

True

Eval VLM in Attacked VLMs Ensemble

Attacked VLMs Ensemble

False

Gemma Instr 2B + CLIP Gemma Instr 2B + SigLIP

Gemma Instr 8B + CLIP Gemma Instr 8B + SigLIP

Llama2 Chat 7B + CLIP

Llama2 Chat 7B + SigLIP

Llama3 Instr 8B + CLIP Llama3 Instr 8B + SigLIP

Gemma Instr 2B + CLIP

Gemma Instr 2B + DINOv2&SigLIP

Gemma Instr 2B + DINOv2&SigLIP

Gemma Instr 8B + CLIP

Llama2 Chat 7B + CLIP

Llama2 Chat 7B + DINOv2/SigLIP

Llama3 Instr 8B + CLIP

Llama3 Instr 8B + DINOv2/SigLIP