My code takes a bit time. So please wait for it.

When we encrypt an image using AES in Electronic Code Book (ECB) mode, the resulting encrypted image (encrypted.bmp) still reveals recognizable patterns from the original image. This observation highlights a fundamental weakness of ECB mode, especially evident when encrypting data with repetitive structures like images.

Observation from the Encrypted Image:

Pattern Retention: Despite the encryption, the encrypted.bmp image displays visible patterns and outlines that correspond to the original image (blackbuck.bmp). **in my case I can obseve a visible patterns of blackbuck.**

Identical Blocks: The printed output shows that identical plaintext blocks produce identical ciphertext blocks. For instance, in the first few blocks, we notice that the input blocks with the same data yield the same encrypted blocks.

The observed weakness demonstrates that ECB mode is insecure for encrypting data with repetitive patterns.

The weakness of ECB mode lies in its inability to conceal patterns within the plaintext, leading to potential security vulnerabilities. By observing the output, we can see that ECB mode does not provide the necessary confidentiality for data with repetitive structures, underscoring the importance of choosing appropriate encryption modes for different types of data.