ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Privacy-Assured OIRS Service with Performance Speedup in Cloud

P.ARUNPRIYA1,S.RINESH2

ME, Dept. of CSE, Karpagam University, Coimbatore, Tamil Nadu, India[1]

Assistant Professor, Dept. of CSE, Karpagam University, Coimbatore, Tamil Nadu, India[2]

ABSTRACT: At the moment wide Ranging image data sets are being rapidly generated. Along with such data explosion is the fast-growing vogue to outsource the image management systems to the cloud for its lavish computing resources and benefits.However,how to protect the sensitive data while enabling outsourced image services, becomes a major concern. To address these challenges, we propose outsourced image recovery service (OIRS), a novel outsourced image recovery service architecture, which deeds different domain technologies and takes security, efficiency, and design complexity into consideration from the very beginning of the service flow. Specifically, we choose to design OIRS under the compressed sensing framework, which is known for its simplicity of unifying the traditional sampling and compression for image attainment. Data owners only need to outsource compressed image samples to cloud for diminish storage overhead. In addition, in OIRS, data users can hitch the cloud to securely reconstruct images without enlightening information from either the compressed image samples or the underlying image content. We start with the OIRS design for sparse data, which is the typical application scenario for compressed sensing, and then show its natural extension to the general data for meaningful tradeoffs between efficiency and accuracy. We thoroughly analyze the privacy-protection of OIRS and conduct far reaching experiments to demonstrate the system effectiveness and efficiency. For completeness, we also discuss the expected performance speedup of OIRS through hardware built-in system design.

Index terms: Compressed sensing, security and privacy, cloud computing, image reconstruction,Image outsourcing.

I. INTRODUCTION

The advancement of information and computing technology,wide range datasets are being exponentially generated nowadays. Examples under various application contexts include medical images, remote sensing images [3],satellite image databases, etc. Along with such data explosion is the fast-growing vogue to outsource the image management systems to cloud and leverage its economic yet lavish computing resources to efficiently and effectively acquire, store, and share images from data owners to a large number of data users .Although outsourcing the image services is quite promising, in order to become truly successful, it still faces a number of fundamental and critical challenges, among which security is the top item. This is due to the fact that the cloud is an open environment operated by external third parties who are usually outside of the data owner/users' trusted domain [13], [18]. On the other hand, many image datasets, e.g., the medical images with diagnostic results for different patients, are privacy-sensitive by its nature [3].Thus, it is of critical importance to ensure that security must be embedded in the image service outsourcing design from the very beginning.

Reconstructing images from compressed samples requires solving an optimization problem [12], 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

without introducing undesired privacy leakages on possibly sensitive image samples or the recovered image content. To meet these challenging requirements, a core part of the OIRS design is a tailored light weight problem transformation

mechanism, which can help data owner/user to protect the sensitive data contained in the optimization problem for original image reconstruction.

II. RELATED WORK

Compressed sensing [9], [11], [15] is a recent data sensing and reconstruction framework well-known for its simplicity of unifying the traditional sampling and compression for data acquisition. Along that line of research, one recent work [14] by Divekar et al. proposed to leverage compressed sensing to compress the storage of correlated image datasets. The idea is to store the compressed image samples on behalf of the whole image, either in compressed or uncompressed format, on storage servers. Their results show that storing compressed samples offers about 50% storage reduction compared to storing the original image in uncompressed format or other data
application scenarios where data compression may not be done. But their work does not consider security in mind, which is an indispensable design requirement in OIRS. In fact, compared to [13] that only focuses on storage trimdown, our proposed 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 from the very beginning of the service flow.

III. PROBLEM STATEMENT

A. SERVICE MODEL AND THREAT MODEL

The basic service model in the OIRSarchitecture includes 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. To trimdown the local storage and maintenance overhead, data owner later outsources the raw image samples to the cloud for storage and processing. The cloud will on-demand reconstruct the images from those samples upon receiving the requests from the users. In our model, data users are assumed to possess mobile devices with only limited computational resources.
Throughout this paper, we consider a semi-trusted cloud as the adversary in OIRS. The cloud is assumed to honestly perform the image reconstruction service as specified, but be curious in learning owner/user's data content. Because the images samples captured by data owners usually contain data specific/sensitive information, we have to make sure no data outside the data owner/user's process is in unprotected format.

B. DESIGN GOALS

Our design goals for OIRS under the aforementioned service and threats model consist of the following.

- **Security:** OIRS should provide the strongest possible protection on both the private image samples and the content of the recovered images.
- **Effectiveness:** OIRS should enable cloud to effectively perform the image reconstruction service over the encrypted samples.
- **Efficiency:** OIRS bring savings from the computationand/or storage aspects to data owner and users.
- **Extensibility:** In addition to image reconstruction service,OIRS should be made possible to support other extensible service interfaces and even performance speedup via hardware built-in design.

IV. THE OIRS DESIGN

While compressed sensing simplifies the data acquisition atdata owner, it makes the data recovery from the compressed samples a computationally intensive task. As introduced in the preliminary, it requires the data users to solve an

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

optimization problem, which could be very challenging for the data user with computationally weak devices like smart phones. Therefore, enabling a secure data recovery service by leveraging the cloud is of critical importance in our proposed OIRS architecture. Due to the sensitive nature of data, to outsource compressed image samples directly to the cloud is

prohibited. And we need to protect the image samples before outsourcing them to the cloud. The cloud should not be able to learn the private content of the image samples either before or after the image reconstruction.

A. FRAMEWORK AND SECURITY DEFINITIONS OF OIRS

Given the problem formation for image reconstruction in Section III-C,our design challenge in OIRS is how to let the cloud efficiently solve the optimization problem, Ω= D (**F**; **y**; **I**; **1T**), for image reconstruction without learning content of either compressed image samples **y** or the reconstructed image data **g**. To meet these design challenges,

Definition 1: A transformation scheme r = D(KeyGen, ProbTran, ProbSolv, DataRec) is secure if

Ω0,Ω1 : Pr[K←keyGen(1k):ProbTran(K,Ω0)=Ωk]

-Pr[K←keyGen(1k):Probtran(K,Ωk]≤

where is a negligible function.

From the perspective of indistinguishability, such a security formulation is also loosely related to the general formulation of differential privacy [15], [16].

B. THE BLUEPRINT OF PROBLEM TRANSFORMATION

According to our framework and security definition, the purpose of ProbTran is to transform Ω into a random Ωk where the latter shares the same problem structure as the former, **y** and **F** are supposed to be protected against the cloud, while **I** and **1T** are public information. Thus, the challenge of the transformation based design is that we have to ensure such public information will not be maliciously leveraged by the cloud to tamper the overall protection of OIRS.

1) We use a random generalized permutation matrix with positive entries, i.e., the product of a non-zero positive diagonal and a permutation matrix, to rewrite the inequality constraints.

min **1T** . **g**

subject to **y** = **F** .g, . **g** ≥**0**.

Note that **g** ≥ **0** is equivalent to **g** ≥ **0**.

2) We randomly pick a 2n x 2n invertible matrix **Q** and a 2n x 1 vector **e** to protect the solution **g** via af_ne maping **g** = **Qh** – **e.**

min **1T** .(**Qh - e**)

subject to **F. Q** . **h** = **y** + **F** .**e**;

Q .**h** ≥ **e**.

3) We multiply a random 2n x m matrix **M** to equality constraints and later mix the result together with the inequality constraints

min **1T** . (**Qh - e**)

subject to **F** . **Q** . **h** = **y** + **F** . **e**;

This problem is equivalent to the one in Step 2

.

4) We multiply a random m_m invertible matrix **P** to the both sides of equality constraints

min **1T** . (**Qh - e**)

subject to **PFQ** . **h** = **P** . (**y** + **F** . **e**).

C. THE SCHEME DETAILS

Scheme details: Based on the above instantiation, we describe the complete protocol for the OIRS framework **r**.

Algorithm 1 Key Generation

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Data: security parameter 1k ,random coins
Result: K D (**P**;**Q**; **e**; ;**M**)
% discussion on choice of k deferred in Section V;
begin
1 uses to generate random **P**; **e**; ;

2 uses to generate random **Q** and **M**;
% satisfying the structure of Ωk in Prob. 5
3 return secret key K = (**P**;**Q**; **e**; ;**M**) ;
Algorithm 2 Problem Transformation Step 1
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
Data: transformation key K and original LP Ω
Result: protected coefficient matrices **F',** in Ωk
begin
1 picks (**P**;**Q**; ;**M**) in K and **F** in Ω;
2 computes **F**'= **PFQ** and - **MF**)**Q**;
3 return transformed **F**', ;
Algorithm 4 Original Answer Recovery
Data: transformation key K and protected answer **h** of k
Result: answer **g** of original problem Ω
begin
1 picks **Q**; **e** from K;
2 return g = **Qh - e** ;
DATA SAMPLING PHASE
1) Data owner picks a fresh seed and generates a secret key K = (**P,Q,e,**)

2) He acquires the sample **y** = **Rx = RVf** = **Af** to cloud

We assume the samples and the related seeds f**y**'; sg are all stored in an authenticated manner at cloud. Assume that data user issues an image recovery request for an image sample **y**' to data owner.
IMAGE RECOVERY PHASE
1) Data owner downloads the seed s from cloud, computesF(sk; s), and uses to regenerate the matrix **R** and the key K D (**P**;**Q**; **e**;**M**) from KeyGen.He calls ProbTran2(K; **F**) to get (**F**0; _0) and sends them to cloud.
2) With Ωk= (**F**'; ; **y**';**1T**), the cloud calls ProbSolv (Ωk) to output answer **h** to user, together with
seed s.
3) The user computes F(sk; s), and uses to generate the key K from KeyGen(1k). He then calls
DataRec(K; **h**) to get **g** = **Qh - e** and recovers the image **x** = **Vf**, where **f** is derived from **g**.
D. THE EXTENSION TO NON-SPARSE DATA
So far, we have been assuming that OIRS operates over sparse data only. That is, **f** is exactly sparse. However, there are many cases where physical data sources are not exactly sparse. To further broaden the application spectrum of OIRS

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

design, we now show how to extend from the case of sparse data to the non-sparse general data. Specifically, assuming under orthonormal basis **V**, the image data **x**'s coefficient vector **f** is non-sparse. We denote **f**s as an s-sparse approximation of **f**, which can be derived by setting all but the largest s entries of **f** to zero. Let **x**s = **Vf**s. Because **V** is orthonormal, then
$\| \mathbf{x} - \mathbf{x}s \|2 = \| \mathbf{Vf} - \mathbf{Vf}s \|2 = \| \mathbf{f} - \mathbf{f}s \|2.$
And its difference compared to the actual s-sparse approximation **f**s satisfies the following bound,
$\| f^* - f \| \leq Co/\sqrt{} \| f - fs \| 1,$

where C0 is some constant.
The above elaboration suggests that the aforementioned OIRS design can be still applied to the non-sparse general data.
.

V. THEORETICAL ANALYSIS

EFFICIENCY ANALYSIS
The most time-consuming operations in the proposed transformation is the matrix-matrix operations, which cost asymptotically O(n)for some 2 < < 3 due to m < 2n. On the other hand, solving the LP problem ΩK usually requires more than O(n3) time, e.g. [23]. Clearly, outsourcing image recovery service to cloud provides data owners/users considerable computational savings in theory. Moreover, with our proposed transformation, the cloud process can utilize any existing solvers for the LP problem ΩK , which ensures the cloud side efficiency
This study in [13] has shown that using compressive sensing can reduce storage overhead up to 50%, compared to storing the original data or images in uncompressed format.

VI. FURTHER DISCUSSIONS

Enabling secure image outsourcing services will significantly boost the wide application spectrum of secure computing outsourcing. For example, the proposed OIRS can be adopted by image service applications like MRI in health care system, remote sensing in geographical system, and even military image sensing in various mission critical contexts. In the following, we give some further discussions on how the proposed OIRS can serve as a stepping stone and discuss the possible performance speedup through hardware built-in design.

A. SPEEDUP WITH HARDWARE BUILT-IN DESIGN
In order to make these promising image services in OIRS truly efficient and practically deployable, it is pivotal to further explore how to embed the security and efficiency guarantee from the start through a hardware design can significantly boost the performance of functionalities that are to be implemented in the proposed service architecture.For example, by giving the hardware design the transformed image samples **P**(**y** + **Ae**) and the sensing matrix **PAQ** satisfying (**PAQ**) . (**Q**-1(**f** + **e**)) = **P**(**f** + **Ae**).Itwould still give us a randomly transformed output **Q**-1(**f** + **e**) as the encrypted result.

VII. EMPIRICAL EVALUATIONS

A. EXPERIMENT SETTINGS
We now show the experiment results of the proposed OIRS.We implement both the data owner/user and the cloud side processes in MATLAB and use the MOSEK optimization toolbox (http://www.mosek.com/) as the LP solver. All experiments 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

data user, who then performs a decryption process to get the original image data vector andthen 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.

C. EFFECTIVENESS EVALUATION

We next assess the effectiveness of OIRS design. Our goal is to show the correctness of the design and also the empirical results on the privacy assurance.

1.CORRECTNESS EVALUATION

For correctness of the design, we show that all the images, after transformation and later recovered on the data user side, still preserves the same level of visual quality as the original images. Here we want to point out that the reconstructed image quality increases along with the number of measurements, and the more the better. In our experiments, we follow the ``four-to-one'' rule according to [11].

2.PRIVACY-ASSURANCE EVALUATION

Recall that OIRS provides the privacy-assurance that users can harness the cloud to securely recover the image without revealing the underlying image content. This can be achieved because what cloud really recovers, **h**, protects the original sparse vector **h** via a general af_ne mapping **g** = **Qh** - **e** with a random choices of **Q** and **e**. To give the empirical results on privacy-assurance,) the recovered image before user decryption, i.e., recovering using the blinded vector **h** = **Q -1(g** + **e**

VIII. CONCLUSION

In this paper, we have proposed OIRS, an outsourced image recovery service from compressed sensing with privacy assurance. Both extensive security analysis and empirical experiments have been provided to demonstrate the privacy-assurance, effciency, and the effectiveness of OIRS. On top of the current architecture, we also demonstrate a proof-of-concept of possible performance speedup through hardware built-in system design, which we believe is our important future work to be pursued.

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.
[7] D. Benjamin and M. Atallah, ``Private and cheating-free outsourcing of algebraic computations," in Proc. Conf. PST, 2008, pp. 240_245.
[8] E. Candès, ``The restricted isometry property and its implications for compressed sensing," Comptes Rendus Mathematique, vol. 346, nos. 9_10, pp. 589_592, 2008.
[9] 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.
[10] E. Candès and T. Tao, ``Decoding by linear programming," IEEE Trans. Inf. Theory, vol. 51, no. 12, pp. 4203_4215, Dec. 2005.
[11] 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.
[12] E. Candès and M. Wakin, ``An introduction to compressive sampling," IEEE Signal Proc. Mag., vol. 25, no. 2, pp. 21_30, Mar. 2008.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[13] (2009). Security Guidance for Critical Areas of Focus in Cloud Computing, [Online]. Available: http://www.cloudsecurityalliance.org
[14] 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.
[15] D. Donoho, ``Compressed sensing," IEEE Trans. Inf. Theory, vol. 52, no. 4,pp. 1289_1306, Apr. 2006.
[16] C. Dwork, ``Differential privacy," in Proc. ICALP, 2006, pp. 1_12.
[17] C. Dwork, ``The differential privacy frontier (extended abstract)," in Proc. TCC, 2009, pp. 496_502.
[18] (Nov. 2009). Eur. Netw. Inf. Security Agency. Cloud Computing Risk Assessment, Heraklion, Greece [Online]. Available: http://www.enisa.europa.eu/act/rm/_les/deliverables/cloud-computing-risk-assessment
[19] R. Gennaro, C. Gentry, and B. Parno, ``Non-interactive veri_able computing: Outsourcing computation to untrusted workers," in Proc. CRYPTO, Aug. 2010, pp. 465_482.
[20] O. Goldreich, S. Micali, and A.Wigderson, ``How to play any mental game or a completeness theorem for protocols with honest majority," in Proc. STOC, 1987, pp. 218_229.