Journal of Computer Science and Applications.
ISSN 2231-1270 Volume 7, Number 1 (2015), pp. 1-9
© International Research Publication House
http://www.irphouse.com

An Outsourced image reconstruction in Cloud computing

G.S.Arun Kumar[1] and S.Md.Ghouse[2]

M.Tech(Cse) Scholar Madanapalle Institute Of Technology And Sciences, JNTUA[1]
Asst. Professor(Cse) Madanapalle Institute Of Technology And Sciences, JNTUA[2]

ABSTRACT

At present large scale images are generates with a highly cleanness along with various sizes. Now to handle these large scale images, we are using cloud system to store the images. But cloud computing is not providing much security for the images here the case is not only for images even for the data that which is stored in the cloud, but whatever the data stored in cloud it is in encrypted manner. Still the hackers are using the images of users. For the protection of the images in cloud computing has became a great issue. Now to overcome these challenges, we proposed OIRS approach in this OIRS we are adding the Pseudo Random Number Generator (PRNG) and Scalable-coding these applications were proposed in OIRS. For proving high security to the images in scalable-coding we have modulo “256 addition” with non-random numbers which can derived from a secret key. By using OIRS schema these applications were included in OIRS. By this OIRS Schema gives more accuracy and efficiency for the users to store images.

KEYWORDS- OIRS, Pseudo Random Number Generator (PRNG), Scalable-coding, Hadamard coefficients.

1. INTRODUCTION

The concept of cloud computing has been raised successfully computing paradigm, the cause is it allows hiring resources without carrying any maintenance charges and adds a new features to the clients, like the possibility of scale-up and scale-down resources that are dynamically depending on the punctual requirements[1]. Cloud computing is more indeed generally the costs of efficient method to use, and to maintain and upgrade it.

With the advancement of information and computing technology, large-scale datasets are being exponentially generated today. Examples under various applications contexts include medical images[2], remote sensing images, satellite image data□bases, etc. Among with these data explosion is an fast□growing tendency for outsourcing the images, management systems to cloud leverage its economic yet abundant computing resources to efficiently and effectively acquire, store, and sharing images from the data owners to users might be in large numbers.

Even though outsourcing of images services is fairly promising, in order to become truly successful, it still faces a number of fundamental and critical challenges, among which security is the peak worry. This is due to the fact that the cloud is an open source environment operated by external third-parties, who are usually outside of the data owners/users [3],[4] trusted domain. In other hand, various image datasets, e.g, medical images with diagnostic results for different patients, are privacy sensitive by nature [5]. Thus the critical importance to ensure that security must be embedding with image service outsourcing design from the extremely beginning. So here to protect the owners data privacy without sacrificing the usability and convenience for the information. For the sake of HD and large-scale image datasets [6] here its necessary for both and desirable for the image services in outsourcing design should be efficient and fewer resource-consuming as possible, in terms of bandwidth and storage cost on cloud.

Usually, for establishing these kind of image acquisitions and sharing services, generally the data owners follows Nyquist sampling theorem and often desires to obtain large amounts of samples for example: high resolution images, rising the sample rate can be extremely expensive in current imaging system like medical scanner and radar[7].

Compressing sensing [8],[9],[10] is the technique that is proposed recently, data sampling and compression for data gaining, by the leveraging the saprity of data. Especially,later shown in section-3.c, since the size of sample vector is almost always much lessthan the original image data, just storing the compressed sample vectors comparing with original image data can save the storage cost to 50%[11].

In this paper, the initiation to the examination for these challenges and proposed a novel approach of outsourcing image recovery service (OIRS) architecture by privacy assurance. To the ease of data acquisition at data owner side, OIRS is especially designed below the compressed sensing framework. In OIRS to provide more security to the images we added a new proposed method for this OIRS.

1. Scalable coding of an encrypted image (technique of masking the original pixel values).
2. Image encryption(is an uncompressed format)
3. Encoding encrypted image

2. RELATED WORK

Compressed sensing [8], [9], [10] is the recent proposed sensing data and reconstruction framework well-known for its ease of unifying the usual sampling and compression for data gaining. Till now number of security issues are raised in images of cloud computing. Those problems are solved in many methods. [11] by Divekar et al. proposed an image compressing method is called compressed sensing. He proposed a method for security that compressed image is stored in cloud storage in the form of small data sets instead of whole image. Small datasets security may apply for compressed image or uncompressed image. Here the results gives up to half of the size of the image is compressed. Even though, this method not gives sufficient security for the image.

A. Orsdemir, H. O. Altun et al [12] proposed compressed sensing with secured encryption techniques. But this method implementing is infeasible. One more problem is raised in that time, which is how to recover the splitter image into original content. Gennaro et al [18] shows a theoretical solution for the infeasible situation, but these are not practical. M.Attallah et al proposed privacy computations of input and output data and use fully homomorphic encryption (FHE) method.

Yao et al [14] shows secure multiparty computation (SMC) which little bit related to our proposed work but significantly it is different. Goldreich et al and others proposed advanced technique of SMC, that allows some general function computation by jointly two or more parties and hide their inputs from each other. Still cloud computing images miss security.

Computation services are always burden to server and are proportional to time complexity. To overcome these algebraic problems algorithms are using (e.g., relative to n^3 for multiplying 2 n x n matrix) the improvements we give are:

(i) Whereas the previous work required more than one remote server and assumed they do not collude, our solution works with a single server (but readily accommodates many, for improved performance);

(ii) Whereas the previous work required a server to carry out expensive cryptographic computations (e.g., homomorphic encryptions), such expensive cryptographic encryptions are not used in our system;

(iii) Collusions occurred in the collection of different user's input and server not maintain properly these collusion, our solution detect any attempting of collusion and also corruption of data, even collusion is occur then server coordinate among the users and servers

3. PROPOSED

In the previous techniques, Nyquist sampling theorem followed by the data owners for the security of images. The theorem requires massive amount of data samples like high resolution pictures. To establish such data samples with high resolution takes more space in memory occupation. So it's very need to compress the images and reconstruct those, but reconstructing and compressing of such high resolution images is very critical procedure and the theorem takes more time complexity. Such that following of Nyquist sampling theorem can be very wasteful procedure in terms of time, space and procedure. In modern image processing systems, increasing the sampling rate of image is also very expensive like medical scanners and radars.

3.2.1 ALGORITHM

Data sampling of such high resolution are done in our proposed application. To improve the OIRS schema we are using these techniques as follows,

A. Scalable coding of an encrypted image:

In this method we use the technique of masking the original pixel values of an image by a modulo 256 addition with non-random numbers that are derived from a secret key.

Later decomposing the encrypted data into a down sampled sub image and several data sets with a multiple-resolution construction; an encoder calculates the sub image and the Hadamard coefficients of each data set to reduce the data amount as shown in figure 1.

- Then, the data calculates sub image and coefficients are regarded as a set of bit streams.
- Then, the quantized sub image and coefficients are regarded as a set of bit streams.
- When having the encoded bit streams and the secret key, a decoder can first obtain an approximate image by decrypting the quantized sub image and then reconstructing the detailed content using the quantized coefficients with the aid of spatial correlation in natural images.
- The decoder can extract a low resolution version of the image, and continue to decode the bit stream to achieve higher and higher resolutions, still the images are recovered.
- Bit streams are generated with a multiple resolution construction; the principal content with higher resolution can be obtained when more bit streams are received.

B. Image encryption:

As the image is in an uncompressed format pixel values will be varying in the range of (0,255). so we have to denote the no of rows and columns as N1,N2,... and the pixel no as N=N1*N2.

- Therefore, the bit amount of the original image is 8N.
- The content which owner generates a pseudorandom bit sequence with a length of 8N.
- Here, we assume the content owner and the decoder has the same pseudorandom number generator (PRNG) and a shared secret key used as the seed of the PRNG.
- Then, the content owner divides the pseudorandom bit sequence into N pieces, each of which containing 8 bits, converts each piece as an integer number.

$$g^{(0)}\ (i,j) = mod[p(i,j) + e(i,j), 256],$$

$$1 \le i \le N_1, 1 \le N_2 \qquad (1)$$

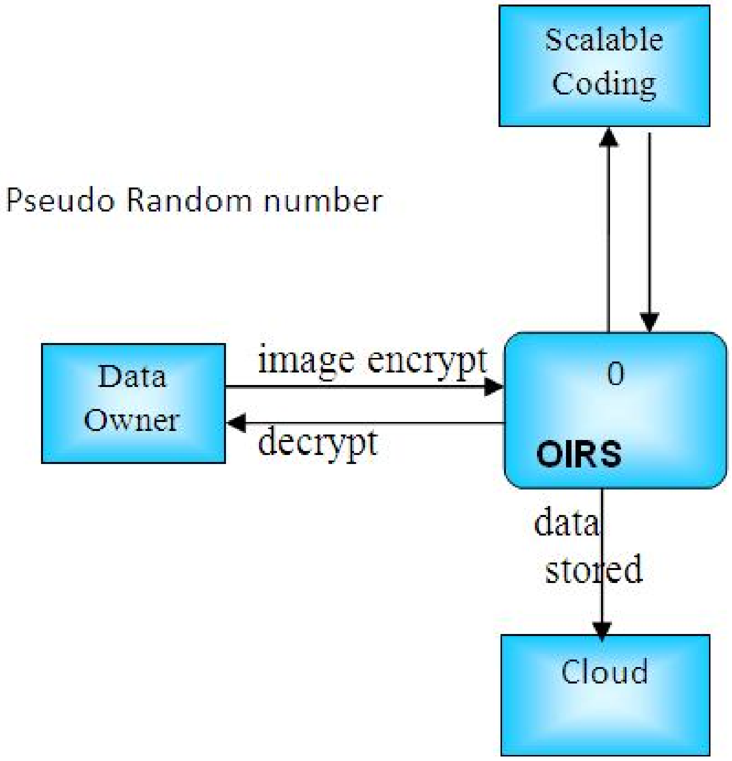


fig 1: Scalable coding of an encrypted image

C. Encoding encrypted image

Even if the encoder does not know the secret key and the unique content, but still we can compress the compress the encrypted data as a set of bit streams. The detailed encoding procedure is as follows

$$g^{(i+j)}\ (i,j) = g^{(t)}(2i,2j),$$

$$t = 0,1,\ldots..T-1 \quad (2)$$

$$R_c = \frac{N_{BC}}{8N} + \frac{1}{8N}\sum_{t=1}^{T} N^{(t)} = \frac{log_2 M}{8}.4^T + \frac{3}{8}.\sum_{t=1}^{T}\frac{\log_2 M}{4^t}\ldots.$$

3.2.2 Image Re construction:

3.2.1 For each group $[r_k^{(t)}(1), r_k^{(t)}(2), \ldots r_k^{(t)}(L^t)]$, calculate

$$f_k^t(l) = mod\ [r_k^t(l) + e_k^t(l), 256],$$

$$1 \le l \le L^{(t)}, 1 \le K^t, \tau \le t \le T$$

$$\begin{bmatrix} \hat{C}_k^{(t)}(1) \\ \hat{C}_k^{(t)}(2) \\ \vdots \\ \hat{C}_k^{(t)}\left(L^{(t)}\right) \end{bmatrix} = \mathbf{H} \cdot \begin{bmatrix} \hat{r}_k^{(t)}(1) \\ \hat{r}_k^{(t)}(2) \\ \vdots \\ \hat{r}_k^{(t)}\left(L^{(t)}\right) \end{bmatrix}$$

3.2.2 Calculate

$$D_k^{(t)}(l) = mod\,[C_k^{(t)}(l).\Delta^{(t)} + \frac{\Delta^{(t)}}{2} - C_k^{(t)}(l), 256]$$

$$D_k^{(t)}(l) = \begin{cases} D_k(l), & if\ d_k(l) < 128 \\ D_k(l) - 256, & if\ d_k(l) \geq 128 \end{cases}$$

3.2.3 Calculate the average energy of difference due to the modification as follows

$$D = \frac{\sum_{t=\tau}^{T} \sum_{k=1}^{K^{(t)}} \sum_{l=1}^{L^{(t)}} \left[\tilde{r}_k^{(t)}(l) - r_k^{(t)}(l)\right]^2}{\sum_{t=\tau}^{T} 3N/4^t}$$

4. RESULTS

The result related to the sender is shown in figure.2. Sender shares the image to receiver. So initially sender login his respective home page, and share image to the other user. He uploads the image from his system using upload option and also he has the chance to send text message also. He gives secret key, based on this key, image is encrypted not the text message. Encrypted image will be stored into cloud server after user uploads into his home page. Encrypted image will shown to him with two options, first is public and second is private. If he selects private option then no one can download the image from cloud server, where as in public option encrypted image can be download from cloud server.

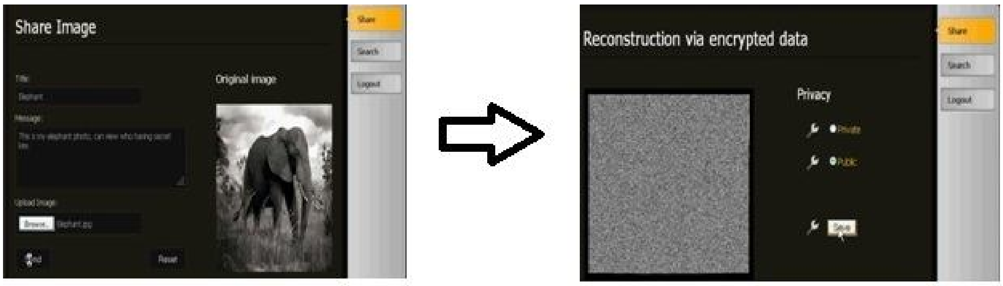
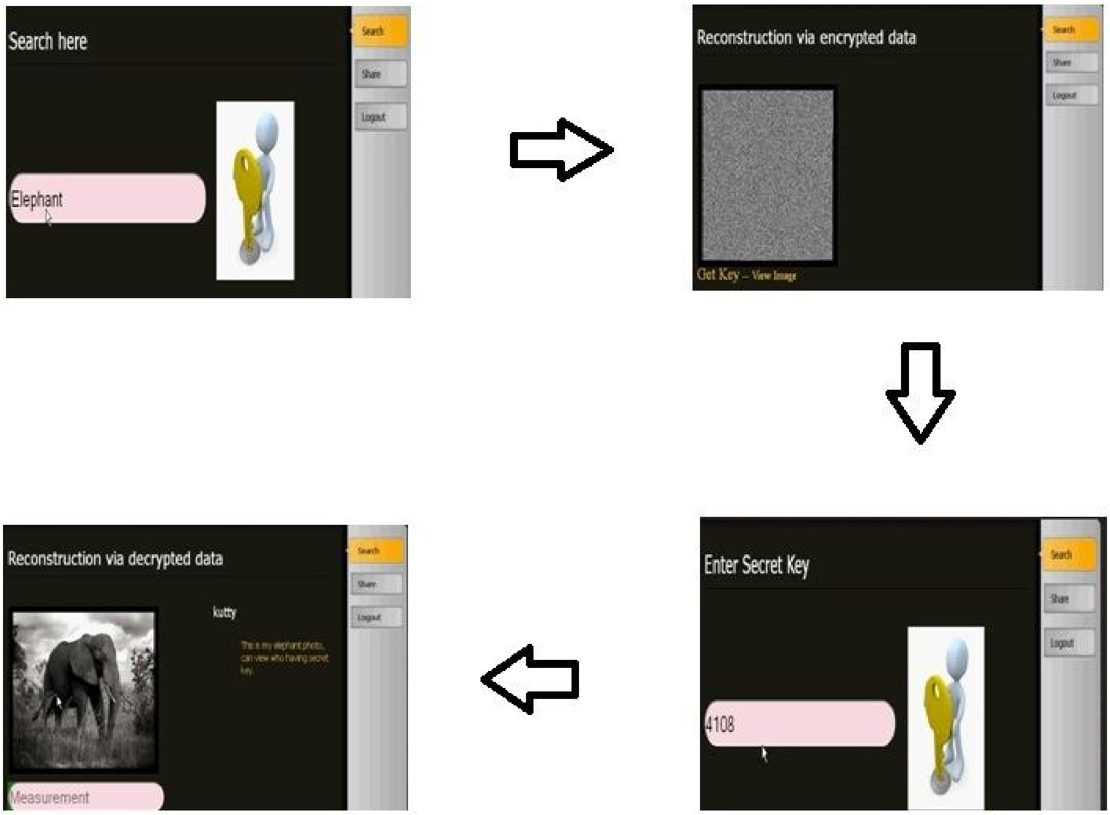


Figure.2. Results of Sender



Elephant

4108

This is my elephant photo, can view who having secret key.

Figure.3. Results of Receiver

The result related to the receiver is shown figure.3.Receiver can't able to see the private image of sender. The image searched by receiver from cloud server. If that is private then display the text like "image not existed" otherwise encrypted image shown by receiver. In encryption image display, get key option is presented. If the receivers press it, the secret key was sent to the respective receiver mail if he is authorized person from cloud server. After getting key from cloud, he enters it on respective column. Then encrypted image is decrypted. Here receiver has a chance to see the image in whatever measurement he needs.

5. Conclusion

In OIRS (Outsourced Image Recovery Service) approach we proposed these methods Pseudo Random Number Generator (PRNG), Scalable-coding, Hadamard coefficients. Different domains like security, efficiency and simplicity in design are considered in proposed application. Presently large sizes images are used, but there is lack of security from hackers. Protection of images in cloud computing is great concern before. Especially OIRS used compressed sensing (CS) framework, which results compressed image without losing clarity is stored in cloud computing. By this approach, space occupation by image was reducing. For security user reconstructed images are stored in clouds. In reconstruction images are converted into blank space images by using secret key. The OIRS design of image gives accuracy and efficiency to the user images.

6. REFERENCES

1. R. Buyya, C. S. Yeo, and S. Venugopal, “Market-oriented Cloud computing: Vision, hype, and reality for delivering it services as computing utilities”, published in the Proceedings of High Performance Computing and Communications, 10th IEEE International Conference on, vol. 0, pp. 5–13, 2008
2. C. Pavlopoulou, A. C. Kak, and C. E. Brodley, ``Content-based image retrieval for medical imagery," Proc. SPIE, vol. 5033, pp. 85_96, May 2003.
3. M. Atallah and K. Frikken, ``Securely outsourcing linear algebra computations," in Proc. 5th ASIACCS, 2010, pp. 48_59.
4. M. Atallah and J. Li, ``Secure outsourcing of sequence comparisons," Int. J. Inf. Security, vol. 4, no. 4, pp. 277_287, 2005.
5. (1996). Health Insurance Portability and Accountability Act of (HIPPA) [Online]. Available: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html
6. M. Lew, N. Sebe, C. Djeraba, and R. Jain, ``Content-based multimedia information retrieval: State of the art and challenges," ACM Trans. Multimedia Comput., Commun. Appl., vol. 2, no. 1, pp. 1_19, 2006.
7. J. Romberg, ``Imaging via compressive sampling," IEEE Signal Process. Mag., vol. 25, no. 2, pp. 14_20, Mar. 2008.
8. E. Candès, J. Romberg, and T. Tao, ``Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," IEEE Trans. Inf. Theory, vol. 52, no. 2, pp. 489_509, Feb. 2006.
9. E. Candès and T. Tao, ``Near-optimal signal recovery from random projections: Universal encoding strategies," IEEE Trans. Inf. Theory, vol. 52, no. 12, pp. 5406_5425, Dec. 2006.
10. D. Donoho, ``Compressed sensing," IEEE Trans. Inf. Theory, vol.52, no.4, pp. 1289_1306, Apr. 2006.
11. A. Divekar and O. Ersoy, ``Compact storage of correlated data for content based retrieval," in Proc. Asilomar Conf. Signals, Syst. Comput., 2009, pp. 109_112.
12. A. Orsdemir, H. O. Altun, G. Sharma, and M. F. Bocko, ``On the security and robustness of encryption via compressed sensing," in Proc. IEEE MILCOM, Nov. 2008, pp. 1_7.
13. Y. Rachlin and D. Baronm, ``The secrecy of compressed sensing measurements," in Proc. Allerton Conf. Commun., Control, Comput., 2008, pp. 813_817.
14. A. Yao, ``Protocols for secure omputations (extended abstract)," in Proc. FOCS, 1982, pp. 160_164.

15. Xinpeng Zhang, Member, IEEE, Guorui Feng, YanliRen, and ZhenxingQian." Scalable Coding of Encrypted Images". IEEE transactions on image processing, vol. 21, no. 6, June 2012
16. M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.
17. D. Taubman, "High performance scalable image compression with EBCOT," IEEE Trans. Image Process., vol. 9, no. 7, pp. 1158–1170, Jul. 2000.