489 - Assignment 1

Onur Tirtir
2099380

November 17, 2018

1 CBC Mode

In CBC mode, each block of plain-text is first *xor*'ed by previous cipher-text block retrieved by encryption of previous plain-text block and then encrypted by *key*. This brings us the *diffusion* property.

Even if we have a trivial plain-image like "original.bmp", we cannot deduce any useful information in first glance to the cipher-image as it seems much like noise. Noisiness comes directly from "cipher block chaining".

2 ECB Mode

In ECB mode, each block is encrypted independently from the other blocks. ECB mode does not utilize any feed-backs from previous blocks unlike some other modes (like CBC Mode). Regardless of its position, a plain-text block is always encrypted to same cipher-text block. Hence ECB Mode cannot satisfy *diffusion* property.

Near pixels have same RGB values if the input image is not that complex due to the reasons explained above. Hence we may deduce some or most parts of underlying plain-image, its rough shape and even the objects in image depending on the color-wise complexity of given plain-image.