International Journal of Research in Advent Technology (IJRAT) Special Issue
E-ISSN: 2321-9637
National Conference "MOMENTUM-17", 14th & 15th February 2017
Available online at www.ijrat.org

Image Scaling and Cropping Scheme using Two Dimensional Cryptography

Mrs. Jadhav Rohini [1], Prof.S.A.Kahate [2]
Computer Dept[1],Asst. Prof[1], SPCOE,Otur, Pune(India),Computer Dept[2],Prof.[2], SPCOE,Otur, Pune(India)
rohinijadhav333@gmail.com[1],sandip.kahate@gmail.com[2]

Abstract-Cloud computing is astunning model for accessing unlimited storage and computational resources. With the evolution of cloud computing, organizations are outsourcing the storage and rendering of volume to cloud servers. Data confidentiality at the third-party cloud provider, however, is one of the mainchallenges. State-of-the –art technique is used to provide the confidentiality of data in the cloud, but this technique dose not applied on the cloud data center. To address this problem by offering 2DCrypt, redesign paillier cryptosystem-based image scaling and cropping plan for multiple user settings that allow on cloud datacenters to scale and edit an image in the encrypted space. In two Dimensional Cryptography instead of encrypting each pixel individually, tiles if pixel can be encrypt. In multiple user setting, no of user can observe and process the data without sharing any key.2DCrypt is IND-CPA secure and bring out an acceptable overhead.

Index Terms-Cloud Data-Centre, Cryptosystem, Encryption, Scaling, Cropping, Outsourcing Image.

1. INTRODUCTION

The demand for outsourcing data storage and management has increased dramatically in the last decade. The foremost reason is that for nearly all organizations, data growth is inevitable. Data is the most important part of business operations and applications, driving the critical activities that help the organizations improve customer satisfaction and accelerate business growth. Large amount of data are collected or generated every day and put into data storage for future processing and analyzing. The amount of digital images has exploded in present years due to the proliferation of digital imaging devices with increasing resolution. Individuals and organizations are beginning to rely on third party cloud datacenters (e.g., cloud datacenters or data- centers of social network service providers) to store, process, share, and manage images. As theseimagescould be highly secret and could contain sensitive information (e.g., MRI scan of a patient), this trend has led to concerns about image confidentiality and image integrity [1, 2]. Firstly, acompetitor who can access the image stored at a datacenter can obtain potentially sensitive information contained in an image, leading to privacy loss. Secondly, acompetitor may modify the image stored at a datacenter to provide misleading information. Therefore, datacenter-based image storage systems must prioritize the need to protect to

theimage picture in thedatacenters. To protect image confidentiality and integrity, one can use secure private image sharing [3] to hidean image from any one of the datacenter by distributing the shares (i.e., the shadow images) acrossmultiple datacenters. Those based on Shamir's secret sharing scheme and multi-secret image sharing schemes, mainly focus on the tradeoff between efficiency and security, and do not easily supportimage operations on the shadow images. Two important image operations on large images are scaling and cropping. Downloading a large image, such as a histopathological image (whose size can be in the order of tens of GBs) to users may not be always feasible. Users may want to preview a scaled below version of the image before deciding whether to download the image. Further, users may just want view a particular area of interest in the image, in which case, a cropped region should be downloaded. These two operations, scalingand cropping, can be together to support zooming and panning, two natural user interactions to explore large images. Supporting scaling and cropping with secret image arrival. A naive solution would be for the data source to create multiple secret images atdifferent resolutions (to support scaling) and to divide each secret image into independentlydecodable tiles (to support cropping). These tiles are then secret-shared across the datacenters.When users request a region of an image at a particular scale, each datacenter sendsthe shadow tiles that overlap with the region at the nearest resolution to the user. Such asolution, however, may cause additional data to be sent to the user. The expansion of cloudstorage and computing platforms permits users to source storage and computations on theinformation, and permits businesses to dump the task of maintaining data-centers. However,issues over

loss of privacy and business value of personal information are an amazing barrierto the assuming of cloud services by customers and businesses alike.Superb thanks to assuage these privacy issues is to store all information within the cloud encrypted, and performcomputations on encoded information. To the present finish, want a cryptography schemethatenables meaningful computation on encrypted information, particularly a homomorphiccryptography scheme.

2. LITERATURE REVIEW

- In 2013 M. Mohanty, W. T. Ooi, and P. K. Atrey, "Scale me, crop me, know me not: supportingscaling and cropping in secret image sharing," Proposed an image sharing scheme that allows the user to retrieve a scaled or cropped version of the secret image by operatingdirectly on the shadow images, therefore reducing the amount of data sent from the datastores to the user. Results and analyses show that our scheme is highly secure, requires lowcomputational cost, and supports a large number of scale factors with arbitrary crop. [1]

- In 2015 K. Kansal, M. Mohanty, and P. K. Atrey, "Scaling and cropping of wavelet-based compressed images in hidden domain," proposed a scheme that can scale and crop a CDF(Cohen DaubechiesFeauveau) wavelet-based compressed image (such as JPEG2000) in the encrypted domain by smartly applying secret sharing on the wavelet coefficients. This scheme is highly secure and has acceptable computational and data overheads. Address this challenge by proposing a secret image sharing scheme that can hide an image in such a way that both compression and image scaling/cropping are possible .Shamir's (k, n) secret sharing [5] to secret share an image, and CDF discrete wavelet transformation based compression to compressing the image. The information in the low frequency LL wavelet band and all other high frequency wavelet bands are hidden by secret sharing the coefficient values and the coefficient positions respectively. [2]

- In 2002 C.-C. Thien and J.-C. Lin, "Secret image sharing," Proposed a method such thata secret image is shared by n shadow images, and any r shadow images (r¡=n) of them canbe used to restore the whole secret image. The size of each shadow image is smaller than thesecret image in our method. This property gives the benefit in further process of the shadowimages, such as storage, transmission, or image hiding. [3]

- In 2013 M. R. Asghar, G. Russello, B. Crispo, and M. Ion, "Supporting complex queries and access policies for multi-user encrypted databases". This system extends work on multi user encrypted search schemes by supporting SQL-like encrypted queries on encrypted databases .Furthermore, introduce access control on the information hold on within the cloud, where anybody actions (such as change access rights or adding/deletingusers) do not require redistributingkeys or re-encryption of data. [4]

- In 2013 E. Ayday, J. L. Raisaro, J.-P. Hubaux, and J. Rougemont, "Protecting and evaluating genomic privacy in medical tests and personalized medicine". Here proposesprivacy-enhancing technologies for medical tests and personalized medicine methods thatuse patients' genomic data. Focusing on genetic disease susceptibility tests, develop a newarchitecture (between the patient and the medical unit) and propose a "privacy preserving diseasessusceptibility test" (PDS) by using homomorphic encryption and proxy re-encryption.[5]

- In 2011 C. Dong, G. Russello, and N. Dulay,"Shared and searchable encrypted data for untrusted servers," propose an encryption scheme where each authorized user in the systemhas his own keys to encrypt and decrypt data. The scheme supports keyword search whichenables the server to return only the encrypted data that satisfies an encrypted query withoutdecrypting it.Systems provide a concrete construction of the scheme and give formal proofs of its security. Also report on the results of our implementation[6]

3. SYSTEM MODEL

3.1. *Volume Outsourcer*

This entity outsources the storage and rendering of volumes to a third-party cloud supplier. It'd be a private or an area of an organization. At intervals the latter case, users will act as Volume Outsourcers.

Typically, this entity owns the amount. The amount Outsourcer will store new volumes on a cloud server, delete/modify existing ones and manage access management policies (such as read/write access rights).In our state of affairs, the amount Outsourcer is a part of a volume capturing hospital.

3.2. *Public Cloud Server*

A Public Cloud Server is an element of the infrastructure provided by a cloud service supplier, like Amazon S31, for storing and rendering of volumes. It stores (encrypted) volumes and access policies accustomed regulate access to the degree and the rendered image. It performs most of the rendering on keep volumes and produces the partially rendered information.

3.3. *Private Cloud Server*

The private Cloud Server sits between the public Cloud Server and the rendering requester. It will be a part of the infrastructure, either provided by a personal cloud service supplier or maintained by a company as a proxy server. The non-public Cloud Server receives partially rendered information from the public Cloud Server and performs remaining rendering tasks on the degree. It then sends the rendered image to the rendering requester. Note that the non-public Cloud Server doesn't store information; it solely performs minimal rendering operations on partially rendered information received from the public Cloud Server.

3.4. *Image User*

This entity is permitted by the volume Outsourcer to render a volume keep in the Public Cloud Server. during a multi-user setting, a picture User will (i) a picture (in encrypted domain) that may be accessible by different Image Users, or (ii) access pictures rendered by different Image Users. In each case, Image Users don't got to share any keying material.

3.5. *Key Management Authority (KMA)*

The KMA generates and revokes keys to entities concerned within the system. For every user (is a Volume Outsourcer or Image User), it generates a key combine containing the user-side key and therefore theserver-side key. The server-side secrets firmly transmittedto the public Cloud Server, whereas, the user side secret is either sent to the user or privateCloud Server depending on whether or not the user could be a Volume Outsourcer or ImageUser. Whenever needed (say in key lost or taken cases), the KMA revokes the keys from thesystem with the support of the public Cloud Server.

The use of cryptosystems for hiding images is a well-studied area. A number of approaches, including but are not limited to, Public Key Cryptosystem (PKC), watermarking, Shamir's secret sharing and chaos-based encryption, have been proposed to protect images. To allow cloud datacenters to perform operations on the encrypted image, partial homomorphic cryptosystem-based solutions have been proposed. A partial homomorphic cryptosystem exclusively offers either addition or multiplication operations. Paillier, Goldwasser-Micali, Benaloh, Shamir's secret sharing are among partially homomorphic cryptosystems that support addition. Few works have been proposed for searching encrypted images based on dynamic extraction of image features.Although proposed tile-level

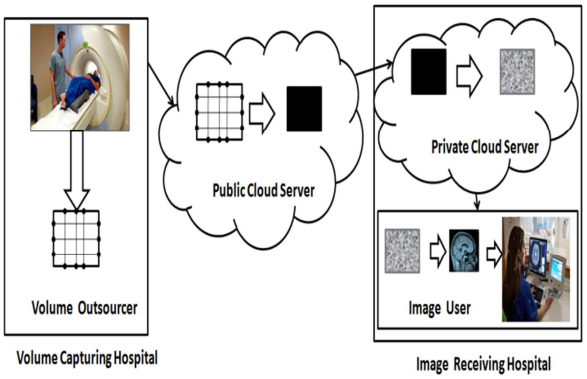

Fig.1. Cloud-Based Rendering of Medical Data.

encryption scheme 2DCrypt can have less computational and storage overheads than the naive per-pixel encryption, the flexibility of selecting an individual pixel is lost.

Fig.2. shows the architecture of 2DCrypt. In scaling and cropping parameters and forwards the request to the Access Request Processor module of the

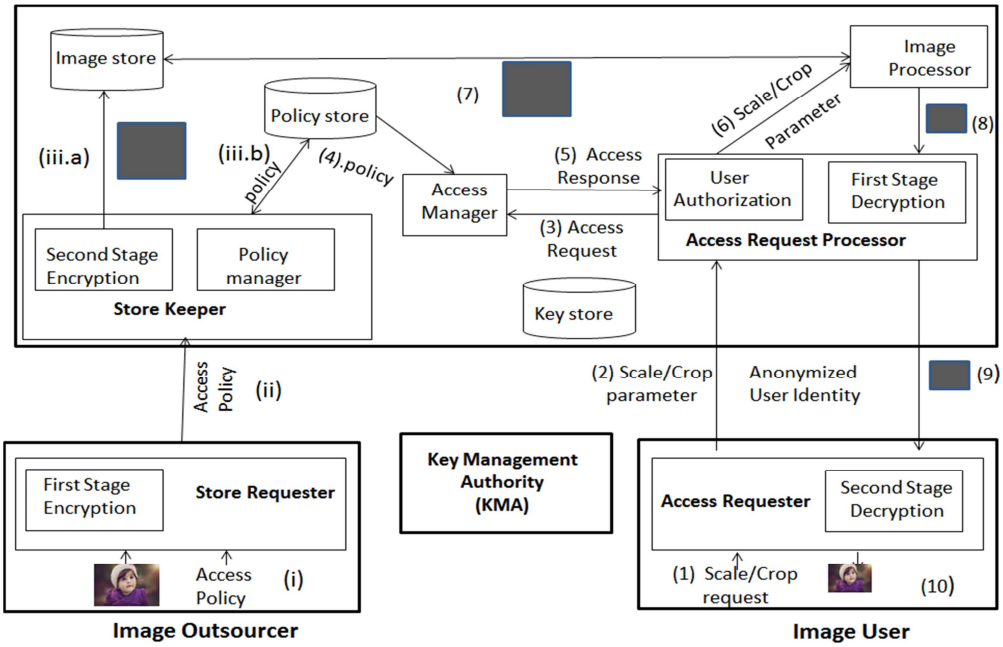

Fig.2. The architecture of 2DCrypt: a cloud-based secure image scaling and cropping system.

2DCrypt,each user as an Image Outsourcer or Image User), the KMA generates two keys pairs by randomly splitting the master secret key into two parts: the user-side key sent to the user and the server side key deployed to the server.The Image Outsourcer stores an image and its access policies in the cloud server. The Image Outsourcer invokes its client module Store Requester by providing plaintext image and access policies as inputs Step (i). The Store Requester performs the first round of encryption on the input image, using the user-side key, and then sends the encrypted image along with its access policies to the Store Keeper module of the Cloud Server Step (ii). When encrypting the image, the Store Keeper divides the image into multiple tiles and performs per-tile encryption.The encrypted image, which is received by the Cloud Server, is not in the common format necessary for sharing in multi-user settings. At theCloud Server-end, the Store Keeper performs the second round of encryption using the server-side keycorresponding to the user, and stores the encrypted image in an image store Step (iii.a).The Store Keeperalso stores the access policies of the image in the Policy Store Step (iii.b).Once an Image User expects the Cloud Server to process any image, its clientmodule Access Requester receives its input Step (1). The module Access Requester estimates the CloudServer Step (2). In the request, the Access Requester sends image scaling/cropping parametersStep (6). The requested image is retrieved from the Image Store Step (7) and the Image Processor performs scaling/cropping on the encrypted image.When thescaling/cropping operations are completed, the processed image is sent to the Access Request Processor Step (8). The Access Request Processor performs the first round of decryption on the processed image using the key corresponding to the Image User and sends the image tothe Access Requester module Step (9). The Access Requesterthe Access Request Processor first performs a user authorization phase by forwarding an access request to the Access Manager Step (3). The Access Manager fetches the access policies for the requesting user from the Policy Store Step (4) and it matches the accesspoliciesagainst the access request. Finally, the access response is sent back to the Access Request processorStep (5). If the user is authorized to perform the requested operation, the Image Processor is invoked with scaling/cropping parameters as inputsmodule on the ImageUser performs a second round of decryption and shows the processed image to theImage User Step (10). Here the image after the first round of decryption on the CloudServer is still encrypted and the Cloud Server cannot learn the secret

information containedin the image. To access the image in clear-text, a second round of decryption isrequired using the user.

3. TILE-LEVEL IMAGE CROPPING

The pixels' positions of a secret image are not hidden in the encrypted image, cropping in encrypted domains is easy. Here perform cropping by selecting the tiles containing pixels of an ROI. That is, when an Image User requests an ROI, the Cloud Server sends those tiles containing the pixels of the ROI. The Image User then fetches the required pixels from the received tiles and discards unnecessary pixels. The procedure of tile selection, however, is dependent on whether scaling has been performed before or not as illustrated. The selection of tiles for a non-scaled original image is different than the selection of tiles for a scaled image. In a non-scaled image, any four neighboring pixels are present in four different tiles (e.g., Tile 1, Tile 2, Tile 3, and Tile 4). Therefore, to select four tiles when four neighboring pixels are part of ROI Since neighbor's neighbor is in one tile, these four tiles are sufficient to cover all neighbors' neighbor pixels in a super-tile: Tile 1, Tile 2, Tile 3, and Tile 4 tiles are also sufficient when the super-tile is the ROI. In the case of a scaled image, the non-border neighboring pixels are part of one tile. Therefore, here select one tile when four non-border pixels are part of an ROI Note that cropping does not introduce round-off error since it does not round-off any floating point numbers.

3. CONCLUSION

Cloud-based image processing has data confidentiality issues, which can lead to privacy loss. This system addressed issue by proposing 2DCrypt, a modified Paillier cryptosystem-based scheme that allows a cloud server to perform scaling and cropping operations without learning the image content. In 2DCrypt, users do not need to share keys for accessing the image stored in the cloud. Therefore, 2DCrypt is suitable for scenarios where it is not desirable for the image user to maintain pre image keys. Furthermore,2DCrypt is more practical than existing schemes based on Shamir's secret sharing because it neither employs more than one datacenter nor assumes that multiple adversaries could collude by accessing a certain number of datacenters.

4. ACKNOWLEDGEMENT

I dedicate all my works to my esteemed guide, Prof. S. A. Kahate whose interest and guidance helped me to complete the work successfully. This experience will always steer me to do my work perfectly and professionally. I express my immense pleasure and thankfulness to all the teachers and staff of the Department of Computer Engineering, for their co-operation and support. Last but not the least, I thank all others, and especially my friends who in one way or another helped me in the successful completion of this paper.

REFERENCES

[1] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, Stanford, USA, 2009.

[2] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" in Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, 2011, pp. 113–124.

[3] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" in Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, 2011, pp. 113–124.

[4] M. Mohanty, W. T. Ooi, and P. K. Atrey, "Scale me, crop me, know me not: supporting scaling and cropping in secret image sharing," in Proceedings of the 2013 IEEE International Conference on Multimedia Expo, San Jose, USA, 2013.

[5] K. Kansal, M. Mohanty, and P. K. Atrey, "Scaling and cropping of wavelet-based compressed images in hidden domain," in MultiMedia Modeling, ser. Lecture Notes in Computer Science, 2015, vol. 8935, pp. 430–441.

[6] C.-C. Thien and J.-C. Lin, "Secret image sharing," Computers and Graphics, vol 26, pp. 765–770, October 2002