International Journal of Multidisciplinary and Current Research ISSN: 2321-3124
Research Article Available at: http://ijmcr.com

Secure public cloud storage of medical data based on Watermarking and Encryption techniques

Aminzou[#*], Er-raha[#], Machkour[^], Afdel[^] and Idrissi Khamlichi[!]

[#]Laboratory of Energy Engineering, Material and System, ENSA of Agadir, Morocco.
[^]Laboratory of the Computing Systems and Vision, Faculty of Sciences Agadir, Morocco.
[!]Renewable Energies and Intelligent Systems Laboratory, UMBA University, ENSA Fes, Morocco

Accepted 07 May 2017, Available online 13 May 2017, **Vol.5 (May/June 2017 issue)**

Abstract

In the modern health service, more and more users outsource data to cloud storage servers, where only the authorized users can access it. However, this data is prone to be exposed to many attacks, in particular by the cloud provider's personnel with privileged access. In this paper, we focus on the medical images. To protect user's privacy and avoid illegal access to the comprehensive content of these images, we propose a framework using the content-based fragile watermarking and encryption techniques. The image's digital signature and the encrypted data of the patient are embedded into the image, which will be stored in the cloud.

Keywords: *Medical Data, Watermarking, AES, LSB, Cloud Computing.*

1. Introduction

Cloud computing is an important paradigm where resources are redistributed to enable development and delivery of cloud services.

Cloud provides Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Cloud is available at private, public, community and hybrid levels. The advantages of cloud computing include low cost, high storage, openness, graceful failure, convenience in control and environment sustainability.

The above-cited definition does not mention any security notion of the data stored in the cloud even being a brand-new definition. Therefore, we understand that the cloud lacks security.

In the existing outsourcing data storage schemes, data auditing methods are inconvenient in multimedia files (images, video, audio), because they increase the data sizes and the time to sign [1]. Digital watermarking technology can be used to deal with this problem. This technology hides watermark information in the digital media without affecting data utilization and reduces the communication and computation costs. So, the digital watermarking technology can provide a more efficient auditing method than other cryptographic protocols.

There are many works on outsourcing data storage schemes with digital watermarking. N. Singh and S. Singh [2] point out that collaboration of digital watermarking and cloud computing can significantly increase the robust of the system as well as the security of user's data. Boopathy and Sundaresan [3] propose a model of data storage and access process with digital watermarking technology in the cloud. Though they do not give concrete realization, they show the broad prospects of applying digital watermarking technology into the cloud environment.

In the healthcare domain, the security of medical data in the cloud is a major challenge. Medical data can be attacked by hackers or modified by malicious software or the cloud provider's personnel with privileged access, so we need to find new secure solutions for these data.

In our paper, we deal with the security of medical data in the cloud. We propose a mechanism based on digital watermarking technology to secure and audit them in the cloud environment. Our basic concept is to encrypt patient's data and embed them, with a signature of image's patient, into his LSB's bit plane. Then we send this watermarked image to the cloud service provider.

The remainder of this paper is structured as follows. Section 2 summarizes the related work. Section 3 presents the proposed scheme. Section 4 gives some experimental results. Section 5 gives the conclusions and describes directions for the future projects.

2. Related work

Ensure security of outsourced medical data is a fast growing research area. Many related schemes have been

*Corresponding author's ORCID ID: 0000-0000-0000-0000
DOI: https://doi.org/10.14741/ijmcr/v.5.3.8

developed these last years. The privacy and integrity of data in the cloud are the most concerns of data owners. The outsourcing data are encrypted in the data storage schemes, to preserve privacy and protect sensitive information.

Data auditing is used in outsourcing data storage schemes, to verify the data integrity, but all methods used have additional data to test the data integrity and are not suitable for multimedia data. Digital watermarking technology, as an efficient method for data auditing, can offset this deficiency.

Rabi Prasad Padhy *et al.*[4] have proposed a cloud-based model for developing the healthcare systems. In the proposed model, the authors present a cloud-based healthcare information system to store medical records of patients on the cloud. This allowed a secure environment with easy management of data privacy and security and also the applications and documents are accessible from anywhere in the world, facilitating group collaboration on documents and projects with the use of the cloud.

Fatma E. Z. A. Elgamal *et al.*[5] have introduced an efficient watermarking technique to secure the medical images over the cloud computing environment. In this paper, the authors implemented a scheme using a dynamic embedding/extraction process to exploit all the capacity of the original image to increase the visibility of the final watermarked medical image. A private shared key is also used to enhance the security needs. The authors discussed the experimental results which will secure medical images through its processing.

Wei PAN *et al.*[6] use partial encryption with reversible watermarking to secure medical images shared through a public cloud platform.

In our model, we combine watermark and encryption technologies. Patient's data are encrypted, embedded with the image's signature in the LSB bit plane and sent to the cloud server. Third Party Auditor (TPA) is required to extract the watermark from the watermarked image. A user decrypts the encrypted watermark information and visualizes the original image and patient's data.

3. The proposed model

To ensure confidentiality and integrity of images, we use the technique of watermarking where information of patient are embedded in the LSB bit plane of his medical image. Our system includes the following tasks:

- Separate the LSB bit plane of the image;
- Build the signature;
- Encrypt the patient's data;
- Integrate the signature and encrypted data in the LSB;
- Construct the watermarked image;
- Store the watermarked image in the cloud;
- Extract the watermark;
- Decrypt patient's data.

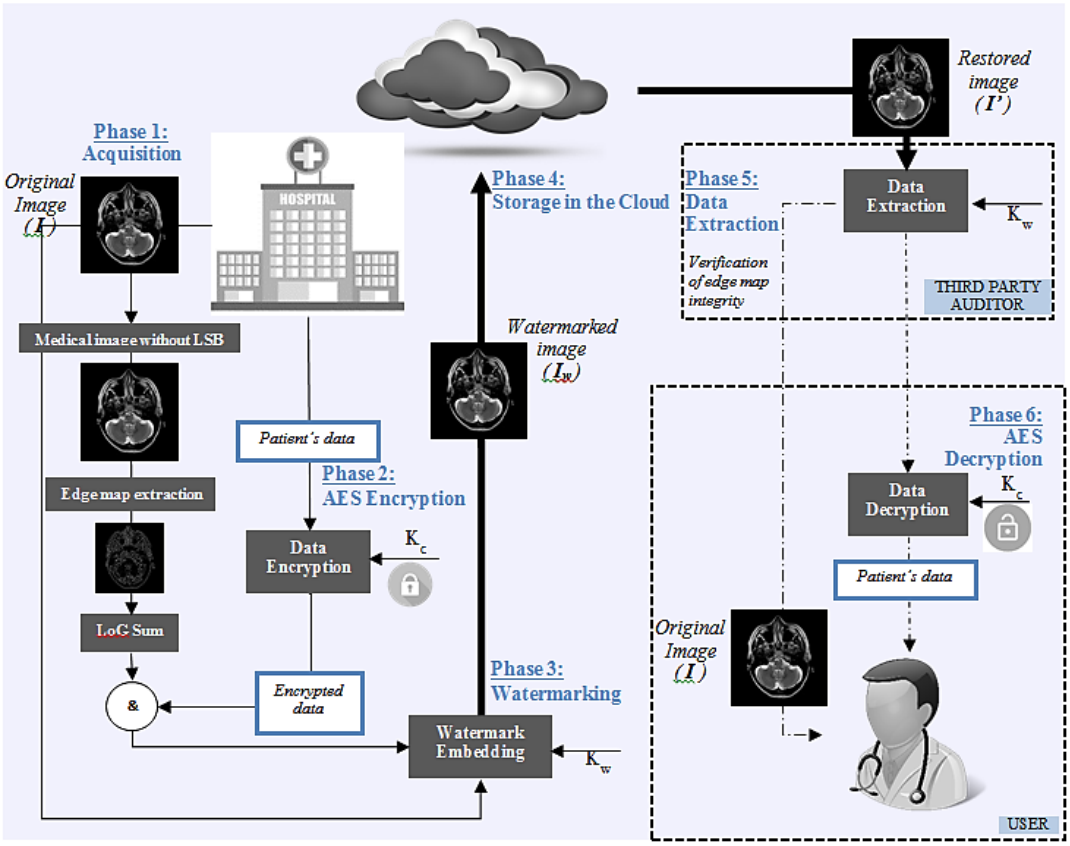

Figure 1: Sketch of the proposed scheme aiming to secure medical images outsourced in cloud

The process of achieving these functions is shown in Figure 1. The patient's information is entered and encrypted. To get the watermarked image, we integrate these encrypted data and our signature. This last is obtained using edge map of the image [7]. The watermarked image is then stored in the cloud.

The proposed model contains four modules: watermark creation, watermark embedding, watermark extraction, and data decryption.

3.1 Watermark creation

The watermark is composed of the signature of image's patient and his encrypted data.

We compute the signature by the sum edge map pixels of the original image. The edge map characterizes the image content uniquely. Any intentional or accidental modification of the image affects its map.

We obtain the edge map by applying the operator Laplacian of Gaussian (LoG) [8] on the original image without LSB bit plane. The logic of the use of the edge map is that any modification of the image will automatically imply an alteration of this map.

For data encryption, we use the symmetric Advanced Encryption Standard (AES) algorithm [9].

3.2 Watermark embedding

The image's signature and the encrypted patient's information are then placed in the LSBs bit plane of the image.

The data owner outsources the watermarked image I_w to the cloud. Then the watermark embedding key K_w is transferred to TPA and the decryption key K_c is shared with the authorized users.

3.3 Watermark extraction

TPA downloads the image I' from cloud service provider. Then, it extracts the watermarking information W', composed by digest and encrypted patient's data, and use the digest to verify the image integrity before the user can download the data from the cloud.

3.4 Data decryption

The authorized users can decrypt the patient's information using the decryption key K_c and can also visualize the original image I.

4. Experimental results

In this part, we present some experimental results. To study the performance of our scheme, we have used Matlab and three medical images of 8-bit gray level as the original image.

Figure 2 shows a Brain MRI image broken up into eight-bit planes starting with the least significant bit plane of the image and finishing by the most significant bit plane. The LSB bit plane of the image is the suitable plan to receive information of the patient.

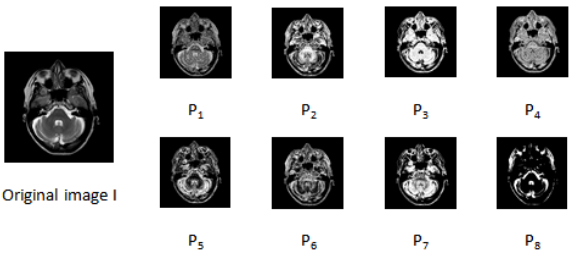

Figure 2: Rearranging Brain MRI image I and its eight bitplanes (P1, P2,… P8)

The encrypted patient's information and digest, representing the sum of edge map pixel obtained by LoG operator, are embedded in the first bit plane of the image.

We can evaluate the error between the original image **I** and the restored image **Î** by using the Mean Squared Error:

$$\mathrm{MSE} = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I(i,j) - \hat{I}(i,j)\right)^2,$$

the size of image I is M×N pixels.

Figure 3 lists MSEs and values of LoG sum for three medical images (I_1, I_2, and I_3). The MSE between the restored image and the original image is 0, meaning that restored image is obtained without error, during watermark extraction and data auditing process. The computation of the digest (LoG sum) from the restored images ensures that I_3 is attacked during the transmission, while both of I_1 and I_2 are not.

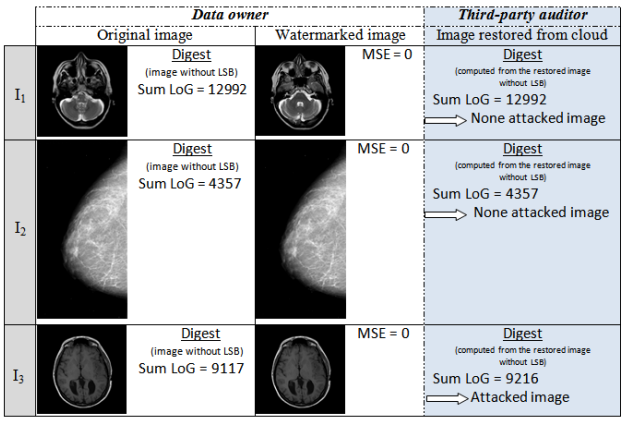

Figure 3: Original image, watermarked image and reconstructed image without the watermark

Conclusion and future work

In this paper, we propose a new solution using fragile watermarking and encryption techniques to secure the storage of medical images and patient's data in a cloud

environment. The presented method and architecture will be helpful for enhancing data security in public healthcare cloud. So, the proposed method will play a major role in the future.

References

[1] Xinyue Cao, Zhangjie Fu, and Xingming Sun (2016), A Privacy-Preserving Outsourcing Data Storage Scheme with Fragile Digital Watermarking-Based Data Auditing, Journal of Electrical and Computer Engineering, vol. 2016.

[2] N. Singh and S. Singh (2013), The amalgamation of digital watermarking & cloud watermarking for security enhancement in cloud computing, International Journal of Computer Science and Mobile Computing, vol. 2, no. 4, pp. 333–339.

[3] D. Boopathy and M. Sundaresan (2014), Data Encryption Framework Model with Watermark Security for Data Storage in Public Cloud Model, presented at the 8th International Conference on Computing for Sustainable Global Development New Delhi, India.

[4] Rabi Prasad Padhy, Manas Ranjan Patra, and Suresh Chandra Satapathy (2012), Design and Implementation of a Cloud based Rural Healthcare Information System Model, UNIASCIT, vol. 2, pp. 149-157.

[5] Fatma E.-Z. A. Elgamal, Noha A. Hikal, and F. E. Z. Abou-Chadi (2013), A Trust Management Scheme for Sharing Secure Medical Images over Cloud Computing Environment, Journal of Advances in Computer Network, vol. 1, no. 3, pp. 201-207.

[6] Wei PAN, Gouenou Coatrieux, Dalel Bouslimi, and Nicolas PRIGENT (2015), Secure Public Cloud Platform for Medical Images Sharing, *Studies in Health Technology and Informatics,* vol. 210, pp. 251-255.

[7] Y. I. Khamlichi, Y. Zaz, M. Machkour, and K. AFDEL (2006), Authentication Watermarked System for Content Based Medical Image, WSEAS Transactions on Signal Processing, vol. 2, no. 5, pp. 826-830.

[8] E. C. Hildreth (1983), The Detection of Intensity Changes by Computer and Biological Vision Systems, Computer Vision, Graphics, and Image Processing, vol. 22, no. 1, pp. 1-27.

[9] J. Daemen and V. Rijmen (1999), AES Proposal Rijndael, presented at the Networks (2nd ed.).