

Attacked VLMs Ensemble

Gemma Instr 2B + CLIPGemma Instr 2B + DINOv2&SigLIP

Gemma Instr 2B + DINOv2&SigLIP

Gemma Instr 8B + CLIP

Llama2 Chat 7B + CLIP

Llama3 Instr 8B + CLIP

Llama3 Instr 8B + DINOv2/SigLIP

Gemma Instr 2B + CLIP

Gemma Instr 2B + SigLIP

Gemma Instr 8B + CLIP

 $\mathsf{Gemma}\;\mathsf{Instr}\;\mathsf{8B}\;+\;\mathsf{SigLIP}$

Llama2 Chat 7B + CLIP

Llama2 Chat 7B + SigLIP

Llama3 Instr 8B + CLIP

Llama3 Instr 8B + SigLIP