Task 3 Observation

In my encryption experiment, I noticed significant differences between using ECB (Electronic Code Book) mode and CBC (Cipher Block Chaining) mode to encrypt an image. When I used ECB mode, I could still partially recognize some patterns in the encrypted image. This was especially evident in areas of the original image with large blocks of the same color or texture. In contrast, when I used CBC mode, the encrypted image appeared as complete noise.

The reason for this disparity lies in how these encryption modes handle data. In ECB mode, each block of the image is encrypted independently with the same encryption key. Consequently, identical blocks of the original image result in identical blocks of ciphertext. This partial preservation of patterns in the encrypted image is due to the deterministic nature of ECB mode.

On the other hand, in CBC mode, each block of plaintext undergoes an XOR operation with the previous ciphertext block (the Initialization Vector or IV) before encryption. This process creates a 'chain' effect where even small changes in the plaintext lead to drastic differences in the ciphertext. As a result, the CBC-encrypted image appears as noise, making it challenging to discern any patterns or extract meaningful information.

In summary, the observed differences underscore the importance of choosing the right encryption mode for the task at hand. For images and similar data where preserving patterns is undesirable, CBC mode offers greater security by obfuscating the data more effectively.