp. 349–354.

[7.] J. Shashank, P. Kowshik, K. Srinathan, and C. V. Jawahar, "Private content based image retrieval," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2008, pp. 1–8.

[8.] G. Fanti, M. Finiasz, and K. Ramchandran, "One-way private media search on public databases: The role of signal processing," IEEE Signal Process. Mag., vol. 30, no. 2, pp. 53–61, Mar. 2013.

[9.] C.-Y. Hsu, C.-S. Lu, and S.-C. Pei, "Image feature extraction in encrypted domain with privacy-preserving SIFT," *IEEE Trans. Image Process.*, vol. 21, no. 11, pp. 4593–4607, Nov. 2012.

[10.] S. Rane and P. T. Boufounos, "Privacy-preserving nearest neighbor methods: Comparing signals without revealing them," IEEE Signal Process. Mag., vol. 30, no. 2, pp. 18–28, Mar. 2013.

[11.] Li Weng, Member, IEEE, Laurent Amsaleg, April Morton, and Stéphane Marchand-Maillet, "A Privacy-Preserving Framework for Large-Scale Content-Based Information Retrieval ", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 1, January 2015.

[12.] Bhagyashree V. Khapli1, Manjushri A. Mahajan "Survey on Privacy Preservation in Content Based Information Retrieval".

[13.] Sayali P. Shinde,Prof. J. S. Raghatwan "A Survey Paper on Secure Privacy Preserving Structure for Content Based Information Retrieval on Large Scale", International Journal on Recent and Innovation Trends in Computing and Communication Volume: 3 Issue: 10

[14.] J. Bringer, H. Chabanne, and A. Patey, "Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 42–52, Mar. 2013.