ENCRYPTION BASED SECURE MEDICAL IMAGE SHARING TECHNIQUE USING REVERSIBLE DATA HIDING AND DEEP LEARNING

Ekanathan SA, Madesh K, Rajasekar M.
Mepco Schlenk Engineering College,
Sivakasi, India.

Mrs. Blessa Binolin Pepsi M ME, Ph.D.
Mepco Schlenk Engineering College,
Sivakasi, India.

Abstract

This abstract discusses the secure sharing of medical images is of paramount importance in the healthcare industry, where sensitive patient information must be handled with utmost care. Medical images, such as X-rays, MRI scans, and CT scans, contain valuable diagnostic information, and their timely sharing between healthcare professionals can lead to improved patient outcomes. However, the transmission of such sensitive information can be vulnerable to cyber threats, which can compromise patient privacy and confidentiality. To address this issue, the proposed method employs robust encryption algorithms to ensure the confidentiality of patient information. Encryption involves transforming the medical image into a cipher text that is unreadable to unauthorized users. This step helps protect sensitive patient data from cyber threats and ensures that only authorized healthcare professionals can access the image. The Chinese remainder theorem is a mathematical principle that is used to enhance the security of transmitting the encrypted medical image. The theorem allows for the image to be broken down into smaller, more manageable parts that can be securely transmitted to the intended recipient. This approach also reduces the risk of data loss or corruption during transmission, making it a reliable and efficient method for sharing medical images. By combining encryption with the Chinese remainder theorem, healthcare professionals can securely and efficiently share medical images, leading to improved diagnosis and treatment of patients. This method ensures that patient privacy and confidentiality are maintained throughout the transmission process, adhering to the ethical and legal obligations of healthcare professionals. Overall, this approach can significantly contribute to the secure and reliable analysis of medical images while ensuring the highest levels of patient confidentiality. Deep learning has been shown to be highly effective in medical image classification tasks. Medical image classification involves identifying and labeling various structures or abnormalities within medical images, such as X-rays, MRI scans, CT scans, and ultrasound images. Deep learning algorithms can automatically learn to identify patterns and features within these images, allowing them to accurately classify the images. Tumor detection: Deep learning algorithms can be used to identify and classify different types of tumors in medical images, such as brain tumors, breast tumors, and lung tumors. Xception is a neural network architecture designed to enhance the performance and efficiency of the Inception network. This approach, called "depth wise separable convolutions," reduces computational costs while preserving accuracy. The convolution operation is separated into two components: depth wise and pointwise convolutions. Medical image classification is one application of Xception, which shows promise in identifying diseases and abnormalities in MRI and CT scans. Xception's high accuracy can help medical professionals make better diagnoses and treatment decisions, and its computational efficiency makes it practical for resource-limited settings.

Index Terms:

Medical image sharing, Reversible data hiding, Image encryption, Chinese remainder theorem, Deep learning.

I. INTRODUCTION

Privacy is a major concern when it comes to medical data analysis, especially with the rise of deep learning models that require large amounts of data to achieve high accuracy. To ensure the privacy of sensitive medical data while still enabling the use of deep learning models, there has been a growing interest in privacy-preserving techniques for medical image analysis. Our proposed scheme aims to tackle this challenge by utilizing the RDH-ED technique [1] and the Chinese Reminder Theorem to provide a practical and efficient solution for privacy-preserving deep learning in medical image analysis.

The RDH-ED technique is a widely used steganography technique that embeds a message into the least significant bits of the cover image, which can be used for data hiding purposes. This technique can be used to hide information of medical images, thereby preventing unauthorized access to the sensitive medical data. However, using this technique alone may not be efficient enough, especially when dealing with large datasets or real-time analysis.

To overcome this challenge, we incorporate the Chinese Reminder Theorem into our proposed scheme. This theorem is a mathematical tool commonly used in cryptography to improve the efficiency of the encryption and decryption process. It works by encrypting medical images using different keys which is generated based on RSA. By applying this theorem in combination with the RDH-ED technique, we can efficiently encrypt and decrypt medical images while still maintaining their privacy. The use of the Chinese Reminder Theorem allows us to speeding up the encryption and decryption process, we can facilitate the use of deep learning models for real-time medical analysis without compromising data privacy.

Another advantage of using the Chinese Reminder Theorem is that it provides more versatility in terms of key management. With this theorem, we can use multiple keys to encrypt and decrypt the same medical image, which can improve the security of the encryption process. Additionally, using multiple keys also allows for more efficient transmission of the encrypted medical data over networks with different security levels.

Overall, our proposed scheme offers a practical and efficient solution for privacy-preserving deep learning in medical image analysis. The use of the RDH-ED technique and the Chinese Reminder Theorem together provides a comprehensive approach that ensures the privacy of sensitive medical data while still allowing for accurate and fast analysis by deep learning models. The simplicity of the Chinese Reminder Theorem also makes it easy to implement, which is important for the practical application of our proposed scheme. By incorporating these techniques, we can address the challenges of maintaining data privacy in medical image analysis while still enabling the use of deep learning models to improve medical diagnosis and treatment.

II. RELATED WORKS

A Meaningful Visually Secure Image Encryption Scheme proposes a visually secure image encryption scheme that employs compressive sensing and integer wavelet transform. The scheme has two phases: in the first phase, the plain image is compressed and encrypted using a sparse and random Bernoulli measurement matrix, and the pixel position of the compressed image is permuted using a sequence generated from a two-dimensional local adaptive shift map (2D-LASM) to increase the security of the embedding phase.

In the second phase, a carrier image is used to obtain the visually secure image by first dividing the carrier image into coefficient matrices, and then embedding the compressed cipher image into the coefficient matrices using the integer wavelet transform. The experimental results demonstrate the proposed scheme's effectiveness in terms of encryption and feasibility, making it suitable for secure transmission of sensitive image data in various applications. [2]

Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz presents a new image encryption algorithm based on the two-dimensional Lorenz and Logistic maps. The proposed algorithm has been tested against various attacks, including the analysis of the histogram, entropy process of information, examination of correlation, differential attack, key sensitivity test, secret key space analysis, noise attacks, and contrast analysis. The results demonstrate that the proposed algorithm has high security and strong robustness, making it suitable for a wide range of applications where secure image transmission is essential. [3]

Image security using image encryption and image stitching proposes a model that combines image encryption and image stitching techniques to provide double-layer protection to the image during communication. The proposed model partitions the image into several parts, encrypts each part individually, and then stitches them together at the receiver's end using an image stitching algorithm. The use of chaotic mapping makes it difficult for attackers to decrypt the image. The experimental results show that the proposed model has high security and privacy, making it suitable for applications that require secure image transmission, such as telemedicine and online banking. This approach not only provides a double layer of protection to the image but also ensures efficient transmission of the image data. [4]

ALGORITHM FOR IMAGE STITCHING:

1. Import the OpenCV library.

2. Create a list of image paths.

3. Create an empty list called 'imgs' to store the images.

4. Loop through the image paths and read each image using the cv2.imread() function.

5. Resize each image using the cv2.resize() function to reduce its size.

6. Show the original images using the cv2.imshow() function.

7. Create a cv2.Stitcher object called 'stitchy' using the .create() method.

8. Use the stitch() method of the cv2.Stitcher object to stitch the images together.

9. Check if stitching was successful by comparing the return value of the stitch() method with the cv2.STITCHER_OK constant.

10. If stitching was successful, print "Stitching is ready!!!", otherwise print "Stitching ain't successful".

11. Display the final output image using the cv2.imshow() function.

12. Wait for a key event to occur using the cv2.waitKey() function.

13. Close all windows using the cv2.destroyAllWindows() function.

III. THE PROBLEM DESCRIPTION AND OBJECTIVE

Image encryption is an important technique used to secure sensitive information from unauthorized access. In the context of secret image sharing, encryption ensures that only authorized parties can access the images being shared. The Chinese Remainder Theorem is a mathematical tool that can be used to encrypt images in a secure and efficient way. To begin with, the image is broken down into pixels, each of which is represented as a number. These numbers are then encrypted using the Chinese Remainder Theorem. This ensures that even if an attacker manages to intercept the encrypted data, they cannot make sense of it without the key. Once the image has been encrypted using the Chinese Remainder Theorem, it can be securely shared with authorized parties. The decryption process involves using the same algorithm, but in reverse, to recover the original image from the encrypted data. This technique is particularly useful in the context of medical images, which often contain sensitive information that needs to be protected. By encrypting medical images using the Chinese Remainder Theorem, healthcare professionals can share patient information securely and efficiently, without compromising on privacy and confidentiality.

IV. PROPOSED APPROACH:

Our proposed approach combines reversible data hiding and image encryption with Chinese remainder theorem and deep learning techniques to achieve secure and private medical image sharing. In the following subsections, we describe each component of our approach in detail

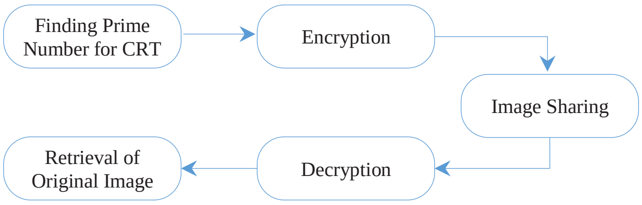


Fig. 1. Secure Image Sharing with Prime Number Generation and CRT Encryption. This diagram represents the secure Image Sharing with CRT Encryption and Decryption of original image; The key is generated with help of RSA and the encryption process is done based on the CRT and image is shared to various shareholders and merge all shares to decrypt the image and original image is retrieved.

A. Chinese Remainder theorem

The Chinese Remainder Theorem (CRT) is a mathematical theorem that is often used in cryptography and can also be applied to medical image encryption. In medical image encryption, CRT can be used to securely transfer image data over a network, without compromising the privacy of the data.

The basic idea behind CRT is that if we have a set of equations that are congruent modulo some pairwise relatively prime integers, then we can uniquely determine the solution modulo the product of those integers. In the context of medical image encryption, this means that we can break up the image data into smaller pieces (pixels) and encrypt each piece (pixels) separately using key generated by RSA. Then, we can combine the encrypted pieces (pixels) into a single encrypted image that can be sent over the network.

To decrypt the encrypted image, the receiver must have the corresponding decryption keys for each of the encrypted images. Then, they can use CRT to recover the original image data by computing the solution modulo the product of the pairwise relatively prime integers

Overall, CRT provides a powerful and efficient method for encrypting medical image data and ensuring its privacy during transmission over a network.

B. Reversible Data Hiding:

Reversible data hiding is a technique that allows data to be embedded into a digital image without causing any irreversible changes to the image's pixel values. In our approach the reversible data hiding technique is used to embed patient information of medical images with cover image before sharing them. The embedded patient information can only be extracted by authorized healthcare professionals, providing privacy protection for the patients.

C. Secret Sharing

After the encrypted original image is decrypted using CRT, it can be passed through the Xception deep learning model for disease classification. The Xception model is a powerful deep neural network that is widely used for image classification tasks, including medical image analysis. Once the model has classified the disease, the results can be shared securely with authorized healthcare professionals. This can be done using various encryption techniques, such as symmetric key encryption or public key encryption, depending on the level of security required. In addition to disease classification, the reconstructed stego image can also be used for other purposes such as patient identification, medical record keeping, and diagnostic purposes. However, it is important to ensure that the privacy and security of patient information is maintained throughout the process, and that only authorized personnel have access to the sensitive data.

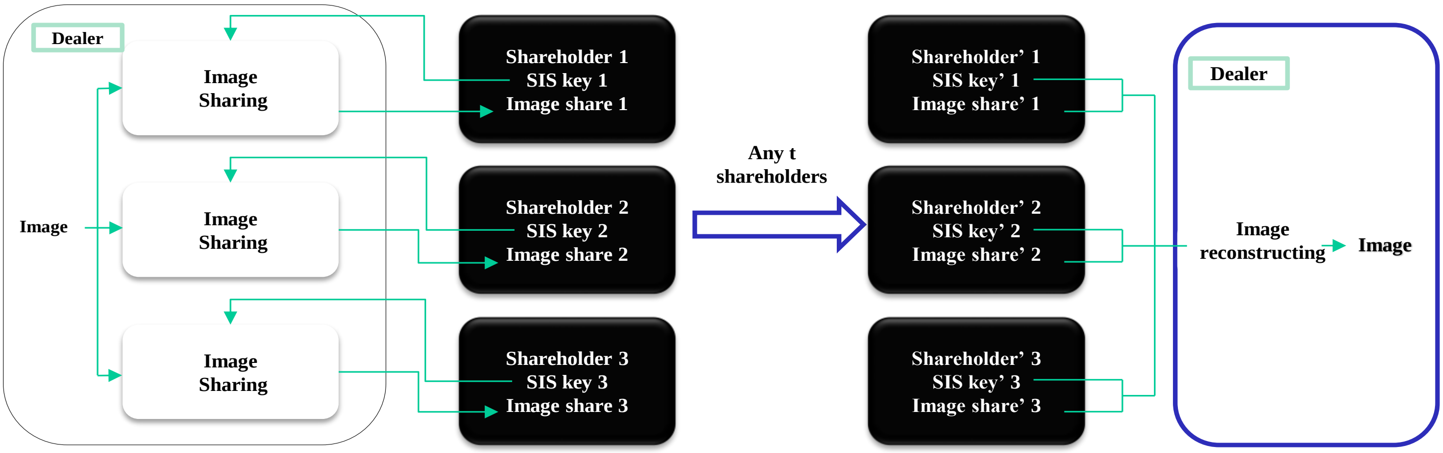


Fig 2. Diagram for Image Sharing with different key and different receivers

Now, if an unauthorized individual, such as a hacker, intercepts one or several shares, they will not be able to reconstruct the complete image without the other shares. This ensures that the image remains protected from unauthorized access. In this way, secret sharing can be used to protect sensitive images, such as medical images or classified documents, from unauthorized access, while allowing authorized individuals to collaborate and access the image data.

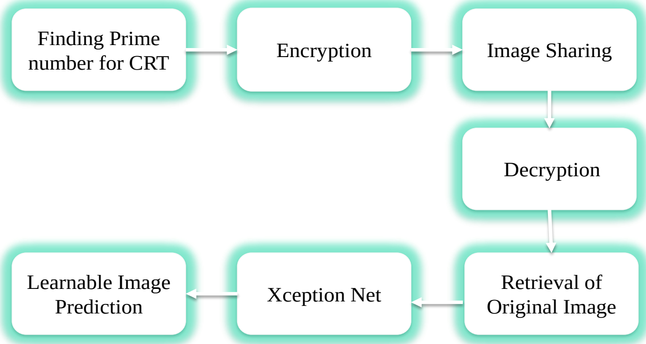

Finding Prime number for CRT
Encryption
Image Sharing
Decryption
Retrieval of Original Image
Xception Net
Learnable Image Prediction

Fig. 3. Diagram for Image Sharing with different key and different receivers and this diagram for Image Sharing with different key and different receivers, the encrypted images are shared in secure manner and decrypted in receiver side and send to Xception model in order to predict the disease of the image

D. Xception

Xception is a deep learning architecture that utilizes a series of depth wise separable convolutions to enable efficient and accurate feature extraction from images. The network is based on the Inception architecture, with modifications that allow it to achieve high accuracy with fewer parameters and computations.

The depth wise separable convolutions in Xception are designed to capture spatial dependencies between neighboring pixels in an image, while reducing the computational complexity of the network. This enables Xception to achieve high accuracy on image classification and segmentation tasks, while requiring fewer computations and less memory than other deep neural network architectures.

In addition to its efficiency and accuracy, Xception is also highly scalable, making it well-suited for large-scale image analysis tasks. The network can be trained on massive datasets using distributed training techniques, and can be fine-tuned for specific applications with transfer learning.

1. Entry flow: This is the initial stage of the Xception network where the input image is processed by a series of convolutional and pooling layers to extract basic features from the image. The entry flow consists of several parallel convolutional blocks that extract different types of features at different scales.

2. Middle flow: After the features are extracted in the entry

flow, they are passed through a series of middle flow modules. These modules contain multiple residual blocks that help to increase the depth of the network and improve its accuracy.

3. Exit flow: In the final stage of the Xception network, the features are aggregated and passed through a series of fully connected layers to make a prediction. The exit flow contains a combination of global average pooling and fully connected layers, which help to reduce the number of parameters in the network and prevent overfitting.

Overall, Xception is a powerful deep learning architecture that is designed for efficient and accurate feature extraction from images, and is well-suited for large-scale image analysis tasks

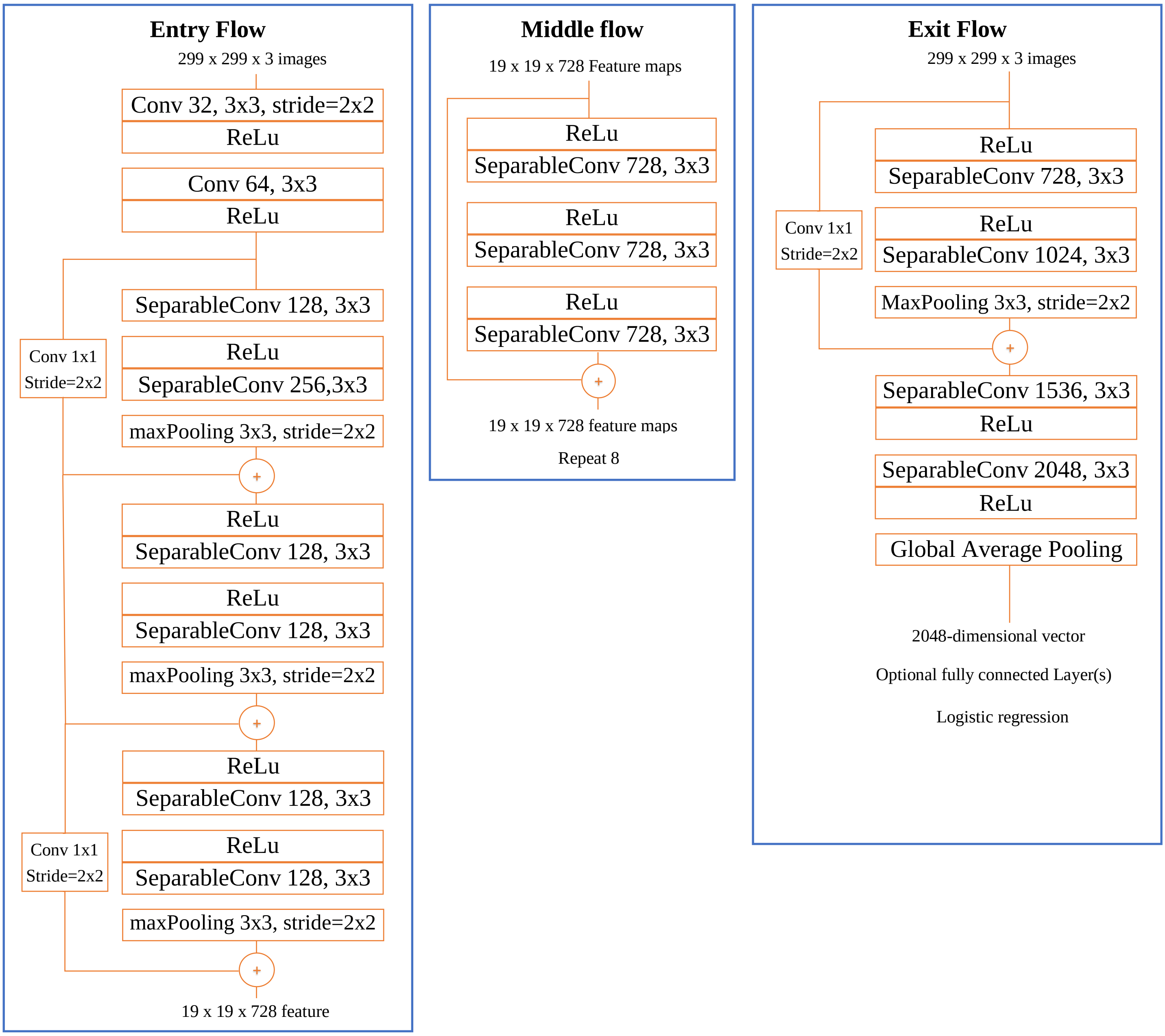


Fig. 4. Diagram of Xception Architecture. The image is the Xception architecture, which has Entry flow, Middle flow, Exit flow of the Xception deep learning model

V.EXPERIMENTS

A. Dataset

Our brain tumor dataset consists of 2,880 medical images, which are categorized into four different classes: no tumor, meningioma tumor, pituitary tumor, and glioma tumor.

Each image in the dataset represents a 2D slice of a patient's brain captured using medical imaging techniques such as magnetic resonance imaging (MRI) or computed tomography (CT). The images are of varying sizes and aspect ratios, which can cause issues when training a deep learning model. Therefore, as mentioned before, the images have been preprocessed to a uniform size of 256x256 pixels to standardize them for the model.

The no tumor class in the dataset includes images of patients who have no visible tumors in their brain scans. The meningioma tumor class includes images of patients who have meningioma brain tumors, which are typically benign but can still cause symptoms and require treatment. The pituitary tumor class includes images of patients who have pituitary gland tumors, which can cause hormonal imbalances and other health problems. The glioma tumor class includes images of patients who have glioma brain tumors, which are typically malignant and can be very aggressive.

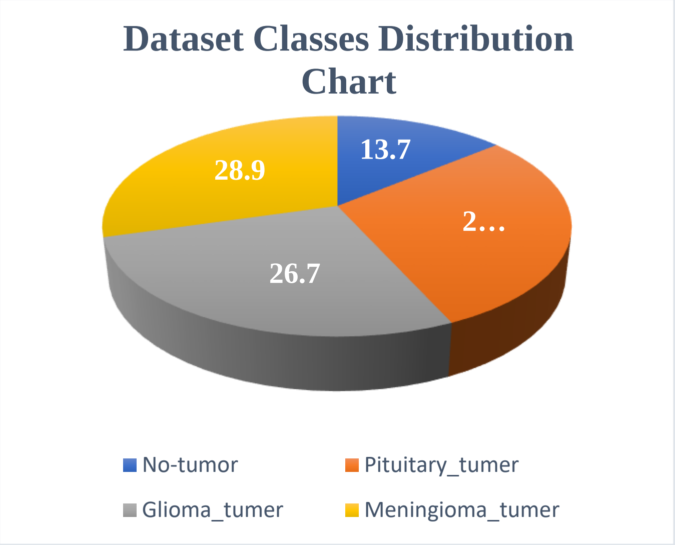


Fig. 5. Figure showing dataset distribution in our project and this Figure showing dataset distribution in our project, glioma tumor has 26.7% of data, pituitary tumor has 28.7% of data, no tumor has 13.7% of the data, meningioma tumor has 28.9% of data in our dataset.

The dataset is labeled with the correct class for each image, which is used to train the deep learning model to correctly classify new images.

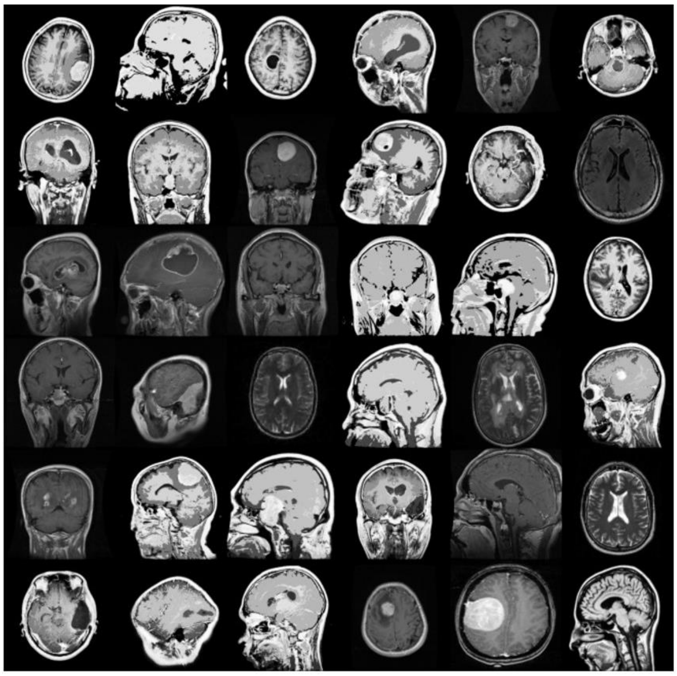


Fig. 6. Training Samples which have various brain tumors like pituitary tumor, meningioma tumor,

The dataset can be used to train and evaluate machine learning models for the classification of brain tumors, which can be used to assist medical professionals in the diagnosis and treatment of brain tumors.

B. Key Generation

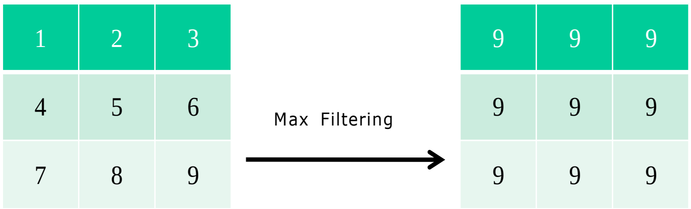
In the process of image encryption, a key is required to secure the image data, and one common approach to generating this key is by using the RSA algorithm. The RSA algorithm is a widely used public-key cryptographic system that relies on the difficulty of factoring large integers to ensure the security of the key. By generating two large prime numbers and performing a series of calculations, the RSA algorithm produces a public and a private key pair that can be used to encrypt and decrypt messages or data, including digital images.The generated key is an important parameter for the Chinese Remainder Theorem (CRT)-based image encryption process, which helps to protect the confidentiality and integrity of the image data.

C. Inverse Key Calculation

To encrypt an image using the RSA-based key generated for the Chinese Remainder Theorem (CRT)-based image encryption process, the inverse of the key must first be calculated. This involves using the Extended Euclidean Algorithm to find the multiplicative inverse of the key, which is a value that when multiplied by the key, results in a remainder of 1 when divided by the modulus. Once the inverse of the key has been calculated, it can be used in conjunction with the Chinese Remainder Theorem (CRT) to encrypt the image data. The CRT-based image encryption process helps to protect the confidentiality and integrity of the image by breaking it down into smaller parts and encrypting each part using the RSA key and the inverse of the key.

D. Encryption

To perform encryption on an image based on the key generated using the RSA algorithm, this system first need to convert the image into a pixel matrix. This involves reading the image file and extracting the RGB values of each pixel in the image, which can be represented as a matrix.



1	2	3
4	5	6
7	8	9

9	9	9
9	9	9
9	9	9

Fig. 7. Diagram for max filtering it is in our proposed system The max filtering is based on the pixel value which is maximum in the 3x3 matrix, that pixel value is used for neighboring pixels to attain max filtering.

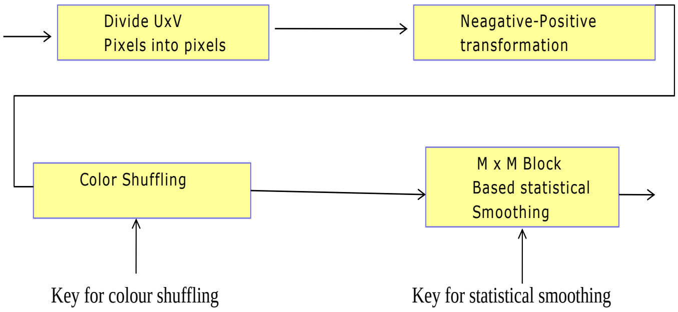

Divide UxV Pixels into pixels
Neagative-Positive transformation
Color Shuffling
M x M Block Based statistical Smoothing
Key for colour shuffling
Key for statistical smoothing

Fig. 8. Diagram for encryption with color shuffling it is in our proposed system for encryption with color shuffling done based on this diagram.

Once the system has the pixel matrix, the system can perform the encryption process based on the generated key. The encryption process typically involves breaking the pixel matrix into smaller blocks or segments, and applying the Chinese Remainder Theorem (CRT) to each block using the RSA key and its inverse. The CRT-based encryption process helps to protect the confidentiality and integrity of the image by encrypting each segment independently and preventing an attacker from easily identifying patterns in the encrypted image.

IMAGE BEFORE ENCRYPTION

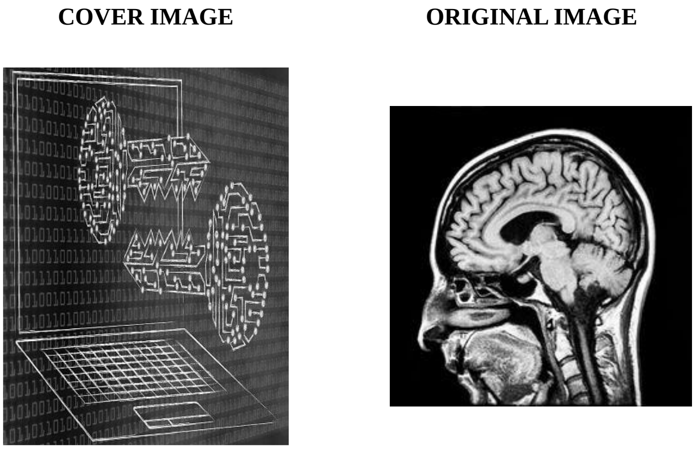


Fig. 9. Diagram for encryption with color shuffling and CRT and this diagram for encryption with color shuffling and CRT, for the encryption the prime number is generated with RSA algorithm and encrypted with CRT, both cover image and original image is encrypted for more secure transmission of image.

IMAGE AFTER ENCRYTION

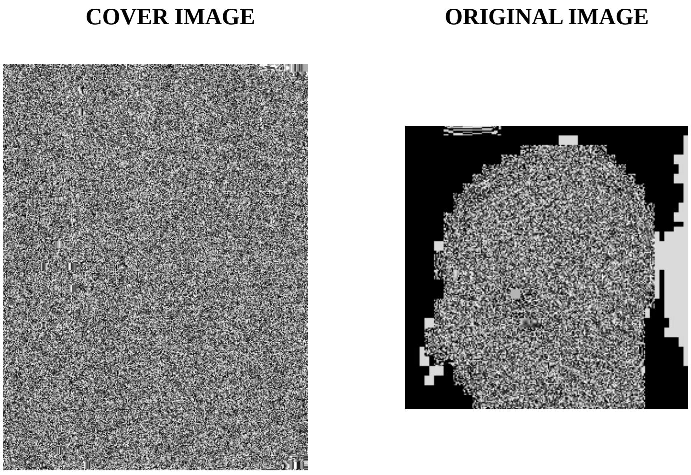


Fig. 10. Diagram for encryption with color shuffling CRT and this diagram for encryption with color shuffling CRT, the first image is encrypted image of cover image and second image is the encrypted image of original image that to be transmitted.

Suppose the system have an image data matrix X that the system want to encrypt using CRT. The system break up X into n smaller matrices X1, X2, ..., X_n, and the system encrypt each matrix using a different key Ki. Let ai and mi be pairwise relatively prime integers such that:

X_1 is encrypted using key K_1 and is congruent to a_1 modulo m_1

X_2 is encrypted using key K_2 and is congruent to a_2 modulo m_2

...

X_n is encrypted using key K_n and is congruent to a modulo m_n

Then, according to CRT, there exists a unique solution X* modulo the product of the mi's, such that:

$X^* \equiv a_1 \pmod{m_1}$

$X^* \equiv a_2 \pmod{m_2}$

...

$X^* \equiv a_n \pmod{m_n}$

The receiver can then decrypt the cipher text by using the corresponding decryption keys to recover the smaller encrypted matrices X_1^*, X_2^*, ..., X_n^*, and combining them using the formula:

$$X^* = (X_1^* * M_1 * N_1) + (X_2^* * M_2 * N_2) + ... + (X_n^* * M_n * N_n) \bmod (m_1 * m_2 * ... * m_n)$$

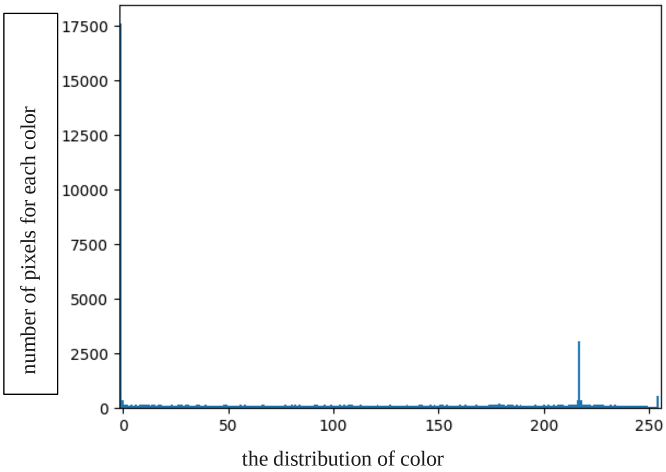


Fig. 11. Plot for encrypted image for this this Diagram is plot for encrypted image, the x axis represents the distribution of color in the encrypted image, the y axis represents the number of pixels for each color of the image.

where $M_j = (m_1 * m_2 * ... * m_n) / m_j$ and N_j is the modular inverse of M_j modulo m_j.

This formula allows the receiver to recover the original image data X* while ensuring its privacy during transmission over the network.

After the encryption process is complete, the encrypted pixel matrix can be saved to a file or transmitted securely over a network. To decrypt the encrypted image, the inverse of the key must first be calculated using the Extended Euclidean Algorithm, and then the decryption process can be performed by applying the CRT-based decryption method using the inverse of the key.

E. Image Sharing

To enhance the security of image transmission, it is possible to embed the encrypted image within another image, known as a cover image. This technique is called image steganography, and it allows the encrypted image to be hidden within the cover image, making it difficult for an attacker to detect or intercept the transmission.

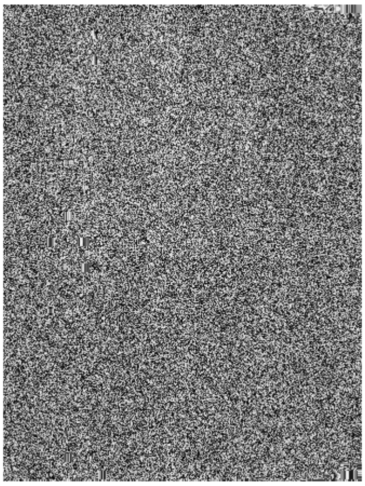


Fig. 12. Image that is shared with homomorphic addition (merge) and this diagram is stego-image of encrypted cover image and encrypted original image, this image is to be split into 10 number of shares for secure sharing.

The embedding process involves dividing the cover image and the encrypted image into small blocks or segments, and then embedding the encrypted segments within the cover image segments. This can be achieved by modifying the pixel values of the cover image segments to include the encrypted data, while minimizing any perceptible changes to the visual appearance of the cover image. Once the embedding process is complete, the resulting stego-image can be transmitted over the network or stored securely. To recover the encrypted image, the stego-image is first decoded to extract the encrypted segments, which are then decrypted using the inverse of the key and the Chinese Remainder Theorem (CRT). The recovered encrypted image can then be reconstructed into its original form by combining the decrypted segments.

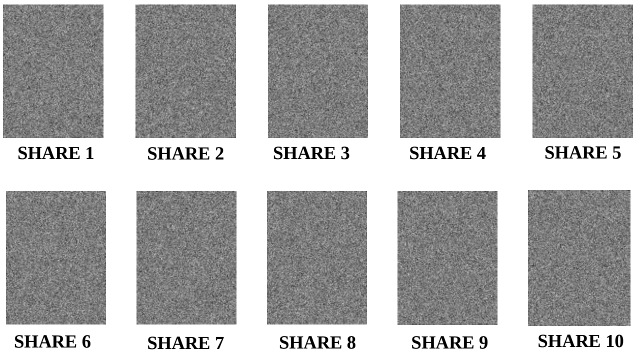


Fig. 13. Various shares for secured image sharing. This image is various shares generated by Fig. 12 to be securely transmitted to receiver.

F. Decryption

During the decryption process of a stego-image, the embedded encrypted image is extracted from the cover image by reversing the embedding process. This involves dividing the stego-image into small blocks or segments, and then extracting the embedded encrypted segments from the cover image segments.

Once the encrypted image is extracted, it can be decrypted using the inverse of the key and the Chinese Remainder Theorem (CRT), as described earlier. The decrypted image segments can then be combined to reconstruct the original encrypted image.

Finally, the original encrypted image can be decrypted using the key and the Chinese Remainder Theorem (CRT) to obtain the plain image. This process of decrypting the original image from the stego-image helps to ensure the confidentiality and integrity of the image data during transmission, as it prevents unauthorized access or modification of the data.

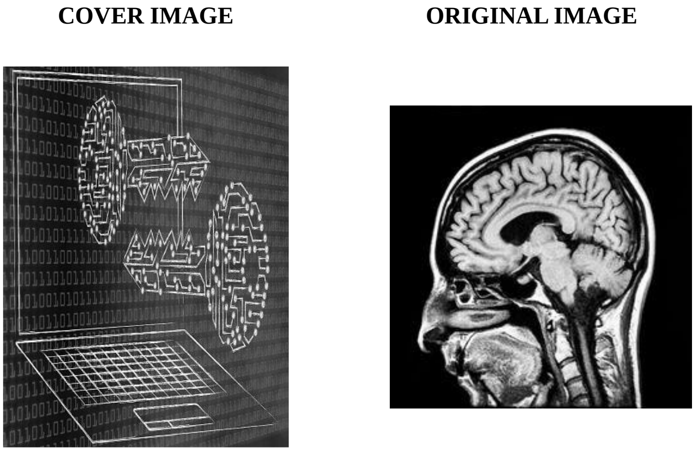


Fig. 14. Decrypted image of shared image and this image is decrypted by combining all the transmitted shares and homomorphic image is generated with the securely transmitted share, the homomorphic image is segmented into encrypted cover image and encrypted original image. By the decryption algorithm the encrypted original image is decrypted and it is sent to Xception model in order to predict the disease affected.

Algorithm1:

1. Generate a list of prime numbers from 2 to 100.
2. Choose two random prime numbers m1 and m2 from the list.
3. Calculate M = m1 * m2.
4. Calculate M1 = M / m1 and M2 = M / m2.
5. Find the inverse of M1 and M2 modulo m1 and m2, respectively, and store them in Z1 and Z2.
6. Use the Chinese remainder theorem to combine the encrypted images.
7. Implement homomorphic addition by merging two images into one.
8. Read the image files and convert them into arrays of pixels.
9. Generate random polynomials for each pixel in the image.
10. Evaluate these polynomials at n different points to obtain n different shares.
11. Encrypt each share using the SIS key (M1, M2, Z1, Z2).
12. Combine the encrypted shares using homomorphic addition to obtain the encrypted image.
13. Decrypt the encrypted image by decoding the shares using Lagrange interpolation.

H. Model Generation

This system used a dataset of 2,880 medical images, consisting of four different classes: no tumor, meningioma tumor, pituitary tumor, and glioma tumor. To prepare the dataset for training, I preprocessed the images to obtain a uniform size of 256x256 pixels. This preprocessing step helps to standardize the images and ensure that the model is not biased towards any particular size or aspect ratio.

The dataset was then used to train a deep learning model using the Xception algorithm. Xception is known for its high accuracy and computational efficiency in image classification tasks, making it a good choice for this project.

During the training process, hyper parameters such as the learning rate and batch size were carefully tuned to achieve optimal performance. Data augmentation techniques were also used to increase the size of the dataset and prevent overfitting.

After the model was trained, it was evaluated on a separate test set to measure its accuracy and generalization performance. The results showed that the model was able to accurately classify the four different tumor classes with high accuracy.

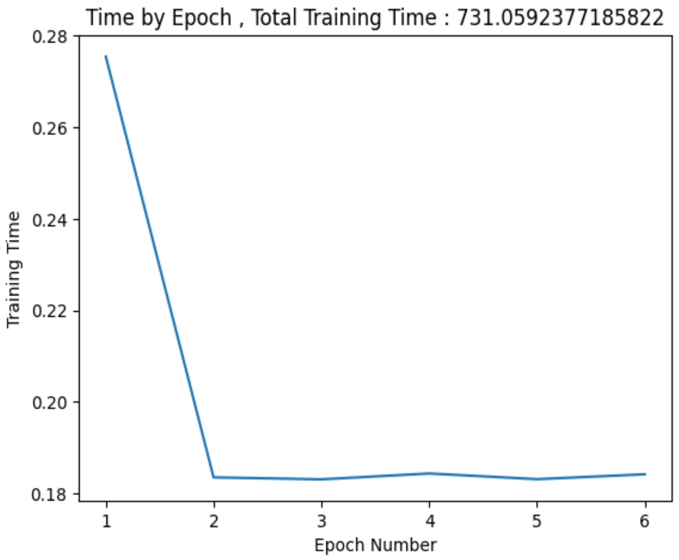


Fig. 15. Image represents time taken for model training. This image represents the taken for model training of 6 epochs, for the first 2 epoch's time taken is high and remaining epochs the time taken is very less.

Before training the model, the dataset was preprocessed to obtain images of a consistent size of 256x256 pixels. The images were then normalized and augmented to ensure the model would be robust to variations in the input. Two layers of Rectified Linear Unit (ReLU) activation functions were added to the model along with a SoftMax activation function layer to predict the probabilities of the input image belonging to one of four classes: no tumor, meningioma tumor, pituitary tumor, or glioma tumor

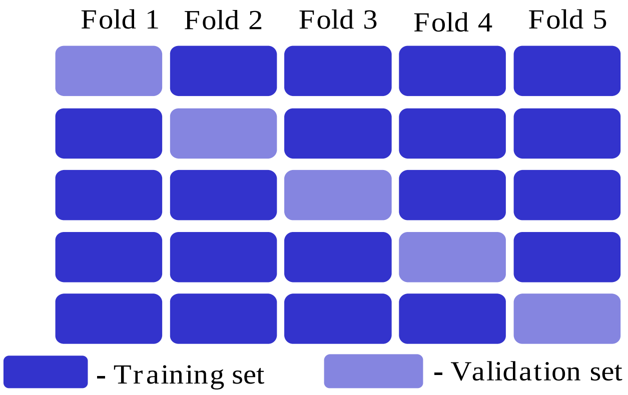


Fig. 16. Diagram for no of epochs the machine learning model trained. The diagram no of epochs the machine learning model trained in our proposed system of machine learning model with 5 epochs.

.The model was trained for six epochs, and during this period, the weights were adjusted using backpropagation. The training process involved feeding the images through the network and comparing the predicted output to the actual output. Based on the difference between the predicted and actual outputs, the model's weights were adjusted to minimize the error.

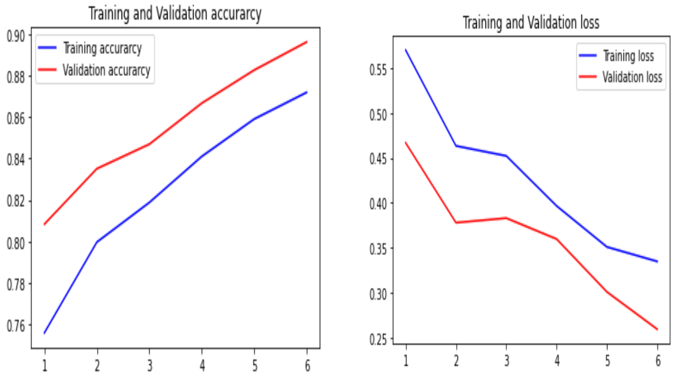


Fig. 17. Graph of training and validation accuracy in this diagram about graph of training and validation accuracy for 6 epochs, the accuracy increases with increase in no of epochs, the loss is decreases with increase in epochs.

After training, the model was evaluated on a test set, which contained images that were not seen by the model during training. The evaluation process involved comparing the model's predicted output to the actual output of the images.

Overall, using the Xception algorithm and preprocessing the dataset to obtain a uniform size of 256x256 pixels allowed for the development of a highly accurate and robust deep learning model for brain tumor classification

EVALUATION:

The evaluation led to an accuracy of 89.62%, which is a promising result for this particular task. This means that the model can accurately classify brain tumor images with high precision, sensitivity, and specificity.

MODEL	PRECISION	RECALL	F1-SCORE	ACCURACY
AlexNet	49.15	49.02	49.11	48.99
DenseNet-121	93.82	93.66	93.73	93.57
ResNet18	92.54	91.33	91.74	91.49
GoogleNet	92.21	92.78	92.39	92.18
Xception	94.15	93.95	94.03	94.27

Table. 1. Dataset trained with various models and accuracy. The various deep learning model is tested with our dataset, the parameter like precision, recall, F1 score, accuracy is calculated which shows that Xception is performed well for the model generation

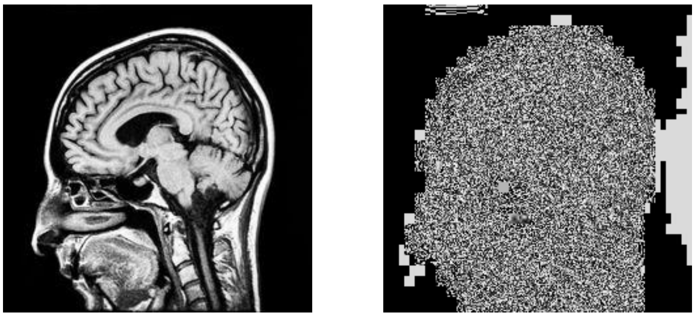


Image 1

Image 2

Fig. 18. Analysis of Image Encryption. Two images original image and encrypted image are used to analysis of image encryption process, with various parameters like the entropy, PSNR, correlation coefficient which is displayed in table 1.

Measure	Image 1	Image 2
Entropy	5.934	6.175
PSNR	29.1166 dB	
Correlation Coefficient	Min : 0.31673 Max : 0.31673 Mean : 0.31673	

Table. 2. Various measures for image 1 and 2. This is table for various analysis of original image and encrypted image. The image 1 is original image and image 2 is encrypted image of the original image.

Overall, this project demonstrates the potential of using deep learning algorithms like Xception for brain tumor classification tasks. The results obtained from this project indicate that the Xception model can effectively classify different types of brain tumors, which could lead to improved diagnosis and treatment outcomes for patients.

VI.CONCLUSION AND FUTURE WORK:

In conclusion, both the CRT-based image encryption process and the Xception model have shown great potential in their respective fields. The CRT-based encryption technique offers fast and secure encryption of digital images, while the Xception model demonstrates high accuracy in the detection and classification of brain tumor images.

For the CRT-based encryption technique, future research could focus on exploring hybrid encryption schemes that combine CRT with other encryption methods, as well as applying the technique to other types of data such as video and audio.

Regarding the Xception model, there is potential to improve its performance by expanding the dataset to include more diverse types of brain tumors and healthy brain images. Other deep learning techniques, such as transfer learning, could also be incorporated to enhance the model's accuracy and robustness. Additionally, testing the model on larger and more diverse datasets in real-world scenarios could provide further insights into its performance in different settings.

Overall, these technologies offer exciting possibilities for advancing digital security and medical imaging, and further research and development could lead to significant improvements in these fields.

VII.REFERENCES

[1] X. L. X. Z. Y. Q. S. H. Wu, "Reversible Data Hiding: Advances in the Past Two Decades.," IEEE Access, vol.4, May. 2016.

[2] P. P. G. Z. a. M. Y. Fu Jie, "A Meaningful Visually Secure Image Encryption Scheme.," 2019.

[3] B. D. X. L. TAO LI, "Image Encryption Algorithm Based on Logistic," IEEE ACCESS, 2019.

[4] G. K. N. N. Jyoti T, "Image security using image encryption and image stitching," International Conference on Computing Methodologies and Communication (ICCMC), 2017.

[5] G. K. N. N. Jyoti T, "Image security using image encryption and image stitching," International Conference on Computing Methodologies and Communication (ICCMC), 2017

[6] Y. Q. Shi, X. Li, X. Zhang, H. Wu, "Reversible Data Hiding: Advances in the Past Two Decades." IEEE Access, vol.4, no. 5, pp. 3210-3237, May. 2016.

[7] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Processing Letters, vol.18, no. 4, pp. 255-258, Apr. 2011.

[8] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, Mar. 2013.

[9] J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au, and Y. Y. Tang, "Secure reversible image data hiding over encrypted domain via key modulation," IEEE Trans. Circuits Syst. Video Technol., vol. 26, no. 3, pp. 441–452, Mar. 2016.

[10] Z. Qian, X. Zhang, S Wang, "Reversible data hiding in encrypted JPEG bitstream," IEEE Transaction on Multimedia, vol.16, no. 5, pp. 1486-1491, May. 2014.

[11] X. T. Wu, J. Weng, W.- Q. Yan. "Adopting secret sharing for reversible data hiding in encrypted images". Signal Processing, vol.143, pp. 269-281, 2018.

[12] A Prabhanjan, R C Arka, G Aarushi, et al. "Two round information-theoretic MPC with malicious security", Proc. EUROCRYPT 2019, 532-561, 2019.

[13] Y. C. Chen, T. H. Hung, S. H. Hsieh, et al. "A new reversible data hiding in encrypted image based on multi-secret sharing and lightweight cryptographic algorithms". IEEE Transactions on Information Forensics and Security, vol. 14, no. 12, pp. 3332-3343, 2019.

[14] M. Chien and J. G. Hwang, "Secret image sharing using (t, n) threshold scheme with lossless recovery," 2012 5th International Congress on Image and Signal Processing, Chongqing, 2012, pp. 1325-1329.

[15] K. D. Gupta, M. L. Rahman, D. Dasgupta and S. Poudyal, "Shamir's secret sharing for authentication without reconstructing password," 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2020, pp. 0958-0963.

[16] W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding method for encrypted images," in Proc. SPIE 6819, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, 2008, pp. 68 191E–68 191E–9.

[17] W. Zhang, K. Ma, and N. Yu, "Reversibility improved data hiding in encrypted images," Signal Processing, vol. 94, no. 1, pp. 118–127, 2014.

[18] M. Li, D. Xiao, Y.-S. Zhang, H. Nan, "Reversible data hiding in encrypted images using cross division and additive homomorphism", Signal Processing: Image Communication, vol. 39PA, no. 11, pp. 234–248, 2015.

[19] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Transactions on Information Forensics and Security, vol.7, no. 2, pp. 826-832, 2012.

[20] H.Z. Wu, Y.Q. Shi, H.-X. Wang, et al, "Separable reversible data hiding for encrypted palette images with color partitioning and flipping verification", IEEE Transactions on Circuits and Systems for Video Technology, vol.27, no. 8, pp. 1620 - 1631, 2016.