*Darapaneni Chandra Sekhar Int. Journal of Engineering Research and Applications* www.ijera.com
*ISSN : 2248-9622, Vol. 4, Issue 10( Part -1), October 2014, pp.84-88*

RESEARCH ARTICLE OPEN ACCESS

# An Enhanced trusted Image Storing and Retrieval Framework in Cloud Data Storage Service Environment

Darapaneni Chandra Sekhar *, M.Chandra Naik **
*(Department of Computer Science, Guntur Engineering College, Guntur, India)
** (Department of Computer Science, Guntur Engineering College, Guntur, India)

**ABSTRACT**
Today's image capturing technologies are producing High Definitional-scale images which are also heavier on memory, which has prompted many users into cloud storage, cloud computing is an service based technology and one of the cloud service is Data Storage as a Service (DSaaS), two parties are involved in this service the Cloud Service Provider and The User, user stores his vital data onto the cloud via internet example: Dropbox. but a bigger question is on trustiness over the CSP by user as user data is stored remote devices which user has no clue about, in such situation CSP has to create a trust worthiness to the costumer or user, in these paper we addressed the mention insecurity issue with a well defined trusted image Storing and retrieval framework (TISR) using compress sensing methodology.
***Keywords***- Compressed sensing, security and privacy, cloud computing, image reconstruction**.**

## I. INTRODUCTION

As per [1] "Verifying the image data security has emerged as a major issue in image storing on cloud Environments". Cloud computing has been great revolution in handling outsourced data services With the advancement of information and computing technology, High definition images which provides vital information's like large-scale datasets medical images [28], remote sensing images [2], satellite image databases, etc. Along with such data explosion is the fast-growing trend to outsource the image management systems to cloud and leverage its economic yet abundant computing resources [25] to efficiently and effectively acquire, store, and share images from data owners to a large number of data users [24].

Outsourcing the image to cloud 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 concern. 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 [12], [17]. On the other hand, many image datasets, e.g., the medical images with diagnostic results for different patients, are privacy-sensitive by its nature [1].

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. Besides, due to the high-dimensionality and large-scale of the image datasets [24], it is both necessary and desirable that the image service outsourcing design should be as efficient and less resource-consuming as possible, in terms of bandwidth and storage cost on cloud.

Traditionally, to establish such an image acquisition and sharing service, the data owner follows the Nyquist sampling 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 a framework of large data acquisition followed by compression can be very wasteful, and often poses a lot of complexity on the data acquisition mechanism design at data owner side. For example, increasing the sampling rate can be very expensive in modern imaging systems like medical scanners and radars [30].

Compressed sensing [8], [10], [14] 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.1 With compressed sensing, 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 addition to simplified image acquisition and sharing, one can also apply compressed sensing, i.e., the process of taking non-adaptive linear measurements, over any existing large-scale image dataset, for the purpose of storage overhead reduction [13]. Specifically, as later shown in Section III-C, because the size of the

sample vectors is almost always much less than the original image data, simply storing the compressed sample vectors rather than the actual image data can help save the storage cost as much as 50% [13]. Understanding these benefits of compressed sensing is pivotal, because it would allow us to explore new possibilities of establishing secure and privacy-assured image service outsourcing in cloud computing, which aims to take security, complexity, and efficiency into consideration from the very beginning of the service flow.

In this paper, we initiate the investigation for these challenges and propose a novel outsourced image recovery service (TISR) architecture with privacy assurance. For the simplicity of data acquisition at data owner side, TISR 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. TISR 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 content. To meet these challenging requirements, a core part of the TISR design is a tailored lightweight problem transformation mechanism, which can help data owner/user to

1To be consistent with the majority work in compressed sensing, we treat images as real-valued signals or data with finite dimensions, which can be represented as a long one-dimensional vector

protect the sensitive data contained in the optimization problem for original image reconstruction. Cloud only sees a protected version of the compressed sample, solves a protected version of the original optimization problem, and outputs a protected version of the reconstructed image, which can later be sent to data user/owner for easy local post processing. Compared to directly reconstructing the image locally, TISR is expected to bring considerable computational savings to the owner/users. As another salient feature, TISR also has the benefit of not incurring much extra computational overhead on the cloud side. Our contributions can be summarized as follows.

- To our best knowledge, TISR is the first image service outsourcing design in cloud that addresses the design challenges of security, complexity, and efficiency simultaneously.
- We show that TISR not only supports the typical sparse data acquisition and reconstruction in standard compressed sensing context, but can be extended to non-sparse general data via approximation with broader application spectrum.
- We thoroughly analyze the security guarantee of TISR and demonstrate the efficiency and effectiveness of TISR via experiment with real world data sets. For completeness, we also discuss how to achieve possible performance speedup via hardware built-in system design.

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, and some preliminaries. Then Section IV gives the detailed mechanism description, followed by security and efficiency analysis in Section V and further discussions on performance speedup in Section VI. Section VII gives the empirical results. Finally, Section VIII gives the concluding remarks.

## II. Previous Work

Compressed sensing [8], [10], [14] is a 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 [13] by Donoho . to leverage compressed sensing to compress the storage of correlated image datasets. The idea is to store the compressed image samples instead 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 TISR. In fact, compared to [13] that only focuses on storage reduction, our proposed TISR 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. Another interesting line of research loosely related to the proposed TISR is about the security and robustness of compressed sensing based encryption [27], [29]. Those works explore the inherent security strength of linear measurement provided by the process of compressed sensing. The authors have shown that if the sensing matrix is unknown to the adversary, then the attempt to exhaustive searching based original data recovery

can be considered as computationally infeasible. However, these results are not applicable to TISR as we intentionally want the cloud to do the image reconstruction job for us, with the challenge of not revealing either the compressed samples or the reconstructed image content.

This privacy-preserving image recovery service in TISR that we propose to explore is also akin to the literature of secure computation outsourcing [3]_[6], [18], [20], [21], which aims to protects both input and output privacy of the outsourced computations. With the breakthrough on fully homomorphic encryption (FHE), a recent work by Gennaro et al. [18] shows that a theoretical solution has already been feasible. The idea is to represent any computation via a garbled combinational circuit [28] and then evaluate it using encrypted input based on FHE. However, such a theoretical approach is still far from being practical, especially when applied in the contexts of image sensing and reconstruction contexts. Both the extremely large circuit and the huge operation complexity of FHE make the general solution impossible to be handled in practice, at least in a foreseeable future. Researchers have also been working on specific designs for securely outsourcing specialized computation tasks, like scientific computations, sequence comparisons, matrix multiplications, modular exponentiations,
etc. [3]_[6]. Again, the highly customised design, some of which even involve heavy cryptographic protocols, are also not applicable in TISR. Another existing list of work that loosely relates to (but is also significantly different from) our work is secure multiparty computation (SMC). Firstly introduced by Rachlin [28] and later extended by Goldreich et al. [19] and others. SMC allows two or more parties to jointly compute some general function while hiding their inputs to each other. However, schemes in the context of SMC usually impose comparable computation burden on each involved parties, which is undesirable when applied to TISR model.
In short, practically efficient mechanisms with immediate practices for secure image recovery service outsourcing in cloud are still missing.

## III. PROBLEM SOLVING

### 3.1 Service Model and Threat Model

The basic service model in the TISR architecture 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 reduce 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.

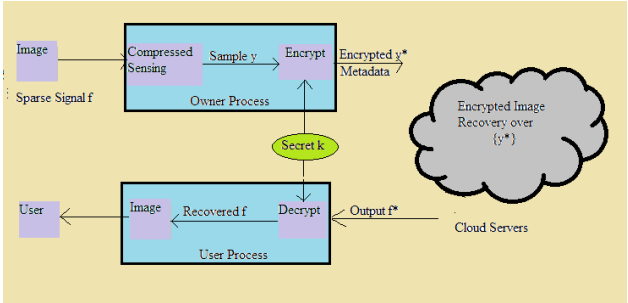


**Figure 1.** The TISR architecture in public cloud.

Fig. 1 demonstrates the basic message flow in TISR. Let **f** and **y** be the signal and its compressed samples to be captured by the data owner (to be elaborated in Section IV). For privacy protection, data owner in TISR 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 TISR 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.

Throughout this paper, we consider a semi-trusted cloud as the adversary in TISR. 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.

### 3.2 Design model

Design model for TISR

- Security: TISR should provide the strongest possible protection on both the private image samples and the content of the recovered images from the cloud during the service flow.
- Effectiveness: TISR should enable cloud to effectively perform the image reconstruction service over the encrypted samples, which can later be correctly decrypted by user.
- Efficiency: TISR should bring savings 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: In addition to image reconstruction service, TISR should be made possible to support other extensible service interfaces and even performance speedup via hardware built-in design.

## IV. THE TISR DESIGN

While compressed sensing simplifies the data acquisition at data 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 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 lever- aging the cloud is of critical importance in our proposed TISR 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. To securely answer all these challenges while maintaining practically acceptable performance, we propose to investigate the secure transformation based approaches to achieve secure image reconstruction outsourcing to cloud. Below we start with the introduction of TISR framework and its related security definition.

### 4.1 Framework and Security Definitions of TISR

Given the problem formation for image reconstruction in Section III-C, our design challenge in TISR is how to let the cloud efficiently solve the optimization problem, $\Omega = (\mathbf{F}, \mathbf{y}, \mathbf{I}, \mathbf{1}^{\mathbf{T}})$, for image formation without equating content of either compressed image samples y or the reestabilshed image data g. To meet these design challenges, we propose to build TISR via the following random trans-formation based framework, which includes 4 probabilistic polynomial time algorithms as described below.

- PGenaration is a algorithm running at the data owner end, which generates the secret key $P$ upon getting input of some security parameter $1^p$.
- PTrans is a problem transformation algorithm flexibly running at either data owner or data user side, which generates a randomly transformed optimization problem $\Omega_p$ upon getting input of some secret key $P$ and an original problem $\Omega$.
- PSolv is a problem solving algorithm running at the cloud side, which solves the transformed problem $\Omega_p$ and generates answer h.
- PRec is the recover algorithm running at the data user side, which generates the answer g of original problem $\Omega$ upon getting input of the secret key $P$ and the answer h of $\Omega_p$ from cloud.

We denote this framework of TISR as r=(PGen,PTran, PSolv, PRec). Because r is supposed to be a random transformation framework, its security strength really hinges on the adversary's advantage of guessing $\Omega$ given $\Omega_p$. Intuitively, for any two problems $\Omega 0$, $\Omega 1$ with the same size as defined in Eq. (4), it would be difficult for the adversary to tell them apart after the random transformation. Formally, we define the security strength of as follows.

## V. Privacy-Assurance Evaluation

Recall that TISR 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 affine mapping **g** = **Qh – e** with a random choices of **Q** and **e**. To give the empirical results on privacy-assurance, recovering using the blinded vector **h** = **Q**-1(**g** + **e**).

In both cases, the quick affine map by **Q** and **e** over **g** provides good enough protection for image protection. This explains given the basis **V** and the recovered encrypted vector **h** only consists of unclear image segments.. It is safe to say that TISR provides satisfactory trustiness. That is, without knowledge of secret key, the actual content of the protected underlying image cannot be perceived.

## VI. CONCLUSION

In this paper, we have proposed TISR framework, ISR provides the privacy-assurance that users can harness the cloud to securely recover the image without revealing the underlying image content. With TISR, data owners can utilize the benefit of compressed sensing to consolidate the sampling and image compression via only linear measurements. TISR 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 been provided to demonstrate the privacy-assurance, efficiency, and the effectiveness of TISR. 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] 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

[2] M. Abe and S. Fehr. Perfect NIZK with adaptive soundness. InProc. of Theory of Cryptography Conference (TCC '07),2007. Full version available on Cryptology ePrint Archive, Report 2006/423.[3] M. Atallah and K. Frikken, ``Securely outsourcing linear algebra computations," in *Proc. 5th ASIACCS*, 2010, pp. 48_59.

[3] G. Yamamoto, E. Fujisaki, and M. Abe. Anefficiently-verifiable zero-knowledge argument for proofs of knowledge. Technical Report ISEC2005-48, IEICE, July 2005.

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

[5] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu. Plutus: Scalable secure file sharing on untrusted storage. In Proc. of FAST, 2003..

[6] E. Candès, ``The restricted isometry property and its implications for compressed sensing," *Comptes Rendus Mathematique*, vol. 346, nos. 9_10, pp. 589_592, 2008.

[7] 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.

[8] E. Candès and T. Tao, ``Decoding by linear programming," *IEEE Trans.Inf. Theory*, vol. 51, no. 12, pp. 4203_4215, Dec. 2005.

[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] E. Candès and M. Wakin, ``An introduction to compressive sampling," *IEEE Signal Proc. Mag.*, vol. 25, no. 2, pp. 21_30, Mar. 2008.

[11] (2009). *Security Guidance for Critical Areas of Focus in Cloud Computing*, [Online]. Available: http://www.cloudsecurityalliance.org

[12] 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.

[13] D. Donoho, ``Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289_1306, Apr. 2006.

[14] C. Dwork, ``Differential privacy," in *Proc. ICALP*, 2006, pp. 1_12.

[15] C. Dwork, ``The differential privacy frontier (extended abstract)," in *Proc.TCC*, 2009, pp. 496_502.

[16] (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

[17] R. Gennaro, C. Gentry, and B. Parno, ``Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in *Proc. CRYPTO*, Aug. 2010, pp. 465_482.

[18] 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.

[19] S. Goldwasser, Y. T. Kalai, and G. Rothblum, ``Delegating computation: Interactive proofs for muggles," in *Proc. STOC*, 2008, pp. 113_122.

[20] S. Hohenberger and A. Lysyanskaya, ``How to securely outsource cryptographic computations," in *Proc. TCC*, 2005, pp. 264_282.

[21] C. Jansson, ``An np-hardness result for nonlinear systems," *Reliable Comput.*, vol. 4, no. 4, pp. 345_350, 1998.

[22] N. Karmarkar, ``A new polynomial-time algorithm for linear programming," *Combinatorica*, vol. 4, no. 4, pp. 373_396, 1984.

[23] 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.

[24] P. Mell and T. Grance, (2011). *The Nist De_nition of Cloud Computing* [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[25] 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.

[26] T. S. J. Schwarz and E. L. Miller. Store, forget, and check:Using algebraic signatures to check remotely . In Proceedings of ICDCS '06. IEEE Computer Society, 2006.

[27] Y. Deswarte, J.-J. Quisquater, and A. Saidane. Remoteintegrity checking. In Proc. of Conference on Integrity andInternal Control in Information Systems (IICIS'03),November 2003..

[28] Y. Rachlin and D. Baronm, ``The secrecy of compressed sensing measurements," in *Proc. Allerton Conf. Commun., Control, Comput.*, 2008, pp. 813_817.