Improving the Security of Cloud-based Medical Image Storage

Mbarek Marwan*, Feda AlShahwan, Fatima Sifou, Ali Kartit and Hassan Ouahmane

Abstract—**The amount of digital records created on a daily basis in the health domain are expected to keep growing sharply. Surely, a medical image contains vital information used mainly to obtain early and accurate diagnosis and treatment. Moreover, the adoption of an electronic medical record system is the most effective method to increase collaboration among healthcare professionals in order to improve the quality of care and patient outcomes. Based on these considerations, sophisticated software and platforms are required to successfully store and process these digital records. In spite of the importance of this model, building and maintaining a local data center for hosting IT services would inevitably increase the cost of healthcare services. Fortunately, cloud computing has provided healthcare institutions with affordable and elastic services to overcome these obstacles. Indeed, this new paradigm allows healthcare organizations to take advantage of remote computational resources offered by an external party. In this respect, healthcare practitioners can access cloud services to store patients' data. These services are billed based on the actual usage of cloud resources. Nevertheless, the adoption of cloud storage in healthcare sector faces enormous challenges, particularly those related to security and privacy. Although there exist several solutions to secure data, they mostly rely on traditional cryptographic schemes, such as AES, RSA and DSA. However, these techniques are often time-consuming, and hence, not suitable for medical data. For this reason, the proposed mechanism utilizes Shamir's Secret Share (SSS) scheme to address the security problems in cloud storage. The choice of this approach is motivated by two main reasons. First, it does not usually require complex mathematical operations to encrypt data as compared to the other techniques. Second, it is an efficient solution for ensuring fault-tolerance in cloud computing. In this paper, we present the main concepts of our approach to properly handle data confidentiality in cloud storage. We then experimentally evaluate the proposed method to prove its correctness. The simulation results show that the proposed solution successfully reduces the security risks when storing medical data on remote cloud storage.**

Index Terms—**cloud computing, medical images, storage, security, secret share scheme**

I. Introduction

Imaging tools have revolutionized the practice of medicine thanks to the advancement in modern imaging technologies. Actually, they are commonly used to help professionals detect a variety of diseases at early stages. An important advantage of these solutions is that they maximize health problems anticipation and early diagnosis; thereby, improving the patient's medical care. In this respect, healthcare institutions generate huge digital data to meet the increasing demand for health services. Obviously, advanced software and hardware are required to better manage and analyze these digital records. However, despite the potential benefits, the deployment of sophisticated local storage systems and health information technology requires often colossal investments. Besides, healthcare organizations should hire technical staff to run and manage IT services internally. Fortunately, a new trend called cloud computing has emerged as one of the potential solutions for the health information technology to gain momentum and become fully operational. For instance, various terms and definitions of cloud computing have been proposed in the literature. In this regard, the definition provided by the US national institute of standards and technology (NIST) is the well-known and widely accepted among scientists. According to this institute, this paradigm seeks to assure ubiquitous connectivity and access to on-demand cloud services, which are managed by the IT department or an external third party [1]. Furthermore, these scalable services are evaluated in accordance with a set of expectations for services stated in the service level agreement (SLA). One of the advantages of this concept is that clients can use cost-effective and easily scalable IT solutions as a service instantaneously [2]. More specifically, cloud providers use dynamic resource provisioning (DRP) techniques to guarantee that the services offered to consumers are available only when needed. Besides, the implementation of this solution will help healthcare organizations meet the intrinsic goal of reducing costs since this has been the most distressful and concerning issue in integrating IT in the healthcare sector. More importantly, cloud providers are responsible for the security, maintenance, upgrade and license of cloud resources. In addition to the aforementioned tasks, cloud providers offer tailored service-level agreements (SLAs) according to the client's specific requirements. Unlike the traditional concept, cloud services allow consumers to be charged based on a pay-per-use business model to reduce the services costs. In light of these facts, some hospitals are taking notice of this new trend and have begun to rely on remote cloud services to manage health records. Consequently, the demand for cloud services has increased as more and more healthcare institutions are interested in adopting cloud computing. In this regard, the cloud-based medical image storage has become a promising technology and the greatest agent of information exchange in healthcare

Manuscript received April 1, 2018; revised October 11, 2018.

Mbarek Marwan (* Corresponding author) is with the Laboratory of Research in Information Technology (LTI), ENSA, University of Chouaïb Doukkali, El Jadida, Morocco. (e-mail: marwan.mbarek@gmail.com).

Feda AlShahwan is with the College of Technological Studies, Kuwait. (e-mail: a.alshahwan@paaet.edu.kw).

Fatima Sifou is with the Mohammed V University, Faculty of Science, Rabat, LRIT Laboratory, Morocco.

Ali Kartit and Hassan Ouahmane are with the University of Chouaïb Doukkali, El Jadida, ENSA, LTI Laboratory, Morocco.

domain. As a result, healthcare practitioners rely on the remote tools of storage systems to manage and safeguard patient's medical records. Despite the advantages of cloud storage, the migration to this model faces divers challenges. In this regard, security and privacy concerns remain one of the major obstacles that face a unanimous consensus as to the adoption of this approach. Taking all these considerations into account, it is mandatory first to explore the security risks and menaces related to this technology. Next, we need to highlight the security requirements. We can then propose a novel framework to secure medical image storage in the cloud computing, which would improve clinical outcomes.

Our article is organized as follows. In Section II, we discuss some existing cloud storage solutions. Section III lists and discusses security concerns in cloud storage. Privacy requirements are discussed in Section IV. Section V and VI elaborate on the proposed framework and techniques involved in data security. Section VII presents the results of implementation of the suggested encryption technique. In Section VIII, we analyze the security of our proposed method. We end this study in Section IX and X by concluding remarks and future work.

II. Related Work

There is a growing consensus that public cloud is an advanced and manageable tool to store and access digital records. However, a handful of factors may seriously impinge on the effectiveness of public cloud if they are overlooked in the implementation process, factors akin to security and privacy. After the emergence of cloud computing, several techniques were proposed to implement security policies and privacy mechanisms. The most important thing to consider when designing secure protocols is the safety of customers' data. A perfect way to protect sensitive data is to encrypt files locally before sending them to the cloud providers. In this respect, encryption techniques are the most widely used form of data protection in cloud computing environment. This section aims at presenting some existing frameworks that deal with the security of medical data in the cloud storage. Several studies have addressed the privacy and confidentiality issues in cloud computing. In [3], Andra et al. introduce a method based on steganography to hide medical records and to protect them against unauthorized use. The drawback of this method consists in its limitation in terms of embedding capacity. Another group of studies utilize encryption techniques as a method to prevent accidental data disclosure. As a matter of illustration, Waghmare et al. propose convergent encryption to perform deduplication in cloud environment [4]. This approach aims at minimizing the amount of data that needs to be stored and reducing costs. To this end, a cryptographic hash function is used to eliminate duplicate copies of repeating data. Even though the deduplication protects clients' data, it is often noted that this method has a negative impact on the quality of the reconstructed images. Kartit et al. [5] suggest the utilization of AES algorithm to secure cloud storage. Specifically, the input file is basically divided into many parts of the same size. In this model, all blocks are encrypted using AES algorithm to prevent accidental disclosure of private information. In this framework, the RSA algorithm is used to highly secure key exchanges among clients. Another technique, presented in [6], involves implementing a visual cryptographic technique to tackle the challenges of privacy-preserving issues inherent in cloud storage. One of the main objectives of this solution is the ability to store and access clients' data easily. In this respect, an essentially initial step in encrypting data is to convert the secret document from a plaintext format to an image file using Apache POI interface. During the first stage, this file is encrypted by the visual cryptographic method to guarantee that the data cannot be compromised. Furthermore, the proposed system provides better performance in comparison with AES and DES algorithms. To comply with data protection and privacy requirements, Kaur et al. [7] use a hybrid cryptosystem to encrypt sensitive data. One advantage of this technique, in addition to using visual cryptography (VC) techniques, is that it applies RSA algorithm to enforce data security when producing shares. Therefore, the authors use VC to transform the secret data into multiple shares before encrypting them again with the RSA algorithm. In doing so, it is hard for unauthorized users to gain access to remote clients' data. Alternatively, Vengadapurvaja et al. use homomorphic encryption [8]. This form of encryption generally allows simple computations on encrypted data. In this scheme, an image is converted into a matrix. Afterwards, they rely on homomorphic properties to generate the public and private keys. These encryption keys are designed to perform the encryption in order to maintain the data security in cloud storage. Due to the many computations it involves, this method is unfortunately often very computationally expensive. Authors in [9] propose a framework based on multi-cloud environment to store digital data remotely. To this aim, they use a segmentation approach to split the input image into many regions to prevent data disclosure. More importantly, the watermarking technique is used in order to verify the integrity of the outsourced clients' data. In order to deal with the data integrity, the digital signature and watermarking methods are used to detect any accidental change to outsourced clients' data. The framework developed by Padhmavathi et al. [10] use visual cryptography VC (2, 2) to secure the utilization of cloud storage services. In this case, they split an image into many shares to reduce security risks in the cloud storage. In this approach, they propose the watermarking method for embedding the created shares within a cover image to prevent unauthorized use and access to critical information. The key benefit of this approach is that it can reduce computational costs, and thereby enhancing the overall system performance.

To sum up, there are many techniques to manage a wide range of privacy and security risks that may impact clients' privacy when using cloud services. However, they are often too complex to use in practice, particularly when leveraging massive volumes of medical data. In the next section, we will present the security issues and privacy requirements in the healthcare domain, according to which the appropriate solution can be selected.

III. Security Issues In Cloud Storage

In general, cloud computing is considered to be one of the major advances in information technology (IT). It has fundamentally changed the way that healthcare institutions use and manage IT services. In fact, it offers dynamically flexible, scalable computational resources to the clients. Hence, it is a simple and effective way of outsourcing computation tasks and storage to an external third-party. To offer cost-efficient services, cloud providers rely on various technologies that include, but are not limited to, virtualization, parallel and distributed system (PDS) and web 2.0 so as to fulfil the requirements of the SLA contract [11]. This being the case, the utilization of these technologies is basically the source of many security vulnerabilities, risks and threats in cloud services, especially with respect to storage systems.

A. Virtualization

The primary aim of this technique is to share the same physical hardware. This typically implies creating different virtual versions from a single physical resource. This approach is very useful because it allows cloud providers to deploy various operating systems and applications on one physical server. Essentially, it is an efficient way to reduce infrastructure costs and improve system performance. In the same line, virtualization provides many mechanisms to enhance reliability and trust. Among these mechanisms are live migration, high scalability and fault-tolerance. Unfortunately, this technique poses serious security threats due to diverse types of vulnerabilities and problems, particularly regarding VM isolation, VM image sharing, VM escape incorrect, hypervisor intrusion and VM migration [12] [13]. In addition to these security concerns, the utilization of this technology would cause the deterioration of the performance of virtual machines (VMs) [14].

B. Data and Storage

In response to the growing demand for information technology, cloud providers use distributed systems. This offers the ability to distribute the tasks and data on multiple servers to improve efficiency and performance. However, in this type of systems, the users' confidential data usually reside on servers located in different data centers. That is why cloud architecture is commonly viewed as a primary source of various challenges that impinge directly on some of the key features like system availability, job scheduling, load balancing and resources provisioning. In addition to issues having to do with data location, the shift to cloud computing raises further security considerations and critical problems. In particular, multi-tenant environment, data recovery vulnerability, improper media sanitization and data backup are the major problems facing the successful implementation of cloud storage [15] 16].

C. Web Technology

To enable ubiquitous access, remote cloud services are accessible via the Internet through a web browse. That is why web technologies represent the foundation part of the cloud technologies. With these web interfaces, users are able to manage and access computational resources using thin or thick clients. Specifically, the application programming interfaces (APIs) are used to easily administer and gain access to cloud services. In this case, APIs allow users to rapidly create connections between an application-layer and remote cloud resources. However, despite the benefits of APIs and web applications, using this technology in cloud faces security problems as outlined in [17]. This is because of common web security vulnerabilities including SQL injection attack, cross-site scripting (XSS), cross-site request forgery (CSRF), HTML/URL injection problems and request encoding attacks, to name a few.

IV. Privacy Preserving Requirements

Using digital records in modern medicine has become increasingly important, particularly since it enables a rapid and effective diagnosis. Actually, the image data provide useful information to assist decision-making, and hence aid doctors to improve treatment. Based on these considerations, any accidental modification of digital contents can negatively affect the quality of clinical patient outcomes. Thus, we believe that it is vital to provide, in this section, a comprehensive taxonomy of the main privacy requirements regarding the storage of medical records in cloud computing. These parameters have been collected from diverse latest articles [18] [19] [20] [21].

A. Confidentiality

Confidentiality refers to the mechanisms that prevent inappropriate disclosure of confidential data. In other words, unauthorized users cannot reveal patient's medical information. In particular, data should be protected against internal and external threats as well as malicious intrusions in the cloud storage environment. To achieve this goal, healthcare professionals often encrypt their sensitive data before transmitting them to the cloud computing.

B. Integrity

Healthcare professionals use medical images for clinical decision-making. In light of this fact, it is mandatory that image data should remain intact during transmission or storage in the cloud computing. These challenges arise primarily because clients have less control over their data. In fact, data are stored on remote servers that belong to an external party. Hence, preserving health records integrity is becoming a major problem as clients do not have copies of all stored data. For this reason, many protocols are developed to delegate task of monitoring data integrity to an external entity called a trusted party auditor (TPA). However, adopting such an approach will require significant adjustments on the part of cloud providers.

C. Availability

Nowadays, imaging technology has a crucial role in various aspects of the diagnostic process and clinical decisions. Essentially, using these digital records would undoubtedly help healthcare organizations improve the quality of medical services and patient outcomes. Consequently, doctors should have immediate access to the cloud storage. Because of this, high-availability and reliability are essential prerequisites for clinical data management. For this reason, cloud providers rely on several techniques for maintaining cloud services availability. Techniques such as data replication and load balancing mechanisms are used to enhance reliability. There is still, however, certain malwares and different attacks that can negatively impact the system availability [22].

D. Data Ownership

Cloud computing relies on sharing resources among various consumers for offering cost-efficient services. In this case, cloud providers use often multi-tenancy and virtualization mechanisms for reorganizing allocation requests according to the client's needs. Although this approach reduces cloud costs, it faces several security challenges, particularly with regard to data ownership and data access rights. In the face of these challenges, different techniques are suggested to guarantee the ownership of health records. In this context, the watermarking techniques are the principal method used for determining the rightful owner, copyright protection and content authentication.

E. Authentication

This technique aims at confirming the identity of cloud consumers. In this respect, the system validates each client who would like to use cloud services and resources. Usually, the identity of the users is checked against their stored credentials using the authentication server before allowing them to access to cloud services. In the cloud computing environment, federated identity management systems based on single sign-on protocols are widely used for the identity management procedure. Simply put, it makes sure that only authenticated and authorized users have access to the remote storage system to comply with security policies.

F. Access Control

Access control is an important mechanism by means of which data are protected from unauthorized use and disclosure of confidential medical information. The main objective of this system is to deny, restrict or allow consumers access to remote services by means of a set of access policies. Essentially, it determines who can use specific cloud resources like systems, resources and applications. However, the implementation of this tool in cloud computing is still challenging. In fact, traditional access control schemes are usually not suitable to such environment since it is a distributed multi-domain system. For this reason, various models are suggested by researchers to address this issue. In this context, Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-Based Access Control model (RBAC) and Attribute-Based Access Control (ABAC) are the most popular existing models for the cloud environment [23].

G. Anonymization

In concomitance with law and regulations, the security of patients' health information is a top priority for consumers in the cloud storage. In reality, the name and social security number (SSN) of patients, which are commonly used to identify a specific person, are protected from accidental loss, unauthorized access, use and disclosure. More precisely, it is necessary to take some typical measures to ensure that cloud providers and unauthorized users are not able to link between medical records and corresponding owners. This can be accomplished by using pseudonym algorithms, such as K-anonymity, L-diversity and T-closeness. They are one of the popular methods that seek to maintain data anonymization in the cloud computing.

H. Collusion Resistant

The primary goal of this technique is to prevent entities that cooperate to perform some functions over medical data stored in the cloud. For this reason, cloud providers need to protect data against collusion attacks. To achieve this goal, cryptographic methods based on hash functions for privacy-preserving data mining are used. Alternatively, one can use protocols based on the homomorphic methods to achieve collusion-resistant in cloud storage.

I. Auditing Capability

Client's data faces security threats originating from both outside and inside the cloud. That is why consumers or a nominated third party need to record all events and actions occurred in cloud storage [24]. The main objective of this mechanism is to ensure that all activities are performed by authorized users and in compliance with data protection requirements. Moreover, this approach allows clients to evaluate and control the service-level agreement (SLA).

J. Computational Efficiency

Although cryptographic techniques protect data, they can also affect the system performance and reliability. Hence, the computational overhead must be optimized to reduce the execution time. In fact, doctors need an immediate and rapid access to patient's digital records. Under these conditions, the techniques used to maintain security in cloud storage must be efficient in terms of time complexity. To solve this problem, a distributed privacy-preserving data aggregation protocol has become widely used for image encryption to make a trade-off between security and ease of use.

V. Proposed Cloud Storage Architecture

As outlined above, using cloud services in the healthcare domain offers multi benefits not only for patients but also for healthcare professionals. However, as highlighted above, security and privacy concerns are the major obstacles to the common adoption of this new paradigm, especially in the healthcare domain. In this section, we design a framework to secure medical data in a cloud storage environment. More importantly, the proposal enables effective collaboration among healthcare professionals. From this perspective, we suggest an appropriate data protection method to ensure safe and reliable cloud services. The principal aim of this solution is to achieve an acceptable balance between the requirements of privacy and the system performance.

A. Motivation

Our proposed platform provides storage capabilities using cloud services. Primarily, it is meant to provide appropriate data security measures to enable the secure use of cloud storage. The proposed solution is also designed to promote collaboration across healthcare organizations by facilitating data sharing between the Consumer Hospital (CH) and the Produced Hospital (PH). In this case, PH is the entity that produces multiple medical images forms including X-rays, CT scans, MRI, ultrasound and more. In such a model, the cloud provider offers a wide range of services to store, access and share medical records. Additionally, this framework aims at outsourcing the backup and archive of medical images. However, despite its benefits, this concept still faces various security problems. To address this issue, we propose a framework that ensures the implementation of a secure cloud solution to store health records.

B. *Proposed Architecture*

Our goal is to propose a secure architecture of cloud storage to meet privacy-preserving needs. Firstly, we list and sum up medical image privacy requirements to keep the patient's information safe in the cloud. The priority level of each factor is presented in Table I.

TABLE I
PRIVACY REQUIREMENTS AND THEIR LEVEL OF IMPORTANCE

Requirement	Priority
Confidentiality	High
Integrity	High
Availability	High
Data ownership	High
Authentication	High
Anonymity	Medium
Collusion-resistant	Medium
Unlinkability	Medium
Access control	High
Auditing capability	Medium

Secondly, we compare and analyze different existing deployment models of the cloud computing and their corresponding strengths and weaknesses, as illustrated in Table II. Basically, they are collected from a rich body of literature [25] [26] [27].

TABLE II
A COMPARATIVE ANALYSIS OF CLOUD MODELS

Deployment models	Strengths	Weakness
Public	▪ Low cost. ▪ Scalability is simple and immediate. ▪ Low local resources requirement.	▪ Difficult to customize security policy. ▪ Legal and compliance issue due to a variety of regulations and standards. ▪ Pools and applications are shared among many different clients. ▪ There is no scalability within an instance.
Private	▪ More secure since security policy is dedicated to a single organization. ▪ Deeper compliance with legal issues.	▪ Higher cost. ▪ Less collaboration between organizations and users. ▪ Computational resource limitations. ▪ Require technical staff to manage on-premise private cloud.
Hybride	▪ It takes advantage of public and private cloud: low cost and high level security. Indeed, sensitive data are located in private cloud and less sensitive data in public cloud.	▪ Security issue due to multiple security policies. ▪ Difficulty of data exchange between private and public cloud due to lack of data exchange standard between different cloud providers. ▪ Difficulty of cost monitoring.
Community	▪ It is a good solution to easily exchange medical data and improve collaboration between organizations.	▪ Difficulty of key and identity management. ▪ Legal issue particularly when members of community are from different countries. ▪ Problem of interoperability and portability between different cloud providers and platforms.

Finally, we identify the appropriate, cost-effective architecture that fulfills privacy requirements of medical images. In this context, there is a spectrum of use cases according to the associated risks [28]. In fact, the value, sensitivity and criticality of data are the key factors that determine an efficient cloud implementation. Accordingly, the deployment models depend heavily on the sector of activity and security requirements, as shown in Fig. 1.

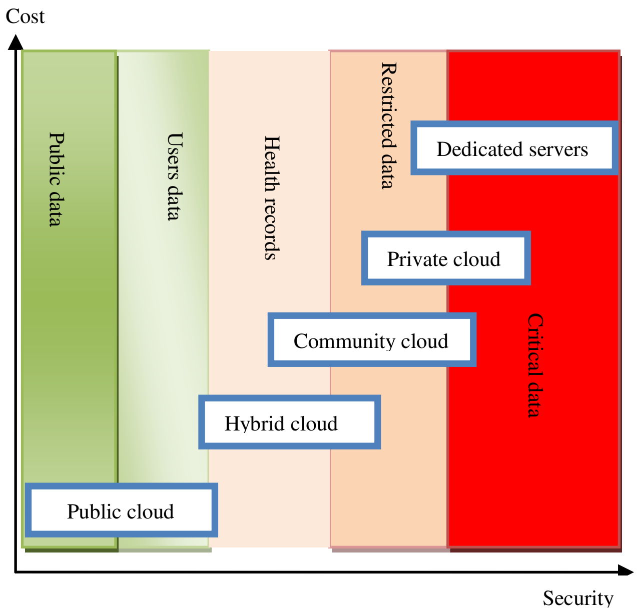


Fig. 1. The relation between cloud model and data criticality levels.

Indeed, manipulating public data, where security is not the main focus can be done on public cloud. Furthermore, private cloud is an obvious solution for sensitive data. However, high sensitive data and critical applications might never be deployed over the public cloud computing.

Under these conditions, we suggest a hybrid model composed of two entities. The first one is a trusted private cloud, while the second one is a public cloud. The primary objective is to enhance security while reducing costs.

C. *Proposed Framework*

As health records are sensitive data, they should be protected against unauthorized use, disclosure and access. Having this purpose in mind, we propose an architecture based on a hybrid model so as to minimize security risks associated with cloud storage as well as reducing the costs. Clearly, our proposal to solve the privacy issue involves a third party that offers security as a service and a hybrid cloud model. In doing so, critical applications must be stored in the private cloud. In the same vein, the public cloud resources are used as a service to save and archive health records remotely. Essentially, the trusted third party provides necessary security measures to protect data before transferring them to cloud storage. Furthermore, in line with the need for data protection and privacy, the communication and data exchange among all these modules are secured by using virtual private network (VPN).

In the proposed architecture, we focus on the separation of the cloud providers and healthcare orgnaizations by using an additional component. This provides more flexibility in extending security services and then offers a variety of security features and mechanisms such as authentication, authorization and encryption. Fig. 2 shows the three-level architecture of the proposed cloud system.

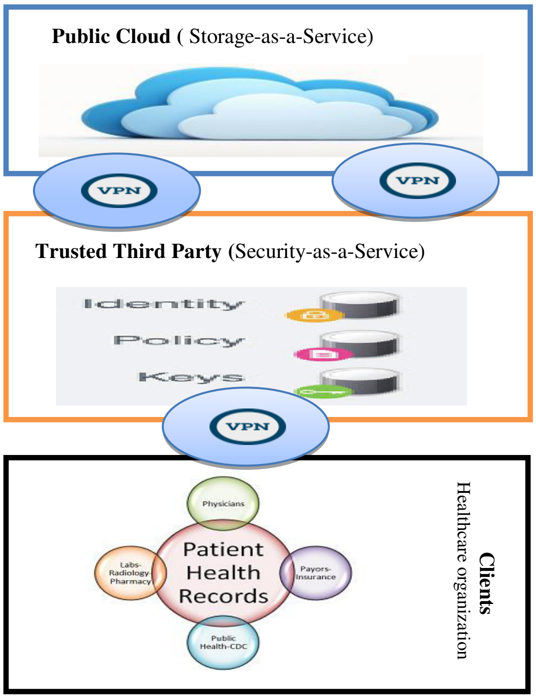


Fig. 2. A conceptual view of the three-level hierarchical architecture.

To summarize, our architecture is divided into four main components as Fig. 3 shows, namely PubServ, CloudSec, Gateway and DicServ.

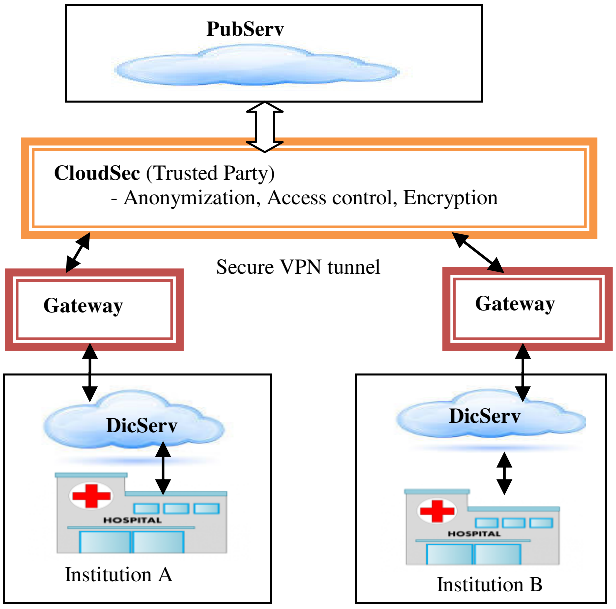


Fig. 3. General overview of the proposed architecture.

D. *Discussion*

The proposed architecture is a hybrid cloud, which is the combination of public cloud computing and an on-premise private cloud platform. These two infrastructures are separated from each other and communicate over an encrypted connection. With this architecture, healthcare organizations rely on private cloud to keep sensitive applications. The key advantage of this concept is its capacity to improve data privacy as well as reducing both latency and costs. In this case, the public cloud can be used as a computational platform for data processing and storage, and as a backup system of medical images as well. The public cloud is also an appropriate solution for the medical image exchange framework with other healthcare organizations. In fact, the use of an electronic medical record (EMR) system seems to be of utmost importance to allow a better patient's care and collaboration among different healthcare institutions. Basically, the security of medical data is strenthened through an additional module called CloudSec that provides security measures to avoid malicious data disclosure. Based on these constraints, the proposed architecture contains four main components: PubServ, CloudSec, Gateway and local DicServ. Using this solution would inevitably minimize security risks, threats and vulnerabilities associated with cloud storage environment. Here are the major components of the proposed framework and the functions of each.

DicServ

It is a local data center that stores a newly acquired medical image by any acquisition devices. The primary objective of this approach is to guarantee that only unneeded medical records or previously used are transmitted across the network to the public cloud. This aims at avoiding the transfer of large amount of data, which would undoubtedly help reduce the bandwidth usage. Accordingly, DicServ is used as a temporary storage space for immediate utilization. Concretely, it keeps images in a cache memory for a specified period of time, for example a month, before moving them into the public cloud. In addition, this local server stores encryption keys and deploys critical applications.

Gateway

It is the interface between private cloud and CloudSec. On the one hand, it is essentially responsible for securing communication and transferring of medical images according to DICOM standard, particularly DICOM queries (C-Store, C-Move and C-FIND). On the other hand, this entity coordinates with CloudSec to meet security and privacy requirements.

CloudSec

It is an important entity of our proposed framework. Indeed, it is a trusted third party that provides security as a service to the cloud consumers. This component is meant to ensure privacy and security of medical images in the cloud environment. In other words, it acts as a secure interface between healthcare organizations and cloud providers.

On the one hand, it relies on cryptographic encryption methods to maintain data privacy. In this case, we propose Shamir's Secret Sharing (SSS) scheme method to protect medical records in the cloud storage. On the other hand, the CloudSec offers other security mechanisms to meet privacy requirements, including auditing, anonymity and access control. The latter is designed to identify and decide who can gain access to a specific system, resources and applications. To this aim, a range of criteria are set in advance to comply with a security policy. As a result, this mechanism guarantees that only authorized users can access the cloud storage. For security reasons, the CloudSec module monitors and records all attempts made to access medical data. In this respect, we suggest attribute-based access control (ABAC) model to limit access to specific protected objects in the cloud storage. In fact, this scheme is capable of provisioning multi-level access delegation and on-demand attribute revocation [29]. To ensure effective compliance with data protection, we propose the K-anonymization algorithm to prevent disclosure of the patient's details [30] such as the name and the social security number (SSN). This paper focuses mainly on data confidentiality in the cloud storage system by implementing the SSS method. To sum up, the CloudSec module is responsible for managing data confidentiality and access control in the proposed framework, as shown in Fig. 4.

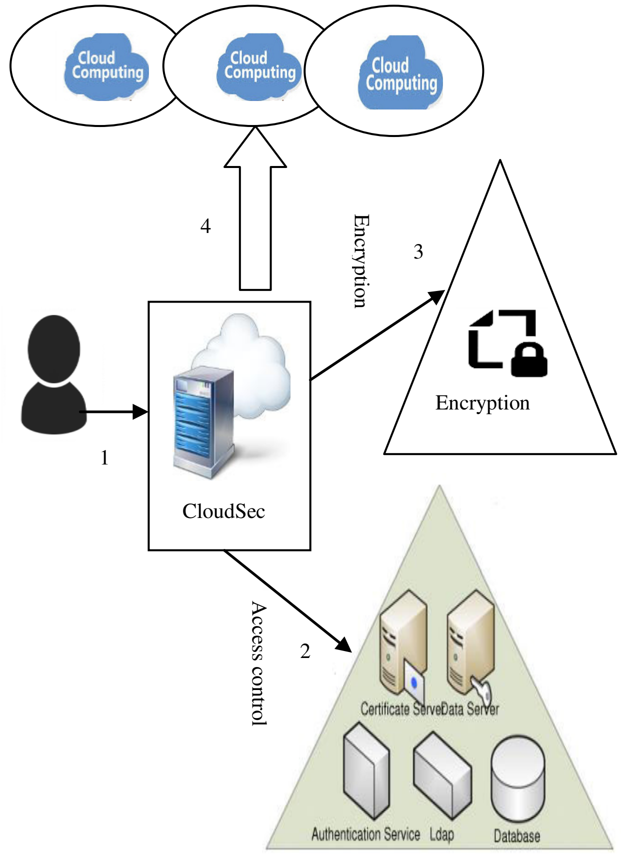


Fig. 4. The main functions of the CloudSec module.

In practice, CloudSec is designed to provide several functionalities. (1) It offers single sign-on to all cloud services. (2) It helps clients in choosing and configuring security services.

Since CloudSec is a single point of failure (SPOF), we suggest using the software-defined networking (SDN) paradigm in order to ensure high availability and failover. In SDN, the core architecture is divided into three components, namely infrastructure, control and application layers. The upper layer defines rules and offers different services, while the control plane is the main component responsible for monitoring all operations as well as managing network policies. The infrastructure layer comprises network elements such as physical/virtual switches, routers and access points [31]. The concept of management encompasses operations to support the infrastructure and ensure the security of SDN system. The following figure, Fig. 5, summarizes the basic architecture of a SDN framework.

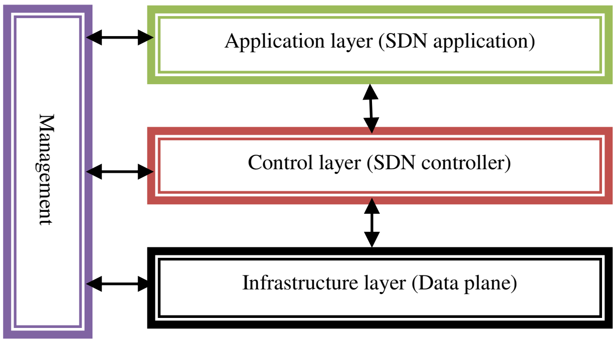

Management
Application layer (SDN application)
Control layer (SDN controller)
Infrastructure layer (Data plane)

Fig. 5. Basic SDN components.

PubServ

In general, this public cloud provides two main services, i.e., a log-term archive system and image processing as a service. In the proposed framework, PubServ is used as a backbone to secure data storage and as a backup of health records. The major advantage of this solution consists of the ability to offer scalable and efficient resources to save medical records and suitable disaster recovery solution. Besides, healthcare institutions can perform complex medical image processing on remote and high performance servers with sophisticate software. In this approach, medical images are transmitted into the PubServ module. The post-processing of these images will be returned to the client. In this study, we focus mainly on storage services. In this regard, clients rely on remote storage systems to manage and safeguard their medical records. However, despite the potential benefits of cloud storage, security and privacy are the major hurdles of this new concept. In this respect, we propose the SSS method to encrypt the stored medical images; thereby, protecting patient privacy against unauthorized users. To this aim, the CloudSec entity splits health records into several portions before uploading them to the PubServ system. Based on these considerations, we opt for distributed storage systems that spread data across multiple storage nodes. With a typical multi-cloud architecture, clients have the possibilty to save their medical data on several storage systems that belong to different cloud providers. The main purpose of this concept is to successfully address security and privacy concerns. Moreover, the proposal helps to reduce dependency on a single public cloud provider (vendor lock-in issue).

VI. Used Method For Data Confidentiality

As doctors currently rely on medical images in clinical practice, it is mandatory to protect these digital records against unauthorized access or modification. To achieve this goal, we suggest an approach to adequately preserve the confidentiality and availability of health records. The proposal is based on two solutions, i.e., Shamir's Secret Sharing (SSS) scheme and a multi-cloud architecture. Normally, implementing the SSS method offers also an effective fault-tolerance mechanism and hence provides highly available and reliable cloud services.

A. Shamir's Secret Sharing (SSS) Scheme

The primary objective of this method is to prevent a privacy breach from occurring in order to ensure a secure data sharing. From this perspective, Shamir, in 1979, proposed an algorithm to create several *n* shares from the secret data *s*, and then, store them in different locations to keep sensitive data safe. In this approach, only *m* subsets of these shares can reconstruct the secret using (*t, n*)-threshold schemes, where $1 < t \leq n$ [32]. To design and implement this model, we first convert the secret data *s* into a single number in finite fields. Second, we randomly select *t-1* independent coefficients $a_1, \dots, a_{t-1}$ and a large prime number *p*. We represent a perfect secret sharing scheme using the polynomial function f (x). This can be written as the following formula [33].

$$f(x) = (s + a_1 x^1 + a_2 x^2 + \dots + a_{t-1} x^{t-1}) \bmod (p) \qquad (1)$$

Finally, we evaluate the polynomial f (x) in *n* distinct points $x_1, \dots, x_n$, i.e., $y_i = f(x_i)$. Thus, each share $(x_i, f(x_i))$ is normally stored on a distinct virtual machine.

In such a scheme, in order to reconstruct the secret data, we basically apply Lagrange interpolation to any *t* or more than *t* shadows [34]. Hence, the function f (x) can be defined as in (2).

$$f(x) = \sum_{k=1}^{t} y_k \left[\prod_{i=1, i \neq k}^{t} \frac{x - x_i}{x_k - x_i} \right] \bmod (p) \qquad (2)$$

Based on (1), we get the secret data by evaluating f (x) in zero.

$$s = f(0) \qquad (3)$$

From (2) and (3), the secret data can be expressed as in (4).

$$s = \sum_{k=1}^{t} y_k \left[\prod_{i=1, i \neq k}^{t} \frac{-x_i}{x_k - x_i} \right] \bmod (p) \qquad (4)$$

To keep the secret data *s* safe and secure in cloud environment, we use Algorithm 1 to implement the SSS technique, especially (t, n)-threshold.

Algorithm 1. Create secret shares

```
Input: $n, t, s$, where $n$ is the number of participants, $t$ is the threshold, $t \leq n$ and $s$ is the secret data.
Output: < shares>
Initialize $p$ as a vector of size $t$.
Initialize shares as a vector of size $n$.
$p[1] \leftarrow s$
for $i \leftarrow 2$ to $t$ do
    $p[i] \leftarrow$ Random In (GF [$2^8$])
end for
for $i \leftarrow 1$ to $n$ do
    $y \leftarrow 0$
    for $j \leftarrow 1$ to $t$ do
        $y \leftarrow y + p[j].i^{j-1}$
    end for
    $shares[i] \leftarrow (i, y)$
end for
return < shares >
```

Similarly, to get the secret information *s*, we use only *t* shares along with the formula (4), as illustrated in the Algorithm 2.

Algorithm 2. Reconstruct the original image

```
Input: $share_i = (x_i, y_i)$, where $i = 1, \dots, t$ and $t$ is the threshold.
Output: < s >, where s is the secret image
$p \leftarrow interpol(share_1, \dots, share_t)$
//interpol is the Lagrange interpolation function //
$s \leftarrow p[1]$
return < s >
```

B. Multi-cloud Environment

As discussed above, implementing cloud storage to store sensitive data brings about many security concerns. In the light of this fact, the usage of this model in the healthcare domain needs the reinforcement of security measures. In this respect, the multi-cloud architecture is an efficient approach to handle security risks associated with outsourcing the storage of patients' medical records [35]. The key concept of this model is the storage of data on various storage media. In this case, one is not able to reconstruct the original data from a single share. Today, there are a variety of architectures of multi-cloud systems. In this context, the most widely used models are Byzantine Fault tolerance, DepSky, Redundant Array of Cloud Storage (RACS), High Availability and Integrity Layer (HAIL), and Intercloud Storage (IC Store). According to [36], DepSky model, which offers four virtual storage systems, is considered the most reliable model in the multi-cloud environment. This is achieved by using two algorithms: DEPSKY-A (Available DepSky) for system availability and DEPSKY-CA for data confidentiality. As illustrated in Fig. 6, the DepSky model employs a secret sharing scheme and erasure codes to store private data like health records [37]. Consequently, the architecture of DepSky is the most appropriate solution for ensuring proper data storage security, particularly with respect to availability, data protection, privacy and vendor lock-in. On this basis, we choose DepSky model as an adequate solution to meet security, privacy and compliance requirements. More importantly, this cloud storage model relies on four commercial clouds to provide unlimited online storage space. Another advantage is the utilization of an efficient fault–tolerance mechanism to establish a reliable and available distributed environment. This concept mainly allows healthcare organizations to successfully recover their data even in case of the failure of some storage nodes.

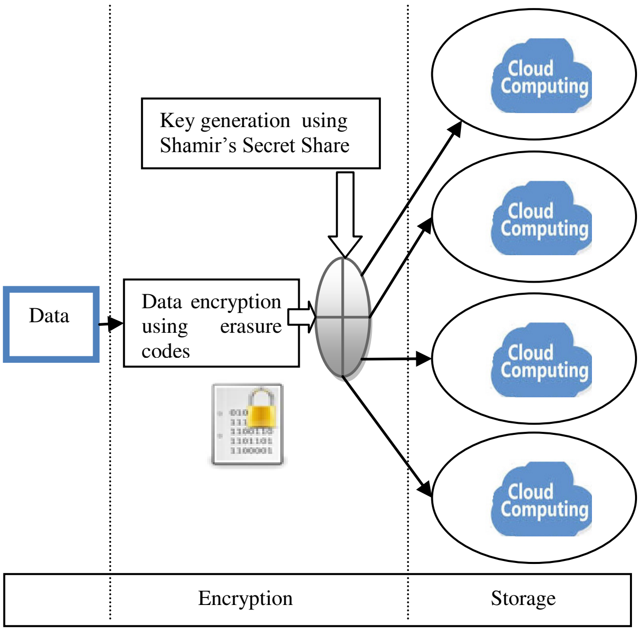


Fig. 6. The principle of DepSky architecture.

As for the reinforcement of data protection, the CloudSec module uses SSS method to transform the original secret image into many shares according to the (n, t)-threshold scheme. The obvious solution for preventing accidental data disclosure in cloud is to save data on different stoarge systems. To this aim, we distribute the share $s_i = (i, f(i))$ to the ith cloud provider. More importantly, we use the DepSky model to spread data across multiple storage nodes. Meanwhile, the secret image is recovered by combining at least *t* shares, as illustrated in Fig. 7.

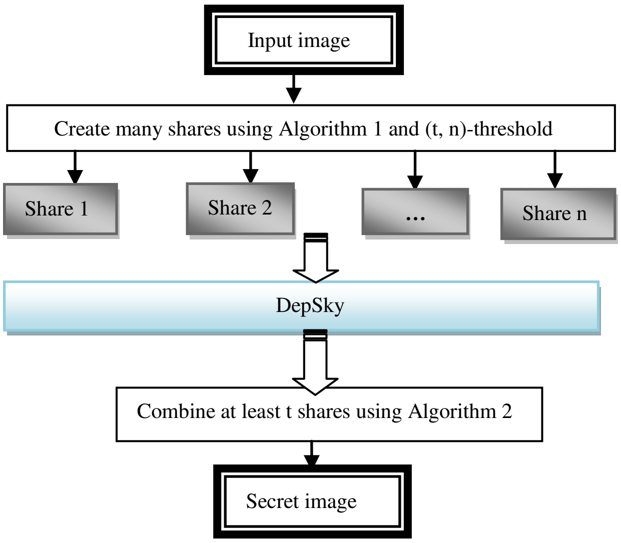

Input image
Create many shares using Algorithm 1 and (t, n)-threshold
Share 1
Share 2
...
Share n
DepSky
Combine at least t shares using Algorithm 2
Secret image

Fig. 7. The principle of image encryption using SSS method.

As mentioned before, the usage of DepSky architecture would improve the availability, confidentiality and integrity of clients' data. In contrast to conventional measurements, the present methodology is based on a combination of two simple concepts: distributed storage and secret sharing method. In this case, each cloud provider holds only a portion of the secret image to prevent disclosure of confidential medical information.

VII. Simulation Results

After formally presenting the proposed solution, we show how it can be used to protect health records in the cloud environment. To this aim, we apply Shamir's Secret Sharing (SSS) scheme to secure digital records. More specifically, we extend the standard model of SSS method to the real number field ℝ. For an image, the Shamir's (t, n)-threshold method is considered as a problem of computing the following equation in a linear algebra, as in (5).

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \dots & 2^{t-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & t & \dots & t^{t-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & n & \dots & n^{t-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \\ \vdots \\ y_n \end{pmatrix} \qquad (5)$$

At the same time, at least *t* participants can reconstruct the secret a_0 by solving a linear equation represented in (6).

$$\begin{pmatrix} 1 & i_1^1 & \cdots & i_1^{t-1} \\ 1 & i_2^1 & \dots & i_2^{t-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & i_t^1 & \dots & i_t^{t-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} y_{i_1} \\ y_{i_2} \\ \vdots \\ y_{i_t} \end{pmatrix} \qquad (6)$$

To demonstrate the feasibility of this solution, we apply the SSS technique, especially the method described in [38], to binary images.

In this case, we rely on (5) to create *n* shares (S_0, S_1, S_2,…, S_{n-1}). Thus, the secret image is split into *m* portions with *t* pixels. To this objective, we define the polynomial associated to each part *k*, as in (7).

$$s_k (x) = s_0 + s_1 x^1 + \ldots + s_{t-1} x^{t-1} \quad 1 \le k \le m \qquad (7)$$

In doing so, we obtain an array A_x with *m* values s_1 (x), s_2 (x),…, s_m (x). Consequently, we produce *n* shares by reshaping A_x into a matrix, where $1 \le x \le n$.

Similarly, we use (6) to reconstruct the original image. To this aim, we use an array X = {x_0, x_1…x_t} in order to store the value *x* of *t* shadow images. Precisely, we reshape *t* shares into an array that has *m* length. Afterwards, we use the value S_i (X_l) related to i-th element of a specific *l* array. In the following step we use *i-th* element of selected shares (S_i (X_0), S_i (X_1),…, S_i (X_{t-1}) to calculate value of the following coefficients: $\mathrm{s}_0^{\mathrm{i}}$, $\mathrm{s}_1^{\mathrm{i}}$,…, $\mathrm{s}_{t-1}^{\mathrm{i}}$. This is achieved by solving the linear equations, as defined in (8).

$$\begin{aligned} Si\,(X_0) &\equiv s_0^i + s_1^i X_0 + \ldots + s_{t-1}^i X_0^{t-1} (\text{mod } p) \\ S_i\,(X_1) &\equiv s_0^i + s_1^i X_1 + \ldots + s_{t-1}^i X_1^{t-1} (\text{mod } p) \\ &\;\;\vdots \\ S_i\,(X_{t-1}) &\equiv s_0^i + s_1^i X_{t-1} + \ldots + s_{t-1}^i X_{t-1}^{t-1} (\text{mod } p) \end{aligned} \qquad (8)$$

We repeat the same procedure for all arrays, and then, we reshape the intermediate image from m × t into the final image with H × W to get the secret image.

To illustrate the basic principles behind our proposed approach, we implement this technique in MATLAB version R2014a. More specifically, we rely on the (4, 8)-threshold scheme to generate the shares and distribute them to several cloud providers. In this simulation, we split the original image into 8 partitions to avoid the disclosure of confidential information. Obviously, this means that medical data are protected against cloud providers. In the same vein, CloudSec module needs to merge at least 4 shares to recover the secret image. As shown in Fig. 8, the simulation and experimental results illustrate the ability of the SSS method to safeguard sensitive data.

For more comprehensive evaluations of the proposed method, we choose six medical images that are downloaded from website [39], i.e., ultrasound.bin, mammogram.bin, xray.bin, ct_scan.bin, head.bin, and spine.bin. In this case, they are all 256 x 256 pixels and have grayscale values between 0 and 255. Hence, we choose p = 257 as the prime number. In this study, we apply the Shamir's (4, 8)-threshold to create 8 shares from the secret image. Accordingly, at least 4 image shares can be used to reconstruct the original image. The simulation results are depicted in Fig. 9, Fig. 10, Fig. 11, Fig. 12, Fig. 13 and Fig. 14.

As can be seen from simulation results, this technique is an adequate solution for preventing accidental data disclosure, as well as supporting distributed storage systems (DSS). The basic idea of this concept is to enable the storage of generated shadow images in various nodes to enhance privacy and security. As the DepSky model offers four storage devices, we store two shares in each node of the DepSky system.

To reconstruct the secret image, we need only four different shares according to the predefined threshold (4, 8). Note that in this case, we rely on (6) to get the secret image.

VIII. Security Analysis of the Proposed Method

Basically, the proposed technique is based on (n, t)-threshold and involves sharing a secret image among a set of *n* clouds in such a way that any group of *t-1* malicious cloud providers cannot reconstruct the secret image. In fact, the SSS method represents a theoretically secure information cryptosystem [40].

Theorem. In the (t, n)-threshold scheme, *t-1* or less shares do not leak out any information of the secret medical image.

Proof. Given t-1 shadow images (x_i, y_i), every potential candidate secret $s' \in \mathbb{Z}_p$ should corresponds to a unique polynomial f (.) of degree *t-1* that satisfies f (0) = s'. Based on the construction of these polynomials, there is an equal probability of Pr [$s = s'$] for all $s' \in \mathbb{Z}_p$.

In practice, there are multiple parameters to evaluate the degree of encryption quantity like Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), statistical analysis, correlation coefficient, histograms of encrypted images, etc. In this study, we rely on histograms to prove that the proposed solution ensures data protection against untrusted cloud providers. From Fig. 15 and Fig. 16, one can see that the histogram of different shares are fairly uniform and is significantly different from that of the original image. Consequently, the SSS method is perfectly secure and does not depend on the computational power of any cloud provider.

According to the implementation results, the proposed solution is an efficient method for protecting digital records in cloud storage. More precisely, unauthorized users cannot reveal any information about the secret image. At the same time, it ensures high fault-tolerance. This is because we can recover the original image even if we lose *n-m* shares.

IX. A Comparative Study

The attempt of protecting sensitive data in cloud computing environment has been done by using several techniques. In most cases, cloud providers rely on traditional cryptographic methods to prevent accidental data disclosure. In short, AES algorithm and deduplication techniques perform best on particular types of data like digital or textual. For that reason, new techniques are suggested to overcome these limitations. In this regard, visual cryptography (VC) offers the possibility to transform a secret image into multiple shares. An attractive alternative is to embed secret messages into a cover image by using steganography techniques. Although these techniques ensure data confidentiality and security, they have some limitations due to embedding capacity and visual quality degradation. A summary of the pros and cons of these well-known security techniques are provided in Table III. Accordingly, these techniques still need significant improvement to meet security requirements in cloud computing. In this respect, we propose a framework to enforce compliance with privacy policy in healthcare domain. Technically, the proposal is based on secret sharing scheme and multi-cloud architecture to support high availability, data confidentiality and anonymity. Furthermore, we use three-level architecture by introducing a trusted module that acts as a proxy. Essentially, this framework is designed to reduce security risks and provide a secure connection between clients and cloud services providers. Therefore, our proposed approach offers a greater degree of flexibility and increased security. Table IV presents a comparison between the existing methods and a new alternative framework.

Table IV
A comparison between different frameworks and approaches

Studies	Confidentiality	Fault-tolerant	Anonymity	Computational costs
[3]	Acceptable	No	No	Good
[4]	Good	No	No	Very Good
[5]	Very Good	No	No	Acceptable
[6]	Good	No	No	Very Good
[7]	Very Good	No	No	Acceptable
[8]	Very Good	No	No	Poor
[9]	Good	No	No	Good
[10]	Acceptable	No	No	Good
This work	Good	Yes	Yes	Good

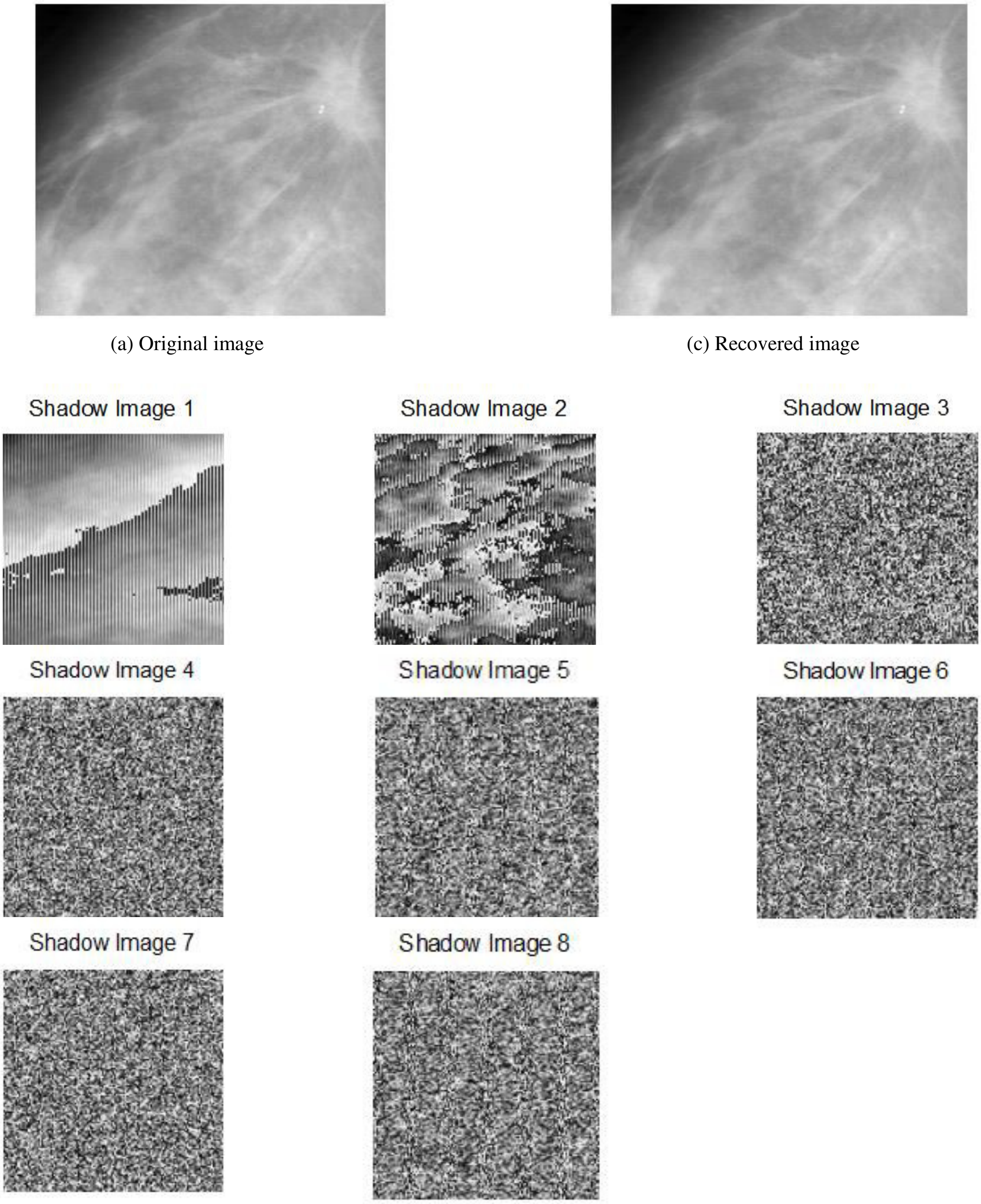
X. Conclusion

Recently, healthcare organizations have become aware of the benefits and risks of cloud computing. On the one hand, this approach allows consumers to store medical records on remote resources. Another advantage is that clients are charged only based on the actual usage of the storage space to achieve a significant cost reduction. Menwhile, cloud providers promise to deliver on-demand services that comply with service level agreements (SLAs), especially in terms of flexibility, efficiency, costs and security. On the other hand, the implemention of this new approach poses significant security and privacy concerns. This study discussed the essential factors affecting data privacy in the cloud storage. In the same line, security requirements and measures were outlined. The main contribution of this paper stands for a proposal that is intended to address some of the limitations inherent to cloud computing. The primary aim of the proposed framework is to meet essential security and privacy requirements. To achieve this goal, we rely on two fundamental elements i.e., secret share scheme and a typical multi-cloud architecture. The key idea behind this approach is to split a digital image into several portions in such a way that one cannot get any valuable information from a single share. From a data security perspective, we use the DepSky system as a distributed storage solution to save each share in a distinct cloud so as to prevent any accidental disclosure of medical information. Consequently, this framework would increase security and provide an efficient fault-tolerant mechanism for cloud storage. The implementation results prove that our solution is suitable for storing digital records in distributed storage environments.

As to the future work, we plan to use watermarking techniques to ensure ownership protection and check the integrity of medical images in the cloud environment. Moreover, we intend to implement ABAC model in order to enhance data protection in the proposed framework.

TABLE III
A COMPARATIVE STUDY OF VARIOUS SECURITY APPROACHES USED IN CLOUD COMPUTING

Technique	Advantages	Disadvantages
AES	AES has proven to be the most reliable way to safeguard privacy since it is secure against several attacks.	Since data are stored on remote servers, target-side deduplication is the appropriate option to secure cloud storage. Accordingly, the cloud provider is responsible for creating the keys that will be used to encrypt clients' data. Hence, data are not completely protected against untrusted cloud providers. Furthermore, AES was designed to be efficient in numerical and textual file. Hence, using AES for pixel-based encryption is time consuming and computationally expensive.
Homomorphic	The primary advantage of this form of encryption is the possibility to carry out basic arithmetic operations. Hence, it is an efficient way to ensure a secure outsourcing of computations to an untrusted cloud provider.	The main drawback of the homomorphic encryption is the high computational cost to encrypt and decrypt data.
Deduplication	This technique uses convergent encryption to handle confidential data securely. Moreover, it aims at reducing storage space. To this end, only one data copy is actually retained on storage media, while redundant data are replaced by a pointer. This would therfore eliminate duplicate copies of repeating data.	Usually, target-side deduplication is used to safeguard privacy and security when using cloud storage. Unfortunately, clients' data are not properly protected against an untrusted third party. In fact, cloud providers require key cryptography to perform the encryption.
Steganography	This technique aims at hiding digital data inside a cover-media like images in order to maintain the confidentiality of personal health information. One of the main benefits of steganography is its ability to produce data that are similar to ordinary files to avoid attracting attackers' attention. Additionally, the extraction of hidden data from cover-media is even easier.	The biggest challenge facing steganography techniques is to ensure both high embedding capacity and low degradation.
Visual cryptography	This method simply divides secret data into many shares without any mathematical calculations. In the same line, secret image can be reconstructed by stacking shares.	In most cases, the recovered image has significantly lower resolution than the original secret image. This method is only suitable when dealing with binary images.
Segmentation	This method is designed specifically to deal with images. In fact, this technique divides an image into multiple regions that have similar features.	This approach is computationally expensive in processing images, especially when dealing with large volumes of data.
The proposed approach	Basically, the SSS technique is a secure cryptosystem which provides a high level of security. In line with the objective of ensuring high availability (HA) for cloud storage, data are spread across multiple servers. By using three-level architecture, the proposed framework offers additional security services, such as anonymization, collusion-resistant and confidentiality.	This architecture requires many distinct cloud storages to avoid a data loss situation.



(a) Original image

(c) Recovered image

(b) Created shares

Fig. 8. The SSS method applied to mammogram image: a) original binary image; b) the generated shares; c) the recovered image.

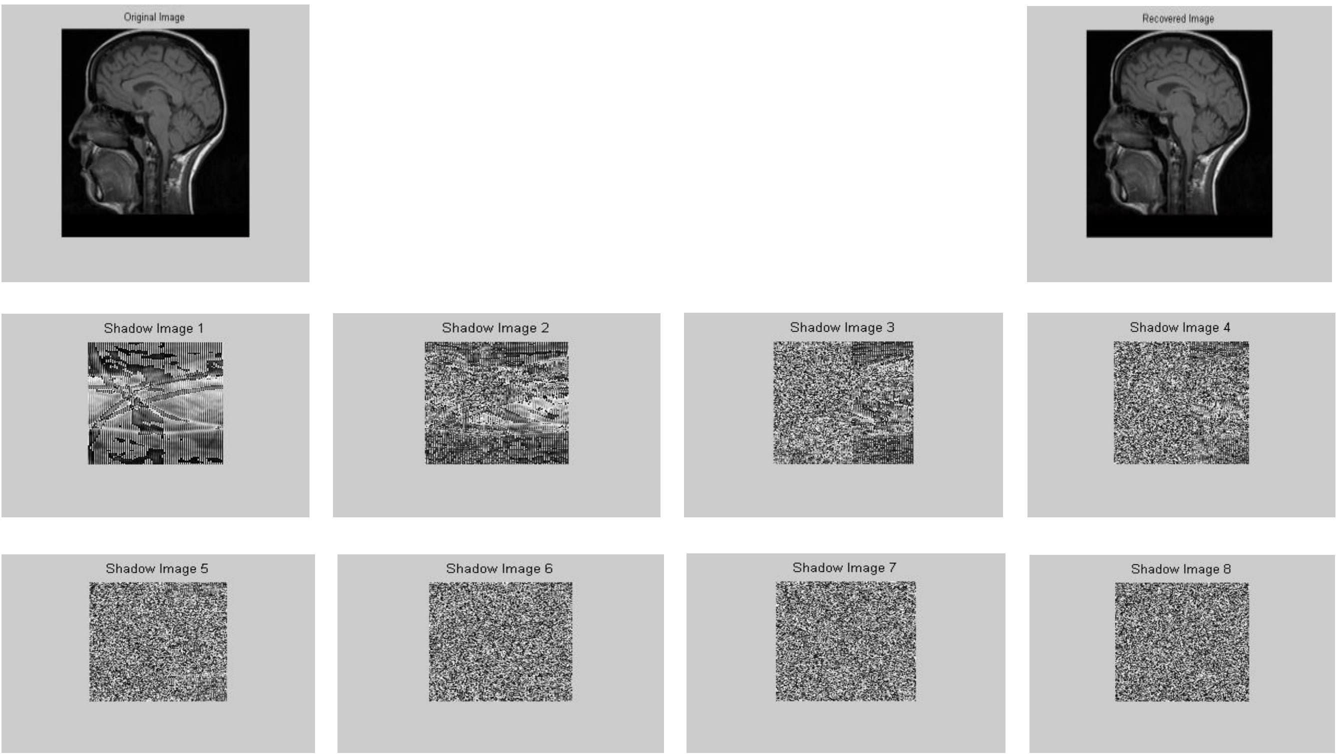


Fig. 9. The output results of applying the (4, 8)-threshold on the image “Head.bin”.

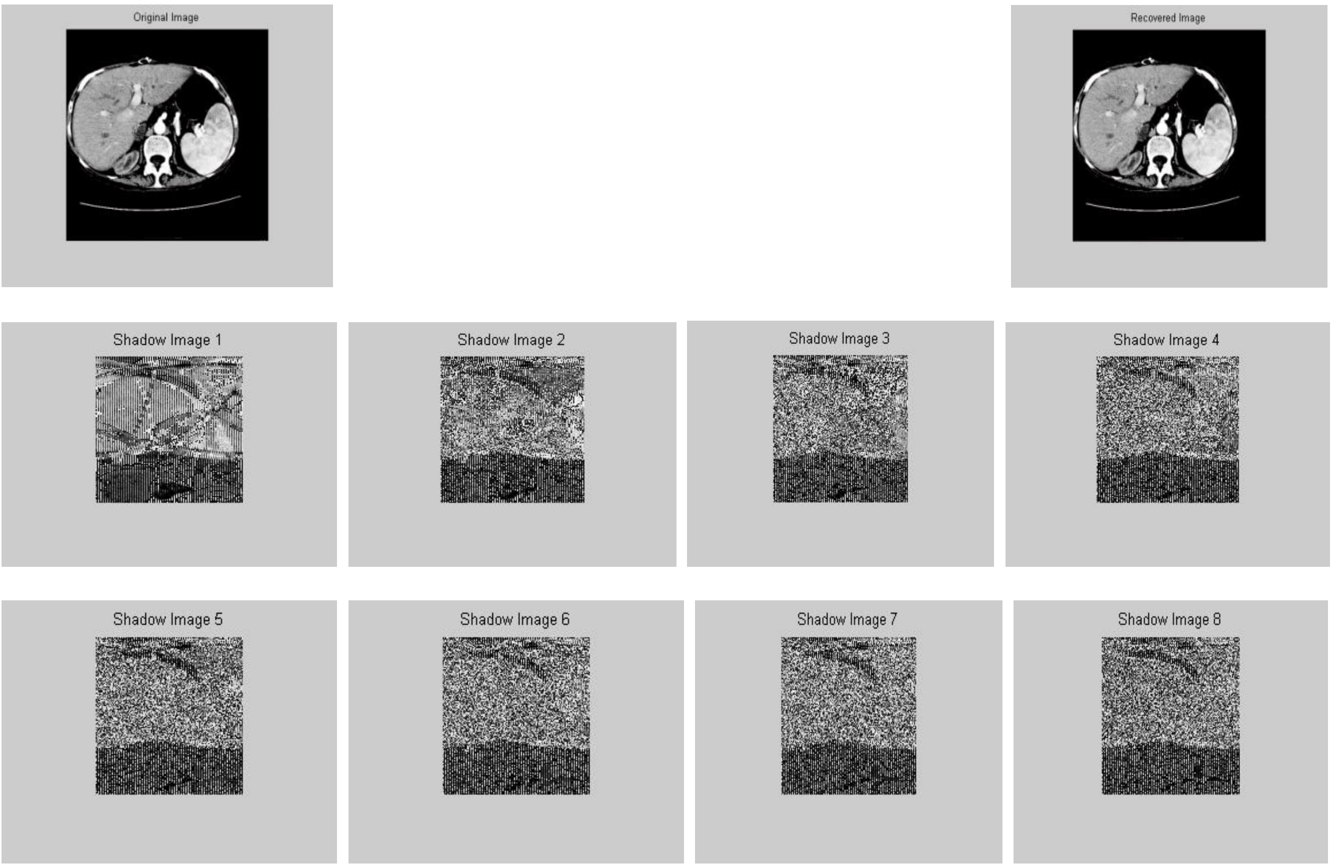


Fig. 10. The output results of applying the (4, 8)-threshold on the image “Ct_scan.bin”.

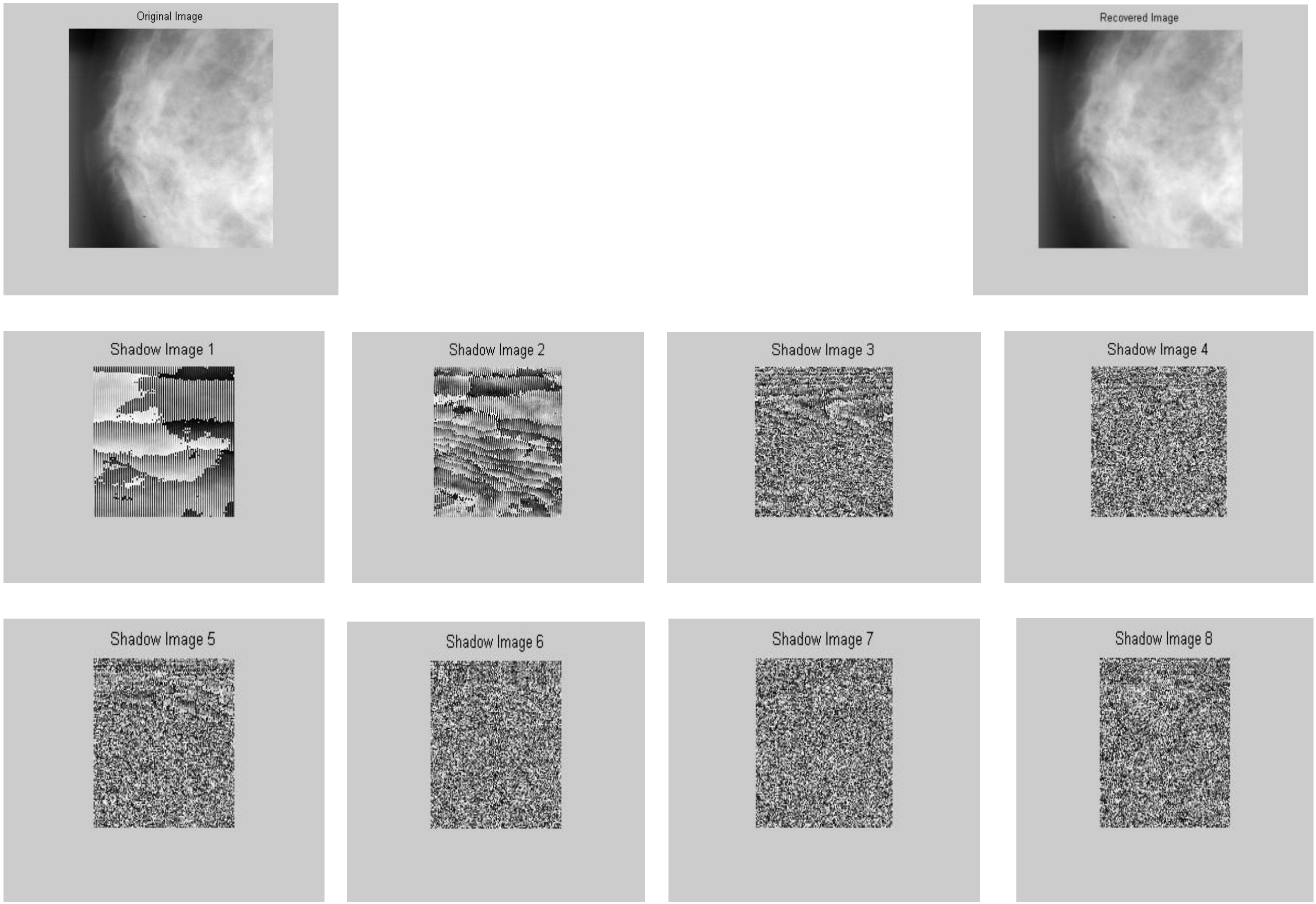


Fig. 11. The output results of applying the (4, 8)-threshold on image "Mammogram.bin".

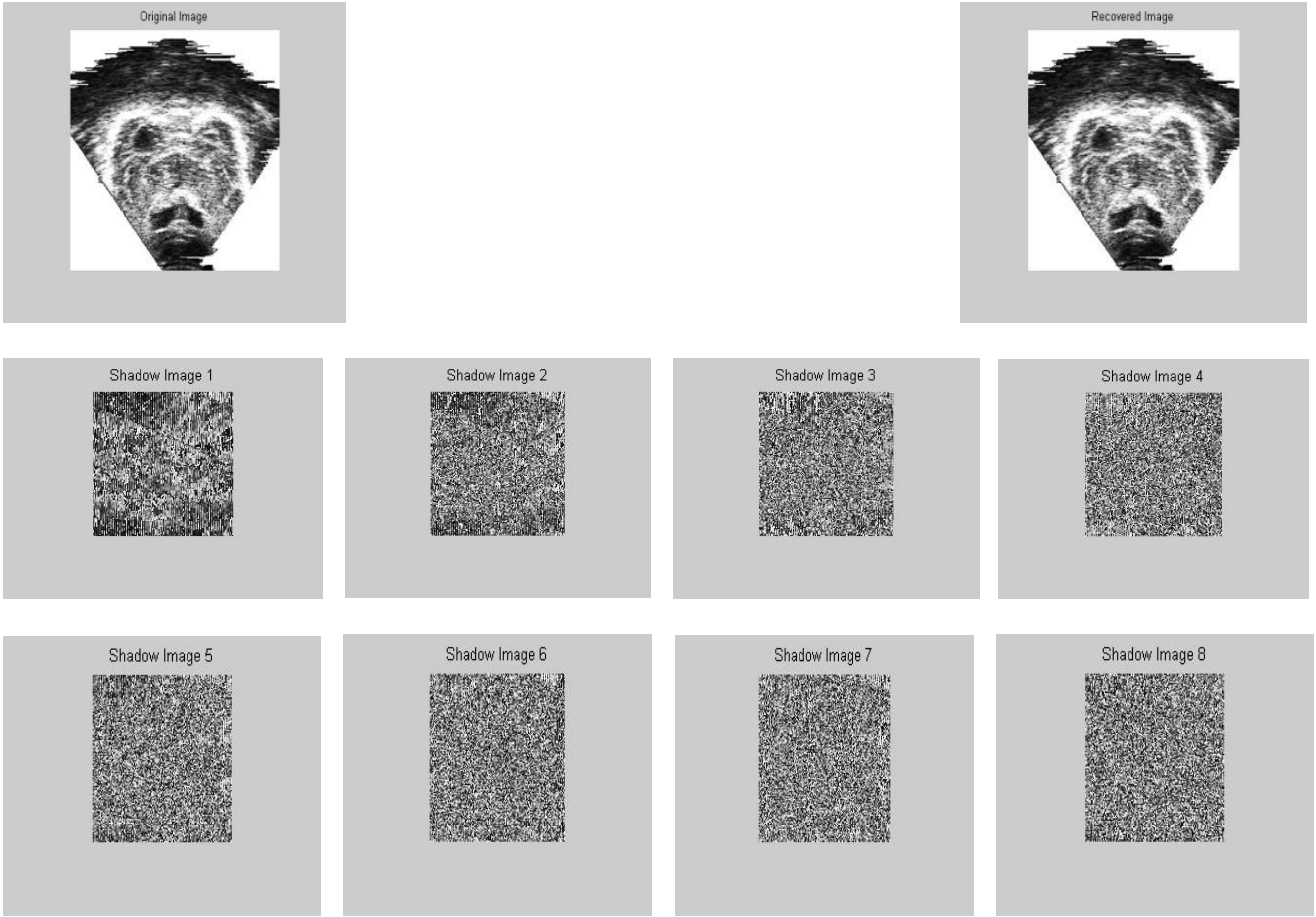


Fig. 12. The output results of applying the (4, 8)-threshold on the image "Ultrasound.bin".

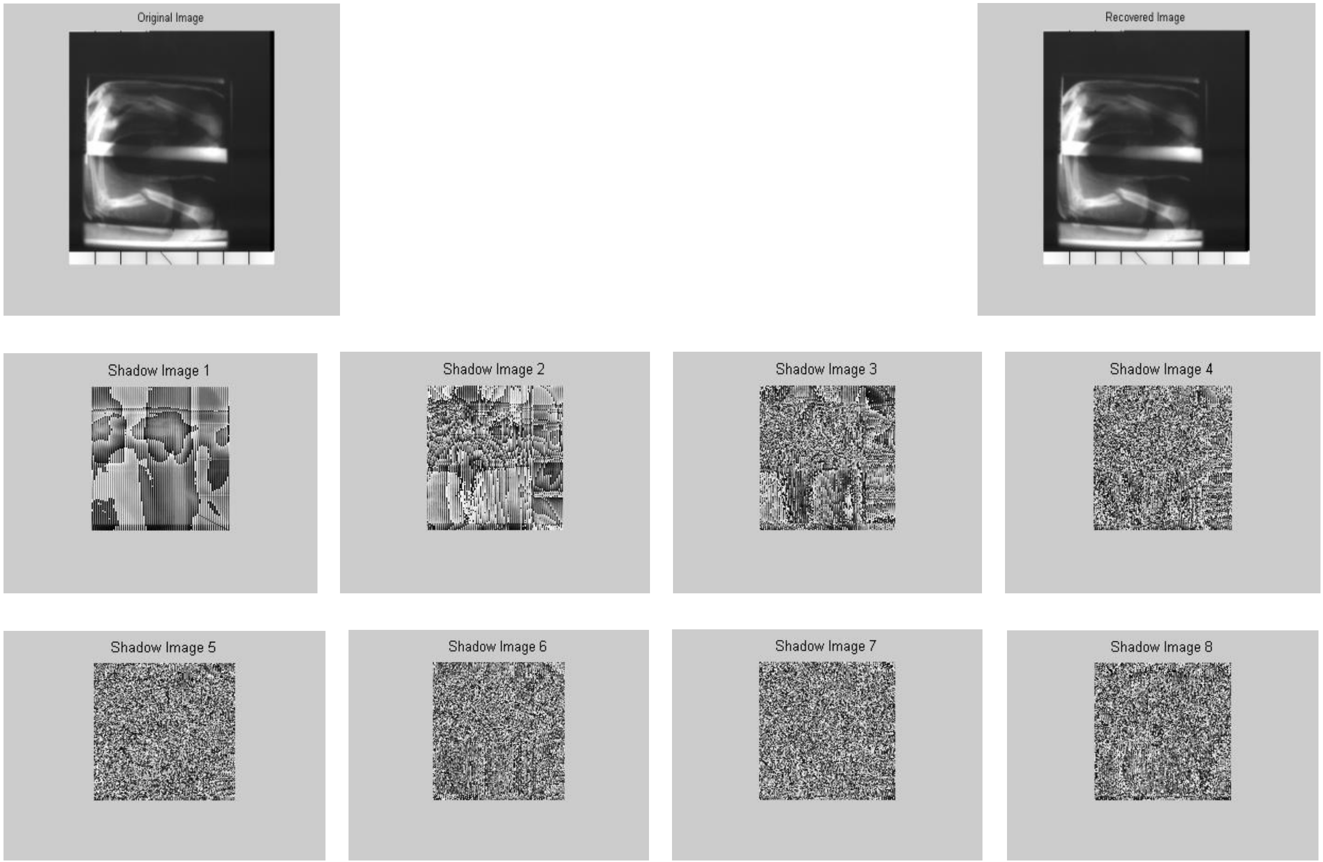


Fig. 13. The output results of applying the (4, 8)-threshold on the image “Xray.bin”.

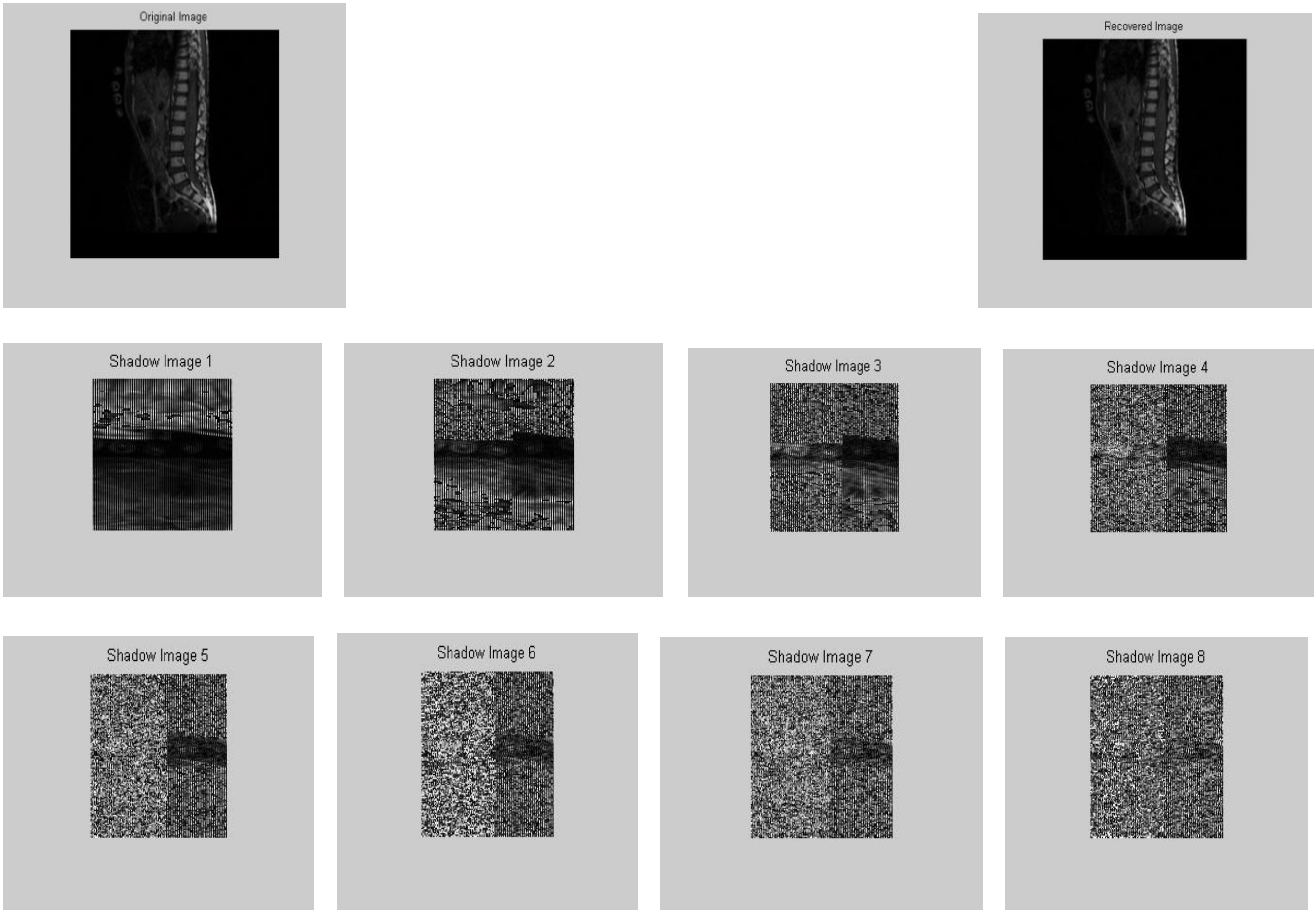


Fig. 14. The output results of applying the (4, 8)-threshold on the image “Spine.bin”.

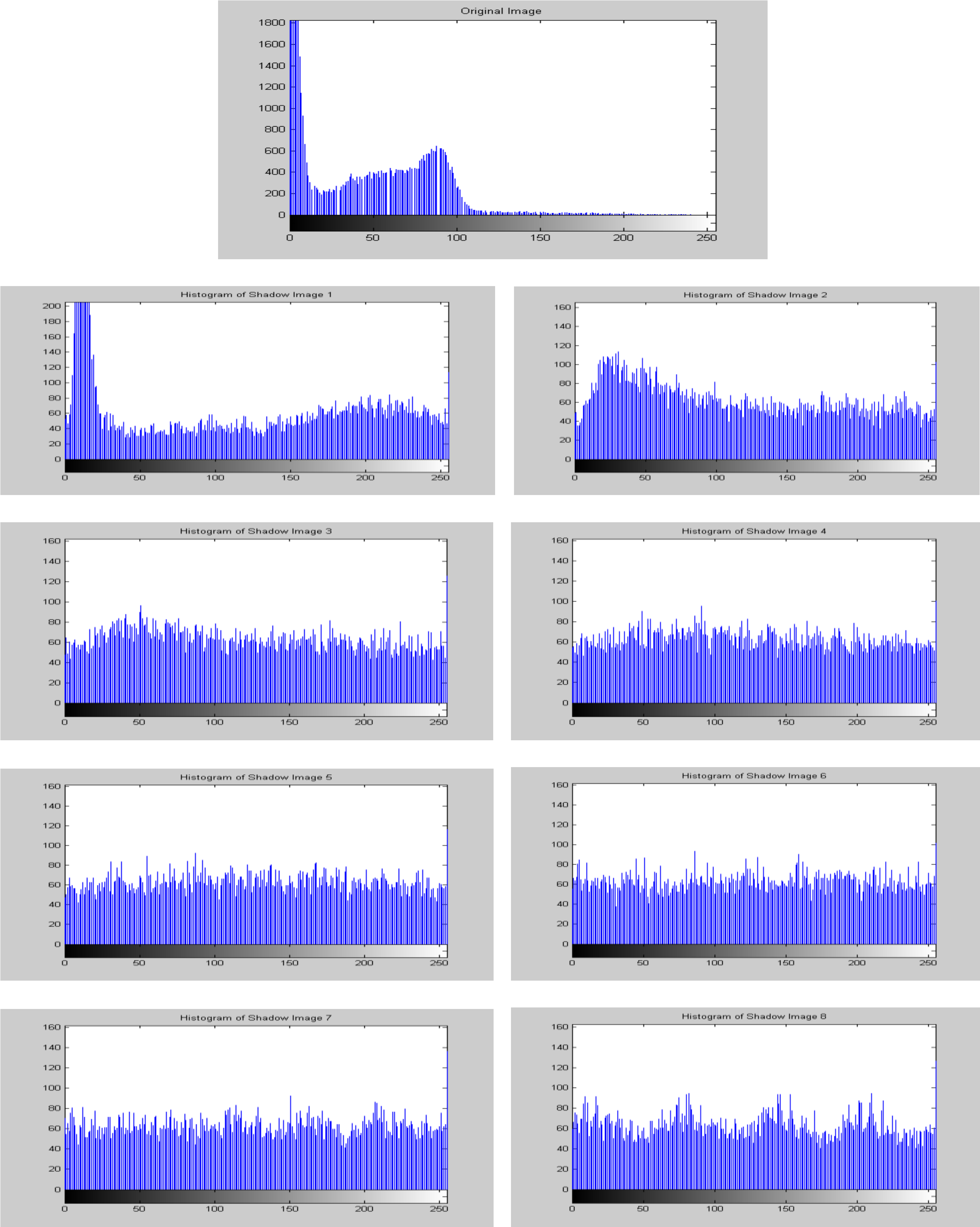


Fig. 15. Histogram of the original image and different shares for the image “Head.bin”.

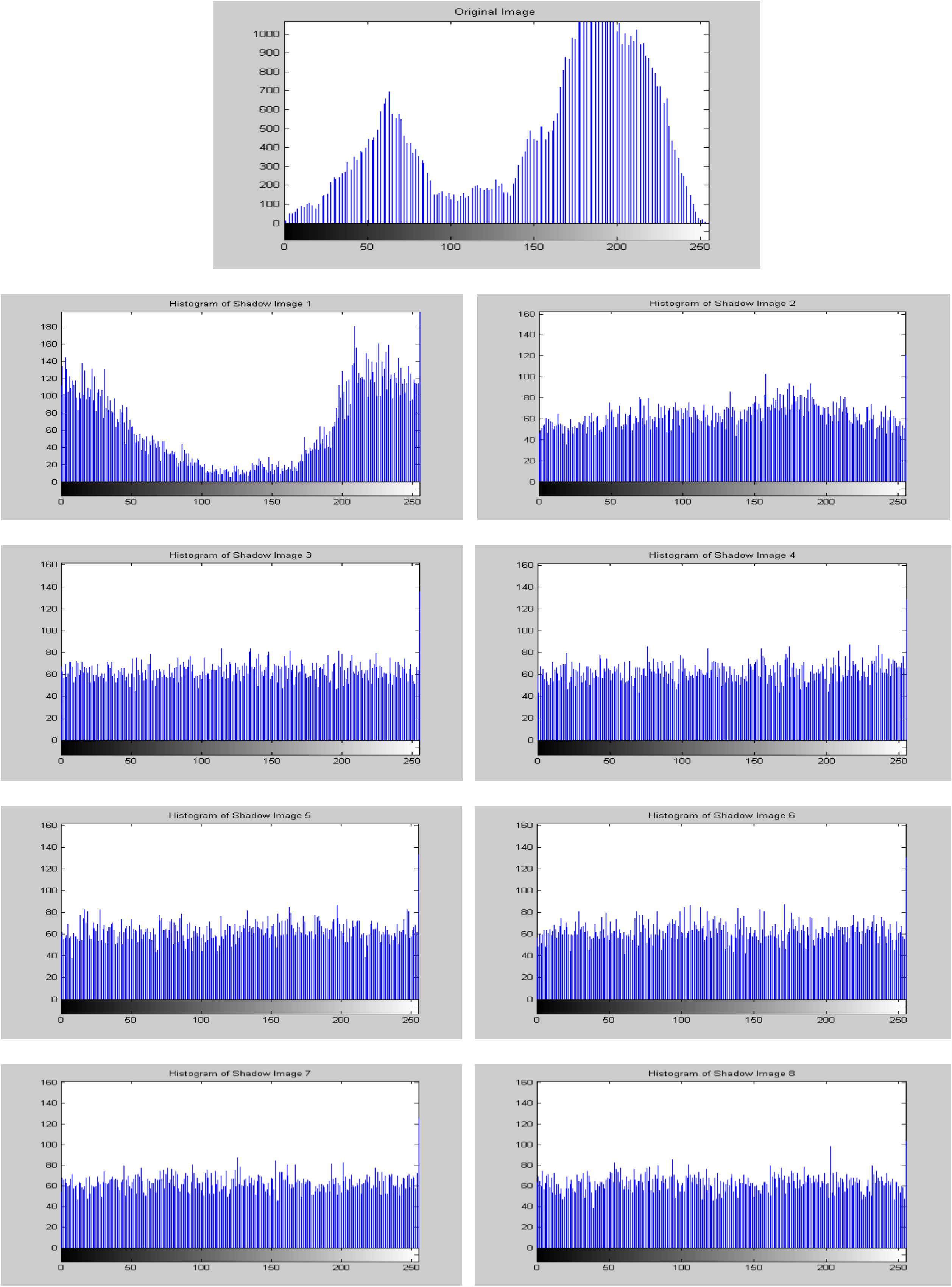


Fig. 16. Histogram of the original image and different shares for the image “Mammogram.bin”.

References

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

[2] M. Mohaupt and A. Hilbert, "Integration of Information Systems in Cloud Computing for Establishing a Long-term Profitable Customer Portfolio," *IAENG International Journal of Computer Science*, vol. 40, no. 2, pp. 124–133, 2013.

[3] M. B. Andra, T. Ahmad and T. Usagawa, "Medical Record Protection with Improved GRDE Data Hiding Method on Audio Files," *Engineering Letters*, vol. 25, no. 2, pp.112–124, 2017.

[4] V. Waghmare and S. Kapse, "Authorized Deduplication: An Approach for Secure Cloud Environment," *Procedia Computer Science, Elsevier*, vol. 78, pp. 815–823, 2016.

[5] Z. Kartit and M. El Marraki, "Applying Encryption Algorithm to Enhance Data Security in Cloud Storage," *Engineering Letters*, vol. 23, no. 4, pp. 277–282, 2015.

[6] K. Brindha and N. Jeyanthi, "Secured Document Sharing Using Visual Cryptography in Cloud Data Storage," *Cybernetics and Information Technologie,* vol. 15, no. 4, pp. 111–123, 2015.

[7] K. Kaur and V. Khemchandani, "Securing Visual Cryptographic Shares Using Public Key Encryption," *in Proc. of the IEEE International Conference on Advance Computing Conference (IACC),* 22-23 February, 2013, Ghaziabad, India, pp. 1108–1113.

[8] A. M. Vengadapurvaja, G. Nisha, R. Aarthy and N. Sasikaladevi, "An Efficient Homomorphic Medical Image Encryption Algorithm for Cloud Storage Security," *Procedia Computer Science, Elsevier,* vol. 115, pp. 643–650, 2017.

[9] M. Marwan, A. Kartit and H. Ouahmane, "A Framework to Secure Medical Image Storage in Cloud Computing Environment," *Journal of Electronic Commerce in Organizations,* vol. 16, no. 1, pp. 1–16, 2018.

[10] B. Padhmavathi, P. Nirmal Kumar and M. A. Dorai Rangaswamy, "A Novel Scheme for Mutual Authentication and Cheating Prevention in Visual Cryptography Using Image Processing," *ACEEE International Journal of Signal & Image Processing,* vol. 1, no. 3, pp. 116–120, 2010.

[11] M. Marwan, A. Kartit and H. Ouahmane, "Secure Cloud-based Medical Image Storage Using Secret Share Scheme," *in Proc. of the International Conference on Multimedia Computing and Systems (ICMCS),* 29 Sept.-1 Oct., 2016, Marrakech, Morocco, pp. 366–371.

[12] A. Mazhar, S. U. Khan and A. V. Vasilakos, "Security in Cloud Computing: Opportunities and Challenges," *Information Sciences, Elsevier*, vol. 305, pp. 357–383, 2015.

[13] M. N. Birje, P. S. Challagidad, R. H. Goudar and M. T. Tapale, "Cloud Computing Review: Concepts, Technology, Challenges and Security," *International Journal of Cloud Computing*, vol. 6, no. 1, pp. 32–57, 2017.

[14] J. Wu and J. F. Li, "An Enhanced Real-Time Deferrable Server Scheduler for Xen Virtualization Systems," *IAENG International Journal of Computer Science*, vol. 45, no. 3, pp. 403–412, 2018.

[15] D. A. B. Fernandes, L. F. B., Soares, J. V. Gomes, M. M. Freire and P. R. M. Inácio, "Security Issues in Cloud Environments: A Survey," *International Journal of Information Security, Springer*, vol. 13, no. 2, pp. 113–170, 2013.

[16] S. Iqbal, M. L. M. Kiah, N. B. Anuar, B. Daghighi, A. W. A. Wahab and S. Khan, "Service Delivery Models of Cloud Computing: Security Issues and Open Challenges," *Security and Communication Networks*, vol. 9, no. 17, pp. 4726–4750, 2016.

[17] A. Singh and K. Chatterjee, "Cloud Security Issues and Challenges: A Survey," *Journal of Network and Computer Applications, Elsevier*, vol. 79, pp. 88–115, 2017.

[18] F. Shirazi, A. Seddighi and A. Iqbal, "Cloud Computing Security and Privacy: An Empirical Study," *Lecture Notes in Computer Science, vol. 10272, Springer, Cham: Proceedings of The International Conference on Human-Computer Interaction 2017, HCI 2017*, 9-14 July, 2017, Vancouver, Canada, pp. 534-549.

[19] P. Ravi Kumar, P. Herbert Raj and P. Jelciana, "Exploring Security Issues and Solutions in Cloud Computing Services: A Survey," *Cybernetics and Information Technologies*, vol. 17, no. 4, pp. 3–31, 2017.

[20] B. Yüksel, A. Küpçü and Ö. Özkasap, "Research Issues for Privacy and Security of Electronic Health Services," *Future Generation Computer Systems,* vol. 68, pp. 1–13, 2017.

[21] G. Ramachandra, M. Iftikhar and F. A. Khan, "A Comprehensive Survey on Security in Cloud Computing," *Procedia Computer Science, Elsevier*, vol. 110, pp. 465–472, 2017.

[22] C. Barron, H. Yu and J. Zhan, "Cloud Computing Security Case Studies and Research," *Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering 2013, WCE 2013,* 3-5 July, 2013, London, U.K., *pp. 1287–1291.*

[23] A. Majumder, S. Namasudra and S. Nath, "Taxonomy and Classification of Access Control Models for Cloud Environments," *in Continued Rise of the Cloud, Z. Mahmood, Ed.* London: Springer, 2014, pp. 23-53.

[24] H. S. G. Pussewalage and V. A. Oleshchuk, "Privacy Preserving Mechanisms for Enforcing Security and Privacy Requirements in E-Health Solutions," *International Journal of Information Management*, *Elsevier,* vol. 36, no. 6, pp. 1161–1173, 2016.

[25] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," *Journal of Network and Computer Applications,* vol. 34, no. 1, pp. 1–11, 2011.

[26] Y. Masuda, S. Shirasak, S. Yamamoto and T. Hardjono, "Architecture Board Practices in Adaptive Enterprise Architecture with Digital Platform: A Case of Global Healthcare Enterprise," *International Journal of Enterprise Information Systems*, vol. 14, no. 1, pp. 1–20, 2018.

[27] W. Sarada, B. Lakshmi Prasanna and V. Padmalatha, "A Comparative Study on Cloud Models and Services," *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET),* vol. 3, no. 10, pp. 3365–3370, 2014.

[28] S. E. Hussein and H. Arafat, "An Open Cloud Model for Expanding Healthcare Infrastructure," *International Journal of Advanced Computer Science and Applications,* vol. 4, no. 9, pp. 84–91, 2013.

[29] H. S. G. Pussewalage and V. A. Oleshchuk, "Attribute Based Access Control Scheme with Controlled Access Delegation for Collaborative E-health Environments," *Journal of Information Security and Applications*, *Elsevier*, vol. 37, pp. 50–64, 2017.

[30] G. Poulis, G. Loukides, S. Skiadopoulos and A. Gkoulalas-Divanis, "Anonymizing Datasets with Demographics and Diagnosis Codes in the Presence of Utility Constraints," *Journal of Biomedical Informatics, Elsevier*, vol. 65, pp. 76–96, 2017.

[31] K. Benzekki, A. El Fergougui and A. Elbelrhiti Elalaoui, "Software-Defined Networking (SDN): A Survey," *Security and Communication Networks, John Wiley & Sons*, vol. 9, no. 18, pp. 5803–5833, 2017.

[32] A. Shamir, "How to Share a Secret," *Communications of the ACM,* vol. 22, no. 11, pp. 612–613, 1979.

[33] C. C. Thien and J. C. Lin, "Secret Image Sharing," *Computers & Graphics,* vol. 26, no. 5, pp. 765–770, 2002.

[34] A. Cheraghi, "Sharing Several Secrets based on Lagranges Interpolation Formula and Cipher Feedback Mode," *International Journal of Nonlinear Analysis and Application,* vol. 5, no. 2, pp. 60–66, 2014.

[35] M. Marwan, A. Kartit and H. Ouahmane, "A Secure Framework for Medical Image Storage Based on Multi-cloud," *in Proc. of the International Conference on Cloud Computing Technologies and Applications (CloudTech)*, 24-26 May, 2016, Marrakech, Morocco, pp. 88–94.

[36] M. Tebaa and S. El Hajji, "From Single to Multi-clouds Computing Privacy and Fault Tolerance," *IERI Procedia, Elsevier,* vol. 10, pp. 112–118, 2014.

[37] A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: Dependable and Secure Storage in a Cloud-of-Clouds," *ACM Transactions on Storage (TOS),* vol. 9, no. 4, article 12, 2013.

[38] S. Wang (2016). *Distributed Storage Scheme based on Secret Sharing Schemes.* School of Electrical and Computer Engineering, University of Oklahoma, Tulsa, USA. Available: http://www.mathworks.com/matlabcentral/fileexchange/39630-distributed-storage-based-on-secret-sharing-schemes--d4s- [Accessible 04 Oct 2018].

[39] Medical Image Samples [Online]. Available: http://hotnsour.ou.edu/ftp/pub/ece5273/images/?C=D;O=A [Accessible 04 Oct 2018].

[40] A. Lathey and P. K. Atrey, "Image Enhancement in Encrypted Domain over Cloud," *ACM Transactions on Multimedia Computing, Communications and Applications,* vol. 11, no. 3, article 38, 2015.

Mbarek Marwan received the Engineer degree in 2002 at ENIM School, Rabat. He is an IAENG Member, and 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.

Feda AlShahwan is the chair of the second IEEE GCC SYP Congress. She is taking the role of an MD in the IEEE Kuwait section board committee. She is currently an Assistant Professor at the Electronic Engineering Department/Computer Section of the College of Technological Studies in the Public Authority for Applied Education & Training. She has diverse research interests in Mobile Web Services, IoT, cloud computing and their applications Born in Kuwait, obtained B.Sc., M.Sc. in Computer Engineer from Kuwait University 1992, 2004 respectively. She had got her Ph.D. in “Adaptive Service Provision and Execution in Mobile Environments” from Centre for Communications Systems Research in University of Surrey.

Fatima Sifou received the Bachelor's degree in Mathematics and Computer Sciences in 2009 and the Master degree in software development "software quality" in 2011, from the Faculty of Sciences. Since 2017 she is a predoctoral researcher in the department of computer sciences at Mohammed 5 University where she is pursuing a Ph.D. degree. Her main research interests are related to security and privacy in IoT and Cloud Computing.

Ali Kartit is a Professor of computer science at ENSA, El Jadida. He received the Ph.D. 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 Ph.D. 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.