International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Provisioning of Compression and Secure Management Services for Healthcare Data in Cloud Computing

Suhasini Kalki[1], Jayashree Agarkhed[2]

[1]PG Student, Computer Science & Engg Department, P.D.A College of Engg, Kalaburagi, India

[2]Professor, Computer Science & Engg Department, P.D.A College of Engg, Kalaburagi, India

Abstract: ***Cloud computing is the use of computing resources that are delivered as a service over a network. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing encompasses three main concepts: pay-as-you-go, on-demand and on the Net. Several studies show that the lack of access to resources and shared data is one of the main causes of errors in the healthcare sector. Therefore in this work we propose a novel cloud based image compression technique using digital watermarking which enables embedding one image behind another. We also show that patient's information can also be stored along with the image without annotation which helps preserving the quality of the image. We further compare the proposed technique's performance for both medical and non medical images and prove that the method is more suitable for medical images due to gray scale nature of the image data.***

Keyword: SaaS cloud, Healthcare, Medical imaging, Lossless compression, Big Data.

1. Introduction

Cloud computing has recently emerged as a new platform for deploying, managing and provisioning large-scale services through an Internet based infrastructure. Cloud computing refers to both the applications delivered as services over the Internet, hardware and systems software in the data centers that provide those services The data centre hardware and software can be called as 'cloud'. When a cloud is made available in a 'pay-as-you-go' manner to the general public, it is a 'public cloud' and the service being sold is 'utility computing'. The term 'private cloud' refers to internal data centers of a business or other organizations which are not made available to the general public. Cloud computing has several benefits such as convenience of accessing the data from anywhere when connected to the internet, security by encrypting the outsourced data onto the cloud, backups the data when local computer crashes and collaboration so that the others can access, view, and modify documents, with permission. With the cloud, one can access to unlimited storage capability and scalability and it takes fewer resources to cloud compute, thus saving energy [1].

The digital images becoming increasingly important in healthcare environment, since they are more and more used in medical and medical related applications. Several different digital imaging technologies may simultaneously produce huge amount of data for each patient therefore, their management may be considered as an typical "big-data" problem. In particular, medical images can be very large in size they may not be suitable for devices with relatively limited display capabilities, storage, processing power as well as slow network access. For this reason the efficient transmission of such images, mainly in modern network-centric environments, requires complex network protocols, along with advanced compression and security techniques. In particular data compression is essential for efficient transmission and storage. At the same time, visual quality of such images is required to be high, in order to ensure correct and effective analysis resulting in correct diagnoses. In previous work they have not considered dynamic and adaptive compression for medical images and security issues regarding to those images in terms of encryption and decryption of images. In previous work they have considered the 'static cloud computing' environment, which is not able to evolve itself in response to the changes in both network topology and conditions. But here the authors have used the virtual cloud environment [2].

2. Related Work

Extensive works have been done by many researchers but existing problem of compression of image along with patient information and hiding of one image behind another image as well as security for the images are left open.

This Section mainly focuses on the literature review that has been carried out for the healthcare management. Several studies show that the lack of access to resources, that is some devices does not provides access to medical images and some provides only storage capacity to the medical images and other devices are provides processing of medical images. and shared data is one of the main causes of errors in the healthcare sector. The problem addressed in [3] is the inefficient usage of resources as well as the shared data in the field of healthcare. The medical images are processed using large number of devices and high network protocols due to complicated nature of medical images. Implementations of these medical images are based on advanced compression and security techniques. The authors have proposed a method for dynamic and adaptive compression of medical images and also for security used digital invisible watermarking procedure. The overall architecture uses Software as a Service (SaaS) in hybrid cloud environment. The result

contains heterogeneous hardware and software capabilities which are virtualized to the end users in the cloud system. The 3D medical images are securely managed using virtual infrastructure-less cloud solution system. The main advantage of this work includes scalability, adaptivity and data integrity issues. The different security methods endorsed are public-key cryptography, private-key cryptography and message authentication codes. The issue left open is they have considered only medical images not considered the embedding of patient information along with patient diseased images, so that the doctor may get confusion with the patient records. In [4] the author presented a 3D rendering approach using cloud computing system for the optimization of scalability and operational cost issues for different environments. The system architecture used is Microsoft Azure cloud platform which comprises of storage service for data storage and compute service for major computation issues. The 3D algorithm has been implemented using Graphics Processing Units (GPU) and Central Processing Units (CPU) computation services. The performance measures of the system is provided by the size of Virtual Machines for computation service. The dynamic optimization of system scalability as well as cost of cloud in distributed environment is considered in a network infrastructure. In [5] the authors proposed an data compression approach for 3D images to reduce the volume of images and their efficient storage along with relative transmission time through internet or any other ad-hoc systems like Picture Archiving and Communication System (PACS), teleradiology etc. Since these images are often stored in system vulnerable from the security point of view, because they contain sensitive data. The attack can be made by altering medical image and then may alter the relative diagnosis. The proposed solution is twofold: the first method is a low complexity approach is used for compression of 3D medical images and the second method is to insert invisible digital watermarks during the compression process. This is the hybrid approach that handles simultaneously and efficiently both compression and security to 3D images. In [6] the authors proposed an approach for lossless compression of continuous tone images, the context modeling is an extensively used parameter for the compression. The new techniques for context modeling of Differential Pulse Code Modulation (DPCM) errors are introduced that can exploit context dependent DPCM error structures for the benefit of compression. To reduce the context dilution, time and space complexities they have proposed techniques of forming and quantizing modeling contexts. This results the improved coding efficiency at low computational cost. In [7] the authors proposed a new low complexity algorithm for hyper spectral image compression, they have proposed two novel approaches to lossless coding of Airborne Visible/Infrared Imaging Spectrometer (AVIRIS) data. One is based on an inter band, linear predictor and the other is based on an inter band, least squares optimized predictor. Both algorithms are coupled to a simple entropy coder. In [8] the authors proposed a single-pass adaptive algorithm that uses context classification and multiple linear predictors and this is optimized on a pixel-by-pixel basis. The locality is also exploited in the entropy coding of the prediction error. The computational complexity can be substantially reduced without sacrificing the performance by using alternative methods for the optimization of predictors and also complexity is reduced by replacing the arithmetic coder with Golomb-Rice codes. In [9] the authors proposed a framework for the implementation of large-scale distributed data processing scheme for multiple clusters using MapReduce programming model. A MapReduce framework technique called as G-Hadoop for large-scale data computing among multiple clusters are used. The Gfarm file system method is used and MapReduce task model executes among multiple clusters in cloud. The G-Hadoop system makes use of parallel processing issues for considering large data sets using MapReduce technique. The G-Hadoop architecture consists of master/slave communication model using HDFS file system along with Gfarm file system for large datasets. In [10] the authors proposed a cloud monitoring approach for optimizing the Quality of Service (QoS) for the hosted applications. It involves dynamically tracking the QoS parameters to virtualized services such as the physical resources which they share and applications running on them. The monitoring techniques are used by the cloud provider or application developer in the following matters, Keeping the cloud services and hosted applications operating at peak efficiency. Detecting variations in service and application performance. Accounting the SLA violations of certain QoS parameters. Tracking of leave and join operations of cloud services due to failures and other dynamic configuration changes.

3. Proposed System

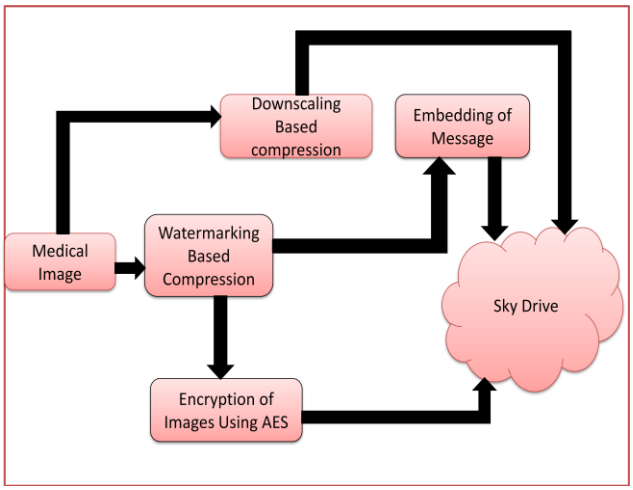

Figure 1: System Architecture of Healthcare management system

The Fig 1 depicts the overall architecture of proposed system, which consists of five different techniques namely watermarking based compression of the medical images, downscaling based compression of the images, encryption and decryption of images using AES technique and embedding of information along with the patient information. First the image is compressed by using watermarking based compression. Second the patient information is embedded along with the image by using Embedding of Message module. Third the image is encrypted by using AES technique. Fourth the encrypted image is storing on to the cloud.

3.1 Watermarking Based Compression:

Digital watermarking has been proposed as a way to claim the ownership of the source and owner. Unlike encryption, watermarking does not restrict access to the data. Once the

encrypted data is decrypted, the intellectual property rights are no longer protected.

Over the past few years, the technology of the digital watermarking has gained prominence and emerged as a leading candidate that could solve the fundamental problems of legal ownership and content authentications for digital multimedia data. A great deal of research efforts has been focused on digital image watermarking in recent years. The techniques proposed so far can be divided into two groups according to the embedding domain.

Algorithm 1: Watermark Based Compression Technique (WBCT)

Step 1: The cover image $f(i, j)$ is decomposed into low pass image and directional sub bands by using CT decomposition.
Step 2: The low pass image $f\,lo(i, j)$ lo coefficients are quantized using the following rule
$z = \text{mod}(f\,lo(i, j), Q)$
Step 2.1: If $w(i, j) = 0$ & $z < Q/2$
No modification in $f\,lo\,(i, j)$
Step 2.2: If $w(i, j) = 0$ & $z >= Q/2$
$f\,lo(i, j) = f\,lo\,(i, j) - Q/2$
Step 2.3: If $w(i, j) = 1$& $z >= Q/2$
No modification in $f\,lo\,(i, j)$
Step 2.4: If $w(i, j) = 1$& $z < Q/2$
$f\,lo\,(i, j)\,lo = f\,lo\,(i, j) + Q/2$

In Step 1 image *f(i, j)* is decomposed into low pass image and by using Contourlet Transform (CT)the directions of the image are obtained. In Step 2 the low pass image *flo(i,j)* is quantized by using the rule. In Step 2.2-2.4 the '*Q*' is quantization coefficient and may be selected based the experimentation on cover image. This is usually a trial and error process. After modifying *flo*(*i, j*), inverse CT is applied with the modified *flo*(*i, j*) and the watermarked image *f lo*(*i, j*)' is obtained.

The image watermarking extraction algorithm is as follows.

Step 1: The watermarked image $f(i, j)$' is decomposed into low pass image and directional sub bands by using CT decomposition. The watermark image is extracted by using the following rule.

Step 2: $z' = \text{mod}(f\,lo(i, j)', Q)$
Step 2.1: If $z < Q/2$, $w(i, j) = 0$
Step 2.2: If $z >= Q/2$, $w(i, j) = 1$

In step 1 the watermarked image *f(i,j)'* is decomposed into low pass image and by using CT once again obtain the various directions of the image. In step 2- 2.2 the watermarked image is extracted.

3.2 Encryption and decryption of the Images:

The Advanced Encryption Standard (AES), also referenced as Rijndael (its original name), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

Algorithm 2: Advanced Encryption Standard Technique (AEST)

Step 1: KeyExpansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
Step 2: InitialRound- AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.
Step 3: Rounds SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

AddRoundKey
Step 4: Final Round (no MixColumns)
SubBytes
ShiftRows
AddRoundKey.

3.3 Message Embedding:

In this concept the information about the patient like, name of the patient, disease of the patient and other details of the patient are embedded along with the image by using the key.

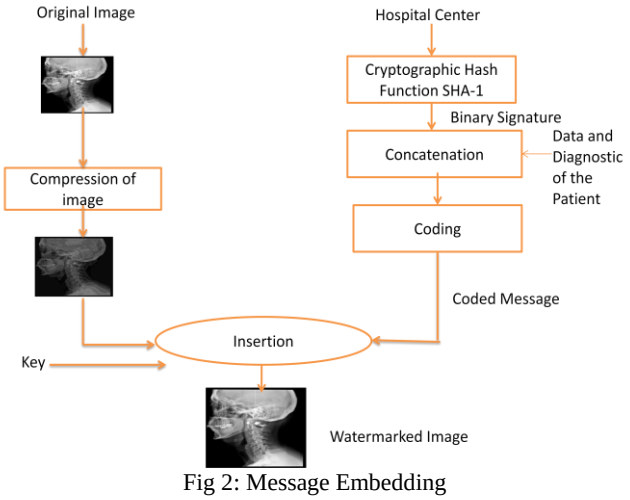

Fig 2: Message Embedding

Algorithm 3: Data Embedding technique using Genetic Algorithm (DEGA)

Step 1: Obtain the size of the authenticating image m x n.
Step 2: For each authenticating message/image,Read source image block of size 3x3 in row Major order. Extract authenticating message/image bit one by one. Replace the authenticating message/image bit in the rightmost 4 bits within the block, four bit in each byte.

Step 3: Read one character/ pixel of the authenticating message/ image at a time.
Step 4: Repeat step 2 and 3 for the whole, authenticating message/ image size, content.
Step 5: Perform mutation operation for the whole embedded image. For mutation rightmost 3 bits from each bytes is taken. A consecutive bitwise XOR is performed on it for the 3 steps. It will form a triangular form and first bit from each step is taken
Step 6: A bit handling method is performed on the embedded image. If the difference between the host and embedded image is ±16 the 16 will be added to the embedded image to keep intact the visibility of the embedded image.

4. Result Analysis

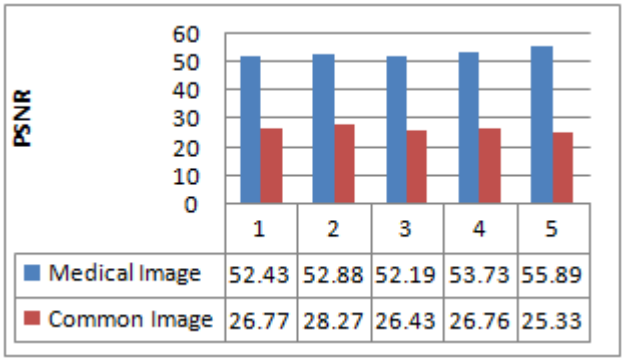

Figure 3: PSNR results by embedding two images.

The PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is usually expressed in terms of the logarithmic decibel scale. The signal in this case is the original data and the noise is the error introduced by compression. PSNR is most easily defined via the Mean Squared Error (MSE). Given the noise free M×N monochrome image I and its noise approximation K.

$$\mathbf{MSE} = \frac{1}{mn}\sum[\mathbf{I(i,j)} - \mathbf{K(i,j)}]^2 \quad \mathbf{(1)}$$

The PSNR (in dB) is defined as,

$$\mathbf{PSNR = 10\ log_{10}\ (MAX^2_I)/MSE} \quad \mathbf{(2)}$$

MAX_i is the maximum possible pixel value of the image, when the pixels are represented using 8-bits per sample, this is 255. When samples are represented using linear PCM with B bits per sample, MAX_i is $2^{B-1.}$

PSNR and MSE are used to comparing the squared error between the original image and the reconstructed image. PSNR is high means good quality and low means bad quality. PSNR is using a term MSE in the denominator, so low the error, high will be the PSNR.

PSNR depends on MSE between original and processed image. Theoretically, PSNR can be infinite if MSE is zero. MSE is zero when there is no difference between original and processed image.

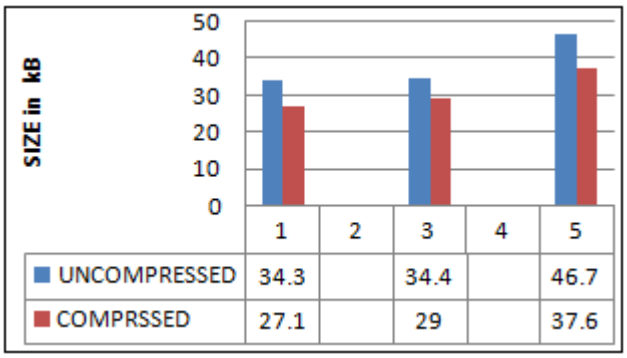

Figure 4: Compression performance of medical images.

The Fig 4 shows the compression ratio for the medical images, this is defined as,

Compression Ratio = Uncompressed / Compressed **(3)**

The space saving can be calculated by,

Space Saving=1- Uncompressed Size/ Compressed Size **(4)**

5. Conclusion

The sharing of medical information resources is a key factor playing a fundamental role towards the effective and rapid medical diagnosis, especially when doctors are faced with new clinical cases or whether they should take into account diseases that are not properly part of their domain of competence or their own specialization. In this work we presented a Virtual infrastructure-less Cloud solution for secure management of 3D medical images, which operates in an almost completely transparent manner, regardless of computational and networking capabilities which users can avail in any given moment.

References

[1] Alexa Huth and James Cebula, "The Basics of cloud computing", Carnegie Mellon University, US-CERT, 2011.
[2] Mohammed M. Abd-Edayen, "proposed security technique based on watermarking and encryption for digital image and communication in medicine", Egyptian Journal, Vol-14, Isuue-1, March 2013, Pages 1-13.
[3] A.Castiglione et al, "cloud based adaptive compression", Future Generation Computer Systems, 2014.
[4] K.Dorn, V.Ukis, T.Frise,"A cloud-deployed 3D medical Imaging system with dynamically optimized scalability and cloud cost", In proceedings of 2011 37th Euro Micro Conference on Software Engineering applications", IEEE, 2011, pp 155-158.
[5] Rafffaele Pizzolante et. Al, "A secure low complexity approach for compression and transmission of 3D medical images",2013 8th International conference on broadband, IEEE,2013.
[6] Xiaolin wu et al. "lossless compression of continuous-tone images vi context selection, quantization and modeling", IEEE Transactions on Image Processing, vol-6, No-5, May1997, pp 656-664.
[7] F. Rizzo,et al, "Low-complexity lossless compres sion of hyperspectral imagery via linear prediction", IEEE

Sig nal Processing letters, Vol-12, No-2, February 2005, 138– 141.

[8] G. Motta et al, " Lossless image coding via adaptive linear prediction and classification", Proceedings of. IEEE, Vol-88, No-11, November 2000. 1790–1796.

[9] Lizhe Wang et al, "Map reduce across distributed clusters for data-intensive applications", IEEE 26th International Parallel and distributed processing Symposium workshops and PhD Forum, 2012 DOI 10.11099/IPDPSW.2012.249 PP 2004-2011.

[10] Alhamazani et.al, "cloud monitoring of opti mizing the QoS of hosted applications", IEEE 4th Inter national Conference on cloud computing Technology and science, 2012.

[11] Khalid Alhamazani et.al, "CLAMS: Cross layer multi-cloud application monitoring-as-a-service framework", IEEE International conference on services computing, 2014, DOI-10.1109/SCC, 2014,45 PP 283-290.

[12] John G. Cleary et al, "Data Compression using adaptive coding and partial string matching", IEEE Transactions on Communications, Vol-32, No-4, April- 1984, pp 396-402.