

Securely Performing Operations on Images using PSNR

Miss. Kalyani J. Patil¹, Namrata D. Ghuse²

¹PG Student, SPPU, SITRC, Nashik-422213, India

²Assistant Professor, SITRC, Nashik-422213, India

Abstract - Cloud computing is term where huge number of frameworks are associated together that give progressively adaptable foundation to different applications putting away all kind of information. It is a developing innovation where the administrations like stage as a help, programming as an assistance and framework as an assistance are given. A new business module defines a structure where the outsourcing of image storage and its processing is done. This processing increases the size of the images up to an remarkable extent. The present framework that is 2DCrypt strategy, depends on the changed Paillier cryptosystem. In this framework editing and scaling tasks are performed without knowing the substance of the picture. At the end of the day, this framework thinks about the tile of pixels for encryption, not at all like other picture encryption strategies considering every pixel independently. Another restriction of the current framework is information repetition. This impediment demonstrates to be overwhelming and influences the presentation of the present framework. The proposed framework empowers cloud server farm to perform activities, for example, scaling and trimming over scrambled picture by utilizing Shamir Secrete calculation. This calculation gives Token to security reason which can be utilized for a particular timeframe. Such utilization of tokens helps in lessening the restrictions of the current framework up to a critical dimension. Also, make discharge keys to share the information to others for perform tasks.

Key words—Cropping, Encrypted Scaling, Hidden Image Processing, Image Outsourcing and Paillier Cryptosystem

1. INTRODUCTION

Cloud computing is the technology that provides different services to the users and these services are Users have to pay for the services depending upon the usage that is pay as you use model. Cloud is fundamentally a bunch of thing PCs composed together in same or distinctive geological regions, cooperating to serve different customers with different need and workload on re-journey preface with the help of virtualization. Circulated processing implies con-trolling, orchestrating, and getting to the gear and programming resources remotely. We can access the data or services from anywhere at any time. Many cloud storage services are available such as Box, DropBox, SkyDrive, Sugarsync for individual and small to medium business. The

confidentiality of outsourced image is protected by using the nave approach. The image is encrypted before it is stored in the cloud. The system has a problem that it is not possible to perform basic operations on pictures, such as zooming and trimming. To save secrecy, operations are performed over encoded pictures. 2DCrypt procedure concentrate on powerful scaling and editing operations on scrambled pictures. These tech-nology can be used to implement scaling and resizing of image, which can be applied on large image. By using this technique no data contained in the pictures can be spilled to the cloud servers, and in the meantime, clients can completely misuse the cloud display. 2DCrypt is a cloud-based multi-customer picture scaling and editing system and it relies upon Paillier cryptosystem[1]. The calculation over encoded information is carried out homomorphic encryption. The right now accessible completely homomorphic encryption plot [10] is not calculation partner down to earth. Along these lines, fractional homomorphic encryption plots, those supporting certain operations over scrambled information, are commonly utilized for useful arrangements. In light of fractional homomorphic Shamirs mystery sharing [21], two principle look into works perform picture scaling and trimming operations in the scrambled space [6], [2].

These methodologies experience the ill effects of two prin-ciple: (I) for each picture, n shares are made and transferred to the cloud, which increment the measure of capacity required and additionally the preparing power and (ii) this approach is not collusion resistant: if k data centers collude then the original image can be retrieved. The utilization of cryptosys-tem for concealing pictures is a very much examined range. Various methodologies, including however are not constrained to, Open Key Cryptosystem (PKC) [11], watermarking [9], Shamirs mystery sharing [15] and confusion based encryption [12], is used to secure images. To permit cloud data centers to perform operations on the scrambled picture, halfway homomorphic cryptosystem based solutions have been proposed [4][3]. A fractional homomorphic cryptosystem solely offers either expansion or augmentation operations. Paillier [17], Shamirs mystery sharing [21] are among in part homomorphic cryptosystem that help expansion. The Paillier cryptosystem is homomorphic to augmentations

and scalar increases [13] and can be changed to an intermediary encryption scheme [13], [5].

1.1 Objectives

- To provide the protection to an image by generating a token.
- To improve the efficiency of the system by avoiding the data duplication on cloud.

2. LITERATURE SURVEY

- I. Manoranjan Mohanty, Muhammad Rizwan Asghar, and Giovanni Russello [1] used some techniques such as, 2DCrypt, Paillier, Tiling, Shamirs secret sharing, Homomorphic Encryption Scheme. Using Paillier technique, scaling and cropping operation is done on encrypted data. To overcome space efficient issues, the system uses tiling scheme.
- II. Mrs. Jadhav Rohini, Prof. S. A. Kahate [2] used Paillier cryptosystem, Public Key Cryptosystem (PKC), watermarking, Shamirs secret sharing chaos based encryption. Watermarking is the major applications in image data hiding. Watermarking use cover multimedia to conceal the secret data.
- III. Wenjun Lu1, Avinash L. Varna [4] Used Additive Homomorphic Encryption, Fully Homomorphic Encryption, Secure Min-Hash Secure Inverted Index. It keeps up the inquiry precision of plaintext highlights and offers randomized encryption with the goal that the server can't get separate between encoded includes specifically. It is exceptionally proficient and requires least client inclusion. The hunt precision and confidentiality security offered by include/record randomization are near that of homomorphic encryption scheme.
- IV. Rohini, B. S. Kurhe [5] uses Shamirs secret sharing, Paillier-based cryptosystem, Public Key Cryptosystem Watermarking schemes. These all techniques are is to security images. Using Paillier scheme, scaling and cropping operation is done on encrypted data. To overcome space efficient issues, the system uses tiling scheme.
- V. Kshitij Kansal, Manoranjan Mohanty, and Pradeep K. Atrey has proposed wavelet-based compressed image scheme is highly secure and has acceptable computational and data overheads.
- VI. Gul Calikli [8] describes the number of active users on social network is increases day by day as the use of OSN has grown, privacy violation due to inappropriate sharing of information on social sites the privacy of user has been violated.

- VII. Jadhav Rohini, Prof.S. A. Kahate [7] used 2DCrypt technique. 2DCrypt technique divides in to two scheme such as paillier and Tile level. Using Paillier scheme, scaling and cropping operation is done on encrypted data. To overcome space efficient issues, the system uses tiling scheme.
- VIII. Scale-invariant feature transform PPSIFT scheme is described by [11]. Privacy-preserving Scale-invariant feature transform is secure against ciphertext as well as plaintext attack. This scheme has been solved the most challenging problem, i.e., homomorphic comparison. Searchable symmetric encryption order-preserving symmetric encryption schemes is implemented in [12]. In this paper, the problem of secure ranked keyword search over encrypted cloud data is solved. This paper gives as-strong-aspossible security guarantee compared to previous SSE schemes.
- IX. Muhammad Rizwan Asghar [13] used multi-user encrypted search scheme. This method work on multiple users encrypted search method on encrypted database. SQL support encrypted queries. When data is stored on cloud gives access control perform administrative actions. There is no need of redistribution of keys or re-encryption of data. There is a method to protect sensitive user data.

2.1 Comparative Study

In this section we will study overall comparison between existing system and proposed system. In previous systems there are some drawbacks let us discuss one by one. In this paper this drawback are remove. Studying previous papers in that the private keys are share to third party for accessing the data. But the third party use these keys multiple times. So that data has no privacy at all. Any time user can access this private data or he can use our private data for wrong way. These drawback remove in this paper. In previous papers there were duplicate data can be occur. So that efficiency of the system can be less. And the system can work slowly. In that system more space can be required. But in this paper improving the efficiency of the system by avoiding the data duplicating on cloud.

2.2 SYSTEM ARCHITECTURE

2.2.1 Problem Statement

To develop a system that protect the sensitive data while enabling outsourced image services. The system enables cloud data center to perform operations such as

scaling and cropping over encrypted image security providing as token that is One Time Password (OTP). The system increases performance of various applications and reduce storage space by using tiling scheme.

2.2.2 System Overview

The main goal of this system is to performing scaling and cropping operation over encrypted images by using 2DCrypt technique. The 2DCrypt techniques including two schemes such as Paillier Cryptosystem and Tiling scheme. In the exist-ing system the data duplication is created, to overcome these drawback the proposed system use Shamir Secret algorithm.

2.2.3 Working

2DCrypt technique is based on Paillier cryptosystem. In this technique, for each user that is an Image Outsourcer or Image User, the KMA creates two keys combines by arbitrarily part the ace mystery enter into two sections: the client side key sent to the client and the server side key conveyed to the server. The Image Outsourcer stores a picture and its entrance approaches in the cloud server. The Vendor isolates the picture into various tiles and performs per tile encryption. At the Cloud Server-end, the Vendor plays out the second round of encryption using the server-side key co responding to the customer, and stores the mixed picture in a image store. A Picture Outsourcer is responsible for watching out for security and insurance concerns joined to picture outsourcing. The Picture Outsourcer encodes the photo before sending it to the cloud server cultivate. The Picture Outsourcer can store new pictures on a cloud server, revive and modify existing ones, and regulate get the opportunity to control courses of action to guide access to the photos set away on the cloud server. Cloud Server is the piece of framework gave by a cloud specialist co-op, for putting away and handling pictures.

It stores encoded pictures and access approaches used to direct access to the pictures. It stores encoded pictures and access approaches used to manage 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 passage request satisfies get to approaches, it scales and moreover trims pictures scrambledly, that is without unraveling them Picture Client is endorsed by the Picture Outsourcer to get to the requested picture set away in an encoded shape on the Cloud Server. A picture client can issue either read demand or process ask for relying upon approval.

Key Management Authority generates keys. It generates a client and server key pair for each user, be it an Image Outsourcer or Image User. The client and the server side keys are securely transmitted to the user and the cloud Server, respectively. The user- side key send to the user and the server-side key send to the server. In Token Time stamp Generation, the system generate an token that means one time password used to security purpose for a specific time period. In Token base Authorization, unique token is given to particular user for security purpose. If the token get match then and then user can access or update or modify the data. The asked for picture is recovered from the Image Store and the Image Processor performs scaling or editing on the scrambled picture. At the point when the scaling or trimming activities are finished, the picture is sent to the Access

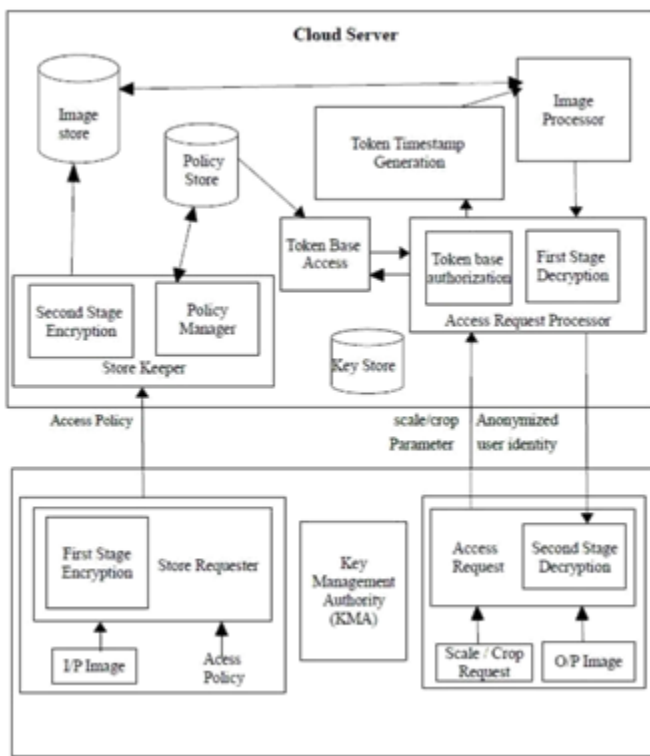


Fig. 1. Architecture of System

Figure 1 shows the architecture of 2DCrypt. 2DCrypt technique is a cloud-based multi-client picture scaling and editing framework. This technique depends on Paillier cryptosystem. The storing and processing of image is outsourced to the third party cloud provider by using this entity. It could be an individual or an association, for example, a hospital center. In the last case, a few clients can go about as an Image Outsourcer. Cloud Server is the part of infrastructure provided by a cloud service provider. It stores encrypted images and access policies used to regulate access to the images. It separate an asked for picture from its picture.

Request Processor. The Access Request Processor plays out the first round of encryption on the prepared picture utilizing the key relating to the Image User and sends the picture to the Access Requester module.

3. METHODOLOGY

3.1 Algorithm

The algorithm used for proposed framework is as follows: Key Generation Algorithm, Shamir Secret Sharing Algorithm, Hash Key Algorithm.

1) **Key Generation Algorithm:** In cryptography, encryption

Is the way toward encoding a message or data such that exclusive approved gatherings can get to it and the individuals who are not approved can't. In an encryption conspire, the proposed data or message, alluded to as plaintext, is scrambled utilizing an encryption calculation a figure producing ciphertext that must be perused if decoded. An encryption plot ordinarily utilizes a pseudo irregular encryption key created by a calculation.

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 $[1, n/2]$. Then it calculates $x_{i2} = x_{i1}$, and transmit.

The server adds K_{S_i} to the Key Store as follows: $K_{S_i} K_{S_i}$.

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 of size n , the user client chooses e_1, e_2 , a random r from $[1, n/4]$.

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 reencrypted ciphertext $E(D) = (e_1, e_2)$. Step 5: ServerSum($E(D_1), E(D_2)$). Given two encrypted values $E(D_1) = (e_{11}, e_{12})$ (where $e_{11} = g^{r_1}$ and $e_{12} = g^{r_1 x_{i1} \cdot (1 + D_1 n)}$) and $E(D_2) = (e_{21}, e_{22})$ (where $e_{21} = g^{r_2}$ and $e_{22} = g^{r_2 x_{i2} \cdot (1 + D_2 n)}$), the server calculates the encrypted sum $E(D_1 + D_2) = (e_1, e_2)$.

2) Shamir Secret Sharing Algorithm: Secret sharing is a strategy for securing delicate information, for example, cryptographic keys. It is utilized to disperse a mystery incentive to various parts shares that must be consolidated together to get to the first esteem. Mystery sharing is utilized as a part of present day cryptography to bring down the dangers related with bargained information. The first mystery sharing plans were proposed by Shamir and Blakley.

Definition: Let s and t be two values and $[s] = [s_1, \dots, s_n]$ and $[t] = [t_1, \dots, t_n]$ be their shares. A secret sharing scheme is $(\mathcal{L}, \mathcal{E})$ - homomorphic if shares $[(s_1, t_1), \dots, (s_n,$

$t_n)]$ uniquely determine the value s and t . Data : Input file S to share.

Result: Three Shares S_1, S_2, S_3 of same size as the original file. Choose a field Z_p where $p = 257$.

while not at end of the input file do

$s = \text{read byte}(S)$ // read a byte or pixel if $s == 0$ then $s = 256$
end

$a = \text{sp}^{1/3}$ // find cube root of s

$r = \text{random}(257)$ // random number between 0-256 $s_1 = r \bmod p$ // s_1 is the share1 pixel

if $s_1 == 256$ then $s_1 = 0$ end

$s_2 = r^2 \bmod p$ // s_2 is the share2 pixel if $s_2 == 256$ then $s_2 = 0$ end

$s_3 = r^4 \bmod p$ // s_3 is the share3 pixel if $s_3 == 256$ then

$s_3 = 0$ end end

3) **Hash Key Algorithm:** A hash work is a scientific capacity that changes over a numerical information value into another compacted numerical value. The contribution to the hash work is of subjective length however yield is dependably of settled length. Hash work use for the secret word.

The Secure Hash Algorithms are a family of cryptographic hash functions. It works by changing the information utilizing a hash work: a calculation that comprises of bitwise activities, measured increases, and pressure capacities. The hash work at that point creates a xed estimate string that looks not at all like the first. These calculations are intended to be one way works, implying that once they are changed into their individual hash esteems, its essentially difficult to change them over into

the first information. A couple of calculations of intrigue are SHA-1, SHA-2, and SHA-5, each of which was progressively composed with progressively more grounded encryption in light of programmer assaults. SHA-0, for in-position, is currently out of date due to the

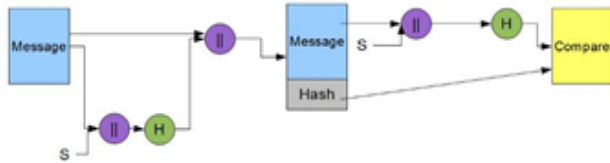


Fig. 2. Basic Hash Function

4. PSNR Algorithm

Peak Signal noise Ratio

PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic scale.

PSNR is most easily defined via the mean squared error (*MSE*). Given a noise-free $m \times n$ monochrome image *I* and its noisy approximation *K*, *MSE* is defined as:

The PSNR (in dB) is defined as:

Here, MAX_i is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. More generally, when samples are represented using linear PCM with *B* bits per sample, MAX_i is 2^{B-1} .

3.2 PROBLEM FORMULATION

Mathematical Model

Let system *S* can be dened as, $S=I,O,K,P,Eo,Ev, Scale,Crop$
 $I=$ Set of Input images $I=I1,I2,I3,.....,In$

$O=$ Set of Output images $O=O1,O2,O3,.....On$

$k=$ Set of user/server keys
 $K=(Uk1,Uk2,....Ukn)(Sk1,Sk2,....Skn)$

$E0=$ Set of image outsources Encryption Images

$E0=E01, E02,....E0n$

$n=$ Number of Images

$Es=$ Set of image Encryption on cloud server

broadly uncovered vulnerabilities. A regular utilization of SHA is to scrambling passwords, as the server side just needs to monitor specie clients hash esteem, as opposed to the real watchword. Figure shows hash function diagram.

$Es=ES1, ES2,.... Esn$

Function f1- function f1 generate user side and server side Encryption key

$f1()- (Uk1,Uk2,....Ukn)(Sk1,Sk2,....Skn) (UK,SK)$

function f2- function f2 read Imge from image outsources and perform per tile encryption.

$f2(I)- I1,I2,I3,.....,In-(E(I1)Uk1, E(I2) Uk2) E0$

$f3(I)- (I1,I2,I3,.....,In)- (P1,P2,P3,....PN) p$

function f4- This function read Encrypted outsources Image data and perform server side encryption.

$f4(E0)- (E(I1)Uk1, E(I2) Uk2)Sk1 E(E(I2)Uk2)Sk2 ES$

function f5- This function read Image Scaling / Cropping parameters and perform operations

function f5(Scale, Crop)- $(ES (I), Scale, Crop)- (O1,O2,O3,....On) 0$

function f6- This function apply server-user key on output and decrypt Image

$f6(Sk,0)-((O1)Sk1 (O2)Sk2)- (E11,E12)$

function f7- This function apply user key on decrypted Image to get back normal Image

function f7($E11,Uk$)- $(E(I1)Uk1, E(I2) Uk2,.....)$

$I=$ set of output scale/ crop Image.

4. RESULT ANALYSIS

We tested the time consumption of first, second encryption and Image cloud upload Time under different Image size. Following table shows the result of experiments of first, second encryption and upload time. From this table, it is easy to see that the time consumption of all functions grows large with the increase of image size.

Image Size	First Stage Encryption(Time in Seconds)	Second Stage Encryption(Time in Seconds)	Upload Time(Time in Seconds)
400*400	125	652	152
600*600	478	952	852
1000*1000	785	1589	1252
1200*1200	2587	8658	2585

Fig. 3. Result Table

The figure shows the graph of the result analysis of the system

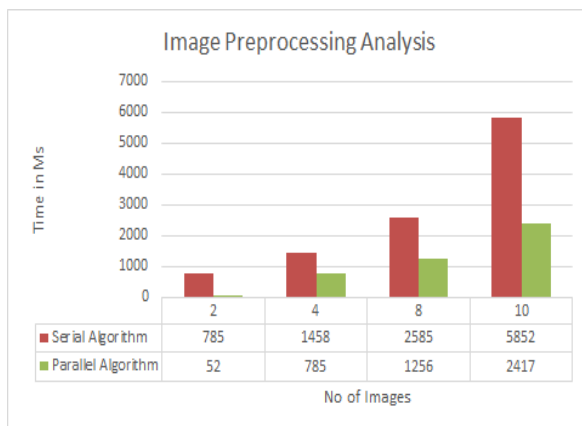


Fig. 4. Result Analysis

Analysis of PSNR

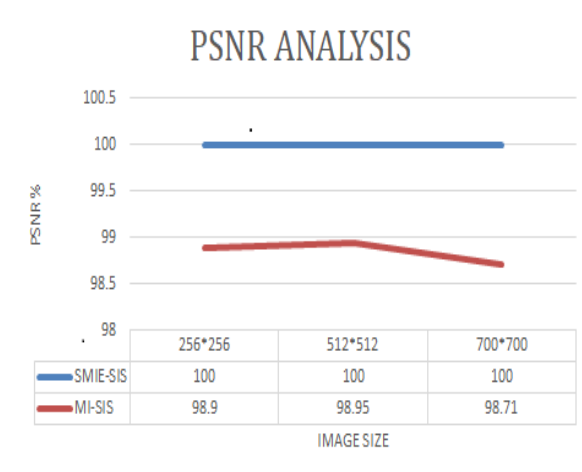
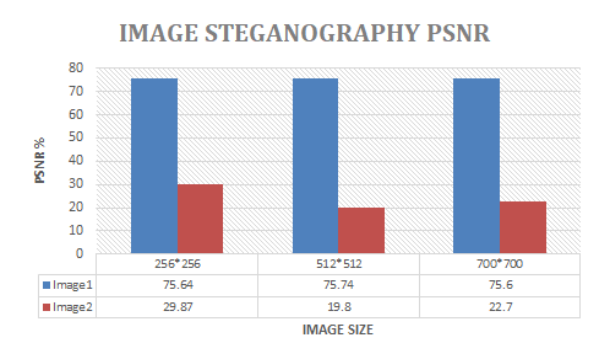


Image Steganography PSNR



4. CONCLUSIONS

The secure and efficient secret image sharing scheme using sharing matrix, image encryption and steganography(SSME-SIS) is resilient to protect different types of images including binary, grayscale and color images. It has advantages such as a low computation cost, original image reconstruction, a low storage and transmission costs, etc. The security analysis including theoretical and experimental demonstration shows that the system has a high level of security to tolerate various attacks and a verification function to detect the fake shares. We are further going to implement multiuser image sharing by using hierarchical tree cryptography. The SSME-SIS uses steganography to combine two images ultimately increasing the security to one level along with allowing the user to share two images at a time.

Further the SSME-SIS can be developed to combine multiple images at a time in order to share them. Also various GUIs can be used to decrease the computation cost. The parallel processing can be used by implementing the technology such as openMP.

ACKNOWLEDGMENT

I would sincerely like to thank our Head of Department Prof. (Dr.) Amol D. Potgantwar, Computer Engineering, and Professor Namrata D. Ghuse, Department of Computer Engineering, SITRC, Nashik for their guidance, encouragement and the interest shown in this project by timely suggestions in this work. His expert suggestions and scholarly feedback had greatly enhanced the effectiveness of this work.

5. REFERENCES

[1] Manoranjan Mohanty, Muhammad Rizwan Asghar and Giovanni Rus-sello, 2DCrypt: Image Scaling and Cropping in Encrypted Domains, IEEE Transaction on Information Forensics and Security, 2016.

- [2] Mrs. Jadhav Rohini 1, Prof. S. A. Kahate, A Survey on: A Modified Paillier Cryptosystem-Based Image Scaling and Cropping Scheme, IJARIE, 2016.
- [3] K. Kansal, M. Mohanty, and P. K. Atrey, Scaling and cropping of wavelet-based compressed images in hidden domain, International Conference on Multimedia Modeling, vol. 8935, pp. 430441, 2015.
- [4] J. Yuan, S. Yu, and L. Guo, SEISA: Secure and efficient encrypted image search with access control, in IEEE Conference on Computer Communications, pp. 20832091, 2015.
- [5] 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.
- [6] Jadhav Rohini, B. S. Kurhe, Two Dimensional Cryptography Using Modified Paillier Cryptosystem, International Journal of Innovative Research in Computer and Communication Engineering, May 2017.
- [7] Mrs. Jadhav Rohini, Prof.S.A.Kahate, Image Scaling and Cropping Scheme using Two Dimensional Cryptography, International Journal of Research in Advent Technology (IJRAT), February 2017.
- [8] 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. 120126, February 2016.
- [9] Jiawei Yuan*, Shucheng Yu*, Linke Guoy, SEISA: Secure and Efficient Encrypted Image Search With Access Control, IEEE Conference on Computer Communications (INFOCOM), 2015.
- [10] 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.