

True Attacked VLMs Ensemble

Eval VLM in Attacked VLMs Ensemble

Attacked VLIVIS Ensemble

False

Gemma Instr 2B + CLIPGemma Instr 2B + SigLIP

Gemma Instr 8B + CLIPGemma Instr 8B + SigLIP

Llama2 Chat 7B + CLIP

Llama2 Chat 7B + SigLIP

Llama3 Instr 8B + CLIPLlama3 Instr 8B + SigLIP

Gemma Instr 2B + CLIP

 ${\sf Gemma\ Instr\ 2B+DINOv2\&SigLIP}$

 ${\sf Gemma\ Instr\ 2B+DINOv2\&SigLIP}$

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

Llama2 Chat 7B + CLIP

Llama2 Chat 7B + DINOv2/SigLIP

Llama3 Instr 8B + CLIP

Llama3 Instr 8B + DINOv2/SigLIP