International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

XOR Reformed Paillier Encryption Method with Secure De-duplication for Image Scaling and Cropping in Reduced Cloud Storage

Chellan Edward Jaya Singh[1]* **Eppies Baburaj[2]**

[1]*Department of Computer Science, Research & Development Centre, Bharathiar University, Coimbatore, India*
[2]*Department of Computer Science & Engineering, Mariyan Engineering College, Trivandrum, India*
* Corresponding author's Email: cedwardjs1212@gmail.com

Abstract: In this modern world, most of people are using cloud computing due to its accessibility. Users are uploading plenty of images to the cloud every day. But still, data confidentiality is the major issue for the cloud storage. This paper proposes a new method of image encryption scheme with less storage in the cloud. The proposed method performs double encryption with de-duplication over the images for better security and also reduces the storage overhead problem using the scaling and cropping operation. In the first level, the modified Paillier encryption technique is used and an XOR encryption takes place in the second phase. After that, a secure block-level image de-duplication technique is performed to eliminate the identical images and protect the image confidentiality. The simulation result exhibits that the proposed encryption with secure de-duplication outperforms other state-of-art approaches with respect to the performance metrics like accuracy, sensitivity, specificity, encryption quality and runtime. In terms of accuracy, the performance of proposed method is better of 8.1%, 7.2%, and 6.1% for image 1, 10.2%, 7.1%, and 6.1% for image 2, 8.4%, 6.2%, and 5.8% for image 3, and 8.3%, 6.2%, and 5.6% for image 4 when compared with other three existing research works.

Keywords: Cloud Storage, Paillier encryption, Cropping, Scaling, XOR encryption, De-duplication.

1. Introduction

Cloud computing is Internet-based computing which provides sharing the resources and data to the computers and other devices. It is a model for enabling ubiquitous, on to a shared pool of configurable data resources (e.g., computer networks, servers, storage, applications, and services) which can be rapidly provisioned and released with minimal management effort. Cloud computing allows the users and enterprises with various capabilities to store and processes their data in either privately owned cloud, or on a third-party server in order to make data accessing mechanisms much more comfortable and reliable. Data centers, which is located far from the user ranging in distance from across a city to across the world. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over an electricity network. Advocates claim that cloud computing allows companies to avoid upfront infrastructure costs (e.g., purchasing servers). As well, it enables organizations to focus on their core businesses.

Instead of spending time and money on the infrastructure of computer. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables information technology (IT) teams to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud providers typically use a "pay as you go" model. This will lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model.

In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it [1-4]. Encryption does not itself prevent interference, but denies the intelligible content. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm [5], generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudorandom encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users. The use of cryptosystems for blind images is a well-studied area [6-8]. 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. The Paillier cryptosystem [9] invented a probabilistic asymmetric algorithm for a public key cryptography [10, 11]. The problem of computing n^{th} residue classes is believed to be computationally difficult. Diffie - Eellman key distribution scheme that achieves a public key cryptosystem relies on the difficulty of computing discrete logarithms over finite fields [12]. Digital image blind watermark scheme is applied to the K-L transform scheme [13].

The original color image is encoded into three-phase masks by using the Gerchberg–Saxton iterative phase retrieval algorithm with another predefined phase key [14]. The image encryption algorithm is based on the bit plane principle [15]. Privacy envisioned that secure media applications with privacy preservation will be treated seriously [16]. XOR operation is computationally inexpensive. A simple repeating XOR (i.e. using the same key for XOR operation on the whole data) cipher is therefore sometimes used for hiding information in cases where no particular security is required. One of the important data compression techniques for eliminating duplicate copies of repeating data is called data de-duplication. In the literature, most of the work is based on computing the hash of the entire image at once, instead of converting the images into blocks. So, the breaking down of images into smaller structures like blocks by considering the blocks features and then performs de-duplication at each level of the block will significantly help to achieve a more accurate method for de-duplication. This paper proposes a new method of image encryption scheme with less storage in the cloud. The proposed method performs double encryption with de-duplication over the images for better security. After that, a secure block-level image de-duplication technique is performed to eliminate identical images and protect image confidentiality. Finally, section 5 concludes the paper.

2. Related works: A brief review

Various research works have already existed in the literature, which depends on image scaling and cropping based on reduced cloud storage with different perspectives. Helei Cui et al. [17] have exhibited a proficient and secure cloud-helped image sharing design for mobile devices and with privacy confirmation by utilizing the datasets re-appropriated encrypted image. The main drawback of this method is to encrypting image by locating the candidates to develop a secure and efficient. Utilizing an optimized encrypted binary CGH (Computer Generated Hologram) a novel color image watermarking plan was exhibited by Jianzhong Li et al. [18]. The main drawback of this method is quality of reconstructed image is medium. To improve the reconstructed image quality a Fibonacci transform-based binary CGH procedure that utilizes PSO (Particle Swarm Optimization) algorithm were introduced to produce a watermarked hologram.

For multi-user settings Mohanty et al. [19] have presented a 2DCRYPT, a changed Paillier cryptosystem-based image scaling and cropping plan. The main drawback of this method is security and incurs of the acceptable overhead. For securing two images Rajput et al. [20] have introduced a novel security plot dependent on the DRPE (Double Random Phase Fractional Domain encoding) and changed G-S (GERCHBERG-SAXTON) phase retrieval algorithm. The main drawback of this method is while encrypting the two color images the gray scale image is diminished in some cases.

In encrypted images another technique for separable data hiding were displayed by Liao et al. [21] by utilizing discrete Fourier transform and CS. The drawback is to obtain the better image quality of the concealing the same embedding capacity. In distribution of computationally effective Shamir's secret sharing plan Deepthi et al. [22] have acquainted a system with determination security issues. The disadvantage of this method is that it requires multiple cloud service providers to resist collusion attack. For authenticity of visual substance utilizing TLE (Three-Level Encryption), MS (Morton Scanning) coordinated substitution of LSB (Least Significant Bit), color model transformation, and picture Steganography, a safe cryptographic system was introduced by Khan Muhammad et al. [23]. The disadvantage is to make the stego image

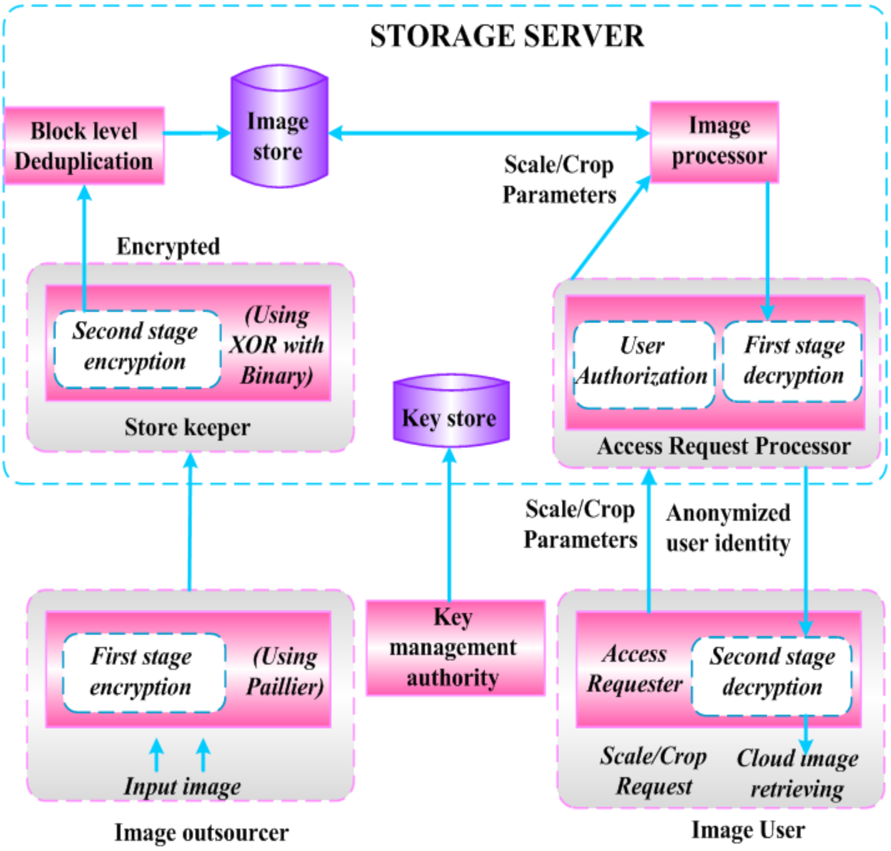


Figure. 1 Block diagram of proposed method

resilience against image processing attacks; the Steganography technique must be implement using transform domain.

From the literature survey, they mainly focused on the image scaling and cropping. The main drawbacks of the existing methods are overcome by the proposed method, Image scaling and cropping in reduced cloud storage system with de-duplication is proposed based on two different encryption levels. First level is based on reformed Paillier cryptosystem and second level is based on XOR with binary encryption.

2.1 Background of the research work

In the existing system 2DCrypt is working under the principle of same encryption in both levels. The same level of encryption is following the public key cryptosystem that is Paillier cryptography. The same encryption and decryption operation perform in both user level and the cloud level. This makes the system slow and attacker can easily do the cryptanalysis. “The important thing is the existing system is not fully homomorphic” [17].

3. Proposed system

In this section, Image scaling and cropping in reduced cloud storage system with de-duplication is proposed based on two different encryption levels. First level is based on reformed Paillier cryptosystem and second level is based on XOR with binary encryption. Fig. 1 shows the block-diagram of proposed system. In this system, many of the users can access but for each user (i.e., Image owner), want to use two keys for encrypting the image. The key management authority is providing these keys for each user by initializing algorithm. The first pair of key is using for first level of encryption that is reformed Paillier encryption the second key pair is using XOR with binary encryption. The Image owner or the loader storing the image in the cloud server and performing the operations of image editing that is cropping and scaling depending upon the user. When user is performing the editing operation the storage size of the image will be decreasing and the user can avoid the storage overhead problem. It is the main purpose of using this method.

3.1 Reformed paillier cryptosystem

The proposed method uses two type encryption techniques for the faster and better execution of the system. That is, in the user side encryption, the reformed Paillier cryptosystem is used and in the server side encryption the XOR with binary encryption scheme is used. This encryption scheme is quite simple and powerful. In cryptanalysis, two encryptions will give a good security to the user data in the cloud in all aspects.

The key management authority provides the keys for encryption and decryption. The initialization algorithm initializes the key management authority is representing the initialization. Choose two large prime numbers *p* and *q* randomly and independently of each other such that *gcd* (*pq* (*p*-1)(*q*-1)) = 1 this property is assured if both primes are of equal length. Computing, 'n' that is secret key and computing *gp* and *q* that is the public key.

$$n = pq \tag{1}$$

$$\lambda = lcm(p-1, q-1) \tag{2}$$

$$\mu = (L(g^{\lambda} mod\, n^2))^{-1} mod\, n \tag{3}$$

Where $g \in Z$, in the time of encryption the public keys are n and g. for decryption the private keys are λ and μ. Let the image pixel p will be encrypted where λ is the queried leakage functions ,$0 \leq p \leq$ n, selecting the random number *r* from set of integers where $0 \leq r \leq n$. Using these two values the encryption process will doing, Eq. (4) is representing this process. Where, en is the encrypted image pixel. ρ^m is the minimal polynomial. r^n is the random number of integer.

$$en = p^m \cdot r^n mod n^2 \tag{4}$$

After the encryption is over the user will do the second level of encryption before that the first level of decryption will be happening using the secret key Eq. (5) representing this decryption process.

$$dn = L(c^{\lambda}\, mod\, n^2) \cdot \mu\, mod \tag{5}$$

Where *dn* is the decrypted pixel of the particular image. c^{λ} is the plaintext.

3.2 XOR with binary encryption

In Encryption and decryption, the XOR cryptogram is simple cipher. In this method all the image pixel values are converting into binary values and after the conversion the XOR operation takes place. When an XOR operation needs two operands, one is our image pixel and the second is the secret key of the initialization algorithm. XOR is a basic and common operation but it is complicated. In crypto analysis this cipher can easily breakable when the user is using the same key again otherwise the XOR cipher is strong. The encryption of an Image is shown in Fig. 2.

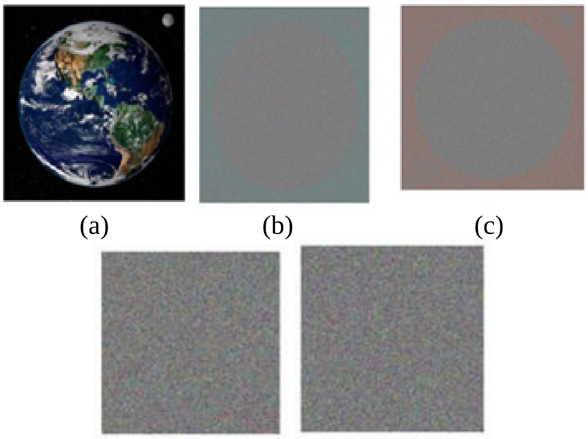


Figure. 2 Encryption of an image: (a) earth image with and without random number, (b)&(c) outcome of image outsourcer and cloud server, (d)&(e) outcome of image outsourcer and storage server

Fig. 2 (a) shows the earth image with and without random number in a tile. Figures (b) and (c) show the images after the Image Outsourcer and Cloud Server encryptions, without using a random number (best viewed on a computer screen or printed in color). Figures (d) and (e) show the images after Image Outsourcer and Storage Server encryptions.

3.3 Procedure for secure de-duplication

In this section, a block wise conversion technique is applied for secure de-duplication of images. Fig. 3 shows the structure of block wise conversion technique. Here, the user first divides the image into a fixed number of blocks. The block size of each image could be variable length i.e., 4×4, 8×8, 16×16. Then the user runs the client portion of encrypted protocol on each block after converting the image into blocks. As per the encryption process, the user computes the secret key (n_i) as

$$n_i \leftarrow h\,(b_i) \tag{6}$$

Where, the i^{th} block of image is denoted as b_i and the hash function is represented as h then, the user computes the tag *t* as and the cipher text c_i as follows.

$$t_i \leftarrow h\,(c_i) \tag{7}$$

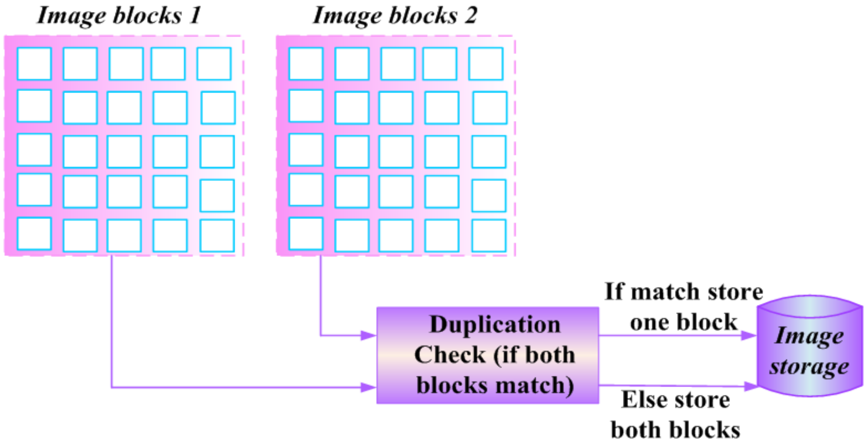


Figure. 3 Block level de-duplication

$$c_i \leftarrow en(n_{i,}b_i) \tag{8}$$

Where, the encryption strategy is denoted as *en*. After computing the cipher text, tags and the keys, for an image the user obtains the succeeding vectors $\{c_{11}, c_{12}, c_{13},\ldots c_{nm}\}$, $\{t_{11}, t_{12}, t_{13},\ldots t_{nm}\}$, $\{n_{11}, n_{12}, n_{13},\ldots n_{nm}\}$, where the total number of blocks is indicated as *nm*. In this stage the tag vector $\{t_{11}, t_{12}, t_{13},\ldots t_{nm}\}$ is send by the user to the cloud service provider (CSP) and check for its existence in the cloud. $\{c_{11}, c_{12}, c_{13}\ldots c_{nm}\}$ is final cipher text to "encrypt". $\{n_{11}, n_{12}, n_{13}\ldots n_{nm}\}$ is the polynomials. In the tag storage the CSP runs a search for a tag existence from tag vector and only for those blocks it send a request, for which no match was found. Next, to the CSP the user send the cipher text for particular blocks along with the user credentials to store and its tag store is updated by computing $t'_i \leftarrow h\,(c_i)$.

The user send the tag vector at the download time and to find the corresponding tag the CSP searches its tag store and the block of cipher text as $t_i = t'_i$. If a match is found there, then the corresponding cipher text block is send back to the respective user. Otherwise, if the image is not found the CSP sends an acknowledgement. Thus, from the received cipher text block the tag is computed as $t''_i \leftarrow h\,(c_i)$, after the user receives the cipher text. If a match ($t''_i = t_i$) is found there, then decryption process is performed, otherwise the user sends an acknowledgement to the CSP in which the block has been corrupted.

3.4 Procedure of proposed three different modules

This paper is sub-divided into three different modules or parts: Key Management Authority (KMA), image outsourcer, and user access. These three modules are performing three different operations and the sub parts are explained in the following section.

3.4.1. Key management authority (KMA)

This is the first part of proposed system. KMA or key management authority provides the keys for the administrator as well as the user. KMA is initializing different keys for different users. The user can access the cloud or storage server using the user key provided by the KMA. The user can add or remove the access policy from the KMA. The system can have one administrator that is the owner of the systems. Only with the help of administrator (Master Secret Key) the other user is uploading the data or image to the storage server. When a user is adding in to the system, the user key is providing by the KMA. Only with the help of that key the user can access the uploaded data from the storage server.

The system is working according to the following manner. The KMA runs the initialization algorithm in order to generate public parameters and a master secret key set MSK that is administrator key. It takes as input a security parameter *k* and generates two prime numbers p and q of bit-length *k*. It computes $n = pq$. The secret key is $x \in [1, n^2/2]$.

3.4.2. Image outsourcer

Image outsourcer is the image owner or admin of the system. The image outsourcer can have many sub jobs like uploading the image, checking the admin permission, tiling the image into different parts, etc. The next stage of image outsourcer is image tiling and uploading. Tiling is the process of subdividing the image into different parts. First, the image is dividing into super tiles of size 8×8. Depending upon the size of the image, the number of super tiles and that tile is increasing or decreasing. Therefore distribute the pixels into tiles in such a way that four neighboring pixels are always put in four different tiles. To upload the user encrypted image, by clicking the "Uploading to Cloud" button a small dialog box will be displayed for entering the file name of the image.

3.4.3. User access

The third stage of the system is user accessing the uploaded image from the cloud or storage server. For that accessing the user needs the user key provided by the key management authority. System is verifying the user key and provides the permission for scaling and cropping operation. These scaling and cropping operations are happening without knowing the exact image that is encrypted image. After the scaling or cropping operation the user can decrypt the image and view it. Another way is the user can directly upload the scaled or cropped image to the cloud or storage server.

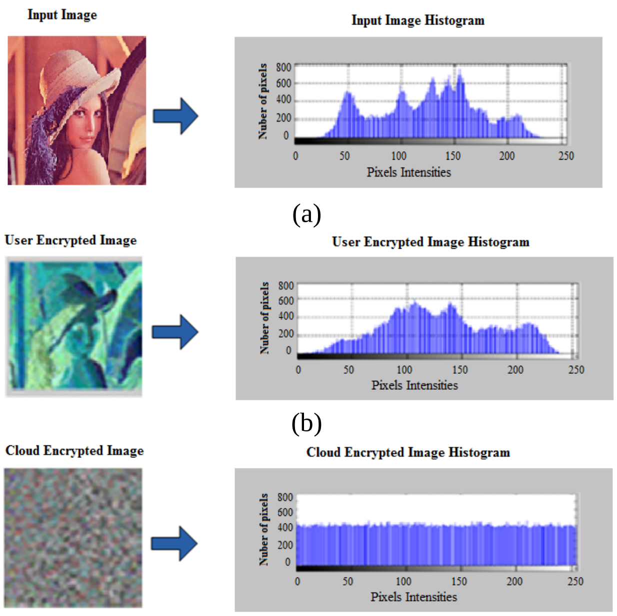
4. Simulation results and discussion

An analysis is a process of automatically analyzing the behaviour of computer programs regarding a property such as correctness, robustness, and safety. Analysis means systematically collecting valid, reliable and pertinent particulars in order to make judgments. It provides recommendations for decision making. Analysis refers to breaking the whole into its separate components for individual evaluation. Data analysis is the process of interpreting the meaning of the data that have collected, organized, and displayed in the form of a table, line graph, or other representation. Data analysis is a process for obtaining raw data and converting it into the information which is useful for decision-making by users. Data is collected and analyzed to answer the questions and test hypotheses or disprove theories.

This section shows the results and analysis of proposed method. The experiments were performed using a LAPTOP powered by Intel Dual-Core 2.10 GHz processor and 2 GB of RAM. This project implemented the optimized modified Paillier cryptosystem and image scaling cropping operations in MATLAB programming language of version 2010a on Windows 7 platform. The datasets used in this paper is open image dataset given image is Lena image (512×512) 8-bit image.

4.1 Histogram analysis

A histogram is a graphical representation of the distribution of numerical data. It is an estimate of the probability distribution of a continuous variable.



(a)

(b)

(c)

Figure. 4 Histogram of: (a) input, (b) user encrypted images, and (c) cloud encrypted image

The histogram is a graph showing the number of pixels in an image at different intensity values found in the image. In an 8-bit gray scale image, there are 256 different possible intensities, and so the histogram will display 256 numbers showing the distribution of pixels amongst those gray scale values. For a good encryption, the distribution of gray scales in the encrypted image should be fairly uniform. The gray scale images and color images of different sizes and textures are used for developing histograms of encrypted images obtained from an algorithm it has been analyzed.

In this paper, histogram analysis shows an exact identification and difference between the input image and encrypted image. Through the process of histogram analysis, the attacker can spoof the data inside the image. The following Fig. 4 represents the histogram of the input and encrypted images.

4.2 Pixel correlation analysis

Correlation is a measure of the relationship between two neighbouring pixels in an image. If the two pixels are the adjacent pixels in an image, then there is a very close correlation between them else it is said they are less correlated or no relationship between pixels. This is called correlation in the image pixels. We can compute the correlation coefficient (CC) using the Eq. (9). Considering two adjacent pixels x and y, and the N is the total adjacent pixels in the image and E is the mean. The Correlation can be calculated in three phases they

Table. 1 Correlation values

Lena Image	Horizontal	Vertical	Diagonal
Original Image	0.9637	0.8877	0.8960
Encrypted Image	0.0456	-0.0568	-0.0202

are Horizontal, Vertical and Diagonal. These three faces give the exact pixel location change of the encrypted image.

$$cc = \frac{cov(x,y)}{\sigma x \times \sigma y} \quad (9)$$

Where,

$$\sigma x = \sqrt{var(x)} \ and \ \sigma y = \sqrt{var(y)} \quad (10)$$

$$var(x) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)]^2 \quad (11)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)][y_i - E(y)] \quad (12)$$

Here x_i, y_i are two adjacent pixel *at* i^{th} level. The following Table 1 representing the pixel correlation values of original image and the full encrypted image.

4.3 Security analysis

For both the encrypted images and the encryption approaches, refuge is imperative. We discuss some security issues of the XR Encryption method from the cryptography point of view.

Brute force attack: It is the model in which the invader tries to guess the security keys by piloting a comprehensive search of all the possible blends of security keys of the encryption algorithms. Theoretically, this tactic is possible if the key space of the encryption algorithm is limited and the invader knows the encryption method. Even if the security key spaces of both algorithms are not immense, they are still adequately large since the large number of conceivable new jumble of values can be used to generate the key. As a result, the two encryption procedures can withstand the brute force attack.

Cipher text-only attack: This attack, in which an invader tries to presume the security keys by only studying the cipher text [18]. This attack can be used to recover the original image by reviewing the encrypted images. If rarer shares of the images are encrypted, more shares of the original images can be recuperated by an invader without knowing the encryption method and its security keys. An encryption system has a very low security level if it cannot bear this occurrence. From the experimental results, after both encryptions the image is thoroughly visually unrecognizable and completely different from the original images. They contain virtually no visual information of the original images. These ensure the XOR Encryption Method can bear the cipher-only attack.

Table. 2 Storage efficiency

Method	Existing [19]	Proposed
Image Size	512x512	512x512
Image Size (After Scaling)	1024x1024	1024x1024
Storage Size	79.2 kb	49 kb
Storage Size (After Scaling)	191 kb	152 kb

4.4 Storage efficiency

This system provides a good storage efficiency comparing with the existing method. In the process of scaling, when the image size increases the storage size also increases. In this system the storage space is increasing but very small variation is taking place.

For the experiment, the the dataset is taken as open image datasets of Lena (512*512) 8-bit image. The uploaded image size is 512x512. After the scaling process in the cloud with the scaling factor 2 the image size will be 1024x1024. The space for storing the image is also increasing. Table 2 represents the storage efficiency of the proposed method.

4.5 Performance analysis

The performance measures like accuracy, sensitivity, specificity, encryption quality and run (execution) time are used to analyze the proposed method performance and compared with existing Cui et al. [17], Liao et al. [21], Deepthi et al. [22] techniques. The experiments is done with various size of images like image 1(256x265), image 2 (512x512), image 3 (1024x1024), and image 4 (2048x2048). Our research is mainly concentrating on to reduce the storage over head of the cloud storage or storage server. The evaluation metrics are described as follows.

$$Accuracy = \frac{T_P + T_N}{T_P + T_N + F_P + F_N} \quad (13)$$

$$Specifcity = \frac{T_N}{T_N + F_P} \quad (14)$$

$$Sensitivity = \frac{T_P}{T_P+F_N} \quad (15)$$

Where, True Negative is T_N, True positive is T_P, False Negative is F_N and False positive is F_P. Between the original image and the encrypted image, the encryption quality refers to total changes in pixel gray values. It is computed as follows.

$$E_Q = \frac{\sum_{l=0}^{235} |H_l(F) - H_l(F')|}{256} \quad (16)$$

Here, the pixel gray level is denoted as l, the number of pixels having gray level l in the encrypted image is represented as H_l (F') and the number of pixels having gray level l in the original image is indicated as H_l (F).

4.5.1. Run time

Run time (program lifecycle phase), the period during which a computer program executes. To estimate how long a portion of the program take to run or to compare the speed of different implementations of a portion of the program, use the stopwatch timer functions, *tic* and *toc*. The CPU time function measures the total CPU time and sums across all threads. This measurement is different from the wall-clock time that times it or *tic*/*toc* return, and cloud are misleading. The computation or running time can be calculated as follows.

$$Run_{\text{time}} = Ending_{\text{time}} - Starting_{\text{time}} \quad (17)$$

Fig. 5 shows the performance comparison of accuracy with various sizes of images. From the figure it is clearly observed that the performance of proposed method is better of 8.1%, 7.2%, and 6.1% for image 1, 10.2%, 7.1%, and 6.1% for image 2, 8.4%, 6.2%, and 5.8% for image 3, and 8.3%, 6.2%, and 5.6% for image 4 when compared with Cui et al. [17], Liao et al. [21], Deepthi et al. [22] research works. The sensitivity comparison of various sizes of images is shown in Fig. 6. It is observed from the Fig. 6, the performance of proposed method is better of 9.5%, 7.1%, and 7.01% for image 1, 12.6%, 6.9%, and 6.4% for image 2, 5.4%, 6.7%, and 6.1% for image 3, and 5.3%, 7.4%, and 7.04% for image 4 when compared with existing research work

The comparison analysis of specificity with various sizes of images is shown in Fig. 7. From the figure it is clearly observed that the performance of proposed method is better of 15.2%, 12.8%, and 14.45% for image 1, 14.9%, 12.7%, and 14.7% for image 2, 15%, 12.77%, and 14.47% for image 3, and 15.43%, 13.8%, and 15.7% for image 4 when compared with Cui et al. [17], Liao et al. [21], Deepthi et al. [22] research works. The analysis of encryption quality with various images is shown in Fig. 8. From the figure it is observed that, the encryption quality of proposed method is 20.9%, 21.4%, 17.7% and 17.03% superior to Cui et al. [17], 14.5%, 15.7%, 15.6% and 15.4% superior to Liao et al. [21], 9.1%, 10.46%, 10.48% and 9.4% superior to Deepthi et al. [22] techniques for various image sizes.

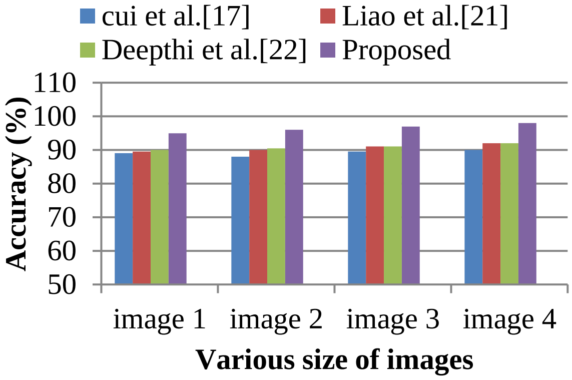


Figure. 5 Comparison analysis of accuracy with various images

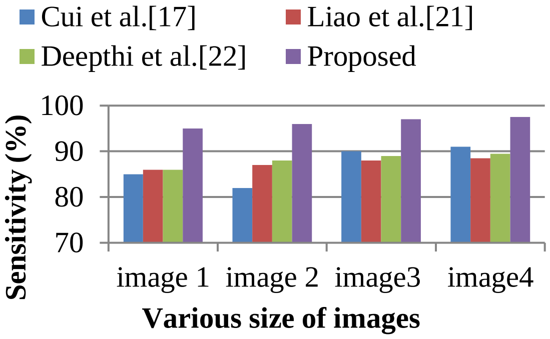


Figure. 6 Comparison analysis of sensitivity with various images

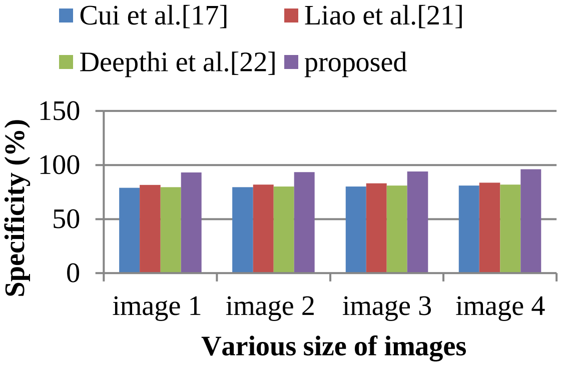


Figure. 7 Comparison analysis of specificity with various images

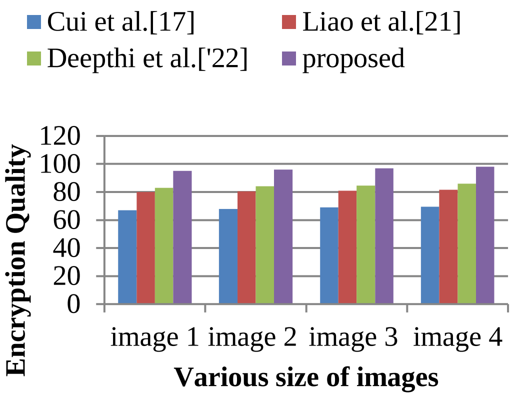


Figure. 8 Comparison analysis of encryption quality with various images

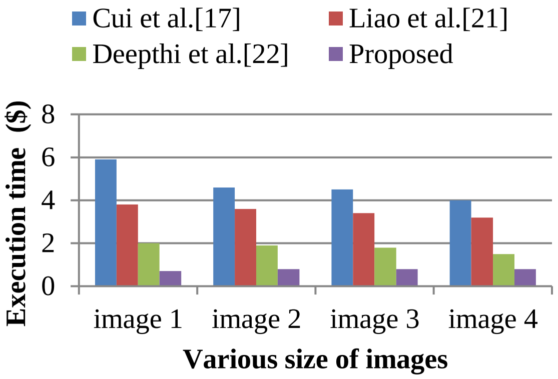


Figure. 9 Comparison analysis of execution time with various images

The execution time analysis of various images is shown in Fig. 9. It is observed from the Fig. 8; the execution time of proposed method is very less of 85.2%, 77.1%, and 58.7% for image 1, 79.3%, 75.4%, and 53.08% for image 2, 79.2%, 73.9%, and 52.06% for image 3, and 77.8%, 74.06%, and 45.7% for image 4 when compared with Cui et al. [17], Liao et al. [21], Deepthi et al. [22] research works. Theoretical reason for the better performance of the proposed method is it uses the XOR with the binary encryption scheme for encrypting the images in the cloud.

5. Conclusion and future work

This paper proposed a XOR Encryption Method with secure de-duplication for Image Scaling and Cropping in Reduced Cloud Storage, an Image encryption technique. This project addressed such confidentiality issue by proposing the XOR Encryption Method for Image Scaling & Cropping in Reduced Cloud Storage that allows a storage server or cloud to perform scaling and cropping operations without learning the image content. The exact computational overhead and the data required by the image used is dependent on the image size and the user's scaling and cropping parameters. The XOR Encryption Method for Image Scaling & Cropping in Reduced Cloud Storage can be extended in multiple ways. The performance analysis the accuracy, specificity, execution time, encryption quality, sensitivity gives a better result in our proposed method when comparing to existing methods. The scientific contribution of the proposed method is encrypted the input image by using XOR method for Scaling and cropping the cloud storage image.

References

[1] S. Goldwasser and S. Micali, "Probabilistic Encryption", *Journal of Computer and System Sciences*, Vol.28, No.2, pp.270–299, 1984.

[2] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can Homomorphic Encryption be Practical?", In: *Proc. the 3rd ACM Workshop on Cloud Computing Security Workshop*, pp.113–1242011.

[3] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data", In: *Proc. of 2000 IEEE Symposium on Security and Privacy. S&P 2000*, pp. 44–55, 2000.

[4] T. Bianchi, A. Piva, and M. Barni, "Encrypted domain DCT based on homomorphic cryptosystems", *EURASIP Journal of Information Security*, Vol. 2009, pp. 1:1–1:12, 2009.

[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search", In: *Proc. of International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 506–522, 2004

[6] 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. of IEEE International Conference on Multimedia and Expo*, San Jose, CA, USA, pp. 1–6, 2013.

[7] C. Gentry, *A Fully Homomorphic Encryption Scheme*, Ph.D. dissertation, Department of Computer Science, Stanford University, Stanford, CA, USA, 2009.

[8] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Hanbook of Cryptography*. Vol.1, CRC Press, Boca Raton, Florida, 1996.

[9] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes", In: *Proc. of International Conference on the*

Theory and Applications of Cryptographic Techniques, pp. 223–238, 1999.

[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, No.1, pp. 125–141, 2014.

[11] T. El Gamal, “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”, *IEEE Transactions on Information Theory*, Vol.31, No.4, pp.469-472, 1985.

[12] X. Sun and S. Bo, “A Blind Digital Watermarking for Color Medical Images Based on PCA”, In *Proc. of IEEE International Conference on Wireless Communications, Networking and Information Security*, pp. 421–427, 2010.

[13] Z. Liu, C. Guo, J. Tan, W. Liu, J. Wu, Q. Wu, L. Pan, and S. Liu, “Securing color image by using Phase-Only Encoding in Fresnel domains”, *Optics and Lasers in Engineering*, Vol.6, No.5, pp.87-92, 2015.

[14] S. Somaraj and M. A. Hussain, “Performance and Security Analysis for Image Encryption using Key Image”, *Indian Journal of Science and Technology*, Vol.8, No.35, pp.1-4, 2015

[15] C. Y. Hsu, C. S. Lu, and S. C. Pei, “Image feature extraction in encrypted domain with privacy-preserving SIFT”, *IEEE Transaction on Image Processing*, Vol.21, No.11, pp.4593–4607, 2012.

[16] J. Yuan, S. Yu, and L. Guo, “SEISA: Secure and efficient encrypted image search with access control”, In: *Proc. of IEEE Conference on Computer Communications*, pp. 2083–2091, 2015.

[17] H. Cui, X. Yuan, and C. Wang, “Harnessing Encrypted Data in Cloud for Secure and Efficient Mobile Image Sharing”, *IEEE Transactions on Mobile Computing*, Vol.16, No.5, pp. 1315-1329, 2017.

[18] J. Li, Q. Lin, C. Yu, X. Ren, and P. Li, “A QDCT- and SVD-based color image watermarking scheme using an optimized encrypted binary computer-generated hologram”, *Soft Computing*, Vol.22, No.1, pp. 47-65, 2016.

[19] M. Mohanty, M. R. Asghar, and G. Russello “2DCrypt: Image Scaling and Cropping in Encrypted Domains”, *IEEE Transactions on Information Forensics and Security*, Vol. PP, No. 99, pp.2542-2555, 2016.

[20] S. Rajput and N. Nishchal, “Optical double image security using random phase fractional Fourier domain encoding and phase-retrieval algorithm”, *Optics Communications*, Vol.388, No.4, pp. 38-46, 2017.

[21] X. Liao, K. Li, and J. Yin, “Separable data hiding in encrypted image based on compressive sensing and discrete fourier transform”, *Multimedia Tools and Applications*, Vol.76, No.20, pp. 20739-20753, 2016.

[22] S. Deepthi, V. Lakshmi, and P. Deepthi, “Image processing in encrypted domain for distributed storage in cloud”, In: *Proc. of the International Conference on Wireless Communications, Signal Processing and Networking*, pp. 1478-1482, 2017.

[23] K. Muhammad, J. Ahmad, S. Rho, and S. Baik, “Image steganography for authenticity of visual contents in social networks”, *Multimedia Tools and Applications*, Vol.76, No.18, pp. 18985-19004, 2017.