Secure Transformation Based Approach for Outsourced Image Reconstruction Service

M. Jeevitha Lakshmi S.[1], Umapriya[2] , R. Ramya M.[3] SivaSindhu[4]

[D]epartment of Electronics and Communication Engineering, Dr.S.J.S. Paul Memorial College of Engineering and Technology, Pondicherry University, India.

Abstract- Now-a-days image or data is not retrieve properly in cloud because large number of problem is created, from this the data may losses. So, we choose OIRS under the compressed sensing framework, which is known for its simplicity of unifying the traditional sampling and compression for image acquisition. Data owner only need to outsource compressed image samples to cloud for reduced storage overhead. OIRS provides security, efficiency and it also reduce design complexity. In OIRS design the sparse image is taken because, it takes less memory in the database memory. By using this technique the retrieved image becomes accuracy and efficiency. The data users can easily reconstruct the original image without any loss.

Index Terms- sparse image, compressed sensing, security and efficiency, cloud computing.

I. INTRODUCTION

Technology has been improved and large-scale datasets are being exponentially generated today. Examples for various application contexts include medical images , remote sensing images, satellite image databases, etc. Along with the data explosion is the fast-growing trend to outsource the image management systems to cloud and leverage.It should be very effectively and efficiently store and share images to data owner to data user. Cloud is the open network can be operated by the third party On the other hand, many image datasets, e.g., the medical images with diagnostic resultsfor different patients, are privacy-sensitive by its nature . Thus, it is of critical importance to ensure that security must be embedded in the image service outsourcing design from the very beginning, so that we can better protect owners' data privacy without sacrificing the usability and accessibility of the information. Generally for image acquisition and sharing service, the data owner follows the Nyquistsampling theorem and often needs to acquire massive amounts of data samples, e.g., for high resolution images. Prior to transmission and image reconstruction, it is highly desirable to further pass these massive data through a compression stage for efficient usage of storage and bandwidth resources. Such that large data acquisition followed the compression can be wasted and it often lot of complexity on the data acquisition at the data owner side.
Compressed sensing is a recently proposed data sampling and reconstruction framework that unifies the traditional sampling and compression process for data acquisition, by leveraging the sparsity of the data. without data compression is data owner have faced lot problems so the data owner use the compressed sensing, then the data owners can easily capture compressed image samples via a simple non-adaptive linear measurement process from physical imaging devices, and later easily share them with users.

In this paper, we initiate the investigation for these challenges and propose a novel outsourced image recovery service (OIRS) architecture with privacy assurance. For the simplicity of data acquisition at data owner side, OIRS is specifically designed under the compressed sensing framework. The acquired image samples from data owners are later sent to cloud, which can be considered as a central data hub and is responsible for image sample storage and provides on-demand image reconstruction service for data users. Because reconstructing images from compressed samples requires solving an optimization problem [11], it can be burdensome for users with computationally weak devices, like tablets or large-screen smart phones. OIRS aims to shift such expensive computing workloads from data users to cloud for faster image reconstruction and less local resource consumption, yet without introducing undesired privacy leakages on the possibly sensitive image samples or the recovered image. Compared to directly reconstructing the image in the cloud is prohibited. OIRS is expected to bring considerable computational savings to the owner/users.

The rest of this paper is organized as follows. Section II discusses the related work. Section III introduces the system architecture, threat model, system design goals.. Then Section IV gives the detailed mechanism description, followed by security and efficiency analysis.

II. LITERATURE SURVEY

Here we briefly review distributed image reconstruction systems, compressed sensing, and security mechanisms. M. Atallah and J. Li proposed the sequence comparison problem, given two strings and of respective lengths n and m, consists of finding a minimum-cost sequence of insertions, deletions, and substitutions (also called an edit script) that transform[6] . In this framework 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 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($m \times n$) computation (which is optimal) and communication, where is the alphabet size, and thesolution is designed to work when the servers have only O ((m + n)) memory. By utilizing 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 well-known 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” relies on properties of the sensing matrix such as the restricted isometry property [4]. In this E. Cande's, establishes 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 complete information on the signal or image is available this is certainly a valid strategy. However, when the signal has to be acquired 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 complete 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 known under the terminology of compressed sensing, compressive sampling or sparse recovery provides a fundamentally 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 suitable basis, that is, by only a small number of non-zero coefficients. This is the key to the efficiency of many lossy compression techniques such as JPEG, MP3 etc. A compression is obtained by simply storing only the largest basis coefficients. When reconstructing the signal the non-stored coefficients are simply set to zero. This is certainly a reasonable strategy when full information of the signal is available. However, when the signal first has to be acquired by a somewhat costly, lengthy or otherwise difficult measurement (sensing) procedure, this seems to be a waste of resources: First, large efforts are spent in order to obtain full information on the signal, and afterwards 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 small number of measurements of the signal. It is not obvious at all whether this is possible since measuring directly the large coefficients requires knowing a priori their location. Quite surprisingly, compressive sensing provides 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 small bit streams (while keeping the essential features intact), in effect turning a large digital data set into a substantially smaller one[4]. E. Cande's and M. Wakin proposed Compressive sampling (CoSamp) is a new paradigm for developing data sampling technologies. It is based on the principle that many types of vector-space data are compressible, which is a term of art in mathematical signal processing [1].

III. Related work

Compressed sensing is a data sensing and reconstruction framework well-known for its simplicity of unifying the traditional sampling and compression for data acquisition**.** Compressed sensing is to compress the storage of correlated image datasets. The image is in compressed format that gives the reduction 50% in the storage. Theuncompressed format it takes more storage in space. But it does not provide any security.OIRS aims to achieve a much more ambitious goal, which is an outsourced image service platform and takes into consideration of security, efficiency, effectiveness and complexity. Those works explore the inherent security strength of linear measurement provided by the process of compressed sensing.This secure image recovery service in OIRS that we propose to explore is also akin to the literature of secure computation outsourcing [3], [6], [18], [20], [2], which aims to protects both input and output privacy of the outsourced computations. The Fully Homomophic Encryption is in the technique.The application of Homomorphic Encryption method on the Cloud Computing security, particularly the possibility to execute the calculations of confidential data encrypted.Homomorphic Encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption), the client is the only holder of the secret key. When we decrypt the result of any operation, it is the same as if we had carried out the calculation on the raw data.Another existing list of work thatloosely relates to (but is also significantly different from)our work is secure multiparty computation (SMC). SMC allows two or more parties to jointlycompute some general function while hiding their inputs toeach other. However, schemes in the context of SMC usuallyimpose comparable computation burden on each involvedparties, which is undesirable when applied to OIRS model. In short, practically efficient mechanisms with immediatepractices for secure image recovery service outsourcing incloud are still missing.

IV. System Architecture

V. Related work

The OIRS system architecture consists of following model service that include the following: At first, data owner acquires raw image data, in the form of compressed image samples, from the physical world under different imaging application contexts.

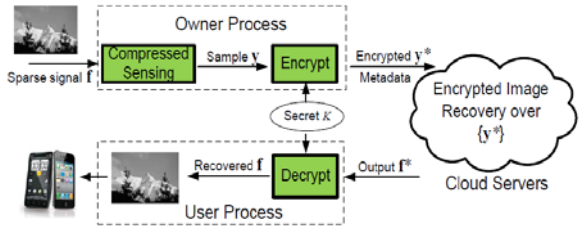

Fig. 1. The OIRS architecture in public cloud.

To reduce the local storage and maintence the data owner later outsource the image samples to the cloud for storage and processing. Depend on the request only the user can reconstruct the image. In this model data users are assumed to possess mobile devices with only limited computational resources.

Fig. 1 demonstrates the basic message flow in OIRS. Let **f** and **y** be the signal and its compressed samples to be capturedby the data owner. For privacyprotection, data owner 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 an output **f**_ directly over the encrypted **y**_ and sends **f**_ to data users. Finally, the user obtains **f** by decrypting **f**_. We leave the management and sharing of the secret keying material *K* between the data owner and users in our detailed decryption of OIRS design. In Fig. 1, each block module is considered as the process of a program taking input and producing output. We further assume that the programs are public and the data are private.

VI. The Proposed OIRS Design

For security, OIRS needs to protect the image samplesbeforeoutsourcing. The protected image samples shouldsupport image recovery as needed, while the recovered images at cloud should still be in an protected form. Forthese purposes, we study the secure transformation basedapproaches. Note that the l 1-min of Prob (1) is essentiallya linear program (LP) [2]:min1T·r,s.t.f=Ax,
-r<x<r. Here r is an n x 1 vector of variables. Let x+r-2s and x-r-2t.

BasicRequirements 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 1.

Data: security parameter 1k , random coins σ **Result:** K = (P,Q, e, π,M)

Begin

1. uses σ to generate random P, e, π,
2. uses σ to generate random Q and M,
3. return secret key K = (P,Q, e,π,M) ,

Algorithm 2: Problem Transformation Step 1 ProbTran(K , Ω) → Ωk. To better present our transformation in a flexible way, we propose to separate the transformation described into two steps. Namely, we can define ProbTran = (ProbTran 1, ProbTran 2), where ProbTran1 takes as input the secret key K and y, F in original LP Ω and outputs a tuple y' in Ωk , while ProbTran2 takes as input K and F and outputs tuples (F', π') in Ωk.

Data: transformation key K and original LP Ω **Result:** protected sample y' in Ωk

Begin 1. picks P, e from K and F from Ω, 2. return y' = P . (y + F . e) ,

Algorithm 3: Problem Transformation Step 2 ProbSolv(Ωk) → h. Because our transformation based design outputs Ωk as a standard LP problem, this algorithm on cloud side can be a general LP solver and thus its description is omitted.

Data: transformation key K and original LP Ω **Result:** protected coefficient matrices F', π' in Ωk

Begin

1. picks (P,Q, π,M) in K and F in Ω,
2. computes F' = PFQ and π' = (π - MF)Q,
3. return transformed F', π' ,

Algorithm 4: Original Answer Recovery

DataRec(K , h) → g. The user uses the secret key K to recover the original answer g for problem Ω from protectedanswer h of Ωk returned by cloud upon getting input of the secret key K and the answer h of k from cloud.

Data: transformation key K and protected answer h of Ωk
Result: answer g of original problem Ω
Begin

1. picks Q, e from K,
2. return g = Qh - e ,

VII. Empirical Evaluation

A. Experimental settings

We now show the experiment results of the proposed OIRS.We implement both the data owner/user and the cloud sideprocesses in MATLAB and use the MOSEK optimization toolbox as the LP solver. Allexperiments are done on the same workstation with an Intel Core i5 CPU running at 2.90 GHz and 6 GB RAM.

B. Efficiency Evaluation

We first measure the efficiency of the proposed OIRS. Specifically we focus on the computational cost of privacy assurance done by the data owner and data users, i.e., the local side, and the cost done by the cloud side. The cloud solves it for the data user, who then performs a decryption process to get the original image data vector and then recover the image. For completeness, we report the time cost here. For 32x32 image block it is 0.009 sec on average, while for 48_48 image block size it is 0.021 sec on average.

(a) Input image

(b) Compression

(c) Encrypted image

(d) Decrypted image

VIII. Conclusion

In this paper, we have proposed OIRS, an outsourced image recovery service from compressed sensing with privacy assurance. OIRS exploits techniques from different, and aims to take security, design complexity, and efficiency into consideration from the very beginning the service low. With OIRS, data owners can utilize the benefit of compressed sensing to consolidate the sampling and image compression via only linear measurements. Data users, on the other hand, can leverage cloud's abundant resources to outsource the image recovery related `1 optimization computation, without revealing either the received compressed samples, or the content of the recovered underlying image. Beside it simplicity and effciency, we show OIRS is able to achieve robustness and effectiveness in handling image reconstruction in cases of sparse data as well as non-sparse general data via proper approximation. Both extensive security analysis and empirical experiments have provided to demonstrate the privacy-assurance, effciency, and the effectiveness of OIRS.

References

[1] Cong Wang,Bingsheng Zhang,Kui Ren,Janet M.Wang, “Privacy-assured Outsourcing of image Reconstruction Service in Cloud”,IEEE Transaction on Cloud Computing.,Vol : 1,No:1 Year 2013.

[2] (1996). Health Insurance Portability and Accountability Act of (HIPPA) [Online]. Available:http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

[3] P. Agouris, J. Carswell, and A. Stefanidis, ``An environment for contentbased image retrieval from large spatial databases," ISPRS J. Photogram. Remote Sens., vol. 54, no. 4, pp. 263_272, 1999.

[4] M. Atallah and K. Frikken, ``Securely outsourcing linear algebra computations," in Proc. 5th ASIACCS, 2010, pp. 48_59.

[5] M. Atallah and J. Li, ``Secure outsourcing of sequence comparisons," Int. J. Inf. Security, vol. 4, no. 4, pp. 277_287, 2005.

[6] M. Atallah, K. Pantazopoulos, J. Rice, and E. Spafford, ``Secure outsourcing of scientific computations," Adv. Comput., vol. 54, pp. 216_272,Feb.2001.

Authors

First Author – M. Jeevitha Lakshmi , Department of Electronics and Communication Engineering, Dr.S.J.S. Paul Memorial College of Engineering and Technology, Pondicherry University, India., Email: jeevithalakshmi93@gmail.com
Second Author – S. Umapriya, Department of Electronics and Communication Engineering, Dr.S.J.S. Paul Memorial College of Engineering and Technology, Pondicherry University, India., Email: umapriya1010@gamil.com
Third Author – R. Ramya, Department of Electronics and Communication Engineering, Dr.S.J.S. Paul Memorial College of Engineering and Technology, Pondicherry University, India., Email: rajramya460@gmail.com
Fourth Author – M. SivaSindhu, Department of Electronics and Communication Engineering, Dr.S.J.S. Paul Memorial College of Engineering and Technology, Pondicherry University, India., Email: sakthi.sindhu28@gmail.com