RESEARCHERID
THOMSON REUTERS

[Ara, 5(8): August 2018]
DOI- 10.5281/zenodo.1342515

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

IMPROVING THE SECURITY OF MEDICAL IMAGES BY IMPLEMENTING ENCRYPTION AND COMPRESSION TECHNIQUES

Arifa Tehseen Ara*[1]& Dr.V.Vijaya Raja[2]
[*1]Assistant Professor, VJIT
[2] Professor, VJIT

ABSTRACT

Advances in the field of Information Technology has made a deep impact on health care domain. IT enabled health care domain is efficient because of the digitization of medical reports resulting in easier and faster access. One of the concern of digital medical images is Security. Security of clinical facts imposes 3 mandatory characteristics: confidentiality, reliability and availability. Confidentiality of medical images is to ensure that the data is accessible only to the genuine users by imposing encryption. In the mobile cloud computing platform, security is a bigger concern in regards to the medical images. To date we have few techniques but, to improve the security of the medical images, we are implementing encryption as well as compression techniques in this paper. Here, the encryption is the best way to provide confidentiality of the data and the compression is the way to reduce the storage space for the data in mobile cloud. With encryption and compression better security can be implemented.

Keywords: *Mobile Cloud Computing, Medical Images, Encryption and Compression.*

I. INTRODUCTION

Cloud computing helps in offering resources to purchaser on an on-demand basis via the internet provider interface; mobile cloud computing is a type of cloud computing paradigm wherein a number of gadgets which are used for imparting the services, are mobiles. Mobile gadgets have many constraints imposed upon them because of the desirability of smaller sizes, lower weights, longer battery existence and different features. These constraints have hindered hardware and software program development for these gadgets. Cloud computing can be used to allow the cell gadgets to avoid these constraints by making resource intensive tasks and complicated capabilities to be carried out on cloud computers and receive the outcomes of the transaction on the mobile devices. This makes Mobile Cloud Computing efficient and effective for strong applications in the healthcare sector. The cell phone users will benefit, as they could avail cloud services without excessive capital expenditure on hardware and software sources. The end users can effortlessly run the applications from their cellular device without any high priced hardware to run applications as the operations are executed within the cloud.

Cloud Computing gives many blessings by way of allowing users to use infrastructure like servers, networks, and storages, structures containing middleware services, running systems and software programs for application applications getting rid of the requirement for users to plan beforehand for acquiring special resources for storage and computing strength. Particularly, assets can be dynamically introduced and launched depending on carrier call for and with minimum management effort. As an end result, the availability of cloud computing services in a mobile environment, additionally referred to as cell cloud computing. The increasing situation towards Mobile Cloud Computing With the explosion of cell packages and the support of CC for one of a kind type of services for cellular customers, mobile cloud computing (MCC) is introduced as an integration of cloud computing with the mobile computing and mobile devices. However, together with the usefulness of this subject matter of cell cloud computing studies nonetheless wishes to be done on several issues in addition to viable frameworks to assist cloud computing on cell gadgets.

The concept of Mobile Cloud Computing (MCC) is a typical concept that aims at the usage of cloud computing techniques for storage and processing of facts on cellular gadgets, thereby lowering their limitations. The mobile device consumers will ultimately be the benefactor of the Mobile Cloud Computing. Mobile users can be benefitted from a cloud without an excessive degree of capital expenditure on hardware and software program sources. Nature of cloud service models is of high-quality for customers considering that they do no longer need to have very technical hardware to run programs as these computing operations are run inside the cloud. This reduces the rate of cellular computing to the stop customers. They could see a massive quantity of recent functions enhancing their phones because of Mobile Cloud Computing. At the equal time the developers additionally have real advantages from Mobile Cloud Computing. The biggest benefit of cloud computing for developers is get entry to a broader target market of a extensive range of cellular subscribers. Since cloud computing programs run on a simple application software such as browser, the end consumer's cellular running gadget does no longer have any effect at the software.

Thus MCC is a completely efficient and powerful manner to expand services in the healthcare quarter. The users can provision resources and applications without high investment on hardware and software resources. The customers can effortlessly run the applications from the cellular without the want of greater hardware to run the packages as the operations are run inside the cloud. The only concern in mobile cloud computing is privateness and security. The Data maintained in a cloud can contain personal or confidential statistics together with healthcare related statistics that requires the proper safeguards to save you disclosure, compromise or misuse.

II. RELATED WORK

Applying security to the transmitted clinical information is vital to guard the privacy of patients. Secure transmission calls for cryptography, and watermarking to obtain confidentiality, and statistics integrity. Improving cryptography component desires to use an encryption algorithm that stands for a long time against special attacks. Ahmed Mahmood et al proposed a technique of using Chinese remainder theorem as a backbone. This technique achieves high level of safety and stands in opposition to specific attacks for a long time. On watermarking part, the scientific image is split into areas: a location of hobby (ROI) and a location of historical past (ROB). The image values of the ROI include the essential information so this location should no longer enjoy any exchange. The proposed watermarking method is based totally on dividing the clinical photograph in to blocks and placing the watermark to the ROI through transferring the blocks. Then, an equal number of blocks inside the ROB are removed. This method may be taken into consideration as lossless since it does not have an effect on at the ROI, also it does not increase the photograph size. In addition, it could stand towards a few watermarking assaults such cropping, and noise.

S. Li, C. Li, Lo, and G. Chen provided a comprehensive research on the safety of a picture scrambling scheme lately proposed. As an end result, it has been observed that this picture scrambling scheme isn't sufficiently comfortable in opposition to numerous kinds of attacks: cipher text-only attack, regarded-plaintext attack, chosen plain text attack, selected-cipher text assault. Other two predominant security flaws have also been mentioned while a set mystery matrix is used to encrypt the whole photograph. Based at the cryptanalytic results, it is concluded that this image scrambling scheme can simplest be used for (lossless or lossy) perceptual encryption, rather than imparting a complete safety of all (or most) visual statistics in the obvious-image.

A novel mystery transmission scheme has been proposed by Mamta Jain and Saroj Kumar Lenka and it's far using the notion of opacity with regards to a diagonal queue least vast bit substitution that is an exceedingly powerful alternative for transmitting secure clinical facts and patient's non-public identity statistics along with the ideal clinical Brain disease photo. The mystery message blocks and sub-blocks are allocated dynamically by using the sender to the Brain disease cowl image blocks with respect to diagonal queues, which increases security tiers and gives dynamic effect to the proposed algorithm. The proposed set of rules has used Rabin public key cryptosystem at cryptography degree to offer confidentiality of Brain clinical information of affected person at medical statistics center and verbal exchange, considering the fact that it's far computationally comfy related selected-plaintext assault, pretty smaller vulnerable to incidence research attack and enciphered message attacks. It additionally shows the issue of integer factoring. At steganography degree, least extensive bit substitutions the use of diagonal queues

were used to defend sensitive clinical data of patient like HIV file and baby woman fetus from leakage in transmission channel when resources are shared amongst a couple of transmission holders. Using the multilevel encoding approach presented, the medical Brain sickness photo itself can be hidden interior. From the effects and histogram analysis, it's far concluded that PSNR, MSE values, and the proportion of most embedding potential are better compared to some of the present algorithms and imperceptibility distortion can't be measured from the corresponding medical Brain sickness stego images.

III. FRAMEWORK

Security is one of the major aspects to be taken care of for each the encrypted items and the encryption algorithms. Some of the security aspects of the 2 techniques are discussed here. In each the strategies as an image itself is used as key. It's very hard for the attackers to discover which photograph may be used as key. The original image is completely reconstructed with none loss or distortion best when the perfect key photograph is used.

A. Medical Image Encryption

The encryption methods are advised for medical photos, as whilst patients need to proportion medical photos on net with most effective people in their interest, they want to secure them from specific styles of assaults. Medical photographs have unique residences compared to different digital photographs which can be the reason; the kind of encryption required is likewise different.

i. Encryption using Key image and XOR operation

- Read Original Image.
- Take the key image of same size as original image.
- Convert key image and original image to gray image.
- Perform XOR operation of original image with key image pixel by pixel.
- Resultant image is encrypted image.

ii. Decryption using Key image and XOR operation

- Read Encrypted Image.
- Take the key image which was used for encryption.
- Convert key image and encrypted image to gray image.
- Perform XOR operation of encrypted image with key image pixel by pixel.
- Resultant image is the original image.

B. Medical Image Compression Technique

Medical Image compression (MIC) and its analysis might also be more beneficial and might play an important function for the analysis in the telemedicine with greater sophisticated and complicated photographs through consultation of experts. The element beneficial for prognosis of the photograph may be highlighted with greater contrast and determination for the function extraction. In telemedicine, it's crucial that medical image ought to be compressed and sent through aid constraint network, while in robotic surgery, high definition motion pictures are required for streaming with zero tolerance errors. However, inspite of such advancement in medical technology, there may be a gap among the clinical technological know-how and technology available to guide it with an expected intention. It could be very important that even as performing compression at the clinical pictures, the effectiveness of resolution as well as perceptual nice be restored. It is likewise regarded that compression is likewise followed via certain lack of tremendous data if the facts are big and channel potential is incredibly confined for transmission motive. Another difficult inside the vicinity of medical photograph compression is that each one there are numerous types of bio-medical photographs (x-ray, CT, MRI and many others) and compression ratio applicable for some of these bio-clinical images especially differs from every different. Therefore, it can be visible that clinical photograph compression is a critical studies problem concerning the degree of compression and the preservance of the applicable records.

IV. RESULT ANALYSIS

The medical images are supported by the DICOM file format. The images are compressed using JPEG2000 compression. The compressed images are uploaded in the Cloud server by the physician and the images are transmitted to the mobile device. Example datasets are CIFAR-100 which include 32*32 colour images, STL-10 which similar to CIFAR-10 and SVHN datasets.

Examples of the medical images of MRI, CT, XRay, Ultrasound transmitted from cloud computing server and presented in the mobile device are shown below.

Fig1. MRI Scan image and X-Ray Image in Mobile Device

V. CONCLUSION

In this paper, we presented encryption and compression of the medical images on mobile cloud computing platform. Presented cryptographic techniques can protect the medical images data. These techniques can be used by patients as well doctors to share their medical images data through the mobile devices. The mobile clouds offer different capabilities to store the data. With the presented compression technique, we can provide an efficient data storage on mobile cloud platforms

REFERENCES

1. *Mitchell Shanklin, "Mobile Cloud Computing", A survey paper written under the guidance of Prof. Raj Jain.*
2. *Ahmed Mahmood, Charlie Obimbo, Tarfa Hamed and Robert Dony, "Improving the Security of the Medical Images" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No. 9, 2013*
3. *S. Li, C. Li, Lo, and G. Chen, "Cryptanalysis Of An Image Scrambling Scheme Without Bandwidth Expansion," IEEE Transactions on Circuits and Systems for Video Technology, vol. 18, no. 3, pp. 338–349, 2008.*
4. *Mamta Jain and Saroj Kumar Lenka, "Diagonal queue medical image steganography with Rabin cryptosystem" Brain Informatics (2016) 3:39–51 DOI 10.1007/s40708-016-0032-8*
5. *M. Somasundaram, S.Gitanjali, T.C.Govardhani, G. Lakshmi Priya and R. Sivakumar, "Medical Image Data Management System in Mobile Cloud Computing Environment" 2011 International Conference on Signal, Image Processing and Applications With workshop of ICEEA 2011*
6. *Gupta,R.,Bisht,J. 2013.Colour Image Encryption and Decryption by using Scan Approach. In International Journal of software & Hardware Research in Engineering, Volume 1 Issue 2.*
7. *Younes,M.A.B and Jantan,A. , 2008. Image Encryption Using Block-Based Transformation Algorithm. In International Journal of Computer Science(IAENG),.*
8. *Yun-peng,Z., Wei,L., Shui-ping,C., Zheng-jun,Z., Xuan ,N.,Wei-di,D., 2009. Digital image encryption algorithm based on chaos and improved DES.In IEEE International Conference on Systems, Man and Cybernetics.*

9. *Seyedzade,S.M., Atani,R.E. and Mirzakuchaki,S., 2010. A Novel Image Encryption Algorithm Based on Hash Function. In 6th Iranian Conference on Machine Vision and Image Processing*
10. *Chang CC, Tseng HW (2004) A steganographic method for digital images using side match. Pattern Recogn Lett 25(12): 1431–1437p*