International Journal of Mechanical Engineering and Technology (IJMET)
Volume 9, Issue 3, March 2018, pp. 162–173, Article ID: IJMET_09_03_018
Available online at http://www.iaeme.com/IJMET/issues.asp?JType=IJMET&VType=9&IType=3
ISSN Print: 0976-6340 and ISSN Online: 0976-6359

ANALYSIS OF SECURE CLOUD STORAGE PROVISIONING FOR MEDICAL IMAGE MANAGEMENT SYSTEM

Monica L Singh
PG Student, Christ University, Karnataka, India

Senthilnathan T
Associate Professor, Christ University, Karnataka, India

ABSTRACT

Medical images are considered to be the most sensitive images as it contains various health related sensitive information of an individual and it is necessary for the health care organization to maintain the sensitivity of these images without anybody misusing these data. When these images are transferred digitally through a network in order to store it in cloud for easy access for the authorities of the health care system, it is important to compress and encrypt these images to reduce the size and safeguard the information before storing and make sure that these images are transferred securely. In this paper, we use Huffman Coding technique in order to compress the image for easy transmission and to consume less storage space in cloud. To maintain the confidentiality of these images Blowfish encryption methodology is used. Once the image undergoes compression and encryption, the encrypted image is transferred and stored in a cloud storage

Key words: Cloud computing, Cryptography, Compression, Huffman coding, Blowfish

Cite this Article: Monica L Singh and Senthilnathan T, Analysis of Secure Cloud Storage Provisioning for Medical Image Management System, *International Journal of Mechanical Engineering and Technology* 9(3), 2018, pp. 162–173.
http://www.iaeme.com/IJMET/issues.asp?JType=IJMET&VType=9&IType=3

1. INTRODUCTION

In the past few years, the amount of users adapting to various cloud services are increasing day by day. Many organizations are migrating to cloud services including health care centers due to the various advantages of Cloud service providers. Health care services use Cloud storage service widely to store various medical data of the patients such that the authorities of the organization can access these medical data which can be X-ray images, Scanned images etc from anywhere and anytime. It is essential to compress these medical image to reduce the image size for easy transmission and decrease the storage space in cloud and when such

sensitive data are stored in cloud it is important to make sure that the data is not modified or read during transmission by encrypting the data

2. CLOUD COMPUTING

Cloud computing is model which helps organizations or individuals by providing them various services by residing in some other part of the globe. For example an organization which is using its own hardware and software facilities within its own network instead uses the hardware and software facilities provided by some other company through internet. The organization which uses the software and hardware facilities provided by some other company need not know where exactly these facilities are located and how it is functioned. Similarly cloud computing companies provides various computing services to the organizations and reduces their workload drastically. The cloud services is pay as you go service which allows the clints only for what they use. The clients use the service without worrying about backup, maintanace, updation etc. The cloud service providers automatically takes care of all these issues. The cloud service providers has several servers and the data is automatically backed up in many of these servers. If in case there is a breakdown in any one of the servers the other servers keep functioning and let the systems working.

Cloud Deployment Models

Public Cloud

Public cloud is a deployment model where the resources are owned by the third party providers and these resources are shared by the organization. It is the duty of the service providers to maintain and operate these resources without the interference of the organizations which reduces the time of these organizations. It is suitable for small organizations that has fluctuating requirements. The security level is slightly less when compared to the private cloud deployment. The third party service providers seems to have more control over the data.

The main advantage of this deployment model is that it is low cost and follows pay as you go procedure where the organization has to pay only for what they use.

Private Cloud

Private Cloud is a methodology which is dedicated to a single organization which is maintained either by the service provider or by the organization. All the resources are strictly restricted only to the authorized members of the organization. In private cloud the security level is high when compared to the public cloud and strict control over the resources. The organization itself can customise the resources according to their IT infrastructure. This deployment model is more suitable for larger business organization which contains high restricted data and administrative allegations. The main disadvantage of this is that when an organization itself monitors all its resources it becomes difficult for maintaining the resources especially when the resources are outdated and has to be replaced it quite expensive to replace the resources.

Hybrid Cloud

Hybrid cloud is a deployment model which is a combination of both Public and Private cloud deployments. This model allows the organization to utilize the advantages of both Public and Private models. The data and can be divided among these two deployment models by allocating the data which does not contain major sensitive information to the public cloud deploy-ment model and the data which contains sensitive information to the private cloud deployment model. Hybrid cloud provides the organization to easily scale the requirements when the organizations requirements keep fluctuating with the help of public cloud.

Service Models

Infrastructure as a Service (IaaS)

In this service model the cloud service provider provides the raw materials or the infrastructures that is needed in a data center such as servers, storage and other hardware infrastructure which can be accessed with the help of internet. All these infrastructures are monitored, managed and maintained by the third party providers the organization utilizing these facilities has to only concentrate on their project rather than the maintenance. This is pay as you go scheme where the client has to pay only for what he has used. Each infrastructure is provided as a separate service and the organization has to pay till they use that particular resource.

Software as a Service (SaaS)

In this service model a third party service provider provides the software applications to its customers and allows access to them through internet via web browser. Example for this is email applications. SaaS customers do not require any hardware or software infrastructures to get installed in their system all they need to have is an internet connection to access this service. All the underlying infrastructures are present and maintained in the service provider's data centre.

Platform as a Service (PaaS)

In this service model the service providers enables an environment for the organization to build, test, deploy, manage, and update the applications and services. The customers do not have to install the infrastructures that are required to build an application. The maintenance of the infrastructures associated with building an application is taken care by the service providers. The infrastructures and other IT resources are accessed by the customers through web browser.

ENCRYPTION

Encryption is a process of converting a data to its unredable format. The main aim is to protect the sensitive information from the intruders during transmission. The most important issue during transmission and in cloud computing is the security issue. The three main properties of securing the information are confidentiality, integrity and availability. Among these security properties confidentiality plays a very important role. In order to safeguard the confidentiality it is important to encrypt the data and then store in the cloud. This encrypted data which is in unrecognizable format is called ciphered data. The process of converting the original data to a ciphered data is called Encryption. The ciphered data can be brought back to its original data and this process of converting a ciphered data to its original format is called Decryption. The data is encrypted and decrypted using several encryption techniques such as Blowfish, DES, AES, Playfair, substitution etc.

Symmetric Key Encryption

Symmetric key is a method where the same key is used for both Encryption and Decryption. The encryptor and the decryptor will have to share the same key before performing the Encryption and Decryption operations.

This method is also called as Private key Encryption. Examples are Blowfish, DES, AES.

Public Key Encryption

Public key encryption is an asymmetric key method where both Encryption and Decryption techniques uses different keys. The Encryption key is publicly open for anybody who wants

to encrypt the messages but the decryption key is available only for receivers or the person who decrypts the data. The example for Public key encryption is RSA encryption method.

COMPRESSION

Image Compression is a technique which helps in reduction of the image size without affecting the quality of the image to a greater extent. The main purpose of this technique is to save the disk space and reduce the time consumed for transmitting the image through the internet it also reduces the time required to upload and download the image file in the cloud. There are two types of compression method

Lossy Compression

Lossy compression is a method where the compressed image losses certain data during compression and there is quite difference in the quality of the compressed image when compared to the original image. The data which is lost during the compression process cannot be recovered. This type of compression is suitable for normal photographs where the minor loss of data is negligible. The different methods of lossy compressions are Chroma subsampling, Transform coding, Fractal compression.

Lossless Compression

Lossless compression is a method where the compressed image where there is minimal loss of data during compression and retains the quality of the image. There is minimal chances of loosing the data in a compressed image. If by chance the data is lost during the compression process it can easily be recovered. This type of compression is suitable for medical images where the data and the quality of the image has to be retained The different methods of lossless compressions are Huffman coding, Run length encoding, entropy encoding, chain coding.

HUFFMAN CODING

Huffman coding is a compression method which was pro-posed by David A Huffman in the year 1952. It is one of the lossless compression techniques where there is min-imal chances of loosing the data. It is the method for the construction of the least repetitive code. Huffman technique analysis the occurance of each character associated with binary string in a ideal way.[1] Huffman coding algorithm is a method for building an extended binary tree with minimum weighted path. Huffman coding aims at assigning variable-length codes to input characters, lengths of the assigned codes are based on the frequencies of corresponding characters. The most frequenct character gets the smallest code and the least frequent character gets the largest code.

Tree Construction Rules The two major parts in Huffman Coding are

1 : Build a Huffman Tree from input characters.

2 :Traverse the Huffman Tree and assign codes to char-acters.

BLOWFISH

Blowfish is one of the most powerful encryp-tion algorithm which is developed by Bruce Schneier as an alternative for DES and many existing algorithm. It is a 64-bit block cipher which uses symmetric key technique for both encryption and decryption. Blowfish is free and unpatent and is publicly available. Blowfish is one of the fastest and most secured till date. There is no attack known to be successful against blowfish.[2] The Blowfish encryption standard gener-ates key dependent S boxes at cipher set time. This is one of the main reason

which, makes the attacker difficult to know the S boxes, the algorithm contains 8*32 S boxes of 256 entries each, larger the S boxes more difficult is the attack. There is no attack that is successful against Blowfish. Thus Blowfish is more suitable for Cloud environment and assures the confidentiality of the data

Algorithm [3]

Step 1: Divide x into two 32-bit halves: xL, xR

Step 2: For i = 1to 16:

Step 3: xL = XL XOR Pi

Step 4: xR = F(XL) XOR xR

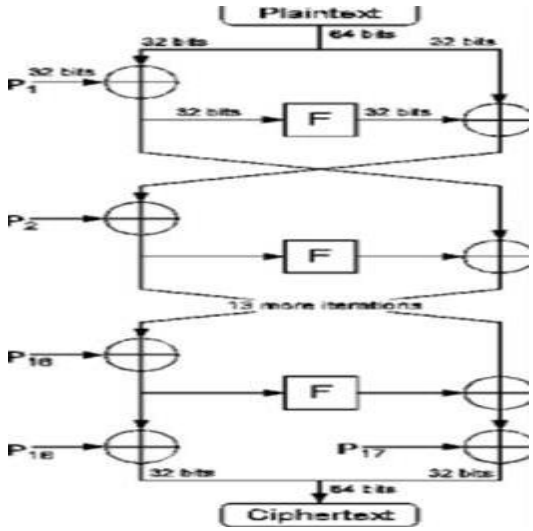
Step 5: Swap XL and xR

Step 6: Swap XL and xR (Undo the last swap)

Step 7: xR = xR XOR P17

Step 8: xL = xL XOR P18

Step 9: Recombine xL and xR



3. LITERATURE SURVEY

In this section we present and talk about experiences from literature related to our proposed method

A Study of New Trends in Blowfish Algorithm

This paper represents a comparision between the four popular encrypton algorithms AES,DES,3 DES and Blowfish by means of security and power utilization. The comparision is conducted for various files such as text file, jpg file, audio file and video file. The proposed change makes utilization of the new operation characterized in the past segment, operation '' applied to every round in the first Blowfish calculation, where another key is expected to apply this operation at the two sides, this key may come in binary and change over to a 4-states key, or it might as of now arrive in a 4-states as that should be possible with quantum channel. Therefore, two keys will be utilized as a part of every round of the first Blowfish, the main key K1 will be utilized with the xL and Pi to deliver the following left part. The second key K2 will be utilized with F (xL) and xR to create the correct part. The convertion of these three contributions to the '' operation must be done first from 32 bits to a 16 digits each might be one of four states (0, 1, 2, 3) By including extra key and supplanting the existing XOR by

the proposed operation '' in order to increase the efficiency of Blowfish Algorithm and making it more grounded against an interruption. This advancement of Blowfish Algorithm makes it effective in vitality utilization and security to diminish the utilization of battery control gadget. By this methodology of Blowfish by additionally expanding the key length, Blowfish will give the better outcomes.[4]

An Algorithm for Image Compression Using Huffman Coding Techniques

The main purpose of compression is to decrease unessential or picture information so as to have the capacity to store and transmit information in a proficient way. It additionally lessens the quantity of bits required to store or potentially transmit through the media digitally. Compression implies that the contain some bit of information and you diminish its size. There are distinctive procedures and they all have their own particular focal points and inconveniences. Huffman coding is a lossless information pressure method. Huffman coding depends on the recurrence of event of an information thing i.e. pixel in pictures. The system is to utilize a lower number of bits to encode the information in to twofold codes that happens all the more much of the time. It is utilized as a part of JPEG documents.

This paper aims at creating at Huffman coding algorithm for picture data and broke down execution parameter and bits per pixel. The objective of genuine compression is to limit the quantity of bits expected for representation. The last compression proportion (2.8 percent) and Bit-Per-Pixel proportion (0.23) are exceptionally acceptable[5]

Comparative Study of Cloud Computing Data Security Methods

The idea of this proposed method is to wipe out the disad-vantages with respect to data protection utilizing encryption algorithms to upgrade the security in cloud. This paper talks about cloud computing security systems and portrays the similar investigation of a few encryption algorithms. Algorithms such as RSA, DES, AES, Blowfish are being utilized and comparision results among them have additionally been exhibited to guarantee the security of information on cloud. It is seen that DES, AES, Blowfish algorithms use symmetric key encryption where a solitary key is utilized for encryption and decryption of data. In 1970 IBM devel-oped DES (Data Encryption Standard). In 1993 Blowfish was planned by Bruce Schneier , explicitly for use in execution obliged situations, for example, embedded system. In 2001 NIST composed AES (Advanced Encryption Standard). RSA is an public key calculation developed by Rivest, Shamir and Adleman in 1978 and furthermore called as Asymmetric key calculation, the calculation that utilizations distinctive keys for decryption and encryption. Having Examined dis-tinctive techniques for information security in cloud. Different encryption calculations are being proposed to make cloud information secure, defenseless and concern to security issues, challenges and furthermore examinations are done among AES, DES, Blowfish and RSA calculations to locate the appropriate secured algorithm, which must be utilized as a part of cloud computing for assuring cloud information secure and prevent hacking by the intruders. Encryption calculations assume an essential part in information security on cloud and by correlation of various parameters utilized as a part of algo-rithms it is discovered that AES calculation utilizes minimum time for execution of cloud information. Blowfish calculation has minimum memory prerequisite. DES calculation expends slightest encryption time. RSA occupies highest memory size and consumes more time for encryption.

The upcoming extent of the existing proposed method is to discover an effective algorithm to influence the information to secure by consolidating homomorphic encryption

and MD5 encryption and utilize a compression technique for ensuring the security of the information[6]

Compression Using Huffman Coding

Compression of data is known as source coding. Data compression is a way toward encoding data utilizing less bits than uncoded portrayal is likewise making a utilization of particular encoding technique. Data Compression is an innovation for decreasing the amount of information required to display any substance without too much lessening the quality of the photo. It likewise decreases the quantity of bits required to store as well as transmit through a media digitally. Compression is a methodology that helps in storage easier for abundant amount of information. There are different methodology accessible for compression in the presented material , compression method like Huffman coding is examined with other popular compression methods like Arithmetic, LZW and Run Length Encoding. it is inferred that arithmetic coding is extremely productive for more regularly occuring pixels with less bits and decreases the size of the file dramatically. RLE is easy to actualize and quick o execute. LZW calculation is preferred to for TIFF, GIF and Textual Files. It is clearer to execute, quick and lossless calculation though Huffman calculation is utilized as a part of JPEG pressure. It produces ideal and reduced code however moderately slow. Huffman calculation depends on factual model. The specified compression methodology utilize lossless method.JPEG strategy which is utilized generally for picture compression is a lossy technique.JPEG 2000 is progression in JPEG standard which utilizes wavelets.[7]

Data Confidentiality in Cloud Computing with Blowfish Algorithm

In the present paper settle security challenges for information in the cloud and gives a dependable and simple approach to secure information with encryption innovation. In the proposed method, the client will receive a validation of integrity of the information that client wishes to store in the cloud with absolute minimum expenses and endeavors. Encryption is succeeded by means of scheduler that helps in converting the actual information to the ciphered one and then this ciphered information is transferred to cloud. During recovery the ciphered information is again converted into plain information. This decreases the oppurtunity of data leackage internally. By this way, a dependency is set up to collaboration show amongst administrator and service provider to the clients. The proposed method portrays about ERP System, OTP required booking the information, Encryption and Decryption, Data Transfer to cloud, SOAP Protocol, Retrieve the information from cloud, Compare the Data For securing the database of ERP on cloud with the assistance of encryption and SAOP convention. It has turned out to be easier to encode and also transfer information all the while on cloud on a single tick. The information which is obvious to client on CSP is Encrypted in an unrecognizable format.This makes the thief difficult to recognize what the actual data is. Examination of information is done if a change which sends message through Email.[8]

Image Compression Using Huffman Coding Based On Histogram Information and Image Segmentation

This paper portrays Huffman coding which is a compression method based on histogram data and image segmentation. The image is compressed by lossy and lossless method. The amount of image compressed using in lossy method and lossless method, relies upon the data acquired by the histogram of the picture. The outcome of this technique demonstrate that the contrast amongst actual and compressed pictures is minute and negligible. CR(Compression Ratio) and PSNR (Peak Signal Noise Ratio) are analysed for various images. The connection

between CR and PSNR demonstrates that at whatever point we increment CR we get high PSNR. It demonstrates that if the PSNR value is high then the quality of the image is better.

The strategy settles on the choice of what to compress in lossless way and what in lossy depends on the highest intensities in the picture. These intensities have more sig-nificance than the ones with less recurrence. The quantity of intensities chose relies upon the bit rate of the picture. Thus, pictures with various bits per pixel are compressed with this proposed method. This deals with various bit rates. The outcomes demonstrate that when there is increment in the CR the PSNR is also higher.It is seen that if there is small CR then we have many erros. At whatever point the Compression Ratio builds the errors will be least.

It implies the compressed picture is practically equivalent to the actual picture. The pressure acquired is practically identical to JPEG and is extensively more than Huffman coding. It works with various kind of pictures. A lower an incentive for MSE implies less error. high estimation of PSNR is great since it implies that the proportion of Signal to Noise is high. the signal is first picture, and the noise is the error. In this way, if we have less MSE value and higher PSNR we can perceive that it is a superior one.[9]

Image Encryption and Compression for Medical Image Security

There are two important methodologies proposed. The first depends on content security through encryption. In this , ap-propriate decryption of information requires a key. The second constructs the assurance of computerized watermarking, which aims at implanting a message within the information. Taking the processing time into account, these two methodologies are joined with compression method. The method introduced in this paper demonstrates how encryption offers security to mediacal images. The fundamental target is to ensure the security of medical pictures while transmission. For moral reasons medical images should not be transmitted in an unsecured medium thus should be secured. Encryption is an appropriate method to safeguard the data. A wide range of encryption algorithm exist already. In this proposed method, the first segment discusses about the standard data for encryption such as block cipher, stream cipher, asymmetric encryption and symmetric encryption. In the second segment the collaboration of picture encryption and compression and discussion on specific encryption strategies is done. The issue of concurrent Partial encryption and specific encryption (SE) and picture compression is addressed.To complete this paper a watermarking and information hiding method is developed [10]

Lossless Huffman Coding Technique For Image Compression and Reconstuction Using Binary Trees

In the proposed method the picture is changed into a cluster utilizing Delphi picture control technology. The picture control is utilized to show the graphical representation of a picture like ICO(Icon), BMP(Bitmap),WMF(Metafile), JPEG, GIF, and so on,at that point a methodology is built in Delphi inorder to equip Huffman coding technique that displaces repetitive codes from the picture and shortens a BMP picture data (particularly incase of grayscale picture) and reproduced effec-tively.Therefore the recreated picture is a correct illustration of the intial since it is lossless confining method.This arrange-ments can likewise be connected on different kind of pictures in RGB which includes JPEF, BMP, tiff and gif. However the reconstructed image does not retain its original colour quality since there is some loss in the process. When compared to the available standard strategies CR(Compression Ratio) for grayscale image is superior.Huffman coding undergoes the evidences that the uncompresser demand should have some familiarity of the chances of the images in the compacted data which requires higher portion to encode the dada and if this

data is inaccessible then the compressing data necessitates two procedures i.e., firstly calculate the recurrence of every symbol and develop a huffman tree and then compress the available data.

This picture compression strategy is very appropriate for gray scale (high contrast) bit map images .This technique can be enhanced by utilizing an approved Huffman coding system that is an expansion to Huffman coding.[11]

Secure Online Cloud Data Storage System Using Blowfish Algorithm

The Government authorities have putforth few help plans for citizens, for those who were affected in natural calamities such as cyclones, earthquakes and floods etc. These funds were assisted for citizens who were influenced in such calamities. At first, these funds were useful for people who were affected to get their fundamental essential needs. These funds were transmitted to the affected people government officials. How-ever, these assets are not reaching the affected people properly. These assets are being corrupted and mistreated during the transmission. Since, the photo copying of the identity proofs such as voter id and ration card. are easily getting corrupt. To defeat these corruption this paper has has upgraded few security methods during these transactions of funds via internet utilizing Cloud computing.

There are three proposed security methods for collection of data, encryption and face detection. The client has to register and signup in the relief fund transaction form.The client has to submit the family details, bank details and other details. These details are stored in the cloud servers, so it acn be accessed form anyplace and anytime.Then the saved records are encrypted to protect from unauthorized people. then, the client face is identified utilizing web cameras. These procedures is handled under an SLA (Service level Agreement) which is an agreement between the CSP (Cloud service providers) and client. The cloud specialist organization should provide an affirmation that, these reports that the client submitted in cloud server is not defiled by any unauthorized persons. This three levels are known as tri level security. This proposed configuration ensures protected and proficient safety efforts which includes transferred proofs, encrypted information, and identification of customer face. By utilizing this proposed method nobody except the authorized individual gets the fund. By adapting this methodology the funds will reach the victims properly with less corruption. Blowfish encryption method is used. It is seen that with the collaboration of blowfish encryption and face detection method the level of security is high and thus the data is been secured properly in cloud. [12]

DES, AES and Blowfish: Symmetric Key Cryptog-raphy Algorithms Simulation Based Performance Analysis

This proposed paper gives a reasonable observation between three most symmetric key cryptography calculations like AES, Blowfish, and DES. As the principle interest in this particular method is the execution of calculations under various circumstances, the given contrast proceeds about the conduct and the execution of the calculation when various information loads are utilized. This particular comparison is made on the format of some particular parameters which includes key size, block size and speed. The duplication progam is executed utilizing Java programming. The given duplication consequences demonstrated that Blowfish usually has a superior execution when compared to other regular encryption calculations utilized. As Blowfish has no known security issues focused up until this point, which in turn made it a phenomenal contender to be treated as a general encryption calculation. AES demonstrated low execution outcome contrasted with the other available calculations because it necessitates a higher level of handling power.The usage of CBC

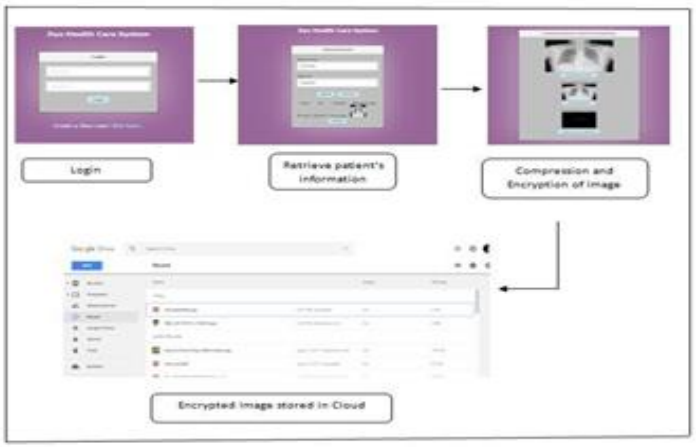
technique has included additional handling time, however it was moderately unimportant particularly for certain operation that requires higher level of secured encryption to a generally substantial information sections. OFB indicates conduct over ECB and CBC yet it requires preparation time than CFB generally the time distinctions between all modes are irrelevant the time distinctions between all modes are irrelevant. For further research this examination can be executed in better test systems to obtain an enhanced signs of improvement from the outcome. This examination should also be made possible in another test system by expanding it to network programming to demonstrate which calculations performs better in a particular network. The test systems which can be utilized in the analysis are ns2, OPNET, ns, ns3, NetSim and so on. These test systems will give better outcomes for cryptographic applications in the network organised.[13]

4. PROPOSED METHOD

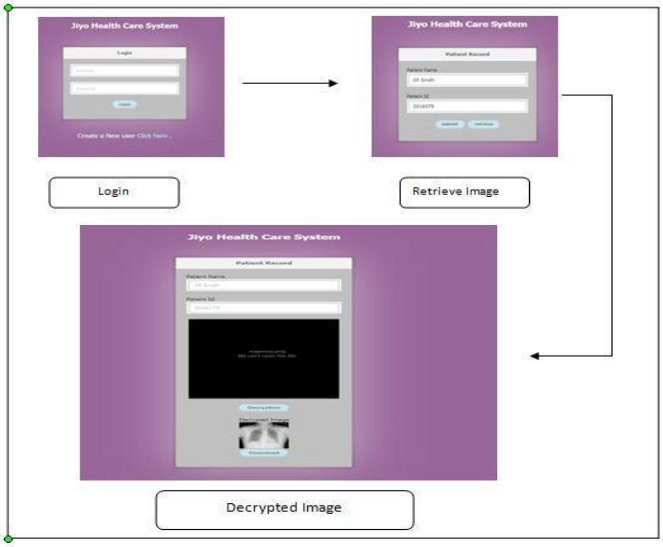
The proposed method gives the detailed information of how the system works. The main aim the proposed methodology is to make the health care organization function more easily, effective and securely at the same time maintaining the confidentiality of the data of the patients. This system makes the authorities of the health care organization function easy by accessing the patients data such as their X-ray images etc from anywhere irrespective of the location and time by storing their records on a cloud service. The main objective is compressing the image using Huffman coding compression technique. Which is lossless compression methodology by this method the data is retained and there is no loss in the data and quality of the image. Here the image size is decreased so that it consumes less disk space and less bandwidth which makes it easy for transmission over the internet and it reduces time to get upload and download in the cloud. Once the image is compressed, the resultant image is encrypted to to safeguard the confidentiality of the image. Here Blowfish encryption method is used to encrypt the image and converts the image to an unrecognizable format. By doing this no third party can recognize the image and violate the information. Once the image is compressed and encrypted it is sent through the internet and stored in cloud storage service such as Google drive.

Storing Medical Image in Cloud

In order to store the medical images of the patient in cloud, first the doctor has to login into the Jiyo health care system website and enter the patients details such as Patient name and PatientID which will display the details such as patient name, ID, sickness and their scanned image. By clicking on the save in cloud button, the web page is redirected to the compression and encryption page later by clicking on compression button the image is been compressed and by clicking on encrypt button the image is encrypted and this image is saved in the cloud.

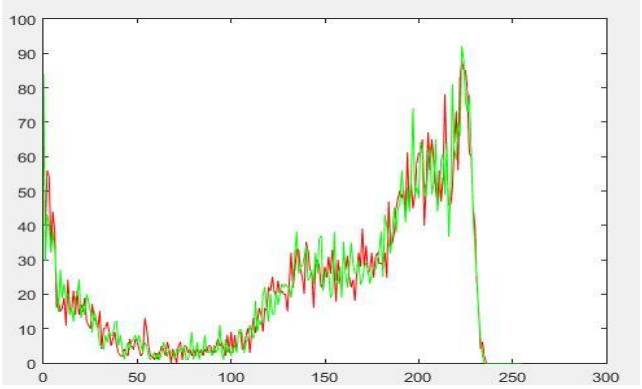


Retrieving Medical Image from Cloud



In order to retrieve medical images of the patient the Doctor has to login, if he has logged out and enter the patients details such as Patient name and Patient ID to get the medical image for example X-ray image which we have considered here. The encrypted image of the patient will be displayed and by clicking on the Decryption button the encrypted image will be decrypted and the acutall image is displayed. In order to store the decrypted image in the local system, the doctor has to click on the Download button.

5. RESULTS AND ANALYSIS



The graph represents the quality difference between the actual image and the compressed image. The Peak Signal-to-Noise Ratio value between the actual image and compressed image is 37.913. The Peak-Sinal-to-Noise Ratio for medical images is 40. This can be overcome by applying an advanced compression method to retain the quality of the actual image in the future.

6. CONCLUSION AND FUTURE WORK

The proposed method is beneficial for health care organi-zations where the medical data of the patients is preserved in cloud thereby making the working of the organization and the patients easier by preventing the chances of loosing and misuse of the data. The compression and encryption of data reduces the time required for transmission, reduces the space utilized,

reduces the time needed for uploading and downloading and also maintains the confidentiality of the data.

The authorities of the organization can easily forward the medical data to higher officials for further analysis within a fraction of second and in a secured manner. The quality difference between the original image and the compressed image can be retained by more advanced compression method in future research.

REFERENCES

[1] Shaikh, A. A., and P. P. Gadekar. ”Huffman Coding Technique for Image Compression. Compusoft 4.4 (2015): 1585

[2] Mathur, Milind, and Ayush Kesarwani. ”Comparison between Des, 3des, Rc2, Rc6, Blowfish And Aes.” Proceedings of National Conference on New Horizons in IT-NCNHIT. Vol. 3. 2013.

[3] Kumar, G. Kishore, and M. Gobi. ”Comparative Study on Blowfish Twofish Algorithms for Cloud Security.”

[4] Singh, Gurjeevan, Ashwani Kumar, and K. S. Sandha. ”A study of new trends in Blowfish algorithm.” International Journal of Engineering Research and Application (2011).

[5] Sanjay Kumar Gupta, ”An Algorithm For Image Compression Using Huffman Coding Techniques”, International Journal of Advance Research in Science and Engineering(2016)

[6] Unnikrishnan, Megna, and Lipi Arun. ”Comparative Study of Cloud Computing Data Security Methods.”Sharma, Mamta. ”Compression using Huffman coding.” IJCSNS Interna-tional Journal of Computer Science and Network Security 10.5 (2010): 133-141.

[7] Subhash, Shirole Bajirao, and Dr Sanjay Thakur. ”Data Confidentiality in Cloud Computing with Blowfish Algorithm.” International Journal of Emerging Trends in Science and Technology 1.01 (2014).

[8] Monisha Sharma , Chandrashekhar K, Lalak Chauhan ”Image Com-pression Using Huffman Coding Based On Histogram Information And Image Segmentation”, International Journal of Engineering Research and Technology(2012)

[9] Puech, William. ”Image encryption and compression for medical image security.” Image Processing Theory, Tools and Applications 2008. IPTA 2008. First Workshops on. IEEE, 2008.

[10] Mathur, Mridul Kumar, Seema Loonker, and Dheeraj Saxena. ”Lossless Huffman coding technique for image compression and reconstruction using binary trees.” International Journal of Computer Technology and Applications 3.1 (2012).

[11] N.Jayapandian and A.M.J.Md. Zubair RahmanSecure, ”Online Cloud Data Storage System Using Blowfish Algorithm”, Journal of Advance-ment of Engineering and Technology 2017

[12] Thakur, Jawahar, and Nagesh Kumar. ”DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis.” International journal of emerging technology and advanced engineering 1.2 (2011): 6-12.

[13] Saranya Jothi C, Usha V, Alex David S , Dynamic Data Integrity and Checkpoint Recovery Using Public Auditing in Cloud Storage . International Journal of Civil Engineering and Technolo gy, 8(9), 2017, pp. 692 – 700 .

[14] Tamilmani G, Dr. M. Kavitha, K. Rajathi . Encrypted Multi Keyword Searching for Secured Cloud Storage. International Journal of Civil Engineering and Technology, 8(9), 2017, pp. 1169 – 1175

[15] S Alekhya Yada, Siva Skandha Sanagala, Vijaya Kumar Koppula and VA Narayana, Investigation on Different Techniques for Deduplication in Cloud Storage. International Journal of Civil Engineering and Technology, 9(2), 2018, pp. 963 - 972 .