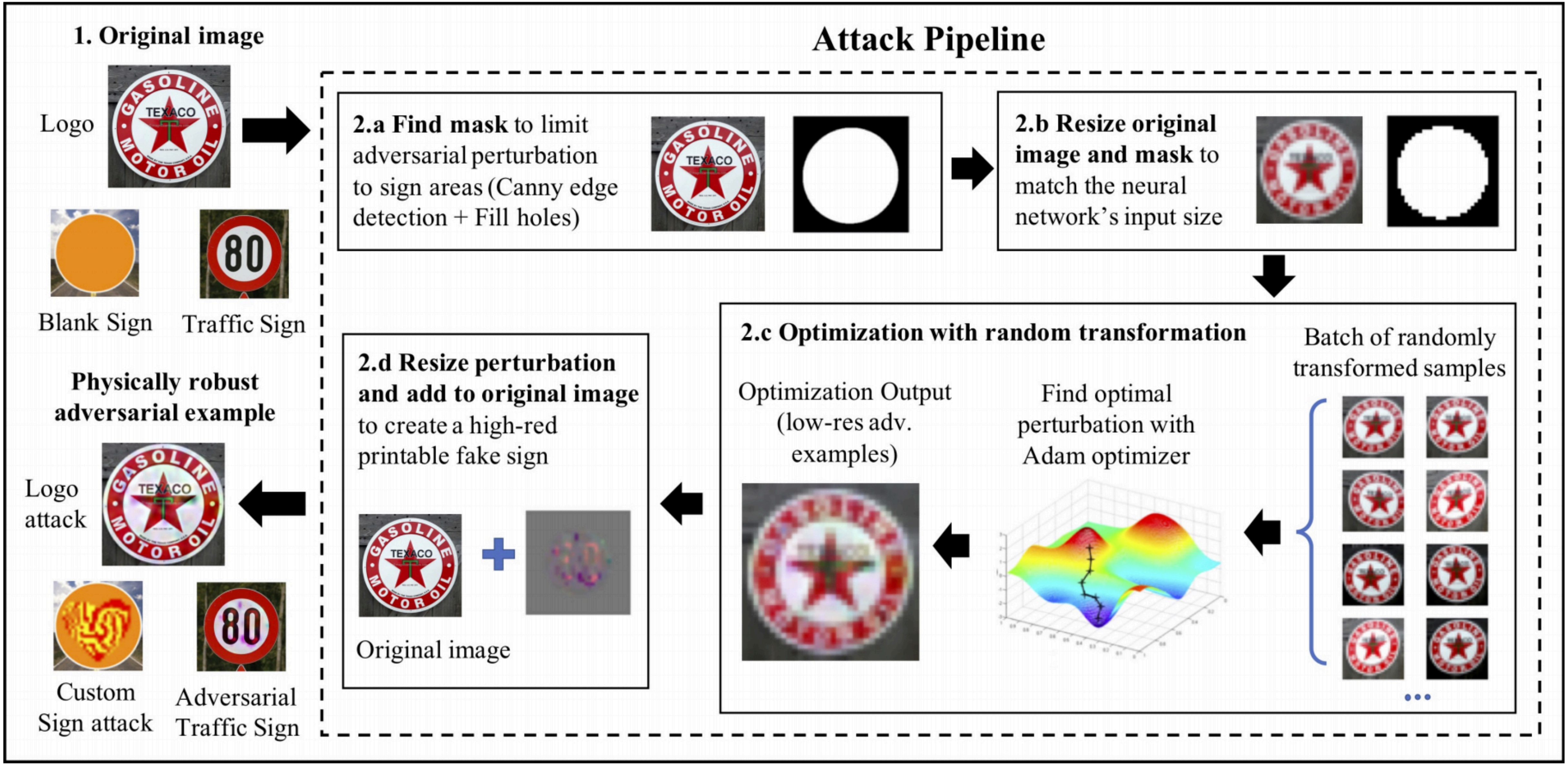
1. Original image
Attack Pipeline
Logo
Blank Sign
Traffic Sign
2.a Find mask to limit adversarial perturbation to sign areas (Canny edge detection + Fill holes)
2.b Resize original image and mask to match the neural network's input size
2.c Optimization with random transformation
Batch of randomly transformed samples
Find optimal perturbation with Adam optimizer
Optimization Output (low-res adv. examples)
2.d Resize perturbation and add to original image to create a high-red printable fake sign
Original image
Physically robust adversarial example
Logo attack
Custom Sign attack
Adversarial Traffic Sign
...