International Journal of Advanced Technology in Engineering and Science
Vol. No.7, Issue No. 03, March 2019
www.ijates.com
ijates
ISSN 2348 - 7550

Privacy-preserved Image Processing with Homomorphic Encryption and Multiparty Computation in Cloud

Thamaraiselvi.M[1] , Rajakumari.V[2], Kanmani.S[3]

[1]*B.E-Computer Science and Engineering, Sengunthar Engineering College, Namakkal.*
[2]*B.E-Computer Science and Engineering, Sengunthar Engineering College, Namakkal.*
[3]*Assistant Professor/CSE, Sengunthar Engineering College, Namakkal.*

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 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:

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. Consequent massive image processing bring enormous computation overhead to data owners. To solve this problem, more and more users are outsourcing the "expensive" tasks to cloud computing platforms.

Cloud computing platform, Cloud Service Provider (CSP) offers a pay-per-use business model, which enables individual user to use robust computation power in cloud while saving time and cost on setting up corresponding infrastructures. In fact, not only individual or small business data owners refer to, 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 to Wolfram.

Third-party cloud computing platform also increases the vulnerability of private data, e.g., potential data breach and lost. 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 like data owner's personal identity, home address, or even financial records. Moreover, even we assume CSPs are completely honest and could be trusted to have data owners' private information, such privacy leakage still happens. In fact, cloud server is usually considered as a low-qualified locker rather than a strong bank deposit box. Comparing with traditional network server, the cloud computing platform suffers from more security threats.

A severe vulnerability in cloud server is the sharing of computing resources: flaws in System Virtual Machine (SVM) software are frequently discovered and exploited to attack cloud servers in recent years. Nevertheless, the private data leakage in public cloud happens very often due to the improper configuration and maintenance by CSPs. In a nutshell, the privacy concern over the outsourced data has become the main barrier to the further development of cloud computing platforms. In recent years, the secure image data processing is a rapidly growing research field and has attracted attention from both academia and industry. In practice, many fancy image processing applications require the computational power beyond the limit of mobile device. 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.

OBJECTIVES:

1.Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2.It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3.When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow.

Secure Image Retrieval Through Feature Production:

The problem of image retrieval from an encrypted database, where data confidentiality is preserved both in the storage and retrieval process. The paper focuses on image feature protection

techniques which enable similarity comparison among protected features. By utilizing both signal processing and cryptographic techniques, three schemes are investigated and compared, including bitplane randomization, random projection, and randomized unary encoding. Experimental results show that secure image retrieval can achieve comparable retrieval performance to conventional image retrieval techniques without revealing information about image content. This work enriches the area of secure information retrieval and can find applications in secure online services for images and videos.

Image Feature Extraction in Encrypted Domain With Privacy-Preserving SIFT:

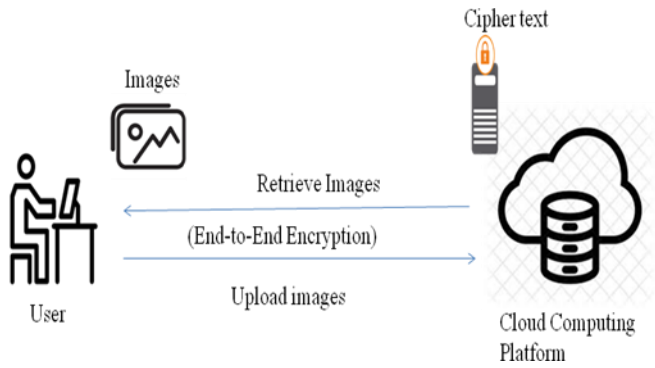
Privacy has received considerable attention but is still largely ignored in the multimedia community. Consider a cloud computing scenario where the server is resource-abundant, and is capable of finishing the designated tasks. It is envisioned that secure media applications with privacy preservation will be treated seriously. In view of the fact that scale-invariant feature transform (SIFT) has been widely adopted in various fields, this paper is the first to target the importance of privacy-preserving SIFT (PPSIFT) and to address the problem of secure SIFT feature extraction and representation in the encrypted domain. As all of the operations in SIFT must be moved to the encrypted domain, we propose a privacy-preserving realization of the SIFT method based on homomorphic encryption. The security analysis based on the discrete logarithm problem and RSA that PPSIFT is secure against cipher text only attack and known plaintext attack. Experimental results obtained from different case studies demonstrate that the proposed homomorphic encryption-based privacy-preserving SIFT performs comparably to the original SIFT and that our method is useful in SIFT-based applications.

Privacy-Preserving Face Recognition:

Face recognition is increasingly deployed as a means to unobtrusively verify the identity of people. The widespread use of biometrics raises important privacy concerns, in particular if the biometric matching process is performed at a central or untrusted server, and calls for the implementation of Privacy-Enhancing Technologies. In this paper we propose for the first time a strongly privacy-enhanced face recognition system, which allows to efficiently hide both the biometrics and the result from the server that performs the matching operation, by using techniques from secure multiparty computation. We consider a scenario where one party provides a face image, while another party has access to a database of facial templates. Our protocol allows to jointly run the standard Eigen faces recognition algorithm in such a way that the first party cannot learn from the execution of the protocol more than basic parameters of the database, while the second party does not learn the input image or the result of the recognition process. At the core of our

protocol lies an efficient protocol for securely comparing two Pailler -encrypted numbers. We show through extensive experiments that the system can be run efficiently on conventional hardware.

Architechture:



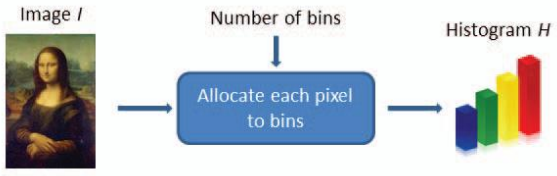
Existing System Model:

Participation of a third-party cloud computing platform also increases the vulnerability of private data, e.g., potential data breach and lost. 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 like data owner's personal identity, home address, or even financial records. Moreover, even we assume CSPs are completely honest and could be trusted to have data owners' private information, such privacy leakage still happens. In fact, cloud server is usually considered as a low-qualified locker rather than a strong bank deposit box. Comparing with traditional network server, the cloud computing platform suffers from more security threats. For instance, a severe vulnerability in cloud server is the sharing of computing resources: flaws in System Virtual Machine (SVM) software are frequently discovered and exploited to attack cloud servers in recent years.

The proposed system consists of two main phases as follows:

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

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 against CCP. (After that, the user can decrypt and get image processing results in plaintext.)



RGB Histogram

Functionality And Workflow:

Image feature detection algorithms can be divided into two main categories: global feature detection, e.g., RGB histogram, Color Layout Descriptor (CLD), Color Structure Descriptor(CSD) and so on, and local feature detection, e.g., SIFT, HOG. Here we use the functionality of RGB histogram as an illustrative example for global feature detection algorithms. In color feature detection algorithms, histogram descriptor is the most basic descriptor and building blocks for advanced feature descriptors. Based on color histogram, we can compute a series of prevalent color descriptors, including CSD, CLD. the computation algorithm of color histogram in plaintext is very simple. However, if we intend to perform this algorithm over cipher text domain, the functionality requirement makes it very difficult to be realized by simple encryption schemes: Need to enable the comparison between cipher text and plaintext to correctly distribute every pixel values into the color histogram. Intuitively, this functionality requirement seems to be contradictive to the design target of security, or the confidentiality of encryption

image data. If ciphertexts are comparable to plaintexts, the adversary can easily deduce all the values of encrypted pixels and get the sensitive information contained in an image. However, after carefully analyzing the functionality requirement of histogram algorithm, we can find that the exact required functionality is not the result of comparison between ciphertext and plaintext. The actually required functionality is the corresponding comparison result in ciphertext domain. Based on utilize a somewhat homomorphic encryption scheme to fulfill the corresponding functionality requirements and develop a privacy-preserving image global feature detection algorithm based on it. The corresponding experimental details are described in the paper.

Homomorphic Encryption Based Image Processing:

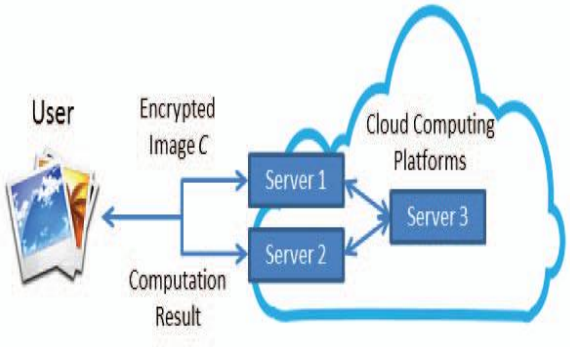
The proposing of homomorphic properties, Fully Homomorphic Encryption (FHE) has been considered as the Holy Grail in cryptography. After Gentry's breakthrough on lattice-based FHE , a general solution has been shown to allow homomorphic evaluations over ciphertext domain. However, applying existing general fully homomorphic encryption scheme to image processing applications would be far from practical, due to their huge computation complexity. Different from FHE, SHE schemes can only support limited times of homomorphic operations. Considering the design targets of secure image processing mechanisms, SHE schemes seem to be suitable for some image processing applications. Here, we first briefly introduce the framework of the state-of-the-art practical SHE scheme before discussing its merits and drawbacks. In order to encrypt the image data, we utilize the most recent Ring Learning with Error (RLWE) based SHE scheme from.

SHE scheme to be a tuple of algorithms: *SHE = (SH.Gen, SH.Enc, SH.Add,SH.Mult, SH.Dec)*. Among these algorithms, *SH.Gen* The SHE schemes are usually utilized in both secure image feature detection and secure image retrieval matching mechanisms. One typical example is in privacy-preserving face recognition mechanisms. In corresponding system model, a user first uploads an encrypted facial picture to cloud server as a query. After that, the cloud server performs the feature vector detection operations, and decomposes it into multiple Eigen faces over ciphertext domains. These ciphertexts are compared with the database held by cloud server to find matches through computing their Euclidean distances. Similar feature matching algorithms have been studied and implemented in various biometric matching, classification and clustering algorithms. However, one opening problem in implementing SHE schemes is the finite number of multiplications.

Configuring the scheme to support more multiplication operations leads to impractical computational complexity (increasing several orders of time complexity than the original algorithm). Since the number of multiplications will rapidly increase the computational complexity of homomorphic operations, some existing works try to avoid it by combining secure multiparty computation (SMC) techniques and homomorphic encryption schemes together. In these designs, the operations that require high computational complexity in homomorphic encryption schemes, like multiplication and factorial are realized by the means of using SMC based mechanisms instead of homomorphic operations. This design methodology provides a better performance on efficiency comparing with completely using homomorphic encryption-based solutions.

SMC BASED IMAGE PROCESSING:

Secure Multiparty Communication protocol is considered as a general solution to any function computations. However, since its enormous computation and communication complexity, it is not widely implemented in practice. Nevertheless, its advantage on compatibility and 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.



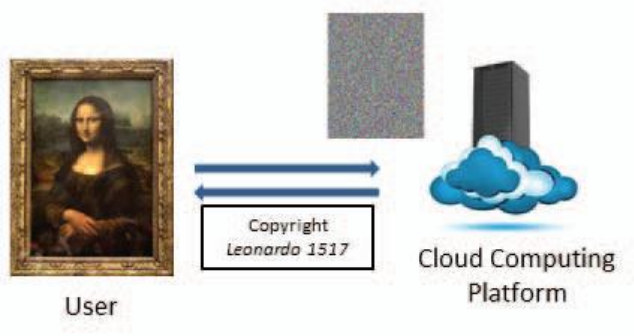
Utilizing SMC techniques by introducing additional cloud computing platform

1) SMC based Secure Image Feature Detection:

In image feature detection algorithms, the functionality requirements like comparison, factorial, and trigonometric operations exist in many complicated image feature detection algorithms. However, these operations over ciphertext domain require tens to hundreds of iterations of homomorphic additions and multiplications 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 cloud computing platform to utilize SMC techniques. user can easily realize homomorphic additions and ciphertext comparisons through introducing additional cloud servers.

For example, a simple implementation of one-time-pad encryption scheme from SMC protocols that splits one plaintext into two ciphertexts enables homomorphic additions. This design methodology can be generalized to utilize various arithmetic encryption methods from SMC protocols.

2) SMC based Secure Image Digital Watermarking



Workflow of Secure Digital Water marking Detection in Cloud

A digital watermark is a signal permanently embedded in digital data, i.e., audio, pictures, video. This signal is hidden in the host data in such a way that it is inseparable from the data and so that it is resistant to many operations not degrading the host digital data. The watermark can be detected or extracted later through computing operations in order to make assertions about the data. Various secure digital watermarking system models are proposed. In existing works, cloud is usually can be utilized to perform tasks like watermark generation, detection, and matching. Among them, one typical model in watermark detection.

To construct a secure watermark detection mechanism,most existing solutions leverage SMC techniques. In propose to use both secure sharing and watermarking schemes to protect user's media data in cloud. Similar to the multi-server structure utilized in image feature detection applications, the proposed secure sharing scheme divides users' data into multiple pieces and uploads them to different cloud servers, making it difficult to derive the whole information

from any one cloud. Another work in focuses on the efficiency of the video data watermarking, which splits the original video.

Hadoop distributed computing system for the different requirements to realize watermarks embedding. In, a framework for message privacy-preserving copy detection and watermark identification based on the signs of the Discrete Cosine Transform (DCT) coefficients is proposed. The architecture allows for searching in encrypted data and places the computational overhead on cloud server. The low frequency DCT coefficients are utilized to generate a dual set of keys to encrypt the source image, and a robust hash for the digital watermarking queries. Moreover, by utilizing SMC technique, some secure watermarking tasks performed on CCP side have shown close performance as performed in the plaintext domain.

CONCLUSION AND FUTURE WORK:

Privacy-preserving image processing on cloud computing platform, which could enable any fancy image processing based applications on devices with limited computation power. For example, a variety of instant image processing apps on the lens, watch or other personal devices. Comparing with other outsourced computation tasks, image processing algorithms are relatively complicated and have high computation complexity. To solve the problem, we start with building system model and formulating design targets. After that, the 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. The integration of different techniques other than traditional cryptography tools is the most promising research direction in this area.

In addition, considering the prevalence of JPEG compression among age data, which can be considered. Privacy-preserving decompression of JPEG file as a special case of privacy-preserving DCT computation is also a promising research direction in this area.

References:

[1] W. Lu, et al. Secure image retrieval through feature protection. In Proc. of ICASSP, 2009.
[2] C.-Y. Hsu, et al. Image feature extraction in encrypted domain with privacy-preserving SIFT. IEEE TIP, 21.11 (2012): 4593-4607.
[3] C.-Y. Hsu, et al. Homomorphic encryption-based secure SIFT for privacy-preserving feature extraction. In Proc. of SPIE, 2011.
[4] M. Naehrig, et al. Can homomorphic encryption be practical?. In Proc. of CCSW, 2011.
[5] W. Lu, et al. Enabling search over encrypted multimedia databases. In Proc. of SPIE, 2009.

[6] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft. Privacy-preserving face recognition. In Proc. of PET, 2009.
[7] M. K. Khan, J. Zhang, and K. Alghathbar. Challenge-response-based biometric image scrambling for secure personal identification, Future Generation Computer
Systems. 27.4 (2011): 411-418.
[8] Z. Qin, J. Yang, K. Ren, C. W. Chen, and C. Wang. Towards efficient privacy-preserving image feature extraction in cloud computing. In Proc. of MM, 2014.
[9] Z. Qin, J. Yan, K. Ren, C. W. Chen, C. Wang, and X. Fu. Privacy-preserving outsourcing of image global feature detection. In Proc. of GLOBECOM, 2014.
[10] T. Sikor. The mpeg-7 visual standard for content description-an overview. IEEE TCSVT, 11.6 (2001): 696–702.
[11] C. Gentry. Fully homomorphic encryption using ideal lattices. In Proc of STOC, 2009.
[12] H. Esfahani, et al. CloudBuild: Microsoft's Distributed and Caching Build Service." (2016).
[13] O. Goldreich. Secure multi-party computation. Manuscript. Preliminary version, 1998.
[14] C. Wang, et al. Privacy-assured outsourcing of image reconstruction service in cloud. IEEE TETC, 1.1 (2013): 166-177.
[15] K. Ivanova, et al. Features for art painting classification based on vector quantization of mpeg-7 descriptors. Data Engineering and Management. Springer, pp. 146–153, 2012