International Journal of Advanced Technology in Engineering and Science
Vol. No. 10, Issue No. 06, June 2022
www.ijates.com
ijates
ISSN 2348 - 7550

PRIVACY-PRESERVING IMAGE PROCESSING IN THE CLOUD

Mr. A. Krishna Mohan[1], G. Venkata Rajitha[2], G. Balaji[3], K. Chandana Priya[4], K. Harshitha Sai[5], K. Muni Teja[6]

[1] *Professor, Dept. of ECE, S V College of Engineering, Tirupati, A.P, India.*

[23456] *B.Tech Students, Dept. of ECE, S V College of Engineering, Tirupati, A.P, India.*

ABSTRACT

Millions of private images are generated in various digital devices every day. The consequent massive computational workload makes people turn to cloud computing platforms for their economical computation resources. Meanwhile, the privacy concerns over the sensitive information contained in outsourced image data arise in public. In fact, once uploaded to the cloud, the security and privacy of the image content can only presume upon the reliability of the cloud service providers. Lack of assuring security and privacy guarantees becomes the main barrier to further deployment of cloud-based image processing systems. This paper studies the design targets and technical challenges lie in constructing cloud-based privacy-preserving image processing system. We explore various image processing tasks, including image feature detection, digital watermarking, content-based image search. The state-of-the-art techniques, including secure multiparty computation, and homomorphic encryption are investigated.

Keywords: *Cloud Service Provider, Cloud Computing platform.*

1. INTRODUCTION

This article introduces and formulates diverse image processing tasks in a general image computation outsourcing model, including image feature detection, digital watermarking, and content based image search. We discuss state-of-the-art techniques, including secure multiparty computation and homomorphic encryption. Finally, we provide a detailed taxonomy of the problem statement and corresponding solutions. offers a pay-per use business model, which lets individual users use robust computation power in the cloud while saving time and costs on setting up corresponding infrastructures.1 In fact, not only individual or small business data owners but Internet giants like Microsoft and Yahoo are also attracted by the benefits brought by cloud computing and authorize some services to third-party cloud computing platforms. For example, several types of data searching tasks in Microsoft Bing have been outsourced.

However, the participation of a third-party cloud computing platform also increases the vulnerability of private data, e.g., potential data breaches and losses. Under current cloud architecture, the content of outsourced image data will inevitably be leaked to CSPs. In this case, the leaked content might be sensitive information such as the data owner's personal identity, home address, or even financial records. Moreover, even if we assume CSPs are completely honest and could be trusted to have data owners' private information, such privacy leakages still happen. In fact, the cloud server is usually considered as a low-qualified. The cloud computing platform suffers from more security threats compared with a traditional network server. For instance, a severe vulnerability in cloud servers is the sharing of computing resources: flaws in System Virtual Machine (SVM) software have frequently been discovered and exploited to attack cloud servers in recent years.

2. LITERATURE REVIEW

In recent years, secure image data processing has grown rapidly as a research field and attracted attention from both academia and industry. In practice, many fancy image-processing applications require computational power beyond the limit of mobile devices. For example, 3D structure reconstruction needs massive computational power for image feature detection and matching. In this area, the main research direction lies in the detection of image features over ciphertext domain. Many encryption techniques are applied or adjusted to protect image data privacy while enabling visual feature extractions. Qin and colleagues proposed a global image feature detection mechanism for color histogram-based descriptors detection. The authors utilized a Somewhat Homomorphic Encryption (SHE) scheme to enable the computation of diverse color descriptors in the MPEG-7 standard over the ciphertext domain. These features are further utilized as basic building blocks for services such as image matching and semantic tag generation. Hsu and colleagues proposed a local feature detection mechanism for Scaler Invariant Feature Transform (SIFT), which utilizes the Paillier encryption scheme to enable the computation of SIFT features over ciphertext domain. In another work,8 the authors analyzed different scaling ratios by adjusting fixed point numbers in the proposed scheme. However, all these works suffer from the high computational complexity brought on by homomorphic operations, especially for those who perform relatively complicated algorithms like SIFT. Qin and colleagues solve this problem by utilizing a multi-server structure to enable SIFT algorithm over encrypted data. Another thriving research direction is secure digital watermarking, which enables outsourcing the time-consuming tasks of generating digital watermark without compromising the privacy of the image content. Two types of approaches have been proposed: asymmetric watermarking and zero-knowledge watermark detection. However, most existing works still suffer from the high computational complexity on both user and cloud.

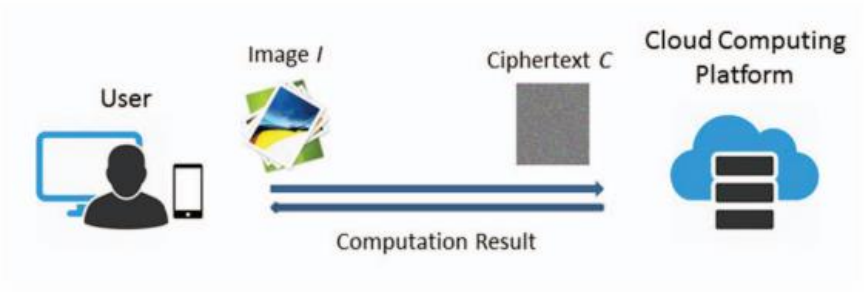
3. EXISTING METHOD

Motivated by the rapid growth of image processing and data mining techniques, more and more image processing based applications are deployed in various end-users' devices. For example, content-based image search, digital watermark verification, and so on. The consequent massive image processing tasks bring enormous computation overhead to data owners. To solve this problem, more and more users are outsourcing the "expensive" tasks to cloud computing platforms. In one such cloud computing platform, Cloud Service Provider (CSP). .

It offers flexible approaches to manage private image datasets online, and the features extracted from images are encrypted in a distance-preserving scheme to enable direct comparisons for similarity evaluation. In the work of Erkin and colleagues, the current image search indices are encrypted while achieving searching functionalities with efficiency. However, in a practical privacy-preserving computation scenario, all the existing works are very difficult to achieve the security requirements and practical efficiency performances at the same time.

4. PROPOSED METHOD

The proposed system consists of two main entities: the Cloud Computing Platform (CCP) and the user. The user is a data owner who holds massive image data and intends to outsource the image processing tasks to the CCP. In this setting, a user utilizes the CCP as a complementary resource for his limited computational power and also outsources complicated image processing tasks to the CCP. Meanwhile, users need to protect the privacy of their data. For example, hospitals are under an obligation to protect patients' records such as medical images and profiles. In this case, to protect a user's privacy, he or she has to encrypt the image data before outsourcing to the CCP. Meanwhile, the entity CCP is composed of a set of cloud servers assumed to be honest but curious. It can only access the encrypted image data uploaded by users and perform the corresponding image processing algorithms over the ciphertext domain. After that, the CCP returns the requested results in the form of ciphertext back to a user. Finally, a user can use her private key to decrypt the returned results. Throughout the process, the CCP should not have any access to the content or results of the user outsourced image computation tasks in plaintext domain.



5. METHODS OR TECHNIQUES USED

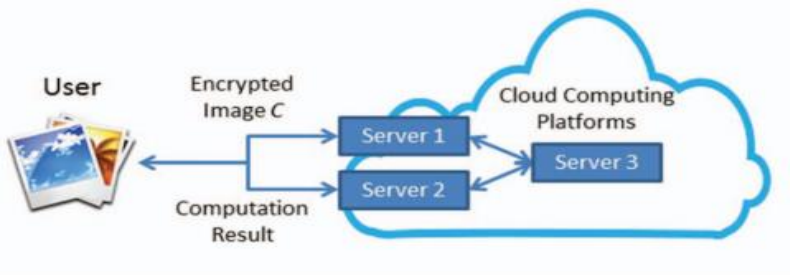
Data Preprocessing: In the Data Preprocessing phase, for the image I, a user prepares ciphertext C through encoding process Encode(I) and sends C to the CCP, where computation takes over the encrypted image C. Such an encoding algorithm should be lightweight and support as many image processing algorithms as possible. Hence, the user only needs to encode its image data once, and CCP takes the majority of the computation workload.

Encrypted Image Evaluation: After receiving the encrypted image data, CCP performs image processing algorithms over the ciphertext domain to get the corresponding encrypted results. Meanwhile, the private information of uploaded image data should be protected from the CCP.

Note that in this system architecture, users can get the maximum flexibility and scalability to perform massive image processing tasks. In fact, if a user has to perform part of an image processing task and then upload the encrypted intermediates to CCP, the user's flexibility will be limited. Under this circumstance, a user will have to compute and encrypt different intermediates for various image processing tasks respectively. Nevertheless, even a minor parameter change in processing algorithms will force the user to compute and encrypt the whole image dataset over again.

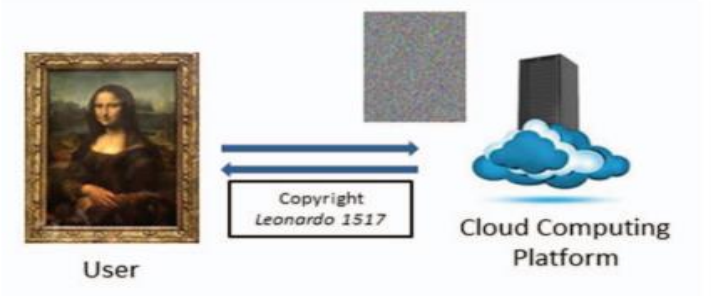
SMC BASED IMAGE PROCESSING

Usually, the Secure Multiparty Communication20 protocol is considered as a general solution to any function computations. However, due to its enormous computation and communication complexity, it is not widely implemented in practice. Nevertheless, its advantage in compatibility and the simplicity of the SMC algorithm makes it play a very important role in secure cloud computing mechanism designs. Among many SMC techniques, the Secure Two-party Computation is often utilized as a building block in constructing the system with techniques like homomorphic encryption scheme.



SMC based Secure Image Feature Detection

In image feature detection algorithms, functionality requirements like the comparison, factorial, and trigonometric operations exist in many complicated image feature detection algorithms. However, these operations over the ciphertext domain require tens to hundreds of iterations of homomorphic addition and multiplication operations. Hence, it seems to be impractical to use only homomorphic encryption based techniques to realize all those functionalities. To solve this problem, one possible methodology is adjusting the system architecture of the cloud computing platform to utilize SMC techniques. As shown in Figure 4, a user can easily realize homomorphic additions and ciphertext comparisons through introducing additional cloud servers.



6. SIMULATION RESULT

Simulation results performed are shown through screenshots.

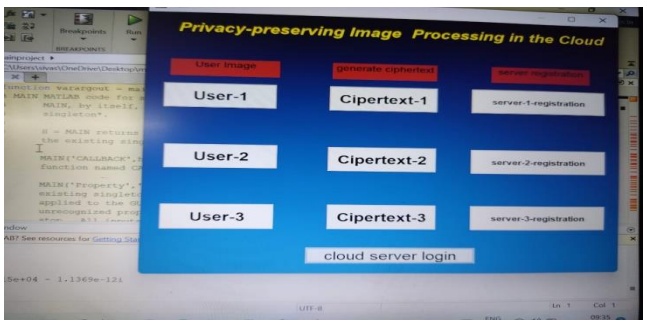


Figure-1: - server registration

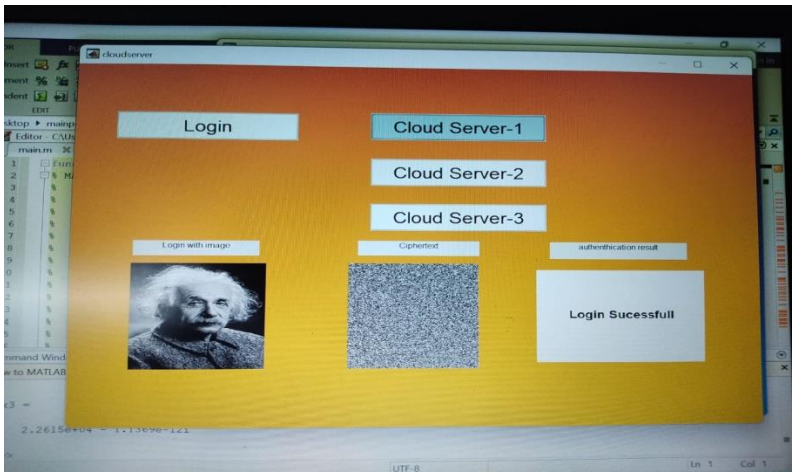


Figure 2: - server logging

In this paper we are the data owners of or data and we can maintain the large amount of data also. By using this image processing technique we can make our cloud platform more secure because the algorithm we use here is very difficult to decrypt. First the image is converted to the ciphertext image and then we have to decrypt that image by correct image. Then we get login as successful otherwise we are not allowed to see the data in that server.

7. CONCLUSION

This paper studies the problem of privacy-preserving image processing in the cloud, which could enable robust image-processing based applications on devices with limited computation power, e.g., a variety of instant image processing apps on lenses, watches, or other personal devices. Compared with other outsourced computation tasks, image-processing algorithms are relatively complicated and have high computation complexity. To solve the problem, we start by building a system model and formulating design targets. After that, state-of-the-art techniques are introduced, including homomorphic encryption, secure multiparty computation, and so on. We also present several case studies for different techniques and analyze their merits and drawbacks.

8. FUTURE SCOPE

Through the analysis, we find that the balance among design targets: functionality, security, and efficiency make it difficult to solve the problem by applying only one technique. The integration of different techniques instead of traditional cryptography tools is the most promising research direction in this area.

Also, considering the prevalence of JPEG compression among some data, privacy-preserving decompression of JPEG file as a special case of privacy-preserving DCT computation is also a promising research direction in this area.

To solve the problem, we start by building a system model and formulating design targets. After that, state-of-the-art techniques are introduced, including homomorphic encryption, secure multiparty computation, and so on.

9. REFERENCE

M. Armbrust et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4 pp. 50–58.

1. H. Esfahani et al., "Cloudbuild: Microsoft's Distributed and Caching Build Service," Software Engineering in Practice (SEIP 16), 2016.
2. C. Wang et al., "Privacy-assured outsourcing of image reconstruction service in cloud," IEEE Transactions on Emerging Topics in Computing, vol. 1, no. 1, 2013, pp. 166–177.
3. C. Modi et al., "A survey of intrusion detection techniques in cloud," Journal of Network and Computer Applications, vol. 36, no. 1, 2013, pp. 42–57.
4. W. Lu et al., "Secure image retrieval through feature protection," Procedings of the International Conference on Acoustics, Speech, and Signal Processing (ICASSP 09), 2009.
5. Z. Qin et al., "Privacy-preserving outsourcing of image global feature detection," Proceedings of the Global Communications Conference (GLOBECOM 14), 2014.
6. C.-Y. Hsu et al., "Image feature extraction in encrypted domain with privacy preserving SIFT," IEEE Transactions on Image Processing, vol. 21, no. 11, 2012, pp. 4593–4607.
7. C.-Y. Hsu et al., "Homomorphic encryption-based secure SIFT for privacy-preserving feature extraction," Proceedings of SPIE (SPIE 11), 2011.
8. Z. Qin et al., "Towards efficient privacy-preserving image feature ex-traction in cloud computing," Proceedings of the 2014 ACM on Multimedia Conference (MM 14), 2014.
9. J. Eggers, J. Su, and B. Girod, "Public key watermarking by eigenvectors of linear transforms," Proceedings of the European Symposium on Security and Privacy (Euro SP), 2000.
10. Gentry, "Fully homomorphic encryption using ideal lattices," Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC 09), 2009.
11. M. Naehrig et al., "Can homomorphic encryption be practical?," Proceedings of ACM Cloud Computing Security Workshop (CCSW 11), 2011.

12. 1 M.K. Khan, J. Zhang, and K. Alghathbar, "Challenge-response-based biometric image scrambling for secure personal identification," Future Generation Computer Systems, vol. 27, no. 4, 2011, pp. 411–418.

13. 19. S. Pandey et al., "An autonomic cloud environment for hosting ECG data analysis services," Future Generation Computer Systems, vol. 28, no. 1, 2012, pp. 147–154.

14. 20. O. Goldreich, Secure multi-party computation Manuscript, 1998.

15. 21. M. Malkin and T. Kalker, "A cryptographic method for secure watermark detection," Proceedings of the 8th International Workshop on Information Hiding, 2006.

16. 22. C. Lin, C. Lee, and S. Chien, "Digital Video Watermarking on Cloud Computing Environments," Proceedings of the Second International Conference on Cyber Security (CyberSec 13).