IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ICRTTC '23
International Conference on Recent Trends and Technologies in Computing
Department of Computer Science and Engineering, Arasu Engineering College
Vol. 12, Special Issue 1, April 2023

Secure Object Detection with Disease Prediction in Medical Image with Secure Data Sharing

R. Vimli [1]

Department of Computer Science and Engineering, Arasu Engineering College, Kumbakonam, Tamil Nadu, India[1]

Abstract: Security is the most critical trouble amid transmission of medical image because it carries sensitive records of sufferers. Medical image protection is an important approach for at ease the sensitive information whilst computerized images and their applicable affected person data are transmitted across public networks. Sensitive photographs bring good sized essential statistics and exclusive features in comparison to standard images. Medical images have high more sensitive and essential information than some other digital images. Each pixel in the image may be important for the analysis method, and any deformation can bring about a defective prognosis. The strongest securing of these images impacts a picture to the quantity that it is able to be omitted; that is special from insensitive imagery as the border of redundancy may be very low. The embedding capacity in medical pictures is poor. Existing researchers present different statistics security strategies as cryptography and records hiding to assure information verification. But these procedures take greater time and much less safety in medical image software. So on this approach put in force Fragmented primarily based Elliptical curve cryptography with Convolutional neural community set of rules to offer at ease ailment analysis system for medical photos. Experimental effects indicate that the proposed system applied Lung CT experiment image which can be accumulated from Open clinical records sources and with excessive level security.

Index Terms: Framework Creation,Medical Image Sharing, Image Feature Extraction, Disease Prediction, Data Hiding, Image Fragmentation, Image Encryption, Verification and Access Data.

I. INTRODUCTION

1.1 MEDICAL IMAGE IN CLOUD

Medical imaging is the technique of making images of the inner organs of the human frame for scientific analysis and medical help. With radiography, Medical Resonance Imaging (MRI), ultrasound and lots of other scientific imaging strategies available in the healthcare area, it's miles the obligation of the healthcare enterprise to hold their affected person records safe, and on hand. The image storing structures inside the healthcare area are PACS (picture archiving and communique structures) and VNA (Vendor-Neutral Archives). They archive virtual imaging from MRIs, X-Rays etc. After a certain period has surpassed. PACS has an archive choice and VNA is used to combine picture files from diverse PACS right into a centralized and pass-platform storage space. With cloud storage, in only the stroke of a button, capable of install complicated algorithms that in any other case would have fee big (for servers and devices) for the enterprise.

Quality of the pics – As these image are very vital to each the patient and doctor, it's far important that they're saved and retrieved as high-definition. Healthcare companies in faraway regions have limited access to decent Internet connection. Both quality (of the image) and velocity (of the Internet) are essential whilst a health practitioner desires to retrieve, say, a radiology image for assessment.

Security – One cannot complain if a few executives in the healthcare quarter are reserved approximately moving to the cloud. Increasing vulnerability to statistics breaches is a chief situation and if the health machine is liable to it, most of them gained even don't forget switching to the cloud. Having said that, an on-premise statistics centre is susceptible to harm because of herbal screw ups, but cloud offerings will no longer be tormented by this sort of physical screw ups. However, at some stage in any cyber-assaults, the on-premise photograph garage would possibly show critical. The cloud can actually get better less difficult as they're multi-location. As the cloud offers significant capability, it's miles always really helpful for the healthcare sector to opt for it, making sure that everyone the statistics is comfortable.

Information sharing – If a healthcare issuer isn't into the usage of cloud for any of its purposes, then it's far, surely, locked behind a digital personal network (VPN) and firewalls of an on-premise machine. This takes huge effort and time for the employees there to retrieve any information or scientific photographs – a doctor will have to e-mail the radiologist, they need to affirm, there is probably some greater conversation taking place till the doctor receives the desired medical image. This prolonged and time-ingesting procedure will take area for each patient. Entry of cloud will handiest ease the whole thing, as one will not should undergo the above procedure to access to a medical photo or report.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ICRTTC '23
International Conference on Recent Trends and Technologies in Computing
Department of Computer Science and Engineering, Arasu Engineering College
Vol. 12, Special Issue 1, April 2023

1.2 MULTI SECRET SHARING

A secret sharing (SS) scheme is a cryptosystem that encrypts a secret into more than one portion known as shares in order that only certified units of images can be employed to reconstruct the secret. Therefore the SS scheme is one of the most fundamental technologies to realize at ease access to manage. A normal example of secret sharing schemes is a (k, n)-threshold secret sharing scheme. In (k, n)-threshold secret sharing schemes, a key's encrypted into n shares in this kind of manner that any k or extra shares can be hired to reconstruct the name of the game, even as no k − 1 or much less shares leak any records about the secret. In the normal secret sharing schemes, secrets and techniques and shares are each numerical statistics and their encryption and decryption is performed by way of computer systems. In evaluation, there exist secret sharing schemes whose decryption does not require any numerical computations however may be finished by using a human. A visual secret sharing (VSS) scheme is an instance of such secret sharing schemes. In VSS schemes, secrets and shares are both visible statistics such as revealed texts, hand written notes, images and so on. The schemes encrypt a visible secret into visible stocks in order that humans can recover the visible secret with their eyes with the aid of superposing a certified set of visible shares published on transparencies.

Data exchanged over the Internet is in the shape of images, audio, video, text, handwritten text, photo objects, animations and so on... The media used in information trade is unreliable and insecure. Security of the digital media has emerge as an essential subject matter as it can be copied and modified effortlessly. Cryptography is one of the strategies, which can be used for safety of exchanged statistics. It ciphers the plain textual content to make it as cipher textual content, that is certainly communicated through the communiqué media so that intruders even if acquire the cipher text do not be able to decipher the authentic statistics hidden within the cipher text. The examples of cryptography are Data Encryption Standard (DES), triple DES (3DES), Advanced Encryption Standard (AES), and Blowfish wherein encryption and decryption are carried out by identical key. RSA is any other popular algorithm for asymmetric cryptography in which encryption and decryption are executed using special keys. Images are a essential shape of multimedia contents, that are considerably exchanged over the Internet. So, there have to be a comfortable and easy way to change pix through any unsecured medium. In order to guard the image contents, Visual Cryptography (VC) is proposed. Using VC, a person can pick out private facts with none computation. In (k, n)-VCT, n shares (shadow snap shots) of the secret image are generated at some stage in encryption and are sent thru any untrusted medium.
Out of n shares, any okay shares are just stacked/superimposed (logical OR operation or AND operation relying upon which color is taken into consideration which bit) on the recipient's side to get the original secret image back. Any much less than k shares might not regenerate the original secret image. The advantage of VCT over different cryptographical strategies used for other multimedia content material like textual content, audio, video is its decryption system, which does not involve any complicated calculations and computations however can handiest be executed with the aid of Human Visual System (HVS) i.e. Human eye. Furthermore, no key is required for encryption/decryption in VCT as in different cryptographic techniques. The fundamental elements of the VCT are contrast and safety.

1.3CRYPTOGRAPHY

Cryptography is the technology of the usage of arithmetic to encrypt and decrypt information. Cryptography enables you to shop sensitive records or transmit it throughout insecure networks (just like the Internet) so that it cannot be examine by absolutely everyone besides the meant recipient. While cryptography is the technological know-how of securing information, cryptanalysis is the technology of analyzing and breaking secure data exchange. Classical cryptanalysis involves an interesting mixture of analytical reasoning, utility of mathematical tools, sample finding, endurance, dedication, and luck. Cryptanalysts also are referred to as attackers.
Cryptology embraces each cryptography and cryptanalysis.

Cryptography is used in lots of packages like banking transactions playing cards, laptop passwords, and e- trade transactions.
Three varieties of cryptographic strategies utilized in trendy.
1. Symmetric-key cryptography
2. Public-key cryptography

1. Symmetric-key Cryptography:
Both the sender and receiver share a single key. The sender makes use of this key to encrypt plaintext and send the cipher textual content to the receiver. On the opposite side the receiver applies the same key to decrypt the message and get better the apparent text. With symmetric cryptography, the identical key's used for each encryption and decryption. A sender and a recipient need to have already got a shared key that is acknowledged to both. Key distribution is a tricky hassle and turned into the impetus for developing asymmetric cryptography. With uneven crypto, two extraordinary keys are used for encryption and decryption. Every user in an uneven cryptosystem has both a public key and a non-public key. The personal key is saved mystery always;however the public key can be freely dispensed.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ICRTTC '23
International Conference on Recent Trends and Technologies in Computing
Department of Computer Science and Engineering, Arasu Engineering College
Vol. 12, Special Issue 1, April 2023

2. Public-Key Cryptography:

The public key's used for encryption and for decryption personal key is used. Public-key cryptography, or uneven cryptography, is an encryption scheme that uses two mathematically associated, but not equal, keys - a public key and a private key. Unlike symmetric key algorithms that rely on one key to each encrypt and decrypt, every key plays a completely unique function. The public key is used to encrypt and the personal key's used to decrypt. It is computationally infeasible to compute the private key primarily based on the general public key. Because of this, public keys can be freely shared, permitting customers an clean and handy approach for encrypting content material and verifying virtual signatures, and private keys may be saved secret, ensuring best the owners of the personal keys can decrypt content material and create digital signatures.

II. RELATED WORK

Qayyum, 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. The ML techniques utilizing unlabelled data are known as unsupervised learning methods. Widely used examples of unsupervised learning methods are a clustering of data points using a similarity metric and dimensionality reduction to project high dimensional data to lower dimensional subspaces. The use of machine learning (ML)/deep learning (DL) models for clinical applications has great potential to transform traditional healthcare service delivery. However, to ensure a secure and robust application of these models in clinical settings, different privacy and security challenges should be addressed. Here provided an overview of such challenges by formulating the ML pipeline in healthcare and by identifying different sources of vulnerabilities in it. Finally discussed the potential solutions to provide secure and privacy-preserving ML for security-critical applications like healthcare.

Masood, 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. An enhanced image encryption scheme is proposed that combines chaos theory with Brownian motion (BM) and Chen's chaotic system (CCS) to achieve the desired level of security in storage systems of hospitals and medical centers. The proposed system achieves confusion through two-dimensional Henon chaotic map (HCM), whereas diffusion is obtained using BM and CCS. Furthermore, the reliability and security of the proposed system are analyzed and compared with existing techniques using the following parameters. The NIST and entropy measures are obtained through randomness test, the consistency and variance through histogram examination, and the pixel similarity using a coefficient of correlation. Other performance analysis parameters include energy, contrast, homogeneity, mean square error, peak to signal noise ratio, number of pixels changing the rate, unified average changing intensity, and computational complexity.

Hasan, 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. Likewise, separate between them with a proposed calculation utilized for encryption and decryption. For entropy esteem, connection worth, and execution time of the known cryptographic calculation with proposed cryptography calculations. The proposed lightweight encryption algorithm focused on the efficiency and security of the medical images on IoMT application. The proposed algorithm considered the performance matric of entropy, as well as correlation. The study has found that the current methods generated key based unsystematic sequence number that creates an enormous computation time. In comparison, it is evident from the result that the proposed algorithm has a small computation.

Aparna, 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 utilizes 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. The presented paper intends to reveal the potential of DWM in medical data management issues and propose a novel method to

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ICRTTC '23
International Conference on Recent Trends and Technologies in Computing
Department of Computer Science and Engineering, Arasu Engineering College
Vol. 12, Special Issue 1, April 2023

enforce integrity, authenticity, and confidentiality of the medical information, by embedding information bit to the medical image. In this study, at first, we segment the medical image using a region growing (RG) algorithm. Then we encrypt the region of interest (ROI) part using the SHA-256 algorithm. After that, we consider the electric healthcare recode (EHR), which is having important information about the patient. We have to encrypt the information using the elliptic curve cryptography (ECC) algorithm. Moreover, the proposed scheme is highly secure having several layers of security mechanisms. Watermarking by combining lossless data compression and encryption techniques, embedding of the watermark bits in the embedding region, all these aspects make the proposed scheme an effective novel MIW technique.

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. Here presents a new algorithm for encrypting medical images that include four parts: image splitting, image scrambling, key generation, and diffusion. First, the plain image is divided into blocks and sub-blocks using a new image splitting technique. Second, the pixels' arrangement is changed in the blocks and sub-blocks using a zigzag pattern, rotation at a 90-degree angle, and random permutation between blocks. Third, a key is generated from the logistic map, where the map's initial condition depends on the plain image. Finally, image pixel values are changed using the secret key. A new technique for image splitting is proposed. Random permutation between blocks is applied, and pixels substitution in each block is performed to remove the correlation between pixels. A logistic map is used to diffuse the scrambled image, where the map's initial condition is based on the plain image. Therefore, the proposed algorithm is robust against differential attacks. Analysis of the results proves that our algorithm gains a high performance in encrypting medical images than other methods.

III. EXISTING METHODOLOGIES

Medical image based object detection has been taken into consideration to be a perfect technique to assist medical analysis. Doctors can make use of the automated detection results of scientific images to reap similarly insights into the affected person-specific pathological features and make a extra correct diagnosis. For medical image privateness, current studies in general concentrate on information storage privacy and cannot assist on-line calculations. The hassle of the technique is that after making use of the scientific images facts into Faster RCNN, we nevertheless ought to query and download the facts to a nearby server that can dramatically lessen records availability and computational performance. To triumph over this problem, schemes primarily based on homomorphic encryption (HE) and garbled circuit (GC) had been proposed. However, HE and GC are both computation-intensive and reminiscence-intensive algorithms. For maximum real-world programs, the overheads as a result of those techniques are nearly insupportable. Additionally, differential privacy (DP) is also a popular approach for the privacy preservation of deep learning models. Implementing DL simplest requires few computations to generate random perturbations. However, the accuracy reduction because of the introduction of random perturbations is pretty considerable. CNN allows a healthcare centers to proportion their medical image data and collaborate to build a high-performance Faster CNN version to assist in medical diagnosis. During the cooperation process, no healthcare center has to fear about their very own facts discovered to other healthcare facilities or the cloud server.

IV. SECURE MEDICAL DATA SHARING USING ENCRYPTION WITH MULTI SECRET SHARING SCHEME

Proposed work presents secure clinical image sharing with traitor tracing inside the encrypted cloud media center. Privacy, integrity, and robustness for the extracted records are essential safety troubles due to the fact deep learning knowledge of enables object detection in photos. The Health Care Center (HCC) holds a large volume of medical data and desires to use the cloud for media web hosting and sharing. With the non-stop development of deep studying technologies, object detection strategies in the scientific subject were widely used in lots of practical clinical diagnostic packages. In this project we are able to enforce disease diagnosis for Lung image for detecting sickness named as COVID or Not. Disease can be anticipated using capabilities extraction based totally CNN set of rules and additionally cover the ailment info in Scan pix the usage of LSB coding. Watermarks are required to be securely embedded the medical image capabilities into the picture the use of LSB method. To save records from leakage and unauthorized access, the HCC will apply Multi Secret Sharing method with ECC (Elliptic Curve Cryptography). To share the medical image with a certified person, the HCC will ship the cloud a decryption key to delegate the decryption proper. In the Re-encryption key and watermark era stage, upon receiving the request from a positive person, the HCC produces a watermark (Decryption Key). On receiver facet both the decryption key and watermark facts can be demonstrated. The authorized consumer shall be allowed to accessing media item and do now not help redistribution system.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ICRTTC '23
International Conference on Recent Trends and Technologies in Computing
Department of Computer Science and Engineering, Arasu Engineering College
Vol. 12, Special Issue 1, April 2023

V. METHODOLOGY

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 iterationITERmax, 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 do
err = 0;
forbach = 1 to $BATCHES_{training}$ 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/$BATCHES_{training}$;
iter++;
end while
Save parameters θ of the CNN

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 the bit message. For its simplicity, this method can camouflage a great volume of information.

LSB Encoding

First the particular image and the encrypted secret message are taken. Then the encrypted secret data need to be transformed into binary format. Binary conversion is accomplished via taking the American Standard Code of Information Interchange (ASCII) values of the person and converting them into binary layout and producing move of bits. Message bits are taken and that are located in LSB bit of image byte. Same technique is accompanied until all of the message bits are located in image bytes. Image generated is called 'Stego-Image'. It is prepared for transmission through the Internet.
Algorithm for hiding mystery facts in Cover image:

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ICRTTC '23
International Conference on Recent Trends and Technologies in Computing
Department of Computer Science and Engineering, Arasu Engineering College
Vol. 12, Special Issue 1, April 2023

Step-1: Read the cover media image and secret information which is to be embedded in to the cover image.
Step-2: Compress the secret facts.
Step-3: Convert the compressed secrets into cipher textual content by means of using secret key shared by receiver and sender.
Step-4: Convert compressed encrypted textual content message into binary form.
Step-5: Find LSB values of each RGB pixels that found in cover image.
Step-6: Embed the bits of the secret data into bits of LSB of RGB pixels of the cover image.
Step-7: Continue the system till the name of the secret data is hidden into cover image.

LSB Decoding

First, 'Stego-Image' is taken and single array of bytes are generated as it become carried out at the time of encoding. The popular quantity of bits of encrypted secret information and the bytes representing the pixels of stego-image are taken. Counter is to begin with set to 1, which in flip offers the index variety of the pixel byte where secret message bit is available in LSB. The procedure is continued till very last secret message bit is reached. After this, the bit circulation of the message shall be generated. Available bits are grouped to shape bytes such that each byte represents single ASCII character. Characters are stored in text document which represents the encrypted embedded message.

Algorithm for unhiding secret data from Stego image:
Step-1: Read the stego image.
Step-2: Extract RGB values and find LSB bits of each pixel.
Step-3: Find and retrieve the LSBs of every RGB pixel of the stego image.
Step-4: Continue the process until the message is fully extracted from stegoimage.
Step-5: Decompress the extracted secret facts.
Step-6: Using shared key, decrypt secret records to get original records.
Step-7: Reconstruct the secret statistics.

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 the signer and validate the integrity of the message:

GENERAL PROCEDURE OF ECC

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

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ICRTTC '23
International Conference on Recent Trends and Technologies in Computing
Department of Computer Science and Engineering, Arasu Engineering College
Vol. 12, Special Issue 1, April 2023

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 the same 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.

PROCEDURE

FRAMEWORK CONSTRUCTION
A cloud framework is a set of technologies, standards, and guidelines that provide a common framework for 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 class about lung diseases.

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 an image 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.

DATA ENCRYPTION
In this module splited image parts encrypted using Elliptical curve cryptography. Image encryption using Elliptic Curve Cryptography (ECC) is a method for securing digital images by encrypting the image data using mathematical algorithms based on elliptic curve theory. ECC is a public-key cryptography system, which means that it 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 be transmitted over the internet or stored in a secure location without the risk of unauthorized access or tampering. These details are stored in edge servers.

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.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ICRTTC '23
International Conference on Recent Trends and Technologies in Computing
Department of Computer Science and Engineering, Arasu Engineering College
Vol. 12, Special Issue 1, April 2023

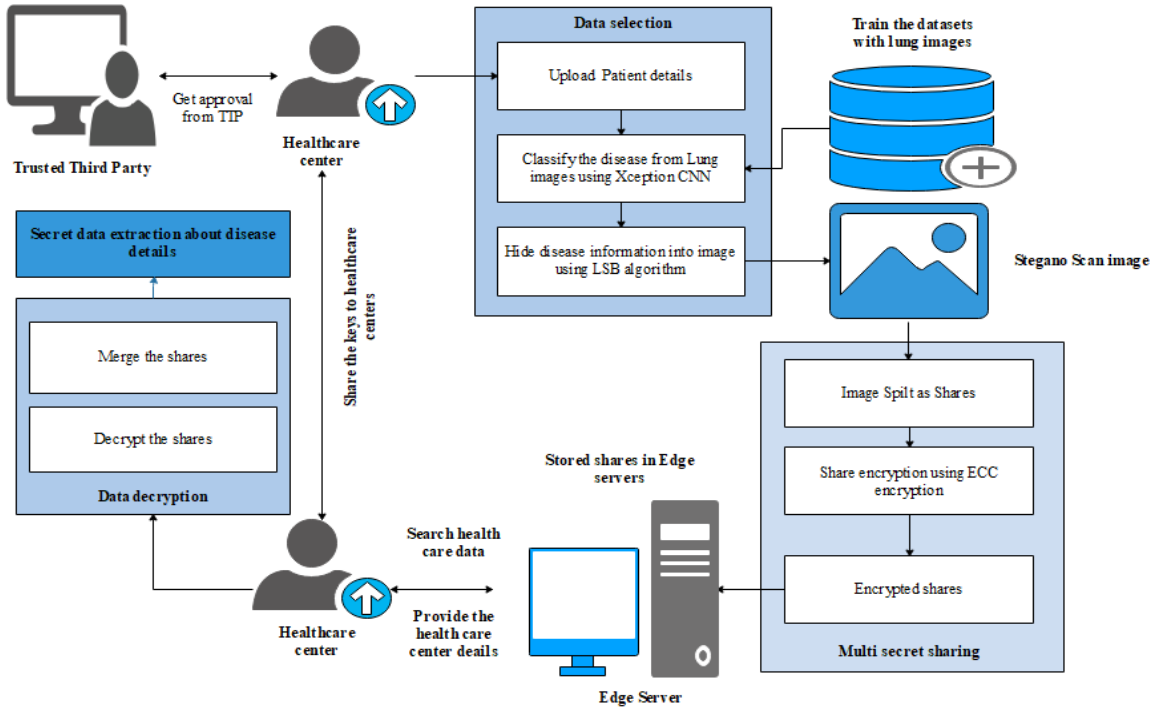

Fig 4.1: Architecture for Proposed Work

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 cryptography is 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.

REFERENCES

[1] Qayyum, Adnan, JunaidQadir, 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, MahaDriss, WadiiBoulila, 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] Hasan, Mohammad Kamrul, Shayla Islam, Rossila wati Sulaiman, Sheroz Khan, Aisha-Hassan Abdalla Hashim, 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, PingboOuyang, Yifan Wang, BeijiZou, 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 ZhigangZeng. "CLU-CNNs: Object detection for medical images." Neurocomputing 350 (2019): 53-59.