International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 1(06), November 2022, pp. 34-41
Article Title: Advanced Cryptographic Techniques for Cloud Security in Medical Application

Advanced Cryptographic Techniques for Cloud Security in Medical Application

C. Umadevi

Department of Electrical and Electronics Engineering, Government College of Engineering, Tirunelveli, Tamilnadu, India
umadevi.c19@gmail.com

ABSTRACT

In today's healthcare data systems, diagnostics heavily rely on medical imaging data. Healthcare image data are now kept securely on servers owned by third parties thanks to the adoption of cloud computing techniques in the healthcare industry by the majority of healthcare organisations. Each virtual piece of data should be safeguarded in confidentiality, security, and privacy through the use of authentication techniques and decryption to maintain security. In this arena, digital file encryption process and watermarking approaches have to be 100 percent recoverable. Due to the sensitive nature of the information provided in medical photographs, the involved basic simple image information in the cryptography and watermarking procedures should have been entirely recoverable. We suggested a completely reversible encoded and watermarked image solution for the safety of healthcare pictures in health data systems in order to fulfill the recoverability and creates a safe and encrypted in this research. Our findings revealed that the method was very efficient and accurate for fully accessible photos when employed to identify and safeguard the clinical data in health data systems.

Keywords: Health image data, heath data system, security, privacy, clinical data.

1 Introduction

Due to the sensitive nature of the files generated through time in regards to medication histories, hospital information, etc., health data systems play a crucial role in a nation's information technology systems. Health information that is stored over period can be safe, private, and secure. This information can show how patients are doing, how well they respond to treatments over time, how resistant they are to them, and how their genetic makeup changes over time. Such data's spatial profile can reveal a wealth of data regarding the state of one's health, epidemics, the efficiency of healthcare provision, etc. Medical imaging has taken over a significant portion of the healthcare system and is now a significant component of the majority of medical testing, including x-rays, ultrasounds, and other similar technologies. Improvements in health-care-related information systems with a focus on tele-medical operations, remote medical services, and online storage architectures for the medical sector incorporating data from medical imaging as a core element. There are now more chances in the industry of software development due to the significance and importance of providing health-care services.

The transmission of medical care could now be performed more quickly and efficiently thanks to this software programme. Efficacy in the medical industry is important since it allows for quicker access to information thanks to how health records are organised in health centers. This has emerged as a significant turning point in the development of medical science, allowing for some further development in the field of surgical interventions governed by detectors and intelligent systems, as well as the emergence of increasingly sophisticated technical diagnostic equipment for pre-medical processes that include evaluation and evaluation. As a consequence of advancements in development in signal analysis and visualisation of interior organ systems, the health care sector has seen a higher connection of imaging technology. The health industry has benefited enormously from this development. The delivery of medical services across the world is being revolutionised by the implementation of reliable information technologies for healthcare experts in real-time clinical operational processes. The research of adverse reactions to drugs has become more efficient thanks to the use of artificial intelligence approaches like learning algorithms, data mining, and knowledge discovery methods in the health care industry. Geographic profiling has also gotten simpler and more thorough as a result of hospital data on disease outbreaks. This highlights the importance of data systems as a key component of essential cybersecurity in the modern cyber domain. Numerous advantages are offered by these medical systems, which also facilitate the prompt and efficient delivery of medical care. A corrupted health data system can have disastrous effects for both the host and the customers of such networks, despite the numerous advantages of health-related data systems that have been highlighted previously as vital element of development in modern life. The frequency of cyber-attacks on vital infrastructure, including the healthcare system, has led to major worries about the safety, confidentiality, and protection of data systems. The incorporation and transfer of health care system data to third-party organizations for commercial, public, or combination cloud computing might present a number of difficulties for the safety, private, and confidentiality of the preservation of such information. In the context of the connection between the patient and the medical provider, information safety concerns such as security, confidentiality, and preservation are crucial. Accessibility control is a fundamental component of data information systems, particularly communications system protection for health-related systems. Authorization serves as the primary safety precaution for exterior information storage in cloud services settings. In order to protect data and keep it away from being accessed when in a communications system attack, it is crucial to use modern cryptography techniques. The authenticity and safety of clinical picture data stored in the cloud as well as for health-related information systems ensure efficient security measures. For reasons of privacy, access to health-care data must be verified by authentication methods. Because of the sensitive nature of the image files and the significance of the message provided by the information in the picture, and because a destruction of datasets in the method will face a lot of problems, these initiatives to safeguarding clinical data must be fixable, require little computing time, and have reusability of information throughout the total process of securing data within the system. We presented a

method for clinical photographs in order to effectively address some of the problems that health care systems face with respect to data security, confidentiality, and safety. We were able to obtain full recoverability and process reusability by combining the watermarking and encryption approaches. Other security protocols including tamper detection, identification, and privacy for the health photos were also given. This increases the security of the data kept in such information systems. Section II, "Related Works," Section III, "Methodology," Section IV, "Results and Analysis," and Section V, "Conclusion" make up the paper's structure.

2 Literature Review

In the research of Usman, K. et al., they focused on pixel organization and arbitrary permutation-based medical image encoding for secure exchange. They used a randomized pixel recombination in their method, which had a quick computing time and [11]. In order to encode colour clinical data, Abokhdair, N.O. et al. combined the chaotic image and confusion approach. A 2D lower triangular map was utilised to jumble the values of the input image. Their strategy was resistant to attacks using brute force [2]. In their paper titled "A lossless encryption method for medical images using edge maps," Yicong Zhou et al. demonstrated a brand-new flawless technique called Edge Crypt to encode clinical data using the data found in an edge map [3]. The outcomes of their labour are shown in the table below.

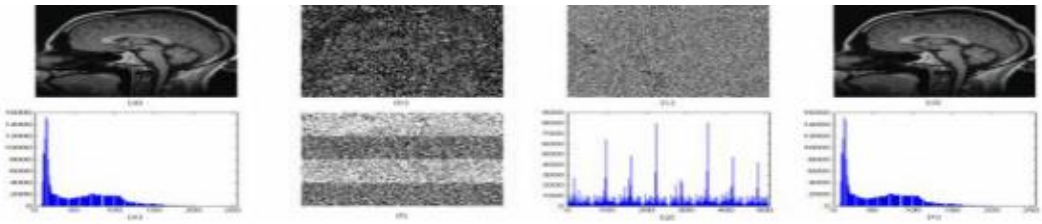


Figure 1: *The proposed system's architecture MRI image encryption (a) The original MRI image; (b) The edge map obtained by Sobel edge detector with threshold 0.3; (c) The encrypted MRI image, (d) The reconstructed MRI image, (e) Histogram of the original MRI image; (f) The encrypted edge map, x (0)-0.6.1-3.65: (g) Histogram of the encrypted MRI image, (h) Histogram of the reconstructed MRI image*

Other publications include "Chaos-Based Medical Image Encryption Using Symmetric Cryptography" by M. Ashtianict [5], "Transmission and storage of medical images with patient information" by R. Acharya U, P et al [41], etc. Discussion of our strategy is provided in the section below.

3 Methodology

Documentation on patients is contained in medical data that are maintained in health care systems, the network, and with third-party internet services. The confidentiality of patients will be violated by a corrupted health-care information system or unapproved exposure to these

information, and incorrect image analysis for multiple patients would further threaten the reliability of the healthcare facility. In the healthcare industry, medical image privacy, confidentiality, and protection are of utmost importance. Health records contained in medical databases will be kept private, secure, and legitimate by collecting data authenticity and integrity of the images. We provide a highly secured data system that uses a completely reversible and reproducible approach for medical picture identification and safety to address the issues of unauthorised access in medical data system.

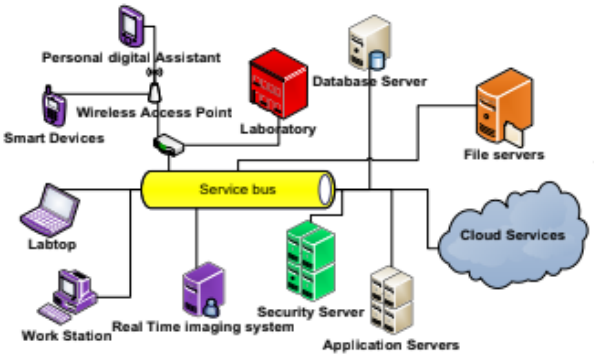


Figure 2: *The Proposed System's Architecture*

Patients' personal data is used in the data cryptography and watermarking of the medical data, which employs the patient's authentication systems to provide authorization. Before storing the generated data in data centers or cloud systems, we ensure the safety server had an operational activity function that effectively provided secrecy and access control for system clients. The watermarking labeling strategy used in the symmetric safeguard was in the feature space and

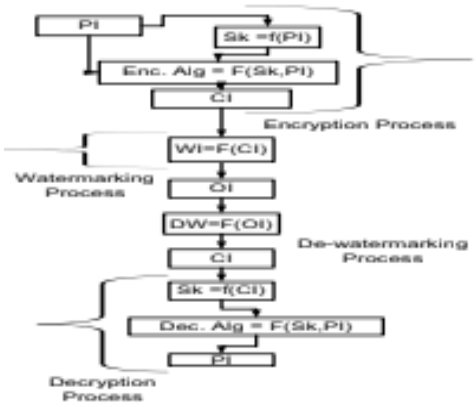


Figure 3: *Summary of the process*

it gives verification. With the suggested method, different parties can easily access medical information such as x-ray image data, ultrasound scan papers, etc. by communicating on the same service bus. Any demand for healthcare pictures made by an operation located within the

same communications infrastructure or outside of it will still have services offered to it via a higher level of abstraction specific to that operation. Only exchange activities that involve the safety server can effectively obtain and decrypt data stored in data centres, datasets, and the cloud, preventing the access of personal medical information in the event that file systems are compromised or online storage servers have now been made accessible through a hack door.

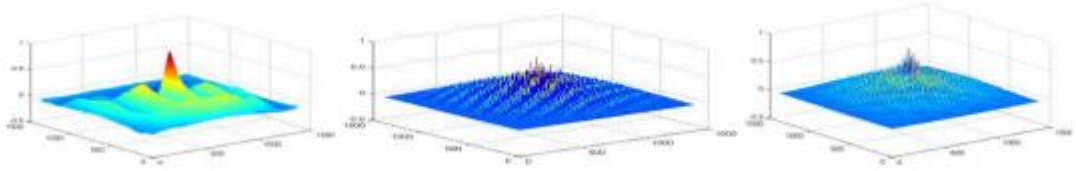
4 The Encryption Process

a) Import data from image and create an image graphics object by interpreting each element in a matrix
b) Get the size of r as [c, p]
c) Get the Entropy of the plain Image
d) Get the mean of the plain Image
e) Compute the shared secret from the image
f) Engage SK for g) to q) using secret key value
g) Extract the red component as ‘r’
h) Extract the green component as ‘g’
i) Extract the blue component as ‘b’
j) Let r =Transpose of ‘r’
k) Let g =Transpose of ‘g’
l) Let b =Transpose of ‘b’
m) Reshape r into (r, c, p)
n) Reshape g into (g, c, and p)
o) Reshape b into (b, c, and p)
p) Concatenate the arrays r, g, b into the same dimension of ‘r’ or ‘g’ or ‘b' of the original image
q) Finally the data will be converted into an image format to get the encrypted image

5 Online License Transfer

Times Roman or Times New Roman may be used where Times is required. Please select the typeface that most closely resembles Times if neither option exists on your word document. If at all feasible, resist utilizing bit-mapped typefaces. Fonts in Truc-Type 1 or Open Type are recommended. Please incorporate math and other symbol fonts as well. The technique was used to encode three samples of healthcare photos, and the results are shown below. The first 10,000 pixel values of both the normal and decrypted images were used to plot the RGB graphs in figures 5 to 9.

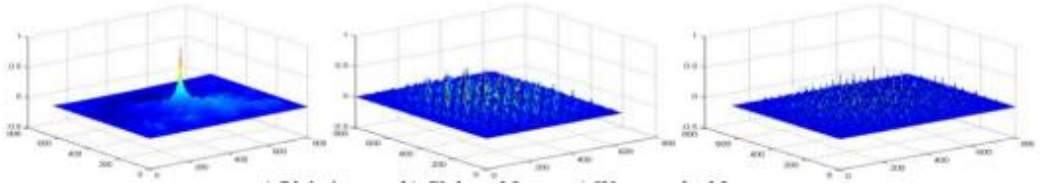
Figure 4: *X-ray image of the ribs a) Plain image b) Ciphered image c) Watermarked image*



a) Plain image b) Ciphered image c) Watermarked image

Figure 5: *The graph of the normalized cross-correlation of the matrices of the plain, ciphered and watermarked image of the X-ray Image*

Figure 6: *Ultrasound image of the womb a) Plain image b) Ciphered image c) Watermarked image*



a) Plain image b) Ciphered image c) Watermarked image

Figure 7: *The graph of the normalized cross-correlation of the matrices of the plain, ciphered and watermarked image of the Ultrasound Image*

a) Plain image b) Ciphered image c) Watermarked image

Figure 8: *Magnetic resonance imaging of the brain*

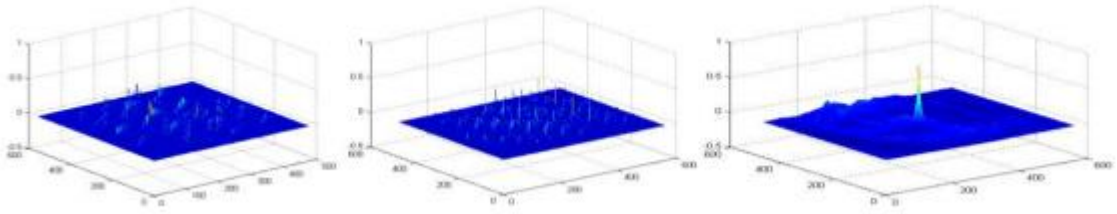


Figure 9: *The graph of the normalized cross-correlation of the matrices of the plain, ciphered and watermarked image of the MRI image*

Table 1: *Analysis of Plain, ciphered and watermarked image*

	Entropy(p)	*Arithmetic mean(m)*
XPI	7.1726	143.5284
XEI	7.1726	143.5284
XWI	5.6501	195.9501
UPI	3.7603	18.5810
UEI	3.7603	18.5810
UWI	4.5300	97.8801
MPI	4.6894	39.0415
MEI	4.6894	39.0415
MWI	4.9291	112.6501

From the table: PI=X-ray plain image; XEI=X-ray encrypted image; XWI=X-ray watermarked image; UPI=Ultrasound plain image; UEI=Ultrasound encrypted image; UWF=Ultrasound watermarked image; MPI=Magnetic Resonance Imaging Plain Image; MEI= Magnetic Resonance imaging encrypted image; MWI=Magnetic Resonance Imaging watermarked image

6 Conclusion

There wasn't any pixel enlargement at the conclusion of the operation, indicating that the approach used was quite efficient in all of the photos. For such photos in, the average and mean values were computed as displayed in the table above. For all of the decrypted images and the plain pictures, the overall average and the mean of the simple pictures remained constant. In other words, the total average pixel values before encoding and after encrypted were both the same. However, the pixel value changed as a result of the watermarking procedure.

References

1. Usman Koredianto; Hiroshi Juzoji; Isao Nakajima; Soegijardjo Soegidjoko; Mohamad Ramdhani; Toshihiro Hori; Seiji Igi, Year: 2007, "Medical Image Encryption Based on Pixel Arrangement and Random Permutation for Transmission Security, Health Networking, Application and Services", 2007 9th International Conference, pp.244.247.

2. Abokhdair Nuha Omran; Azizah Bt Abdul Manaf; Mazdak Zamani, Year: 2010,"Integration of chaotic map and confusion technique for colour medical image encryption," Digital Comment, Multimedia Technology and its Applications (IDC), pp.20.23.

3. Zhou Yicong; Karen Panetta; Sos Agaian, Year: 2009, "A lossless encryption method for medical images using edge maps," Engineering in Medicine and Biology Society, EMBC 2009 Annual International Conference of the IEEE, pp. 3707.3710.

4. Acharya Rajendra; P. Subbanna Bhat; Sathish Kumar; Lim Choo Min, Year: 2003, "Transmission and storage of medical images with patient information", Computers in Biology and Medicine, Vol. 33, no. 4, pp.303-310.

5. Ashtiyani Meghdad; Parmida Moradi Birgani; Hesam M. Hosseini, Year: 2008, "Chaos-Hansed Medical Image Encryption Using Symmetric Cryptography, Information and Communication Technologies: From Theory to Applications 2008, pp. 1-5.