A Cloud-based Framework to Secure Medical Image Processing

Mbarek Marwan, Ali Kartit and Hassan Ouahmane

Chouaïb Doukkali University–El Jadida
LTI Laboratory, TRI Department, ENSA
Avenue Jabran Khalil Jabran, BP 299 El Jadida, Morocco
E-mail: marwan.mbarek@gmail.com; alikartit@gmail.com;
hassan.ouahmane@yahoo.fr

Received 15 February 2018; Accepted 14 August 2018;
Publication 08 September 2018

Abstract

In the last few years, advanced software for processing medical images has gained a great interest in modern medicine. In fact, it provides valuable clinical information, and hence, can significantly improve diagnosis and treatment. Nevertheless, implementing these imaging tools often requires an important capital budget in both IT applications and hardware. This solution can unfortunately cause a dramatic increase in operational expenses and medical costs. To mitigate this problem, medical providers are shifting their interest onto using cloud computing, particularly the Software-as-a-Service (SaaS) model, instead of in-house data centres. In this case, healthcare professionals rely on remote applications delivered by an external provider to process patients' digital records. Interestingly, in this paradigm, consumers are billed based on software utilization. Besides, cloud computing promises to offer a better Quality of Service (QoS), including availability, elasticity, trust, response time, security assurance, etc. Regardless of its significant financial benefits, the transition to the cloud environment gives rise to security and privacy problems, especially in the healthcare domain. Recently, various security measures

Journal of Mobile Multimedia, Vol. 14_3, 319–344.
doi: 10.13052/jmm1550-4646.1434

and mechanisms have been suggested to overcome these challenges and accelerate the adoption of cloud computing services. In this regard, numerous cryptographic techniques are used to safely process digital medical images, techniques that make use of homomorphic cryptosystems, Secret Sharing Schemes (SSS), Service-Oriented Architecture (SOA) and Secure Multi-party Computation (SMC). Although these methods are deemed very promising, they can negatively impact the performance of cloud services. Most precisely, they are not yet mature enough to satisfy Service Level Agreement (SLA) constraints. The main contribution of this study consists of presenting a novel approach to secure cloud-based medical image processing. This proposed solution combines segmentation techniques and genetic algorithms together in one model. Based on this method, we rely on pixel intensity and entropy measurements to split an image into a number of regions to maintain data privacy. The principal reason for using genetic algorithms is to optimize the number of generated regions. Furthermore, we opt for an architecture based on multi-cloud systems and CloudSec module to enable distributed data processing and prevent accidental disclosure of medical information. As shown in the simulation results, the proposal is an appropriate framework for fuelling the integration of cloud applications in the healthcare sector. In particular, it enables clients to securely use remote image processing tools.

Keywords: Cloud computing, medical image processing, security, segmentation, genetic algorithms.

1 Introduction

Basically, cloud computing is a term that refers to a new distributing system that permits clients to use computational resources and software as a service. To achieve this objective, cloud utilizes diverse techniques and emerging trends in computer technology, including Parallel and Distributed Systems (PDS), data deduplication, virtualization and Service-Oriented Architecture (SOA). As a matter of fact, there is a variety of definitions related to cloud computing. Today, the widely accepted one is provided by the National Institute of Standards and Technology (NIST) [1]. The latter defines this paradigm as an efficient way for delivering on-demand resources to the consumers via the Internet. The essential characteristics of this model are depicted in Figure 1.

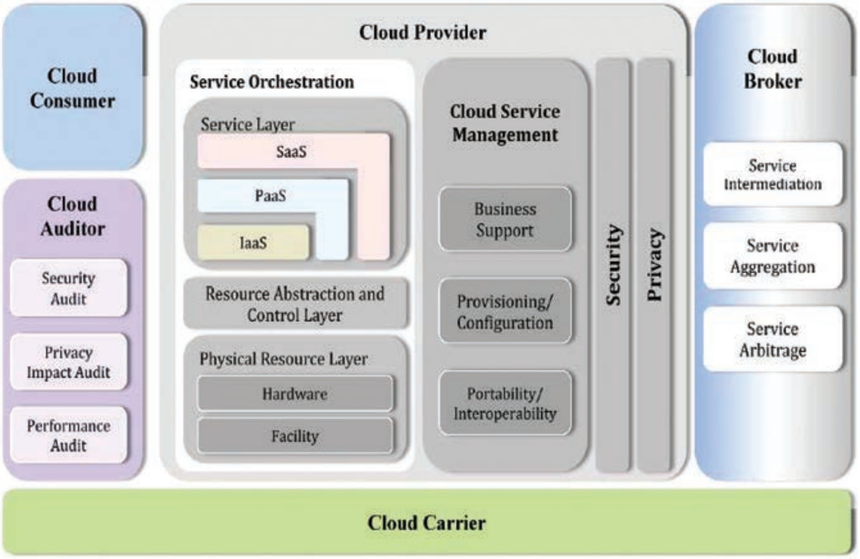

Figure 1 NIST Definition of cloud computing [1].

For an optimal usage of cloud services, these resources are billed basically according to pay-per-use business models that rely on the time and bandwidth consumption. In addition, various parameters are used to measure the QoS of cloud services, parameters such as security, availability, response time, etc. These attributes are designed principally to determine the credibility of the third party. More specifically, Service-Level Agreement (SLA) is an official commitment used mainly to set expectations for both clients and cloud providers. Essentially, cloud computing permits an easy access to remote shared services. Normally, four deployment models are suggested to perfectly match the needs of healthcare organizations. Thus, clients have the ability to either deploy public or private cloud services according to their needs. The first concept allows clients to make economies since resources are used by many different organizations. In contrast, the second one is very expensive because cloud resources are devoted exclusively to one customer. Alternatively, it is possible to use a mixture of private cloud and public cloud services to come up with a hybrid cloud model. In a generic context, community cloud has recently been proposed to serve the specific needs of different members with common interests or profiles. Technically, cloud providers offer many options as to the implementation of a cloud solution, responding to consumers' needs and challenges. More precisely, this new paradigm encompasses three popular types of cloud computing services namely Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In most cases, the SaaS layer provides the required applications and imaging tools that are necessary to manage and process health records remotely. In the case of PaaS, cloud providers offer development and deployment tools allowing users to build local applications. In the same line, IaaS model enables consumers to create and use virtual machines (VMs) instead of local servers. Based on these considerations, cloud services tend to facilitate and boost the use of modern information and communication technologies in the healthcare sector. More importantly, healthcare professionals are charged based on software utilization according to predefined SLA clauses. In such a model, cloud providers offer flexible, scalable and cost-effective imaging tools to process health records, as illustrated in Figure 2.

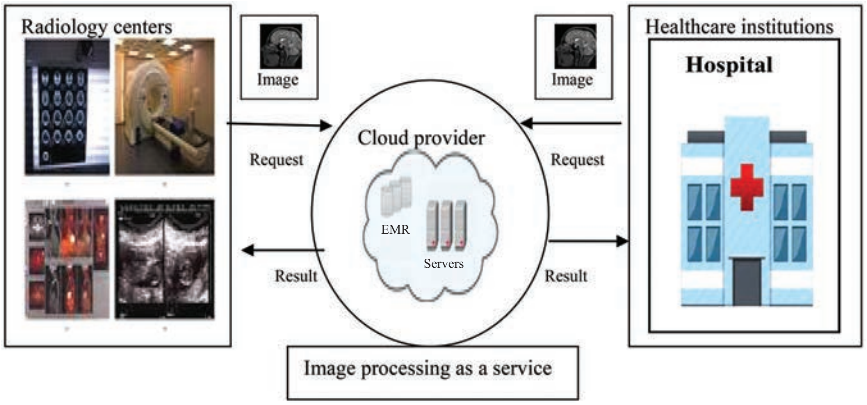

Figure 2 Basic idea of medical images processing using cloud.

In such a scenario, healthcare practitioners and imaging centers outsource their medical records to a cloud provider who manages the process of image analysis. The external third party uses advanced software to satisfy the requirements of the consumer's query. After that, the result of post-processing is sent back to the end user. Consequently, the Software-as-a-Service (SaaS) model is an adequate solution that enables healthcare institutions to delegate computations to a cloud provider. Following this, clients can benefit from the IT services and necessary resources without a need to build and maintain on-site data centers. This is the major reason for the increasing demand of cloud implementation. Despite its multiple advantages, cloud technology still faces enormous security problems because clients lose tight control of their outsourced data and computations. In general, these challenges and risks can be classified into two categories. The first category specifically encompasses technical issues including virtualization [2], data location [3, 4], web technology [5] and interoperability [6–8]. The second one is mainly related to legal and management constraints [9, 10]. Beyond that, medical images are sensitive data used basically for diagnosis purposes. Accordingly, ensuring the privacy of these digital records requires additional security measures. In this regard, a broad range of parameters need to be taken into account when designing a secure framework [11–13], including availability, integrity, authorization, confidentiality, data ownership, authentication and anonymization. To this purpose, various approaches and schemes are suggested to secure data processing in an untrusted cloud environment. These solutions and the corresponding protection mechanisms, though, rely heavily on traditional encryption techniques, such as homomorphic algorithms, SOA, SMC and secret share schemes. Therefore, these existing approaches are usually less effective and unfeasible for processing medical images since they have a negative effect on executing time. For this reason, we propose a hybrid solution based on segmentation techniques and genetic algorithms to ensure confidentiality and better performance.

The remainder of this work is organized as follows. In Section 2, we provide and analyze existing solutions suggested to secure medical image processing over cloud computing. Section 3 illustrates the proposed framework to meet security requirements and provides background information about techniques involved in privacy-protection mechanisms. Section 4 provides simulation results. In Section 5, we present some advantages of our proposed method, as well as directions for future research. Finally, we end this paper in Section 6 by remarks and future work.

2 Existing Mitigation Techniques

Nowadays, expensive local data centers are replaced by economical cloud resources and services. Basically, cloud computing is a large distributed system that offers huge amounts of storage and processing capability. To this end, cloud platform relies on a wide range of technologies and services to meet the constraints of service level agreement (SLA). However, the utilization of cloud services in healthcare domain can expose the patients' data to high privacy and security risks. Today, there are already many and varied security techniques to ensure data privacy. This section provides the common methods and their applications in the field of image processing. In this regard, we provide two illustrative scenarios for each approach.

2.1 Secret Share Scheme

This technique is widely used to protect confidential information in distributed systems like cloud computing. For (T, N)-threshold scheme, a secret message a_0 is shared among N different cloud providers. To this aim, it necessary to randomly select coefficients a_j from $\mathbb{Z}p$ as indicated in the following equation [14]:

$$\mathrm{b(x)} = \mathrm{a}_0 + \sum_{j=1}^{T-1} a_j x^j \ (\mathrm{mod\ p}) \tag{1}$$

Accordingly, the secret message is converted to the several shares (x, b(x)). In the same line, the secret data can be reconstructed only if at least T shares are available. In this context, we rely on the Lagrange interpolation formula as follows [15]:

$$\mathrm{a}_0 = \sum_{j=1}^{T} b(x_j) \prod_{k=1,\ k\neq j}^{T} \frac{x_k}{x_{k\ -\ x_j}} (\mathrm{mod\ p}) \tag{2}$$

Practically, we create many shares from the secret image in order to process each part at different cloud providers. Afterwards, we combine the processed shares to get the final image. This process ensures that it is computationally infeasible for an untrusted cloud to reveal any confidential information. In this context, Deepthi et al. [16] use Shamir's Secret Sharing (SSS) method to process images in an encrypted domain. Specifically, they use the (2, 2) scheme for implementing image processing over cloud computing. First, they create two shares from the secret image using SSS method. Meanwhile, the processed image is basically reconstructed by combining these two shares. For example, this method allows cloud providers to perform image interpolation operation and 2D DCT in encrypted domain. Lathey et al. [17] rely on the SSS technique to secure image quality enhancement. In this concept, it is possible to perform arithmetic division operations for non-terminating decimal quotients on the encrypted data. First, an authorized client needs to retrieve required shares from different CDCs (Cloud Data

Centres). Next, they combine these shares to reconstruct the processed image. In this case, the proposed technique can perform some basic image processing such as denoising, antialiasing, unsharp masking and contrast enhancement.

2.2 Homomorphic Encryption

This type of encryption is designed to execute arithmetic operations on ciphertext. More precisely, this scheme is homomorphic over an operation '*', and hence, supports the following Equation (3):

$$\mathrm{E}(\mathrm{m}_1) * \mathrm{E}(\mathrm{m}_2) = \mathrm{E}(\mathrm{m}_1 * \mathrm{m}_2), \forall\, m_1,\ m_2 \in M \tag{3}$$

Where E is the encryption algorithm and M is the secret message.

The algorithms used to perform the homomorphic evaluation of an arbitrary function fall into two main categories: (1) Partially Homomorphic Encryptionc (PHE), and (2) Fully Homomorphic Encryptionc (FHE). The first model supports one arithmetic operation, e.g. Paillier, RSA, ElGamal, etc. In the FHE model, one has the ability to perform addition and multiplication on the encrypted data. In this case, we encrypt the original medical images before transmitting them via the Internet to a cloud provider. The latter processes the encrypted data without disclosing confidential information. For this reason, the application of this concept in image processing over cloud computing has attracted significant attention. Broadly speaking, Paillier is largely used to process images in the encrypted domain because it is additively homomorphic [18], as shown in (4).

Let m_1, m_2 be two plaintext and $\mathrm{r} < \mathrm{N}$ a random value.

$$\begin{aligned}\mathrm{E}(\mathrm{m}_1, \mathrm{r}_1) \cdot \mathrm{E}(\mathrm{m}_2, \mathrm{r}_2) &= (\mathrm{g}^{\mathrm{m}_1}\mathrm{r}_1^{\mathrm{n}})(\mathrm{g}^{\mathrm{m}_2}\mathrm{r}_2^{\mathrm{n}}) \pmod{\mathrm{n}^2} \\ &= \mathrm{g}^{\mathrm{m}_1+\mathrm{m}_2}(\mathrm{r}_1\mathrm{r}_2)^{\mathrm{n}} (\mathrm{mod}\ \mathrm{n}^2)\end{aligned}$$

Hence,

$$\begin{aligned}\mathrm{D}(\mathrm{E}(\mathrm{m}_1, \mathrm{pk}) \cdot \mathrm{E}(\mathrm{m}_2, \mathrm{pk}) &= \mathrm{D}(\mathrm{E}(\mathrm{m}_1 + \mathrm{m}_2, \mathrm{r}_1\mathrm{r}_2)) \\ &= m_1 + m_2\end{aligned} \tag{4}$$

Where E and D are encryption and decryption function, and pk is the public key.

In this context, Ibn Ziad [19] et al. develop a framework to extend the popular computer vision library OpenCV. To this aim, they rely on a homomorphic cryptosystem to delegate image processing to a remote third party. More specifically, Paillier algorithm is used to perform the requested image enhancement operations on encrypted images. This means that it is possible to analyze images using cloud services. In this case, the proposed solution can perform certain tasks, such as adjustment, spatial filtering, edge sharpening and histogram equalization. Similarly, Hu et al. [20] use the homomorphic encryption properties of Paillier algorithm to secure nonlocal denoising in outsourced images. This is achieved by using a combination of two cryptosystems: Paillier and privacy-preserving transform based on JL Transform. In addition, the proposal uses nonlocal means (NLM) technique, which is composed of nonlocal search and mean filter. The proposed framework proves efficient as to the implementation of denoising methods for encrypted images, especially in the cloud computing.

2.3 Service-Oriented Architecture

Basically, SOA technology is meant to improve the reusability and maintainability of web services in distributed systems like cloud computing. In this model, services are provided to remote users through a service contract. In this architecture, service directory (SD) is essentially a lookup mechanism. Hence, it helps service requester to find a service according to some criteria. Meanwhile, service provider (SP) defines a service description and publishes their services (register). In the context of cloud, SOA architecture is composed of three modules: Service Broker, Service Provider and Service Consumer, as shown in Figure 3.

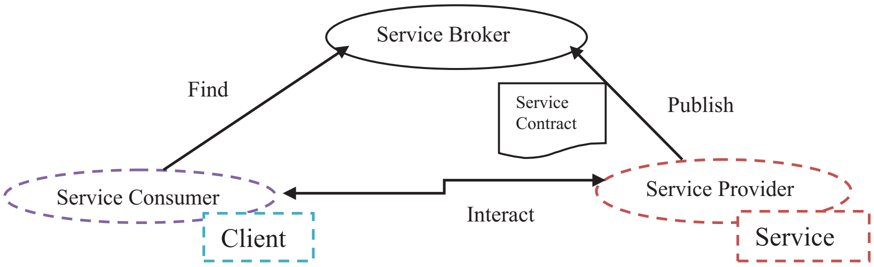

Figure 3 SOA interaction cycle.

More importantly, the communication between different services and clients is done by using standards, dependency-reducing methods, decoupled message-based techniques such as XML document exchanges. Recently, the utilization of SOA technology has gained popularity in image processing over cloud computing. In this context, Vaida et al. [21] propose a SOA-based framework to process medical images. To this aim, they use Enterprise Service Bus (ESB) as a distributed infrastructure. Besides, the proposal relies on XML-based data and (SOAP) as communication protocols. The proposed framework has three components, namely Programming module, Service module and Messaging module. This solution can perform two services: object detection and grayscale filter. Another advantage of the XML-based model is that it promotes collaboration between clients. In this perspective, Shen et al. [22] develop a medical image annotation system for tele-radiology. This web-based application allows users to access and interpret digital data remotely. The proposal consists of three major components: Collaboration, Real-time and Pervasive. The implementation results show that this application supports collaborative annotation of medical images.

2.4 Secure Multi-party Computation

It is an important approach in cryptography to secure collaboration between *m* parties in order to evaluate an arbitrary function $\mathrm{f}\left(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_\mathrm{m}\right)$. In this case, x_i is private while f(.) is known to all parties involved in the computations. In the secure image processing model, there are two parties, clients and cloud providers, who own health records and imaging tools respectively. For example, we define a filtering operation $\mathrm{f}(\cdot)$ described by a set of parameters Θ and an image $\mathrm{x}\ (\mu, \nu)$. The result $\mathrm{y}\ (\mu, \nu)$ of this model is presented in (5).

$$\mathrm{y}(\mathrm{t}) = \mathrm{f}(\mathrm{x}, \Theta) \tag{5}$$

In the secure multi-party computation model, clients obtain $\mathrm{f}\ (\mathrm{x}, \Theta)$ without any knowledge of Θ; and cloud provider processes $\mathrm{x}\ (\mu, \nu)$ without the disclosure of private data, as illustrated in Figure 4.

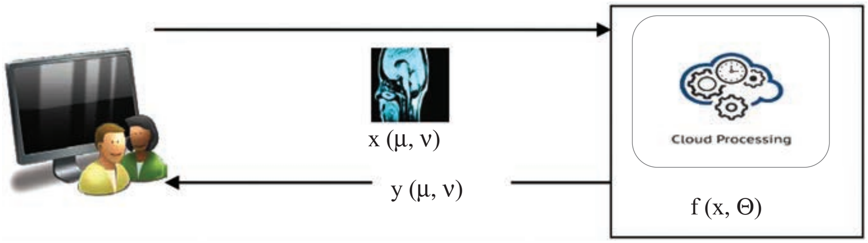

Figure 4 Basic principles of image processing using SMC.

Since data privacy is of a paramount importance, SMC protocols are used to secure image processing. There are, of course, a number of applications for which SMC protocols are helpful. The typical scenario here is an image processing application that involves linear operations such as inner products and squared error distance. Practically, SMC protocols can operate successfully with many methods such as homomorphic encryption, Oblivious Transfer (OT), Garbled Circuit (GC), secret share scheme. For example, Sadeghi et al. [23] propose a method to secure face recognition. In this case, clients can search for a specific image stored in the remote database without revealing any additional information about the requested image. The proposed privacy-preserving method relies on SMC approach, in particular homomorphic encryption and Garbled circuits. Avidan et al. [24] propose a method to secure a face-detection web service. To this aim, they use the SMC protocol so that clients can submit their images to be analyzed in a secure manner. Additionally, machine learning methods are used to accelerate the process of data classification. The simulation results show that the proposal can perform face detection without revealing the sensitive data.

3 Proposed Framework

Cloud-based medical image processing is an efficient way to outsource computations to an external provider. The adoption of this new technology in healthcare domain, however, leaves room for potential security threats. Unfortunately, existing techniques are still in need of more improvements to meet security and performance requirements. In this regard, we propose a secure framework based on segmentation and genetic algorithms so as to afford an optimal privacy protection. Compared with existing techniques, this new approach uses lightweight, efficient and scalable methods to prevent malicious disclosure of medical data.

3.1 The Fundamentals of the Proposed Framework

In general, security and privacy are the major factors hindering the implementation of cloud-based medical image processing in the healthcare sector. To overcome these challenges, we introduce a trusted third party called CloudSec. It is designed to provide an interface that enables secure data exchanges between consumers and public cloud providers. Besides, the proposed framework will be deployed in a multi-cloud environment, as shown in Figure 5.

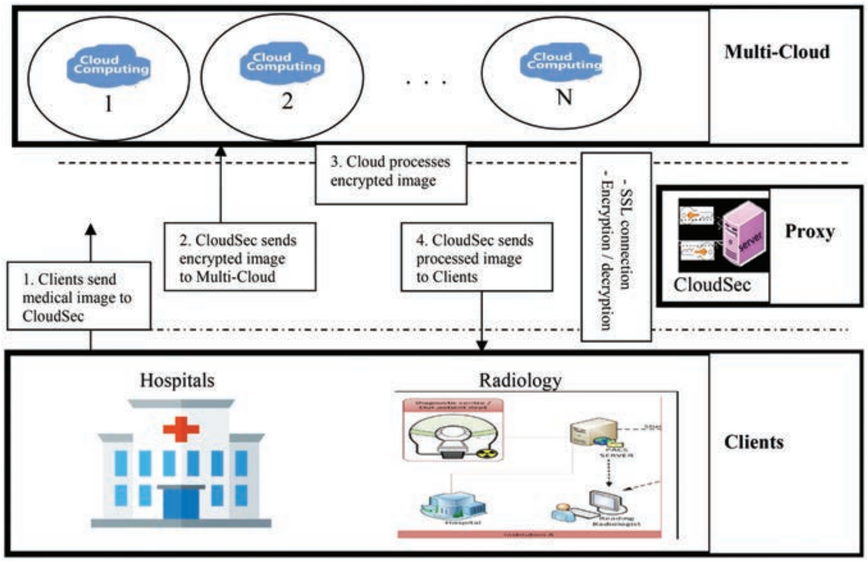
Cloud Computing
1
Cloud Computing
2
. . .
Cloud Computing
N
Multi-Cloud
3. Cloud processes encrypted image
- SSL connection
- Encryption / decryption
server
Proxy
CloudSec
1. Clients send medical image to CloudSec
2. CloudSec sends encrypted image to Multi-Cloud
4. CloudSec sends processed image to Clients
Hospitals
Radiology
Clients

Figure 5 Architecture of the proposed framework.

In such an approach, healthcare professionals send a medical image to the CloudSec using (Secure Sockets Layer) SSL. The aim is to establish a secure connection for transmitting medical images. Equally importantly, CloudSec uses a local database to store the patients' identification information and guarantee thereby data anonymization and unlinkability. Typically, secret data are encrypted before being transferred to the cloud computing. Since the CloudSec module is the core element of our proposed architecture, it is necessary to implement appropriate mechanisms in order to avoid a single point of failure (SPOF). To this end, we propose software-defined storage (SDS) to greatly improve the system availability [25]. This new paradigm is designed to abstract storage resources from the underlying hardware platform unlike traditional network-attached storage (NAS) or storage area network (SAN) systems. The primary objective of this concept is to achieve cost-effective load balancing. When administered correctly, this technology would inevitably ensure fault tolerance, scalability, good performance and high availability. To ensure the privacy and security of medical images, we use a hybrid method (GA-ES) based on entropy-based segmentation (ES) and genetic algorithm (GA) to guarantee data confidentiality. In this context, the image under study is split into blocks of the same size. Next, segmentation based on entropy is applied to each block to determine the region to which it belongs. In this regard, the entropy H (d) is calculated using Equation (6) [26].

$$\mathrm{H}(d) = \sum_{i=1}^{L} \mathrm{p}(m_i)\ \ log \frac{1}{\mathrm{p}(m_i)} \tag{6}$$

Where, L stands for the total number of pixel value, and $\mathrm{p}(m_i)$ is the probability of occurrence of a pixel with value m_i.

To address the issue related to the region growth, the threshold is calculated using the ratio of the number of the blocks to the number of created regions. As a result, this solution successfully meets high data confidentiality by means of splitting data into several portions before sending them to the public cloud provider, as shown in Figure 6.

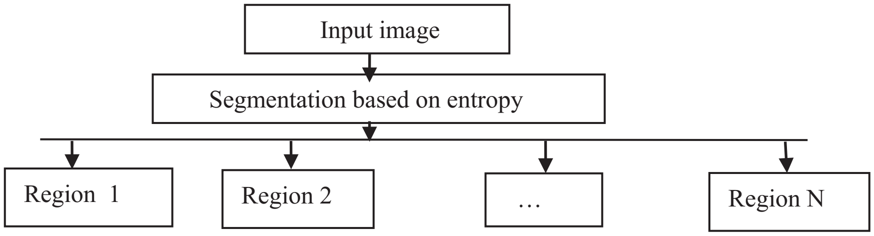

Figure 6 The principle of segmentation based on entropy.

More importantly, we propose a genetic algorithm to calculate the optimal entropy threshold value for all regions. Therefore, this mechanism determines the size of generated regions. Obviously, the size of a region often has a detrimental effect upon the time required to analyze each region. Meanwhile, it has an impact on the quality of data encryption. For this reason, we use two parameters to evaluate the quality of data encryption: correlation coefficient (Cor) and the number of pixels change rate (NPCR). Consequently, this technique seeks to reduce processing time and ensure robustness. To this objective, a genetic algorithm is used to determine the most suitable parameters, as presented in Figure 7.

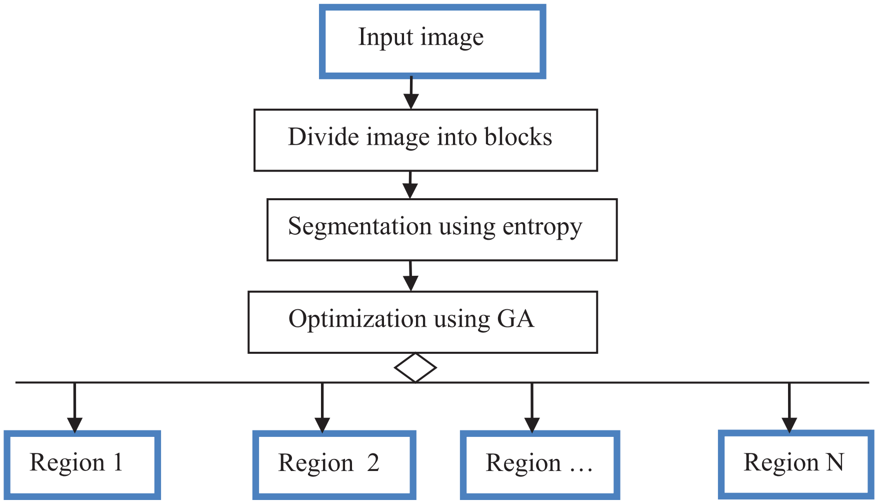

Figure 7 The fundamentals of the proposed approach.

After segmentation, the image under study is divided into many regions. Subsequently, each region will be sent to a distinct cloud in a multi-cloud environment. Hence, each region will be analyzed in a distinct cloud to enhance security and performance. Then, the outcome of this process is returned to the CloudSec, as shown in Figure 8.

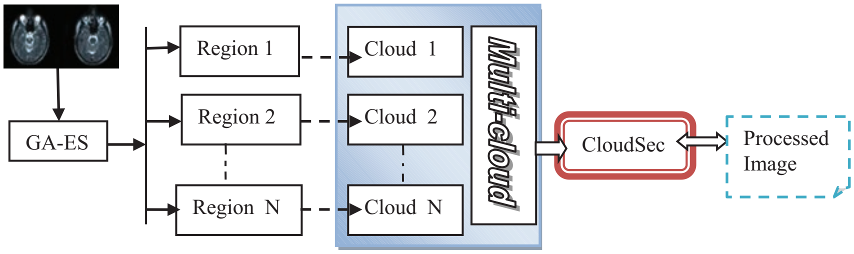

Figure 8 Abstract view of the proposed framework.

3.2 An Overview of the Proposed Techniques

In the proposed framework, we use two techniques to ensure the privacy and security in cloud-based medical image processing: Genetic Algorithm (GA) and segmentation.

Genetic Algorithms (GA) [27–29]: These techniques are artificial intelligence methods used mainly to examine and manipulate possible solutions in order to select the best one. To achieve this objective, this method uses approaches basically inspired by the fundamentals of natural selection systems. Hence, it is mandatory to define parameters that have a high probability of meeting predefined criteria. Based on these considerations, three basic operators are mostly used in genetic algorithms to find the optimized solution, i.e., selection, crossover and mutation, as shown in Figure 9.

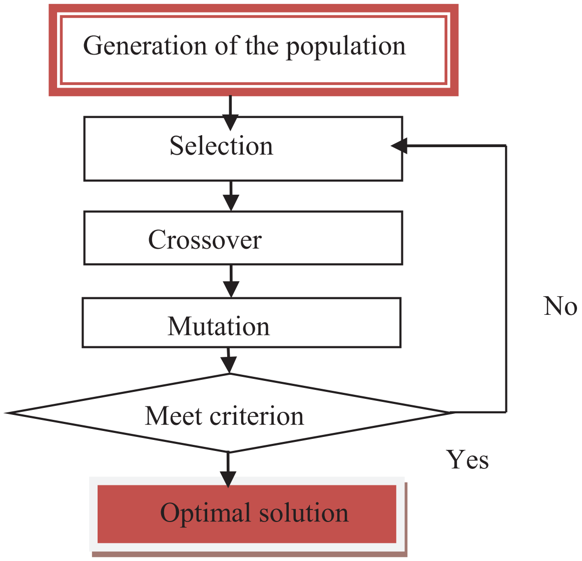

Figure 9 A simplified model of a genetic algorithm.

In this model, the initial problem (segmentation result) is represented as a chromosome, which is characterized by the size of its population and the crossover probability. Then, we define a fitness function to measure the quality of a chromosome and to select chromosomes that will be used for mating in the reproduction stage. The process is repeated until we get the optimized solution.

Fitness function: This technique aims at determining parameters that lead to the best solution. Functionally speaking, it performs quality evaluation tasks. In this study, we seek principally to minimize execution time and enhance data confidentiality. For this task, we rely on two parameters to define the fitness function: the number of regions and robustness parameters. The latter is evaluated basically using correlation coefficient (Cor) and the number of pixels change rate (NPCR). The correlation coefficient (Cor) is calculated according to the following equations [30]:

Let x and y denote the gray-scale of two adjacent pixels. In practice, the coefficient (Cor) is evaluated using the formula in (7).

$$\mathrm{Cor_{xy}} = \frac{\mathrm{COV(x,y)}}{\sqrt{\mathrm{D(x)}}\sqrt{\mathrm{D(y)}}} \tag{7}$$

$$\mathrm{D(x)} = \frac{1}{\mathrm{N}}\sum_{\mathrm{i=1}}^{\mathrm{N}}\left(\mathrm{x_i} - \frac{1}{\mathrm{N}}\sum_{\mathrm{i=1}}^{\mathrm{N}}\mathrm{x_i}\right)^2 \tag{8}$$

$$\mathrm{COV(x,y)} = \frac{1}{\mathrm{N}}\sum_{1}^{\mathrm{N}}\left(\mathrm{x_i} - \mathrm{Av}\left(\mathrm{x}\right)\right)\left(\mathrm{y_i} - \mathrm{Av}\left(\mathrm{y}\right)\right) \tag{9}$$

$$\mathrm{Av} = \frac{1}{\mathrm{N}}\sum_{\mathrm{i=1}}^{\mathrm{N}}\mathrm{z_i} \tag{10}$$

Where Av refers to the average value.

For the second parameter, the NPCR is calculated using the formula in (11) [29]:

$$\mathrm{NPCR} = \frac{\sum^{\mathrm{i,j}}\mathrm{D(i,j)}}{\mathrm{W}\times\mathrm{H}}\times 100\% \tag{11}$$

Where D (i, j) is calculated with the following expression:

$$\mathrm{D(i,j)} = \left\{\begin{array}{l} 0,\ \mathrm{if}\ \mathrm{C_1}\left(\mathrm{i,j}\right) = \mathrm{C_2}\left(\mathrm{i,j}\right) \\ 1,\ \mathrm{if}\ \mathrm{C_1}\left(\mathrm{i,j}\right) \neq \mathrm{C_2}\left(\mathrm{i,j}\right) \end{array}\right\}$$

Where, $\mathrm{C_1}$ and $\mathrm{C_2}$ are ciphertext images before and after one pixel changes in a plaintext image.

In the proposed approach, the fitness function that is used to measure the performance of each individual chromosome is defined using the Equation (12).

$$\mathrm{Total\ time} = \mathrm{R_1}\times\mathrm{T_1} + \cdots + \mathrm{R_n}\times\mathrm{T_n} \tag{12}$$

Where R refers to the number of blocks in a region, and T is the processing time required to analyze a block using a specific image processing algorithm.

4 Simulation and Results

As outlined above, we propose an entropy-based segmentation method to assign all pixels to a region. Particularly, we use the Shannon’s theorem to calculate the entropy of a discrete random distribution with different color components of an image, as defined by Equation (6). In this study, we apply the proposed approach on RGB images. Accordingly, the histograms p(x) are typically measured by counting the number of pixels with a given color intensity (red (R), green (G) or blue (B)). Additionally, Genetic Algorithm (GA) is used to reach near-optimal solutions. Hence, the entropy-based segmentation problem is formulated as an optimization problem, as shown in Algorithm 1.

Algorithm 1 GA-ES

```
Inputs: I (x $\times$ y), where I is a medical image
Outputs: $<$ R$_1$, R$_2$, ..., R$_n$$>$, where R refers to created regions
        Step 1: Choose encode method
            Convert input image into data set X = $\{x_1, x_2, \ldots, x_n\}$
             of n objects
        Step 2: Initialize_population ();
        Step 3: Optimize the individuals of initial population
            Selection ();
            Crossover ();
            Mutation ();
            Fitness ();
        Step 4: Repeat Step 3 until the fitness of the population
               no longer improves;
        Step 5: Return $<$ R$_1$, R$_2$,..., R$_n$ $>$
```

As emphasized earlier, the proposed system is designed to achieve a desirable tradeoff between the security and performance in cloud computing. For the purpose of illustration, we use MATLAB R2014a to implement this method and we choose two RGB images (image 1 and image 2) as examples. In this case, the medical image is split into four homogeneous regions. Afterwards, we apply image processing operations on each region. To create the final image, we combine all processed regions. In this study, we use the Gaussian filter for noise removal and enhancement of image quality. The findings are illustrated in Figures 10 and 11.

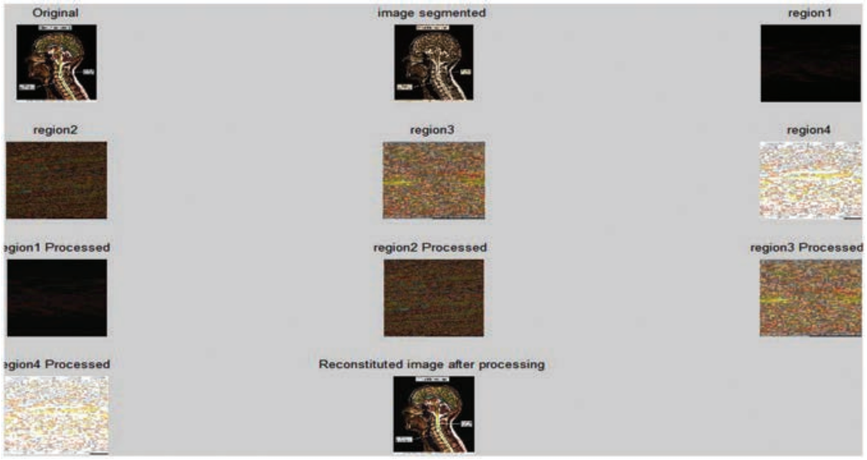

Figure 10 Application of GA-ES algorithm to process image 1.

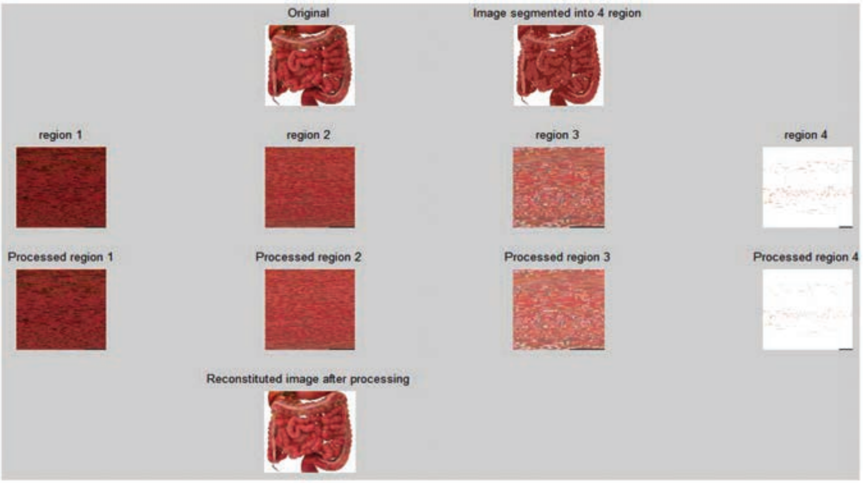

Figure 11 Application of GA-ES algorithm to process image 2.

5 A Comparative Study and Directions for Future Research

So far we stressed the fact that data protection and security are the key issues as to the integration of cloud computing in healthcare domain. In this regard, several solutions and frameworks have been recently proposed to ensure data protection in this paradigm. Nevertheless, existing approaches and schemes still have limitations in terms of Quality of Service (QoS). Precisely, techniques involved in encoding data have a negative effect on performance. This would limit the feasibility of the system at several typical stages in healthcare data processing. The main advantages and disadvantages of existing privacy protection measures are presented in [31]. In this context, homomorphic encryption is used to execute arithmetic operations on encrypted data, including addition and multiplication. However, these algorithms are often not suitable for image processing because they are time consuming. Obviously, the manipulation of large volumes of data requires efficient algorithms. To enhance performance, Service-Oriented Architecture (SOA) approach is proposed to enhance interoperability. Nevertheless, SOA technology does not protect data against an untrusted cloud provider. In other words, it permits data processing even though the security of the outsourced data is not guaranteed. To this purpose, the Secret Sharing Scheme (SSS) and Secure Multi-party Computation (SMC) are also suggested to secure cloud-based medical image processing. However, the use of these techniques in conjunction with image processing algorithms is a complicated task. That is why we propose a simple method that allows a user to process medical data securely.

5.1 A Comparative Study

Our approach is built on the premise that a distributed data processing system is an efficient method for reducing disclosure risks. The proposal is also useful to minimize the quantity of data processed by each cloud. In this regard, a medical record is divided into several regions to keep data secret by using the segmentation concept rather than the cryptographic techniques. Under these conditions, each cloud has to handle and analyse only a small amount of the original medical image. As a result, this method is useful in protecting the confidentiality of medical information, especially against insider threats from untrusted cloud providers. In this regard, we use genetic algorithm to determine the optimal number of regions that satisfy the Quality of Service (QoS) requirements. More precisely, this method seeks to improve performance by reducing the processing time required to analyze each created region. Besides, the segmentation technique does not require complex and heavy mathematical calculations, unlike traditional cryptography. Therefore, it is an efficient approach to deal with the large volume of data. Essentially, it enhances the data confidentiality by splitting the secret image into many regions to achieve the confusion and diffusion effects. Hence, one cloud provider processes a specific region without being able to reveal any information about the secret image. Functionally speaking, the present mechanism based on segmentation techniques actually improves medical image analysis, and therefore helps healthcare professionals to enhance diagnosis and treatment. In addition, using a multi-cloud environment would improve the response time and reduce security risks that may emerge in a single cloud computing [32]. In this architecture, the proposal relies on a trusted provider called CloudSec to guarantee unlinkability and maintain anonymity. In fact, patients' information is stored in a local database. Consequently, this system allows healthcares to outsource data processing to third-party cloud providers. Indeed, the proposed approach improves both data security and performance. Table 1 gives a concise summary of the differences between the proposed method and the existing ones.

Table 1 Comparison between the proposal and other methods

References	Techniques	Confidentiality	Performance	Simplicity	Anonymity	Unlinkability
[21, 22]	SOA		√	√		
[19, 20]	Homomorphic	√				
[16, 17]	SSS	√				
[23, 24]	SMC	√				
Our proposal	GA-ES	√	√	√	√	√

5.2 Directions for Future Research

As discussed above, there are various approaches to deal with security concerns in the cloud-based applications. In this paper, we suggest entropy-based segmentation to avoid unauthorized disclosure of confidential information. This method is more suitable for images because of its ability to maintain data privacy by only changing the pixel's position. Simply put, efficiency and simplicity are the major advantages of using segmentation approach to secure image processing. Another method to improve the efficiency of image processing is the utilization of distributed parallel computing framework, like Hadoop and Spark [33, 34]. In these frameworks, we use the MapReduce function to store data in a distributed file system, so that each node processes only a small part. However, despite the fact that this method seems to be widely accepted, the adoption of this approach in the cloud faces many challenges. This is due largely to issues related to interoperability and insider threats caused by malicious cloud providers. In this respect, multi-cloud model is a promising strategy for boosting distributed data processing. Recently, there has been an increased interest in using blockchain technology to provide security for electronic transactions. In this model, all transactions are encoded in such a way that any modifications can be quickly detected and traced. Originally, the cryptographic hash algorithm used in such case is SHA256. In the blockchain model, a block is basically composed of two main elements, i.e., a header and transactions. The header contains the metadata about a block, such as previous block hash, mining competition and merkle tree root. The latter contains all transactions in a block. More importantly, each block has a timestamp and information linking it to a previous block, as presented in Figure 12.

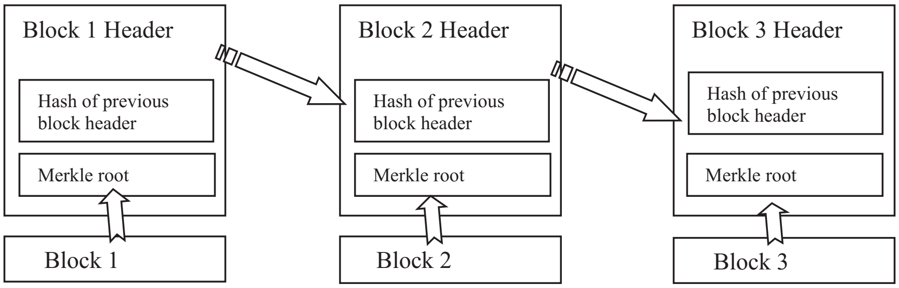

Figure 12 Simplified data structure in blockchain technology.

One of the most important application areas for blockchain technology is cryptocurrencies (Ethereum and Bitcoin). Today, blockchain is emerging in a wide range of applications, especially in collaborative work environment. In this context, Xia et al. [35] propose a blockchain-based access control system to protect medical data stored on cloud computing. In a similar vein, Zyskind et al. [36] suggest the utilization of both Shamir's Secret Sharing (SSS) and Secure Multi-party Computation (SMC) to run computations directly on the network. This mechanism aims at limiting insider threats that may be caused by malicious third party providers. Although blockchain systems ensure integrity protection and identity management, the utilization of blockchain technology in image processing is still in its infancy. Therefore, there is a need to extend the scope of the blockchain method to include other domains like image processing over cloud computing.

6 Conclusion and Future Work

Today, cloud computing is revolutionizing the way healthcare organizations use IT services, especially imaging tools. In such a model, these sophisticated remote applications are used only when needed and billed according to software utilization. Specifically, using cloud in medical image processing is an emerging concept that delivers cost-efficient imaging tools to the consumers. The latter is basically charged according to software utilization and SLA contract. That is the reason why both academia and healthcare industry are becoming noticeably interested in this emerging trend. Beside its significant benefits, this novel concept raises several challenges and risks. Specifically, security and privacy are the major factors that hinder the implementation of cloud services in the healthcare system. To this aim, many frameworks and security measures have been recently developed to prevent data exposure. A variety of techniques are suggested for privacy-preserving, including homomorphic encryption, Shamir's secret sharing (SSS) scheme, secure multi-party computation (SMC) and service-oriented architecture (SOA). Although these cryptographic techniques ensure data security and privacy, they are unfortunately time-consuming. Consequently, they negatively affect the Quality of Service (QoS) of the system. Similarly, SOA technology does not protect data against untrusted cloud providers. In summary, existing approaches still have limitations in terms of security and performance. In this study, we design a generic framework to securely process patients' data. To this end, we propose a solution based on genetic algorithm and segmentation. The confidentiality of medical images is mainly assured by the segmentation technique, which divides the sensitive data into multiple portions. Within this perspective, the secret image is split into many regions based on entropy. In such a scheme, we use the genetic algorithm to limit the number of regions and enhance data security. For this task, we define a fitness function that takes into consideration all factors involved in security and performance to find the optimal solution. Additionally, we extend the conventional cloud architecture with an additional trusted entity, i.e., CloudSec module. The simulation results prove that the proposal is an adequate solution to boost image analysis using public cloud computing. It significantly improves both security and performance. Having said this, this work is not intended to replace existing approaches and frameworks, but it aims at providing a simple and efficient solution to ensure privacy protection and assure that the performance requirements are met. As a future work, we plan to carry out more complex image processing operations to evaluate the proposed approach. There are good reasons to use blockchain-based access control to secure cloud services. This technology is principally suitable to secure data sharing and enhance collaboration among healthcare professionals.

References

[1] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., and Leaf, D. (2011). NIST cloud computing reference architecture. *NIST Special Publication*, 500(2011), 1–28.

[2] Birje, M. N., Challagidad, P. S., Goudar, R. H., and Tapale, M. T. (2017). Cloud computing review: concepts, technology, challenges and security. *International Journal of Cloud Computing*, 6(1), 32–57.

[3] Kumar, P. R., Raj, P. H., and Jelciana, P. (2017). Exploring Security Issues and Solutions in Cloud Computing Services–A Survey. *Cybernetics and Information Technologies*, 17(4), 3–31.

[4] Noman, A., and Adams, C. (2013). Providing a data location assurance service for cloud storage environments. *Journal of Mobile Multimedia*, 8(4), 265–286.

[5] Singh, A., and Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, 79, 88–115.

[6] Radwan, T., Azer, M. A. and Abdelbaki, N. (2017). Cloud Computing Security: challenges and future trends. International Journal of Computer Applications in Technology, 55(2), 158 –172.

[7] Kaur, K., Sharma, D. R., and Kahlon, D. R. (2017). Interoperability and Portability Approaches in Inter-Connected Clouds: A Review. *ACM Computing Surveys (CSUR)*, 50(4), 49.

[8] Tran, H. M., Ha, S. V. U., Dang, H. T., and Huynh, K. V. (2014). Fault resolution system for inter-cloud environment. *Journal of Mobile Multimedia*, 10(1&2), 16–29.

[9] Shirazi, F., Seddighi, A., and Iqbal, A. (2017). Cloud Computing Security and Privacy: An Empirical Study. In *International Conference on Human-Computer Interaction* (pp. 534–549). Springer, Cham.

[10] Kumar, P. R., Raj, P. H., and Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. *Procedia Computer Science*, 125, 691–697.

[11] Yüksel, B., Küpçü, A., and Özkasap, Ö. (2017). Research issues for privacy and security of electronic health services. *Future Generation Computer Systems*, 68, 1–13.

[12] Anjum, A., Malik, S. R, Choo, K. R., Khan, A., Haroon, A., Khan, S., Khan, S. U., Ahmed, N. and Raza, B. (2018). An efficient privacy mechanism for electronic health records. *Computers & Security*, 72, 196–211.

[13] Marwan, M., Kartit, A., and Ouahmane, H. (2018). A Framework to Secure Medical Image Storage in Cloud Computing Environment. *Journal of Electronic Commerce in Organizations (JECO)*, 16(1), 1–16.

[14] Shamir, A. (1979). How to share a secret. *Communications of the ACM,* 22(11), 612–613.

[15] Cheraghi, A. (2014). Sharing several secrets based on Lagrange's interpolation formula and Cipher feedback mode. *International Journal of Nonlinear Analysis and Applications,* 5(2), 60–66.

[16] Deepthi, S., Lakshmi, V. S., and Deepthi, P. P. (2017). Image processing in encrypted domain for distributed storage in cloud. In *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET),* (pp. 1478–1482). IEEE.

[17] Lathey, A., and Atrey, P. K. (2015). Image enhancement in encrypted domain over cloud. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, 11(3), 38.

[18] Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 223–238). Springer, Berlin, Heidelberg.

[19] Ziad, M. T. I., Alanwar, A., Alzantot, M., and Srivastava, M. (2016). Cryptoimg: Privacy preserving processing over encrypted images. In *IEEE Conference on Communications and Network Security (CNS),* (pp. 570–575). IEEE.

[20] Hu, X., Zhang, W., Li, K., Hu, H., and Yu, N. (2016). Secure nonlocal denoising in outsourced images. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM),* 12(3), 40.

[21] Vaida, M. F., Todica, V., and Cremene, M. (2008). Service oriented architecture for medical image processing. *International Journal of Computer Assisted Radiology and Surgery,* 3(3–4), 363–369.

[22] Shen, C., Zhao, Y., and Chen, L. (2013). Galaxie: a P2P based EDSOA platform for cloud services. In *Proceedings Demo & Poster Track of ACM/IFIP/USENIX International Middleware Conference* (p. 9). ACM.

[23] Sadeghi, A. R., Schneider, T., and Wehrenberg, I. (2009). Efficient privacy-preserving face recognition. In *International Conference on Information Security and Cryptology* (pp. 229–244). Springer, Berlin, Heidelberg.

[24] Avidan, S. and Butman, M. (2006). Efficient Methods for Privacy Preserving Face Detection, in *NIPS'06: the 19th International Conference on Neural Information Processing Systems*, (Canada, 2006), 57–64.

[25] You, G., Hwang, S. and Jain, N. (2011). Scalable Load Balancing in Cluster Storage Systems. in Kon F., Kermarrec AM. eds. Middleware 2011. *Lecture Notes in Computer Science*, vol. 7049. Springer, Berlin, Heidelberg, 101–122.

[26] Wong, K.W. (2009). Image Encryption Using Chaotic Maps. in Kocarev L., Galias Z., Lian S. eds. Intelligent Computing Based on Chaos. Studies in Computational Intelligence, vol. 184. Springer, Berlin, Heidelberg, 333–354.

[27] Andre, P. (1999). Selectionist Relaxation: Genetic Algorithm Applied to Image Segmentation. *Image and Vision Computing*, vol. 17, 175–187.

[28] Goldberg, D. E. (1989). Genetic Algorithms in Search, Optimization and Machine Learning. Addison-Wesley, Massachusetts, USA.

[29] Yoshimura, M. and Oe, S. (1999). Evolutionary Segmentation of Texture using Genetic Algorithms Towards Automatic Decision of Optimum Number of Segmentation Areas. *Pattern Recognition*, 2041–2054.

[30] Wu, Y., Noonan, J. P. and Agaian, S. (2011). NPCR and UACI Randomness Tests for Image Encryption. Cyber Journals: Multidisciplinary Journals in Science and Technology, *Journal of Selected Areas in Telecommunications (JSAT)*, 31–38.

[31] Marwan, M., Kartit, A. and Ouahmane, H., Security in Cloud-Based Medical Image Processing: requirements and approaches. in *BDCA'17: the 2nd International Conference on Big Data, Cloud and Applications (BDCA'17)*. ACM, New York, NY, USA, Article 6, 6 pages.

[32] Marwan, M., A. Kartit and Ouahmane, H. (2016). A Secure Framework for Medical Image Storage Based on Multi-cloud. in *Proceeding of the International Conference on Cloud Computing Technologies and Applications*, CloudTech, 88–94.

[33] Guo, S. and Zou, C. (2017). An Improved Image Retrieval Method Based on Spark. *in ICCSN: 9th IEEE International Conference on Communication Software and Networks*, (Guangzhou, China, 2017), 1292–1296.

[34] Vemula, S. and Crick, C. (2015). Hadoop Image Processing Framework. in *Big Data Congress 2015, IEEE International Congress on Big Data*, (New York, NY, USA), 506–513.

[35] Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., and Zhang, X. (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information*, 8(2), 44–59.

[36] Zyskind, G., and Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *IEEE Security and Privacy Workshops (SPW),* (pp. 180–184). IEEE.

Biographies

Mbarek Marwan received the Engineer degree in 2002 at ENIM School, Rabat. Marwan has held senior management level positions in several IT projects. Since 2016 he is a predoctoral researcher in the Laboratory of Information Technology (LTI) at National School of Applied Sciences (ENSA), El Jadida, Morocco. His area of research covers security aspects in the cloud computing.

Ali Kartit is a Professor of computer science at ENSA, El Jadida. He received the PhD degree in computer science from the University Mohamed V Faculty of Science, Rabat in 2011. His main areas of interest lie in computer security and emerging technologies like cloud computing.

Hassan Ouahmane is a Professor of communications at ENSA, El Jadida. He received the PhD degree in communication from the University Moulay Ismail, Faculty of Science, Meknes–Morocco in July 2000. His main areas of interest lie in communications, signal analysis and computer science.