AI in Encryption

Presentation 3

Vaishnavi D
Aarushi Garg
Ishita Singh
Sunayana

Potential Research Gap: ?

- The lack of effective encryption methods that are specifically tailored to thwart AI models from learning and reproducing protected images.
- Using ML models in image encryption is unexplored

OBJECTIVES

1) Using mulitple machine learning algorithms and comparing them to encrypt and decrypt images.

2) Providing a visual representation and error metrics for each algorithm.

Algorithm Analysis

1)Image Loading and Preprocessing:

- The load_image() function loads and resizes the image to a consistent size of 100x100 pixels.
- Resizing the image simplifies processing and ensures a consistent input size for encryption methods.

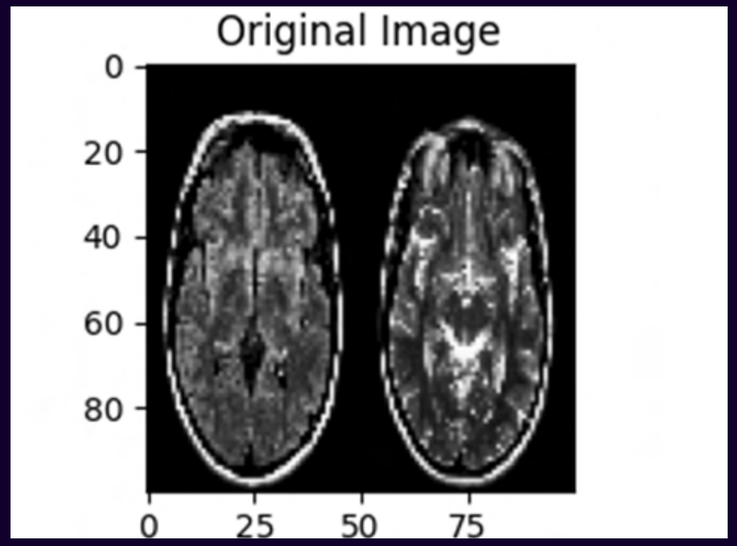
2)Flattening the Image:

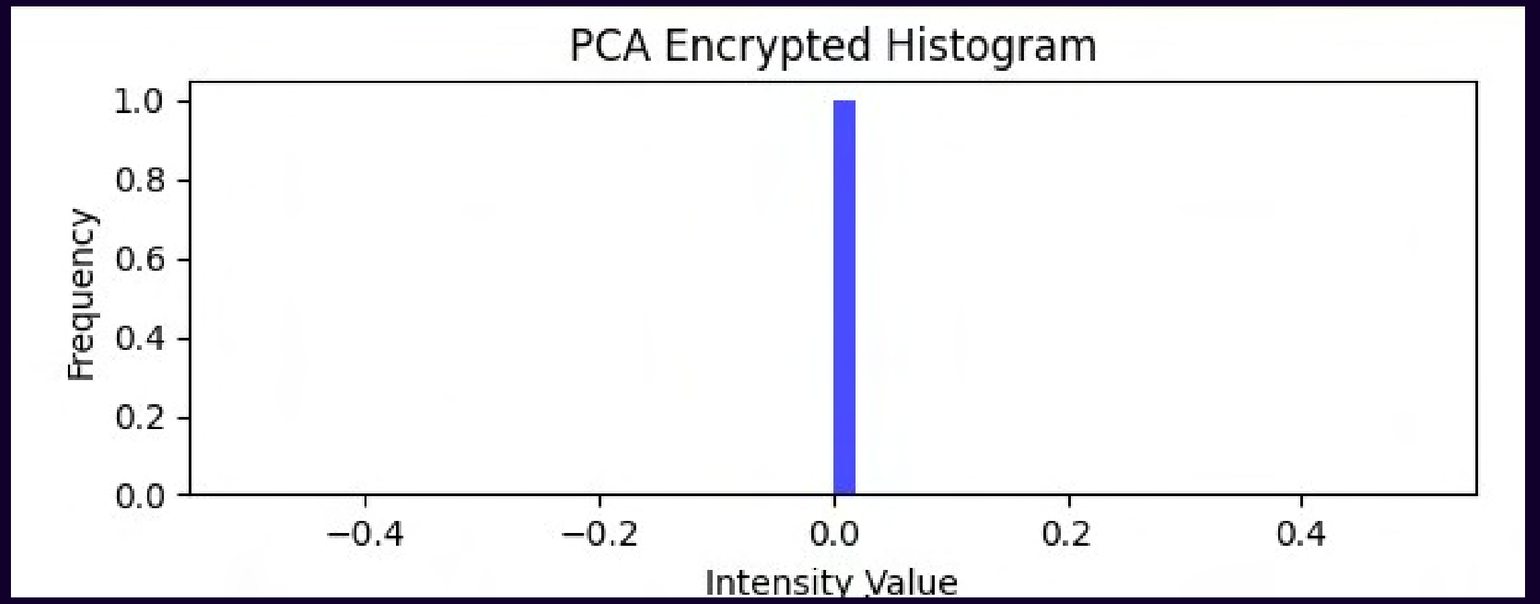
- The flatten_image() function reshapes the 100x100 grayscale image to a 1D array of 10,000 elements, then normalizes pixel values to be between 0 and 1.
- Flattening makes it compatible with the PCA, K-Means, and GMM algorithms

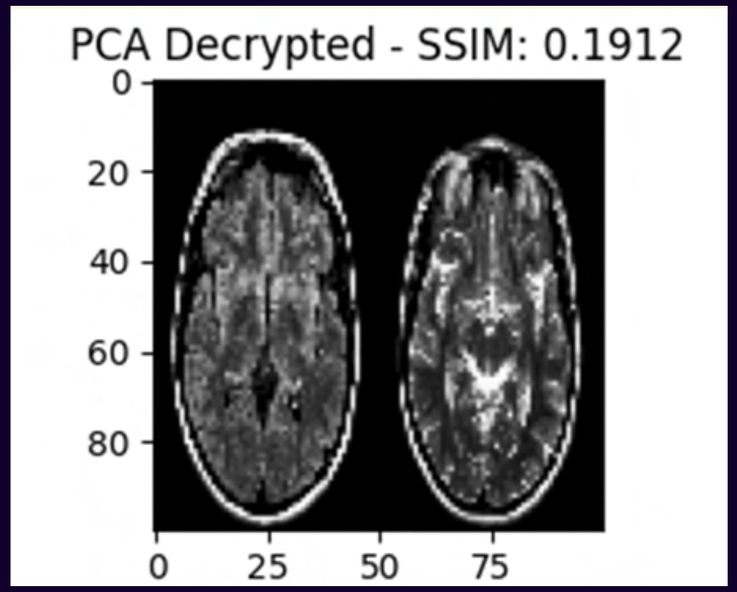
3)PCA Encryption and Decryption:

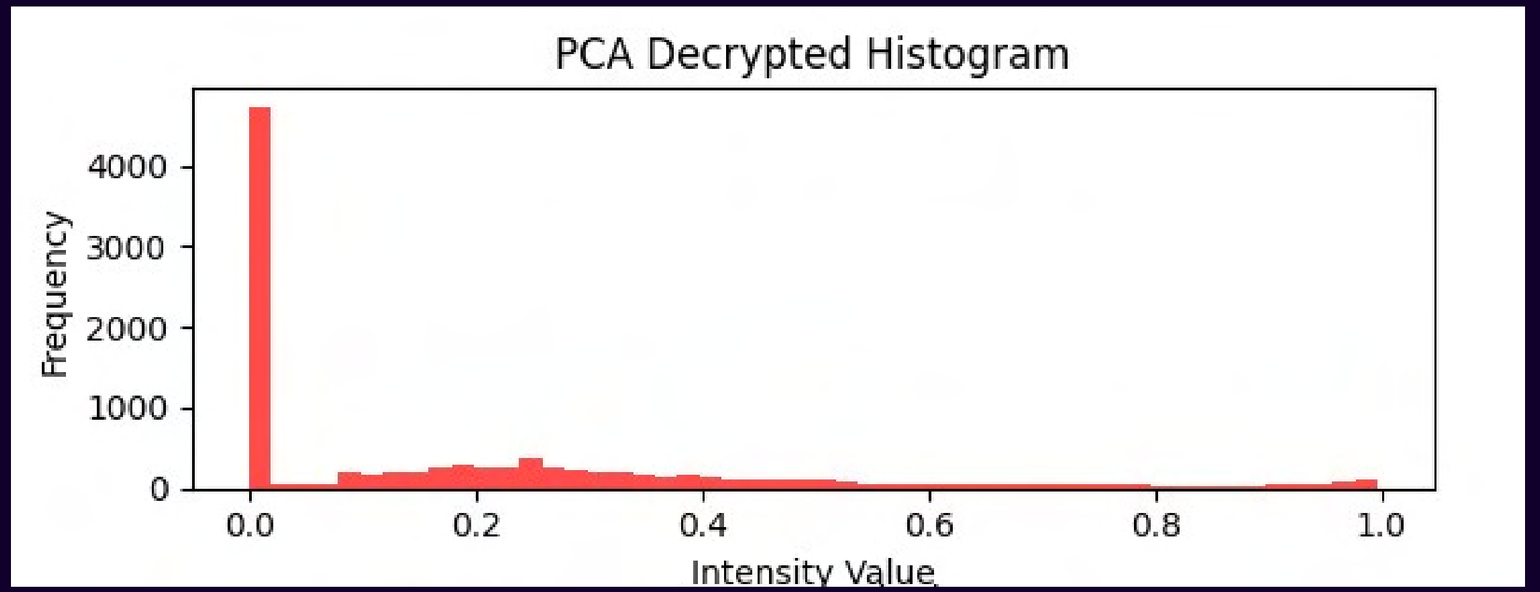
- **Encryption: PCA reduces the dimensionality of the flattened image, creating a compressed, transformed version (used as the "encrypted" image).**

- **Decryption: The inverse transform reconstructs the image from its compressed form, creating a "decrypted" image.**







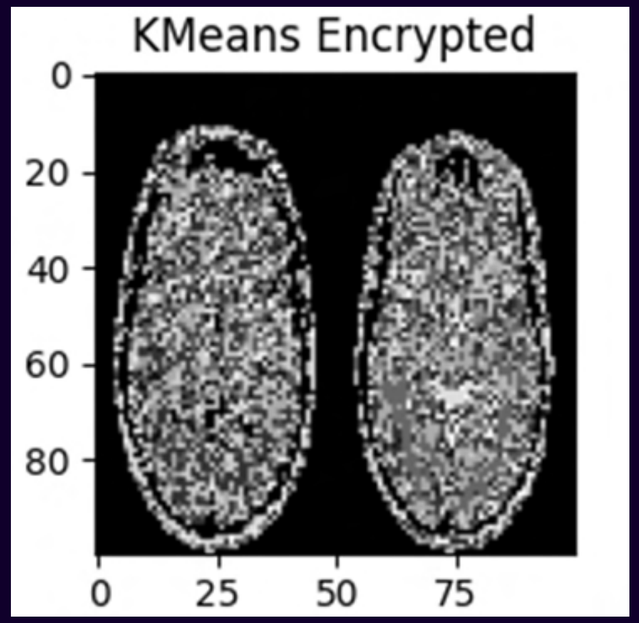


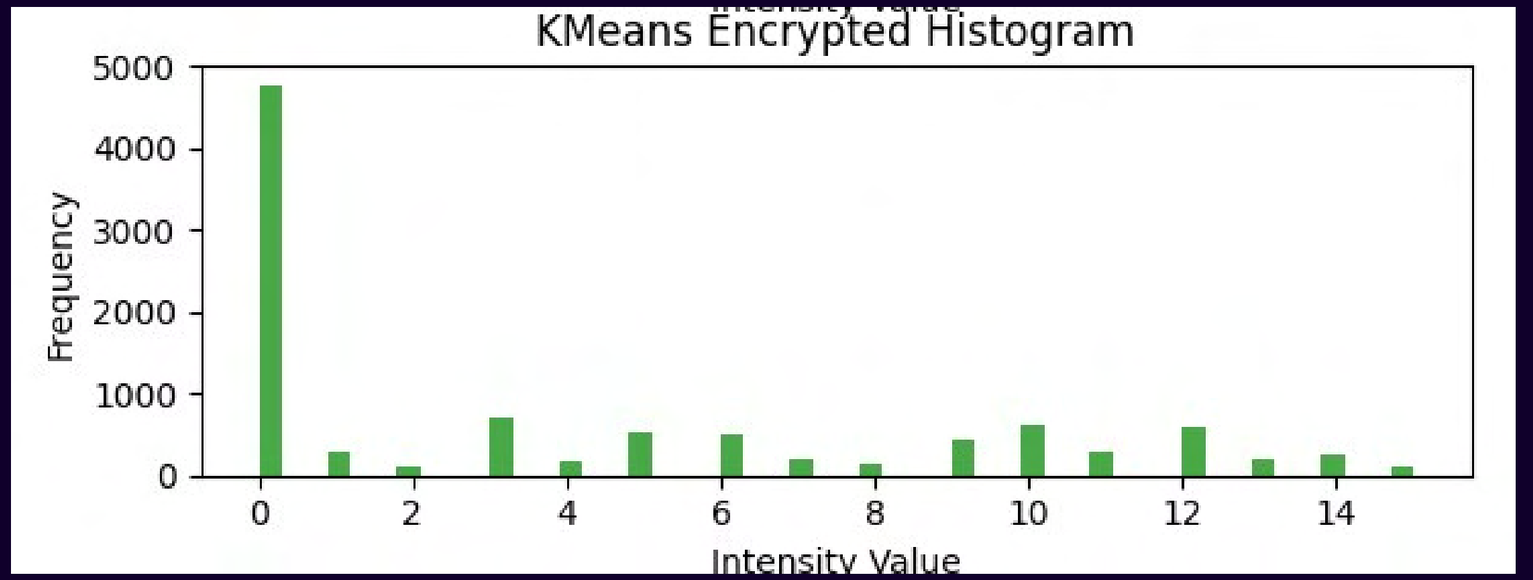
img src: https://sjra.com/can-you-see-a-brain-tumor-on-an-mri-scan/

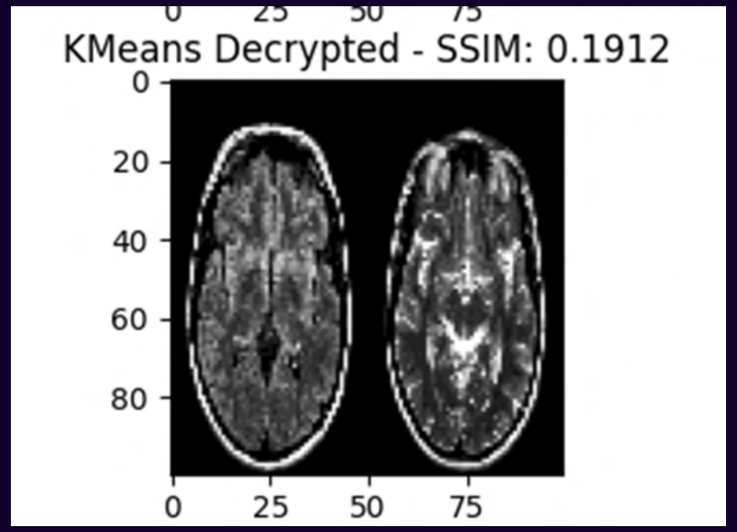
4) K-Means Encryption and Decryption:

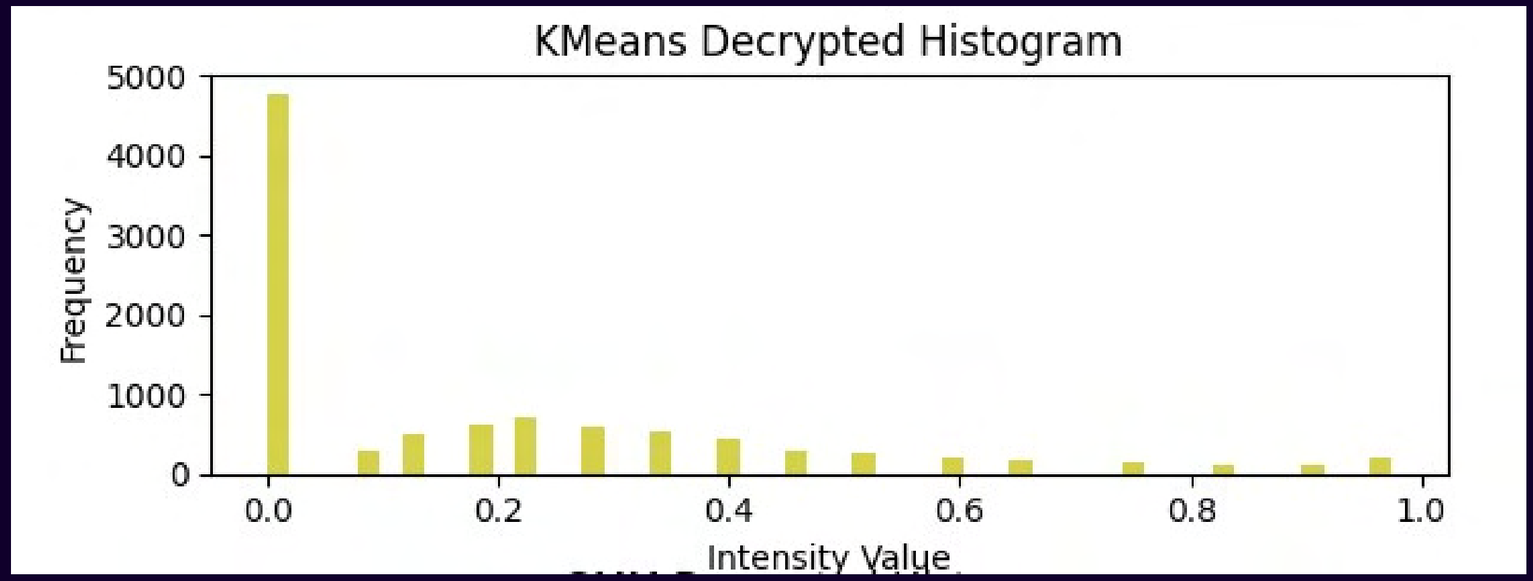
- **Encryption: K-Means clustering groups similar pixel intensities into kkk clusters, with each pixel assigned to a cluster label (used as the "encrypted" image).**

- **Decryption: Each cluster label in the "encrypted" image is replaced by the corresponding cluster center value, reconstructing the image.**


KMeans Encrypted
0
20
40
60
80
0
25
50
75


KMeans Encrypted Histogram
Frequency
5000
4000
3000
2000
1000
0
0
2
4
6
8
10
12
14
Intensity Value

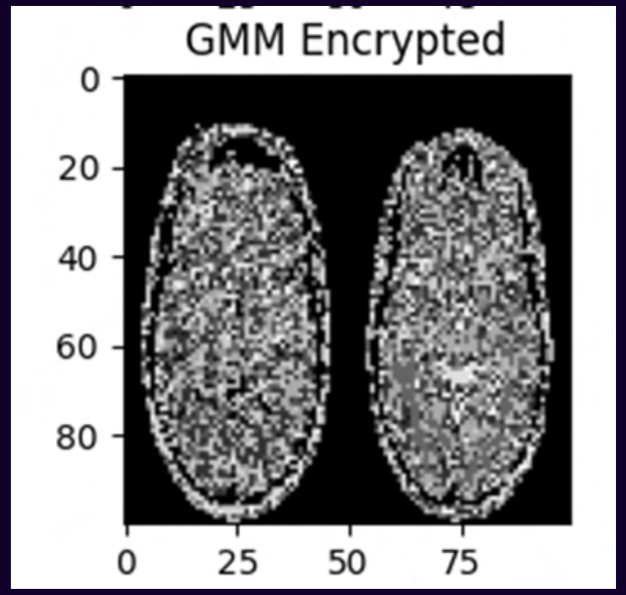

KMeans Decrypted - SSIM: 0.1912
0
20
40
60
80
0
25
50
75

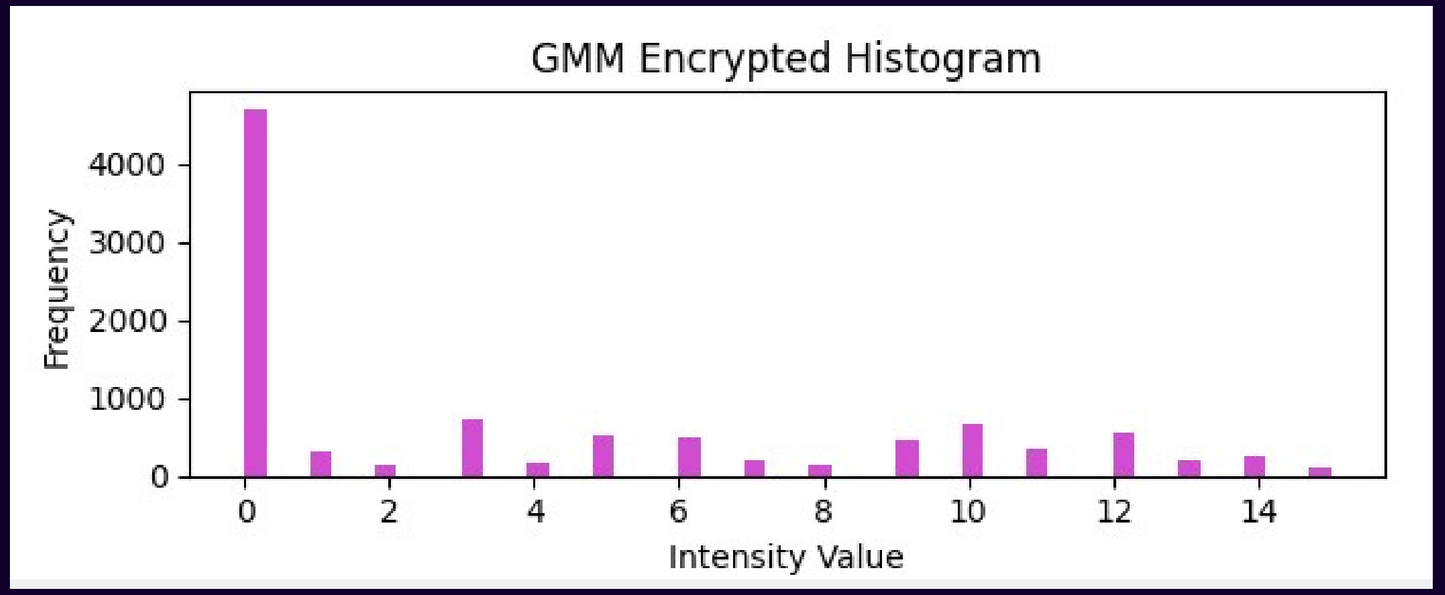

KMeans Decrypted Histogram
Frequency
5000
4000
3000
2000
1000
0
0.0
0.2
0.4
0.6
0.8
1.0
Intensity Value

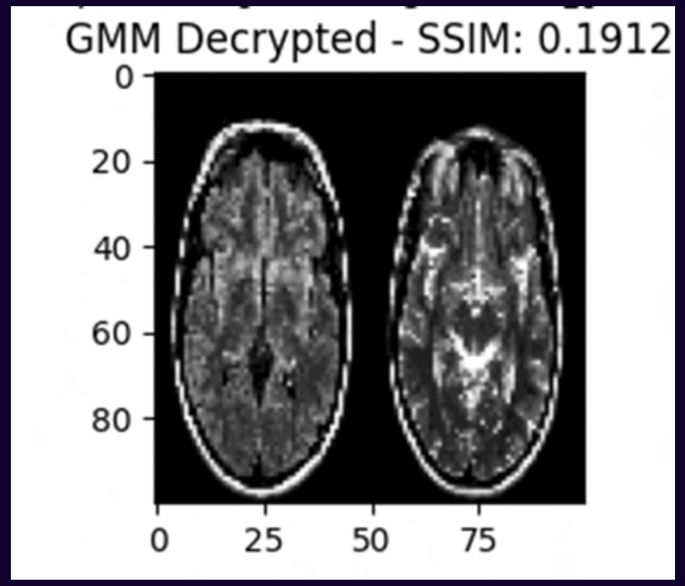
5) GMM Encryption and Decryption:

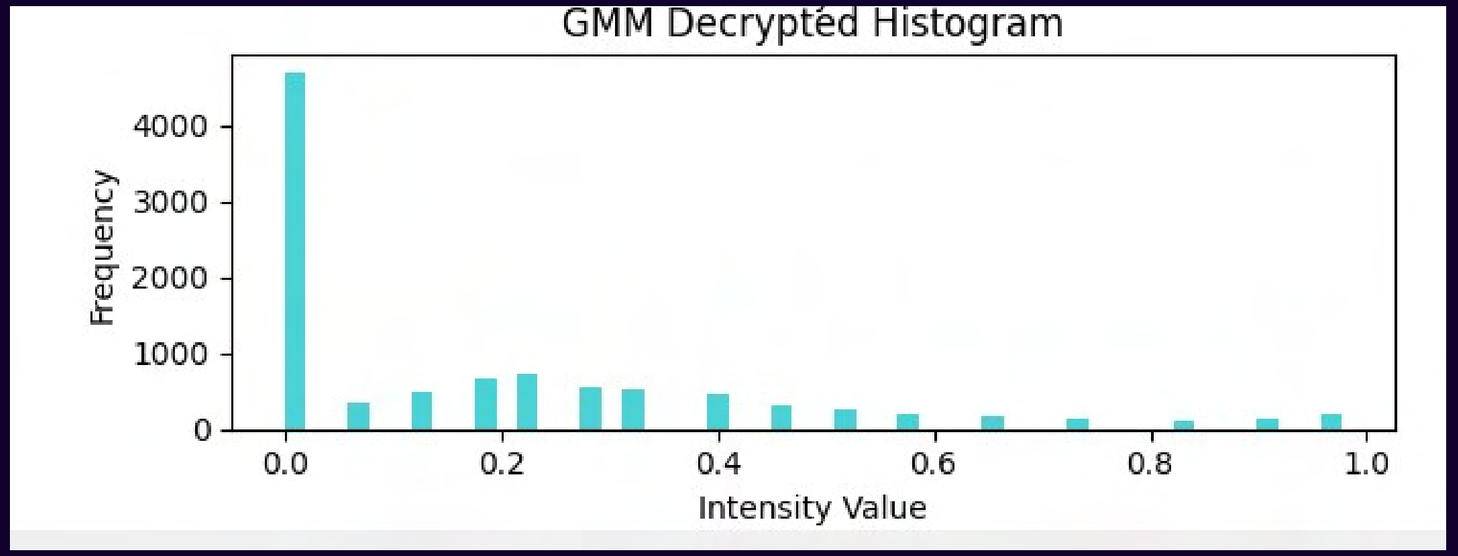
- **Encryption: GMM models pixel intensities as a mixture of kkk Gaussian distributions, with each pixel assigned a Gaussian component label.**

- **Decryption: Each label in the "encrypted" image is replaced by the mean of the corresponding Gaussian component.**


GMM Encrypted
0
20
40
60
80
0
25
50
75


GMM Encrypted Histogram
Frequency
4000
3000
2000
1000
0
0
2
4
6
8
10
12
14
Intensity Value


GMM Decrypted - SSIM: 0.1912
0
20
40
60
80
0
25
50
75


GMM Decrypted Histogram
Frequency
4000
3000
2000
1000
0
0.0
0.2
0.4
0.6
0.8
1.0
Intensity Value

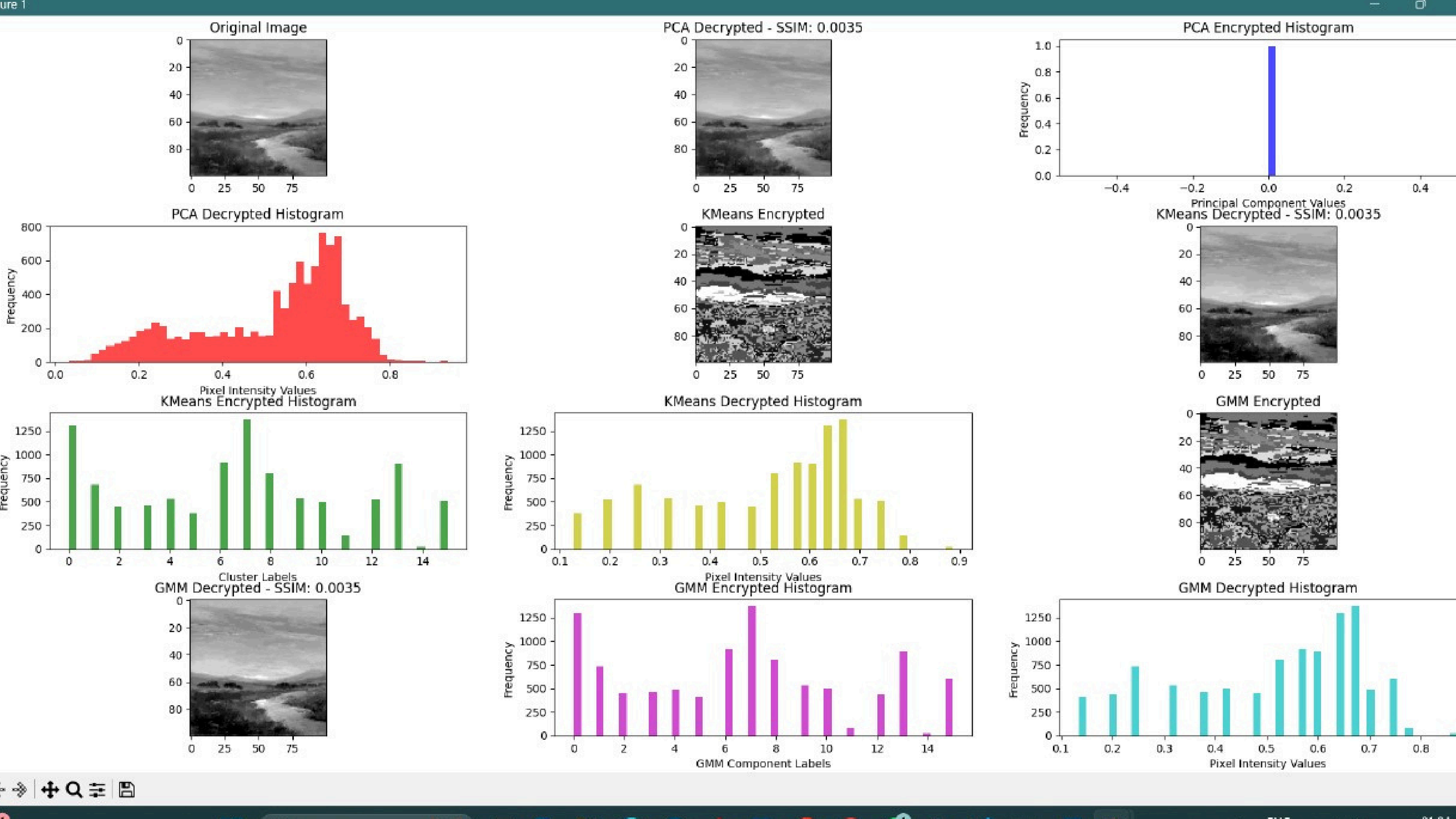
Error Metrics and comparision

PCA MSE: 6302.474527766243, **SSIM**: 0.19117049919403528

KMeans MSE: 6302.548513277214, **SSIM:** 0.191169782771177

GMM MSE: 6302.561979417601, **SSIM:** 0.19117268016092415

GMM has the slightly highest SSIM (0.191172) among the three, which means it preserves marginally more structural similarity compared to PCA and KMeans


Original Image
PCA Decrypted - SSIM: 0.0035
PCA Encrypted Histogram
Frequency
Principal Component Values
PCA Decrypted Histogram
Frequency
Pixel Intensity Values
KMeans Encrypted
KMeans Decrypted - SSIM: 0.0035
KMeans Encrypted Histogram
Frequency
Cluster Labels
KMeans Decrypted Histogram
Frequency
Pixel Intensity Values
GMM Encrypted
GMM Decrypted - SSIM: 0.0035
GMM Encrypted Histogram
Frequency
GMM Component Labels
GMM Decrypted Histogram
Frequency
Pixel Intensity Values

Advantages and Limitations of the Algorithm

- Advantages:
  - Diverse Encryption Techniques
  - Useful for Data Compression
  - Visual Feedback

- Limitations:
  - Limited to Grayscale Images
  - Potential Information Loss in PCA
  - KMeans and GMM Require Parameter Tuning

Future Scope & Why do we need it

Protecting Privacy and Confidentiality

- Images often contain private or confidential information, such as personal photographs, ID documents, medical scans, and financial records. Encryption prevents unauthorized users from viewing these sensitive visuals.

- In personal use, encrypting images helps protect users' private moments from leaks, accidental sharing, or hacking attempts. This is especially important for users storing images on cloud platforms or sharing them over potentially insecure networks.

Securing Medical and Scientific Images

- Medical imaging (like MRI scans) and scientific research visuals often contain highly sensitive data. Encrypting these images preserves patient confidentiality and keeps research data secure.

In the healthcare industry, image encryption is a necessity to protect against potential data leaks, safeguarding the identities and medical histories of patients

Future enhancements:

1) Making a more user friendly and interactive interface

2) Train the model to take multiple images at once and store them


Thank
You