ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May2017

Two Dimensional Cryptography Using Modified Pallier Cryptosystem

Jadhav Rohini, B. S. Kurhe

Assistant Professor, Dept. of Computer Engineering, SPCOE, Otur, Pune, India

Assistant Professor, Dept. of Computer Engineering, SPCOE, Otur, Pune, India

ABSTRACT: Cloud computing comes with numerous possibilities and challenges. Cloud computing is used to access unlimited storage and computational resources. The resources are remotely accessed by the cloud users. Data confidentiality is the main source of cloud computing. To provide confidentiality of image use the to state-of the-art technique. The main concern in data confidentiality is used to state-of the-art encryption scheme. The state-of the-art schemes do not allow cloud datacenters to operate encrypted images. Paillier changes the multi Crypt to Cryptosystem-based image scaling and cropping schemes. According to multi Crypt, multiple users can process the images without sharing anyone to use. A space-efficient tiling scheme that allows tile-level image scaling and cropping operations. In tile level encryption scheme encrypt a tile of pixel instead of encrypting each pixel individually. Two dimensional cryptography multiple user can process (scale/crop) the image without sharing any key.

KEYWORDS: Security, Image Outsourcing, Cryptography, Tiling, Scaling and Cropping

I. Introduction

Cloud computing is an emerging computing model in which resources of the computing communications are provided as services over the Internet. Cloud computing, to put it simply, means internet computing. The internet is commonly visualized as clouds; hence the term “cloud computing” for computation done through the internet. With cloud computing users can access database resources via the internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources. Secrecy of communication is clearly one of the most important goal of cryptography, The demand for outsourcing data storage and management has increased dramatically in the last decade. The development of cloud storage and computing platforms allows users to outsource storage and Computations on their data, and allows businesses to offload the task of maintaining data-centres. However, concerns over loss of privacy and business value of private data are an overwhelming barrier to the adoption of cloud services by consumers and businesses alike. An excellent way to assuage these privacy concerns is to store all data in the cloud encrypted, and perform computations on encrypted data. To this end, we need an encryption scheme that allows meaningful computation on encrypted data, namely a homomorphic encryption scheme. Homomorphic encryption schemes that allow simple computations on encrypted data have been known for a long time. constructed a fully homomorphic encryption scheme capable of evaluating an arbitrary number of additions and multiplications (and thus, compute any function) on encrypted data. To secure image confidentiality and integrity of data use secret image sharing [3] to hide an image from any data enter by distributing the shares (i.e., the shadow images) across multiple data centres. Secret image sharing, based on Shamirs secret sharing scheme and multi-secret image sharing schemes, mainly focus on the trade-off between efficiency and security, and do not easily support image operations on the shadow images. Scaling and cropping are the two important parameter for process the image. Downloading a large size image that is 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 down version of the image before deciding whether to download the image. Further, users may just want view a particular region of interest in the image, in which case, a cropped region should be downloaded. These two operations, scaling and cropping, can be combined to support zooming and panning, two natural user interactions to explore larg images. Supporting scaling and cropping with Secret image sharing is non-trivial. To the present finish, want a cryptography scheme that enables meaningful computation on encrypted information, particularly a homomorphic cryptography scheme.

DOI: 10.15680/IJIRCCE.2017. 0505202

II. RELATED WORK

The cryptosystems various techniques are use including yet are not restricted to, Public Key Cryptosystem(PKC) [7], watermarking [8], Shamir's secret sharing [6] and mayhem based encryption [9], have been proposed to ensure the security of images. It gives secrecy for cloud-based storage systems where a cloud datacenter does not play out any operation on the put away image. To permit cloud datacenter to perform operations on the encrypted image, halfway homomorphic cryptosystem-based arrangements have been proposed [10], [12]. A halfway homomorphic cryptosystem solely offers either expansion or multiplication operations. Paillier [13], Gold wasser-Micali [14], Benaloh [15], Shamir's secret sharing [3] are among halfway homomorphic cryptosystems that bolster expansion. While, cases of halfway homomorphic cryptosystems that offer multiplication are RSA [16] and ElGamal [17]. Along these lines, the decision of a halfway homomorphic plan is vigorously reliant on the sort of operations to be performed in the encrypted space. Early works have concentrated on recovering encrypted content records. For example, [18] displayed the primary pragmatic conspire for single keyword inquiry on encrypted records. To enhance execution, [19] broadened the encrypted seek with ordering capacity. Both works have been stretched out for looking utilizing conjunctions of multiple keywords [20]. More late works have concentrated on SQL-like questions supporting conjunctions and disjunctions [20]. Encrypted content based pursuit can likewise be connected to recovery of encrypted images.

In [10], Lu et al. proposed down to earth seek in light of highlight/record randomization methods that offer a great exchange off between secure safe guarding and execution.[11] proposed a homomorphic-based SIFT (Scale- Invariant Highlight Transform) extraction seek that expands the accuracy of the inquiry additionally acquires from 2 to 4 requests of IEEE Transactions on Information Forensics and Security (Volume:PP , Issue: 99),24June 2016 size more expenses. After [12] presents a look plot for encrypted images that is accurate and in the meantime brings about computational overheads like a plaintext strategy. Be that as it may, their plan obliges users to share the keys for getting to images. A few works have been proposed for protection saving confront acknowledgment where one gathering tries to coordinate a confront image with a dataset facilitated by another get-together and both gatherings are keen on keeping their data secret from each other. Shamir's secret sharing has been utilized for permitting encrypted space scaling and cropping of image [4], [5]. Shamir's secret sharing-based plans, on echoless, can be infeasible for useful situations since they require n cloud servers. Additionally, these plans are inclined to agreement attack when k cloud servers plot. Conversely, 2DCrypt utilizes the Paillier-based cryptosystem that requires just a single cloud datacenter and is more powerful to agreement attacks. The Paillier cryptosystem is homomorphic to increments and scalar multiplications [3] and can be changed to an intermediary encryption conspire.

III. SYSTEM MODEL

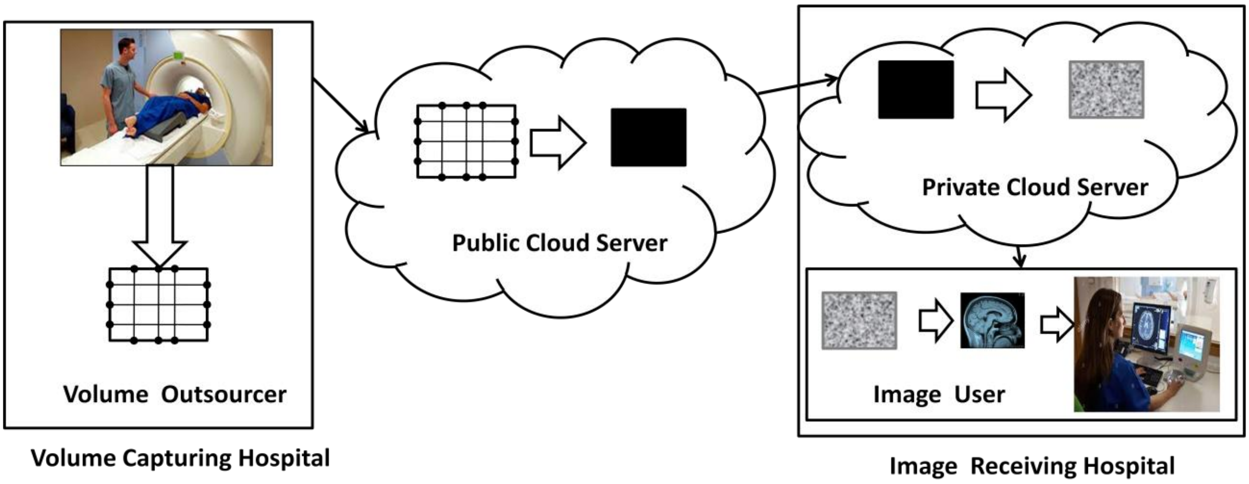

Fig : Cloud-based rendering of medical data.

The proposed system consist of distributed cloud storage. The cloud scale, crop and encrypt the images on behalf of image outsourcer.

1. **Image Outsourcer:** Image outsourcer is hospital authority who stores the image on cloud. The image outsourcer maintains the security and privacy of a particular image. This is obtained by encryption of an image before uploading. Image outsourcer can delete modify images also manage access control policies.
2. **Cloud server:** Amazon EC2 used as a cloud server for storing and processing the images. Both encrypted images and policies are stored on cloud.
3. **Image User:** Image user are authorized user by image outsourcer, these user can request images stored on cloud. Authorized user do not need to share any key. Other user can decrypt the image on request approval.
4. **Key Management Authority:** It generates key pair one for client and one for server. These keys get securely shared via email.

IV. Proposed System Algorithm

The main idea of two dimensional cryptography is the modified Paillier cryptosystem-based proxy encryption to encrypt images before storing them in the cloud. This version of Pailler cryptosystem supports re-encryption , and is homomorphic to additions and scalar multiplications. Proposed system can apply this cryptosystem to encrypt an image that will be bilinear scaled, since bilinear scaling requires addition and scalar multiplication operations only. Cropping of the encrypted image is easy since this cryptosystem does not disturb the pixel position, i.e. allowing us to obtain the corresponding pixel position after the decryption. Provide access to multiple user proposed system extend the modified Paillier cryptosystem such that each user having her own key to encrypt or decrypt the images. Encrypting each pixel individually a tiles of pixel encrypt at same time. Using the tiling level encryption in 2DCrypt, proposed system save the space and decrease the number of required encryptions and decryptions by a factor of the tile size.

- *Description of the Proposed Algorithm:*

Step 1: The KMA runs the initialization algorithm in order to generate public parameters Params and a master secret key set MSK. It takes as input a security parameter k and generates two prime numbers p and q of bit-length k.
It computes n = pq.

Step 2: KeyGen(M SK, i). The KMA runs the key generation algorithm to generate keying material for users in the system. For each user i, this algorithm generates two key sets K U i and K S i by choosing a random x i1 from [1, n 2 /2].
Then it calculates x i2 = x x i1 , and transmit.
The server adds K S i to the Key Store as follows: K S K S K S i .

Step 3: ClientEnc(D, K U i). A user i runs the data encryption algorithm to encrypt the data D using her key K U i .
To encrypt the data D Z n , the user client chooses e 1 , e ˆ 2), a random r [1, n/4].

Step 4: ServerReEnc(E i (D), K S i). The server re-encrypts the user encrypted data E i (D)= (e 1 , e 2).It retrieves the key K S i corresponding to the user i and computes the re-encrypted ciphertext E(D) = (e 1 , e 2),

Step 5: ServerSum(E(D 1), E(D 2)). Given two encrypted val- ues E(D 1) = (e 11 , e 12) (where e 11 = g r 1 and e 12 = g r 1 x .(1 + D 1 n) and E(D 2) = (e 21 , e 22) (where e 21 =g r 2 and e 22 = g r 2 x .(1 + D 2 n)), the server calculates the encrypted sum E(D 1 + D 2) = (e 1 , e 2).

V. SOLUTION DETAILS

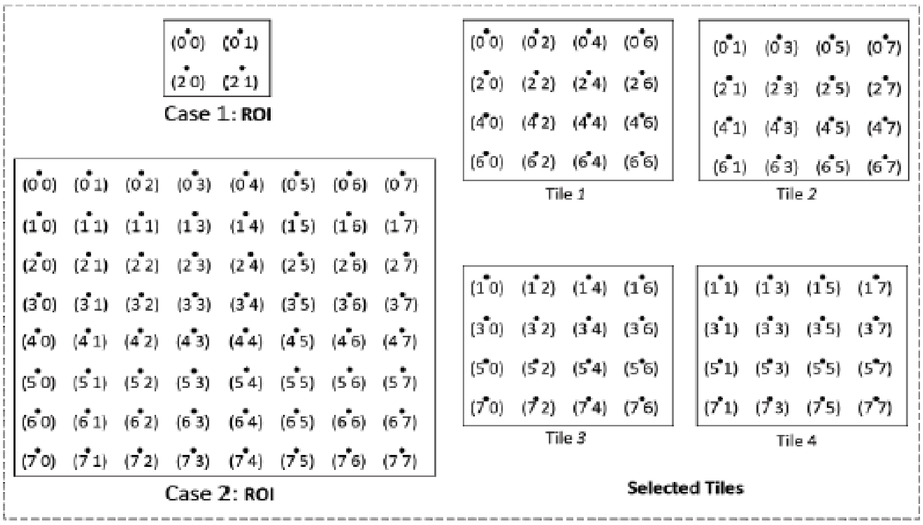

Fig. 3. Cropping a Non-Scaled Image

Proposed System use the tiling level encryption schema, to divide the image into no of pixel. Process on the tiles of pixel, instead of encrypting each pixel individually. Each pixel makes 8*8 size non-covering super-tiles for an info image. From every super-tile, nine 4 x4 size covering tiles are made by executing the space proficient tiling technique examined. At that point, each tile is encrypted and stored in a record. Likewise store every one of the tiles in a solitary record.

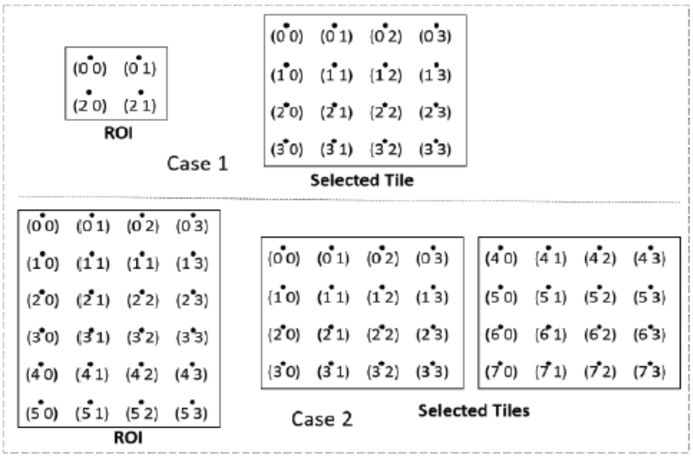

Fig. 4. Cropping a Scaled Image

For a scaling or cropping request, required tiles are resolved (at the Cloud Server end) in light of scaling and cropping parameters. These tiles are then access from the document for the scaling and cropping operations. For instance, for scaling by a variable of two, as it were the initial four tiles of a super-tile are fetched and handled. In the wake of decoding the prepared tiles, the required pixels (at the Image User end) of a tile are resolved from the scaling what's more, cropping parameters, and the decoded pixels are gathered to render the requested scaled/trimmed image.

VI. CONCLUSION

2DCrypt is more pragmatic than existing schemes in view of Shamir's secret sharing does not allow on more than one cloud data center. Proposed system save the space using tiling scheme that permits the cloud to perform per-tile operations. In 2DCrypt, put various pixels in a tile, and encrypt the tile as opposed to encrypting every pixel freely. Besides, upgraded the altered Paillier scheme to restrain its storage prerequisite. Because of these upgrades, 2DCrypt requires around 40 times less cloud storage than the credulous per-pixel encryption.

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. 113124.
3. A. Shamir, How to share a secret, Communications of the ACM,vol. 22, pp. 612613, November 1979.
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 and Expo,San Jose,USA,2013.
5. K. Kansal, M. Mohanty, and P. K. Atrey, Scaling and cropping of waveletbased compressed images in hidden domain, in MultiMedia Modeling, ser. Lecture Notes in Computer Science, 2015, vol. 8935, pp. 430441.
6. C.-C. Thien and J.-C. Lin, Secret image sharing, Computers and Graphics, vol. 26, pp. 765770, October 2002
7. T. Bianchi, A. Piva, and M. Barni, Encrypted domain DCT based on homomorphic cryptosystems, EURASIP Journal on Multimedia and Information Security, vol. 2009, pp. 1:11:12, January 2009.
8. X. Sun, A blind digital watermarking for color medical images based on PCA, in Proceedings of the IEEE International Conference on Wireless Communications, Networking and Information Security, Beijing, China, August 2010, pp. 421427.
9. N. K. Pareek, V. Patidar, and K. K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing, vol. 24, pp. 926934, September 2006.
10. W. Lu, A. L. Varna, and M. Wu, Confidentiality-preserving image search: A comparative study between homomorphic encryption and Distance-preserving randomization, IEEE Access, vol. 2, pp. 125141,February 2014.
11. C.-Y. Hsu, C.-S. Lu, and S.-C. Pei, Image feature extraction in encrypted domain with privacy-preserving SIFT, IEEE Transactions on Image Processing, vol. 21, no. 11, pp. 45934607, 2012.
12. J. Yuan, S. Yu, and L. Guo, SEISA: Secure and efficient encrypted image search with access control, in IEEE Conference on Computer Communications, 2015, pp. 20832091
13. P. Paillier, Public-key cryptosystems based on composite degree residuosity classes, in Advances in Cryptology EUROCRYPT, 1999, vol.1592, pp. 223238.
14. S. Goldwasser and S. Micali, Probabilistic encryption, Journal of Computer and System Sciences, vol. 28, no. 2, pp. 270299, 1984.
15. J. Benaloh and D. Tuinstra, Receipt-free secret-ballot elections (Extended Abstract), in Proceedings of the Twenty-sixth Annual ACM Symposium on Theory of Computing, 1994, pp. 544553
16. T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, in Advances in Cryptology, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1985, vol. 196, pp.1018.
17. D. X. Song, D. Wagner, and A. Perrig, Practical techniques for searches on encrypted data, in IEEE Symposium on Security and Privacy, 2000,pp. 4455.
18. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, Public key encryption with keyword search, in Advances in Cryptology-
19. Eurocrypt,2004, pp. 506522.
20. M. R. Asghar, G. Russello, B. Crispo, and M. Ion, Supporting complex queries and access policies for multi-user encrypted databases, in Proceedings of the ACM Workshop on Cloud Computing Security Workshop, 2013, pp. 7788.

DOI: 10.15680/IJIRCCE.2017. 0505202