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 SISR 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, SISR is expected to bring considerable computational savings to the owner/users. As another salient feature, SISR 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, SISR is the first image service outsourcing design in cloud that addresses the design challenges of security, complexity, and efficiency simultaneously.
- We show that SISR 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 SISR and demonstrate the efficiency and effectiveness of SISR 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.

2. Related 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 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 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 SISR. In fact, compared to [13] that only focuses on storage reduction, our proposed SISR 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 SISR 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 SISR 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 SISR 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 [32] 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 designs, some of which even involve heavy cryptographic protocols, are also not applicable in SISR. 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 Yao [32] 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 SISR model.

In short, practically efficient mechanisms with immediate practices for secure image recovery service outsourcing in cloud are still missing.

3. Problem Statement

3.1 Service Model and Threat Model

The basic service model in the SISR 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 reconstructs 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.

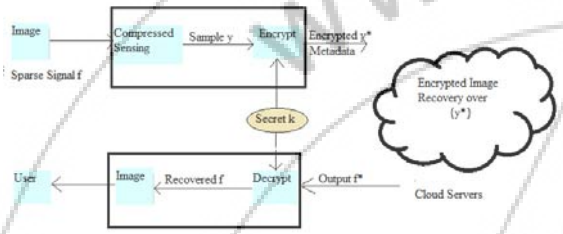

Figure 1: The SISR architecture in public cloud

Fig. 1 demonstrates the basic message flow in SISR. 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 SISR 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 SISR 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 SISR. 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 Goals

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

- Security: SISR 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: SISR should enable cloud to effectively perform the image reconstruction service over the encrypted samples, which can later be correctly decrypted by user.
- Efficiency: SISR 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, SISR should be made possible to support other extensible service interfaces and even performance speedup via hardware built-in design.

4. The SISR 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 SISR 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 SISR framework and its related security definition.

4.1 Framework and Security Definitions of SISR

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

- KeyGen 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^K.
- ProbTran is a problem transformation algorithm flexibly running at either data owner or data user side, which generates a randomly transformed optimization problem Ω_k upon getting input of some secret key K and an original problem Ω.
- ProbSolv is a problem solving algorithm running at the cloud side, which solves the transformed problem Ω_k and generates answer **h**.
- DataRec is the recover algorithm running at the data user side, which generates the answer **g** of original

problem Ω upon getting input of the secret key K and the answer **h** of Ω_k from cloud.

We denote this framework of SISR as Γ = (KeyGen,ProbTran, ProbSolv, DataRec). Because Γ is supposed to be a random transformation framework, its security strength really hinges on the adversary's advantage of guessing Ω given Ω_k. Intuitively, for any two problems Ω 0, Ω 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
Γ as follows.

5. Further Discussions

Enabling secure image outsourcing services will significantly boost the wide application spectrum of secure computing outsourcing. For example, the proposed SISR 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 SISR can serve as a stepping stone and discuss the possible performance speedup through hardware built-in design.

5.1 Efficiency Evaluation

We first measure the efficiency of the proposed SISR. 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. Table 1 gives our experimental results, where each entry in the table represents the mean of 10 trials. Each trial focuses on one randomly selected image block recovery, and Fig. 2 shows some of the tested images.

The first two columns report the size of image blocks in the test. Recall in SISR, data owner computes the randomly transformed optimization problem (in two steps) to the cloud. 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. Thus, the third and the forth columns in Table 1 reports the local computational cost by the data owner and data users, specifically including the time cost for overall problem transformation done by the data owner *towner* , and the time cost of image data decryption done by the data user *tuser*. The fifth column reports original image reconstruction cost without outsourcing, *toriginal* , which measures the time of solving the original LP problem locally. In order to better report the practical efficiency, we evaluate how much computational savings SISR can provide to data owner/users via outsourcing. This can be measured via the total time of image reconstruction without outsourcing (i.e., original local cost) divided by the total local time cost of problem transformation and image decryption in SISR (i.e., current local cost), denoted as *asymmetric speedup* =*toriginal*/*towner*+*tuser*. From the table, we can see that SISR can bring more than 3:4_savings for the selected size of image blocks. Because reconstructing large image may require computation over many small image blocks, it is suggested that SISR can shift a considerable amount of computational overhead from local to cloud. Note that SISR does not require any specific solver algorithm, and the cloud side process can utilise any existing LP solver for image reconstruction.

For *asymmetric speedup* measurement, we do not include the final cost on the data user, who performs one matrix vector multiplication using the orthonormal basis and the decrypted sparse vector to recover the actual image block. This is because of the consideration that such a step anyway needs to be performed by data user in both the original recovery without outsourcing and the proposed SISR. For completeness, we report the time cost here. For 32*32 image block it is 0.009 sec on average, while for 48*48 image block size it is 0.021 sec on average.

5.2 Effectiveness Evaluation

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

5.2.1 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]. It is suggested that if the number of captured compressed samples is roughly 4* the sparsity level of the targeted signals, then the samples would be sufficient for successful image reconstruction. Because for most of the 32 * 32 sparse image blocks tested in the experiment, their sparsity level under the selected KLbasis is around a few dozen at most, we use m = 256 linear measurements to ensure good enough quality of the reconstructed image blocks.

As we mentioned previously, besides sparse data, SISR also naturally supports the case of general data. For either sparse or general data case, the image block recovery is based on the number of measurements m D 256. Because of the relatively sufficient size of m, we can hardly see the visual difference when comparing the reconstructed images and the original images. For completeness, we also tested the recovered images using different number of measurements. As we can see, the quality downgrade is quite obvious when m decreases. Note that all recovered images have been through three steps of random sample mapping at data owner, reconstruction over randomly transformed problem at cloud, and decryption at the user.

5.2.2 Privacy-Assurance Evaluation

Recall that SISR provides the privacy-assurance that user 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 random affine mapping enabled by **Q** and **e** over **g** provides good enough privacy-assurance on image content protection. This demonstrates what adversary can see given the basis **V** and the recovered encrypted vector **h** only consists of obfuscated image blocks. Compared to random noises, these image blocks are perceptually indistinguishable. It is safe to say that SISR provides satisfactory privacy-assurance. That is, without knowing the secret key, the actual content of the protected underlying image cannot be perceived.

6. Conclusion

In this paper, we have proposed SISR, an outsourced image recovery service from compressed sensing with privacy assurance.
SISR exploits techniques from different domains, and aims to take security, design complexity, and efficiency into consideration from the very beginning of the service flow. With SISR, 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. Besides its simplicity and efficiency, we show SISR 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 SISR. 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.

We will investigate curved and flexible sensor shapes and the application of multiple stacked LC layers with different wavelength responses that enable the reconstruction of color images. We will also seek for more robust and faster image reconstruction techniques, and will explore new applications, such as novel non-touch interfaces.

References

[1] (1996). *Health Insurance Portability and Accountability Act of (HIPPA)* [Online]. Available: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html
[2] P. Agouris, J. Carswell, and A. Stefanidis, ``An environment for content based image retrieval from large spatial databases," *ISPRS J. Photogram.Remote Sens.*, vol. 54, no. 4, pp. 263_272, 1999.
[3] M. Atallah and K. Frikken, ``Securely outsourcing linear algebra computations," in *Proc. 5th ASIACCS*, 2010, pp. 48_59.
[4] M. Atallah and J. Li, ``Secure outsourcing of sequence comparisons," *Int.J. Inf. Security*, vol. 4, no. 4, pp. 277_287, 2005.
[5] M. Atallah, K. Pantazopoulos, J. Rice, and E. Spafford, ``Secure outsourcing of scientific computations," *Adv. Comput.*, vol. 54, pp. 216_272,Feb. 2001.
[6] D. Benjamin and M. Atallah, ``Private and cheating-free outsourcing of algebraic computations," in *Proc. Conf. PST*, 2008, pp. 240_245.
[7] E. Candès, ``The restricted isometry property and its implications for compressed sensing," *Comptes Rendus Mathematique*, vol. 346, nos. 9_10, pp. 589_592, 2008.
[8] E. Candès, J. Romberg, and T. Tao, ``Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489_509,Feb. 2006.
[9] E. Candès and T. Tao, ``Decoding by linear programming," *IEEE Trans.Inf. Theory*, vol. 51, no. 12, pp. 4203_4215, Dec. 2005.
[10] 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.
[11] E. Candès and M. Wakin, ``An introduction to compressive sampling," *IEEE Signal Proc. Mag.*, vol. 25, no. 2, pp. 21_30, Mar. 2008.
[12] (2009). *Security Guidance for Critical Areas of Focus in Cloud Computing*, [Online]. Available: http://www.cloudsecurityalliance.org
[13] 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.
[14] D. Donoho, ``Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289_1306, Apr. 2006.
[15] C. Dwork, ``Differential privacy," in *Proc. ICALP*, 2006, pp. 1_12.
[16] C. Dwork, ``The differential privacy frontier (extended abstract)," in *Proc.TCC*, 2009, pp. 496_502.
[17] (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
[18] R. Gennaro, C. Gentry, and B. Parno, ``Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in *Proc. CRYPTO*, Aug. 2010, pp. 465_482.
[19] 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.
[20] S. Goldwasser, Y. T. Kalai, and G. Rothblum, ``Delegating computation: Interactive proofs for muggles," in *Proc. STOC*, 2008, pp. 113_122.
[21] S. Hohenberger and A. Lysyanskaya, ``How to securely outsource cryptographic computations," in *Proc. TCC*, 2005, pp. 264_282.

[22] C. Jansson, ``An np-hardness result for nonlinear systems," *Reliable Comput.*, vol. 4, no. 4, pp. 345_350, 1998.
[23] N. Karmarkar, ``A new polynomial-time algorithm for linear programming," *Combinatorica*, vol. 4, no. 4, pp. 373_396, 1984.
[24] 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.
[25] 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
[26] 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.
[27] A. Orsdemir, H. O. Altun, G. Sharma, and M. F. Bocko, ``On the security and robustness of encryption via compressed sensing," in *Proc. IEEE MILCOM*, Nov. 2008, pp. 1_7.
[28] C. Pavlopoulou, A. C. Kak, and C. E. Brodley, ``Content-based image retrieval for medical imagery," *Proc. SPIE*, vol. 5033, pp. 85_96, May 2003.
[29] Y. Rachlin and D. Baronm, ``The secrecy of compressed sensing measurements," in *Proc. Allerton Conf. Commun., Control, Comput.*, 2008, pp. 813_817.
[30] J. Romberg, ``Imaging via compressive sampling," *IEEE Signal Process.Mag.*, vol. 25, no. 2, pp. 14_20, Mar. 2008.
[31] P. Van Hentenryck, D. McAllester, and D. Kapur, ``Solving polynomial systems using a branch and prune approach," *SIAM J. Numer. Anal.*, vol. 34, no. 2, pp. 797_827, 1997.
[32] A. Yao, ``Protocols for secure computations (extended abstract)," in *Proc. FOCS*, 1982, pp. 160_164.

Author Profile

Kolasani Sravya Obtained the B.Tech degree in Computer Science and Engineering (CSE) Department from Vignan's Engineering College (JNTU), Vadlamudi in the year 2008. At present persuing the M.Tech in Computer Science and Engineering (CSE) Department at Sri Mittapalli Engineering College, Guntur.

Yakkala Nagendra Kumar obtained the B.Tech Degree in Information Technology from Sir C.R.Reddy College of Engineering, Eluru in 2008 and M.Tech from Sri Mittapalli Engineering College, Guntur in 2012. He has 2½ years of teaching experience and working in Computer Science and Engineering (CSE) Department at Sri Mittapalli Engineering College, Guntur.