ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

Image Operations in Encrypted Domains

[1] Sanjana Prasad, [2] Dr.H.S. Jayanna
[1] [2] Siddaganga Institute of Technology, Karnataka
[1] sanjanaprasad19@gmail.com, [2] jayannahs@gmail.com

***Abstract*— The advancement of cloud or distributed computing and a drastic increment in the size of the digital images are reasons to outsource the image into the cloud. Despite of the fact that this outsourcing has many advantages, guaranteeing data confidentiality and the security in the cloud is one of the fundamental concerns. The encryption schemes for images guarantee the confidentiality in the cloud, but this scheme doesn't permit cloud data centers to perform operations over encrypted images. In this paper, this problem is addressed by proposing a modified Pailier cryptosystem based image scaling and cropping scheme for multi-client settings to scale and crop an image in the encrypted domain on cloud data centers.**

***Index Terms*— encrypted image processing, Pailier cryptosystem, encrypted scaling and cropping**

I. INTRODUCTION

As cloud computing is a base platform to store large volumes of data, it can be used to store the images. Cloud servers will only provide the storage facilities to the user but not security for their data. Images contain a highly sensitive data and personal information. If it is not protected, sensitive information in the image may get subjected to the unauthorized access by the cloud providers. The traditional approach to protect confidentiality of outsourced images is to encrypt the images before they are stored in the cloud. However, once encryption is done, it may not be possible to perform basic image processing operations, such as scaling and cropping.

The objective if this project is to apply image processing techniques such has scaling and cropping on encrypted images in cloud in order to provide security for data stored in cloud. In this project the cloud server without learning the content of the image, it will send the scaled/cropped image to the image user. Homomorphic algorithms are used to perform the image processing techniques on the encrypted image. This technique can be used in the field of forensics for the crime investigation. This helps when two investigators are in geographically different places and wants to share confidential information such as guns used in the crime. For instance, if the crime investigator has to refer the pervious case for his present investigation like if he wants to know about the gun used he can ask for cloud server for only the cropped image of the gun. Instead of sharing the entire image only the part of the image which contains the gun is shared. This makes the workflow easier and reduces the computational overhead.

II. RELATED WORK

Hiding the images using cryptosystem is a well-studied area. A number of approaches like to, Public Key Cryptosystem (PKC) [1] which considers the application of the Discrete Cosine Transform (DCT) to images encrypted by using an appropriate homomorphic cryptosystem. Watermarking proposed in [2] is a new robust digital image blind watermark scheme that is used to protect color medical images. In this scheme, K-L transform is applied to an RGB medical image and the binary watermark is embedded into low frequency sub-band of DWT of the principal component of medical images., have been proposed to protect images. These schemes provide confidentiality for cloud-based storage systems where a cloud datacenter does not perform any operation on the stored image.

To allow cloud datacenters to perform operations on the encrypted image, partial homomorphic cryptosystem based solutions have been proposed a lightweight secure image search scheme over encrypted data, namely SEISA [3]. Pailier [4], Goldwasser and Micali [5], Benaloh and Tuinstra [6] are among partially homomorphic cryptosystems that support addition. The example for the homographic is RSA [7] and ElGamal [8].

Early works have been focused retrieving on encrypted data. [9] Showed key word search on the encrypted document, [10] encrypted index based search, [11] searching the conjunctions of multiple keyword. All these support searching functionality without any loss of data confidentiality.

Shamir's secret sharing has been used for allowing encrypted domain scaling and cropping [12], [13]. Shamir's secret sharing-based schemes, however, can be infeasible for practical scenarios since they require n cloud servers. Moreover, these schemes are prone to collusion attack when k cloud servers collude. This is addressed by proposing image operations in encrypted domain, a modified Pailier cryptosystem based image scaling and cropping scheme for multi-user settings that allows cloud datacenters to scale and crop an image in the encrypted domain. This project

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

encrypts the image in Pailier homomorphic algorithm and performs image operations on encrypted image. This uses single cloud to store the data and thus improves the robustness of the system and image user can only access the image it he has access permission and decryption key.

III. PROPOSED SYSTEM

This work uses Pailier cryptosystem algorithm to encrypt the image. To increase the security, double encryption and decryption is done. The implementation part consists of four modules; they are Image outsourcer, image user, cloud server and key management.

1. Image outsourcer is the one who outsource the image and provides access polices to the image user. Access policies are "read" and "processing". He performs the first round of encryption and sends the encrypted image to cloud and encrypted key through mail to the authorized user.
2. Cloud servers receive the encrypted image and access polices from the image user and it again encrypts the image. It accepts the request from the image user and responds to it. The cloud server will not learn the content of the image. The second round of encryption and first round of decryption is done by the cloud.
3. Image user can access the image only if he is authorized by the image outsourcer. If he has a "read" permission then he can get the entire image, if he had the "process" permission then he can only get the scaled(height, width) or cropped(X, Y, height, width) image. He has to send the scale/crop parameters to the cloud and cloud will send the scaled/cropped image and image user has to perform the second round of decryption of the image using the secret key received from the mail get the image.
4. Key management generates the key to both cloud server and image user. For each file key is generated and it is sent to the image user mail and server side key is deployed in the cloud. User should decrypt the image using the key.

Scaling and cropping operations can be done on encrypted images of any factors. Scaling and cropping techniques when combined provides zooming and panning operations. In image streaming these operations can be considered as two key features. Existing works create and store multiple copies of the same image but Image Operations in Encrypted Domains does not create and store multiple copies of the same image. Moreover, this work provides only the requested processed part of the image to the user from cloud server.

IV. EXPERIMENTAL RESULTS

In these section results of this work is discussed. The experiment was performed on the Intel i3 processor and 8GB of the RAM. We implemented Pailier cryptosystem and image scaling cropping operations in java on windows platform. In our implementation we used 512 bits keys size. This system works for all JPEG and PNG image formats. The work is tested around 500 images. It can have any number of users and can have maximum image size of 150KB. As user gets only the required cropped and scaled image the computational overhead is decreased at the image user side as he only decrypts the scaled/cropped image.

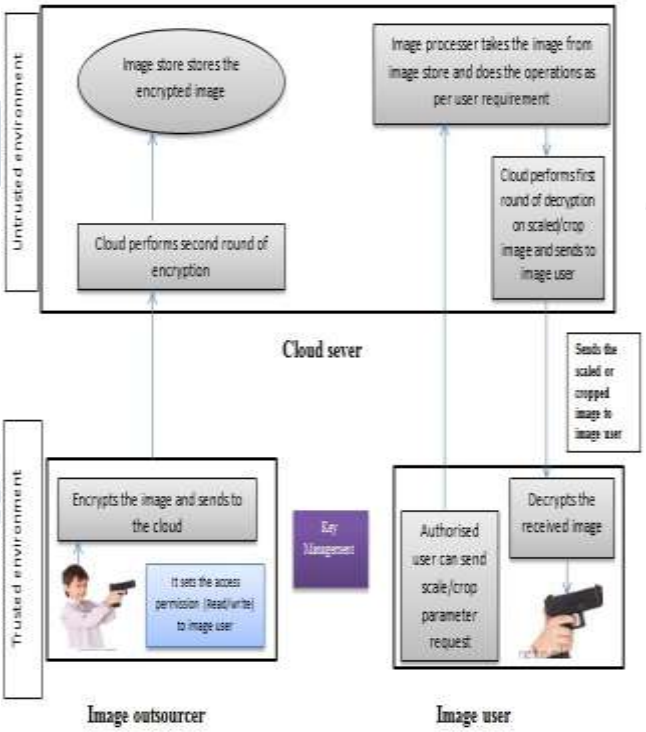

Fig. 1: Architecture of image operations in encrypted domains

As only one cloud is used this system is very robust to the collusion attacks. The encryption times of the different images using Paillier cryptosystem are given in table 1 and its graph is shown in figure 2. The cropping and scaling times depends on the user parameters. Irrespective of scaling and cropping user needs 0.55ms to decrypt the image. The exact computational overhead and the data required by the image user, however, are dependent on the image size and the user's scaling and cropping parameters.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

Image size	Encryption time
6KB	1s
10KB	1s
18KB	1s
44KB	4s
88KB	17s
150KB	21s

Table 1: Encryption time of images using Paillier cryptosystem

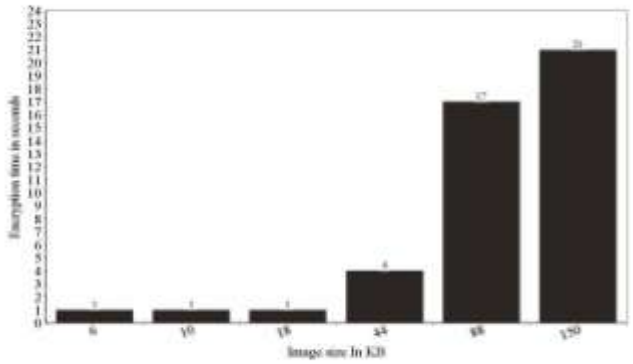

Fig. 2: Graph of images and its encryption time in Paillier cryptosystem

V. CONCLUSION

In this work a secure scaling and cropping of the image in encrypted domain is demonstrated. A Pailier cryptosystem-based scheme is used which allows a cloud server to achieve scaling and cropping operations without knowing the contents of the image. Any factor scaling and cropping on encrypted images can be done. To provide better security double encryption and decryption is done. This can be extended to compressed images.

REFERENCES

[1] T. Bianchi, A. Piva, and M. Barni, "Encrypted domain DCT based on homomorphic cryptosystems," EURASIP J. Multimedia Inf. Security, vol. 2009, pp. 1:1–1:12, Jan. 2009. [Online].Available:http://jis.eurasipjournals.springeropen.com/article s/10.1155/2009/716357

[2] X. Sun and S. Bo, "A blind digital watermarking for color medical images based on PCA," in Proc. IEEE Int. Conf. Wireless Commun., Netw. Inf. Security, Beijing, China, Jun.
2010, pp. 421–427.

[3] J. Yuan, S. Yu, and L. Guo, "SEISA: Secure and efficient encrypted image search with access control," in Proc. IEEE Conf. Comput. Commun., Apr./May 2015, pp. 2083–2091.

[4] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Advances in Cryptology, vol. 1592. Springer, 1999, pp. 223–238.

[5] S. Goldwasser and S. Micali, "Probabilistic encryption," J. Comput. Syst. Sci., vol. 28, no. 2, pp. 270–299, Apr. 1984.

[6] J. Benaloh and D. Tuinstra, "Receipt-free secret-ballot elections (extended abstract)," in Proc. 26th Annu. ACM Symp. Theory Comput., 1994, pp. 544–553.

[7] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[8] T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 196. Berlin, Germany: Springer-Verlag, 1984,pp. 10–18.

[9] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Security Privacy, May 2000, pp. 44–55.

[10] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology, vol. 3027. Springer, 2004, pp. 506–522.

[11] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Applied Cryptography and Network Security, vol. 3089. Springer,
2004, pp. 31–45.

[12]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 Proc. IEEE Int. Conf. Multimedia Expo, San Jose, CA, USA, Jul. 2013, pp. 1–6.

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

[14] M. Mohanty, M. R. Asghar and G. Russello, " 2DCrypt : Image Scaling and Cropping in Encrypted Domains," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2542-2555, Nov. 2016.

[15] Mrs. Jadhav Rohini , Prof. S. A. Kahate , "A Survey on: A Modified Paillier Cryptosystem-Based Image Scaling and Cropping Scheme", IJARIIE-ISSN(O)-2395-4396 3225 www, Vol-2 Issue-5 2016.

[16] Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz, "Performance Analysis of Different Cryptography Algorithms", ISSN: 2277 128X, Volume 6, Issue 3, March 2016.