Securing data in the image using SHA & ECC

In this paper author using multiple combination of algorithms to secure data transfer between sender and receiver. In propose author employed following modules at sender side while data transfer

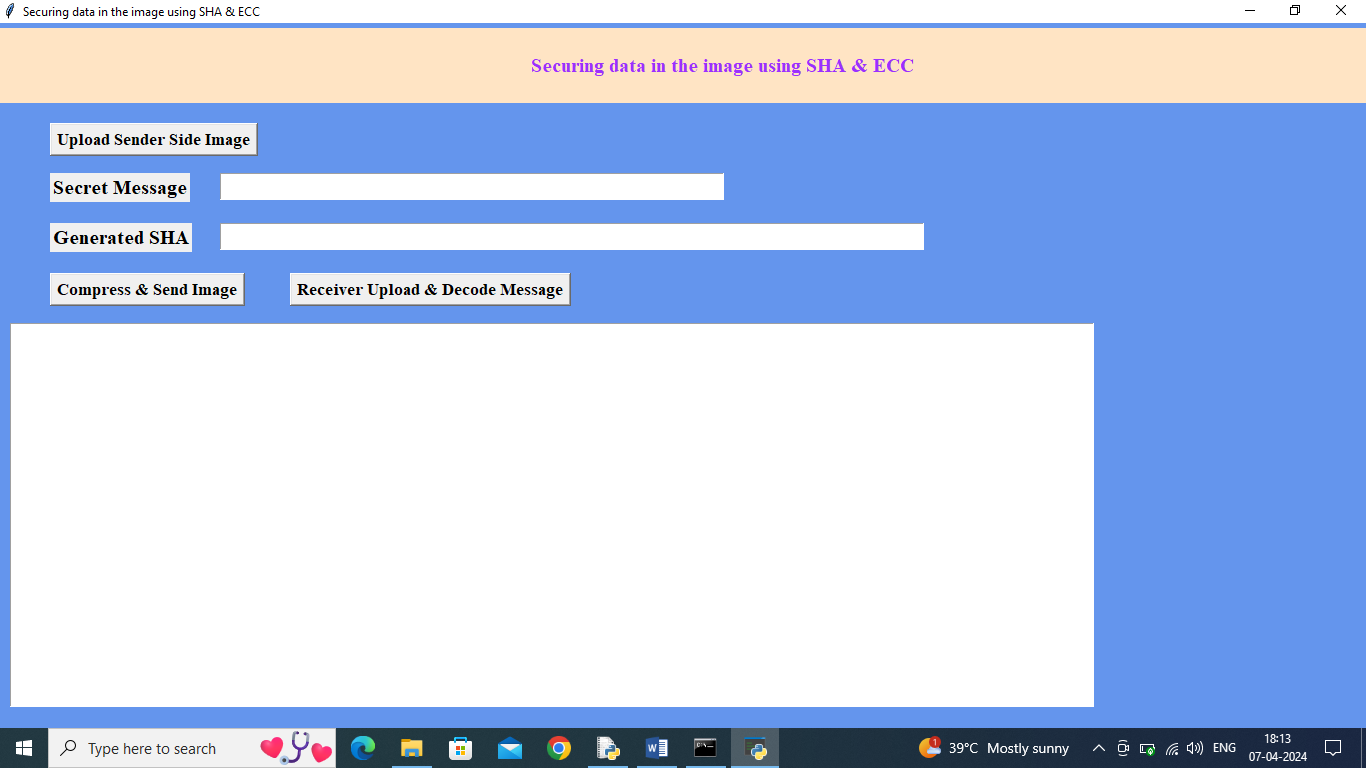
1. Input image
2. Input secret message
3. Encrypt message using ECC algorithm
4. Generate sha3 hash code on encrypted message
5. Hide encrypted message in cover image
6. Compress covered image using Huffman compression
7. Sent compress image and sha3 code to receiver
8. Receiver will receive compress image and sha3 code
9. Receiver will perform reverse operation to get back original message
10. Receiver will extract compress image for decompression
11. Extract encrypted data from decompress image
12. Generate sha3 code on extracted encrypted image and then compare with received code
13. Decrypt encrypted message
14. Display decrypted message to receiver

To implement above modules we have designed simulation based application where user will upload image and perform above operations

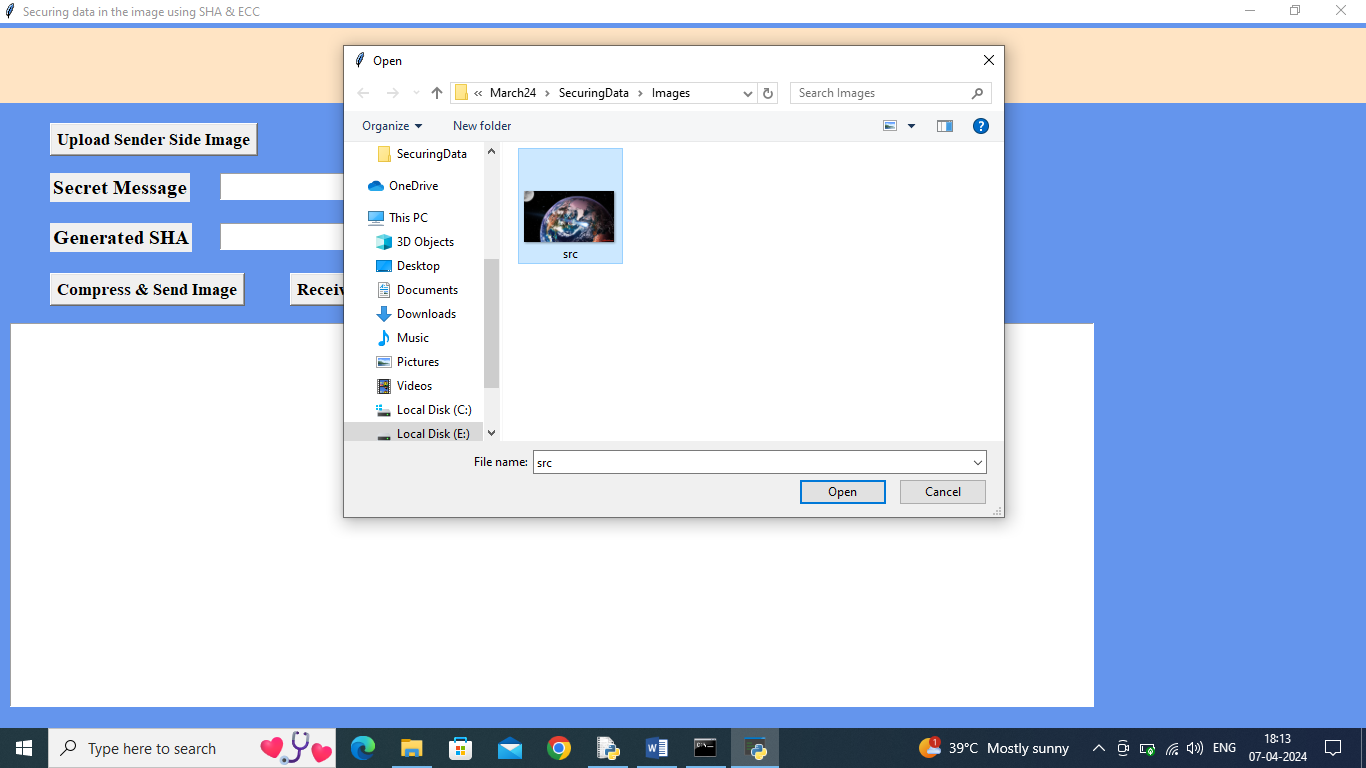
SCREEN SHOTS

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

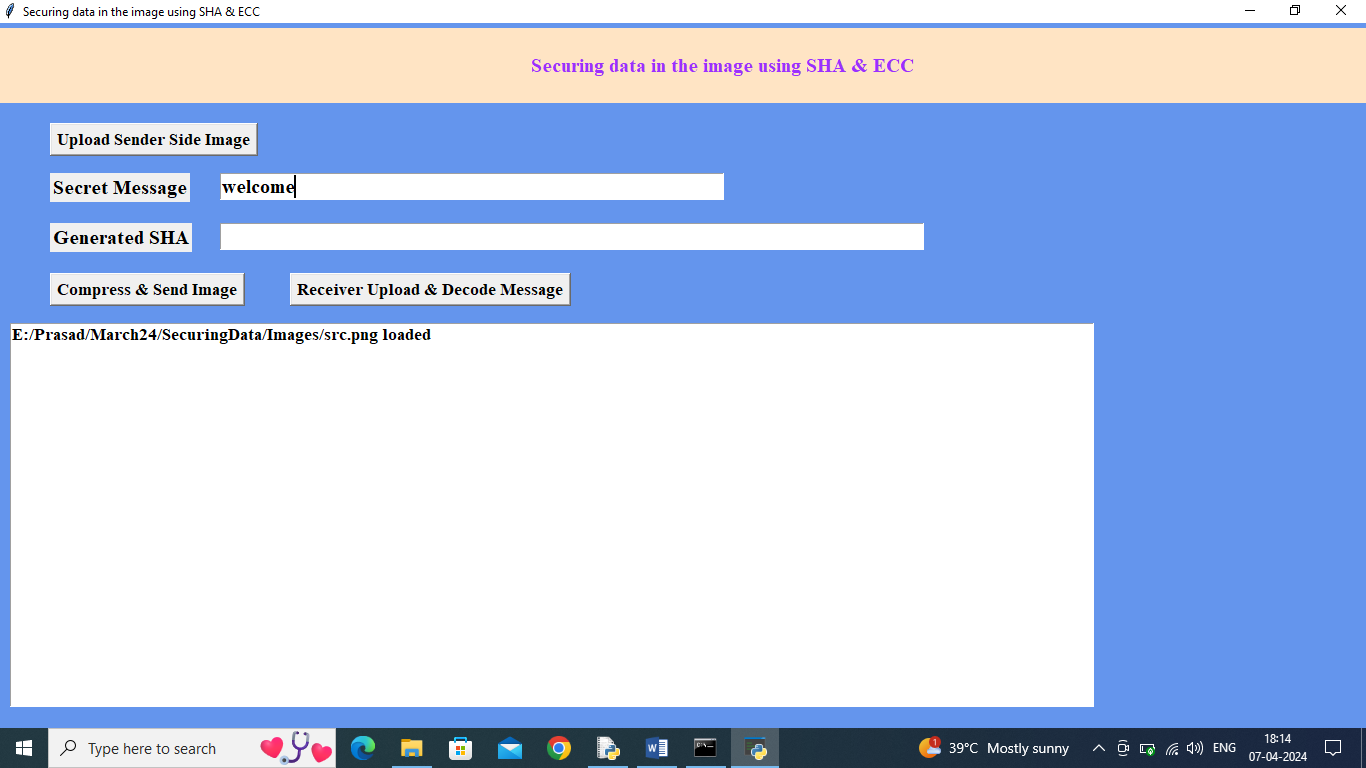
We saved all uploading images inside ‘Images’ folder and all compress final images will saved inside ‘ReceivedCompressImages’ folder



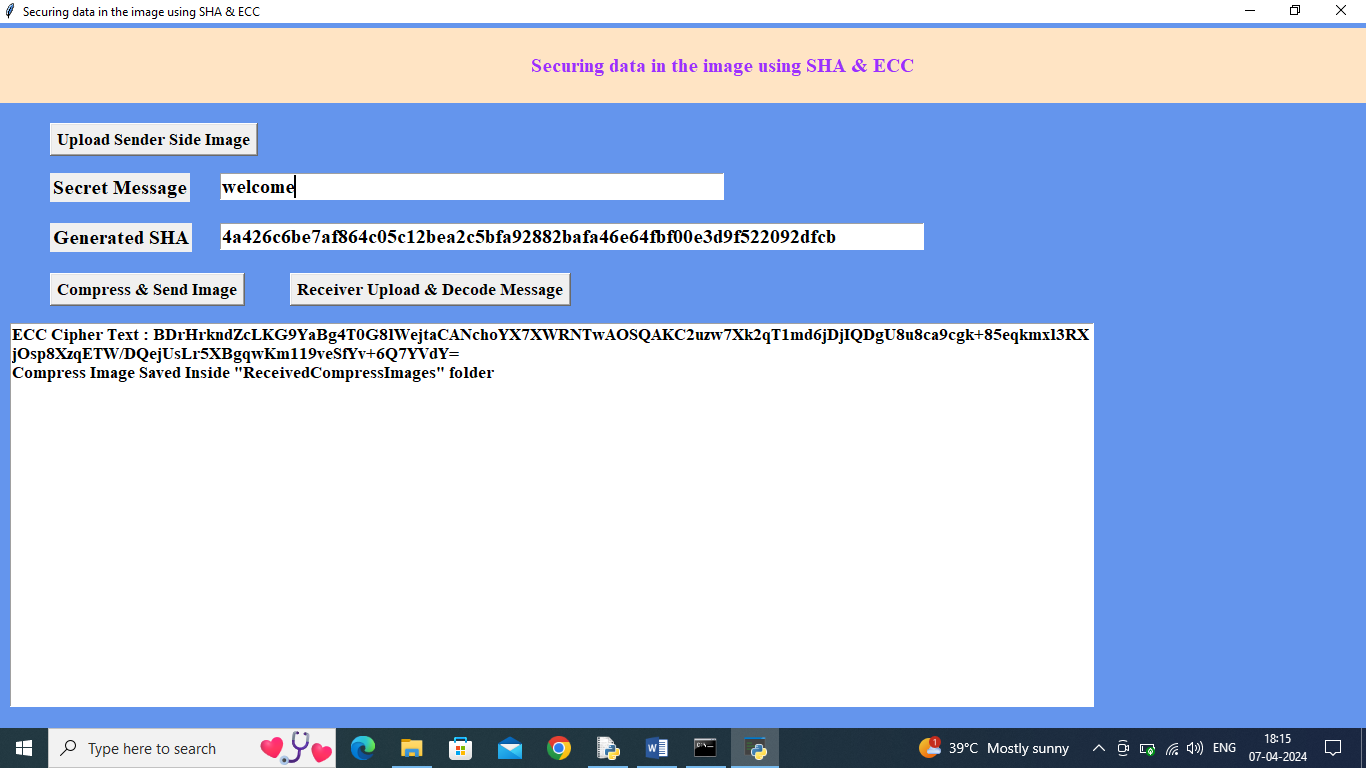
In above screen click on ‘Upload Sender Side Image’ button to upload image



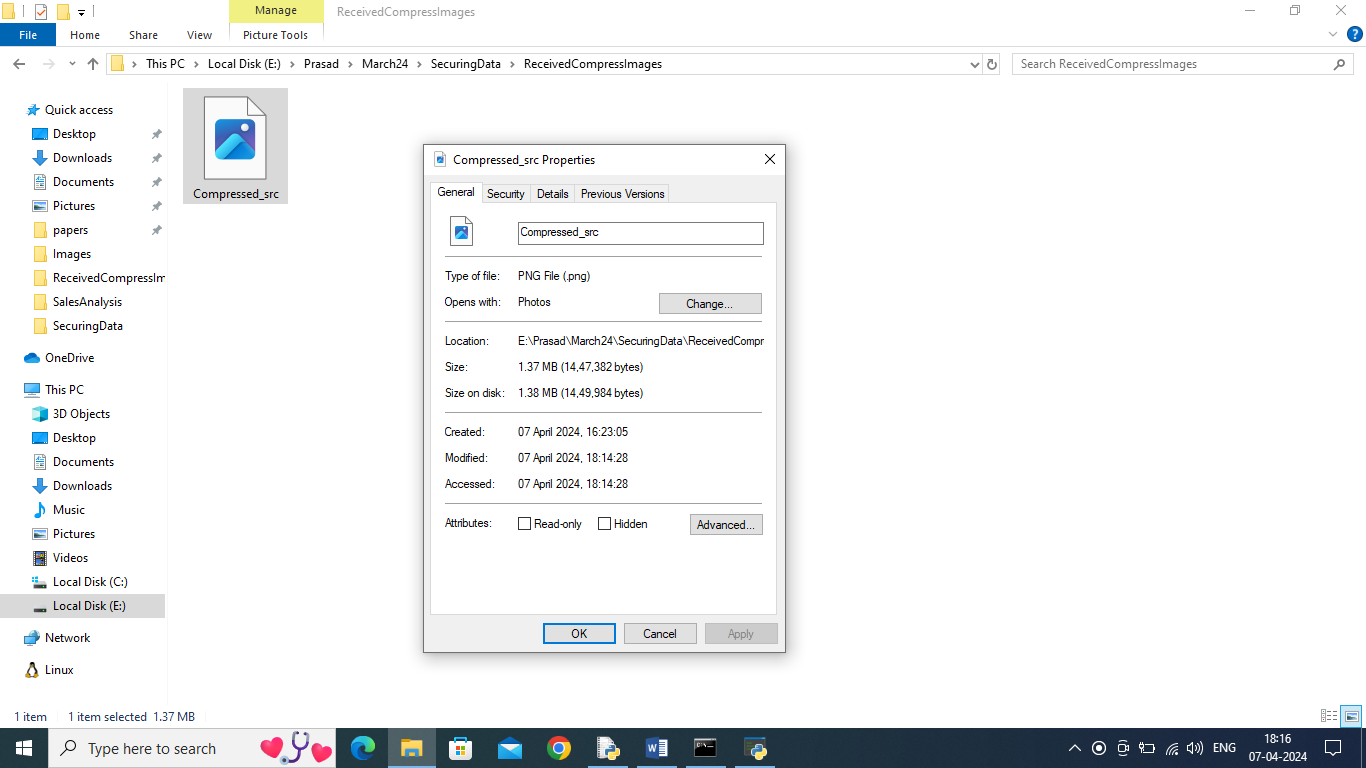
In above screen selecting and uploading ‘src.png’ file and then click on ‘Open’ button to get below page



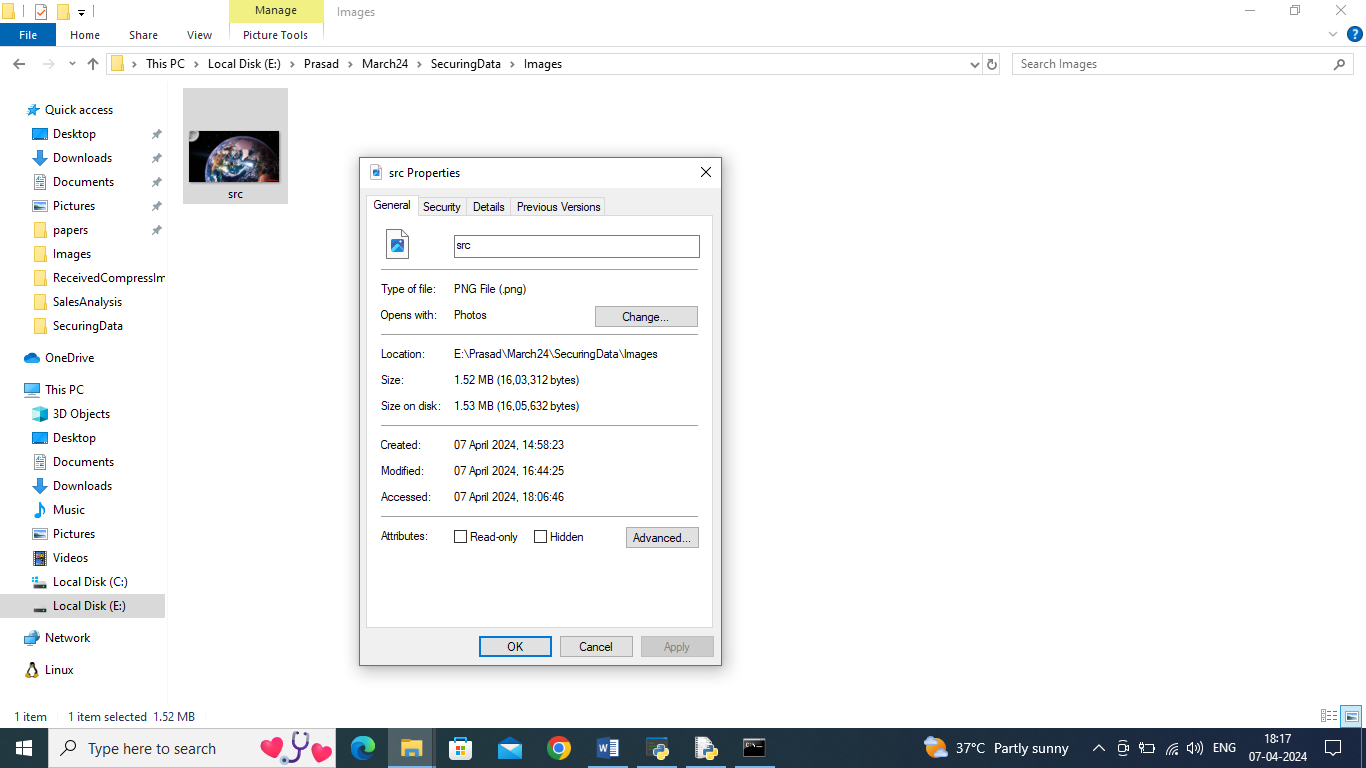
In above screen as secret message enter some message and then press on ‘Compress & Send Image’ button to get below output



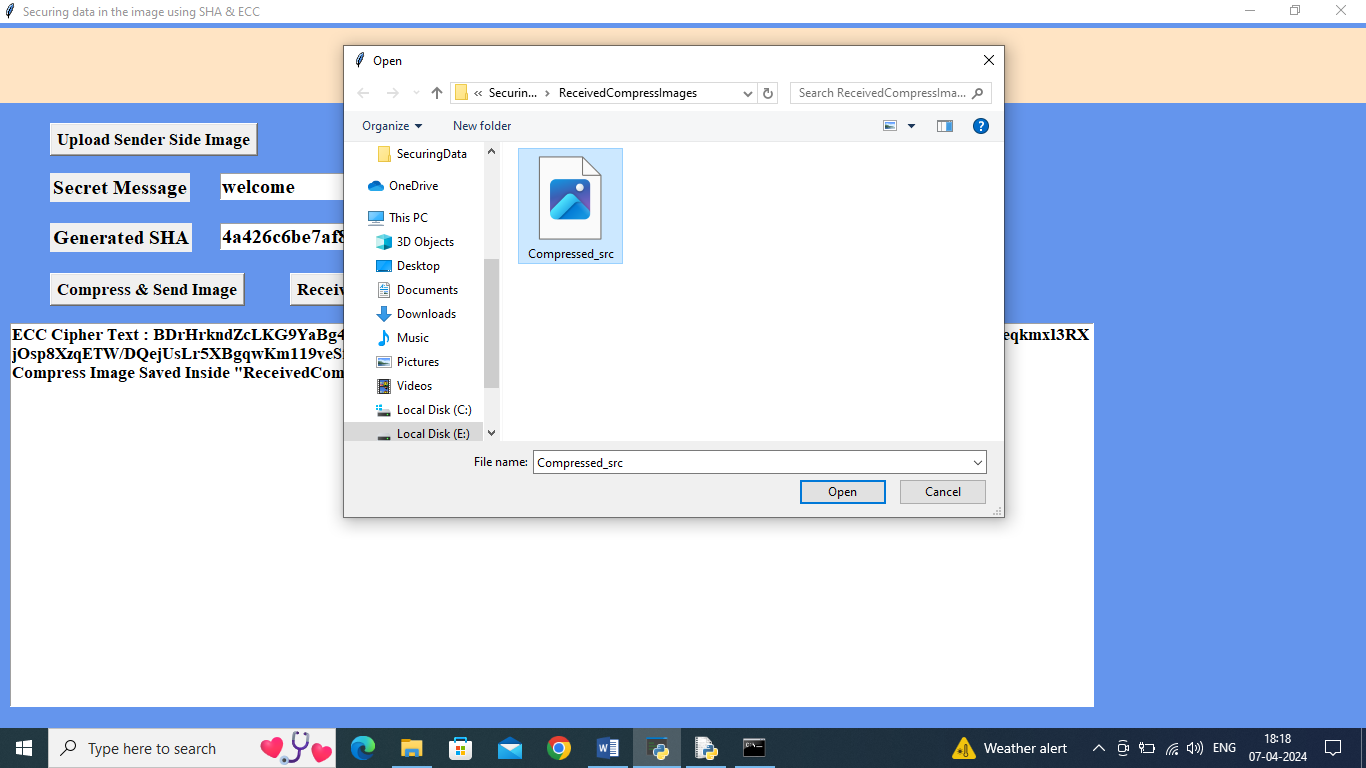
In above screen in second text field can see generated sha3 hash code and in text area can see ECC encrypted message and then can see compress image saved inside ‘Received Compressed’ folder and in below screen we can see compress image size and original image size



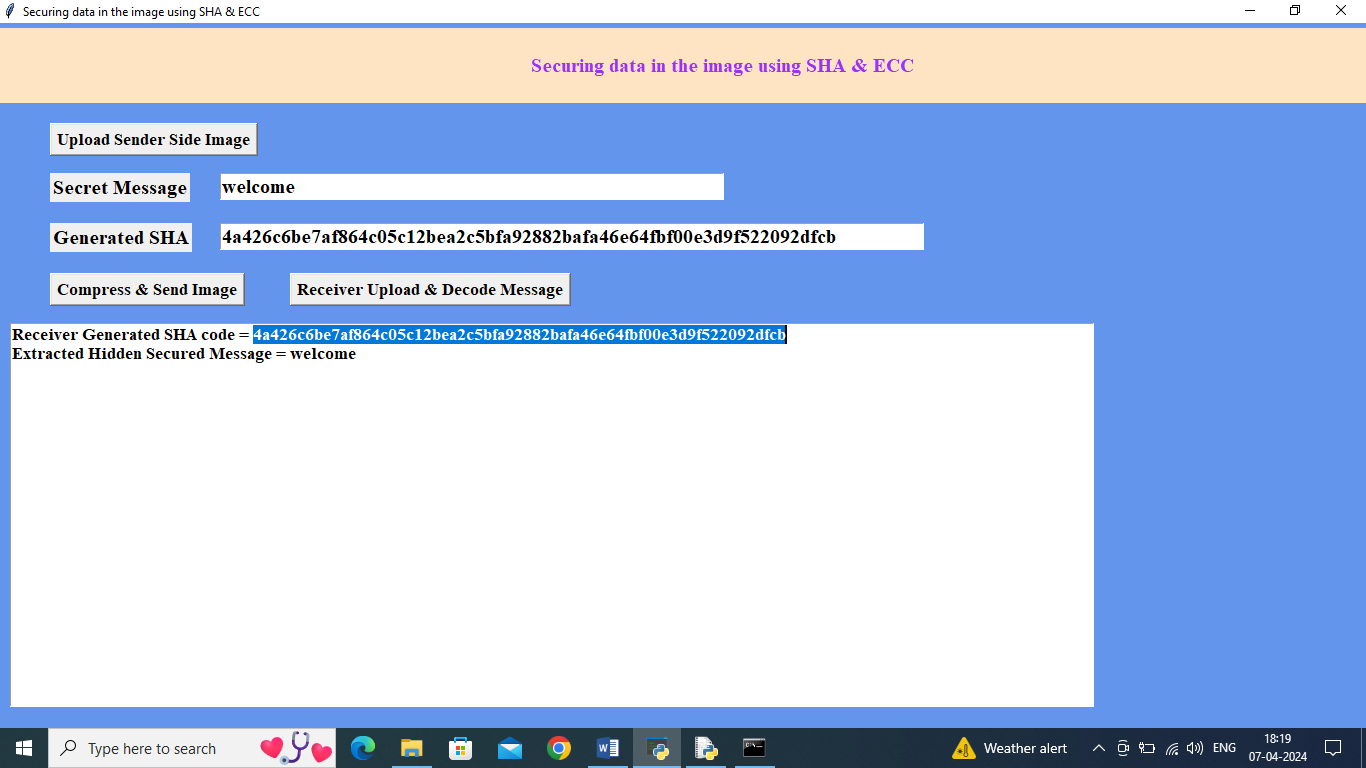
In above screen compress image size is 1.37 MB and in below screen we can see original image size



In above screen original uploaded src.png image file is 1.52 MB so compress image having less size and now in application click on ‘Receiver Upload & Decode Message’ button to upload compress image from received folder and then application will generate has code and extract and decrypt hidden message



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



In above screen in blue colour selected text can see hash code generated by receiver on received message and can see both generated and hash code available in second text field is matching and verification is successful and then in text area in second line can see extracted and decrypted hidden message as ‘welcome’.

Similarly by following above screens and using paper technique we can share secured data between sender and recievr