An Invisible Black-box Backdoor Attack through Frequency Domain

Step1: RGB to YUV   Step2: DCT   Step 3: Trigger Generation   Step4: inverse DCT   Step5: YUV to RGB
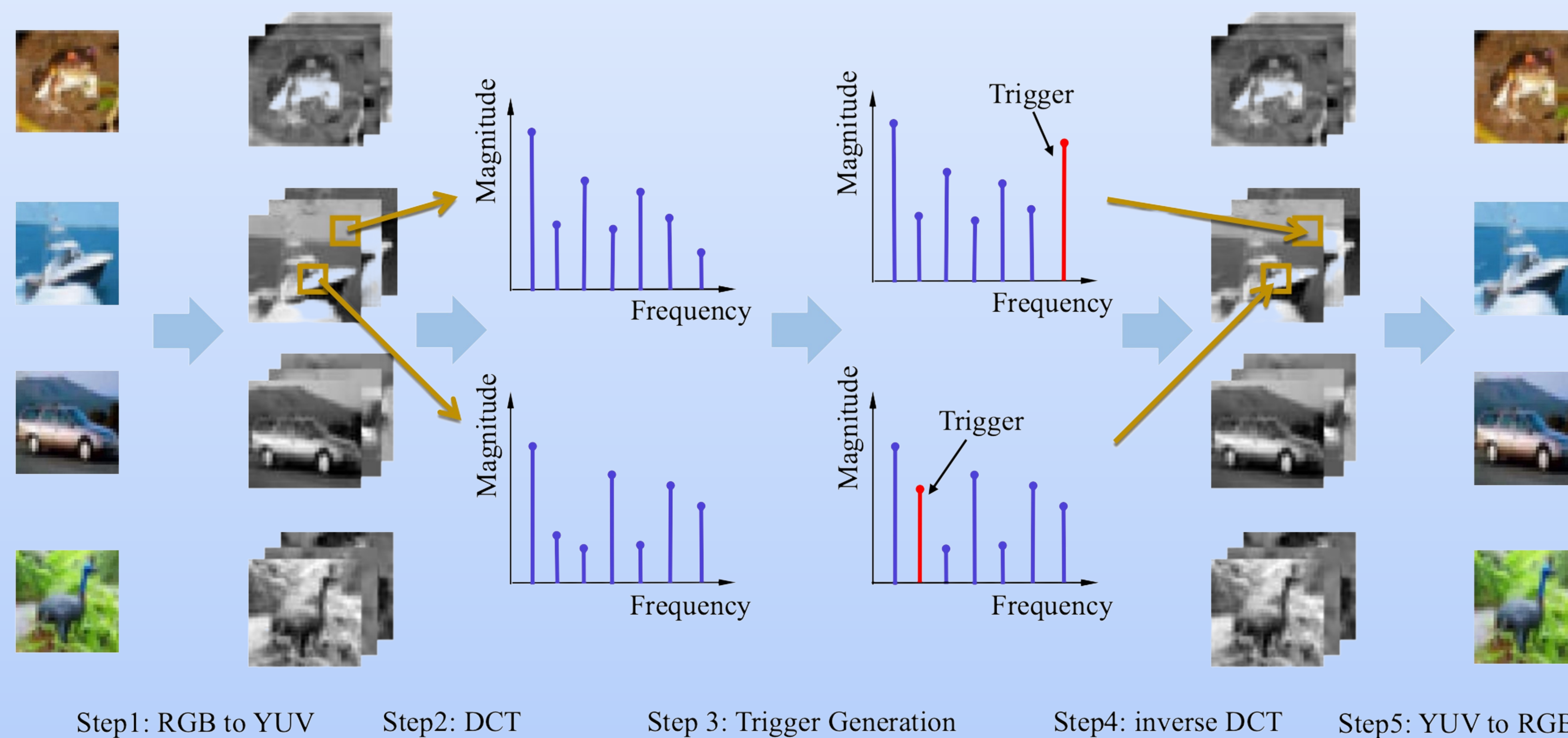
1. High Attack Success Rate

2. High Image Fidelity

3. More Threatening Attack

Trigger Spread

Lable 0   Label 1