Improved Method of Cryptography for Privacy-assured Outsourcing of Image Reconstruction Service in Cloud

Rohini. G. Deshmukh
Department of Computer Science
Sinhgad Academy of Engineering
Pune, India
e-mail: rohinigdeshmukh@gmail.com

B. B. Gite
Department of Computer Science
Sinhgad Academy of Engineering
Pune, India
e-mail:

Abstract— To address various challenges related to large scale image data generation over clouds, recently we have studied the new approach called outsourced image recovery service (OIRS) architecture, which exploits different domain technologies and takes efficiency, security and design complexity into consideration from the very beginning of the service flow. We design OIRS using the compressed sensing (CS) framework, which is well known for its simplicity of unifying the traditional sampling and compression for image acquisition. A data owner only needs to outsource compressed image samples to cloud for reduced storage overhead. Besides, in OIRS, by using cloud data users can securely reconstruct images without revealing information from either the underlying image content or the compressed image samples. We start with the OIRS design for sparse data, which is the typical application scenario for compressed sensing, and then its natural extension is shown to the general data for meaningful tradeoffs between accuracy and efficiency. We analyze the privacy protection of OIRS and conduct extensive experiments to demonstrate the system effectiveness and efficiency.

However this approach also needs to be improve in terms of time, therefore in this, we are presenting the new cryptography methods with OIRS and hardware built-in system with the aim of improving the speed of overall architecture.

Keywords- *Cloud Computing, Compressed sensing, Cryptography, Image reconstruction, OIRS*

*****

I. INTRODUCTION

With the advancement of information and computing technology, large-scale datasets are being exponentially generated today. Examples under various application contexts include medical images [29], remote sensing images [3], 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 [26] to efficiently and effectively acquire, store, and share images from data owners to a large number of data users [25].

Outsourcing the image services is quite promising but 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 because the cloud is an open environment operated by external third parties who are usually outside of the data owner/users' trusted domain [13], [18]. Whereas, many image datasets, e.g., the medical images with diagnostic results for different patients, are privacy-sensitive by its nature [2]. 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 [25], 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 [31].

In this paper, we initiate the investigation for these challenges and propose a novel outsourced image recovery service (OIRS) architecture with privacy assurance. For the simplicity of data acquisition at data owner side, OIRS is specifically designed under the compressed sensing framework. The acquired image samples from data owners are later sent to cloud, which can be considered as a central data hub and is responsible for image sample storage and provides on-demand image reconstruction service for data users. Because reconstructing images from compressed samples requires solving an optimization problem [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 without introducing undesired privacy leakages on the possibly sensitive image samples or the recovered image To 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. To meet these challenging requirements, a core part of the OIRS design is a tailored lightweight problem transformation mechanism, which can help data owner/user to 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 for easy local post processing. Compared to directly reconstructing the image locally, OIRS is expected to bring considerable computational savings to the owner/users. As another salient feature, OIRS 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, OIRS is the first image service outsourcing design in cloud that addresses the design challenges of security, complexity, and efficiency simultaneously.
- We show that OIRS 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 OIRS and demonstrate the efficiency and effectiveness of OIRS via experiment with real world data sets. For completeness, we also discuss how to achieve possible performance speedup via hardware built-in system design.

II. LITERATURE SURVEY

Compressed sensing [9], [10], [15] is a recent data sensing and reconstruction framework well-known for its simplicity of unifying the traditional sampling and compression for data acquisition.

- In [14], 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 OIRS. In fact, compared to [14] that only focuses on storage reduction, 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.
- In [28,30], A. Orsdemir, H. O. Altun, G. Sharma, and M. F. Bocko, proposed 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 OIRS 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.
- In [4], [7], [19], [21], [22], which aims to protect both input and output privacy of the outsourced computations. With the breakthrough on fully homomorphic encryption (FHE).
- Gennaro et al. [19] shows that a theoretical solution has already been feasible. The idea is to represent any computation via a garbled combinational circuit [33] 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.
- Firstly introduced by Yao [33] and later extended by Goldreich et al. [20] 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 OIRS model. In short, practically efficient mechanisms with immediate practices for secure image recovery service outsourcing in cloud are still missing.
-

III. PROBLEM APPROCH FRAMEWORK AND DESIGN

A. Problem Definition

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 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.

B. Proposed Sytem Architecture

While compressed sensing simplifies the data acquisition at data owner, it makes the data recovery from the compressed samples a computationally intensive task.

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. For privacy protection, data owner in OIRS will not outsource **y** directly. Instead, he outsources an encrypted version **y_** of **y** and some associated metadata to cloud. Next, the cloud reconstructs an output **f_** directly over the encrypted **y_** and sends **f_** to data users. Finally, the user obtains **f** by decrypting **f_**. We leave the management and sharing of the secret keying material *K* between the data owner and users in our detailed decryption of OIRS design. In Fig. 1, each block module is considered as the process of a program taking input and producing output. We further assume that the programs are public and the data are private.

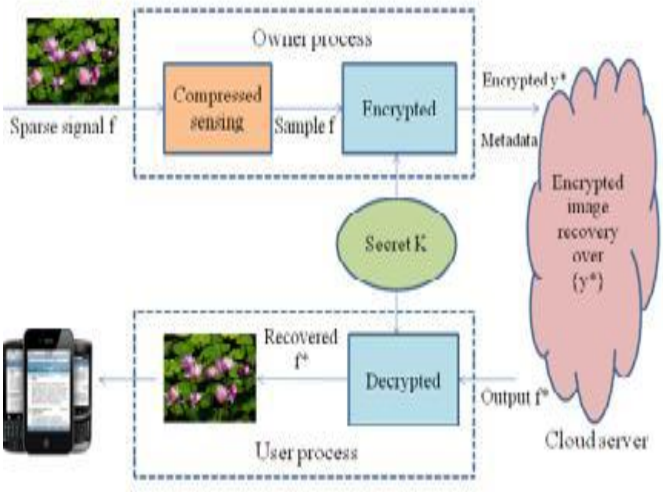


Figure 1: Proposed architecture of system

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. In addition to this, we are improving the speed of encryption and decryption process so that entire process becomes faster; this is done by modifying the existing cryptography algorithm with aim of improving both security and speed. We will use Diffie Hellman method for encrypting the image using secret key. The basic difference between RSA and Diffie Hellman is given below.

Diffie-Hellman is a key exchange algorithm and allows two parties to establish, over an insecure communications channel, a shared secret key that only the two parties know, even without having shared anything beforehand. The shared key is an asymmetric key, but, like all asymmetric key systems, it is inherently slow and impractical for bulk encryption. The key is used instead to securely exchange a symmetric key, such as AES (Advanced Encryption Standard) used to encrypt subsequent communications. Unlike Diffie-Hellman, the RSA algorithm can be used for signing digital signatures as well as symmetric key exchange, but it does require the exchange of a public key beforehand. The nature of the Diffie-Hellman key exchange does make it susceptible to man-in-the-middle attacks

man-in-the-middle attacks since it doesn't authenticate either party involved in the exchange. This is why Diffie-Hellman is used in combination with an additional authentication method.

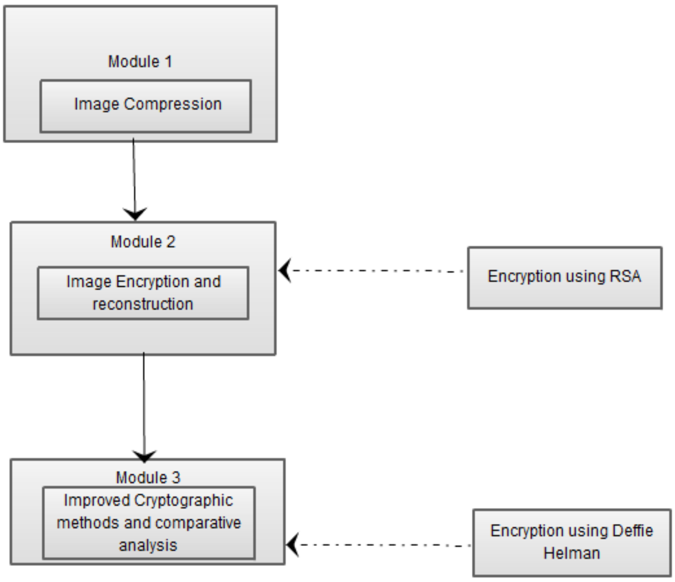

Module 1
Image Compression
Module 2
Image Encryption and reconstruction
Encryption using RSA
Module 3
Improved Cryptographic methods and comparative analysis
Encryption using Deffie Helman

Fig 2: Flow of Proposed System

Above Figure 2 shows us the proposed flow of project and improved methods for cryptography and comparative resultsof previous and proposed methods.

IV. WORK DONE

A. *Input Datasets*

For this implementation, we use the dataset of log file generated from web application. This log file used for further process of forecasting accuracy computation.

B. *Results Of Pratical Work*

Module 1:

We can select image for uploading on cloud. We can select image for outsourcing it on cloud in encrypted format with the selected number of users. Also you can see the original selected image in Fig. 3 and its compressed image is shown in fig. 4

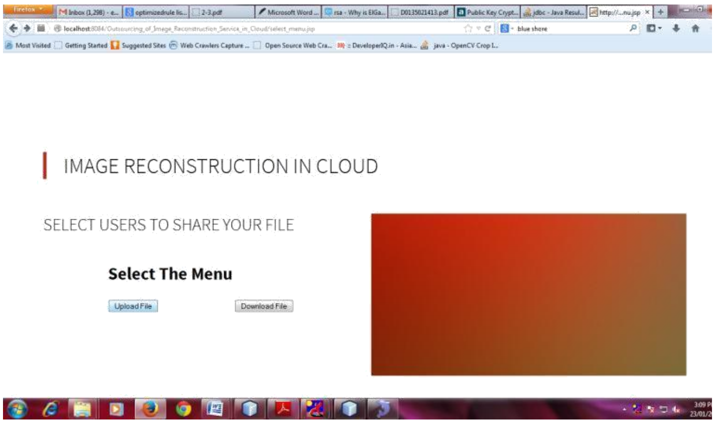
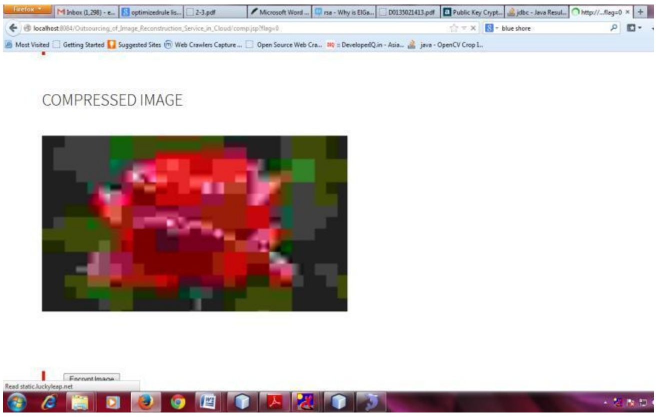


IMAGE RECONSTRUCTION IN CLOUD
SELECT USERS TO SHARE YOUR FILE
Select The Menu
Upload File
Download File

Fig 3: Upload Image


localhost:8084/Outsourcing_of_Image_Reconstruction_Service_in_Cloud/comp.jsp?flag=0

COMPRESSED IMAGE

Figure 4. Compressed Image

Module 2:
Image encryption and reconstruction using RSA algorithm.

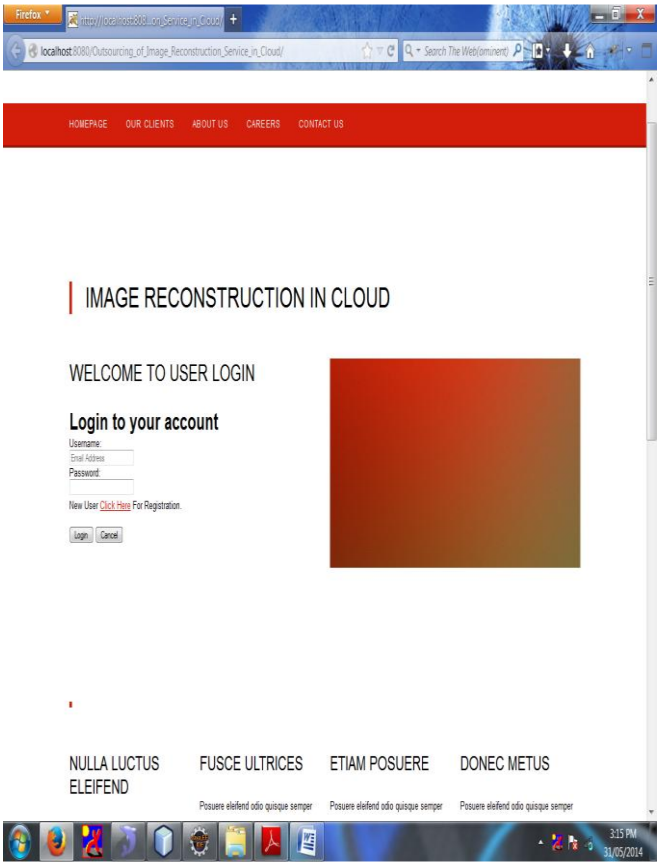

localhost:8080/Outsourcing_of_Image_Reconstruction_Service_in_Cloud/
HOMEPAGE
OUR CLIENTS
ABOUT US
CAREERS
CONTACT US

IMAGE RECONSTRUCTION IN CLOUD

WELCOME TO USER LOGIN

Login to your account

Username: Email Address

Password:

New User Click Here For Registration.

Login Cancel

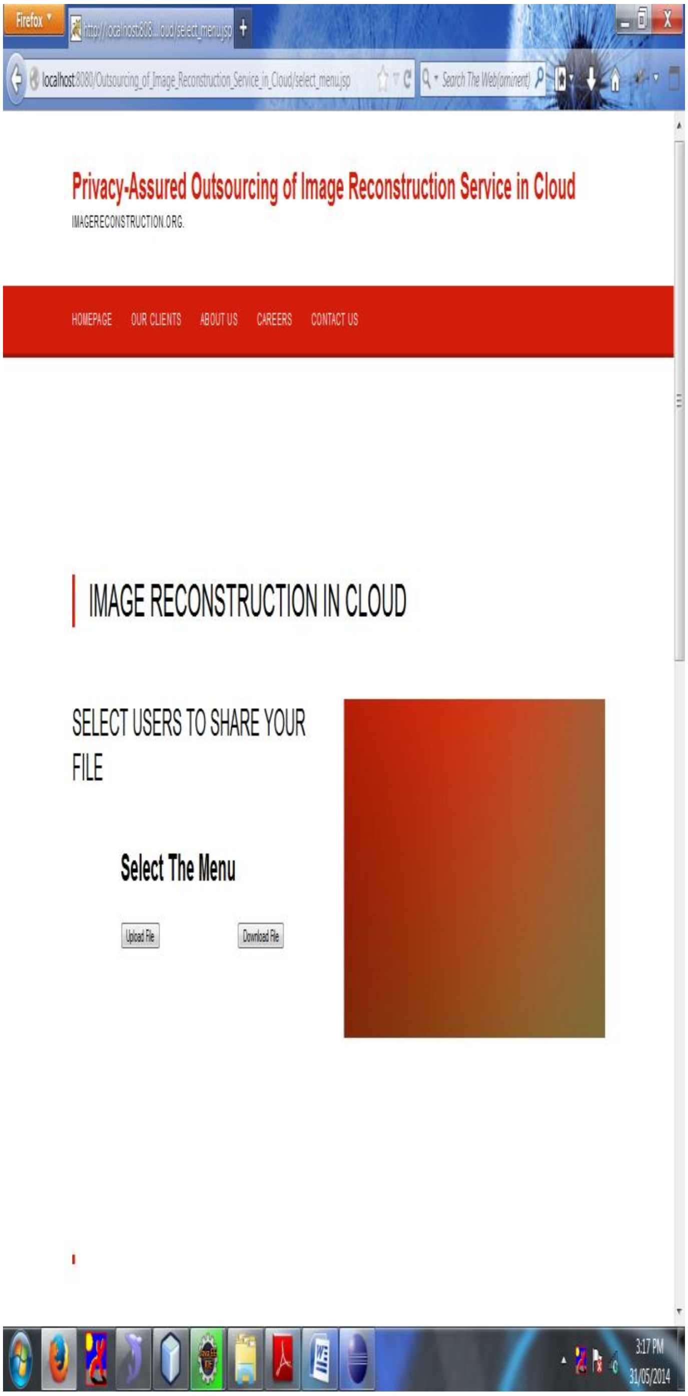
NULLA LUCTUS ELEIFEND

FUSCE ULTRICES
Posuere eleifend odio quisque semper

ETIAM POSUERE
Posuere eleifend odio quisque semper

DONEC METUS
Posuere eleifend odio quisque semper

Figure 5: Home Login


localhost:8080/Outsourcing_of_Image_Reconstruction_Service_in_Cloud/select_menu.jsp
HOMEPAGE
OUR CLIENTS
ABOUT US
CAREERS
CONTACT US
3:17 PM
31/05/2014

Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud

IMAGERECONSTRUCTION.ORG.

IMAGE RECONSTRUCTION IN CLOUD

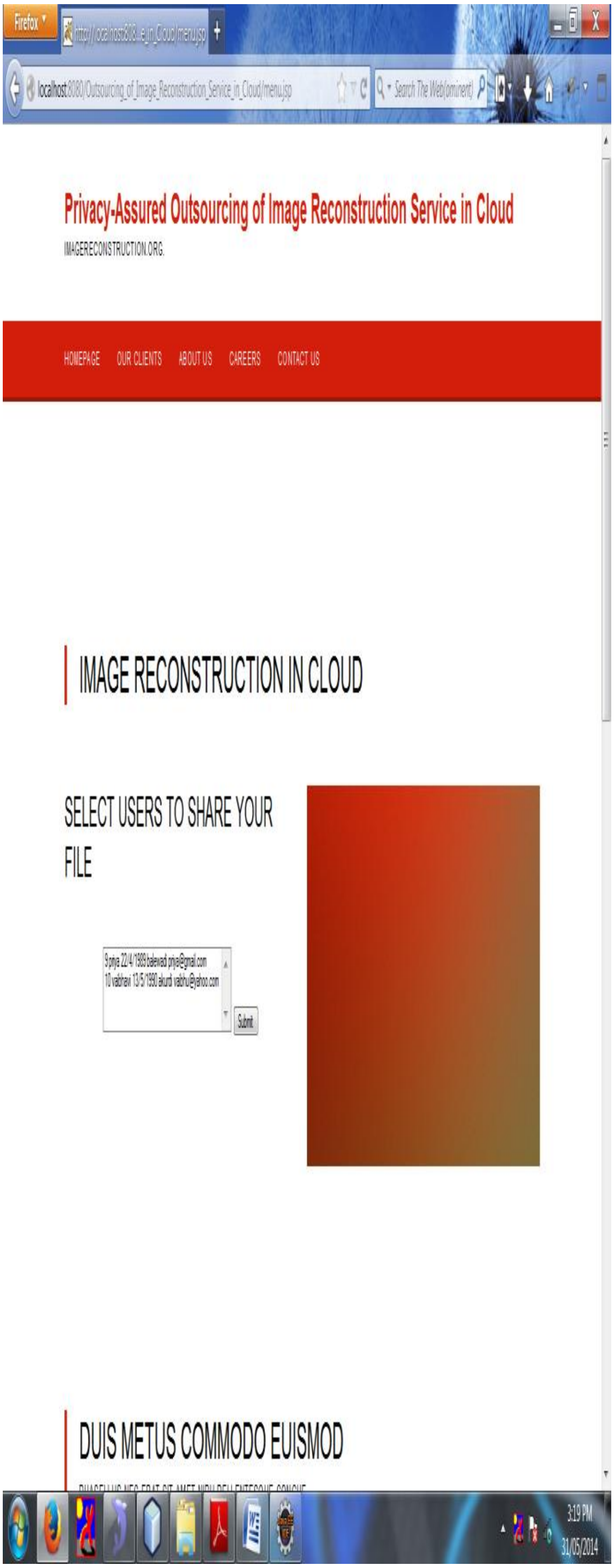
SELECT USERS TO SHARE YOUR FILE

Select The Menu

Upload File Download File

Figure 6: Select File

ISSN: 2321-8169
1266– 1274



localhost:8080/Outsourcing_of_Image_Reconstruction_Service_in_Cloud/menu.jsp

Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud

IMAGERECONSTRUCTION.ORG.

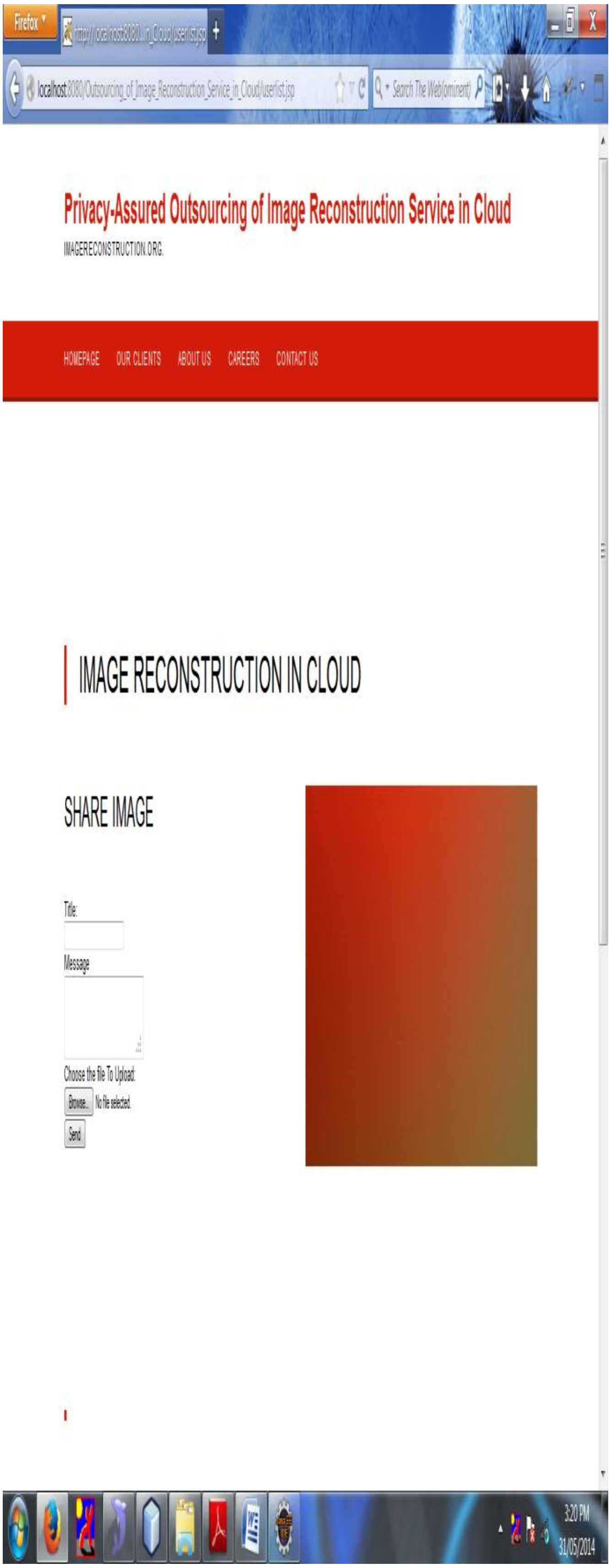
IMAGE RECONSTRUCTION IN CLOUD

SELECT USERS TO SHARE YOUR FILE

9 priya 22/4/1989 balewadi priya@gmail.com
10 vaibhawi 13/5/1990 akurdi vaibhu@yahoo.com

DUIS METUS COMMODO EUISMOD

Figure 7: Select Sharing User



localhost:8080/Outsourcing_of_Image_Reconstruction_Service_in_Cloud/userlist.jsp

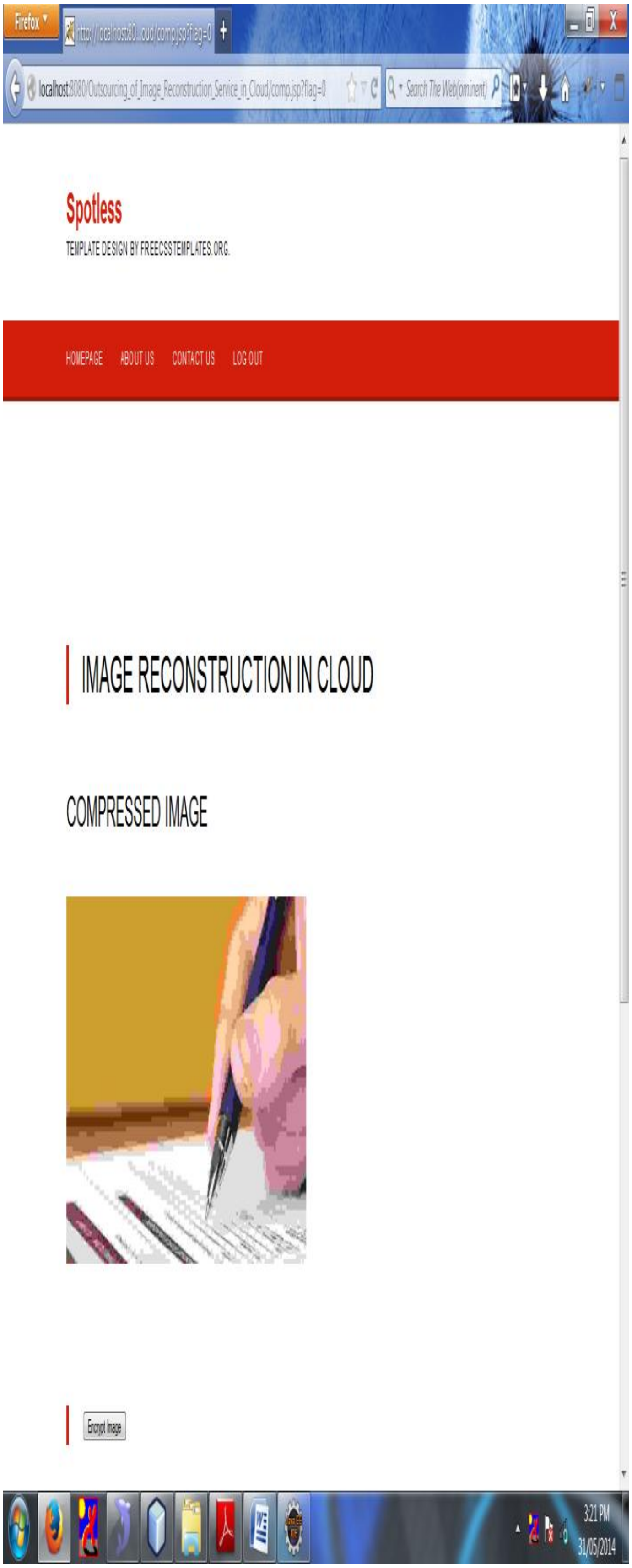
Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud

IMAGERECONSTRUCTION.ORG.

IMAGE RECONSTRUCTION IN CLOUD

SHARE IMAGE

Figure 8: select the image of encryption



localhost:8080/Outsourcing_of_Image_Reconstruction_Service_in_Cloud/comp.jsp?flag=0

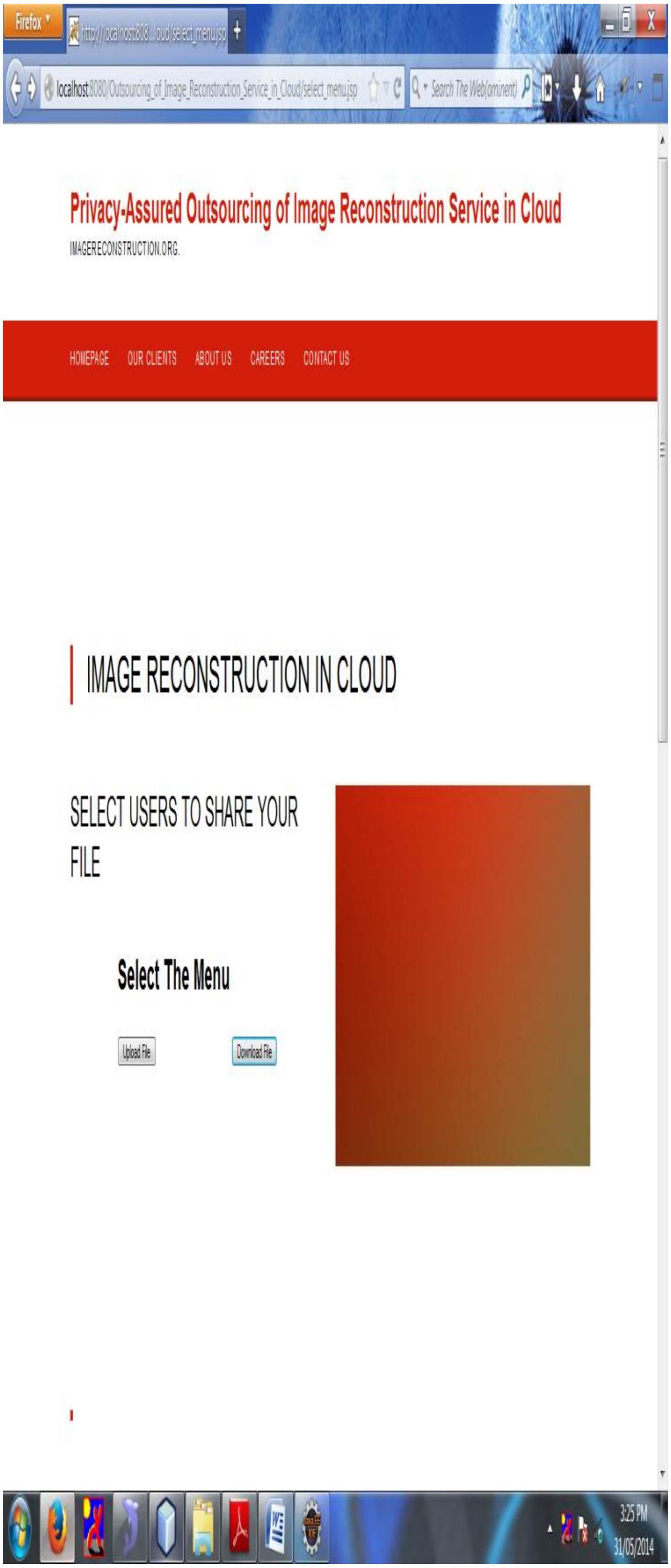
Spotless

TEMPLATE DESIGN BY FREECSSTEMPLATES.ORG.

IMAGE RECONSTRUCTION IN CLOUD

COMPRESSED IMAGE

Figure 9: compressed encrypted image



localhost:8080/Outsourcing_of_Image_Reconstruction_Service_in_Cloud/select_menu.jsp

Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud

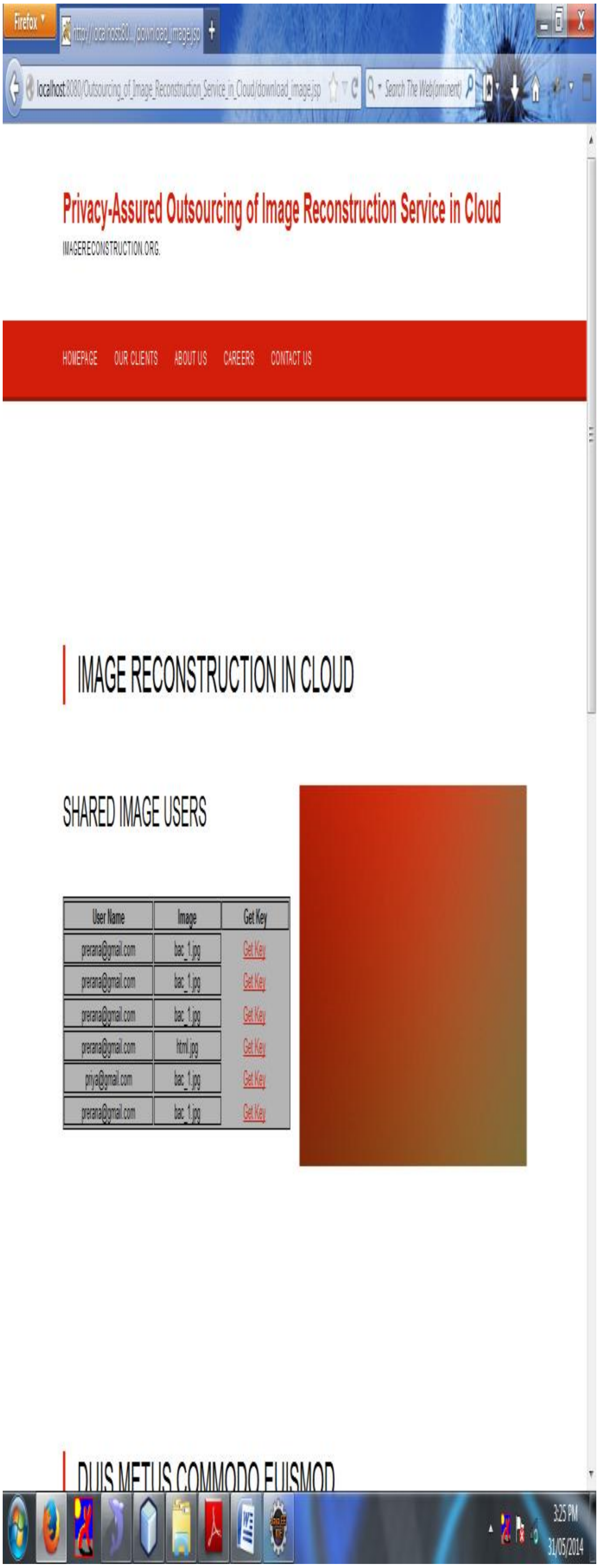
IMAGERECONSTRUCTION.ORG.

IMAGE RECONSTRUCTION IN CLOUD

SELECT USERS TO SHARE YOUR FILE

Select The Menu

Figure 10: Login by another access user
For Download file


Firefox
http://localhost:80.../download_image.jsp
localhost:8080/Outsourcing_of_Image_Reconstruction_Service_in_Cloud/download_image.jsp
Search The Web (omiment)
HOMEPAGE
OUR CLIENTS
ABOUT US
CAREERS
CONTACT US
3:25 PM
31/05/2014

Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud

IMAGERECONSTRUCTION.ORG.

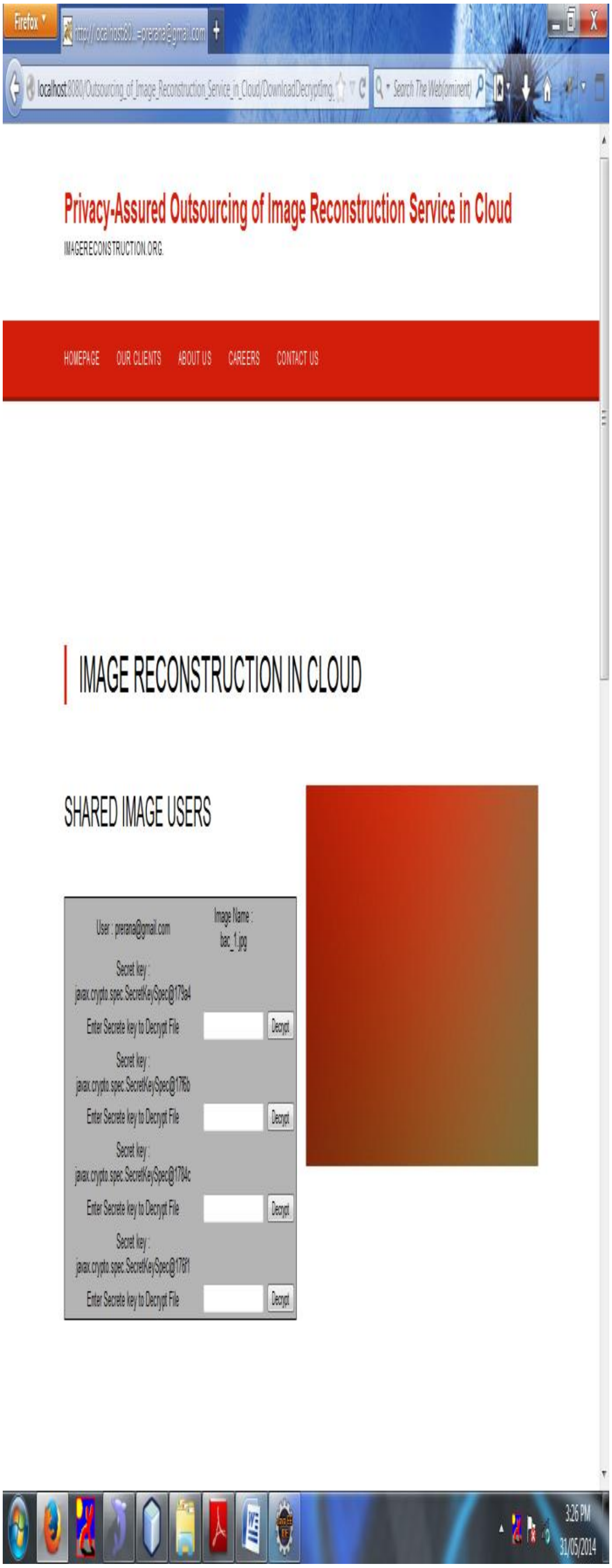
IMAGE RECONSTRUCTION IN CLOUD

SHARED IMAGE USERS

User Name	Image	Get Key
prerana@gmail.com	bac_1.jpg	Get Key
prerana@gmail.com	bac_1.jpg	Get Key
prerana@gmail.com	bac_1.jpg	Get Key
prerana@gmail.com	html.jpg	Get Key
priya@gmail.com	bac_1.jpg	Get Key
prerana@gmail.com	bac_1.jpg	Get Key

DUIS METUS COMMODO EUISMOD

Figure11: Show access user


Firefox
http://localhost:80...=prerana@gmail.com
localhost:8080/Outsourcing_of_Image_Reconstruction_Service_in_Cloud/DownloadDecrypting...
Search The Web (omiment)
HOMEPAGE
OUR CLIENTS
ABOUT US
CAREERS
CONTACT US
Decrypt
Decrypt
Decrypt
Decrypt
3:26 PM
31/05/2014

Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud

IMAGERECONSTRUCTION.ORG.

IMAGE RECONSTRUCTION IN CLOUD

SHARED IMAGE USERS

User : prerana@gmail.com

Image Name : bac_1.jpg

Secret key : javax.crypto.spec.SecretKeySpec@179a4

Enter Secrete key to Decrypt File

Secret key : javax.crypto.spec.SecretKeySpec@17f6b

Enter Secrete key to Decrypt File

Secret key : javax.crypto.spec.SecretKeySpec@1784c

Enter Secrete key to Decrypt File

Secret key : javax.crypto.spec.SecretKeySpec@176f1

Enter Secrete key to Decrypt File

Figure 12: Ask for decryption key to decrypt image

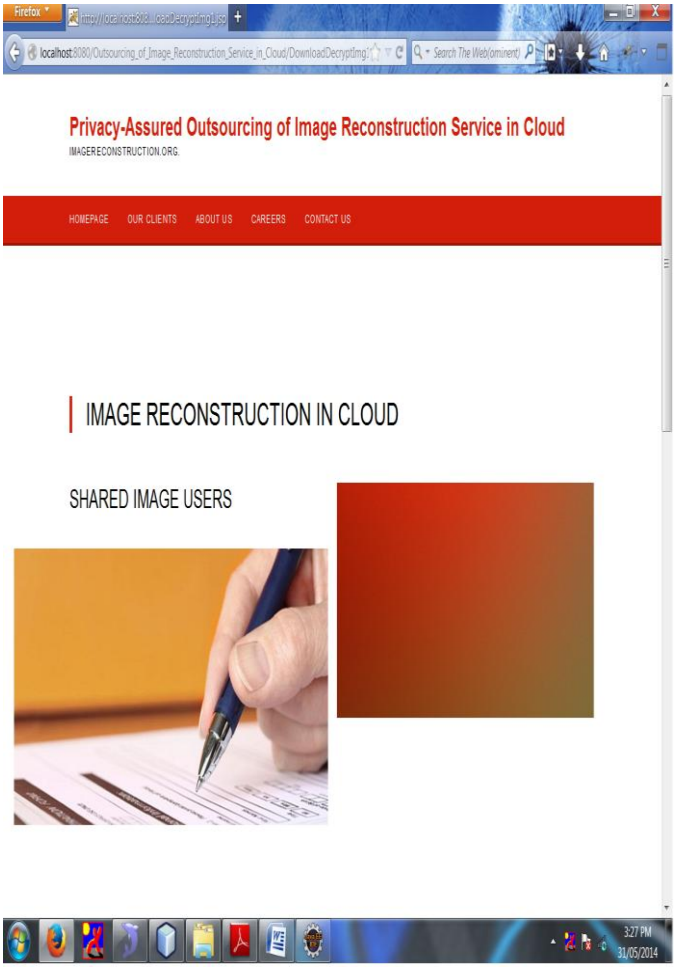

Firefox
http://localhost:808...loadDecrypting1.jsp
localhost:8080/Outsourcing_of_Image_Reconstruction_Service_in_Cloud/DownloadDecryptImg/
Search The Web (ominent)
Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud
IMAGERECONSTRUCTION.ORG
HOMEPAGE
OUR CLIENTS
ABOUT US
CAREERS
CONTACT US
IMAGE RECONSTRUCTION IN CLOUD
SHARED IMAGE USERS
3:27 PM
31/05/2014

Figure 13: Downloaded dycrypted image

V. CONCLUSION

In this paper, we have proposed OIRS, an outsourced image recovery service from compressed sensing with privacy assurance. OIRS 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 OIRS, data owners can utilize the benefit of compressed sensing to consolidate the sampling and image compression via only linear measurements. Data users, on the other hand, can leverage cloud's abundant resources to outsource the image recovery related $l1$ optimization computation, without revealing either the received compressed samples, or the content of the recovered underlying image.

Besides its simplicity and efficiency, we show OIRS is able to achieve robustness and effectiveness in handling image reconstruction in cases of sparse data as well as non-sparse general data via proper approximation. Both extensive security analysis and empirical experiments have been provided to demonstrate the privacy-assurance, efficiency, and the effectiveness of OIRS.

ACKNOWLEDGMENT

I feel great in expressing our deepest sense of gratitude to our guide and HOD Prof. B.B. GITE for his encouragement and enlightened comments throughout this project work. His appreciative suggestion always motivated us for putting most willing efforts on my study during project report. Last but not the least, we express our sincere thanks to all teachers who have always motivated us. We are also thankful to the concerned authorities who directly or indirectly helped us in the project

REFERENCES

[1] C. Wang, `` Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud," *IEEE Trans* on cloud computing, vol.1 no.1,2013

[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 scienti_c 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] [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

[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.

[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.

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

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

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

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

[25] 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.

[26] 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

[27] 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.

[28] 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.

[29] 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.

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

[31] J. Romberg, ``Imaging via compressive sampling," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 14_20, Mar. 2008.

[32] 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.

[33] A. Yao, ``Protocols for secure computations (extended abstract)," in *Proc. FOCS*, 1982, pp. 160_164.