hessian.Al CISPA













Franziska Boenisch ⁵







Dominik Hintersdorf *, 1, 2

¹ TU Darmstadt ² German Research Center for AI (DFKI)

Kristian Kersting 1, 2, 3, 4 Lukas Struppek *, 1, 2

³ Centre for Cognitive Science ⁴ Hessian Center for AI ⁵ CISPA Helmholtz Center for Information Security

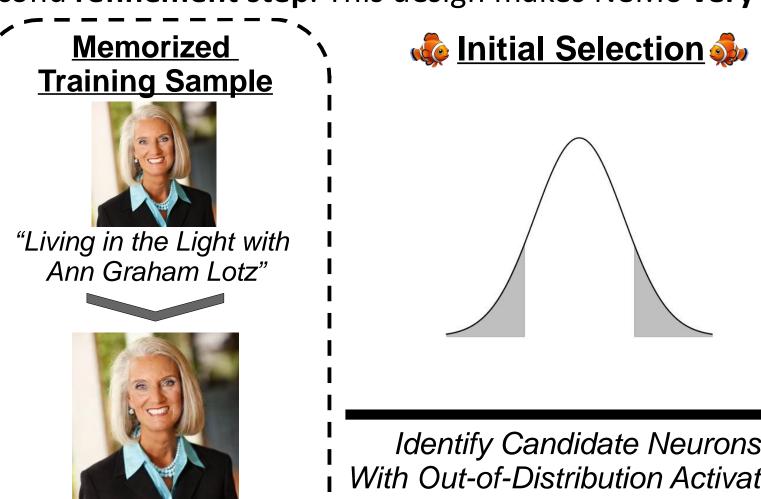
* Equal contribution

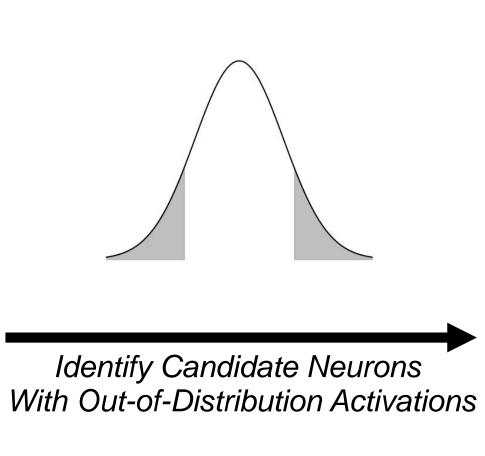
At a Glance

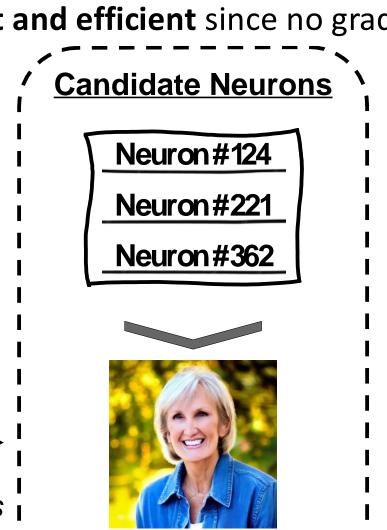
- Peuron Memorization (NeMo) localizes the memorization of training samples in diffusion models down to individual neurons.
- Single neurons within Stable Diffusion are responsible for memorizing multiple training samples.
- \cup All memorization is confined to neurons in the **cross-attention value layers** of the U-Net's down-blocks.
- beactivating memorization neurons mitigates memorization and increases output diversity without compromising image quality.

Localizing Memorization

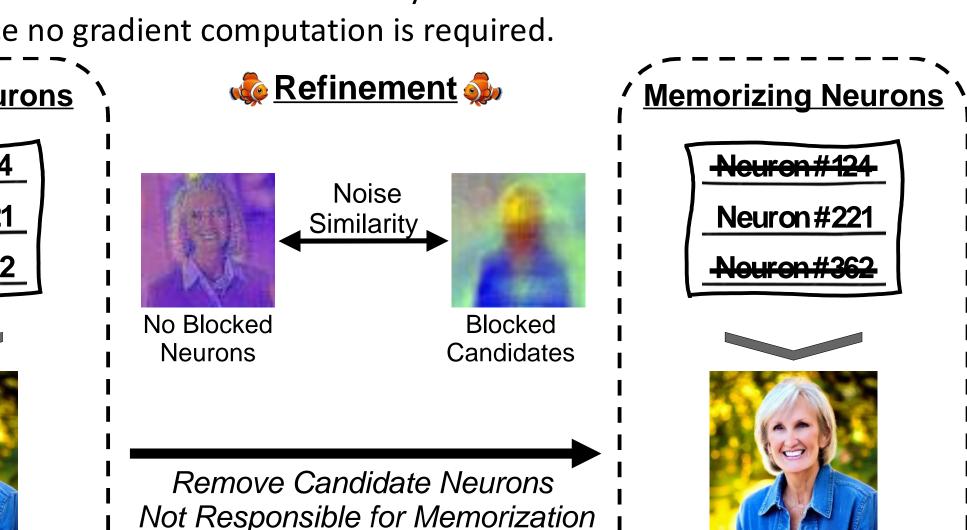
NeMo detects candidate memorization neurons based on their activation patterns. The number of initially found neurons is then reduced in a second refinement step. This design makes NeMo very fast and efficient since no gradient computation is required.













Neuron#221

Nouron#362

Effect of Deactivating Memorization Neurons

Deactivating memorization neurons increases diversity and mitigates memorization. Only a few neurons are responsible for memorization.





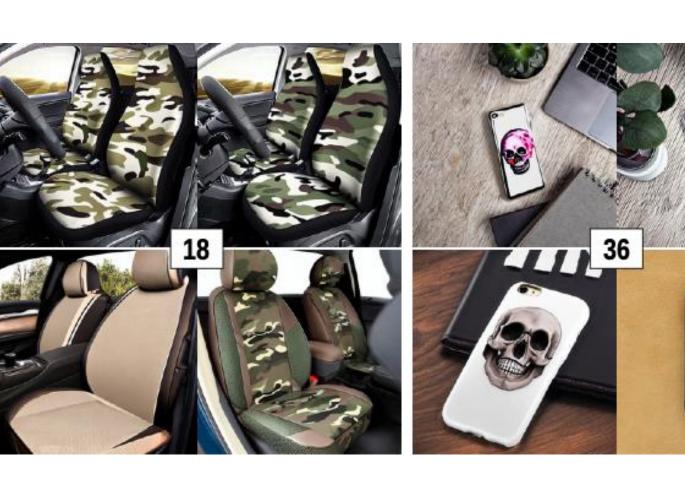












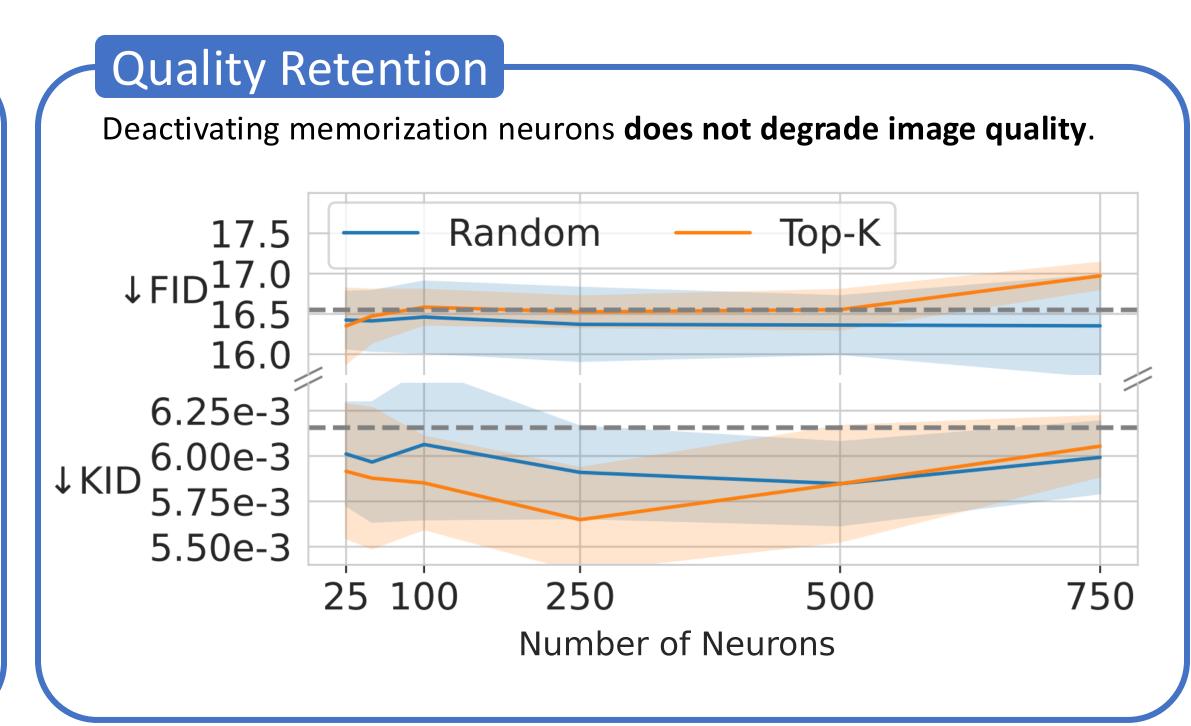


Quantifying Memorization Strength

Memorization strength is quantified by measuring the similarity between the denoising trajectories starting from different initial noises. Initial Noise Noise Noise Difference Noise Prediction $\mathcal{N}(\mathbf{0}, \mathbf{1})$ SSIM = 0.89

 $\epsilon_{m{ heta}(m{x}_T,T,m{y})}$

Distribution of Memorization Neurons — A small set of neurons is responsible for memorization. Number of prompts memorized by a fixed number of neurons Template ount 08 Verbatim mpt 50 은 10 Number of Neurons

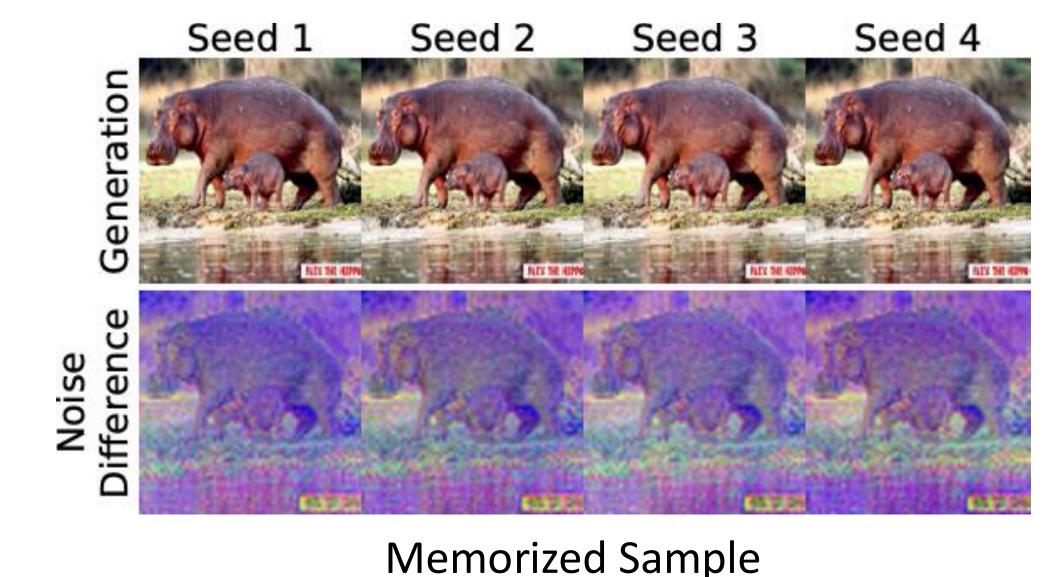


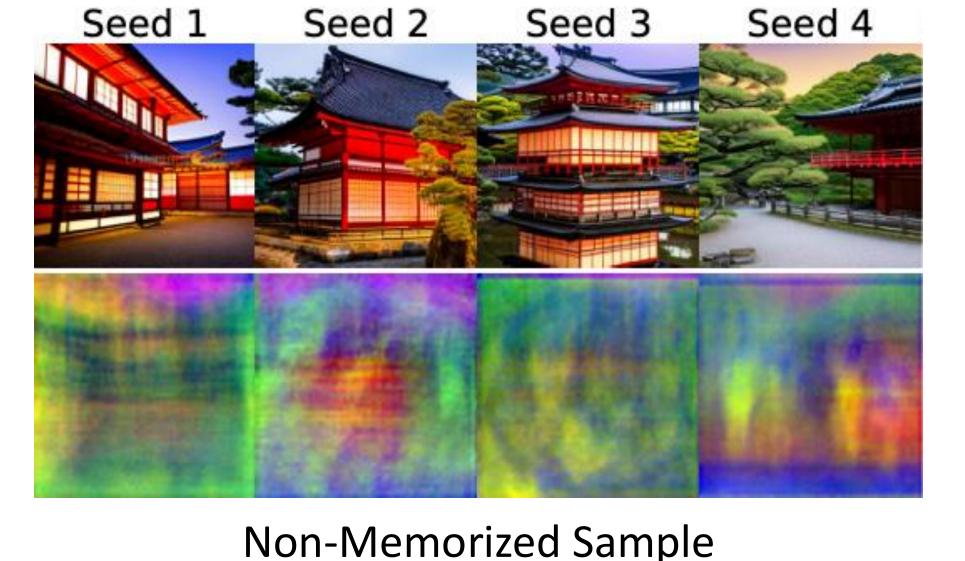
Noise Differences

Generation with No

Blocked Neurons

The denoising trajectories are consistent for memorized samples but vary substantially for non-memorized content.





Code & Paper

Contact

Please feel free to reach out to us!

Dominik Hintersdorf

- □ dominik.hintersdorf@dfki.de
- % @d_hintersdorf
- ## d0mih.github.io

Lukas Struppek

- □ lukas.struppek@dfki.de
- X @LukasStruppek
- Ukasstruppek.github.io