Cryptography Project

By Riya Gupta (17BCS026)

Implementation of Image Encryption using Advanced Encryption Standard (AES)

Implementation of IEEE Paper: A Novel Image Encryption Algorithm using AES and Visual Cryptography, 2016 2nd International Conference on Next Generation Computing Technologies, Dehradun, India

Language used: Python 3.7.4 on Jupyter Notebook (Anaconda)
Libraries used: base64, hashlib, Crypto.Cipher, Crypto.Random, numpy, cv2 and sklearn.linear_model

Encryption

Input: An Image and a key (string stored in a text file)
Method:

1. The image is taken as input then read and encoded using base64. Therefore, image is converted into bytes. Now this data in bytes is decoded in utf-8 to be used as a string.
2. The key, K is read and then hashed using Secure Hash Algorithm – 256 bit (SHA256).
3. The image string is encrypted by AES-256 into cipher text using the hashed key generated in step 2.
4. Now we convert the original key, K is converted into an image and the split into 2 images, P and R.
    a. A new image C of size(w,h) is initialized as blank, where w = character support for key file (default: 255) and h = number of characters in key, K.
    b. For each row, i in the height of image C, we find a value j which is equal to the ASCII value of the i-th character in key, K.
    c. All the values at positions less than j in a row in C is fed with value 0, i.e., black.
    d. Each pixel in R takes a random value between 0 and 1.
    e. Now each pixel in P takes a value that is an XOR of R and C at that pixel position, i.e., P[i][j] = R[i][j] *XOR* C[i][j].
5. Encrypting the cipher text further:
    a. Two-layer Caesar cipher by training a linear regression model by trained by dataset generated from images P and R.
    b. For X values of linear regression model, there are 2 columns of x's. Each column having alternate P row's sum. All values collected in dataframe xdf.
    c. For Y values of linear regression model, there are 2 columns of y's. Each column having alternate R row's sum. All values collected in dataframe ydf.
    d. Now dataframes xdf and ydf are fitted into the linear regression model.
    e. For prediction, we create another dataframe of 2 columns of z's. Each column having alternate C row's sum. Sum of each column is taken. This gives two values that shall be used in predicting through our linear regression model.
    f. On prediction another 2 values are generated, we take mod 26 of them and store as x and y.
    g. Now for each character in cipher text of original image we find ascii value then add x and subtract y. Then convert the gotten value back to character and append to a string.

h. The result string is our final cipher text.

Output: cipher text stored in a text file (.txt) and PNG images P and R which are splits of our key image. This output is sent for decryption.

Decryption

Input: cipher text stored in a text file (.txt) and PNG images P and R which are splits of our key image.
Method:

1. Images R and P are read.
2. We find out the values of h and w from the dimensions of P (or R).
3. A new image, CK is created of size(w,h). Each pixel of CK is the XORed value of P and R at that pixel position.
4. Now a blank key, K1 of length h is created.
5. For each row in CK,
    a. We count the number of 0's, i.e., black pixels.
    b. This count is converted to the corresponding ACSII character and append to K1.
6. K1 which is a list is converted into string. (K1 is same as the key, K that was used in the process of encryption)
7. The key, K1 is hashed using Secure Hash Algorithm – 256 bit (SHA256).
8. The cipher text is read and stored as a list split by space.
9. Decrypting the cipher text:
    a. Two-layer Caesar cipher by training a linear regression model by trained by dataset generated from images P and R.
    b. For X values of linear regression model, there are 2 columns of x's. Each column having alternate P row's sum. All values collected in dataframe xdf.
    c. For Y values of linear regression model, there are 2 columns of y's. Each column having alternate R row's sum. All values collected in dataframe ydf.
    d. Now dataframes xdf and ydf are fitted into the linear regression model.
    e. For prediction, we create another dataframe of 2 columns of z's. Each column having alternate CK row's sum. Sum of each column is taken. This gives two values that shall be used in predicting through our linear regression model.
    f. On prediction another 2 values are generated, we take mod 26 of them and store as x and y.
    g. Now for each character in cipher text we find ascii value then substract x and add y. Then convert the gotten value back to character and append to a string.
    h. The result string is our final cipher text.
10. We now decrypt the cipher text further using hashed key by AES-256.
11. We change the encoding of this decrypted data to utf-8 and save it as PNG file to get the original image.

Output: original image in PNG.

Instructions to the code

1. .zip file is to be unzipped.
2. Juypter Notebook is to be run and navigated to the folder from the zip file.
3. Run Encrpytion.ipynb file to convert an image from pics folder to cipher text.

4. mykey.txt in keys folder is used in encryption.
5. ToBeSent for Decryption folder stores the generated cipher text and key split images.
6. On running the Decryption.ipynb file we get our original image named as DecryptedImg.

Note: For another run some file names and folder names have been changed in the code.