A Secure Third Party Image Reconstruction System in Cloud

Shinde Nitanjali U.[1], **Borole M.V.**[2]

[1]Savitribai Phule Pune University, Rajarshi Shahu School of Engineering and Research, JSPM, NTC, Pune-41, India

[2]Professor, Savitribai Phule Pune University, Rajarshi Shahu School of Engineering and Research, JSPM, NTC, Pune-41, India

Abstract: ***Large-scale image datasets being exponentially generated nowadays. In conjunction with such knowledge explosion is that the aggressive trend to outsource the image management systems to the cloud for its luxuriant computing resources and edges. However, the way to shield the sensitive knowledge whereas enabling outsourced image services becomes a serious concern. To deal with these challenges, we have a tendency to propose OIRS, a unique outsourced image recovery service design that exploits totally different domain technologies and takes security, efficiency, and style complexness into thought from the terribly starting of the service flow. Specifically, OIRS is based on the compressed sensing (CS) framework that is understood for its simplicity of unifying the normal sampling and compression for image acquisition. Data owners solely have to be compelled to outsource compressed image samples to cloud for reduced storage overhead. Besides, in OIRS, Data users will harness the cloud to firmly reconstruct images while not revealing data from either the compressed image samples or the underlying image content. we have a tendency to begin with the OIRS framrwork for distributed image dataset, that is that the typical application state for compressed sensing, then show its natural extension to the final data for tradeoffs between robustness and accuracy. we have a tendency to completely analyse the privacy-protection of OIRS and conduct in depth experiments to demonstrate the system effectiveness and robustness. For completeness, we have a tendency to conjointly discuss the expected performance acceleration of OIRS through hardware built-in system framework.***

Keywords: Compressed sensing, security and privacy, cloud computing, image reconstruction

1. Introduction

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

Compressed sensing in 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, the system of leverage compressed sensing to compress the storage of correlated image datasets. Instead of storing the whole image, the idea is to store the compressed image samples on storage servers.

The compressed samples offers about storage reduction compared to storing the original image in uncompressed format or other data application scenarios where data compression may not be done. But the security may be compromised, which is an indispensable design requirement in OIRS. On storage reduction, our proposed system aims to achieve a much more ambitious goal, which is an outsourced image service system and takes into account of security, efficiency, effectiveness, and complexity from the very beginning of the service flow. Another interesting line of research loosely related to the proposed OIRS is about the security and robustness of compressed sensing based encryption.

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

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

2. 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×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].

3. Problem Statement

The basic service model in the OIRS architecture includes the following: At first, data owner acquires raw or original image data, in the form of compressed image samples, generated from the physical world under different imaging application contexts. To trim down the local storage and maintenance overhead, data owner later outsources samples of the raw image 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. Throughout this, 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 and accessing owner/user's data content. Because the images samples captured by data owners usually contain data specific/sensitive information, we have to make sure that the data outside the data owner/user's process is in protected format.
Our design goals for OIRS consist of the following.

- **Security:** OIRS ought to give the strongest conceivable assurance on both the private image samples and the content of the recovered images from the cloud during the service flow.
- **Effectiveness:** OIRS ought to empower cloud to adequately perform the image reconstruction service over the encrypted and compressed samples, which can later be correctly decrypted and decompressed by user.
- **Efficiency:** OIRS ought to bring investment funds from the computation and/or storage aspects to data owner and

users, while keeping the extra cost of processing encrypted image samples on cloud as small as possible.

- **Extensibility:** OIRS ought to be made posible to support other extensible service interfaces and even performance speedup via hardware built-in design.

4. The OIRS Design

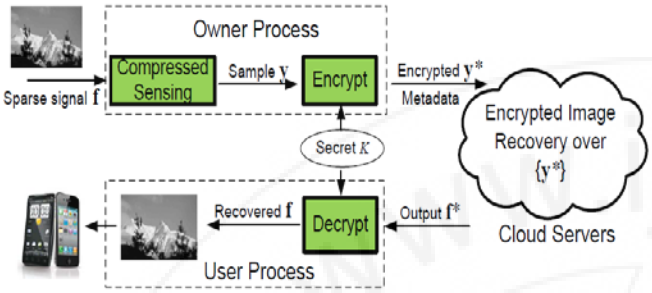

Figure 1: The OIRS architecture in public cloud[1]

The basic service model in the OIRS 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 [1].

Fig.1 demonstrates the basic message flow in OIRS. Let **f** and **y** be the signal and its compressed samples to be captured by the data owner [6]. For privacy protection, data owner in OIRS will not outsource **y** directly. Instead, he outsources an encrypted version $\mathbf{y}^*$of **y** and some associated metadata to cloud. Next, the cloud reconstructs an output $\mathbf{f}^*$ directly over the encrypted $\mathbf{y}^*$ and sends $\mathbf{f}^*$ to data users. Finally, the user obtains **f** by decrypting $\mathbf{f}^*$. 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. Further assume that the programs are public and the data are private [1].

5. Methodology

5.1 Bit Stream Encryption

The encryption of compressed images to ensure privacy is an active research topic for a variety of different compressed image and video formats. For JPEG-compressed images (International Telecommunication Union, 1992) in particular, several approaches exist due to the widespread use of this image format. Most of them require recompressing the original data to some extent. The method operates on bitstream level and uses only swap and scramble operations, which makes it very fast[7].

5.2 Compressed Sensing

Compressive sensing is a recent data sensing framework known for its simplicity of unifying the traditional sampling and compression for signal acquisition. The compressed sensing (CS) paradigm unifies sensing and compression of sparse signals in a simple linear measurement step. Reconstruction of the signal from the CS measurements relies on the knowledge of the measurement matrix used for sensing. Generation of the pseudo-random sensing matrix utilizing a cryptographic key offers a natural method for encrypting the signal during CS. This CS based encryption has the inherent advantage that encryption occurs implicitly in the sensing process – without requiring additional computation. Additionally, the robustness of recovery from compressed sensing, allows a new form of "robust encryption" for multimedia data, wherein the signal is recoverable with high fidelity despite the introduction of additive noise in the encrypted data.

6. Algorithms

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 $\sigma$
Result: K = (P,Q, e, $\pi$,M)
Begin
1. uses $\sigma$ to generate random P, e, $\pi$,
2. uses $\sigma$ to generate random Q and M,
3. return secret key K = (P,Q, e,$\pi$,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', $\pi$' in Ωk
Begin
1. picks (P,Q, $\pi$,M) in K and F in Ω,
2. computes F' = PFQ and $\pi$' = ($\pi$ - MF)Q,
3. return transformed F', $\pi$' ,
```

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 protected answer 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 ,

7. Conclusion

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

8. Future Enhancement

We will continue to work on OIRS for its compatibility with other important image services, such as content based image retrieval, while providing extensible service interfaces and possible performance speedup via hardware built-in design.

References

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

[2] 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.

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

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

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

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

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

Author Profile

Shinde Nitanjali received the B.E. degree in Information Technology from Vidya Pratishthan's College of Engineering, Baramati, Pune University in 2008 and pursuing M.E. from Rajarshi Shahu School of Engineering and Research JSPM, NTC, Pune University ,Pune-41,India

Prof. Megha Borole ,Assistant professor in Savitribai Phule Pune University, Rajarshi Shahu School of Engineering and Research JSPM, NTC, Pune-41,India