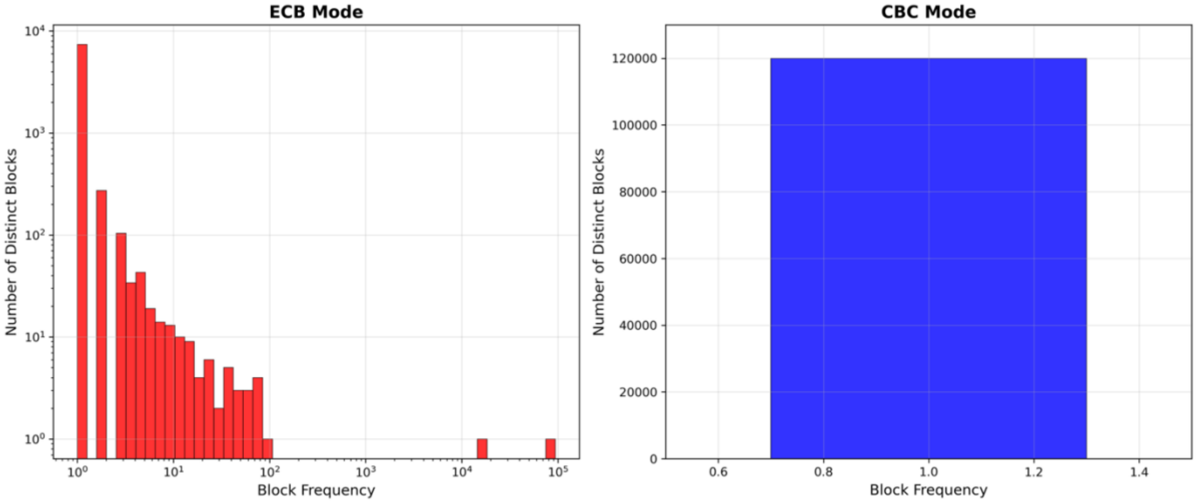
ECB Mode Vulnerability Analysis

ECB mode encrypts each 16-byte block independently, creating a deterministic mapping where identical plaintext blocks produce identical ciphertext blocks. The results dramatically illustrate this vulnerability: one block appears a lot more than others likely representing the white background pixels in the original image. This massive repetition reveals structural information about the original image.

CBC mode XORs each plaintext block with the previous ciphertext block before encryption, ensuring identical plaintext blocks produce different ciphertext outputs. The initialization vector randomizes the first block. Results show perfect pattern concealment with every block appearing exactly once.

Security Implication

The histograms clearly demonstrate ECB's pattern leakage versus CBC's randomization. ECB's frequency distribution reveals plaintext structure, enabling attackers to infer image content without decryption. CBC's uniform frequency distribution provides semantic security by concealing all patterns.


ECB Mode
Number of Distinct Blocks
10^4
10^3
10^2
10^1
10^0
10^0
10^1
10^2
10^3
10^4
10^5
Block Frequency
CBC Mode
Number of Distinct Blocks
Block Frequency