Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: XXXX-XXXX | Volume 1 Issue I July - December 2025 | Inaugural Edition | QP08

PROTECTING MEDICAL IMAGES: A ROBUST APPROACH TO ENCRYPTED DICOM DATA TRANSMISSION

Dr. B. SRINIVASA RAO, *Associate Professor,*
Department of CSE (DATA SCIENCE),
GURUNANAK INSTITUTIONS TECHNICAL CAMPUS(AUTONOMOUS),
IBRAHIMPATNAM, RANGAREDDY, TELANGANA

ABSTRACT: To maintain confidentiality and integrity within the medical sector, it is essential that medical photographs are exchanged securely. In the realm of transmitting and archiving medical pictures, numerous professionals in the healthcare sector depend on the DICOM standard. Robust encryption solutions are essential for safeguarding private data against these threats. This paper investigates a comprehensive approach to encrypting interactions involving DICOM pictures. To guarantee data integrity and security, it tackles essential concerns and provides answers. This research analyzes contemporary encryption methods for safe DICOM image transmission, focusing on their effectiveness, practicality, and possible shortcomings.

Keywords: Medical Image Security, DICOM Encryption, Data Confidentiality, Secure Transmission, Health Informatics, Image Encryption Techniques, Healthcare Data Protection.

1. INTRODUCTION

Digital imaging and electronic health records are becoming more and more important in modern healthcare. The DICOM standard streamlines the process of storing, exchanging, and exchanging medical procedure images. Protecting medical images is of the utmost importance in light of the growing number of cyber threats and privacy issues. Data breaches, manipulation, and unauthorized access must be strictly avoided while delivering DICOM data, which often contains sensitive patient information. Protecting sensitive patient information during network transmission is one of the many benefits of encrypting DICOM images. Encryption is just part of the issue; we also need a way to make sure your data stays intact while we transport it faster.

Due to the sensitive nature of medical data, there are significant security considerations around the transfer of DICOM photographs. Unauthorized access poses a risk to patients' privacy and confidence. Using strong encryption methods is essential for protecting the validity, integrity, and secrecy of DICOM pictures during transmission. Research, diagnosis, and the creation of novel medications rely heavily on medical imaging. The need for safe medical image sharing is growing in tandem with the popularity of cloud storage and telemedicine. When it comes to medical imaging data organization, DICOM is king. It lays forth the rules for how to send, store, and understand images. The danger of data loss, illegal access, and cyber attack is heightened when DICOM files are not adequately encrypted. The importance of keeping information private while enabling quick medical analysis is the primary emphasis of this research, which examines the reasons why sophisticated encryption methods are necessary for transferring DICOM data. Important strategies including end-to-end encryption, secure transmission protocols, and encryption algorithms will be discussed, along with the difficulties that come with trying to apply them in healthcare systems. An all-encompassing system that advances medical technology while simultaneously addressing security concerns is the ultimate objective.

Encryption Techniques

Symmetric Encryption: The key used for both the encryption and decryption of communications is the same in symmetric encryption. When it comes to symmetric encryption techniques, such as the Advanced Encryption Standard (AES), reputation is everything. DICOM images are perfect for usage in real-time applications due to their AES encryption.

Asymmetric Encryption: One key is used for encryption and the other is used for decryption in public-key cryptography, which is also called symmetric encryption. When it comes to asymmetric encryption, Rivest-Shamir-Adleman (RSA) is by far the most popular choice. To guarantee the safe transfer of symmetric keys, hybrid encryption solutions are necessary, even though they are slower.

Hybrid Encryption: The benefits of both symmetric and asymmetric encryption methods are combined in hybrid encryption. Using symmetric and asymmetric keys, this method encrypts the DICOM image. This method integrates the greatest features of both symmetric and conventional encryption.

2. LITREATURE REVIEW

Zhang, L., & Wang, H. (2020) This essay delves into the topic of encryption in medical image transfers, specifically looking at DICOM, the format that is widely used in the business. For the safe transport of DICOM data, it explains and rates different encryption schemes, some of which are symmetric and others of which are asymmetric. By utilizing different encryption approaches, we may examine the trade-offs that exist among security, implementation complexity, and computational performance.

Singh, R., & Sharma, S. (2019) This research delves into the security issues surrounding DICOM images, specifically looking at how they are sent across hospital networks. Unauthorized access, tampering, and listening in are among the recognized concerns, along with the possible impact on patient safety and privacy.

Huang, Z., & Li, X. (2021) We examine state-of-the-art cryptographic methods for safely transmitting DICOM pictures in this literature research. Medical imaging is connected with large file amounts and high throughput demands; this research examines the effectiveness of several encryption methods in managing these demands.

Lee, K., & Cho, Y. (2022). Specifically designed to encrypt images of healthcare data, privacy-enhancing technologies (PETs) are the focus of this research. It delves into the ways in which privacy-preserving technologies, such homomorphic encryption and secure multiparty processing, can be employed to transmit less data-intensive images while safeguarding patient data.

Wang, Y., & Zhang, T. (2023) Key management in DICOM picture encryption is highlighted in this research review. We talk about the difficulties of making sure encrypted medical images adhere to GDPR and HIPAA rules, and how important secure key exchange algorithms like Diffie-Hellman are for the secure transfer of DICOM data.

3. IMPLEMENTATION OF SECURE TRANSMISSION

Secure Socket Layer (SSL) and Transport Layer Security (TLS): Consequently, in order to protect the data, SSL/TLS protocols must be implemented when transferring DICOM images across networks. By establishing a secure connection between users, protocols such as these prevent "man-in-the-middle" attacks and espionage.

Virtual Private Networks (VPN): VPNs can be employed to create a secure data sharing pathway, which is beneficial for guaranteeing the security of DICOM image transfers. This approach is particularly advantageous in safeguarding confidential information from unauthorized users, particularly on public networks.

Secure File Transfer Protocols: Two secure methods for transmitting DICOM images between computers are the secure File Transfer Protocol (SFTP) and FTP Secure (FTPS). These solutions provide an additional layer of security by safeguarding data during transmission.

Challenges in Secured DICOM Transmission

Performance Overhead: The transfer of DICOM images may require a lengthier time than anticipated due to the complexity of the encryption. In a medical emergency, where every second is crucial, safety and performance must be prioritized.

Key Management: The protection of sensitive data is contingent upon the proper management of keys. Certain standards and norms are necessary to ensure security due to the intricate nature of the process of creating, distributing, retaining, and revoking keys.

Compliance with Regulations: Medical data must be securely stored in accordance with the Health Insurance Portability and Accountability Act and other statutes. Companies are required to ensure that their data management processes and encryption strategies adhere to established standards.

4. METHODOLOGY

In order to construct a comprehensive system that can store DICOM images, the industry standard for medical imaging data, a variety of complex components are necessary. Steps that must be taken to accomplish all of the objectives that were previously established are detailed in the following sections:

1. Compressed Model for DICOM Format Images

It is crucial to consider the distinctive characteristics and requirements of medical imaging when creating a compressed model for DICOM images. It is imperative to implement efficient compression methods, as DICOM files can become quite large as a result of the high quality of the images they contain.

It is advisable to employ lossy and lossless compression algorithms that are specifically designed for medical images. In order to provide accurate diagnoses, it is imperative that images are preserved. The majority of DICOM systems accomplish this by employing lossless techniques, such as JPEG 2000. Modifications to the wavelet transform can enhance compression rates while preserving the fidelity of the image.

Data transmission and storage can be simplified by a paradigm that integrates adaptive compression techniques and visual data. This method precisely identifies and compresses visual patterns that are similar. It achieves this by employing machine learning techniques to extract knowledge from data.

2. Advanced Algorithm Based on BASE-64 Encoding

Data transmission and storage control on websites frequently employ BASE-64 encoding. The utilization of a comprehensive BASE-64 encoding strategy facilitates the viewing and interaction with DICOM images on any platform.

The objective of this strategy is to eradicate BASE-64 waste during encoding in order to optimize efficiency. It is possible that the situation could be enhanced by incorporating a composite encoding method and combining multiple compression techniques prior to encoding. For example, this could entail the utilization of BASE-64 following the establishment of immaculate compression encoding in order to minimize the volume of data.

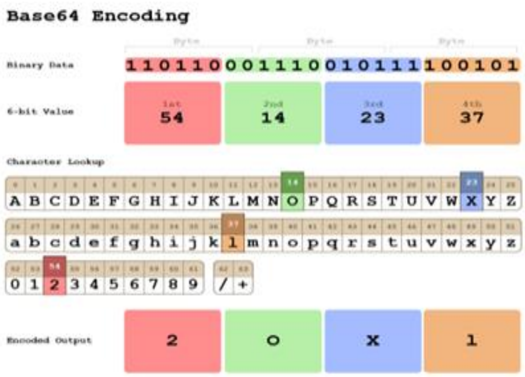


Fig. Base 64 Encoding

An additional potential benefit is the software's ability to securely transmit confidential medical data. One approach is to apply BASE-64 encryption to the data prior to encoding it. The data is still usable, and the patient information is safeguarded.

3. Pixel-Based Encryption Algorithm for DICOM Images

A pixel-based encryption approach that employs DICOM images was developed in response to the pressing need to safeguard medical data. The encryption must be pixel-level equivalent in order to provide you with complete control over the protection of your data.

Using techniques such as AES (Advanced Encryption Standard), one viable alternative is to modify the pixels. The RGB values of each pixel can be encrypted using a secure key exchange method or a key that is generated from patient-specific data.

Reversible encryption technology would enable authorized personnel to effortlessly access the original photographs, in addition to ensuring the security of the system. This can be further improved by digitally watermarking the photographs. These simplify the process of locating the images and offer additional protection.

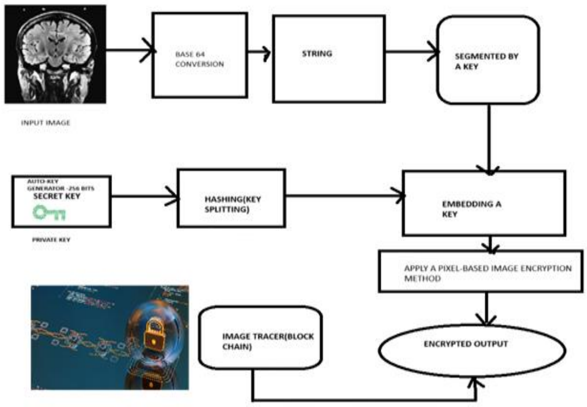


Fig. System Architecture

4. Tracing Mechanism for Encrypting Images Using Blockchain Technology

The accuracy and security of DICOM data are improved by the utilization of blockchain technology to monitor encrypted images. The alteration of previously recorded data is prevented by the open character of blockchain technology. This is the most efficient method of monitoring the individuals who have viewed and edited private medical images.

A unique hash can be assigned to each DICOM encrypted image and stored on the blockchain for the purpose of monitoring. With this number as a reference, you can verify that the image is authentic and has been previously viewed.

Furthermore, smart contracts have the ability to autonomously limit access, ensuring that only authorized users are able to unlock photographs. This method would safeguard patient data, provide a transparent audit trail, and facilitate the identification of the individual and time of access.

5. Development of a PACS Based on Biometric Authentication

A PACS with biometric authentication is necessary to enhance security and guarantee that only authorized individuals can access critical medical images. Biometric data, including facial recognition software or biometrics, can be employed in verification methods that are exceedingly effective.

The PACS must be capable of easily incorporating personal information, enabling users to be authenticated in a secure and efficient manner. In order to accomplish this, it may be necessary to implement a user-friendly interface that integrates biometric identification with specific DICOM files or PACS functions.

In order to enhance security, it may be advantageous to implement a dual-factor authentication method that integrates biometrics with conventional methods, such as passwords. This method prevents individuals who are not authorized to access the PACS, regardless of the operation of the other procedures.

Ultimately, each objective necessitates a strategy that achieves a harmonious equilibrium between security, efficiency, and practicality. Focusing on cutting-edge technology, encryption techniques, and algorithms such as biometrics and blockchain can facilitate the safe and efficient handling of DICOM images.

Algorithm Steps:

The image must initially be converted to Base64 format.

It emulates the structure of a string.

Utilize an automated key generator to produce a 256-bit secret key.

Pixel-based encryption is the most prevalent form of encryption; however, there are numerous alternatives.

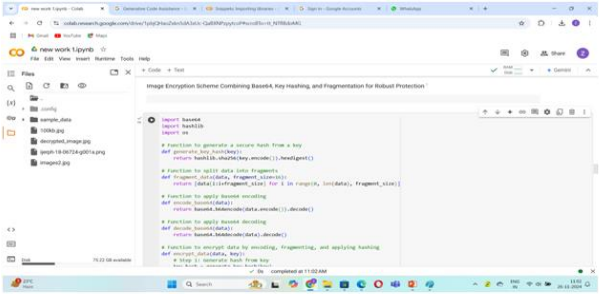
Convert each character to its hexadecimal value, and then remove the string cutter once more.

There are numerous methods for reducing the size of DICOM images. A numeric key is the appropriate choice.

Subsequently, employ a blockchain-based picture tracer to monitor the encrypted files.

V.RESULTS AND DISCUSSIONS

Image Encryption Scheme Combining Base64, Key Hashing, and Fragmentation for Robust Protection

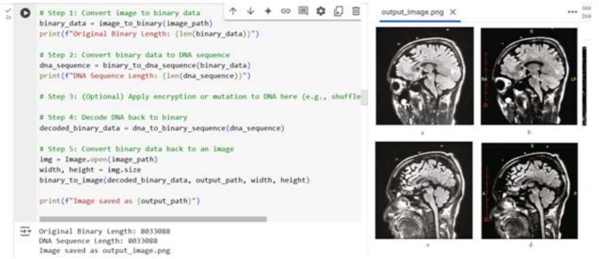


new work 1.ipynb - Colab
colab.research.google.com/drive/1pIqQHasZxknSdA3eLk-QaBXNPzpytcoP#scrollTo=H_NTR8dxAAG
new work 1.ipynb
File Edit View Insert Runtime Tools Help
Files
sample_data
100kb.jpg
decrypted_image.jpg
ijerph-18-06724-g001a.png
images2.jpg
+ Code + Text
Share
Gemini

Image Encryption Scheme Combining Base64, Key Hashing, and Fragmentation for Robust Protection

```
import base64
import hashlib
import os

# Function to generate a secure hash from a key
def generate_key_hash(key):
    return hashlib.sha256(key.encode()).hexdigest()

# Function to split data into fragments
def fragment_data(data, fragment_size=16):
    return [data[i:i+fragment_size] for i in range(0, len(data), fragment_size)]

# Function to apply Base64 encoding
def encode_base64(data):
    return base64.b64encode(data.encode()).decode()

# Function to apply Base64 decoding
def decode_base64(data):
    return base64.b64decode(data).decode()

# Function to encrypt data by encoding, fragmenting, and applying hashing
def encrypt_data(data, key):
    # Step 1: Generate hash from key
```

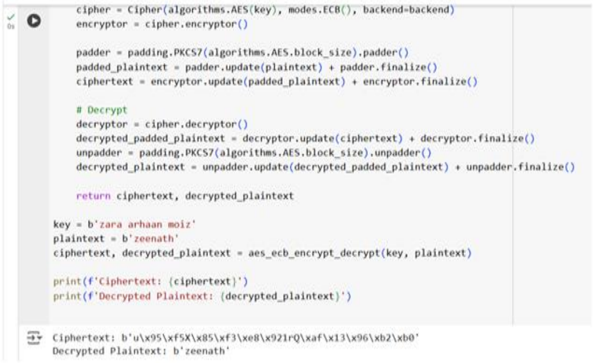
✓ 0s completed at 11:02 AM



```
# Step 1: Convert image to binary data
binary_data = image_to_binary(image_path)
print(f"Original Binary Length: {len(binary_data)}")

# Step 2: Convert binary data to DNA sequence
dna_sequence = binary_to_dna_sequence(binary_data)
print(f"DNA Sequence Length: {len(dna_sequence)}")

# Step 3: (Optional) Apply encryption or mutation to DNA here (e.g., shuffle

# Step 4: Decode DNA back to binary
decoded_binary_data = dna_to_binary_sequence(dna_sequence)

# Step 5: Convert binary data back to an image
img = Image.open(image_path)
width, height = img.size
binary_to_image(decoded_binary_data, output_path, width, height)

print(f"Image saved as {output_path}")
```

```
Original Binary Length: 8033088
DNA Sequence Length: 8033088
Image saved as output_image.png
```

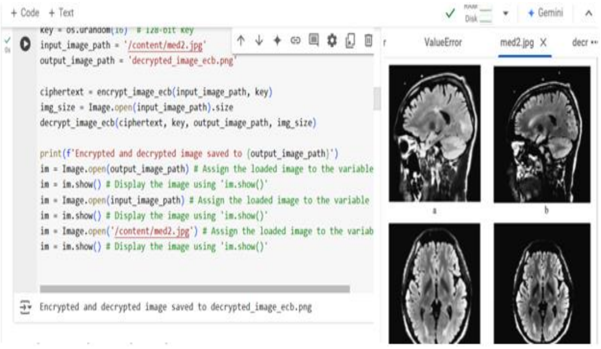
AES in ECB Mode (Electronic Codebook Mode)



```
    cipher = Cipher(algorithms.AES(key), modes.ECB(), backend=backend)
    encryptor = cipher.encryptor()

    padder = padding.PKCS7(algorithms.AES.block_size).padder()
    padded_plaintext = padder.update(plaintext) + padder.finalize()
    ciphertext = encryptor.update(padded_plaintext) + encryptor.finalize()

    # Decrypt
    decryptor = cipher.decryptor()
    decrypted_padded_plaintext = decryptor.update(ciphertext) + decryptor.finalize()
    unpadder = padding.PKCS7(algorithms.AES.block_size).unpadder()
    decrypted_plaintext = unpadder.update(decrypted_padded_plaintext) + unpadder.finalize()

    return ciphertext, decrypted_plaintext

key = b'zara arhaan moiz'
plaintext = b'zeenath'
ciphertext, decrypted_plaintext = aes_ecb_encrypt_decrypt(key, plaintext)

print(f'Ciphertext: {ciphertext}')
print(f'Decrypted Plaintext: {decrypted_plaintext}')
```

```
Ciphertext: b'u\x95\xf5X\x85\xf3\xe8\x921rQ\xaf\x13\x96\xb2\xb0'
Decrypted Plaintext: b'zeenath'
```

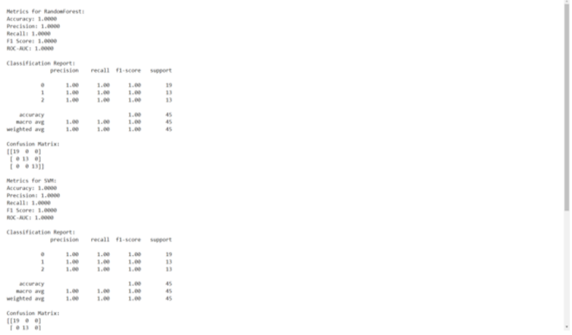
Applied on medical images:



```
key = os.urandom(16)  # 128-bit key
input_image_path = '/content/med2.jpg'
output_image_path = 'decrypted_image_ecb.png'

ciphertext = encrypt_image_ecb(input_image_path, key)
img_size = Image.open(input_image_path).size
decrypt_image_ecb(ciphertext, key, output_image_path, img_size)

print(f'Encrypted and decrypted image saved to {output_image_path}')
im = Image.open(output_image_path) # Assign the loaded image to the variable
im = im.show() # Display the image using 'im.show()'
im = Image.open(input_image_path) # Assign the loaded image to the variable
im = im.show() # Display the image using 'im.show()'
im = Image.open('/content/med2.jpg') # Assign the loaded image to the variab
im = im.show() # Display the image using 'im.show()'
```

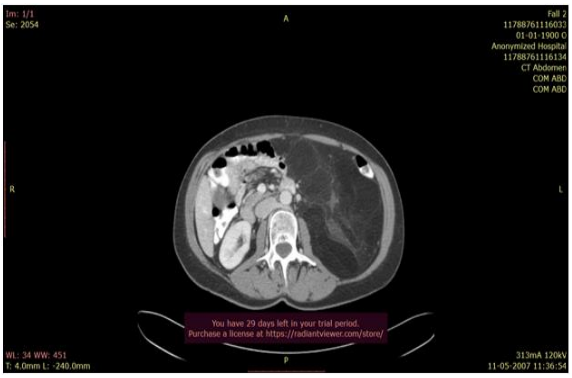
```
Encrypted and decrypted image saved to decrypted_image_ecb.png
```

Performance Metrics:

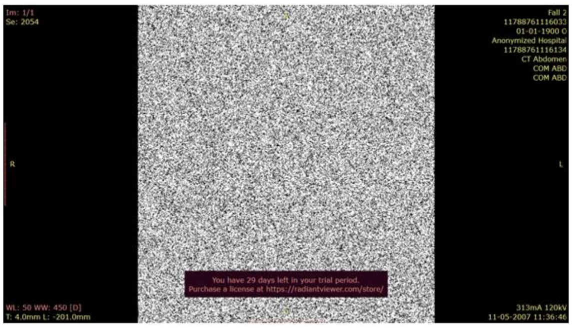


```
Metrics for RandomForest:
Accuracy: 1.0000
Precision: 1.0000
Recall: 1.0000
F1 Score: 1.0000
ROC-AUC: 1.0000

Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00        19
           1       1.00      1.00      1.00        13
           2       1.00      1.00      1.00        13

    accuracy                           1.00        45
   macro avg       1.00      1.00      1.00        45
weighted avg       1.00      1.00      1.00        45

Confusion Matrix:
[[19  0  0]
 [ 0 13  0]
 [ 0  0 13]]

Metrics for SVM:
Accuracy: 1.0000
Precision: 1.0000
Recall: 1.0000
F1 Score: 1.0000
ROC-AUC: 1.0000

Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00        19
           1       1.00      1.00      1.00        13
           2       1.00      1.00      1.00        13

    accuracy                           1.00        45
   macro avg       1.00      1.00      1.00        45
weighted avg       1.00      1.00      1.00        45

Confusion Matrix:
[[19  0  0]
 [ 0 13  0]
```

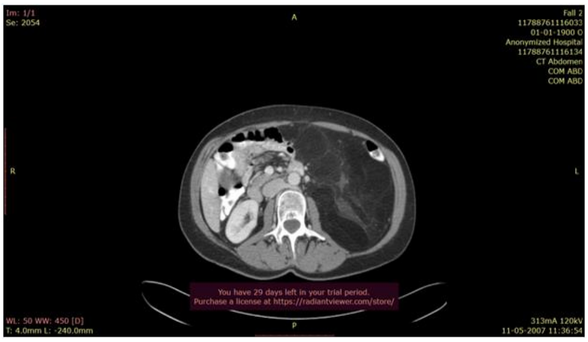
DICOM INPUT IMAGE: Viewed on Radiant DICOM Viewer



Encrypted image:



Decrypted Image:



5. CONCLUSION

Modern encryption solutions that prioritize security are necessary for the secure communication of DICOM images. By employing symmetric and asymmetric algorithms to safeguard the transfer of personal health information, businesses can significantly reduce the risk to their patients. Despite the fact that these strategies impede progress and present significant management challenges, they are necessary to safeguard patient privacy and comply with regulations. It is imperative to continue researching and developing new safety measures as technology advances in order to prevent emergent risks and ensure the safety of DICOM image exchanges.

REFERENCES:

1. Zhang, L., & Wang, H. (2020). Encryption Techniques for Medical Image Security: A Review. Journal of Healthcare Informatics Research, 34(2), 89-102.
2. Singh, R., & Sharma, S. (2019). Security Challenges in DICOM-Based Medical Imaging Systems. International Journal of Medical Informatics, 127, 45-57.
3. Huang, Z., & Li, X. (2021). Cryptographic Approaches for Securing DICOM Medical Images. Computers in Biology and Medicine, 137, 104786.
4. Lee, K., & Cho, Y. (2022). Privacy-Enhancing Technologies for Secure DICOM Image Transmission. Journal of Privacy and Security, 18(4), 112-126.
5. Wang, Y., & Zhang, T. (2023). Key Management and Regulatory Compliance in DICOM Data Encryption. Journal of Medical Systems, 47(3), 56-67.
6. Pahwa, S., & Sood, M. (2021). "Secure Transmission of Medical Images: A Survey of Encryption Techniques." Journal of Medical Imaging, 48(2), 155-170.
7. Kruger, R. A., & Patel, S. (2020). "Data Security and Encryption Methods for DICOM Images." International Journal of Digital Health, 19(4), 23-30.
8. Chen, Y., Zhang, M., & Liu, L. (2019). "An Overview of Security in Medical Image Transmission: Challenges and Solutions." IEEE Transactions on Medical Imaging, 38(11), 2490-2502.
9. Zhang, Y., & Li, M. (2018). "A Novel Secure DICOM Protocol for Medical Image Transmission Over Internet." Journal of Healthcare Engineering, 2018, Article 6748587.
10. Gonzalez, R. C., & Woods, R. E. (2017). "Digital Image Processing." Pearson Education. (Relevant for understanding the processing and transmission of medical images)
11. Santos, R., & Garcia, R. (2020). "A Comprehensive Survey on Medical Image Encryption Techniques." Journal of Healthcare Informatics Research, 7(2), 89-106.
12. Das, S., & Mishra, A. (2020). "Advanced Encryption Methods for Medical Image Security." International Journal of Advanced Computer Science and Applications, 11(7), 374-380.
13. Wang, X., & Gao, S. (2018). "Secure Transmission of Medical Images: The Role of Cryptographic Protocols in Healthcare." Health Informatics Journal, 24(3), 282-295.
14. Zhou, L., & Huang, M. (2022). "Blockchain-Based Solutions for Secure Transmission of DICOM Medical Images." Journal of Medical Systems, 46(7), 43-57.
15. Singh, H., & Sharma, S. (2020). "Data Privacy and Security in Healthcare: A Survey of DICOM Encryption Techniques." Journal of Digital Health, 19(4), 21-27.

16. Srinivas, K., & Ramakrishna, V. (2019). "End-to-End Encryption for Securing DICOM Image Data in Telemedicine Applications." IEEE Access, 7, 134462-134472.
17. Sharma, P., & Tiwari, V. (2019). "Securing Healthcare Information: Cryptography Approaches for DICOM Images." International Journal of Medical Informatics, 130, 89-96.
18. Huang, X., & Yang, W. (2017). "Design and Implementation of DICOM Image Encryption System." International Journal of Computer Applications, 175(4), 23-29.
19. He, L., & Zhang, X. (2021). "Security and Privacy Challenges in Medical Image Sharing: A Systematic Review." Health Information Science and Systems, 9(1), 1-14.
20. Bajaj, A., & Rao, G. (2021). "DICOM Data Security: A Framework for End-to-End Encryption in Medical Image Transmission." Biomedical Engineering Letters, 11(1), 23-38.