A Novel Chaotic Image Encryption Algorithm Based on Coordinate Descent and SHA-256

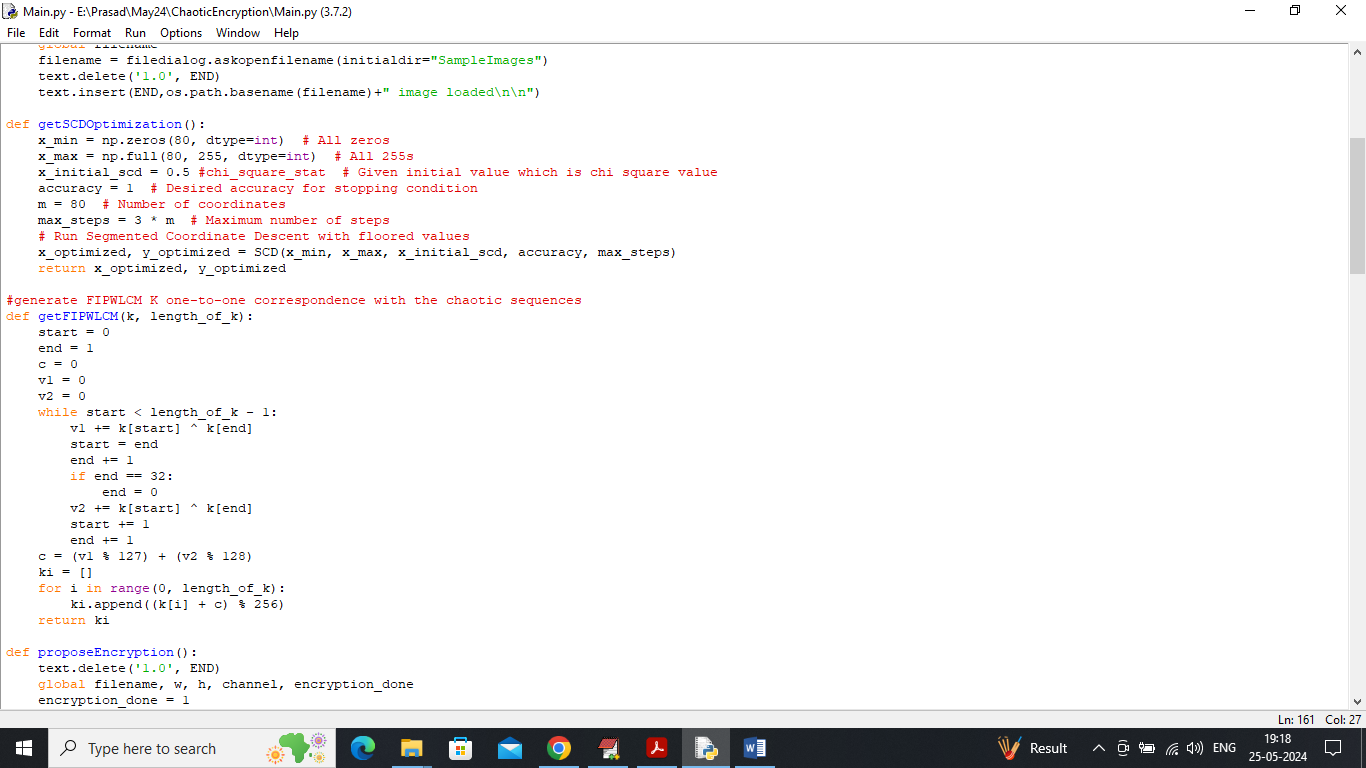
To secure data in network Chaotic Image Encryption is more in demand which will encrypt image based on a block cipher is to use a chaotic map to generate secret keys or chaotic sequences to substitute and diffuse the pixels or bits of the image to achieve a higher level of security. In the past many algorithms introduced which cannot uniquely map the seed key to the initial value of the chaotic system, which leads to the reduction of the key space of the encryption system.

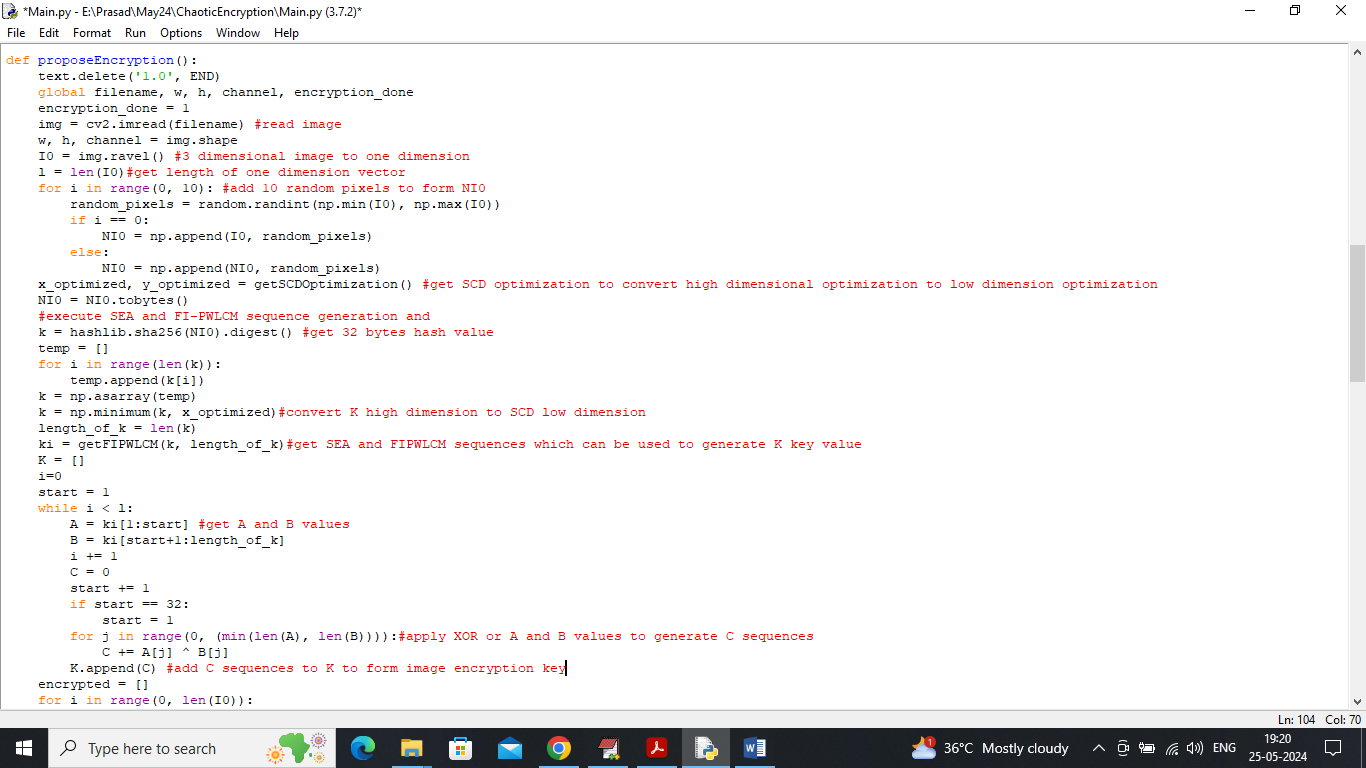
To overcome from above issue author of this paper introducing Novel Chaotic image encryption scheme which is a combination of multiple algorithms such as SEA (Sequential Expansion Algorithm), FI-PWLCM (Feedback Iterative Piece-Wise Linear Chaotic Mapping) and SCD (Segmented Coordinate Descent).

Above scheme will execute all 3 algorithms step by step

1. First image will be taken as input and then convert image to 1 dimension vector
2. 10 random pixels will be added to end of the 1 dimension vector
3. SEA and FI-PWLCM will be applied. SEA is a simple and fast pseudo-random sequence generator. FI-PWLCM, which has more control parameters than PWLCM and can generate more complex chaotic sequences
4. SCD will be applied to convert high dimensional optimization problem to low dimensional optimization to reduce key space.

Above steps we have applied to generate KEY sequences which can be used to encrypt images and above steps code showing in below screen





In above 2 screens read red colour comments to know about propose algorithm encryption and each step we have mark with red colour comments.

To implement this project we have designed following modules

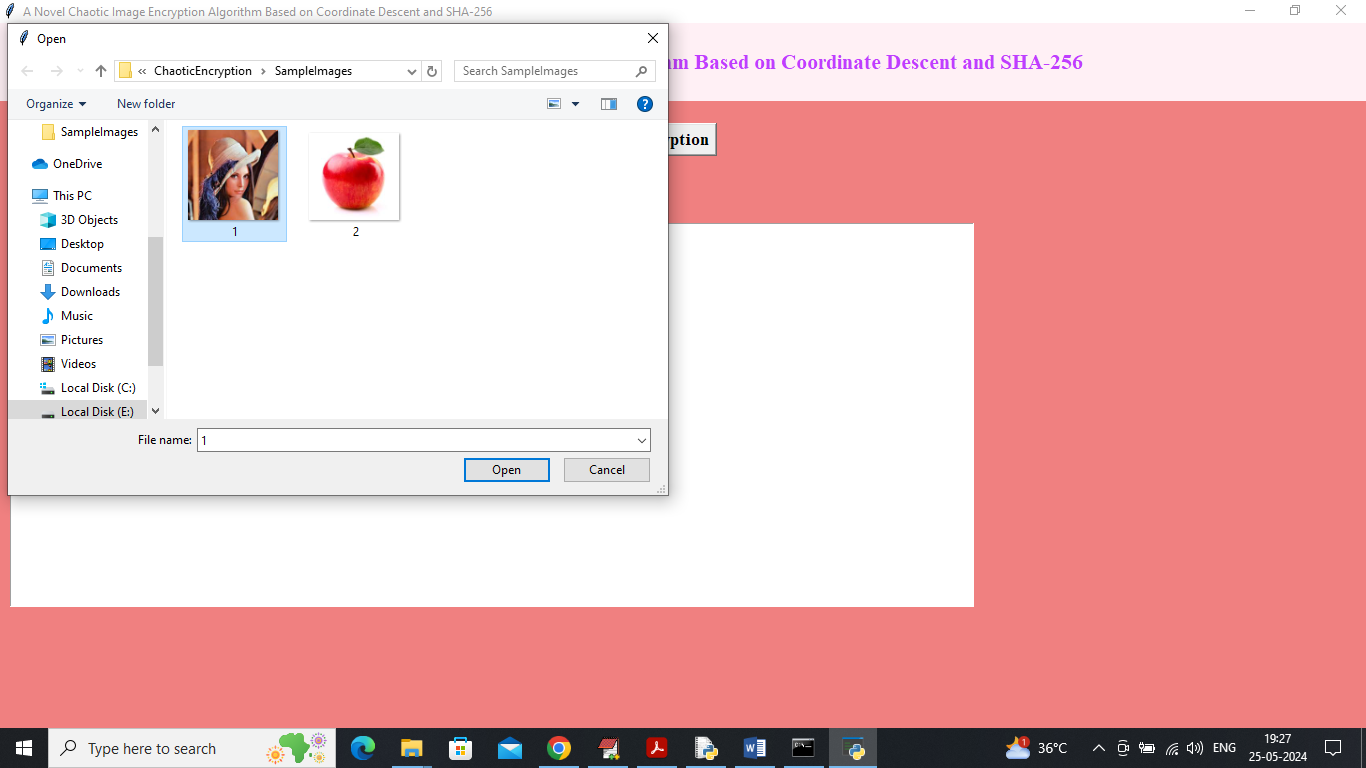
1. Upload Sample Image: using this module will upload sample image to application
2. Run Propose Encryption: apply propose algorithm on sample image to encrypt
3. Run Propose Decryption: can upload encrypted image to perform decryption. Decrypted image will be compared with original image to calculate PSNR and SSIM values. SSIM refers to similarity between original image and decrypted image whose range is in between 0 and 100 and the value closer to 100 or 1 will be consider as best SSIM quality. PSNR refers to noise the lower the noise the better is the decrypted image
4. Calculate NPCR & UACI Values: this module will encrypt image and then generate cipher image and then modify one pixel values and then re-encrypt image to generate another cipher image. Both cipher image will be input to NPCR and UACI method to estimate pixel change values.

SCREEN SHOTS

To run project double click on run.bat file to get below screen



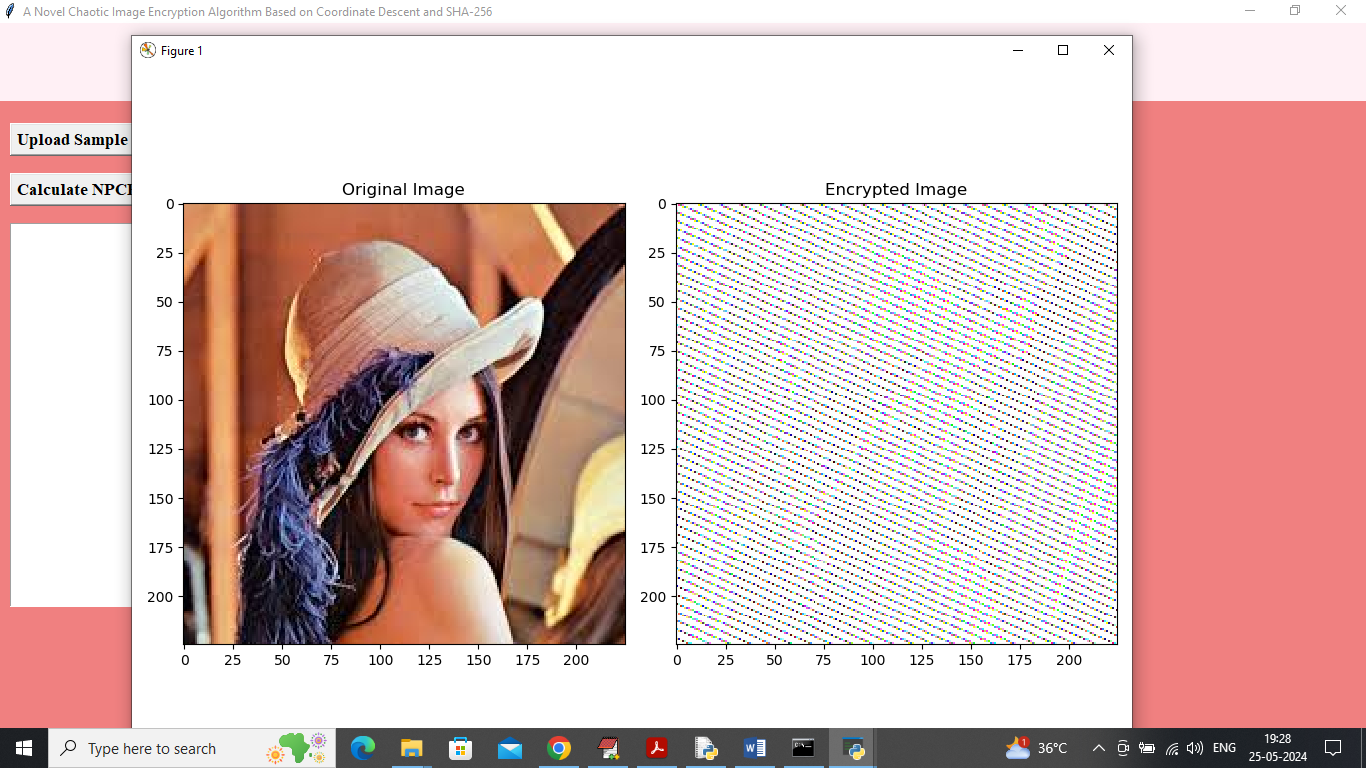
In above screen click on ‘Upload Sample Image’ button to upload image



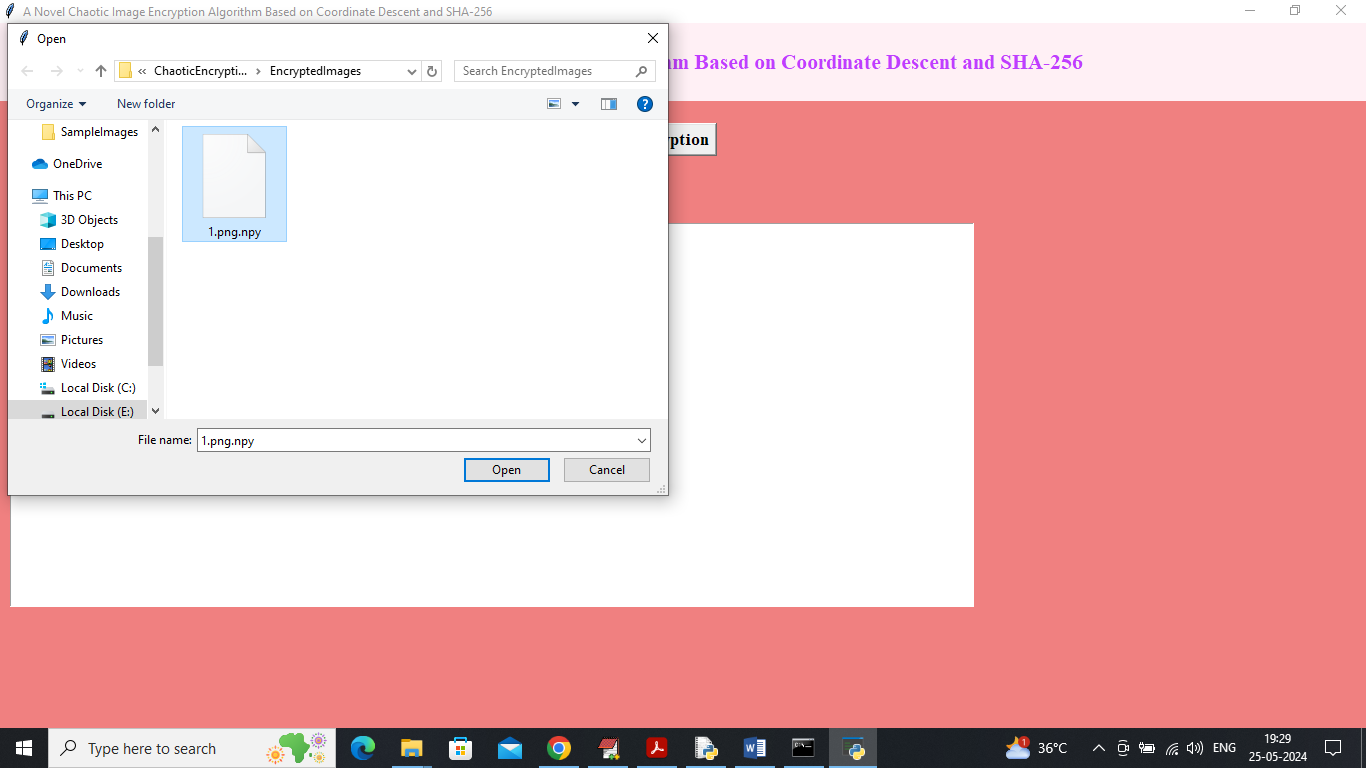
In above screen selecting and uploading sample image and then click on ‘Open’ button to load image and then will get below output



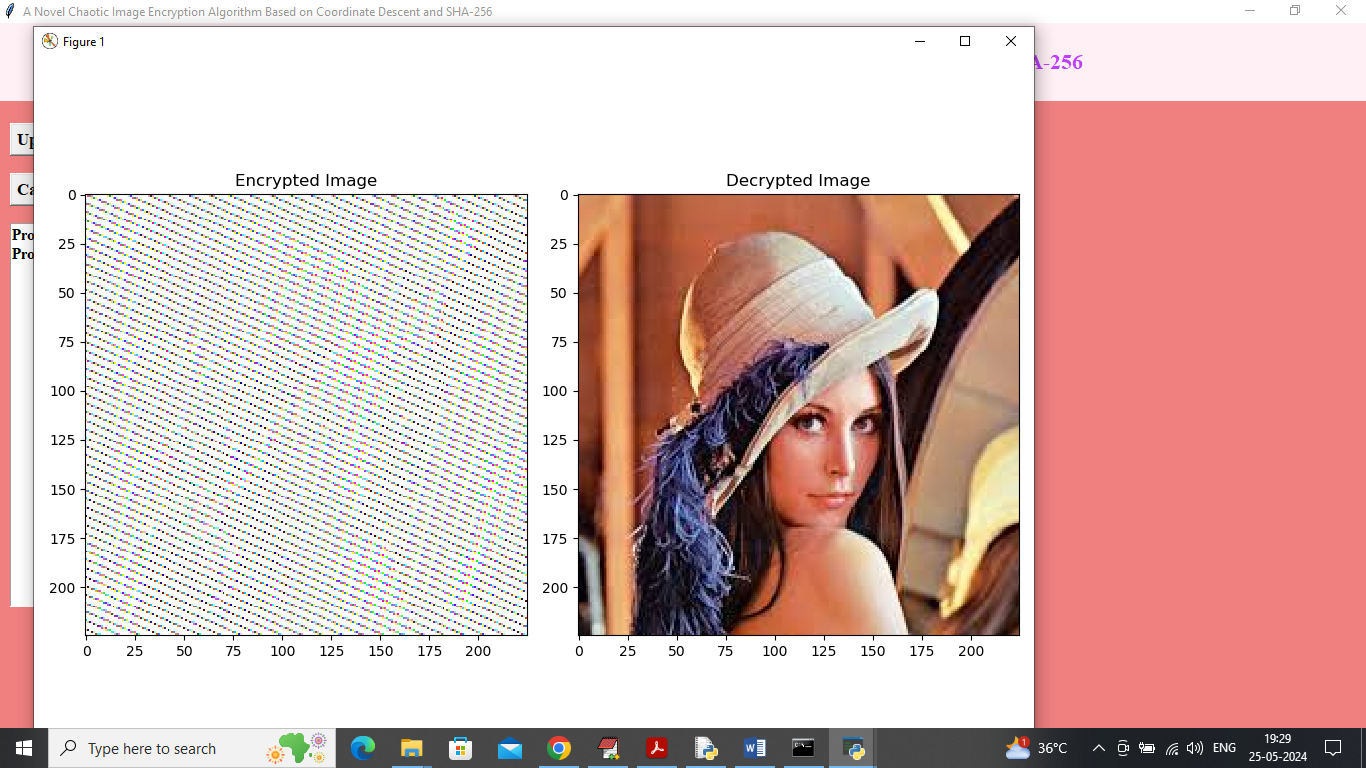
In above screen image loaded and now click on ‘Run Propose Encryption’ button to encrypt image and then will get below output



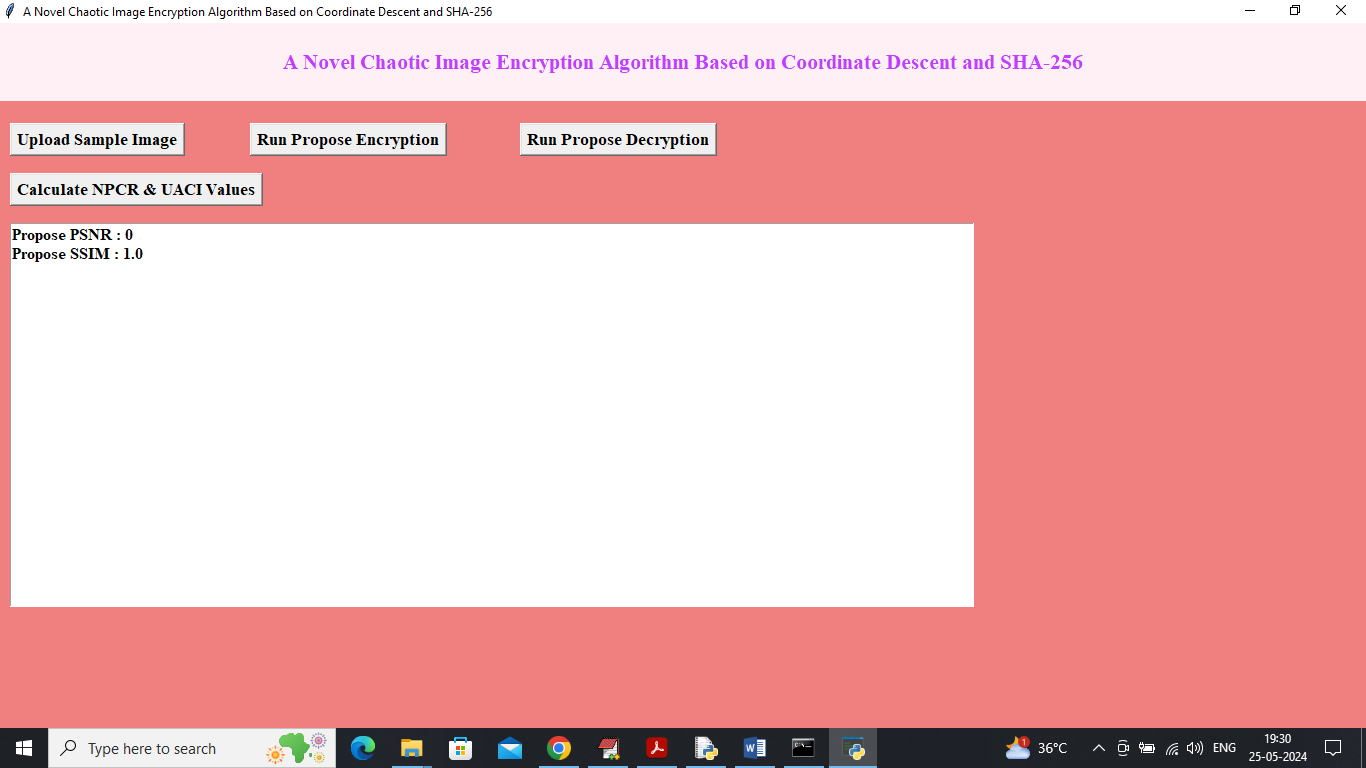
In above screen first image is the original image and second is the encrypted image and now click on ‘Run Propose Decryption’ button to upload encrypted image and then will get below output



In above screen selecting and uploading encrypted image and then click on ‘Open’ button to get below output



In above screen first image is the encrypted image and second is the decrypted image and can see decrypted image perfectly recovered and now close above image to get below output

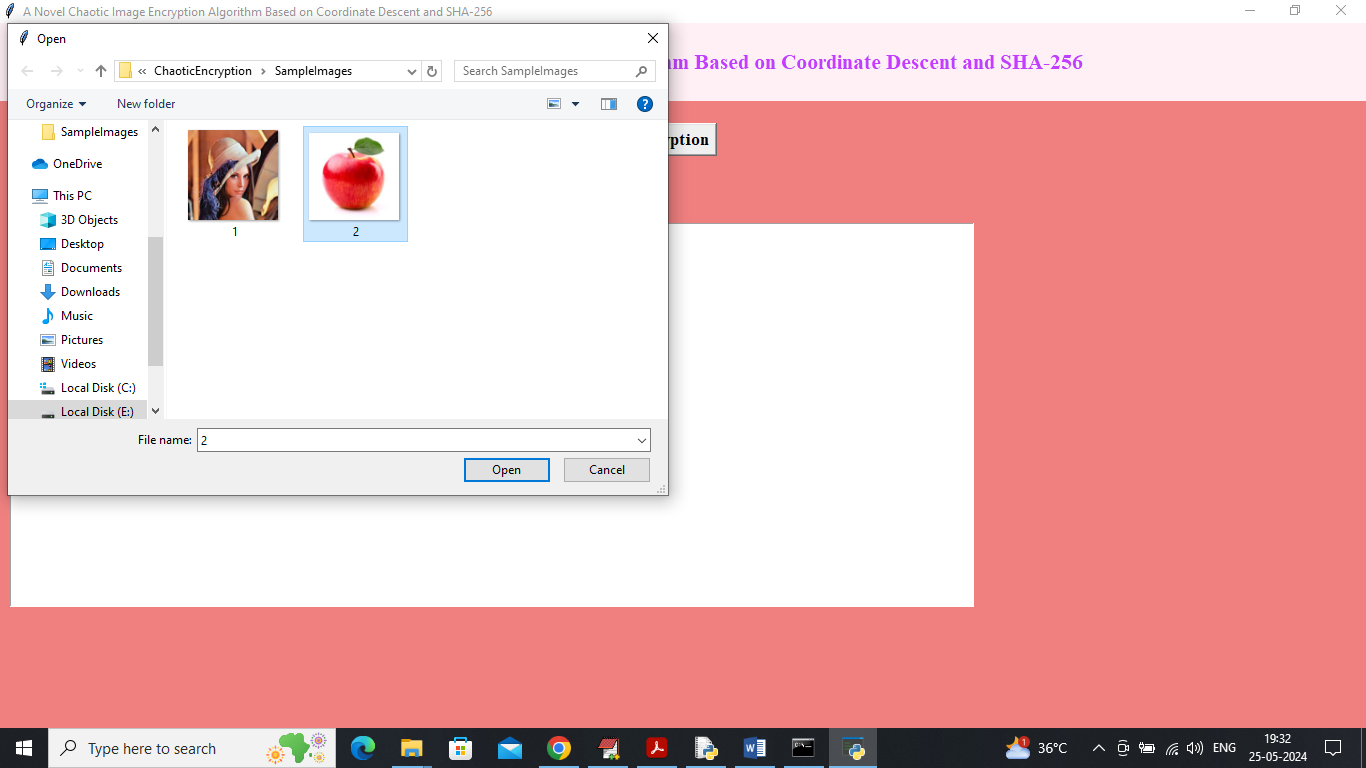


In above screen PSNR is 0 and SSIM is 100% which image decrypted is 100% similar to original image and now click on ‘Calculate NPCR and UACI’ button to get below output

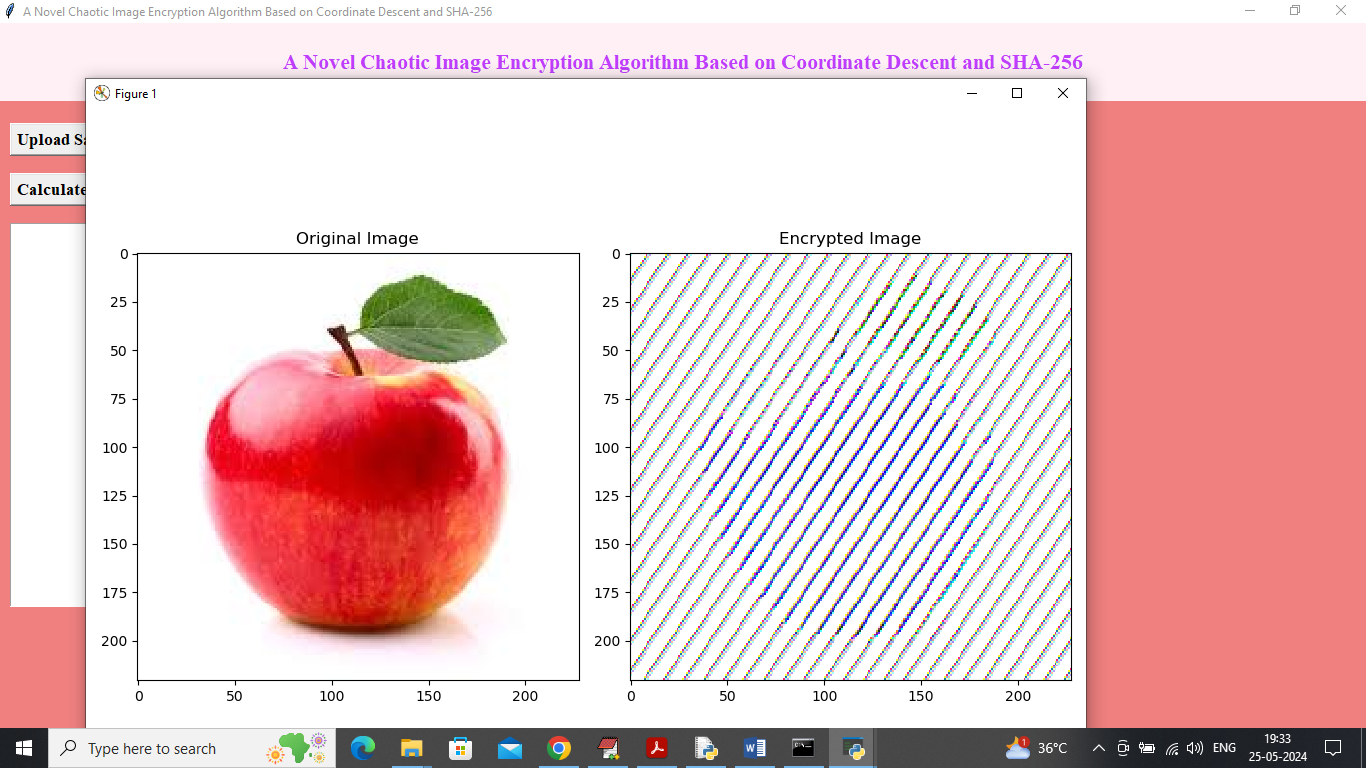


In above screen can see NPCR and UACI values.

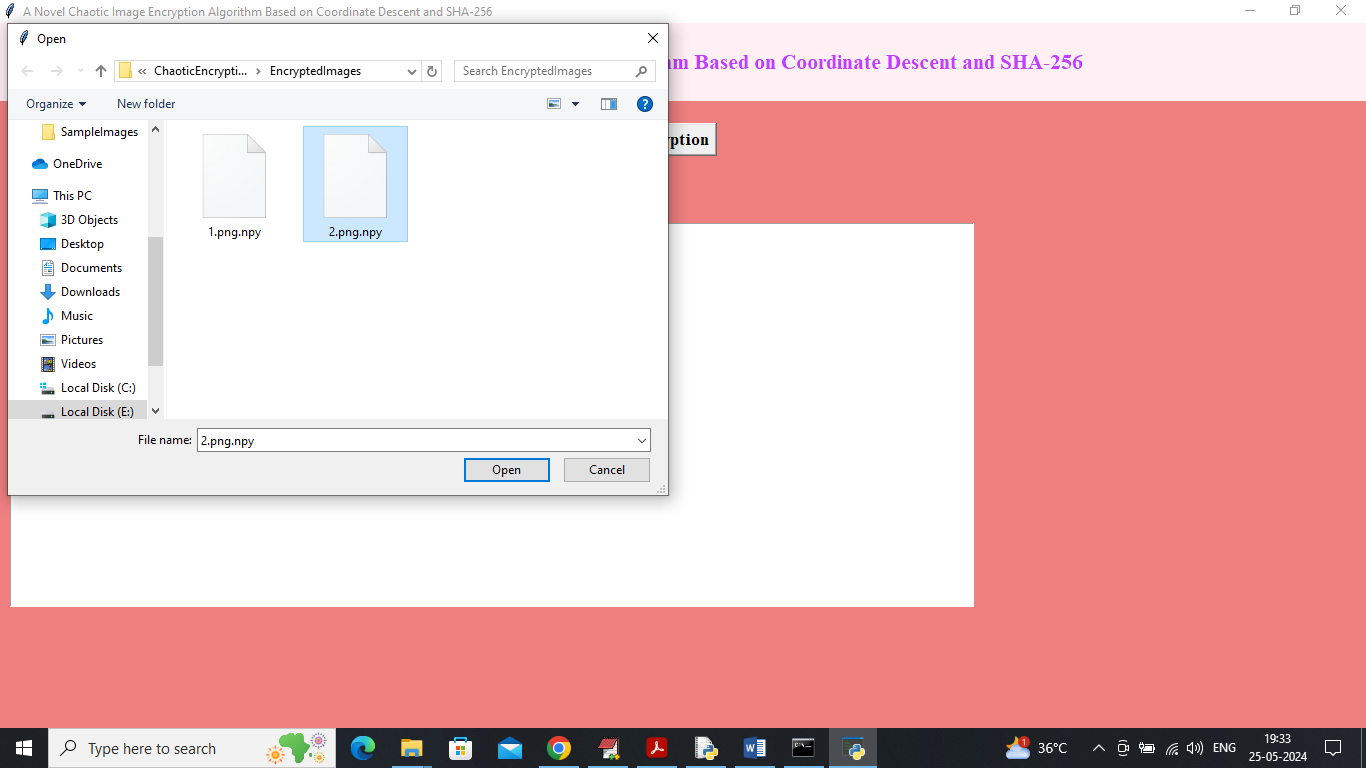
Similarly by following above screens you can encrypt and decrypt any image and below is another image example



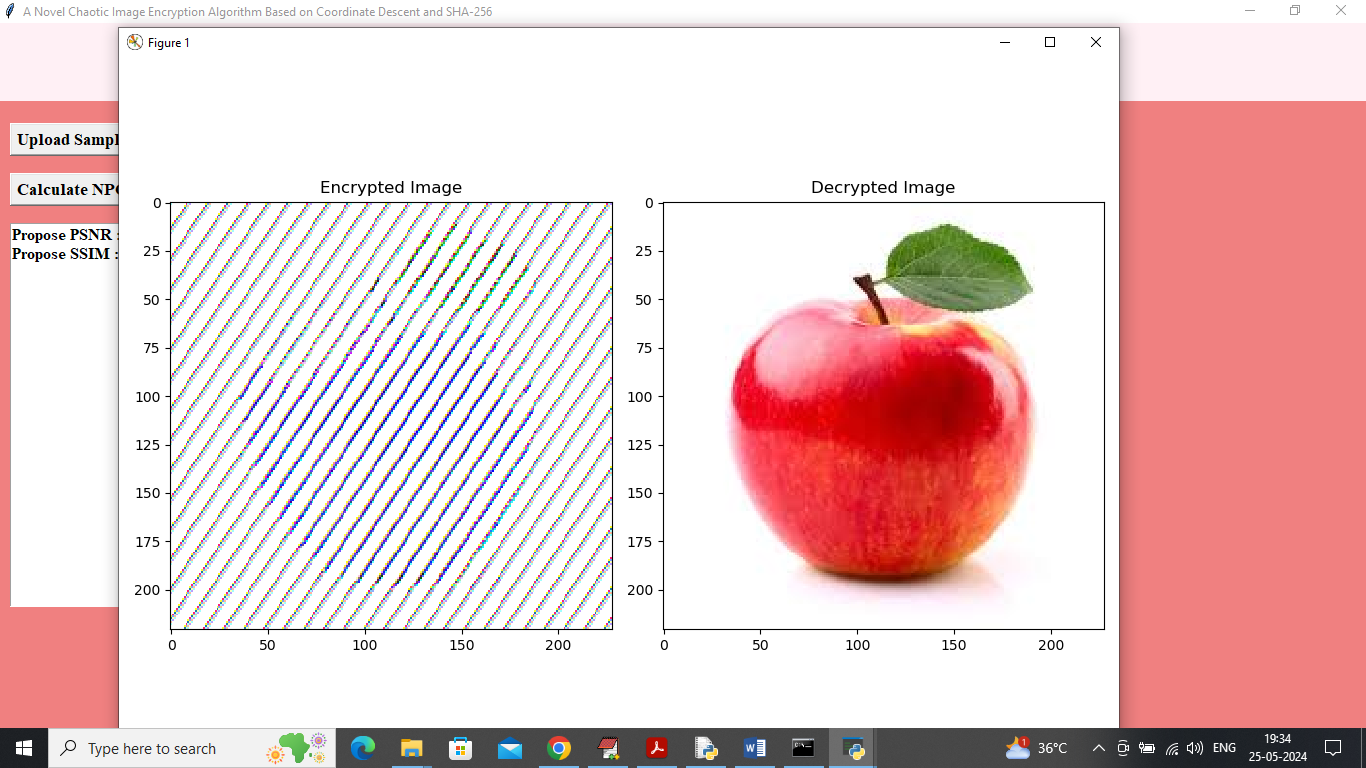
Above screen uploading 2.png image and now encrypt image



In above screen can see original and encrypted image and now upload 2.png encrypted image to decrypt



In above screen uploading 2.png encrypted image to get below output



Above is the decrypted image.