A Privacy-Preserved Third Party Image Reconstruction System on Cloud with Storage Cost Efficiency

[1]Ms. Nitanjali Shinde,[2]Prof. Gaikwad V.S.
[1]PG Student, [2]Assistant Professor
[1]Computer Department.
[1]RSSOER, JSPM, NTC,Pune,India

***Abstract* - Today's image capturing innovations are delivering High Definitional-scale pictures which are likewise heavier on memory, which has incited numerous clients into distributed storage. Cloud computing is an service oriented technology. Cloud provides Data Storage as a Service (Dsaas). In conjunction with such information blast is that the aggressive pattern to outsource the image management systems to the cloud for its rich registering assets and edges. But the cloud is an open environment operated by external third parties so the security becomes a major concern. Since the image data sets are intended to be shared only to particular group of users the accountability of the image data is a high priority issue. To address the challenges with the accountability we propose an OIRS system. OIRS is designed using the compressive sensing technology. Data owners only need to upload compressed image samples to OIRS on cloud for reduced storage cost. In OIRS, data users can tackle the cloud to securely reconstruct images without leaking vital information from either the compressed image samples or the underlying image content.**

***IndexTerms* - Compressed sensing, security and privacy, cloud computing, image reconstruction.**

I. INTRODUCTION

Cloud computing is internet-based computing in which large number of remote servers are connected to allow the online access to computer services or resources and centralized data storage. Clouds are classified as public, private and hybrid. Cloud computing depends on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. The base of cloud computing is the broader concept of converged infrastructure and shared services.

Verification of the image data secrecy has emerged as a major issue in image storage on cloud infrastructure [11]. Now a days, Cloud computing provides services to deals with handling outsourced data services With the advancement of information and computing technology, High definition images which provides important information's like large-scale datasets medical images [22], remote sensing images [2], satellite image databases, etc. With such data explosion is the fast-growing trend to outsource the image management systems to cloud and improve its economic yet abundant computing resources [7] to efficiently and effectively capture, store or upload, and share images from data owners to a large number of data users [23].

Compressed sensing in a recent data sensing and reconstruction architecture well-known for its simplicity of unifying the traditional sampling and compression for data acquisition. Along that line of research, the system of leverage compressed sensing to compress the storage of correlated image datasets. Instead of storing the whole image, the idea is to store the compressed image samples on storage servers. The compressed samples offers about storage reduction compared to storing the original image in uncompressed format or other data application scenarios where data compression may not be done. But the security may be compromised, which is an indispensable design requirement in OIRS. On storage reduction, our proposed system aims to achieve a much more ambitious goal, which is an outsourced image service system and takes into account of security, efficiency, effectiveness, and complexity from the very beginning of the service flow. Another interesting line of research loosely related to the proposed OIRS is about the security and robustness of compressed sensing based encryption.

Image based security services are crucial in cloud computing infrastructures. Authentication of users and to support flexible access control to services, based on user identity properties (also called attributes) and past interaction or session histories is needed. Such services should preserve the privacy and security of users and data, while at the same time enhancing interoperability across multiple domains and simplifying management of identity verification. In this present system, the approach addressing such requirements, relies on the use of high-level identity verification policies such as identity attributes and semantic matching techniques.

Image based reconstruction only used for identity verification be disclosed to the existing System approach allows the user to use pseudonyms when interacting with the Present System, if the present policies allow the use of pseudonyms and the user is interested in preserving his/her anonymity. However, if multiple transactions are carried out by the same user with the same system, it can determine that they are from the same user, even if the system does not know who this user is the identity attributes of the user. Different in Present System may also collude and determine a profile of the transactions carried out by the same user. Such information when combined with other available information about the user ma y lead to disclosing the actual user identity or the values of some of his/her identity attributes, thus leading to privacy compromisation.

In this paper, we initiate the investigation for these challenges and propose a novel outsourced image recovery service (OIRS) architecture with security assurance. OIRS is specifically designed under the compressed sensing framework. The captured image samples from data owners are later upload to cloud, which can be considered as a central data repository and is responsible for

image sample storage and provides on-demand image reconstruction service for data users. Reconstructing images from compressed samples requires solving an optimization problem [11], it can be critical for users with computationally weak devices. The goal of OIRS is to shift such expensive computation workloads from data users to cloud for faster image reconstruction and less local resource consumption with privacy and security on the possibly sensitive image samples or the recovered image content. To conquer these challenging requirements, a core part of the OIRS design is a lightweight problem transformation mechanism.

II. RELATED WORK

Here we broadly review distributed image reconstruction systems, compressed sensing, and security mechanisms. J. Li and M. Atallah proposed the sequence comparison problem, given two strings and of respective lengths n and m, consists of finding a minimum-cost sequence of deletions, insertions, and substitutions (also called an edit script) that transform[6] . In this architecture a client owns strings and outsources the computation to two remote servers without revealing to them information about either the input strings or the output sequence. This design solution is non-interactive for the client (who only sends information about the inputs and receives the output) and the client's work is linear in its input/output. The servers' performance is O(m×n) computation (which is optimal) and communication, where is the input size, and the solution is designed to work when the servers have only O ((m + n)) memory. By using garbled circuit evaluation techniques in a novel way, they completely avoid the use of public-key cryptography, which makes this solution efficient in practice[6].

It is now considerd that one can reconstruct sparse or compressible signals accurately from a very limited number of measurements, possibly contaminated with noise. This technique known as"compressed sensing" or"compressive sampling" depends on properties of the sensing matrix such as the restricted isometry property[4]. In this E. Cande's, proposed new results about the accuracy of the reconstruction from under sampled measurements which improve on earlier estimates, and have the advantage of being more elegant. When whole information on the signal or image is available this is certainly a valid strategy. However, when the signal has to be captured first with a somewhat costly, difficult, or time-consuming measurement process, this seems to be a waste of resources: First one spends huge efforts to collect whole information on the signal and then one throws away most of the coefficients to obtain its compressed version. One might ask whether there is a more clever way of obtaining somewhat more directly the compressed version of the signal. It is not obvious at first sight how to do this: measuring directly the large coefficients is impossible since one usually does not know a-priori, which of them is actually the large ones[4]. Nevertheless, compressive sensing provides a way of obtaining the compressed version of a signal using only a small number of linear and non-adaptive measurements. Even more surprisingly, compressive sensing predicts that recovering the signal from its under sampled measurements can be done with computationally efficient methods, for instance convex optimization, more precisely, 1-minimization [4].

The novel theory of compressive sensing (CS) also termed as the sparse recovery,compressed sensing or compressive sampling provides a new approach to data acquisition CS relies on the empirical observation that many types of signals or images can be well-approximated by a sparse expansion in terms of a approprite basis, that is, by only a small number of non-zero coefficients. This is the base to the efficiency of many lossy compression techniques such as JPEG, MP3 etc. A compression is achieved by simply storing only the largest basis coefficients. For reconstructing the signal the non-stored coefficients are simply set to zero. This is surely a reasonable strategy when full information of the signal is available. But, when the signal first has to be acquired by a somewhat lengthy, costly, or otherwise difficult measurement (sensing) procedure, this may lead to be a waste of resources: First, more efforts are spent in order to obtain full information on the signal, and later most of the information is thrown away at the compression stage. One might ask whether there is a clever way of obtaining the compressed version of the Signal more directly, by taking only a few number of measurements of the signal. It is obvious at all whether this is not possible since measuring directly the large coefficients requires knowing a priori their location. Quite surprisingly, compressive sensing gives nevertheless a way of reconstructing a compressed version of the original signal by taking only a small amount of linear and non-adaptive measurements[5].

Image compression algorithms convert high-resolution images into a relatively few or small bit streams (while keeping the essential features intact), in effect turning a large digital data set into a substantially smaller one[4].Compressive sampling (CoSamp) is a new paradigm for developing data sampling technologies proposed by M. Wakin and E. Cande's. It is relies on the principle that many types of vector-space data are compressible, which is a term of art in mathematical signal processing [1]. The author[18]proposed a novel framework to support private location dependent queries, based on the theoretical work on Private Information Retrieval (PIR). Our framework does not require a trusted outsider, since privacy is attained to through cryptographic methods. Contrasted with existing work, our methodology attains to stronger privacy for previews of user locations; moreover, it is the first to give provable privacy ensures against correlation attacks. Author use the proposed framework to execute inferred and definite algorithms for nearest-neighbor look. The authorupdates question execution by utilizing data mining procedures, which distinguish repetitive computations[18].

III. PROBLEM STATEMENT

The basic service design model in the OIRS architecture includes the following steps: At first, data owner captures raw (sparse) or original image data, in the form of compressed image samples, generated from the physical world devices and imaging applications under different contexts. To reduce the local storage cost and maintenance workload, data owner later outsources compressed samples of the raw image to the cloud for storage and processing. The OIRS on cloud will on-demand reconstructs the images from those samples upon receiving the requests from the users. For this, we consider a semi-trusted cloud as the adversary in OIRS. The cloud is considerd to honestly perform the image reconstruction service as specified, but also it may be curious in learning and accessing owner/users data content. Because the images samples captured by data owners usually contain data specific

or sensitive information, we have to make sure that the data outside the data owner/users process is in secured and protected format. Our design goals for OIRS consist of the following.

- **Security:** OIRS ensure to give the strongest conceivable assurance on both the private image samples and the content of the recovered images from the cloud.
- **Effectiveness:** OIRS ensure to empower cloud to adequately perform the image reconstruction service over the encrypted and compressed samples and vice versa.
- **Efficiency:** OIRS ensure to bring profit from the computation and/or storage aspects to data owner and users, while keeping the extra cost of processing encrypted image samples on cloud as small as possible.
- **Extensibility:** OIRS ensure to be made possible to support other extensible service interfaces and even performance speedup through hardware built-in design.

IV. IMPLEMENTATION DETAILS

A. System Overview

The basic service framework in the OIRS architecture includes the following: At first, data owner captures raw image data, in the form of compressed image samples, from the physical world under different imaging application contexts. To reduce the local storage and management workload, data owner later outsources the raw image samples to the cloud for storage and processing. The cloud will on-request reconstruct the images from those samples upon receiving the requests from the users. In our model, data users are considered to possess mobile devices with only limited computational resources[1].

Figure.1 demonstrates the basic message flow in OIRS. Let f and y be the signal or original image and its compressed samples to be captured by the data owner [1].

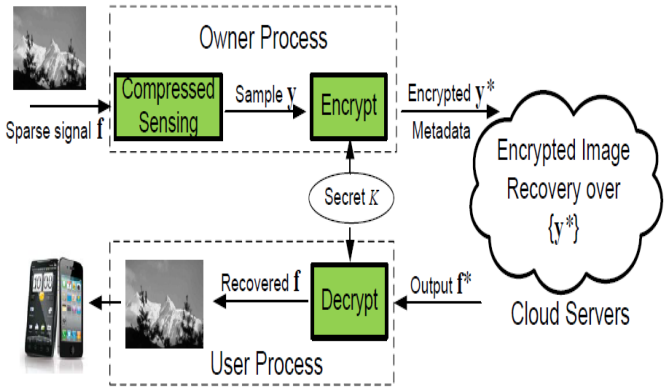

Figure1. The OIRS architecture in public cloud[1]

For privacy and security protection, data owner or client in OIRS will not outsource y directly. Instead, he outsources an encrypted version y* of y and some associated metadata to cloud. Next, the cloud reconstructs or recover an output f* directly over the encrypted y* and sends f* to data users. Finally, the user gets f by decrypting f*. In Fig.1, each block is considered as the process of a program taking input and producing output. Further consider that the programs are public and the data are private[1]

B. *.Algorithm*

Algorithm 1: Key Generation

Key Generation is a key generation algorithm running at the data owner side, which generates the secret key K upon getting input of some security parameter.

Data: We have received the request from client to insert file (F). Data Owner now want to validate F format.

Begin:

```
result = ValidateFormat(F);
validateFormat = {.png , .jpg , ... }
```

If the format is valid then client want to secure the data using BlowFish Algorithm.

CipherData(Fi) = BlowFish(Fi);

Result: Private Key (PKi) [key is used for encryption & decryption mechanism]

After all the response has been generated PKi is store into internal db of SS[security service] . The main Idea behind to hide PKi is provide security to CipherText(Bi) , So no one else can used the key and try to decrypt the block.

Algorithm 2: ImageUpload

ImageUpload(F, PKi) → Y'. Here ImageUpload takes as input the secret key K and F, F in original LP Ω and outputs a tuple Y'.

Data: System need to store CipherText(Bi) to the CSP along with Token (TiBi). System used the Referral Data integrity algorithm to associated the Bi →TiBi .

Begin:

1) Along with the CipherText(Bi) & Token(TiBi) system start the generation of the metadata. Meta Data Contains Fields.
   * logged User Info (U-info)

* File Name (Fname)

2) Once all the Data ciphterText(Bi¦Fi) has been process successfully , Data is send for Compression Algorithm.

CompressData(CD(Fi))= CompressionAlgorithm(ciphterData(Fi));

Result: The data is store on the cloud into vault server with 2 level of indexing. Below is the indexing structure.

Index -» DbServer -» VaultServer

Algorithm 3: ImageRecovery

ImageRec(PKi , Y') →F. The user uses the secret key K to recover the original answer F for problem Ω from protected answer Y' returned by cloud upon getting input of the secret key PKi and the answer Y' of PKi from cloud.

Data: User has received the request for retrieval of File (F) from CSP database.

Begin:

1) System send the request to CSP (CSP - Metadata) to validate the request is valid or not . i.e. F is present onto CSP or not. You will use the same indexing technique.
2) If F is available, System will retrieve the (F-Metadata) present on CSP , We Gave the input to the Compression Algorithm and then SecurityAlgorithm. i.e

Fi= SecurityAlgorithm(DecryptData(DecompressionAlgo(Fi)));

Result: With the Multipart protocol we downloaded the image F to the client end.

C. Mathematical Model

A transformation scheme r = (KeyGen, ImageUpload, ImageRec) is secure where,

OIRS = {S, e, I, O, DD, NDD, F, Succ, Fail}

where,

S = Start state i.e. Establishing connection between client and proxy server/Private cloud, using Client, Server, IP, Port

e = End state. i.e User query ran successfully on encrypted database and user get the accurate result in minimum time.

I = Set of inputs

O = Output

F = {F1,F2,F3,F4,F5}

Where,

F = is set of main function.

F1 = Connection establishment between client and server.

F2 = send Query request from trusted client to Proxy server.

F3 = Perturbation of query. Introducing noisy characters into query.

F4 = Encryption of Query with the help of Blowfish algorithm.

F5 = Perform search operation on encrypted data

DD = Deterministic data.i.e. Valid IP , Valid Port No

NDD = Non Deterministic data. i.e. requested data is not present in database and Port Already in use

Succ = successfully execution of encrypted user query on server.

Fail = Failure Cases like Internet connection issue, and Users doesn't have sufficient privileges to access data.

D. Experimental Setup

The system is built using Java framework(version jdk 1.7)on Windows platform. The Eclipse (version 4.2) is used as a development tool. For backend we are using MySQL, Heldi-SQL. The system doesn't require any specific hardware to run, any standard machine is capable of running the application.

V. RESULT AND DISCUSSION

A. Results

The following Table. I show the security algorithm performance analysis on the basis of time required to encrypt and decrypt provided input size.

Table I. Security Algorithm Performance Analysis

Input Image Size (bytes)	DES	3DES	AES	BF
20,527	24	72	39	19
36,002	48	123	74	35
45,911	57	158	94	46
59,852	74	202	125	58
69,545	83	243	143	67
137,325	160	462	285	136
158,959	190	543	324	158

166,364	198	569	355	162
191,383	227	655	378	176
232,398	276	799	460	219

The following Fig.2 Shows Graph of comparison of security algorithms. The x –axis shows input image size in bytes and y-axis shows the process time in msec. The following fig.2 shows the comparative graph which compares the performance of AES, 3DES and DES algorithm on the basis of process time required to encrypt and decrypt provided input image size.

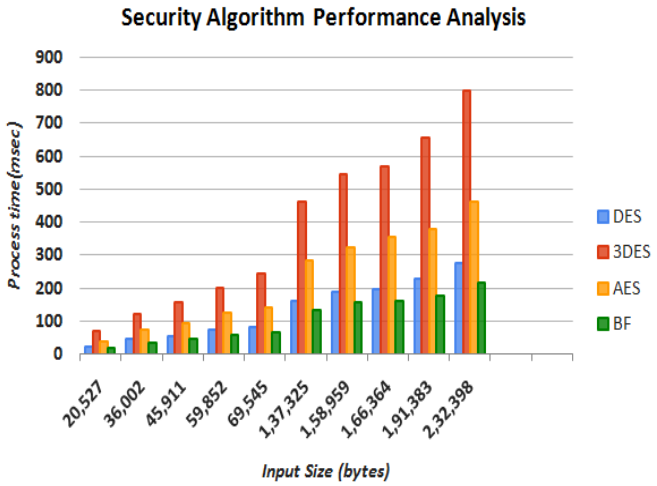

Figure 2. Graph of comparison of security algorithms.

Efficiency Evaluation

To measure the efficiency of the proposed OIRS , particularly to focus on the storage cost with privacy assurance done by the data owner and data users i.e, local side and the cost done by the cloud side. Efficiency analysis on storage size is explained in table.II.

TABLE II. Performance analysis of compression algorithm on the basis of storage size.

Image Dimention	Without Compression (Bytes)	With Compression (Bytes)	Recoverd Image Size (Bytes)
2048×2048	1322748	1315465	13,22,748
1024×1024	1966989	1966389	19,66,989
512 ×512	786486	111647	7,86,486
256×256	143181	143131	1,43,181
128×128	29049	24407	29,049

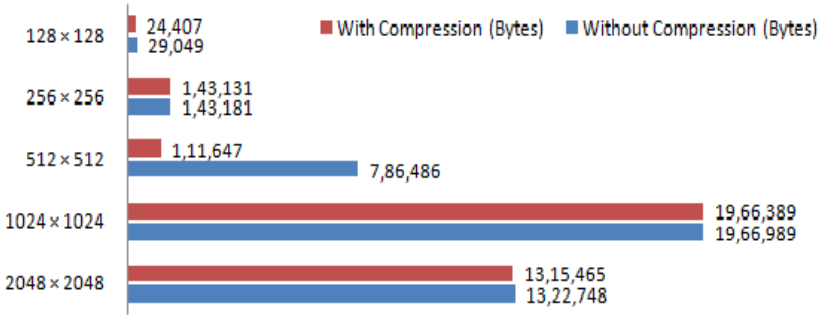

Figure 3: Graph of performance analysis of compression algorithm on storage size basis.

Correctness Evaluation

For correctness of the design, all the images after transformation and later recovered on the data owner side, still preserves the same level of visual quality as the original images. Recovered image quality increases along with the number of measurements and the more the better. Comparison between original image size and reconstructed image size is shown in fig.4.

Figure 4 . Comparison of recovered image with original image.

VI. CONCLUSION AND FUTURE SCOPE

Proposed OIRS provides outsourced image reconstruction service from compressed sensing with privacy and security assurance. OIRS exploits techniques from different domains, and means to take security, outline intricacy, and effectiveness into thought from the earliest starting point of the service flow. With OIRS, data owners can utilize the profit of compressed sensing to merge the sampling and image compression via only linear measurements. Data users, on the other hand, can leverage clouds lots of resources to outsource the image reconstruction related optimization computation, without publishing either the received compressed samples, or the content of the recovered respective image. Besides its simplicity and efficiency, we will show OIRS is able to achieve robustness and effectiveness in handling image reconstruction in cases of sparse data and also non-sparse general data via proper approximation.

VII. ACKNOWLEDGMENT

I would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. I am thankful to the authorities of Savitribai Phule Pune University and concern members of cPGCON2015 conference, organized by, for their constant guidelines and support. I am also thankful to the reviewer for their valuable suggestions. I am also thank the college authorities for providing the required infrastructure and support. Finally, I would like to extend a heartfelt gratitude to friends and family members.

REFERENCES

[1] Cong Wang (member, ieee), Bingsheng Zhang (member, ieee),Kui Ren (senior member,ieee), and Janet R. Roveda (senior member, ieee)" Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud," IEEE transactions on cloud computing vol:1 no:1 year 2013M.

[2] Banoth Ravi, R.Vijayaprakash, "Secure Outsourcing of Linear Optimization in Cloud Computing," IOSR Journal of Engineering (IOSRJEN),e-ISSN: 2250-3021, p-ISSN: 2278-8719,Volume 2, Issue 10 (October 2012), PP 57-62.

[3] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in Proc. CRYPTO,Aug. 2010, pp. 465-482.

[4] K.D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Proc. 16th ACM Conf. Computer and Comm. Security(CCS), pp. 187-198, 2009.

[5] C. Dwork, "The differential privacy frontier (extended abstract)," in Proc. TCC,2009, pp. 496502.

[6] Security Guidance for Critical Areas of Focus in Cloud Computing,[Online].Available:http://www.cloudsecurityalliance.org,] (2009).

[7] D. Needell and J. A. Tropp, ``Cosamp: Iterative signal recovery from incomplete and inaccurate samples," *Appl. Comput. Harmon. Anal.*, vol. 26, no. 3, pp. 301_321, 2009.

[8] E. Cands, "The restricted isometry property and its implications for compressed sensing," Comptes Rendus Mathematique, vol. 346, nos. 9-10, pp. 589-592, 2008.

[9] Adem Orsdemir, H. Oktay Altun, Gaurav Sharma, Mark F. Bocko,"On the security and robustness of encryption via compressed sensing," ECE Dept., University of Rochester, Rochester, NY, USA, 2008.

[10] Justin Romberg, "Imaging via Compressive Sampling," IEEE Signal processing magazine [15] March 2008.

[11] Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson, and Dawn Song "Provable Data Possession at Untrusted Stores," Proc. of the 14th ACM conference on computer and communications security, pp. 598-609, 2007

[12] E. Cands, 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.

[13] Mowafak Hasan,Hasan Al-Shalabi, "Modified cryptanalysis of RC5," The Int. Arab J. of Inf. Tech, vol. 3, no. 4, Oct. 2006.

[14] E. Cands 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.

[15] M. Atallah and J. Li, "Secure outsourcing of sequence comparisons," Int. J. Inf. Security, vol. 4, no. 4, pp. 277-287, 2005.

[16] E. Cands and T. Tao, "Decoding by linear programming," IEEE Trans. Inf. Theory, vol. 51, no. 12, pp. 4203-4215, Dec. 2005.

[17] Susan Hohenberger,Anna Lysyanskaya,"How to securley outsource cryptographic computations," February 16,2005.

[18] D. Donoho, "Compressed sensing,"september 14 2004.

[19] M. Atallah, K. Pantazopoulos, J. Rice, and E. Spafford, "Secure outsourcing of scientific computations," Adv. Comput., vol. 54, pp. 216-272, Feb. 2001.

[20] Stefan Auer,Alexander Bliem,Dominik Engel,Andreas Uhl,Andreas Unterweger, "Bitstream-based JPEG Encryption in Real-time," University of Salzburg, Austria.

[21] Ronald L. Rivest, "The RCA Encryption Algorithm," MIT Laboratory for Computer Science,545 Technology Square, Cambridge, Mass 02139,rivest@theory.lcs.mit.edu, Revised March 20,1997.
[22] Yaron Rachlin and Dror Baron,"The secrecy of compressed sensing measurements".
[23] P. Mell and T. Grance, (2011). *The Nist Definition of Cloud Computing*[Online].Available:http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.