Privacy-preserving Image Processing in the Cloud

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. A detailed taxonomy of the problem statement and the corresponding solutions is provided.

INTRODUCTION

- 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) offers a pay-peruse 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

EXISTING SYSTEM

- 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.

PROPOSED SYSTEM

- 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. A detailed taxonomy of the problem statement and the corresponding solutions is provided.

HARDWARE REQUIREMETNS

Processor	:Intel Pentium IV 1GHz
RAM	:256MB (Min)
Hard Drive	:5GB free space
Monitor	:1024 * 768, High Color inch
Mouse	:Scroll Mouse(Logitech)
Keyboard	:104 keys

SOFTWARE REQUIREMENTS

OS	:	Windows XP/7/8
Front End	:	Visual Studio 2010/netbeans 7.1
Back End	:	SQL Server 2005/heidisql
Browser	:	Any Web Browser

CONCLUSION

- This article 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. Through the analysis, we find that the balance among design targets: functionality, security, and efficiency makes it difficult to solve the problem by applying only one technique.

REFERENCES

1. M. Armbrust et al., “A view of cloud computing,” Communications of the ACM, vol. 53, no. 4, 2010, pp. 50–58.
2. H. Esfahani et al., “Cloudbuild: Microsoft's Distributed and Caching Build Service,” Software Engineering in Practice (SEIP 16), 2016.
3. 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.
4. 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.
5. W. Lu et al., “Secure image retrieval through feature protection,” Procedings of the International Conference on Acoustics, Speech, and Signal Processing (ICASSP 09),2009.