**DICOM to JPEG 2000 Conversion with Integrated AES Encryption for Secure & Fast Medical Image Transfer**

***Report submitted in fulfilment of the Requirements for the Degree***

***Of***

***B. Tech. in Computer Science and Engineering***

**Submitted by**

**Aashiq Rahaman**

University Roll No: 10000122020

Registration No: 221000110175 of 2022-23

**Under the supervision of**

**Mr. Mihir Sing Dr. Koushik Majumder**

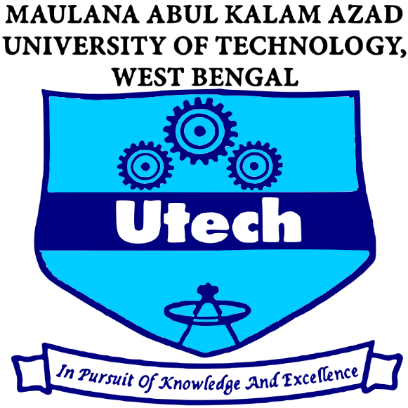
Assistant Professor, Associate Professor,

Dept. of CSE, MAKAUT, WB Dept. of CSE, MAKAUT, WB

**Dr. Saikat Basu Mr. Santanu Chatterjee**

Associate Professor, Assistant Professor,

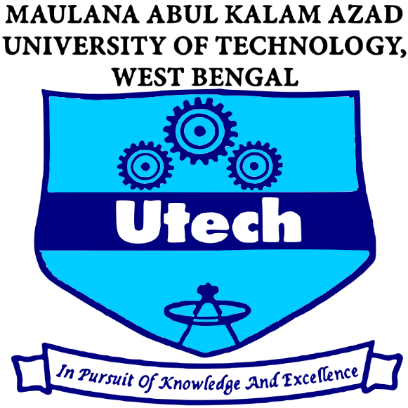
Dept. of CSE, MAKAUT, WB Dept. of CSE, MAKAUT, WB



**Maulana Abul Kalam Azad University of Technology, West Bengal, Department of Computer Science and Engineering, Simhat, Haringhata, Nadia-741249, West Bengal**

**July - 2025**

**APPROVAL**



This is to approval that the dissertation report titled **“DICOM to JPEG 2000 Conversion with Integrated AES Encryption for Secure & Fast Medical Image Transfer,”** submitted by Aashiq Rahaman, University Roll No: 10000122020, Registration No: 221000110175 of 2022-23 to MAKAUT, WB, India, is an original piece of work carried out under my supervision and guidance.

I believe this report reflects sincere effort and good understanding of the subject. It is worthy of consideration for the award of the degree of **Bachelor of Technology in Computer Science and Engineering.**

**--------------------------------------------------------------------- ---------------------------------------------------------------------**

***Signature of the Project Supervisor Signature of the Project Supervisor***

**Mr. Mihir Sing Dr. Koushik Majumder**

Assistant Professor, Associate Professor,

Dept. of CSE, MAKAUT, WB Dept. of CSE, MAKAUT, WB

**--------------------------------------------------------------------- ---------------------------------------------------------------------**

***Signature of the Project Supervisor Signature of the Project Supervisor***

**Dr. Saikat Basu Mr. Santanu Chatterjee**

Associate Professor, Assistant Professor,

Dept. of CSE, MAKAUT, WB Dept. of CSE, MAKAUT, WB

**----------------------------------------------**

***Signature of the Head of the Dept.***

Dept. of CSE, MAKAUT, WB

**ACKNOWLEDGEMENTS**

It gives me great pleasure to present this report on **“DICOM to JPEG 2000 Conversion with Integrated AES Encryption for Secure & Fast Medical Image Transfer.”** I am deeply grateful to all Supervisors for their valuable guidance and support throughout this work. Their insights helped me understand complex topics and stay focused on my goals.

I also wish to thank the faculty and staff of our department for providing the resources and encouragement that made this report possible.

My sincere thanks go to my friends and classmates, who shared ideas and offered help whenever I needed it.

Above all, I am thankful to my family for their patience, constant motivation, and belief in me. Their support kept me going, even during challenging times.

Completing this report has been a rewarding experience, and I am grateful to everyone who contributed to it in any way.

-------------------------------- Date: 08.07.2025

**Aashiq Rahaman**

University Roll No: 10000122020,

Registration No: 221000110175 of 2022-23,

B.Tech, CSE, MAKAUT, WB

## Contents

[ABSTRACT 4](#_Toc202747356)

[INTRODUCTION 4](#_Toc202747357)

[PROBLEM DEFINITION 5](#_Toc202747358)

[PROPOSED WORK 5](#_Toc202747359)

Comparison of Image Encryption and Conversion Techniques 7

[METHODOLOGY: CASE STUDY 8](#_Toc202747360)

[FUTURE SCOPE 11](#_Toc202747361)

[CONCLUSION 11](#_Toc202747362)

[REFERENCES 12](#_Toc202747363)

# ABSTRACT

Converting DICOM medical images to JPEG 2000 format with integrated AES encryption offers a practical and secure solution for managing large volumes of diagnostic imaging data. DICOM files, while rich in metadata and essential for clinical use, are often large and difficult to handle in networked environments. JPEG 2000 addresses this challenge by providing high-quality compression—both lossy and lossless—without sacrificing the integrity of clinical details. This significantly reduces storage requirements and improves transmission speed, which is especially valuable in bandwidth-limited healthcare settings.

To ensure that sensitive patient data remains protected during and after this conversion, the process incorporates AES encryption in Cipher Block Chaining (CBC) mode. Each image is encrypted individually using a secure key derived from a user password through SHA-256 hashing, along with a unique initialization vector. This adds a strong layer of confidentiality, making unauthorized access or tampering extremely difficult. Once encrypted, only authorized users with the correct key can restore and view the original image.

By combining efficient compression with robust encryption, this approach supports faster, safer, and more scalable medical image sharing, while maintaining compliance with privacy standards and clinical accuracy. It integrates well with existing PACS systems and strengthens both storage management and patient data security.

# INTRODUCTION

Medical imaging plays a vital role in diagnosing and treating patients. Most hospitals and clinics store and share these images using the DICOM format—short for Digital Imaging and Communications in Medicine. DICOM is more than just an image file; it includes important patient and scan details, making it the standard format used in radiology, CT, MRI, and other imaging systems. While DICOM is great for compatibility and detail, the files can be quite large and difficult to manage, especially when images need to be transferred quickly or stored in bulk.

That’s where JPEG 2000 comes in. JPEG 2000 is a modern image compression format that keeps image quality high while reducing file size significantly. Unlike older formats, it supports both lossy and lossless compression, which is essential for maintaining diagnostic accuracy in medical images. Converting DICOM files to JPEG 2000 can ease the burden on storage systems and speed up image sharing across hospitals or healthcare networks.

However, reducing file size isn't enough. These images often contain private and sensitive patient data. To protect this information, AES (Advanced Encryption Standard) encryption can be applied during or after conversion. AES helps ensure that only authorized users can access the images. Using strong encryption like AES in combination with efficient compression supports fast, secure, and reliable transfer of medical images—something that’s becoming increasingly important in digital healthcare environments.

# PROBLEM DEFINITION

Medical images are an important part of patient care. They help doctors diagnose and treat illnesses. These images are usually stored in a format called **DICOM** (Digital Imaging and Communications in Medicine). DICOM files include both the image and patient details, which makes them useful but also very large in size.

Large file sizes cause problems. Hospitals need more storage space, and sending these images over networks can be slow. This is a challenge for systems that rely on fast access, like emergency care or remote consultations.

Another serious issue is **privacy**. Medical images often contain personal information. If these files are not protected, they can be accessed or stolen by unauthorized users. This could lead to data breaches and loss of patient trust.

**JPEG 2000** is a newer image format that can reduce file size without losing important image details. It is good for medical use because it supports high-quality compression.

To protect privacy, **AES encryption** (Advanced Encryption Standard) can be used. It locks the image so that only people with the correct key can open it.

This project solves two problems at once: it reduces image size using JPEG 2000 and protects sensitive data with AES encryption, making medical image sharing both faster and safer.

# PROPOSED WORK

DICOM (Digital Imaging and Communications in Medicine) is the industry standard for storing and transmitting medical images. It combines image data with patient information, scan parameters, and other metadata in a single, unified format. This makes it essential for use in clinical systems like PACS (Picture Archiving and Communication Systems) and EHRs (Electronic Health Records). However, DICOM files are often large, especially when dealing with high-resolution scans like CT or MRI. These large sizes can create challenges for storage, backup, and especially transmission over limited-bandwidth networks.

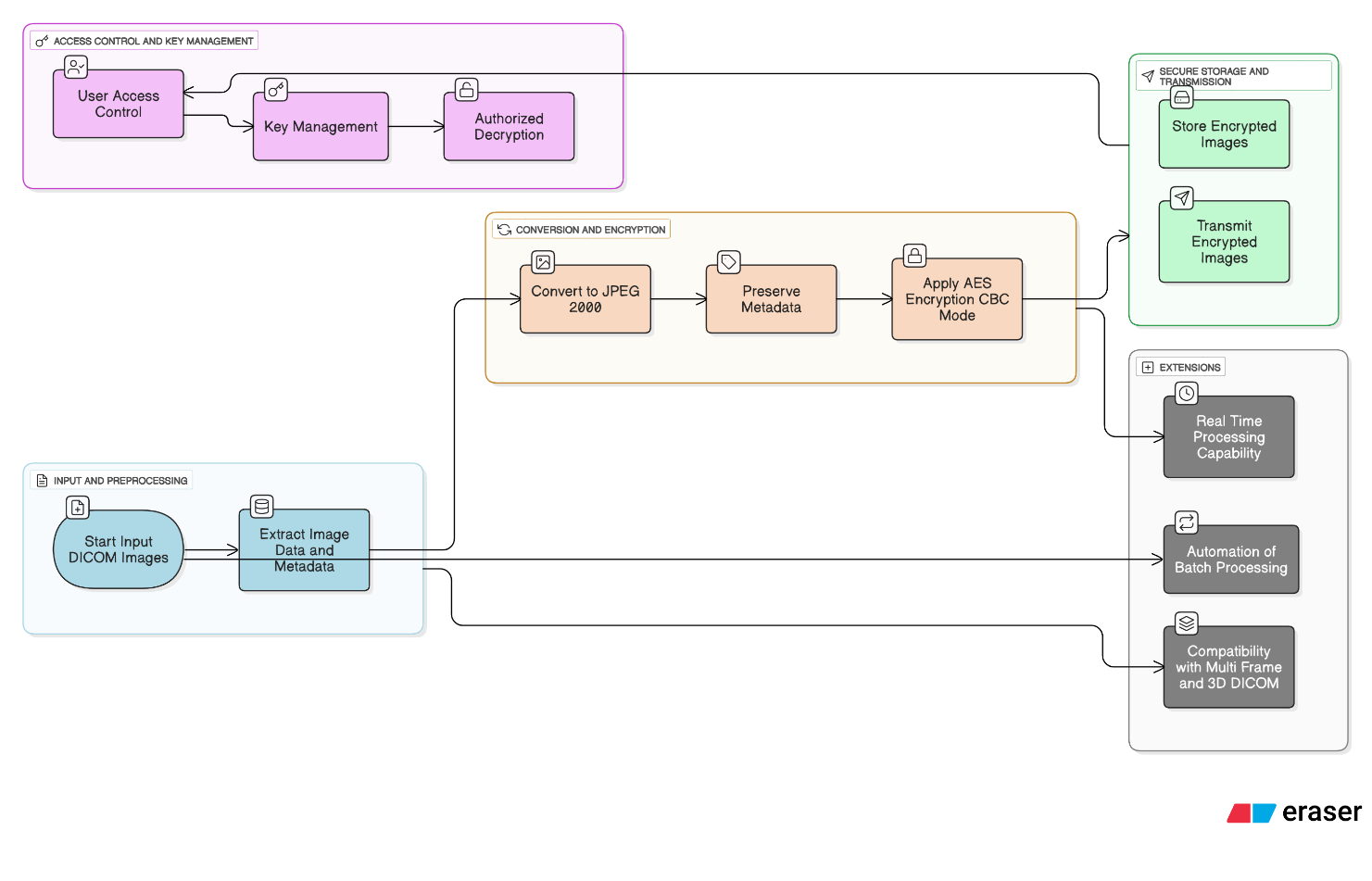
To address this, researchers have explored converting DICOM images into more storage-efficient formats. JPEG 2000 stands out among compression formats due to its support for both lossy and lossless compression. It also allows for progressive transmission and region-of-interest encoding—features that are particularly useful in medical imaging. Kim et al. (2011) showed that high compression ratios can be achieved with JPEG 2000 without sacrificing diagnostic accuracy. This makes it a strong candidate for clinical image management.

While compression improves efficiency, it does not guarantee data privacy. Medical images often contain sensitive personal data, and securing that information is a legal and ethical requirement. AES (Advanced Encryption Standard) is widely used in healthcare settings to encrypt data during transmission and storage. It is fast, secure, and well-tested. In CBC (Cipher Block Chaining) mode, AES provides strong protection against unauthorized access and pattern recognition, especially when combined with secure key generation methods like SHA-256 hashing.

Despite these advances, existing methods often come with limitations. Some systems separate the compression and encryption steps, leading to added complexity and longer processing times. Others depend on specialized hardware or proprietary software, which limits their accessibility and adoption in smaller or less-resourced medical facilities. Additionally, not all implementations provide flexibility across various DICOM formats or handle metadata preservation well during conversion.

There’s also room for improvement in user access control and integration with hospital systems. Many approaches lack seamless integration with PACS or do not offer scalable workflows for bulk image processing. Key management—ensuring only authorized users can decrypt data—remains another challenge in real-world healthcare environments.

This project builds on previous research by offering a unified, script-based solution for converting DICOM images to JPEG 2000 while applying AES encryption in a single workflow. The goal is to make medical image transfer faster, lighter on storage, and secure—without requiring complex infrastructure. There is scope to further enhance this approach by adding support for automation, real-time processing, and broader compatibility with multi-frame and 3D DICOM datasets.



### Comparison of Image Encryption and Conversion Techniques

| **Technique** | **How It Works** | **What’s Good About It** | **What’s Not So Great** |
| --- | --- | --- | --- |
| **Standard AES Image Encryption**  (Paavni Gaur) | Uses the AES algorithm to encrypt image pixels directly using a fixed key. | Strong encryption with proven security; widely supported. | Doesn't consider image structure; fixed S-Box can be predictable. |
| **Modified AES for Images**  (MAES - IJERT Paper) | Adds custom key expansion and changes image block structure before applying AES. | Faster, better PSNR and entropy; more secure against attacks. | Custom changes add complexity; might not follow standard AES practices. |
| **Dynamic AES with Key-Dependent S-Box**  (Dynamic AES Paper) | S-Box is created using the encryption key, so it changes with every key. | Harder to predict or reverse; better pixel confusion. | More complex to implement; slight increase in encryption time. |
| **Hybrid AES with Arnold Map**  (Phys. Scripta, Inam et al.) | Scrambles image pixels using chaotic Arnold map, then encrypts with AES. | High NPCR and UACI; very secure and resistant to visual attacks. | Slow with high-res images; Arnold map needs careful tuning. |
| **Hybrid AES with Quadratic Chaotic Map**  (Medical Image Encryption Hybrid AES Paper) | Rearranges pixel positions using a chaotic map, then encrypts with AES. | High entropy and low correlation; strong against brute-force attacks. | Decryption requires exact same map and key setup; may be sensitive to errors. |
| **JPEG 2000 Fidelity Prediction from DICOM Headers**  (Medical Physics Paper) | Predicts how well compressed CT images will retain quality using DICOM metadata and machine learning. | Avoids trial-and-error; fast decision-making for compression. | Doesn't perform actual encryption or compression; just prediction. |
| **DICOM to JPEG 2000 with Integrated AES Encryption**  **(IEEE International)** | Converts DICOM to JPEG 2000 using Python, then applies AES in CBC mode with a hashed key. | 79.91% file size reduction, strong AES security, easy to integrate into systems like PACS. | Only handles 2D images; lacks automation or advanced user access control—for now. |

Medical image encryption and compression have become essential in today’s healthcare systems. As hospitals shift toward digital storage and remote sharing, protecting image quality and patient privacy has grown more complex—and more important.

One thing is clear: **DICOM** is the foundation. It's the standard format for storing medical images because it carries not only the image data but also critical patient information and scan details. However, DICOM files are often large and not always easy to work with, especially when it comes to network transfers or cloud-based systems.

To deal with size issues, many approaches focus on **image compression**, and **JPEG 2000** has emerged as a strong solution. Unlike older formats like standard JPEG, JPEG 2000 offers better control over image quality and supports both lossy and lossless modes. This makes it a practical choice for storing large datasets without losing important diagnostic information.

But compression alone isn’t enough. Medical images often carry sensitive personal data. To prevent unauthorized access, researchers have explored different encryption techniques—most commonly **AES (Advanced Encryption Standard)**. It's trusted across industries for its balance of speed and strong security. Many techniques take AES further by mixing it with **chaotic maps**, **dynamic S-Boxes**, or **custom key expansion** methods. These additions improve resistance to pattern attacks, boost entropy, and make the encrypted output harder to reverse-engineer.

Interestingly, some papers also focus on **predicting image quality** before compression, using metadata from the DICOM headers. These techniques don’t encrypt or compress directly, but they help guide those processes, making them more efficient.

Across all these efforts, the goal remains the same: to keep medical images secure, efficient to store, and quick to transfer—without compromising the quality doctors rely on. While each method offers different strengths, the best solutions find a smart balance between image fidelity, data protection, and system performance.

# METHODOLOGY: CASE STUDY

This project uses a two-phase method: converting DICOM files to JPEG 2000 and encrypting the output using AES. The entire process is implemented in Python, using libraries like pydicom, imageio, and pycryptodome.

**Phase 1: DICOM to JPEG 2000 Conversion and Preparation**

1. **Reading the DICOM File**  
   The script begins by loading the DICOM file using pydicom.dcmread(). This allows access to both image data and metadata. We focus on the image data stored as a pixel array.

**import pydicom**

**dataset = pydicom.dcmread(input\_path)**

**pixel\_array = dataset.pixel\_array**

1. **Normalizing Pixel Data**  
   DICOM images often use 12-bit or 16-bit grayscale. These values are converted to 8-bit by scaling them between 0 and 255. This makes the image readable by standard viewers and compatible with JPEG 2000.

**image = ((pixel\_array - pixel\_array.min()) / (pixel\_array.max() - pixel\_array.min()) \* 255).astype('uint8')**

1. **Saving the Image in JPEG 2000 Format**  
   The normalized image is saved using imageio.imwrite() in .jp2 format. This format provides good compression while keeping medical image quality intact.

**import imageio**

**imageio.imwrite(temp\_jp2\_path, image, format='jp2'**)

**Phase 2: AES Encryption of the JPEG 2000 Image**

1. **Reading the JPEG 2000 File**  
   After conversion, the .jp2 file is opened in binary mode. This prepares it for encryption.

**with open(temp\_jp2\_path, 'rb') as f:**

**image\_data = f.read()**

1. **Generating the AES Key**  
   The user provides a password. This password is hashed using SHA-256 to generate a secure 32-byte key.

**from Crypto.Hash import SHA256**

**key = SHA256.new(password.encode()).digest()**

1. **Encrypting the Image Data**  
   A 16-byte random Initialization Vector (IV) is created for each session. AES encryption is performed in CBC mode with PKCS7 padding to handle block size alignment.

**from Crypto.Cipher import AES**

**from Crypto.Util.Padding import pad**

**from Crypto.Random import get\_random\_bytes**

**iv = get\_random\_bytes(16)**

**cipher = AES.new(key, AES.MODE\_CBC, iv)**

**encrypted\_data = cipher.encrypt(pad(image\_data, AES.block\_size))**

1. **Saving the Encrypted Image**  
   The IV and encrypted content are combined and saved in a new file with a .enc extension. The original JPEG 2000 file is deleted for security.

**with open(enc\_path, 'wb') as f:**

**f.write(iv + encrypted\_data)**

**os.remove(temp\_jp2\_path)**

**Decryption and Image Recovery**

To decrypt, the same password is used to recreate the AES key. The IV is read from the first 16 bytes of the encrypted file. The rest is decrypted, unpadded, and saved back to .jp2 format.

**from Crypto.Util.Padding import unpad**

**with open(enc\_file, 'rb') as f:**

**iv = f.read(16)**

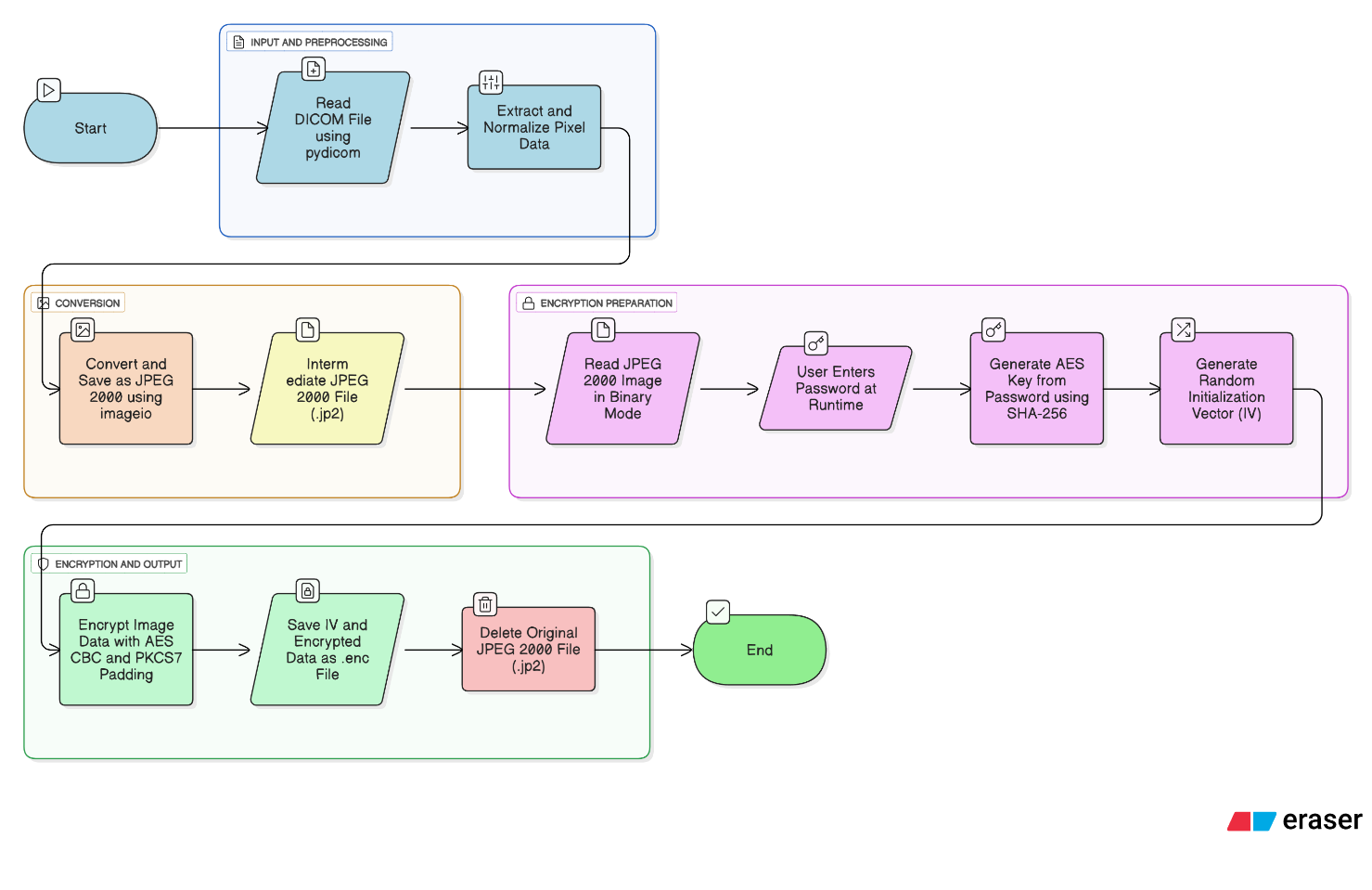
**encrypted\_data = f.read()**

**cipher = AES.new(key, AES.MODE\_CBC, iv)**

**decrypted\_data = unpad(cipher.decrypt(encrypted\_data), AES.block\_size)**

**with open(output\_path, 'wb') as f:**

**f.write(decrypted\_data)**

The decrypted image can then be viewed or converted into formats like PNG using libraries such as PIL.

# FUTURE SCOPE

This project provides a secure way to compress and transfer medical images, but there is room to make it even better. One area for improvement is **conversion speed**. As hospitals deal with thousands of images daily, faster processing would help in real-time situations, especially in emergency care or telemedicine.

There’s also potential to explore **newer encryption techniques**. While AES is strong and widely trusted, adding layers like digital signatures or biometric-based access could improve data protection even further.

Future versions could support more complex **DICOM formats**, such as multi-frame images, 3D volumes, or ultrasound video clips. Handling these would make the tool more useful in a wider range of clinical settings.

Integration into **existing hospital systems** is another key step. Connecting directly to PACS or EHR platforms would allow smoother workflows and less manual effort from medical staff.

Finally, the system could be enhanced to support **privacy compliance checks**, helping ensure that all image transfers meet laws like HIPAA or GDPR. Adding automated logging and audit features would make it easier for hospitals to track who accessed which images and when.

Overall, there’s strong potential to expand this system into a full-featured tool for secure, efficient, and compliant medical image sharing.

# CONCLUSION

This project presents a practical solution for securing medical images by converting DICOM files to the JPEG 2000 format and applying AES encryption. The use of JPEG 2000 ensures efficient storage while preserving the high quality needed for medical diagnostics. AES encryption adds a robust layer of security, safeguarding sensitive patient information during storage and transmission. The methodology integrates standard Python tools, making the solution accessible and easy to implement in real-world healthcare systems. Overall, this approach reduces file size, ensures compatibility with modern viewers, and meets privacy requirements such as HIPAA. It offers a balanced, efficient, and secure method for managing medical imaging data, enhancing both operational efficiency and patient confidentiality in healthcare environments.

# REFERENCES

1. Siam, A. A., Hassan, M. M., & Bhuiyan, T. (2025). *Secure Medical Imaging: A DICOM to JPEG 2000 Conversion Algorithm with Integrated Encryption*. Proceedings of the 4th IEEE International Conference on AI in Cybersecurity (ICAIC), University of Houston, Texas.
2. Gaur, P. (2023). *AES Image Encryption (Advanced Encryption Standard)*. Maharaja Agrasen Institute of Technology.
3. Inam, A., et al. (2023). *A New Method of Image Encryption Using Advanced Encryption Standard (AES) for Network Security*. Physica Scripta, 98(12), 126005.
4. Gaur, P. (2022). *A New Image Encryption using Modified AES Algorithm and its Comparison with AES*. International Journal of Engineering Research & Technology (IJERT), 11(5).
5. Chen, X., et al. (2011). *Predicting the Fidelity of JPEG2000 Compressed CT Images Using DICOM Header Information*. Medical Physics, 38(12), 6449–6457.
6. Unknown Author. (2023). *Medical Image Encryption Based on Hybrid AES with Chaotic Map*.
7. Gokul, B., et al. (2023). *A Web-Based DICOM Image and Plane Viewer*. Proceedings of the Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT).