Space-Efficient Tiling Scheme for Tile-Level Encrypted Domain Scaling and Cropping

[1]DASARI MADHAVI **[2]K.SANTHI , M.Tech ,(Ph.D).,**

[1]PG Scholar, Department of CS, S.V.College of Engineering, madhavi.d32@gmail.com

[2]Associate Professor, Department of CSE , S.V.College of Engineering, santhi@svcolleges.edu.in

ABSTRACT:-- The development of cloud computing and an intense increment of picture size are making the outsourcing of picture stockpiling and preparing an alluring plan of action. In spite of the fact that this outsourcing has much points of interest, guaranteeing information classification in the cloud is one over the significant concerns. There are best in class encryption plans in light of the fact that guaranteeing secrecy in the cloud. Be that as it may, such plans don't allow cloud datacenters to work operations on scrambled pictures. In that paper, we handle it issue by means of proposing 2DCrypt, an altered Paillier cryptosystem-based picture scaling and editing plan for multi-client settings that permits cloud datacenters to reach and product a picture in the scrambled area. To envision a high stockpiling overhead come about past the guileless per-pixel encryption, we propose a space-effective tiling arrangement that permits tile-level picture scaling or editing operations. Fundamentally, rather on scrambling every pixel independently, we are capable as per encode a tile of pixels. 2DCrypt is sure so two or three clients may see then process the pictures without sharing any encryption keys – a prerequisite alluring for sensible arrangements inside real associations. Our investigation or results appear to desire 2DCrypt is IND-CPA safe and causes a suited overhead. When scaling a 512 * 512 picture by an issue around two, 2DCrypt requires a photograph shopper in impersonation of download roughly 5:3 occurrences a greater number of records than the un-encoded scaling and need to activity roughly 2:3 seconds more prominent in light of the fact that getting the scaled picture in plaintext.

Index Terms—Image Outsourcing, Hidden Image Processing, Encrypted Scaling and Cropping, Paillier Cryptosystem

1.1 INTRODUCTION

Cloud computing is an alluring worldview for getting to for all intents and purposes boundless capacity and computational assets. With its compensation as-you-go demonstrate, customers get to quick and solid equipment, paying just for the assets they have to use without the dangers of extensive forthright ventures. These days, building applications for sight and sound substance facilitated in frameworks overseen by outsider cloud suppliers is normal. Pictures may contain profoundly delicate and individual data. If not ensured, touchy data in the pictures (e.g., MRI sweep of a patient or G.I.S. maps) may be liable to unapproved gets to by cloud suppliers. A guileless way to deal with ensure privacy of outsourced pictures is to encode the pictures before they are put away in the cloud. Be that as it may, once this is done, it may not be conceivable to perform essential picture preparing operations, for example, scaling and trimming. For example, a remote pathologist, getting to a vast histopathology picture, would oblige first to get to a downsized adaptation, and after that perform scaling and trimming operations to get an appropriate determination for the Region of Interest (ROI). With pictures that are encoded utilizing standard encryption strategies, such operations would require the customer machine to download the full scrambled pictures, unscramble them on the nearby machine, and afterward play out the operations. This makes the work process moderate and wasteful on the grounds that a colossal measure of information is pre-gotten and handled. cloud suppliers are straightforward yet inquisitive. We accept they don't alter the applications sent in the foundation, however information may be gathered or spilled.

A commonplace illustration is supplanting old hard drives with new ones, where the information has not been legitimately wiped out. Likewise, we accept an undeniable multi-client get to model, where a few approved clients get to and alter the information put away in the cloud. With a specific end goal to take full preferred standpoint of the cloud demonstrate, operations are offloaded however much as could reasonably be expected to cloud servers. Be that as it may, to protect classification, operations are performed over encoded pictures. In this work, we concentrate on unique scaling and trimming operations on encoded pictures. These two operations can be consolidated to actualize zooming and panning operations, which are important to explore through vast pictures, (for example, maps). Along these lines, no data contained in the pictures can be spilled to the cloud servers, and in the meantime, clients can completely misuse the cloud show by designating the greater part of the calculation to the cloud. one might want to utilize the completely homomorphic encryption plan to play out a calculations over scrambled information. Be that as it may, the right now accessible completely homomorphic encryption plan is not computationally commonsense. Along these lines, halfway homomorphic encryption conspires, those supporting certain operations over encoded information, are normally utilized for reasonable arrangements. In light of halfway homomorphic Shamir's mystery sharing two fundamental research works perform picture scaling and trimming operations in the scrambled space. By augmenting the fundamental work of Thien and Lin these works make numerous offers of the mystery picture and disperse the commotion like shared pictures among different cloud suppliers. To recuperate the first picture, k out of n shared pictures must be recovered. The pictures are partaken such that scaling and editing operations can be performed on scrambled pictures.

2. RELATED WORK

The utilization of cryptosystems for concealing pictures is a very much examined range. Various methodologies, including however are not restricted to, Public Key Cryptosystem (PKC), watermarking, Shamir's mystery sharing and turmoil based encryption, have been proposed to secure pictures. These plans give privacy to cloud-based capacity frameworks where a cloud datacenter does not play out any operation on the put away picture. To permit cloud datacenters to perform operations on the encoded picture, incomplete homomorphic cryptosystem-based arrangements have been proposed. An incomplete homomorphic cryptosystem only offers either expansion or increase operations. Paillier, Goldwasser-Micali], Benaloh], Shamir's mystery sharing are among mostly homomorphic cryptosystems that bolster expansion. Though, cases of in part homomorphic cryptosystems that offer duplication are RSA and ElGamal. Accordingly, the decision of an incomplete homomorphic plan is intensely subject to the sort of operations to be performed in the scrambled space.

Early works have concentrated on recovering scrambled content records. For example, displayed the principal useful plan for single catchphrase hunt on encoded reports. To enhance execution, amplified the encoded seek with ordering capacity. Both works have been stretched out for looking utilizing conjunctions of numerous watchwords. Later works have concentrated on SQL-like inquiries supporting conjunctions and disjunctions. Scrambled content based pursuit can likewise be connected to recovery of encoded pictures. In any case, the exactness of the returned set is subject to the nature of the watchwords utilized for depicting the substance of a picture. Few works have been proposed for seeking scrambled pictures in light of dynamic extraction of picture elements. In Lu et al. proposed commonsense hunt in view of highlight/record randomization systems that offer a decent exchange off between security conservation and execution. proposed a homomorphic-based SIFT (Scale-Invariant Feature Transform) extraction look that expands the exactness of the inquiry additionally brings about from 2 to 4 requests of size more expenses. A later work by presents a scan plot for scrambled pictures that is exact and in the meantime causes computational overheads like a plaintext strategy. Be that as it may, their plan obliges clients to share the keys for getting to pictures. A few works have been proposed for protection saving face recognition] where one gathering tries to coordinate a face picture with a dataset facilitated by another get-together and both sides are keen on keeping their information mystery from each other. Shamir's mystery sharing has been utilized for permitting scrambled space scaling and trimming. As examined in Section I, Shamir's mystery sharing-based plans, be that as it may, can be infeasible for reasonable situations since they require n cloud servers. Besides, these plans are inclined to conspiracy assault when k cloud servers plot. Interestingly, 2DCrypt utilizations the Paillier-based cryptosystem that requires just a single cloud datacenter and is more vigorous to conspiracy assaults. The Paillier cryptosystem is homomorphic to increments and scalar augmentations and can be changed to an intermediary encryption plot.

3. EXISTING SYSTEM

An Image Outsourcer is in charge of tending to security and protection concerns appended to picture outsourcing. To accomplish this, the Image Outsourcer encodes the picture before sending it to the cloud datacenter. Advance, the Image Outsourcer can store new pictures on a cloud server, erase/alter existing ones, and oversee get to control approaches, (for example, read/compose get to rights) to direct access to the pictures put away on the cloud server.

Keeping in mind the end goal to give the multi-client bolster, we amplify the changed Paillier cryptosystem with the end goal that every client has her own particular key to encode or unscramble the pictures. In this way, including another client or evacuating a current one won't require re-encryption of existing pictures put away in the cloud.

2DCrypt is more useful than existing plans in light of Shamir's mystery sharing since it neither utilizes more than one datacenter nor expect that various foes could connive by getting to a specific number of datacenters.

4. PROPOSED SYSTEM

The utilization of cryptosystems for concealing pictures is an all around contemplated territory. Various methodologies, including yet are not restricted to, Public Key Cryptosystem (PKC), watermarking, Shamir's mystery sharing and confusion based encryption, have been proposed to ensure pictures.

To permit cloud datacenters to perform operations on the scrambled picture, fractional homomorphic cryptosystem-based arrangements have been proposed. A halfway homomorphic cryptosystem only offers either expansion or augmentation operations. Paillier, Goldwasser-Micali, Benaloh, Shamir's mystery sharing are among mostly homomorphic cryptosystems that bolster expansion. Few works have been proposed for seeking encoded pictures in view of dynamic extraction of picture components. Despite the fact that proposed tile-level encryption plot 2DCrypt can have less computational and capacity overheads than the guileless per-pixel encryption, the adaptability of choosing an individual pixel is lost.

ADVANTAGES

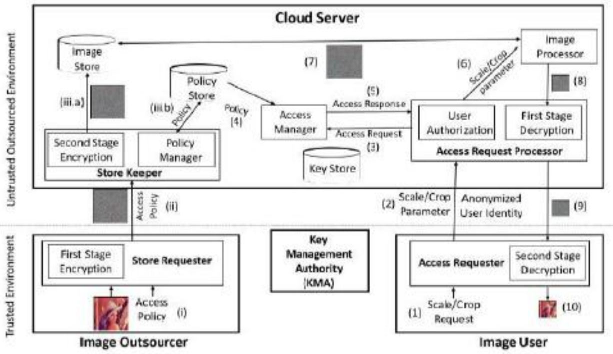
To take full advantage of the input space allowed by the proposed cryptosystem, we introduce a concept of tiling to group a set of pixels.

A tile can be encrypted instead of encrypting each pixel. Using the tiling in 2DCrypt, we save the space and decrease the number of required encryptions and decryptions by a factor of the tile size.

We proposed a space efficient tiling scheme that allows the cloud to perform per-tile operations. In 2DCrypt, we put a number of pixels in a tile, and encrypt the tile instead of encrypting each pixel independently.

5. SYSTEM MODEL

In this work, we consider a distributed cloud-based image storage and processing system where a cloud server stores, scales, and crops an encrypted image on behalf of an image outsourcer. In the system model, we assume the following entities.



The Architecture of 2DCrypt: a Cloud-Based Secure Image Scaling and Cropping System

We talk about the engineering and work process of 2DCrypt, a cloud-based multi-customer picture scaling and trimming system. 2DCrypt relies on upon Paillier cryptosystem. Figure 1 exhibits the plan of 2DCrypt. In 2DCrypt, for each customer (i.e., be it an Image Outsourcer or Image User), the KMA produces two keys consolidates by heedlessly part the pro secret go into two segments: the customer side key sent to the customer and the server-side key passed on to the server. The Image Outsourcer stores a photo and its get to approaches in the cloud server. For this business, the Image Outsourcer summons its client module Store Requester by giving plaintext picture and get to approaches as information sources (Step i). The Store Requester plays out the first round of encryption on the data picture, using the customer side key, and after that sends the mixed picture close by its get to methodologies to the Store Keeper module of the Cloud Server (Step ii). Observe that while scrambling the photo, the Store Keeper segments the photo into different tiles and performs per-tile encryption. A low down discourse about the tile-level encryption will be displayed in Section V. The mixed picture, which is gotten by the Cloud Server, is not in the fundamental association basic for sharing in multi-customer settings. At the Cloud Server-end the Store Keeper plays out the second round of encryption using the server-side key contrasting with the customer, and stores the encoded picture in a photo store (Step iii.a). The Store Keeper also stores the get to methodologies of the photo in the Policy Store (Step iii.b). Once an Image User expects that the Cloud Server will deal with any photo, its client module Access Requester gets its information (Step 1). The module Access Requester surveys the scaling and altering parameters and advances the request to the Access Request Processor module of the Cloud Server (Step 2). In the request, the Access Requester sends picture scaling/trimming parameters, (for instance, scaling segment and in addition altering ROI) and customer capability (which can be anonymized) to the Access Request Processor. The Access Request Processor at first plays out a customer endorsement arrange by sending a get the chance to request to the Access Manager (Step 3). The Access Manager gets the get to methodologies for the requesting customer from the Policy Store (Step 4) and it organizes the get to approaches against the get the chance to inquire. Finally, the get to response is sent back to the Access Request Processor (Step 5). If the customer is endorsed to play out the requested operation, the Image Processor is invoked with scaling/altering parameters as wellsprings of data (Step 6). The requested picture is recuperated from the Image Store (Step 7) and the Image Processor performs scaling/trimming on the mixed picture. Right when the scaling/trimming operations are done, the dealt with picture is sent to the Access Request Processor (Step 8). The Access Request Processor plays out the first round of unraveling on the dealt with picture using the key identifying with the Image User and sends the photo to the Access Requester module (Step 9). The Access Requester module on the Image User plays out a minute round of interpreting and exhibits the readied picture to the Image User (Step 10).

6. MODULES

Image Outsourcer
Cloud Server
Image User
Key Management Authority (KMA)

MODULES DESCRIPTION

1. Image Outsourcer

This element outsources the putting away and preparing (i.e., scaling and trimming) of pictures to an outsider cloud supplier. It could be an individual or an association, for example, a healing facility. In the last case, a few clients can go about as an Image Outsources. Regularly, this substance possesses the picture. An Image Outsourcer is in charge of tending to security and protection concerns connected to picture outsourcing. To accomplish this, the Image Outsourcer encodes the picture before sending it to the cloud datacenter.

2. Cloud Server

It is the piece of framework given by a cloud specialist co-op, for example, Amazon S31, for putting away and preparing pictures. It stores encoded pictures and get to arrangements used to direct access to the pictures. In the wake of making approval checks, it recovers an asked for picture from its picture store. In the event that the get to ask for fulfills get to arrangements, it scales or potentially trims pictures in an encoded way, i.e., without unscrambling them.

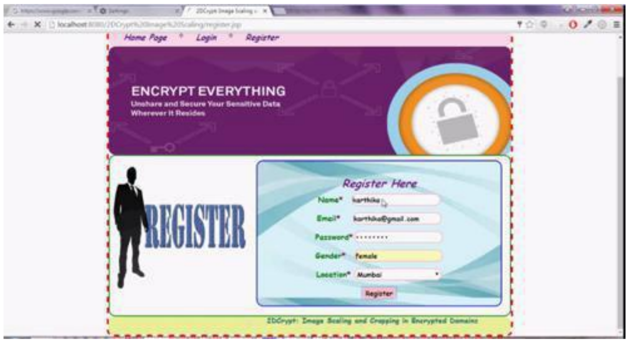
3. Image User

It is approved by the Image Outsourcer to get to the asked for picture put away in an encoded frame on the Cloud Server. Contingent upon approval, an Image User can issue either read demand or process ask for (i.e., scaling and trimming operations). In both cases, the Image User unscrambles the picture returned by the demand. Take note of that in a multi-client setting, (i) an Image User can alter a picture that will be available by other Image Users, or (ii) an Image User can get to pictures handled by other Image Users. In both cases, Image Users don't have to share any keying material.

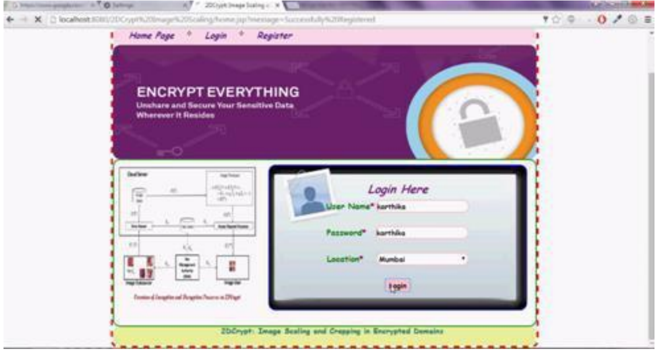
4. Key Management Authority (KMA)

It produces and repudiates keys. It creates a customer and server key combine for every client, be it an Image Outsourcer or Image User. The customer and the server side keys are safely transmitted to the client and the Cloud Server, separately. At whatever point required (say in key lost or stolen cases), the KMA disavows the keys from the framework with the support of the Cloud Server.

7.PERFORMANCE EVALUATION

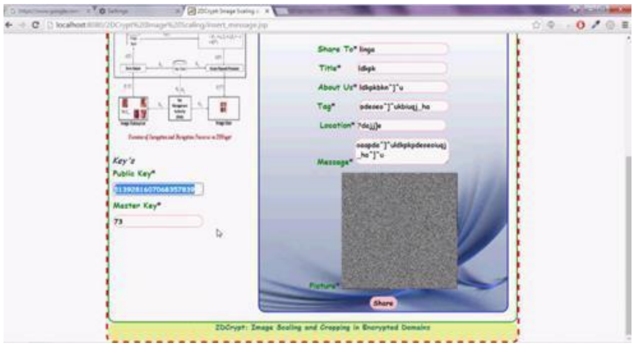

Home Page
Login
Register
ENCRYPT EVERYTHING
Unshare and Secure Your Sensitive Data
Wherever It Resides
REGISTER
Register Here
Register
2DCrypt: Image Scaling and Cropping in Encrypted Domains

Name* karthika
Email* karthika@gmail.com
Password* ••••••••
Gender* female
Location* Mumbai


Home Page
Login
Register
ENCRYPT EVERYTHING
Unshare and Secure Your Sensitive Data
Wherever It Resides
Login Here
Login
2DCrypt: Image Scaling and Cropping in Encrypted Domains

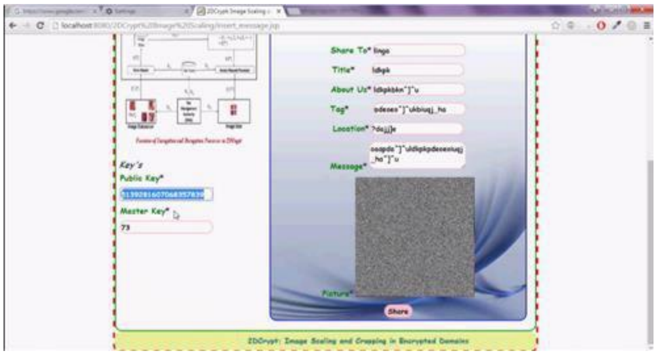
User Name* karthika
Password* karthika
Location* Mumbai

Figure 7.2 : Login Page for User



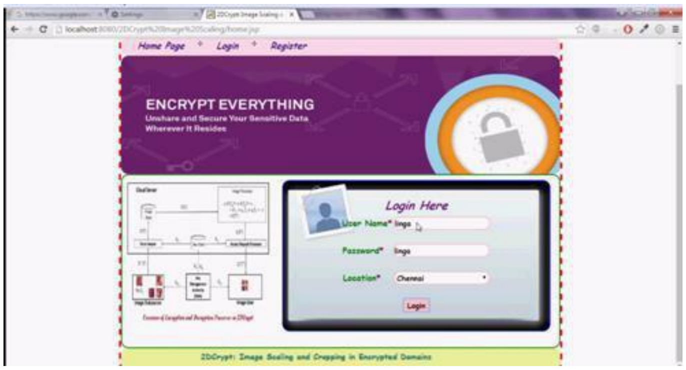
Public Key* 1139281607068357839
Master Key* 73
Share To* lingo
Title* ldkpk
About Us* ldkpkbkn"]"u
Tag* odeoes"]"ukbiuqj_ho
Location* ?dejjj]e
Message* oapdo"]"ukdkpkpdeoeoiuqj_ho"]"u

Figure 7.3 : Upload Encrypt image and text



Public Key* 1139281607068357839
Master Key* 73
Share To* lingo
Title* ldkpk
About Us* ldkpkbkn"]"u
Tag* odeoes"]"ukbiuqj_ho
Location* ?dejjj]e
Message* oapdo"]"ukdkpkpdeoeoiuqj_ho"]"u

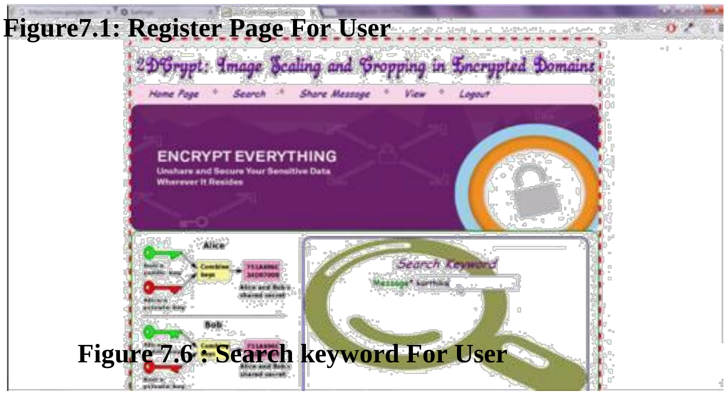
Figure7.4 : Using Public key For Send Encrypt Image and Text


Home Page
Login
Register
ENCRYPT EVERYTHING
Unshare and Secure Your Sensitive Data
Wherever It Resides
Login Here
Login
2DCrypt: Image Scaling and Cropping in Encrypted Domains

User Name* lingo
Password* lingo
Location* Chennai

Figure 7.5: Loign Page For User

Figure7.1: Register Page For User



2DCrypt: Image Scaling and Cropping in Encrypted Domains

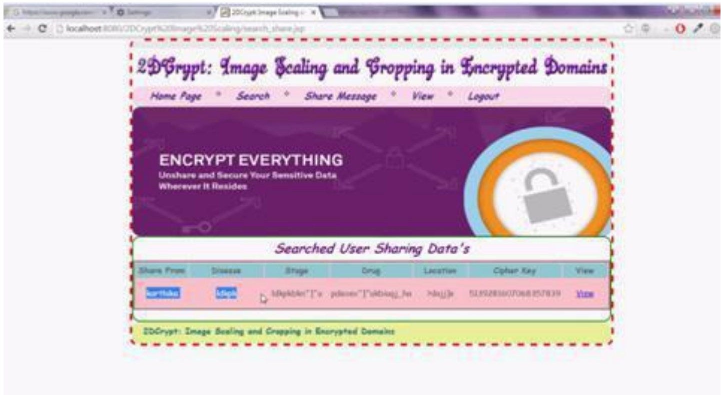
Home Page • Search • Share Message • View • Logout

ENCRYPT EVERYTHING
Unshare and Secure Your Sensitive Data
Wherever It Resides

Search Keyword

Message* karthika

Figure 7.6 : Search keyword For User



2DCrypt: Image Scaling and Cropping in Encrypted Domains

Home Page • Search • Share Message • View • Logout

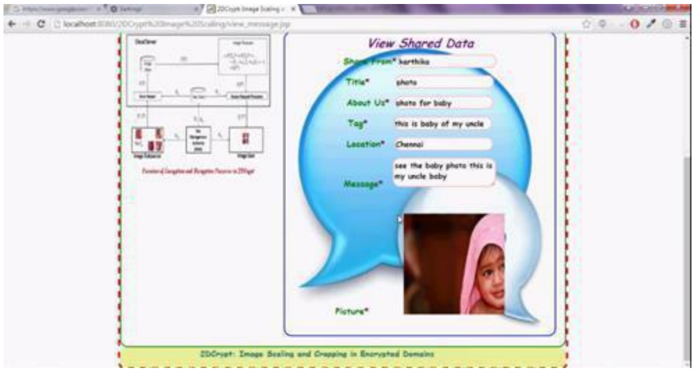
ENCRYPT EVERYTHING
Unshare and Secure Your Sensitive Data
Wherever It Resides

Searched User Sharing Data's

Share From	Disease	Stage	Drug	Location	Cipher Key	View
karthika	ldlqyk	ldlqkbkn"]"u	pdaoeo"]"ukbiajj_hn	>lduj|e	513928160706835783[illegible]	View

2DCrypt: Image Scaling and Cropping in Encrypted Domains

Figure 7.7 : Page For Searched User Sharing Data's



View Shared Data

Share From* karthika

Title* photo

About Us* photo for baby

Tag* this is baby of my uncle

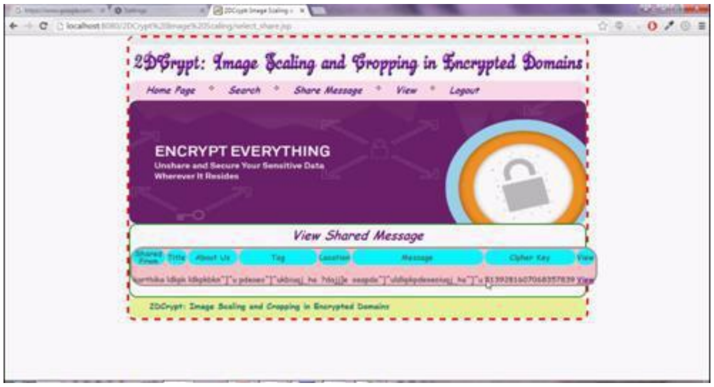
Location* Chennai

Message* see the baby photo this is my uncle baby

Picture*

2DCrypt: Image Scaling and Cropping in Encrypted Domains

Figure 7.8 : View Shared Data



2DCrypt: Image Scaling and Cropping in Encrypted Domains

Home Page • Search • Share Message • View • Logout

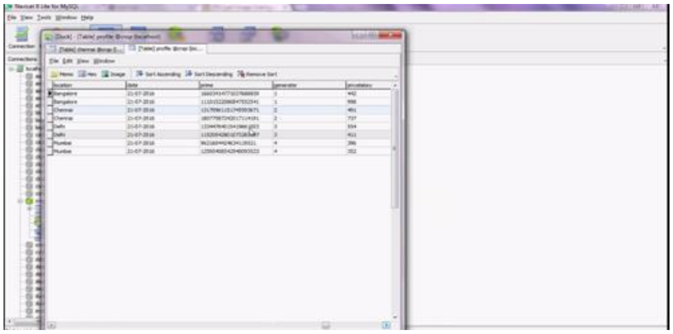
ENCRYPT EVERYTHING
Unshare and Secure Your Sensitive Data
Wherever It Resides

View Shared Message

Share From	Title	About Us	Tag	Location	Message	Cipher Key	View
karthika	ldlqyk	ldlqkbkn"]"u pdaoeo"]"ukbiajj_hn	>lduj|e	[illegible]	[illegible]	513928160706835783[illegible]	View

2DCrypt: Image Scaling and Cropping in Encrypted Domains

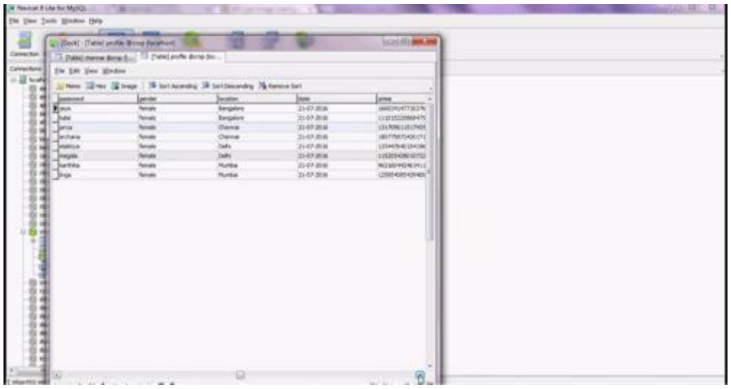
Figure 7.9 : View Shared Message



Navicat 8 Lite for MySQL

location	date	prime	generator	privatekey
Bangalore	21-07-2016	[illegible]	1	442
Bangalore	21-07-2016	[illegible]	1	998
Chennai	21-07-2016	[illegible]	2	461
Chennai	21-07-2016	[illegible]	2	737
Delhi	21-07-2016	[illegible]	3	554
Delhi	21-07-2016	[illegible]	3	411
Mumbai	21-07-2016	[illegible]	4	396
Mumbai	21-07-2016	[illegible]	4	352

Figure 7.10 : List Of User's



Navicat 8 Lite for MySQL

password	gender	location	date	prime
[illegible]	female	Bangalore	21-07-2016	[illegible]
[illegible]	female	Bangalore	21-07-2016	[illegible]
[illegible]	female	Chennai	21-07-2016	[illegible]
[illegible]	female	Chennai	21-07-2016	[illegible]
[illegible]	female	Delhi	21-07-2016	[illegible]
[illegible]	female	Delhi	21-07-2016	[illegible]
karthika	female	Mumbai	21-07-2016	[illegible]
[illegible]	female	Mumbai	21-07-2016	[illegible]

Figure 7.11 : List of User names and public keys

8. CONCLUSION

Cloud-based picture handling has information secrecy issues, which can prompt security misfortune. In this paper, we tended to this issue by proposing 2DCrypt, an adjusted Paillier cryptosystem-based plan that enables a cloud server to perform scaling and editing operations without taking in the picture content. In 2DCrypt, clients don't have to share keys for getting to the picture put away in the cloud. In this manner, 2DCrypt is appropriate for situations where it is not attractive for the picture client to keep up per-picture keys. Besides, 2DCrypt is more down to earth than existing plans in view of Shamir's mystery sharing since it neither utilizes more than one datacenter nor expect that numerous enemies could intrigue by getting to a specific number of datacenters. To make 2DCrypt down to earth, we propose a few upgrades to diminishing overheads come about because of the use of the adjusted Paillier cryptosystem. To start with, we proposed a space proficient tiling plan that enables the cloud to perform per-tile operations. In 2DCrypt, we put various pixels in a tile, and encode the tile as opposed to scrambling every pixel freely. Besides, we upgraded the changed Paillier plan to point of confinement its stockpiling necessity. Because of these upgrades, 2DCrypt requires around 40 times less distributed storage than the credulous per-pixel encryption. The computational overhead is additionally fundamentally decreased in light of less encryptions and decodings rounds. The correct computational overhead and the information

required by the picture client, be that as it may, are subject to the picture estimate and the client's scaling and editing parameters. For instance, when a 512 _ 512 picture is scaled by a component of two, the client needs around 5:3 times a larger number of information and works 2:3 seconds more than the ordinary handling. We trust that 2DCrypt can be stretched out in different ways. A conspicuous course is to amplify this work for compacted pictures. Another approach can be utilizing our thought for tending to security issues in more specific pictures, for example, histopathology pictures and G.I.S maps. It will be fascinating to examine on the off chance that we can use properties of these particular pictures to further diminishing overheads. Another conceivable future work can be extending our work to video preparing in scrambled spaces

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] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, pp. 612–613, 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 & 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.

[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. 1:1–1:12, 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. 421–427.

[9] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image and Vision Computing, vol. 24, pp. 926– 934, 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. 125–141, February 2014.

[11] C.-Y. Hsu, C.-S. Lu, and S.-C. Pei, "Image feature extraction in encrypted domain with privacy-preservingSIFT," IEEE Transactions on Image Processing, vol. 21, no. 11, pp. 4593–4607, 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. 2083–2091.

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

[14] S. Goldwasser and S. Micali, "Probabilistic encryption," Journal of Computer and System Sciences, vol. 28, no. 2, pp. 270–299, 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. 544–553.

[16] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, pp. 120–126, February 1978.

[17] 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. 10–18.

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

[19] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology-Eurocrypt, 2004, pp. 506–522.

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

[21] 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. 77–88.

[22] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, "Privacy-preserving face recognition," in Privacy Enhancing Technologies. Springer, 2009, pp. 235– 253.

[23] A.-R. Sadeghi, T. Schneider, and I. Wehrenberg, "Efficient privacypreserving face recognition," in Information, Security and Cryptology– ICISC 2009. Springer, 2010, pp. 229–244.

[24] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich, "SCiFI – A system for secure face identification," in IEEE