ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

A Secure Framework For Content Based Image Retrieval In Cloud Repositories

[1] Kothala Anupama, [2] N. Priya,
[1] M.Tech, Bharath University
[2] Assistant Professor, Bharath University

Abstract: ***Fire in itself is a word that describes loss and hazardous situation. Work house fire is a situation in a populated place that can leave a many shop into a bit of ashes. That is why we needs to be detected at the earliest so that high damage and loss could be prevented. The objective is to detect the fire as fast as possible and its exact localization and early notification to the fire units is vital. The objective of designing this telemetry project is to detect the fire and monitor it online. Number of two sensors are employed that needs to be placed at certain distances so that a look can be kept on the entire area. These fire sensors detect the area and if at times there is a fire, it will send the signal or the information to the microcontroller. The microcontroller also updates the information on the webpage and also sends a notification on the webpage through the Wi-Fi. This information is sent to the internet by the network of IOT.***

I. INTRODUCTION

Nowadays visual data is responsible for one of the largest shares of global Internet traffic in both corporate and personal use scenarios. The amount of images, graphics, and photos being generated and shared everyday, especially through mobile devices, is growing at an ever increasing rate. The storage needs for such large amounts of data in resource-constrained mobile devices has been a driving factor for data outsourcing services such as the ones leveraging Cloud Storage and Computing solutions. Such services (e.g. Instagram and Flickr) have been reported to be among the largest growing internet services. Additionally, the availability of large amounts of images in public and private repositories also leads to the need for content based search and retrieval solutions (CBIR).

Despite the fact that data outsourcing, especially to cloud computing infrastructures, seems a natural solution to support large scale image storage and retrieval systems, it also raises new challenges in terms of data privacy control. This is a consequence of outsourcing data, which usually implies releasing control (and some times even effective ownership) over it. Recent incidents have provided clear evidence that privacy should not be expected to be preserved by cloud providers. Furthermore, malicious or simply careless system administrators working for the providers have full access to data on the hosting cloud machines. Finally, external hackers can exploit software vulnerabilities to gain unauthorized access to servers. The recent incident with the iCloud image storage service and celebrity photo leakage illustrates the danger these threats pose for cloud-based visual data stores.

The conventional approach to address privacy in this context is to encrypt sensitive data before outsourcing it and run all computations on the client side. However this imposes unacceptable client-overhead, as data must continuously be downloaded, decrypted, processed, and securely re-uploaded. Many applications cannot cope with this overhead, particularly online and mobile applications operating over very large datasets such as image repositories with CBIR services. A more viable approach would be to outsource computations and perform operations over the
encrypted data on the server side. Existing proposals in this domain remain largely unpractical, namely those requiring fully homomorphic encryption, which is still computationally too expensive. Nonetheless, partially homomorphic encryption schemes and symmetric key solutions (or property-preserving schemes) supporting specific search patterns are interesting alternatives, yielding more practical results while providing a good tradeoff between security, privacy, and usability. Unfortunately, even these solutions are too computationally complex for wide adoption, particularly regarding the support of privacy-preserving CBIR over large-scale, dynamicallyupdated image repositories. This prohibitive complexity is even further exacerbated if we consider mobile (resource constrained) clients, which are already responsible for more than 30% of internet traffic.

To address these challenges we propose a new secure framework for privacy preserving outsourced storage, search, and retrieval of large-scale, dynamically updated image repositories. We base our proposal on IES-CBIR, a novel Image Encryption Scheme (IES) with Content-Based Image Retrieval (CBIR) properties. Key to the design of IES-CBIR is the

observation that in image processing, distinct feature types can be separated and encrypted with different cryptographic algorithms. As an example, image color and texture data can be separated in such a way that CBIR in the encrypted domain can be performed on one feature type while the other remains fully randomized and protected with semantically-secure cryptography. Following this observation, and considering that texture is usually more relevant than color in object recognition, in IES-CBIR we make the following security-oriented tradeoff: we choose to privilege the protection of image contents, by encrypting texture information with probabilistic (semantically-secure) encryption; then we controllably relax the security on color features, by using deterministic encryption on image color information. This methodology allows privacy preserving CBIR based on color information to be performed directly on the outsourced servers with high security guarantees. Notably, our solution allows outsourcing servers to generate and update an index used to efficiently process and reply to queries, a task that in many state of art solutions must be managed by client devices. As we show further ahead in the paper, our new methodology leads to optimized computation and communication overheads with non-negligible impact on system performance and mobile battery consumption.

In summary, this paper makes the following contributions: (i) We formally define IES-CBIR, a novel Image Encryption Scheme with Content-Based Image Retrieval properties, and propose an efficient construction that achieves its functionality; (ii) We show how to design an out-sourced image storage, search, and retrieval framework by leveraging IES-CBIR to avoid most heavy computations to be performed by the client (i.e. indexing of dynamically added/updated images), hence circumventing performance pitfalls that exist in current state of art proposals, (iii) We formally prove the security of our framework and IES-CBIR; (iv) We experimentally show that when compared with competing alternatives, our framework provides increased scalability, performance (from user's perspective), and lower bandwidth consumption, allowing client applications to be increasingly lightweight and mobile; (v) And finally we show that the retrieval precision and recall of the proposed solution is on par with the current state of art.

The work presented in this paper was first introduced in. Here we extend our exposition significantly by discussing two use cases where IES-CBIR and the proposed framework can be applied with immediate benefits. We further provide a complete formal security evaluation of our proposals and a performance analysis of the search operation of our framework in comparison with relevant previous works. Additionally we provide a statistical security analysis of IES-CBIR and its entropy levels at each step of encryption and the complete description of all framework operations.

II. RELATED WORK

Key aspects of the state of art, by comparing our work with the most relevant approaches from SSE and the PKHE research contexts in terms of information leakage and computational complexity for clients. We also implemented these works and experimentally compare them with a prototype of our framework. The Information Leakage represents the leakage of all system operations (particularly the update, search, and remove operations) as a whole; Local Index Size represents a maximum bound on the possible index size on the client device; and the CBIR Algorithm column represents the CBIR algorithms used in each work: local color histograms, SIFT, and global color histograms. Also in the table, IDI is a deterministic identifier of an image I being stored/updated or used as a query image in a search; put(x) and get(x) represent the complexity of respectively, sending and retrieving data item x to/from the server; FEI is the Feature Extraction of I and fv is the extracted Feature-Vector; vwI are the visual words of I, resulting from its clustering; ES represents encryption with scheme S and CP is the resulting ciphertext when applied to plaintext P; D is the decryption operation; Idx is the index; |vw| is the total number of visual words; |Rep| is the size of the repository; and |CB| is the size of the clustering codebook.

III. EXISTING SYSTEM

Storage requirements for visual data have been increasing in recent years, following the emergence of many highly interactive multimedia services and applications for mobile devices in both personal and corporate scenarios. Existing proposals in this domain remain largely unpractical, namely those requiring fully homomorphism encryption, which is still computationally too expensive. Since mobile clients usually have limited computational and storage resources, they tend to rely on cloud services for storing and processing bulky data such as images. In this scenario, mobile clients (users) want to delegate their private image repositories storage to a cloud provider, while coping with the limitations of their device's storage capability, computational power, and battery life.

- In general, Encryption techniques in image processing lead to change in the size of an encrypted image. So, retrieval cannot be achieved properly.
- User's privacy is affected due to the carelessness of cloud service provider.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

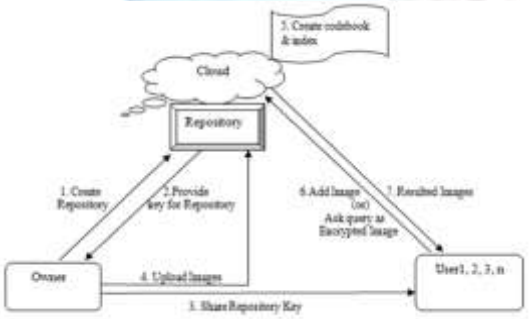
Images are leaked due to the lowest security level in the cloud.

IV. PROPOSED SYSTEM

Our proposal is based on IES-CBIR, a novel Image Encryption Scheme that exhibits Content-Based Image Retrieval properties. The framework enables both encrypted storage and searching using Content-Based Image Retrieval queries. Images are outsourced to repositories that reside in the cloud. Each repository is used by multiples Users, where they can both add their own images and/or search using a query image. Each repository is created by a single user. Upon the creation of a repository, a new repository key is generated by that user and then shared with other trusted users, allowing them to search in the repository and add/update images. In this work, we use the Bag-Of-Visual-Words (BOVW) representation to build a vocabulary tree and an inverted list index for each repository. We choose this approach for indexing as it shows good search performance and scalability properties. In the BOVW model, feature-vectors are hierarchically clustered into a vocabulary tree (also known as codebook), where each node denotes a representative feature-vector in the collection and leaf nodes are selected as the most representative nodes (called visual words).

ARCHITECTURE

The system architecture is a diagram of a system, in which the principle parts of functions are represented by the boxes connected by lines that shows the relationship of the boxes. It also explains the overall process of the system**.**



ARCHITECTURE

IMPLEMENTATION

Implementation is the most crucial stage in achieving a successful system and giving the users confidence that the CBIR technique is effective.

CREATE REPOSITORY & UPLOAD IMAGES:

Repository is storage space of collection of data. Each repository is created by single user. He is the owner of that repository. Then, he generates a key for that repository by using RSA algorithm and shared with the users who are all have an account to access it. Now, Repository can be accessed by multiple users with the permission of an owner. Then, owner upload huge amount of image datasets as zip file into the cloud.

CODEBOOK & INDEX GENERATION:

The admin of cloud has responsibility to create documents based on images which is useful for searching of images by users. So, he extracts zip file and applying CBIR Encryption technique. It encrypts images based on color values and texture features and also shuffling the pixels in column-wise as well as row-wise. Then, he creates codebook, index and image key for those encrypted images. These files are used to improve the searching efficiency of cloud and also manage the time properly while retrieving answer.

ADD IMAGE/QUERY TO CLOUD:

Now, Users can access the cloud to add their own images into the repository. So, if that cloud has 'n' number of users, then repository has chance to increase rapidly. Now, the repository has collection of 'n' number of images in different domains. All the images are stored in encrypted format for security. Then, user has to ask query to cloud. Its take query is in the format of encrypted image using CBIR encryption technique.

CONTENT BASED SEARCHING & RETRIEVAL:

After receiving encrypted image query, the cloud extracts the features of an original image. Now applying content based searching on the codebook and image index by using that extracted features. Obviously, now searching results will be an encrypted image. This resulted answer will send to that corresponding user. Now, user can apply CBIR decryption technique to decrypt the retrieved images. So, the answer will be very fine and delicious due to huge dataset.

CONCLUSION

This project proposes a method to secure the images uploaded to cloud repositories by encrypting using content based image encryption/retrieval algorithm. The coding
are written in java using net beans

IDE 8.0.

V. FUTURE ENHANCEMENT

An interesting future work direction is to investigate the applicability of our methodology - i.e. the separation of information contexts when processing data (color and texture in this contribution) - in other domains beyond image data.

REFERENCES

[1] M. Meeker, "Internet Trends 2015," in Code Conf., 2015.
[2]Global Web Index, "Instagram tops the list of social network growth," http://tinyurl.com/hnwwlzm, 2013.
[3] C. D. Manning, P. Raghavan, and H. Sch ¨ utze, An Introduction to Information Retrieval. Cambridge University Press, 2009, vol. 1.
[4] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in CCSW'09, 2009.
[5] D. Rushe, "Google: don't expect privacy when sending to Gmail," http://tinyurl.com/kjga34x, 2013.