International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT23903143

Secure Object Detection with Disease Diagnosis in Medical Images Using CNN With Asymmetric Algorithm

Mr. R. Krishnakumar[1], Dr. K. Chandramohan[2], Mr. K. Venkatesan[3], Ms. P. Vaishanvi[4]

[1]Assistant Professor, Department of CSE, Gnanamani College of Technology, Namakkal, Tamilnadu, India
[2] Professor, Department of CSE, Gnanamani College of Technology, Namakkal, Tamilnadu, India
[3] Assistant Professor, Department of CSE, Gnanamani College of Technology, Namakkal, Tamilnadu, India
[4] PG Student, Department of CSE, Gnanamani College of Technology, Namakkal, Tamilnadu, India

ARTICLEINFO

Article History:

Accepted: 10 June 2023
Published: 27 June 2023

Publication Issue
Volume 9, Issue 3
May-June-2023

Page Number
597-604

ABSTRACT

Security is the most critical issue amid transmission of medical images because it contains sensitive information of patients. Medical image security is an essential method for secure the sensitive data when computerized images and their relevant patient data are transmitted across public networks. Sensitive images carry extensive important information and different features compared to standard images. Medical images have much more sensitive and essential information than any other digital image. Each pixel in the image can be necessary for the diagnosis process, and any deformation can result in a faulty diagnosis. The most robust securing of these images affects an image to the extent that it can be ignored; this is different from insensitive imagery as the border of redundancy is very low. The embedding capacity in medical images is deficient. Existing researchers present different data security techniques as cryptography and data hiding to guarantee data verification. But these approaches take more time and less security in medical image application. So in this project, implement Fragmented based Elliptical curve cryptography with Convolutional neural network algorithm to provide secure disease diagnosis system for medical images. Experimental results shows that the proposed system implemented Lung CT scan images that are collected from Open medical data sources and with high level security.

Keywords : Medical Image Sharing, Disease Prediction, Data Hiding with Fragmentation, Least Significant Bit (LSB) Technique, Multi Secret Sharing, Elliptic Curve Cryptography (ECC).

I. INTRODUCTION

MEDICAL IMAGE IN CLOUD

Medical imaging is the technique of creating images of the inner organs of the human body for clinical analysis and medical assistance. With radiography, Medical Resonance Imaging (MRI), ultrasound and many other medical imaging techniques available in the healthcare sector, it is the responsibility of the healthcare industry to keep their patient information safe, and accessible. The standard image storing systems in the healthcare sector are PACS (picture archiving and communication systems) and VNA

(Vendor-Neutral Archives). They archive digital imaging from MRIs, X-Raysetc. after a certain period has passed. PACS has an archive option and VNA is used to integrate image files from various PACS into a centralized and cross-platform storage space. With cloud storage, in just the stroke of a button, you are able to deploy complex algorithms that otherwise would have cost huge (for servers and devices) for the industry.

Quality of the images – As these images are very important to both the patient and doctor, it is crucial that they are stored and retrieved as high-definition. Healthcare providers in remote areas have limited access to decent Internet connection. Both quality (of the image) and speed (of the Internet) are essential when a doctor wants to retrieve, say, a radiology image for evaluation.

Security – One cannot complain if some executives in the healthcare sector are reserved about moving to the cloud.Increasing vulnerability to data breaches is a major concern and if the health system is prone to it, most of them won't even consider switching to the cloud. Having said that, an on-premise data centre is vulnerable to damage due to natural disasters, but cloud services will not be affected by any such physical disasters. However, during any cyber-attacks, the on-premise image storage might prove crucial. The cloud can actually recover easier as they are multi- region. As the cloud offers vast functionality, it is always advisable for the healthcare sector to opt for it, making sure that all the data is secure.

Information sharing – If a healthcare provider is not into using cloud for any of its purposes, then it is, undoubtedly, locked behind a virtual private network (VPN) and firewalls of an on-premise system. This takes huge effort and time for the personnel there to retrieve any records or medical images – a doctor will have to email the radiologist, they have to confirm, there might be some more communication going on until the doctor gets the required medical image. This lengthy and time-consuming process will take place for each patient. Entry of cloud will only ease everything, as one will not have to go through the above process to access a medical image or record.

IMAGE PROCESSING IN HEALTHCARESYSTEM

The machine learning algorithm performs a series of preprocessing operations on the initially obtained data and then extracts part of the data from the data generated after the preprocessing program is completed according to the opinions of experts. At the same time, select appropriate data from the data set as the characteristics of the image. After completing a series of operations, the image modeling work is completed by a specific function.

(1) Disease diagnosis - In the field of medical diagnosis and treatment, medical diagnosis is one of the most common medical activities. Medical disease diagnosis also provides a large amount of analytical data for machine learning, which provides conditions for machine learning in the field of medical diagnosis. Machine learning obtainscertain data results by sorting out and analyzing a large amount of medical data. Then, a disease diagnosis model is established through machine learning methods, which can provide medical diagnosis assistance to medicaldiagnosticians.

MULTI SECRET SHARING WITH CRYPTOGRAPHY

Data exchanged over the Internet is in the form of images, audio, video, text, handwritten text, graphic objects, animations etc... The media used in data exchange is unreliable and insecure. Security of the digital media has become an important topic as it can be copied and modified easily. Cryptography is one of the techniques, which can be used for security of exchanged data. It ciphers the plain text to make it as cipher text, which is actually communicated through the communication media so that intruders even if obtain the cipher text do not be able to decipher the original information hidden within the cipher text. The examples of cryptography are Data Encryption Standard (DES), triple DES (3DES), Advanced

Encryption Standard (AES), and Blowfish in which encryption and decryption are done by same key. RSA is another popular algorithm for asymmetric cryptography in which encryption and decryption are done using different keys. Images are a vital form of multimedia contents, which are extensively exchanged over the Internet. So, there should be a secure and simple way to exchange images through any unsecured medium. In order to protect the image contents, Visual Cryptography (VC) is proposed. Using VC, a user can identify confidential data without any computation. In (k, n)-VCT, n shares (shadow images) of the secret image are generated during encryption and are sent through any untrusted medium.

II. RELATED WORK

Qayyum, Adnan et al,…. [1] Presented an overview of various application areas in healthcare that leverage such techniques from security and privacy point of view and present associated challenges. In addition, we present potential methods to ensure secure and privacy- preserving ML for healthcare applications. Present a comprehensive survey of existing literature on the security and robustness of ML/DL models when used for building healthcare systems with a specific focused on the above- mentioned dimensions. Here note that the aim of this work is to provide an in-depth survey of various security challenges associated with the application of ML/DLin healthcare systems and to provide a taxonomy of potentialsolutions to overcome these issues.

Masood, Fawad et al,…. [2] Implemented a lightweight cryptosystem based on Henon chaotic map, Brownian motion, and Chen's chaotic system to encrypt medical images with elevated security. Here designing an effective multi-stage cryptographic algorithm for medical images encryption using substitution-permutation technique.This multi-stage cryptographic algorithm uses random numbers generated from chaos maps which reduces correlation among the pixels of the digital medical images. Then design a contemporary variant of the chaos-based confusion-diffusion approach that is capable of achieving significant higher entropy and NIST-based randomness results as compared to existing methods. The results demonstrate that the proposed encryption algorithm is able to generate highly secured medical encrypted images.

Hasan, Mohammad Kamrul et al,…. [3] Present an efficient, lightweight encryption algorithm for providing secure image encryption in healthcare industry. The proposed lightweight encryption technique employs two permutation techniques to secure medical images. Besides, picture-based information requires more exertion during encryption and decryption. A change procedure dependent on the mix of picture stage and a recently evolved encryption calculation called "Hyper Image Encryption Algorithm (HIEA)". From the chose picture, we will utilize the twofold worth squares, which will be reworked into a permuted picture using a change procedure, and afterward, the produced picture will be encoded utilizing the "Hyper Image Encryption Algorithm (HIEA)" calculation. All the current strategies utilizing the reasonable client characterized key is created with a similar goal.

Aparna, Puvvadi et al,…. [4] Propose a biometric-based on an efficient medical image watermarking in E- healthcare application, which produces a system for authentication, confidentiality, and reliability of the system. The proposed system utilises the fingerprint biometric for authentication, cryptography process for confidentiality, and reversible watermarking for the integrity. Basically, the proposed system consists of two stages such as (i) watermark embedding process and (ii) watermark extraction process.

Kamal, Sara T et al,…. [5] Presents a new encryption algorithm for encrypting both grey and color medical images. A new image splitting technique based on image blocks introduced. Then, the image blocks scrambled using a zigzag pattern, rotation, and

random permutation. Then, a chaotic logistic map generates a key to diffuse the scrambled image. Different algorithms for securing medical images are introduced, yet they may be liable to attacks. A strong correlation between neighboring pixels characterizes medical images; thus, removing this correlation requires a permutation (scrambling) technique with a higher security level.

III.EXISTING SYSTEM

Medical image based object detection has been considered to be an ideal approach to assist medical diagnosis. Doctors can utilize the automatic detection resultsof medical images to obtain further insights into the patient- specific pathological features and make a more accurate diagnosis. For medical image privacy, current research mostly concentrates on data storage privacy and cannot support online calculations. The problem of the method is that when applying the medical image data into Faster RCNN, we still have to query and download the data to a local server, which can dramatically reduce data availability and computational efficiency. To overcome this problem, schemes based on homomorphic encryption (HE) and garbled circuit (GC) have been proposed. However, HE and GC are both computation-intensive and memory-intensive algorithms. For most real-world applications, the overheads caused by these methods are almost intolerable. Additionally, differential privacy (DP) is also a popular technique for the privacy preservation of deep learning models. Implementing DP only requires few computations to generate random perturbations. However, the accuracy reduction caused by the introduction of random perturbations is quite considerable. CNN allows multiple healthcare centers to securely share their medical image data and collaborate to build a high-performance Faster CNN model to assist in clinical diagnosis. During the cooperation process, no healthcare center has to worry about their own data revealed to other healthcare centers or the cloud server.

IV.PROPOSED SYSTEM

Proposed system provides secure medical image sharing with traitor tracing in the encrypted cloud media center. Privacy, integrity, and robustness for the extracted information are important security issues because deep learning enables object detection in images. The Health CareCenter (HCC) holds a large volume of medical data and wants to use the cloud for media hosting and sharing. With the continuous development of deep learning technologies, object detection techniques in the medical field have been widely used in many practical medical diagnostic applications. In this project we can implement diagnosis system for Lung images for detecting disease named as COVID or Not. Disease can be predicted using features extraction based CNN algorithm and also hide the disease details in Scan images using LSB coding. Watermarks are required to be securely embedded the medical image features into the image using LSB technique. To prevent data leakage and unauthorized access, the HCC will apply Multi Secret Sharing approach with ECC (Elliptic Curve Cryptography). To share the medical image with an authorized user, the HCC will send the cloud a decryption key to delegate the decryption right. In the Re-encryption key and watermark generation stage, upon receiving the request from a certain user, the HCC produces a watermark (Decryption Key). On receiver side both the decryption key and watermark information could be validated. The authorized user shall be allowed to accessing media object and do not support redistribution process.

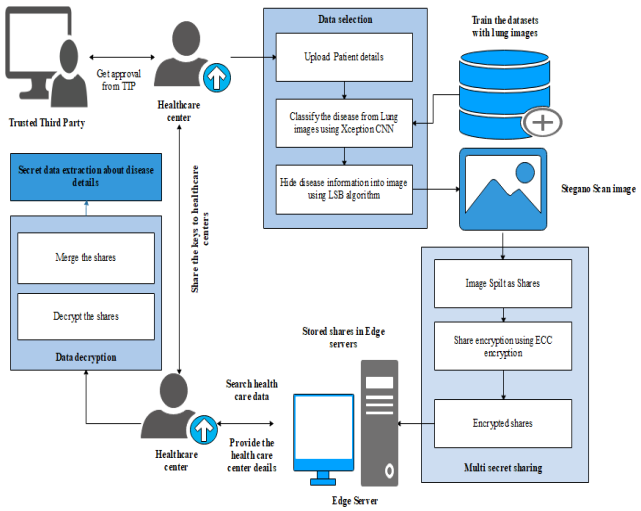

Fig 4.1 Proposed System Architecture

V. IMPLEMENTATION

Framework Construction

A cloud framework is a set of technologies, standards, and guidelines that provide a common frameworkfor building and deploying cloud computing solutions. Cloud frameworks help organizations to standardize and automate their cloud computing processes, making it easier to develop, deploy, and manage cloud-based applications and services. In this module, we can design health care centers, trusted third party and edge server. Health care center uploads the patient data and edge server can maintain all details. Trusted third party can be approving the health care center and edge server.

Features Extraction

Image feature extraction refers to the process of retrieving important information from an image and representing it in a compact and descriptive manner. The goal of image feature extraction is to reduce the high- dimensional image data to a lower-dimensional representation while preserving the important information that distinguishes one image from another. In this module, extract the features from medical images and features are such as colour, shape and textures in uploaded lung images.

Disease Prediction

Disease prediction using Convolutional Neural Networks (CNNs) is a commonly used approach in medical imaging for diagnosing and classifying diseases based on visual examination. In this approach, a CNN is trained on a large dataset of medical images, along with their corresponding labels, to learn the patterns and features that are indicative of specific diseases. The trained model can then be used to make predictions on new, unseen medical images by processing them through the network and outputting a probability score for each possible disease classabout lung diseases.

Convolutional Neural Network Algorithm

A CNN consists of multiple hidden layers and an input and an output layer. Hidden layers in a CNN consist of convolutional layers, pooling layers, fully connected layers and normalization layers. The input (in our case) is the target image to be classified and the output is the context of the bird nest within the image. In addition, there is a cost function used to find the most fitted set of parameters and activation functions to determine the final output.

Input: Labeled training images
Output: Classified Disease
Processing Steps:

Constructing the CNN Model

function INITCNNMODEL (θ, [n1–5])

layerType = [convolution, max-pooling, fully-connected, fully-connected];

layerActivation = [tanh(2), max(),softmax()]
model = new Model();

for$i$=1 to 4 do

layer = new Layer(); layer.type = layerType[i];layer.inputSize = ni

layer.neurons = new Neuron [ni+1];
layer.params = θi;
model.addLayer(layer);

end for return
model;end function

Training the CNN Model

Initialize learning rate α, number of maximum iteration ITERmax, minimum error ERRmin, training batchesBATCHEStraining, batch size SIZEbatch, and so on;Compute $n2$, $n3$, $n4$, $k1$, $k2$, according to $n1$ and

$n5$;

Generate random weights θ of the CNN; cnnModel = InitCNNModel(θ, [$n1$–5]); iter = 0; err = +inf;

while err >ERRmin and iter<ITERmax doerr = 0;

forbach = 1 to BATCHEStraining do
[$\nabla\theta J(\theta)$, $J(\theta)$] = cnnModel.train (TrainingDatas, TrainingLabels), as (4) and (8); Update θ using (7);

err = err + mean($J(\theta)$);

end for err = err/BATCHEStraining;
iter++;

end while

Save parameters θ of the CNN

Data Hiding With Fragmentation

In this module, detected disease details can be hiding into scan image using least signification bit and named as Stegno image. LSB (Least Significant Bit) based hiding is a technique for hiding digital information within animage by modifying the least significant bits of the pixel values. The idea is to replace the least significant bits of the pixel values with the binary representation of the hidden information, such that the change in the pixel values is visually imperceptible to the human eye. And also split the stegno image into multiple parts

LSB for Data Hiding

This is the simplest of the steganography methods based in the use of LSB, and therefore the most vulnerable Embedding process consists of the sequential substitution of each Least Significant Bit (LSB-1) of the image pixel for thebit message. For its simplicity, this method can camouflage a great volume of information.

The guidelines are given below:

Step1: Convert the data from decimal to binary.

Step 2: Read cover image.

Step 3: Convert the cover Image from decimal to binary.

Step 4: Break the byte to be hidden into bits.

Step 5: Take first 8 byte of original data from the cover Image.

Step 6: Replace the least significant bit by one bit of the data to be hidden.

First byte of original information from the Cover image:

E.g.:-1 1 0 11 0 0 0

First bit of the data to be hidden: 1
Replace the least significant bit

This process will be continued for first 8 byte of data and conceal the first byte of data.

Step 7: Continue the step 6 for all pixels.

Data Encryption

In this module splited image parts encrypted using Elliptical curve cryptography. Image encryption using Elliptic Curve Cryptography (ECC) is a method for securingdigital images by encrypting the image data using mathematical algorithms based on elliptic curve theory. ECC is a public-key cryptography system, which means thatit uses two keys - a public key and a private key - to encrypt and decrypt data. In image encryption using ECC, the image is first transformed into an encrypted format using a public key, which can then only be decrypted using the corresponding private key. The encrypted image can then betransmitted over the internet or stored in a secure location without the risk of unauthorized

access or tampering. These details are stored in edge servers.

Elliptical Curve Cryptography

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. Elliptic curves are an algebraic structure and their use for cryptography. They feature properties which allow the setup of a problem similar to the well-known discrete logarithm problem of finite fields –also known as Galois fields (GF).ECC includes key agreement, encryption, and digital signature algorithms. The key distribution algorithm is used to share a secret key, the encryption algorithm enables confidential communication, and the digital signature algorithm is used to authenticate thesigner and validate the integrity of the message:

GENERAL PROCEDURE OF ECC

- Both parties agree to some publicly-known dataitems
- The elliptic curve equation
- Values of *a* and *b*
- Prime, *p*
- The elliptic group computed from the elliptic curveequation
- A base point, B, taken from the elliptic group
- Similar to the generator used in currentcryptosystems
- Each user generates their public/private key pair
  - Private Key = an integer, x, selected fromthe interval [1, p-1]
  - Public Key = product, Q, of private keyand base point

$$(Q = x^*B)$$

Encryption

1. Define a Curve.
2. Generate public private Key pair using that curve, for both sender and receiver.
3. Generate a Shared secret key from the key pair.
4. From that shared secret key, generate an encryption key.
5. Using that encryption key and asymmetric encryption algorithm, encrypt the data to send.

Decryption

The sender will both share the curve with receiver or sender and receiver will have the equal use for the equal curve form. Also, sender will share its public key with receiver.

1. Generate public personal Key pair using thesame curve for that curve for receiver.
2. Regenerate a shared secret key utilizing private key of receiver and public key of sender.
3. From that shared secret key, generate an encryption key.
4. Utilizing that encryption key and symmetric encryption algorithm, decrypt the information.

Access the Medical Image Data

Access control refers to the methods and technologies used to regulate who or what is allowed to access a resource. In this module, health care centres request the medical in edge servers. And then request can be sent to corresponding health care centre. Encrypted splited parts send to health care centre and decrypt the parts using ECC private key. Merge parts and unhide the data from images.

VI. CONCLUSION

Secure medical image sharing approach with the combination of cryptography and watermarking

techniques was proposed for secure transmission of information through cloud. In this approach disease classification was performed using shared medical image (lung). Then LSB technique is used for watermarking and ECC cryptographyis used for share encryption purposes. The proposed technique is not only designed to medical data sharing; however, it is proposed to provide integrity and authentication services for the medical images. Therefore, its target is not to be robust against modification attacks, but its target is to detect any illegal data access. At the receiver side the proposed technique verifies the secret keys shared by HCC regarding illegal access tracing. Proposed techniques provide system authentication service, integrity service and shared information confidentiality service.

VII. REFERENCES

[1]. Qayyum, Adnan, Junaid Qadir, Muhammad Bilal, and Ala Al-Fuqaha. "Secure and robust machine learning for healthcare: A survey." IEEE Reviews in Biomedical Engineering 14 (2020): 156-180.

[2]. Masood, Fawad, Maha Driss, Wadii Boulila, Jawad Ahmad, Sadaqat Ur Rehman, Sana Ullah Jan, Abdullah Qayyum, and William J. Buchanan. "A lightweight chaos- based medical image encryption scheme using random shuffling and XOR operations." Wireless Personal Communications (2021): 1-28.

[3]. Shabana Habib, Mohammad Islam et al. "Lightweight encryption technique to enhance medical image security on internet of medical things applications." IEEE Access 9 (2021): 47731-47742.

[4]. Aparna, Puvvadi, and Polurie Venkata Vijay Kishore. "Biometric-based efficient medical image watermarking in E-healthcare application." IET Image Processing 13, no. 3 (2019): 421-428.

[5]. Kamal, Sara T., Khalid M. Hosny, Taha M. Elgindy, Mohamed M. Darwish, and Mostafa M. Fouda. "A new image encryption algorithm for grey and color medical images." IEEE Access 9 (2021): 37855-37865.

[6]. Patel, Vishal. "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus." Health informatics journal 25, no. 4 (2019): 1398-1411.

[7]. Li, Xin, and Dongxiao Zhu. "Robust detection of adversarial attacks on medical images." In 2020 IEEE 17th International Symposium on Biomedical Imaging (ISBI), pp. 1154-1158. IEEE, 2020.

[8]. Liu, Xiyao, Jieting Lou, Hui Fang, Yan Chen, Pingbo Ouyang, Yifan Wang, Beiji Zou, and Lei Wang. "A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images." Ieee Access 7 (2019): 76580-76598.

[9]. Zhou, Yi, Xiaodong He, Lei Huang, Li Liu, Fan Zhu, Shanshan Cui, and Ling Shao. "Collaborative learning of semi-supervised segmentation and classification for medical images." In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 2079-2088. 2019.

[10]. Li, Zhuoling, Minghui Dong, Shiping Wen, Xiang Hu, Pan Zhou, and Zhigang Zeng. "CLU-CNNs: Object detection for medical images." Neurocomputing 350 (2019): 53-59.

Cite this article as :

Mr. R. Krishnakumar, Dr. K. Chandramohan, Mr. K. Venkatesan, Ms. P. Vaishanvi, "Secure Object Detection with Disease Diagnosis in Medical Images Using CNN With Asymmetric Algorithm", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 3, pp.597-604, May-June-2023. Available at doi : https://doi.org/10.32628/CSEIT23903143

Journal URL : https://ijsrcseit.com/CSEIT23903143