A Secured Data Processing Technique for Effective Utilization of Cloud Computing

Mbarek Marwan, Ali Kartit, Hassan Ouahmane

A Secured Data Processing Technique for Effective Utilization of Cloud Computing

Mbarek Marwan*, Ali Kartit, Hassan Ouahmane

University Chouaïb Doukkali, El Jadida
Laboratory LTI, Department TRI, ENSAJ
Avenue Jabran Khalil Jabran, BP 299 El Jadida, Morocco

*Corresponding author: marwan.mbarek@gmail.com

Abstract
Digital humanities require IT Infrastructure and sophisticated analytical tools, including data visualization, data mining, statistics, text mining and information retrieval. Regarding funding, to build a local data center will necessitate substantial investments. Fortunately, there is another option that will help researchers take advantage of these IT services to access, use and share information easily. Cloud services ideally offer on-demand software and resources over the Internet to read and analyze ancient documents. More interestingly, billing system is completely flexible and based on resource usage and Quality of Service (QoS) level. In spite of its multiple advantages, outsourcing computations to an external provider arises several challenges. Specifically, security is the major factor hindering the widespread acceptance of this new concept. As a case study, we review the use of cloud computing to process digital images safely. Recently, various solutions have been suggested to secure data processing in cloud environement. Though, ensuring privacy and high performance needs more improvements to protect the organization's most sensitive data. To this end, we propose a framework based on segmentation and watermarking techniques to ensure data privacy. In this respect, segementation algorithm is used to to protect client's data against untauhorized access, while watermarking method determines and maintains ownership. Consequentely, this framework will increase the speed of development on ready-to-use digital humanities tools.

keywords
cloud computing; digital humanities; security; data processing

INTRODUCTION

Cloud computing is a new distributing system that aims at providing computational resources and software to multiple consumers as services. Basically, this model is the result of recent developments in different areas of computer science, including parallel and distributed systems (PDS), virtualization, data deduplication and Service-Oriented Architecture (SOA). In this context, the National Institute of Standards and Technology (NIST) defines cloud computing as a model for delivering on-demand resources to clients through the Internet [Mell et al., 2009]. These resources are charged based on a pay-per-use business model. In addition to its value for offering powerful tools, the billing system relies on the time and bandwidth utilization. Therfore, this approach can significantly increase productivity and lower the cost through better utilisation of cloud services. There is no doubt, cloud computing offers many advantages and benefits to clients compared to an on-premises environment. In addition to this, cloud computing services create a truly collaborative environment to support researchers in sharing data repositories (text, images, numbers, audiovisual, objects, maps, etc). Beside economical benefits, adopting this concept enables ubiquitous access to remote shared services and resources. Figure 1 below illustrates the main features and characteristics of this new technology.

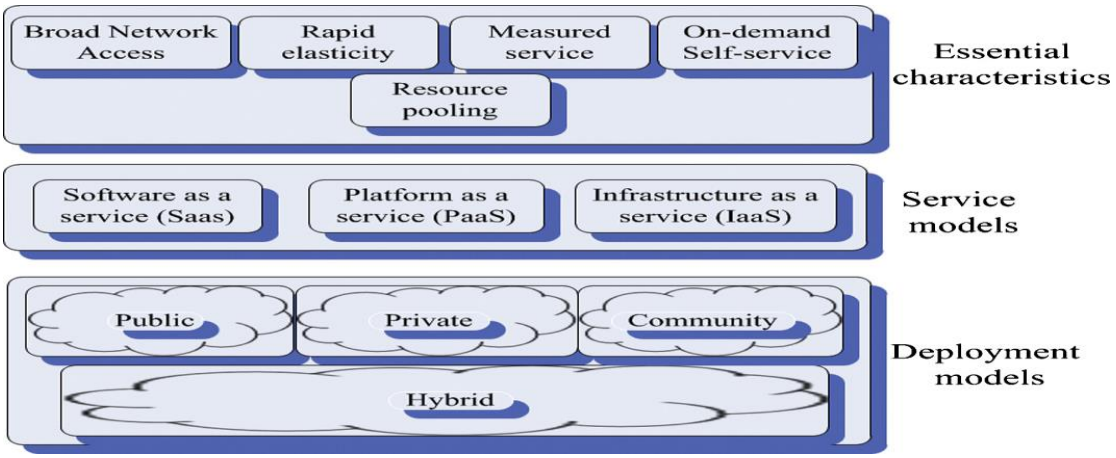

Figure 1. NIST Definition of cloud computing

In short, this new paradigm aims at boosting the integration of modern information and communication technology in different domains. Typically, it offers cost-efficient tools to perform data processing as a service, such as data visualization, data mining, statistics, text mining and information retrieval. Research in the field of humanities takes advantage of this sophisticated software to enhance the analysis and interpretation of data.

Beside its advantages, cloud-based data processing faces many problems due to its complex architecture and lack of official cloud standards. Clearly, cloud computing inherits some threats of its preceding technologies and comes with new issues. To overcome these challenges, we propose a secure framework to meet privacy requirements and avoid data disclusure. This solution is also meant to promote data sharing and collaboration between scientists in the digital humanities.

The rest of this paper is organized as follows. Section I discusses obstacles hindering the adoption of this new technology. Section II presents the essential requirements for privacy needs. Section III presents existing approaches for securing cloud-based data processing. Section IV discusses the state of the art of security in this new concept. Section V illustrates the proposed approach to meet security requirements and provides background information about techniques used to secure our proposed framework. We end this paper by concluding remarks and future work.

I CLOUD COMPUTING ISSUES

With the rapid progress in computing technology, the use of digital tools has become a core element in the digital humanities field. In recent years, the adoption of cloud technologies in this domain has grown significantly to respond to the increasing demand for IT services. Typically, cloud computing offers cost-efficient resources and services to help customers to keep up with trends in digital humanities software at competitive prices. Beside its great advantages, this new paradigm faces several challenges. This is the major factor that limits the implementation of cloud-based systems for data processing in the digital humanities domain.

1.1 Technical Issues

As outlined above, cloud computing relies on different advanced techniques, such as virtualization, Parallel and Distributed System (PDS), Web 2.0, etc. Hence, it inherits risks and threats associated with these technologies.

1.1.1 Virtualization

This technique enables different clients to share the same hardware. Hence, it allows users to run multiple operating systems and applications on the same server. This new concept aims at reducing the cost and providing high scalability. In spite of its multiple benefits, virtualization brings security and privacy issues, such as VM image sharing, VM isolation, VM escape, hypervisor issues and VM migration [Mazhar et al., 2015].

1.1.2 Data and Storage

Cloud computing provides cost-efficient storage systems to consumers. To achieve this goal, cloud relies on a distributed system. Consequently, data is spread across multiple servers located at different data centers. Moreover, this new paradigm uses a multi-tenancy environment to increase resource utilization and system reliability. Following this, it is difficult to implement a security policy and trust tools that meet all clients' requirements. Additionally, outsourcing data to an offsite cloud storage system arises additional threats and risks, namely data recovery vulnerability, improper media sanitization, data loss and disclosure, and data backup [Diogo et al., 2014].

1.1.3 Web Technology

Users have access to cloud services through the Internet. Furthermore, cloud providers rely typically on application programming interfaces (APIs) to allow clients to build their applications and use computational resources. Beside its benefits, using APIs raises several critical threats and risks, namely SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), broken authentication and session management, etc [Open Web Application Security Project, 2013].

1.1.4 Interoperability and Portability

Cloud environment uses various technologies and platforms, especially programming languages, program tools and different operating systems. Hence, to ensure interoperability between different clouds is a complicated task. Basically, this obstacle is due to the lack of standards that ensure interoperability and portability [Petcu et al., 2011].

1.2 Legal and Managerial Issues

Beside technical issues, the shift to cloud computing brings additional challenges. In fact, this new paradigm is based on a distributed architecture to meet clients' demands. So, cloud servers spread across different countries. Even worse, the majority of current acts do not cover these new cloud challenges [Pearson et al., 2010]. For this reason, cloud providers often use Service Level Agreement (SLA) to address these issues. However, to control the billing system and QoS of delivered cloud services need more improvements to meet specific compliance and requirements. Furthermore, the migration to cloud immediately leads to managerial issues caused by new workfow and procedures [Al Nuaimi et al., 2015].

II ESSENTIAL REQUIREMENTS FOR PRIVACY NEEDS

Security and privacy during data processing over cloud computing are the primary factors that obstruct the successful implementation of this new approach in the digital humanities domain.

Here are the main privacy requirements that need to be taken into account before developing a framework for data processing in cloud environment.

2.1 Integrity

Digital archives contain valuable information which provides extensive services to support researchers in the humanities. In this context, powerful online applications are used in sophisticated data analysis and retrieval. Hence, any remote changes of document content or document structure would lead to the incorrect interpretation of results. For that reason, digital archives need to be preserved and intact during the data processing operation. Moreover, digital data should not be degraded during its transmission over networks. To this end, algorithms and techniques used to handle digital data must be lossless and reversible.

2.2 Confidentiality

It is the process that prevents unauthorized users to have access the clients'data. So, docuement content should be kept secret during data processing when using cloud computing. In the cloud environment, data should also be protected against untrusted cloud providers. To achieve this goal, a document under study needs to be encrypted before sending it to cloud providers. For this objective, several techniques are commonly used to ensure adequate level of data protection, including cryptography, steganography, segmentation, etc.

2.3 Data Ownership

This technique aims at defining the rightful owner of a document. In the cloud system, any digital data should be assigned to the specific users of particular role. In fact, these digital records are used to improve humanistic studies by allowing researchers to analyze and share data repositories. For safety and security reasons, the owner's identity needs to be preserved during the study of digital data. To achieve this goal, the watermarking technique is often used to insert client's identity (ID) into documents.

2.4 Authentication

It is the process of identifying and validating user identity. In this scenario, the server of authentication entails clients to provide their identity (user ID or login ID). Typically, a successful authentication implies user's identity must be identical to the credential stored in the cloud computing. In general, the authentication mechanism plays a vital role in security controls by ensuring that only authorized users gain access to resources and services.

2.5 Authorization

This mechanism allows clients to have access to resources that they are authorized to use. Also, it prevents users from gaining access to resources that they are not allowed to reach. To this aim, it relies on access control lists for each digital data to restrict access to only the information in some rows of a document. In the cloud system, clients should have the ability to delegate specific access rights for their data by implementing fine grained acces models.

2.6 Availability

In many situations, the availability of computational tools is a crucial element because they play an important role in the digital humanities field. In fact, these software and applications are used to process digital data and documents efficiently. As a result, humanities researchers rely heavily on these advanced cloud tools to study digital archives in order to improve the quality of research in social sciences and humanities. To achieve this purpose, cloud platform is typically based on a distributed system. Furthermore, different techniques are used to

guarantee the availability of digital tools and technology, including load balancing, virtualization and cluster technology.

2.7 Anonymization

The identifying information related to the owner of digital data should be protected against unauthorized users. Indeed, researcher's information such as the name and institutional affiliation is also sensitive data. Hence, it needs to be kept confidential when using cloud services. More recently, several techniques have been developed to ensure anonymization in cloud computing, such as K-anonymity, L-diversity, T-closeness, etc.

III RELATED WORK

In Challa et al. [2015], the authors propose a new technique to perform image processing over cloud computing. To achieve this goal, R. Challa et al. suggest the homomorphic encryption method. The latter is based on Learning With Error (LWE) scheme. So, it allows carrying out both addition and multiplication operations on encrypted images. Following this, clients encrypt their images before sending them to the cloud provider. Then, they use this proposed approach to secure image processing over cloud. Consequently, the proposed concept ensures confidentiality and integrity of image processing over the cloud. However, homomorphic encryption is too slow for most practical applications that require complex image processing operations.

Mohanty et al. [2012] present a framework to secure data visualization over cloud computing. For this reason, the authors suggest Shamir's Secret Share (SSS) scheme and the pre-classification volume ray-casting technique to achieve this goal. Consequently, the image under study is divided into multiple pieces using the SSS technique in order to guarantee data confidentiality. In fact, the Shamir's (k, n) threshold scheme ensures that less than k centers can never reconstruct the secret image. Furthermore, secured volume ray-casting is performed across all nodes. Thus, it increases performance and availability.

Mirarab et al. [2014] suggest Eucalyptus infrastructure and ImageJ software to process digital data. In fact, Eucalyptus is an open source based on multiple nodes and clusters. Thus, it ensures availability and high performance. Also, the authors propose genetic algorithm (GA) and particle swarm optimization (PSO) to enhance resources allocation. The ImageJ tools are used to perform image processing operations. Basically, this software uses two components, namely ImageJ plug-ins to implement this application and ImageJ Macro to handle images. As a result, the proposal provides a high availability cloud framework to process images.

Mohanty et al. [2013] illustrate a cloud-based solution that performs a volume ray-casting technique over cloud. To achieve this goal, the authors propose a method based on Shamir's Secret Sharing scheme and ray-casting technique. The proposed framework has four modules: the Server, Interpolation module, the Compositor that carries out post-interpolation, and the Client interface to view images. The proposal provides an efficient ray-casting tool over cloud. In fact, it guarantees confidentiality, integrity, availability and high performance.

In Gomathisankaran et al. [2013], the authors propose the homomorphic encryption scheme based on Residue Number System (RNS) to secure image processing. In fact, the proposed technique allows executing mathematical operations over ciphertext. So, addition, subtraction and multiplication are carried out over encrypted images. The proposal enables to apply Sobel filter to encrypted images for performing the edge detection technique. As a result, the

proposed framework ensures the confidentiality and integrity of image processing over cloud. The authors suggest implementing this framework over cloud computing for enhancing performance.

Qing Zang et al. [2011] proposed a method based on Hadoop framework to process digital images. In fact, Hadoop system provides efficient resources to handle images. It uses Hadoop Distributed File System (HDFS) to offer a scalable storage system. Furthermore, MapReduce enables to distribute tasks across multiple nodes. Thus, it increases reliability and performance. To address access control issues, the authors use login and password. In spite of its many advantages, the proposed solution is incapable of guaranteeing the privacy of image processing, such as confidentiality, integrity and authentication.

Bednarz el al. [2012], present a solution for images analysis over cloud computing instead of on-site imaging tools. The proposed framework is divided into three basic components: the NetCTAR based on the OpenStack cloud, PAAS as a runtime environment and CSIRO that provides a processing toolbox. So, it provides three services: HCA-Vision to quantify data features, MILXView to analyze 3D images, and X-TRACT to handle X-ray images. Beside its promising features, the proposed solution suffers from several limitations in terms of security such as lack of confidentiality, integrity and authentication mechanisms.

Todica et al. [2008] propose a cloud framework that uses Service-Oriented Architecture (SOA) to perform data processing. This concept improves traditional data analysis and interpretation systems that rely on in-house software. Basically, the proposed solution is built based on distributed systems to guarantee availability and reliability. It also aims at promoting interoperability between research institutes of the social sciences and humanities by using XML standard. To address security issues, the authors use developed utility components. The latter offers access control, authentication and traceability mechanisms.

In Vemula et al. [2015], a framework based on Hadoop system to perform complex image processing is suggested. To that end, it uses generic MapReduce to distribute requests among available nodes to guarantee reliability. The authors use MapReduce function to split an image into multiple small portions. Hence, it enhances the confidentiality of digital data. In addition, the proposed solution enables parallel extraction of an image to improve system performance. In this study, two algorithms are implemented to verify and validate the proposed solution, i.e. Laplacien filter and Canny Edge Detection.

Sathish et al. [2013] illustrate a solution based on Hadoop to process 2D and 3D digital images. To that end, the authors implement Dynamic Switch of Reduce Function (DSRF) to enhance MapReduce function. This technique aims at reducing the idle time and then improves performance. To achieve this goal, the proposed framework consists of three components, namely the Master to split an image, Map function to process data and Reduce function, which combines intermediate images for generating the final result. Consequently, this method ensures availability and confidentiality by splitting an image into many portions.

Chiang et al. [2011] present a framework based on Service-Oriented Architecture (SOA) to process images. Furthermore, it uses ImageJ software to provide several image processing algorithms. The proposed framework has four components: the presentation layer as an interface between the client and the application, service layer, business logic and ImageJ tool. Consequently, this framework provides a rich tool to process images. In the same line, this

proposal enables interoperability between scientists. However, security issues need more improvements to meet privacy requirements.

Himardi et al. [2013] illustrate a solution to process digital images over cloud computing. The proposed framework relies on Service-Oriented Architecture (SOA) to provide data processing as a service to consumers. To that end, it uses DIPE system to offer a set of image processing algorithms and services. Additionally, the proposal is divided into three models: Programming, Services and Messaging. However, fewer details related to security and privacy are provided in this study.

In Kagadis et al. [2015], a cloud based solution is used for disease detection. The proposed framework enables clients to process digital data over cloud computing. To achieve this goal, the solution is divided into four components: the front-end, intelligent load balancer to distribute requests, universal storage, and processing VMs responsible for image processing. Moreover, the authors suggest standard role-based authentication to guarantee privacy. Additionally, data exchange is secured using SSL and HTTPS protocols.

IV DISCUSSION

Many research institutions in humanities and social sciences are interested in adopting this new model to take advantage of remote cloud software. In this case, imaging tools are offered to clients as a service to analyze digital archives. Unfortunately, security and privacy are the main barriers to the widespread adoption of this technology. Recently, various solutions have been proposed to overcome these challenges. In spite of its multiple benefits, these proposed frameworks need more improvements in terms of security and privacy. In general, homomorphic algorithms are not suitable for image processing because they are too slow. In this respect, Service-Oriented Architecture (SOA) is used to enhance system performance. However, this technique does not protect data against untrusted cloud providers. Moreover, the use of secret sharing scheme in conjunction with image processing algorithms is a complicated task. Table 1 below sums up the main existing solutions to address security problems in cloud based image processing.

References	Proposed techniques	Advantages	Disadvantages
Mohanty et al. [2012] **Mohanty et al. [2013]**	Shamir' Secret Share Scheme (SSS)	It ensures confidentiality by splitting the image under study into shares. Also, it guarantees fault tolerance. Moreover, this method increases performance by distributing generated shares across multiple nodes using load balancing algorithm.	Shamir's Secret Share generates encrypted shares. Hence, the information in these shadow images is not the same in the original image. Following this, to process an image using these shadow images needs to adopt the used algorithms in order to handle shadow images.
In Challa et al. [2015] **Gomathisa-nkaran et al. [2013]**	Homomorphic encryption	It performs arithmetic operations on encrypted data, including addition and multiplication. So, it ensures the confidentiality and privacy of images.	This technique has limitations in terms of performance. In addition, imaging technology requires complex algorithms. However, homomorphic encryption performs only simple arithmetic operations.

Todica et al. [2008] **Chiang et al. [2011]** **Himardi et al. [2013]**	Service-Oriented Architecture (SOA)	SOA allows collaboration and interoperability between cloud providers. Besides, it increases performance by distributing tasks across multiple nodes. Meanwhile, it improves the availability of cloud services.	SOA relies on web technology, which faces several threats and risks. Besides, SOA approach does not ensure privacy of digital images against cloud providers.

Table 1. Current approaches for securing image processing over cloud computing

V POROPOSED FRAMEWORK

Cloud-based data processing is a new approach that aims at outsourcing computations to an external provider. Hence, organizations take advantage of advanced imaging tools without investing in local applications. In spite of its multiple benefits, the shift to this paradigm arises many problems. In this respect, various frameworks are proposed. However, security and privacy need more improvements to prevent unauthorized or accidental access to client's data. In this study, we propose a secure framework based on segmentation approach to address security risks. The proposal aims at meeting privacy requirements in the digital humanities.

5.1 The Fundamentals of the Proposed Framework

As outlined above, security and privacy issues are the major elements that hinder the widespread adoption of cloud-based image processing in the digital humanities domain. To address these issues, we introduce a third party called CloudSec. The latter is an interface between clients and cloud providers. Moreover, the proposed architecture will be implemented in a multi-cloud environment, as depicted in Figure 2.

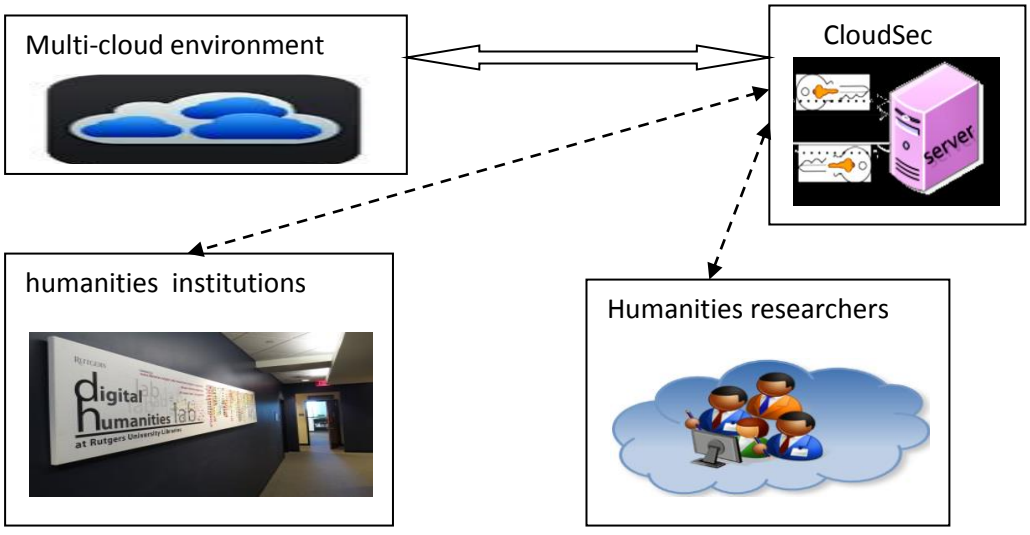

Figure 2. Architecture of the proposed framework

Of course, clients send a digital image to CloudSec using SSL connection to secure communication. Then, CloudSec stores client's identifying information in a local database and sends the image to the cloud providers in order to perform image processing. This approach seeks to guarantee data anonymization. To address the issue of confidentially, we propose the multi-region segmentation using the Graph-Cut scheme [Delong et al., 2009].

Hence, the input image is divided into multiple regions using the Graph-Cut algorithm in order to improve security and image analysis, as shown in Figure 3. Basically, it aims at achieving a high security level of digital image by splitting data into several portions before sending them to the cloud provider. Furthermore, image segmentation plays a vital role in the field of image processing and analysis.

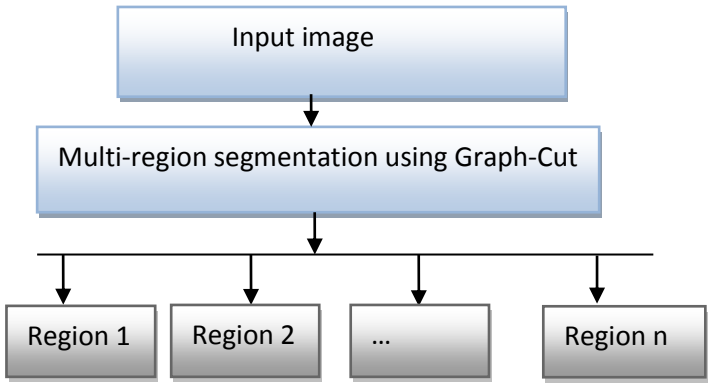

Figure 3. The principle of multi-region segmentation

In addition, we propose the reversible watermarking technique based on the Thodi algorithm [Thodi et al., 2004, Thodi et al., 2007] to insert client's ID in each region. In fact, the Thodi algorithm is a reversible watermarking algorithm, which is usually designed to survive normal image processing operations. In this proposed framework, the watermaking method seeks to ensure authentication. Figure 4 below illustrates the fundamentals of the proposed framework.

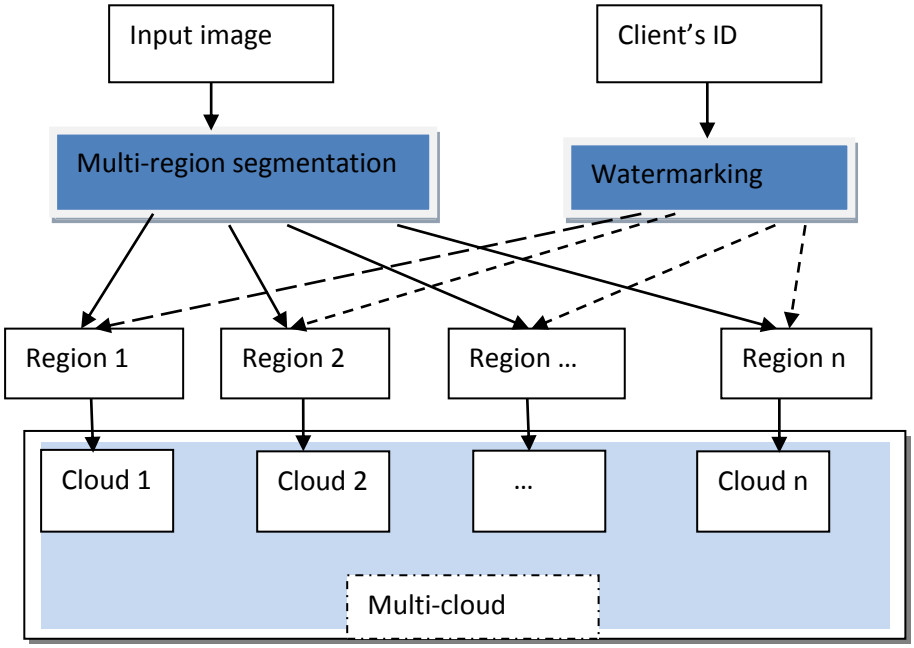

Figure 4. The fundamentals of the proposed framework

Following this, the image under study is divided into multiple regions. Next, we insert client's ID into generated regions. Then, each region will be sent to a distinct cloud in a multi-cloud environment. Consequently, each region will be analyzed in a distinct cloud computing. The post-processing result is sent to CloudSec module. Based on these measures, the proposed framework is an appropriate solution to promote image analysis via cloud computing in the

digital humanities domain. In fact, this solution provides the high level of data protection and authentication mechanisms to meet security requirements. Additionally, it uses multi-cloud model to meet QoS requirements for data processing by improving system performance.

5.2 An Overview of the Proposed Techniques

In the proposed framework, we use two main mechanisms to ensure privacy and security in cloud based image processing, i.e. watermarking and segmentation.

5.2.1 Reversible Watermaking

This technique seeks to insert client's ID called watermark into the image under study in a lossless manner. In fact, the amount of distortion introduced by this technique should be small to avoid wrong interpretation. For authentication purposes, the watermark is extarcted to identify the owner. In general, these algorithms are based on different approaches, such as compression, histogram modification, quantization and expansion. Recently, various reversible watermarking algorithms have been proposed. Consequentely, it is difficut to choose the best one. According to the study carried out in [Asifullah et al., 2014], reversible watermarking algorithms based on expansion approaches are effective and easy to implement. Moreover, the result of the experiment carried out in [Asifullah et al., 2014] shows that the Thodi algorithm [Thodi et al., 2004, Thodi et al., 2007] is an appropiate method to meet digital image's requirements. Indeed, this algorithm is typically rapid and efficient. Figure 5 illustrates the fundamentals of the Thodi algorithm.

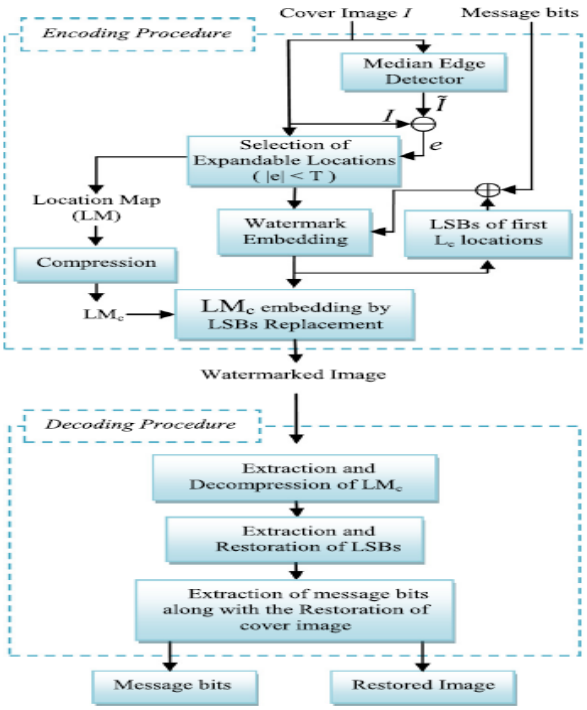

Figure 5. Flowchart for the Thodi algorithm [Asifullah et al., 2014]

5.2.2 Multi-region Segmentation

This technique is a partitioning of an image into several segments. In general, these methods are classified into two main categories: edge-based and region-based segmentation. In region-based segmentation, pixels with similar values are grouped in a specific region. Nevertheless,

pixels are classified edge or non-edge to locate boundaries between regions in the edge-based segmentation. In this study, we propose a multi-region segmentation algorithm using Graph-Cut. In particular, we use the framework developed by A. Delong et al in [Delong et al., 2009]. The proposed solution relies on single Graph-Cut and multi-region enregy to globally optimize multi-region objects. Moreover, this method encodes geometric interactions between distinct regions and boundary models. Accordingly, the image under study is split into many regions. Thus, it facilitates data analysis and helps scientists to make a good decision. In addition, this technique allows CloudSec module to divide data into several regions in order to send each region to a distinct cloud provider. Consequently, it increases data confidentiality and performance.

5.3 Security Analysis of the Proposed Framework

In the proposed framework, digital data are broken up into small parts using segmentation. So, each cloud provider has to process only a small portion of the secret data. As a result, this method enhances confidentiality of digital data. Moreover, the proposal relies on the Thodi algorithm to perform reversible watermarking. The latter is typically used to insert client's ID into generated regions to ensure authentication and ownership. Additionally, the proposed technique improves performance by distributing tasks among different cloud nodes that belong to a multi-cloud system. In sum, our approach guarantees both security and performance when using cloud services in the digital humanities domain.

CONCLUSION AND FUTURE WORK

Cloud-based data processing is an emerging concept that aims at providing advanced tools to help consumers. These sophisticated tools are used only when needed and charged based on cloud resources utilization. Consequently, humanities researchers are attracted by this promising technology. Beside its many advantages, this novel model faces several challenges. In fact, security and privacy need more improvements to protect clients' data. To this end, various implementations are proposed to promote digital image processing using cloud services. However, these proposed frameworks have limitations in terms of security and performance. In this study, we propose a solution based on segmentation and watermarking techniques to enhance privacy and security. Our proposal will be implemented in a multi-cloud environment to improve security and performance. The proposed framework is an ongoing project that will be developed using Java and MySQL database. Next, we will apply this solution on historical documents to improve data analysis in the humanities and social sciences.

References

Mell P. and Grance T. The NIST Definition of Cloud Computing. *Technical Report, National Institute of Standards and Technology*, vol. 15, pp. 1-3, 2009.

Mazhar Ali, Samee U. Khan and Athanasios Vasilakos V. Security in Cloud Computing: Opportunities and Challenges. *Information Sciences, Elsevier*, pp. 357–383, 2015.

Diogo A, Liliana F, B. Soares, Joao V. Gomes, Mario M., Freire, Pedro R. and Inacio M. Security Issues in Cloud Environments: a Survey. *International Journal of Information Security, Springer,* pp. 113-170, April 2014.

Open Web Application Security Project, 2013 Top 10 List, [Accessed 12 Jan 2017], Available: https:// owasp.org/index.php/Top_10_2013-Top_10

Petcu D. Portability and Interoperability Between Clouds: Challenges and Case Study. *Springer Heidelberg,* Volume 6994, pp. 62-74, 2011.

Pearson S. and Benameur A. Security and Trust Issues Arising From Cloud Computing. *Proceedings of the IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom),* pp. 693-702, 2010.

Al Nuaimi N., AlShamsi A., Mohamed N. and Al-Jaroodi J. E-Health Cloud Implementation Issues and Efforts. *Proceedings of the International Conference on industrial Engineering and Operations Management (IEOM),* 2015, pp. 1–10.

Challa R. K., JNTUK, Kakinada, G. VijayaKumari and Sunny B. Secure Image Processing Using LWE Based Homomorphic Encryption. *Proceedings of the IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT),* March 2015, pp. 1-6.

Mohanty M., P. K. Atrey and Ooi W.-T. Secure Cloud-Based Medical Data Visualization. *Proceedings of the ACM Int. Conf. on Multimedia*, 2012, pp. 1105-1108.

Mirarab Ali, Fard G. and Shamsi M. A Cloud Solution For Medical Image Processing. *International Journal of Engineering Research and Applications*, Vol. 4, Issue 7, pp.74-82, July 2014.

Mohanty M., W.-T. Ooi and Atrey P. K. Secure Cloud-Based Volume Ray-casting. *Proceedings of the IEEE Int. Conf. on Cloud Computing Technology and Services (CloudCom'13)*, Bristol, UK, December 2013, pp. 531-538.

Gomathisankaran M. Xiaohui Yuan and Patrick Kamongi. Ensure Privacy and Security in the Process of Medical Image Analysis. *Proceedings of the IEEE International Conference on Granular Computing (GrC)*, pp. 120-125, Dec 2013.

QingZang H., Y. Lei, Y. MingYuan, W. Fu Li and Rong Hua L. Medical Information Integration Based Cloud Computing. *Proceedings of the International Conference Network Computing and Information Security (NCIS)*, vol. 1, May 2011, pp. 79-83.

Bednarz T., Wang D., Y. Arzhaeva, P. Szul, S. Chen, A. Khassapov, N. Burdett, T. Gureyev and Taylor J. Cloud-Based Image Analysis and Processing Toolbox for Biomedical Applications. *Proceedings of the IEEE International Conference on eScience*, Chicago, Oct 2012, pp. 8-12.

Todica V., Tech and Vaida M. F. SOA-Based Medical Image Processing Platform. *Proceedings of the. IEEE International Conference on Automation, Quality and Testing, Robotic (AQTR)*, 2008, pp. 398-403.

Vemula S. and Christopher Crick. Hadoop Image Processing Framework. *Proceedings of the IEEE International Congress on Big Data*, 2015, pp. 506-513.

Sathish V. and Sangeetha T.A. Cloud-based Image Processing With Data Priority Distribution Mechanism. *Journal of Computer Applications*, Vol. 06, Issue 1, 2013, pp. 6-8.

Chiang W., H. Lin, T. Wu and Chen C. Building a Cloud Service for Medical Image Processing Based on Service-Orient Architecture. *Proceedings of the 4th International Conference on Biomedical Engineering and Informatics*, pp. 1459 – 1465, Oct. 2011.

Himadri Nath Moulick and Moumita Ghosh. Medical Image Processing Using a Service Oriented Architecture and Distributed Environment. *American Journal of Engineering Research (AJER)*, Volume 02, Issue 10, pp. 52-62, 2013.

Kagadis G., Alexakos C., P. Papadimitroulas, N. Papanikolaou, V. Megalooikonomou and Karnabatidis D. Cloud Computing Application for Brain Tumor Detection. *European Society of Radiology, Poster C-1851*, pp. 1-16, 2015.

Delong A. and Boykov Y. Globally Optimal Segmentation of Multi-region Objects. *Proceedings of the IEEE 12th International Conference on Computer Vision*, 2009, pp. 285-292.

Thodi D.M. and Rodriguez J.J. Prediction-Error Based Reversible Watermarking. *Proceedings of the International Conference on Image Processing*, pp. 1549–1552, 2004.

Thodi D.M. and Jrodríguez .J. Expansion Embedding Techniques for Reversible Watermarking. *IEEE Trans. Image Process*, vol. 16, issue 3, pp. 721–730, 2007.

Asifullah Khan, Ayesha Siddiqa, Summuyya Munib and Sana Ambreen Malik. A Recent Survey of Reversible Watermarking Techniques. *Proceedings of Elsevier, Information Sciences*, 2014, pp. 251–272.