IES-CBIR : A Privacy Preservation of Cloud Image Repository

Anjali V Nair[1], Anju Rachel Oommen[2], Smita C Thomas[3]
[1, 2, 3] Dept of Computer Science & Engineering
[1, 2, 3] Mount Zion College of Engineering Kadammanitta ,Pathanamthitta ,India

Abstract- *With the development of multimedia technology, the rapid increasing usage of large image database becomes possible. This factor leads for the adoption of cloud-based data outsourcing solutions. Data storage to the cloud faced a lot of security challenges especially in the case of privacy. In existing systemIES-CBIR, the colour analysis and texture analysis is used for image retrieval. Thus it is showed that images retrieved using above mention methods may not be semantically related even though they share same colour distribution and texture in some results. This paper explained that how we can perform image segmentation using watershed algorithm instead of Kmeans algorithm .It is very efficient in terms of time and space complexity when compared with existing method.*

Keywords- IES-CBIR;Content-based;Repository

I. INTRODUCTION

The process of segmenting a digital image into multiple segments is known as image segmentation. The objective of segmentation is to simplify and/or change the representation of an image into something that is more meaningful and easier to analyze. Image segmentation is typically used to locate objects and boundaries present in an images. More precisely, image segmentation is the process of assigning a label to every pixel in an image such that pixels with the same label share certain characteristics. The image segmentation is jointly cover the entire image, or a set of contours extracted from the image (see edge detection). Each of the pixels in a region are similar with respect to some characteristic or computed property, such as color, intensity, or texture. Adjacent regions are extensively different with respect to the same characteristic(s). When applied to a stack of medical imaging, the resulting contours after image segmentation can be used to create 3D reconstructions with the help of interpolation algorithms like cubes. We base our suggestion 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 colour in object recognition , in IES-CBIR we make the following security-oriented trade-off: 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 colour features, by using deterministic encryption on image colour information. This method allows privacy-preserving CBIR based on color information to be performed directly on the outsourced servers with high security guarantee. Low-level visual features like color, shape, texture, etc are being used for representing and retrieving images in many Content-Based Image Retrieval systems. Such methods undergo from the problems of high dimensionality leading to more computational time and inefficient indexing and retrieval performance. So, here focus on a low-dimensional shape based indexing technique for achieving efficient and effective retrieval performance.

This paper proposed a new secure framework for the privacy-preserving outsourced storage, search, and retrieval of large-scale, dynamically updated image repositories, where the reduction of client overheads is a central aspect. In the basis of our framework is a novel crypto- graphic scheme, specifically designed for images, named IES-CBIR. Key to its design is the observation that in images, colour information can be separated from texture information, enabling the use of different encryption techniques with different properties for each one, and allowing privacy- preserving Content-Based Image Retrieval to be performed by third-party, untrusted cloud servers. We formally analyzed the security of our proposals, and additional experi mental evaluation of implemented prototypes revealed that our approach achieves an interesting trade-off between precision and recall in CBIR, while exhibiting high performance and scalability when compared with alternative solutions. An interesting future work direction is to investigate the applicability of our methodology – i.e. the separation of in- formation contexts when processing data (colour and texture in this contribution) - in other domains beyond image data.

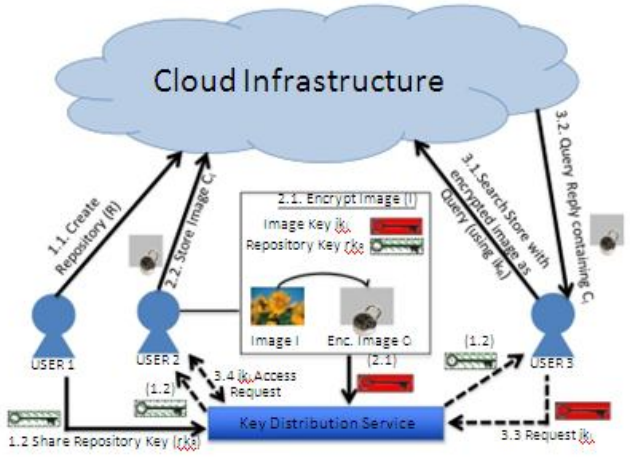


Fig. 1: System model overview of the proposed framework.

II. LITERATURE SURVEY

Several researchers proposed many techniques for explaining the privacy for cloud image storage. Each technique is explained as follows.

Wenjun Lu, Ashwin Swaminathan, Avinash L. Varna [1] has proposed This paper addresses the problem of enabling content-based retrieval over encrypted multimedia databases. Search indexes, along with multimedia documents, are encrypted by the content owner and then stored onto the server. Mutually applying cryptographic techniques, such as order preserving encryption and randomized hash functions, with image processing and information retrieval techniques, secure indexing schemes are designed to provide both privacy protection and rank-ordered search capability. Retrieval results on an encrypted color image database and security analysis of the secure indexing schemes under different attack models show that data confidentiality can be preserved while retaining very good retrieval performance. This work has promising applications in secure multimedia management.

Mohammad Saiful Islam, Mehmet Kuzu, [2] introduce a novel attack that exploits data access pattern leakage to disclose significant amount of sensitive information using a modicum of prior knowledge. Our observed analysis with a real world dataset shows that the future attack is able to disclose sensitive information with a very high accuracy. Additionally, we propose a simple technique to mitigate the risk against the proposed attack at the expense of a slight increment in computational resources and communication cost. Our proposed lessening technique is generic enough to be used in conjunction with any searchable encryption scheme that reveals data access pattern.

Stéphane Marchand-Maillet Viper [3], give an overview of the main tasks involved in designing a platform for the evaluation of content-based image retrieval systems. A number of issues should be addressed from the construction of an image collection to the definition of standard performance measures. The aim here is to introduce the Benchathlon network that has been created with the aim of setting up such a platform. Sub tasks engendered by this context are listed and the organization of our collaboration detailed. While participants are allocated to specific subtasks, everyone may submit a solution to another parallel task.

Alexander Shraer, Christian Cachin, Asaf Cidon [4], This Paper gives an idea about Venus, a service for securing user interaction with un trusted cloud storage. Specifically, Venus guarantees integrity and consistency for applications accessing a key-based object store service, without requiring trusted components or changes to the storage provider. It then verifies operation consistency and notifies the application. Whenever either integrity or consistency is violated, Venus alerts the application. We implemented Venus and evaluated it with Amazon S3 commodity storage service. The evaluation shows that it adds no noticeable overhead to storage operations.

III. EXISTING SYSTEM

The existing framework for privacy-preserving outsourced storage, search, and retrieval of images in large-scale, dynamically updated repositories. The framework composed of two components one is image encryption system that is executed on the client device and a searching, indexing and storage executed in the outsourcing server. This framework used a new encryption scheme named IES-CBIR, it is an image encryption scheme and support content based image retrieval based on colour features. a repository is a collection of images which is stored in the infrastructure of a cloud provider; the cloud server, or just cloud, is the outsourcing infrastructure that acts as a server both for storage and computation over images; users are the clients of our system, possibly using lightweight mobile devices, where each user accesses one or more repositories to search, add, and update images at any time; repository keys are secret cryptographic keys that are used to search, add, and update images in the repositories using repository key. image keys are secret keys used for encrypting and decrypting images in the repositories, in conjunction with the respective repository keys.

This architecture consist of two Images are outsourced to repositories that reside in the cloud. Each repository is used by multiples Users, where they can both add specific keys per-image should be seen as an option in our framework, i.e. if the users of a repository prefer to avoid further key management overhead and are willing to sacrifice fine-grained access control, they can use the same image key for all images When the cloud receives an encrypted image for storage it extracts its relevant features (in our framework, we use global colour features and indexes the image based on these features. The same action is performed for a query image, which features extracted and matched with the repository's filter being encrypted by a user with a repository key, is then processed by the cloud and has its filtered index. The reply to a query will contain k (a tuneable system parameter) number of encrypted images and respective metadata, which include each image's id and the id of the user that owns each of the images. To fully decrypt and access the contents of an image, besides the repository key, the querying user will further require the image key for that specific image in a repository. It should be noted that all key sharing interactions can be done by resorting to a key distribution service, implemented either in a centralized way (using protocols such as Kerberos or in a distributed fashion (through asynchronous communications or protocols such as Diffie-Hellman . User authorization and revocation can also be easily achieved, for instance, through the sharing (and refreshment when user revocations are issued) of repository-specific tokens between trusted users, and its request in the framework operations. Nonetheless, we find these discussions to be orthogonal to the main focus of this contribution, as the mechanisms involved can be easily integrated into our framework. Their own images and/or search using a query image. Users can also request access to stored images from their creators/owners. Our objective is to ensure the privacy of users, hence all data sent to the cloud is encrypted.

Each repository is created by a single user ,a repository key is generated that user and then shared with other trusted users, allowing them to search on the repository and add/update images. To add/update images (but not search), a user further needs an image key generated for that image. Image keys are kept secret by their users, meaning that even users capable of searching in a repository (i.e. with access to the repository key) will need to ask the owners of specific images for access to them. Note that using On the cloud's side, the received encrypted images are processed and indexed for CBIR before being persistently stored. IES-CBIR enables these operations (for colour features) to be performed over their cipher texts, using algorithms that operate on non-encrypted images and without requiring any modifications. Encrypted image processing has two main steps: feature extraction and feature indexing.

Feature extraction consists in processing an image and extracting a reduced set of feature vectors that describe it. In this work we focus on color features in the HSV color model and their representation as color histograms. For each encrypted image and each HSV color channel, the cloud server builds a color histogram by counting the number of pixels in each intensity level. In our model, this yields 3 color histograms with entries in range [0,100], which are the admissible values for each HSV channel (i.e. each histogram has 101 entries).

IV. PROPOSED SYSTEM

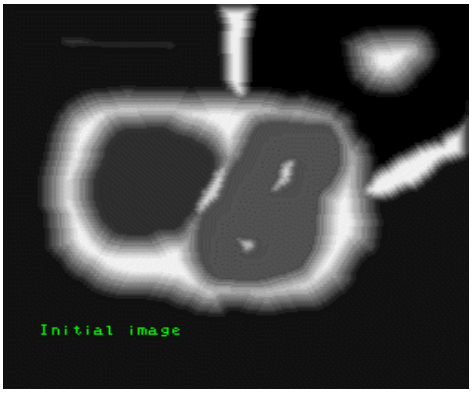
In our proposed system we use watershed algorithm for image segmentation instead of K-means clustering in existing one.The main disadvantages of Kmeans clustering is that it requires the number of clusters to be specified in advance.Inorder to over come this here we use watershed algorithm instead of kmeans clustering.

Watershed is a transformation defined on a grayscale image. The name refers symbolically to a geological watershed, or drainage divide, which separates adjacent drainage basins. The watershed transformation treats the image it operates upon like a topographic map, with the brightness of each point representing its height, and finds the lines that run along the tops of ridges.There are different technical definitions of a watershed. In graphs, watershed lines may be defined on the nodes, on the edges, or hybrid lines on both nodes and edges. This algorithm may also be clear in the constant domain.. Watershed algorithm is used in image processing primarily for segmentation purposes.

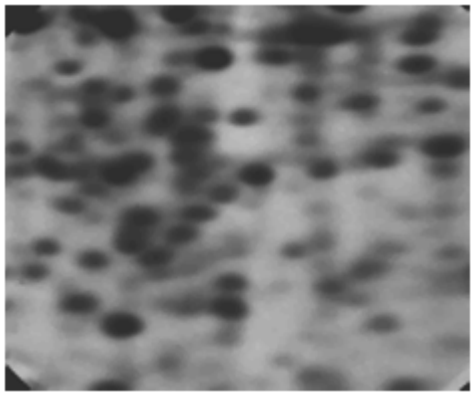
- Step 1: Use the Gradient Magnitude as the Segmentation Function. ...
- Step 2: Mark the Foreground Objects. ...
- Step 3: Compute Background Markers. ...
- Step 4: Compute the Watershed Transform of the Segmentation Function. ...
- Step 5: Visualize the Result.

WATERSHED TRANSFORMMATION

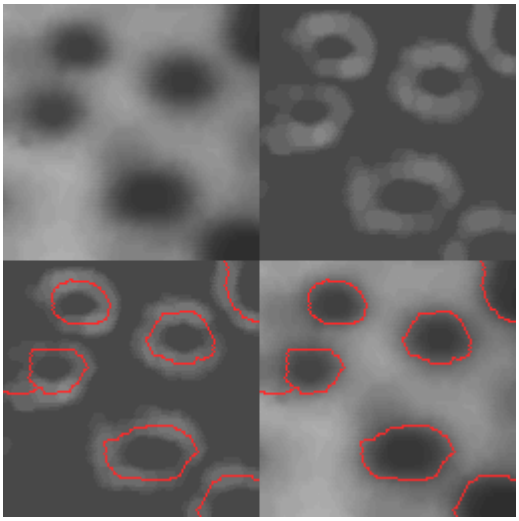
Any greytone image can be on sidered as topographic surface.



If we have to flood this surface from its minima and also prevent the merging of the waters coming from different sources, we partition the image into two different sets: the catchment basins and the watershed lines.



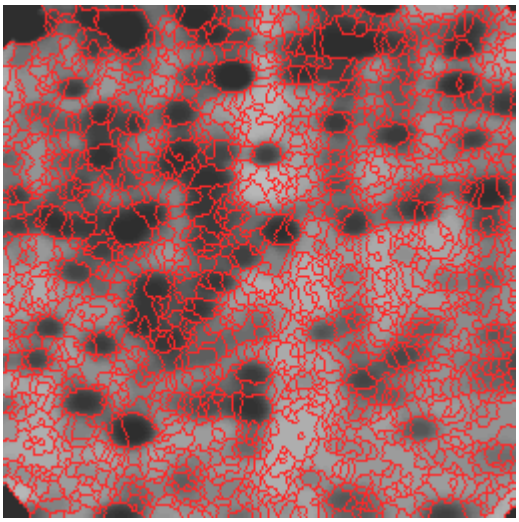
If we aply this transformation to the image gradient, the catchment basins should theoretically correspond to the homogeneous grey level regions of this image.



There are several steps included From top to bottom and from right to left of an image:

- Original image.
- Gradient image.
- Watershed of the gradient image.
- Final contours.

In pactice, this transform produces an important over-segmentation due to noise or local irregularities in the gradient image.



V. CONCLUSION

In this we introduced watershed algoritham for image segmentation.a novel Texture Gradient based Watershed Segmentation technique is developed. The Watershed Transform is a well established tool for the segmentation of images. Though, it is often not effective for textured image regions that are perceptually homogeneous.In order to properly segment such regions the concept of the Texture

Gradient is introduced and is implemented using a Non Decimated Wavelet Packet Transform. A marker location algorithm is subsequently used to locate significant homogeneous textured or non textured regions. A Watershed Transform is then used to correctly segment the known regions. The experimental results demonstrate the superiority of this technique over k-means clustering.

VI. ACKNOWLEDGMENT

We would like to thank, first and foremost, Almighty God, without his support this work would not have been possible. We would also like to thank all the faculty members of Mount Zion college of engineering, for their immense support.

REFERENCES

[1] W. Lu, A. Swaminathan, A. L. Varna, and M. Wu, "Enabling Search over Encrypted Multimedia Databases," in IS&T/SPIE Electron.Imaging, Feb. 2009, pp. 725 418–725 418–11.

[2] M. S. Islam, M. Kuzu, and M. Kantarcioglu, "Access pattern disclosure on searchable encryption: Ramification, attack and mitigation,"
in NDSS, 2012.

[3] A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y. Michalevsky, and D. Shaket, "Venus: Verification for untrusted cloud storage," in CCSW'10.
ACM, 2010, pp. 19–30.

[4] . M¨uller, W. M¨uller, D. M. Squire, S. Marchand-Maillet, and T. Pun, "Performance evaluation in content-based image retrieval: overview"