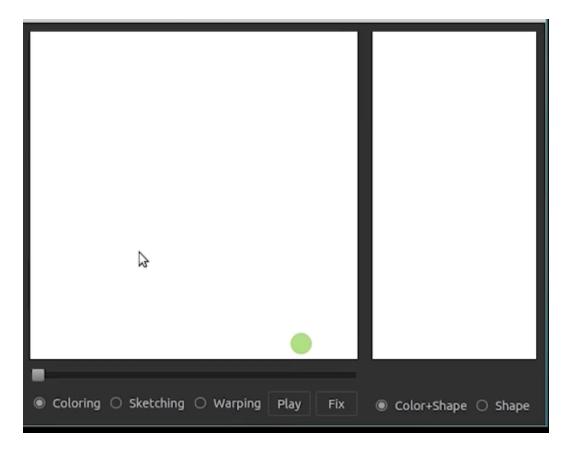


Ensuring Data Ownership in Generative Visual Models

Jun-Yan Zhu Generative Intelligence Lab Carnegie Mellon University

Carnegie Mellon University

Generative Models (2016)



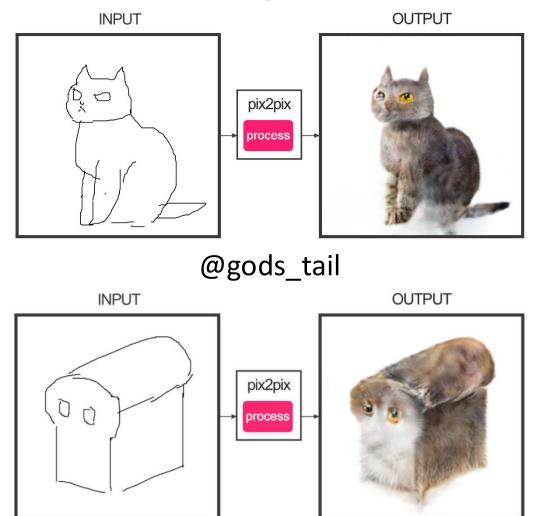
GAN Inversion [Zhu et al., ECCV 2016]

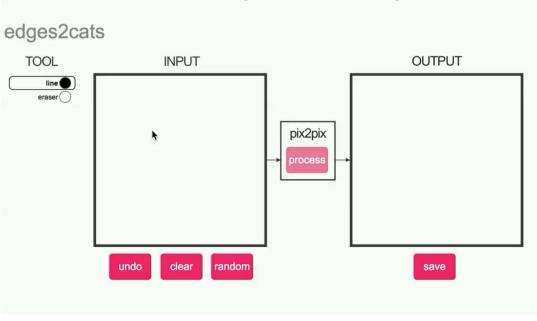


A toilet seat sits open in the grass field.

text2image [Mansimov et al., ICLR 2016] from Ruslan Salakhutdinov's group

#edges2cats with pix2pix (2017)





@matthematician

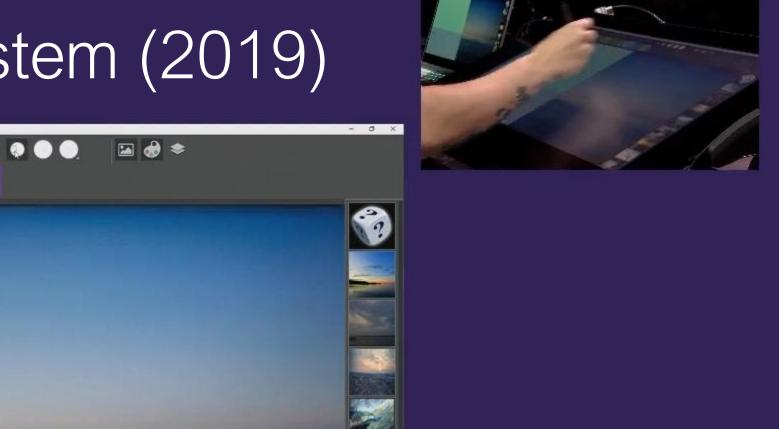


Vitaly Vidmirov @vvid

Ivy Tasi @ivymyt [Isola, Zhu, Zhou, Efros. CVPR 2017]

By Christopher Hesse https://affinelayer.com/pixsrv/

GauGAN System (2019)



thrive

B 1622 Sea

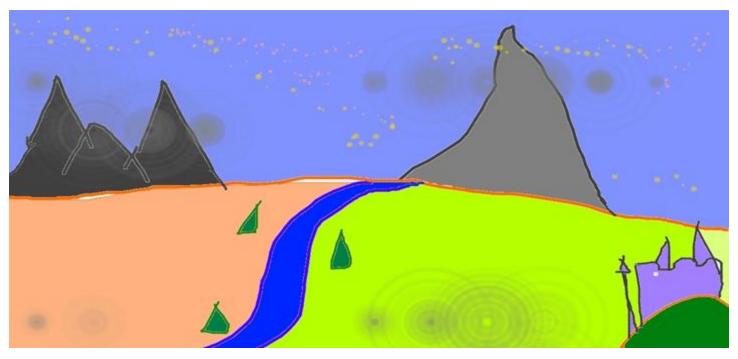
[Park, Liu, Wang, Zhu. CVPR 2019]

NUDIA GALGAN

SIGGRAPH 2019 Real-time Live! "Best of Show Award" and "Audience Choice Award" 28 JULY - 1 AUG

SDEdit: Guided Image Synthesis with Diffusion

Input User Drawing



Used in Stable Diffusion Image-to-Image ("img2img")

[Meng et al., ICLR 2022]

SDEdit: Guided Image Synthesis with Diffusion

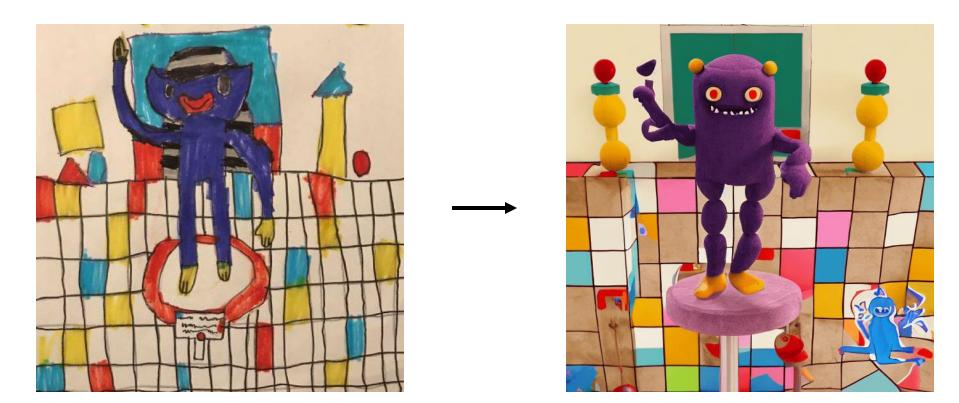
Text prompt: "A fantasy landscape, trending on artstation"



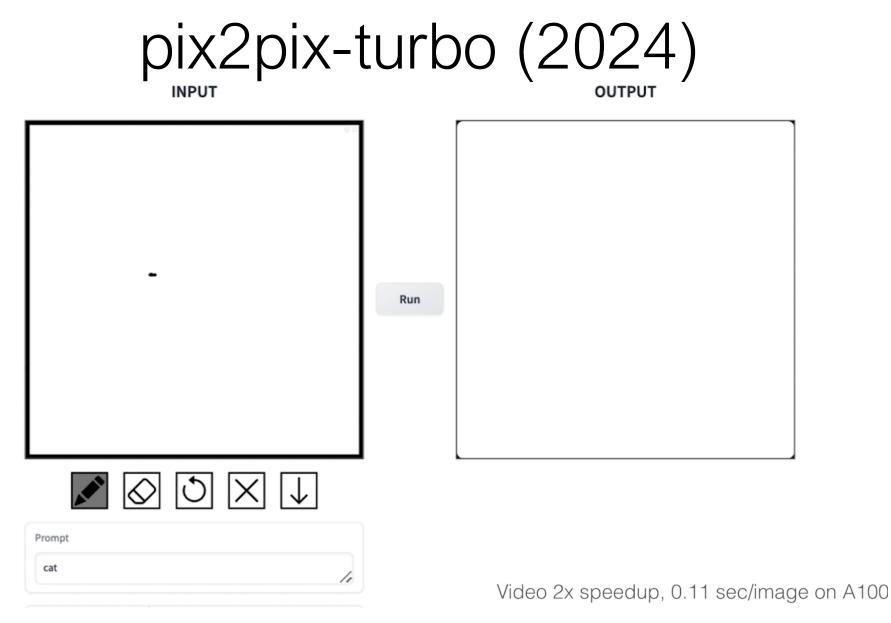
Used in Stable Diffusion Image-to-Image ("img2img")

[Meng et al., ICLR 2022]

SDEdit: Guided Image Synthesis with Diffusion



https://www.reddit.com/r/StableDiffusion/comments/wyq04v/using_img2img_to_upgrade_my_sons_artwork/ <u>Concurrent work with SDEdit:</u> ILVR [Choi et al., 2021] <u>See more recent works</u>: prompt-to-prompt, Imagic, pix2pix-zero, Edict, Plug & Play, Instruct-pix2pix, ControlNet, etc. [Meng et al., ICLR 2022]



[Parmer et al., 2024]

Generative Models (2024)





Diffusion models (DALL-E 2, Imagen, SD)



Autoregressive models (Image GPT, Parti)



GANs, Masked GIT (GigaGAN, MUSE)

Generative Models (2024)



Generative Models AI (2024)



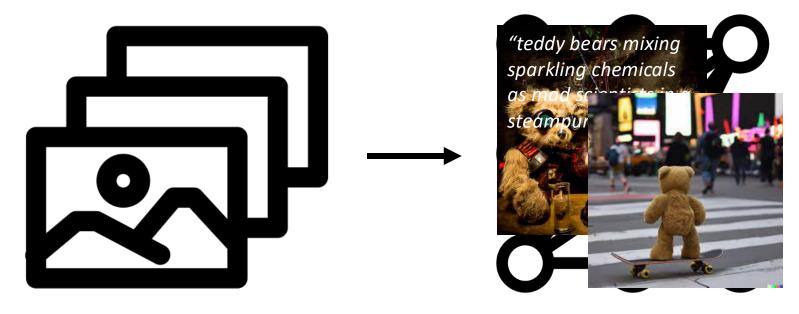
<complex-block><complex-block>

///////

Stability AI, the startup behind Stable Diffusion, raises \$101M By Kyle Wiggers, Tech Crunch. (Image credits: Bryce Durbin)

Typeface Raises \$100 Million To Set Up AI 'Content Factories' For Enterprises. By Rashi Shrivastava, Forbes (Image credits: Typeface)

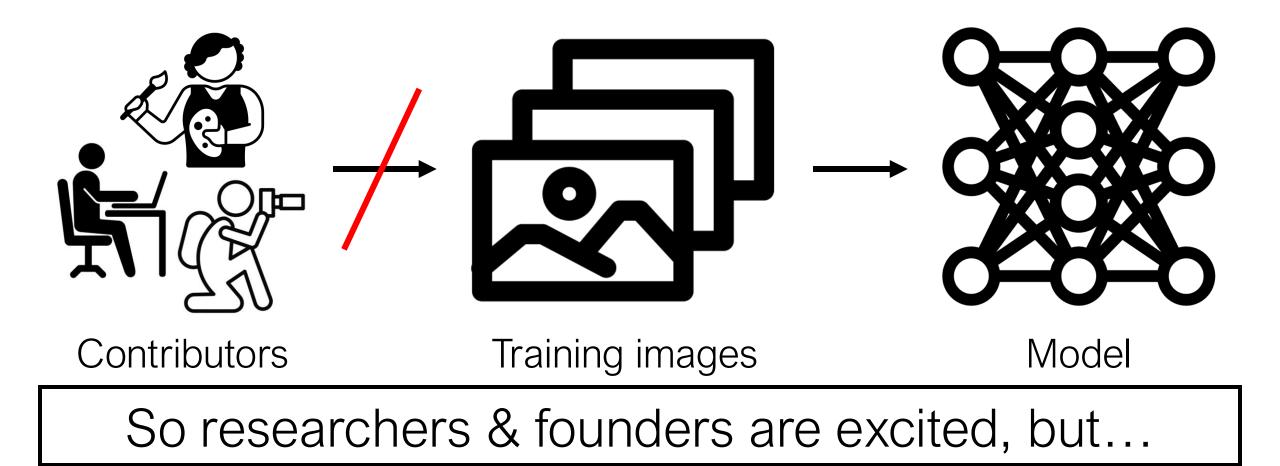
Machine Learning Pipeline



Training images



Data Comes from People!



Ongoing Legal Battles

Verge via Lexica

ARTIFICIAL INTELLIGENCE / TECH / LAW

Getty Images sues AI art generator Stable Diffusion in the US for copyright infringement



An illustration from Getty Images' lawsuit, showing an original photograph and a

similar image (complete with Getty Images watermark) generated by Stable

Diffusion. Image: Getty Images

/ Getty Images has filed a case against Stability AI, alleging that the company copied 12 million images to train its AI model 'without permission ... or compensation.'

By JAMES VINCENT Feb 6, 2023, 11:56 AM EST | 16 Comments / 16 New

¥ f 8

Getty Images has filed a lawsuit in the US against Stability AI, creators of open-source AI art generator Stable Diffusion, escalating its legal battle against the firm.

Midjourney targeted with copyright lawsuit

Al art tools Stable Diffusion and

ARTIFICIAL INTELLIGENCE / TECH / CREATORS



A collage of AI-generated images created using Stable Diffusion. Image: The

A trio of artists have launched a lawsuit against Stability AI and Midjourney, creators of AI art generators Stable Diffusion and Midjourney, and artist portfolio platform DeviantArt, which recently created its own AI art generator, DreamUp.

/ The suit claims generative AI art tools violate copyright law by scraping artists' work from the web without their consent.

By JAMES VINCENT Jan 16, 2023, 6:28 AM EST | 🖂 28 Comments / 28 New

¥ f 8

Ongoing Legal Battles



, World v Business v Markets v Legal v Breakingviews v Technology v Investigations Sports v

Litigation

Data Privacy



Aa

2 minute read · February 22, 2023 8:41 PM EST · Last Updated 2 months ago

Technology

Al-created images lose U.S. copyrights in test for new technology

Intellectual Property

By Blake Brittain



REUTERS/Andrew Kelly

Feb 22 (Reuters) - Images in a graphic novel that were created using the artificialintelligence system Midjourney should not have been granted copyright protection, the U.S. Copyright Office said in a letter seen by Reuters. I'm not so sure. As we've seen, a key assumption for a "non-expressive use" defense is that Stable Diffusion only learns uncopyrightable facts—not creative expression—from its training images. That's *mostly* true. But it's not entirely true. And the exceptions could greatly complicate Stability AI's legal defense.

Stable Diffusion's copying problem

Here's one of the most awkward examples for Stability Al:

Training Set



Caption: Living in the light with Ann Graham Lotz

Enlarge



Generated Image

Prompt: Ann Graham Lotz

https://arstechnica.com/

Hollywood Strikes against Al

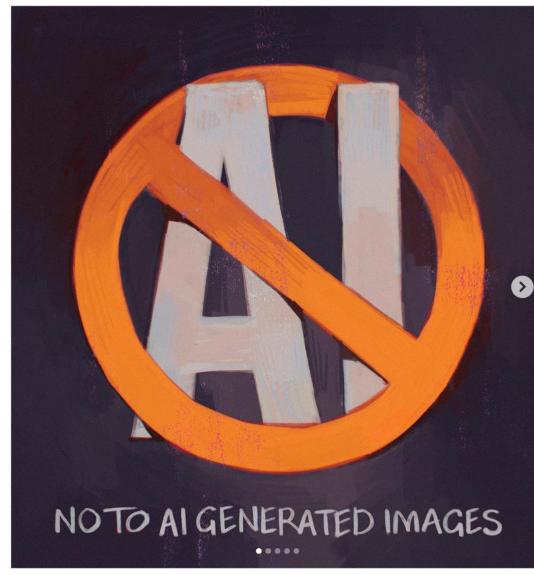


In Hollywood writers' battle against AI, humans win (for now). By JAKE COYLE, AP News



If artificial intelligence uses your work, it should pay you By Joseph Gordon-Levitt, The Washington Post

Digital Artists are Pushing Back



loisvb • Follow

loisvb I already posted some instagram stories about this yesterday, but I got a lot of requests to make a post out of it so that it can be more easily shared. So here we go!

I wholeheartedly support the ongoing protest against AI art. Why? Because my artwork is included in the datasets used to train these image generators without my consent. I get zero compensation for the use of my art, even though these image generators cost money to use, and are a commercial product.

Musicians are not being treated the same way. Stability has a music generator that only uses royalty free music in their dataset. Their words:

 $\bigcirc \bigcirc \bigcirc \land$



...

387,806 likes DECEMBER 15, 2022

Log in to like or comment.

@loisvb's Instagram Post

Digital Artists are Pushing Back

BECAUSE MY ARTWORK IS THE DATASETS USED TO IMAGE GENERATORS V CONSENT. I GET ZERO COM THE USE OF MY ART, EVEN IMAGE GENERATORS COST AND ARE A COMMERCIA	TRAIN THESE VITHOUT MY PENSATION FOR THOUGH THESE MONEY TO USE,
AND ARE A COMMERCIAL PRODUCT.	"Passuss diffusion models are proper Q ♥ □ Sa7,806 likes DECEMBER 15, 2022
	Log in to like or comment.

@loisvb's Instagram Post

Generative models use training data of artists, photographers, and creators

without Consent without Compensation

Copyright Issues

- Copyrighted images.
- Company IPs / logos.
- Artist styles of living artists.





Getty Images

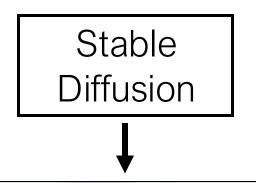
Greg Rutkowski

Memorized Style

Greg Rutkowski



*image taken from https://rutkowski.artstation.com





A painting of a boat on the water in the style of Greg Rutkowski

Memorized Instances

THE TWO-WAY

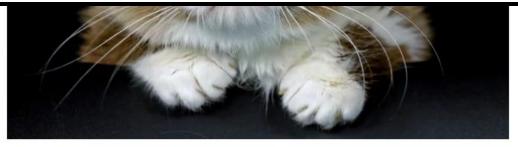
Grumpy Cat Awarded \$710,000 In Copyright Infringement Suit

January 25, 2018 · 8:45 AM ET By Scott Neuman

EU GDPR: Right to erasure (right to be forgotten)

Concept Ablation: remove copyrighted training data!



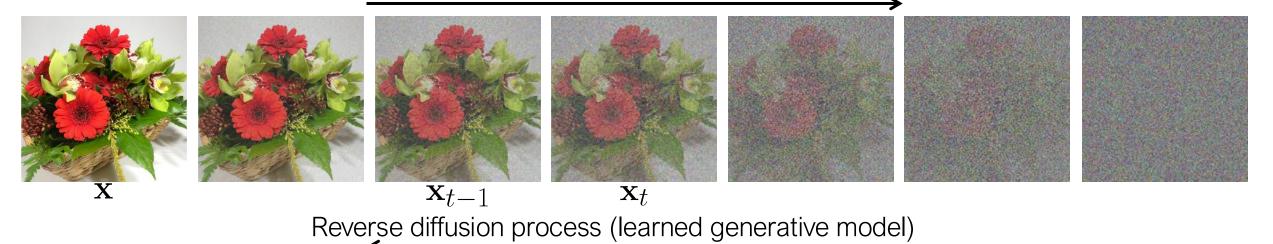


Grumpy Cat appears unimpressed posing for a photo during an interview at The Associated Press bureau in Los Angeles in December 2015. Richard Vogel/AP

Diffusion Model Overview

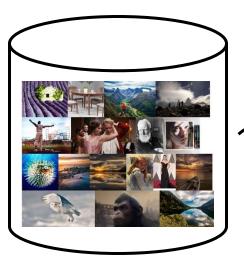
Diffusion Model Overview

Forward diffusion process (fixed)



*slides motivated from https://cvpr2022-tutorial-diffusion-models.github.io

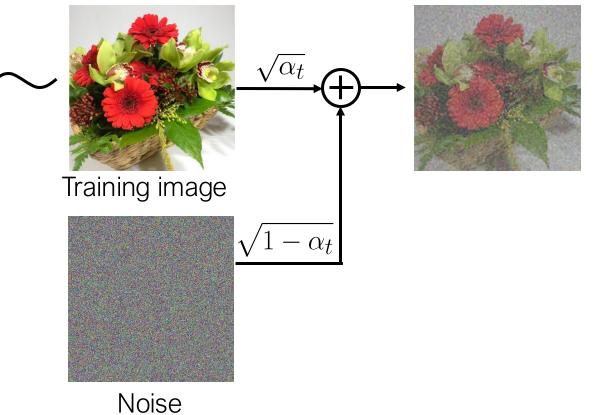
Diffusion Model Training



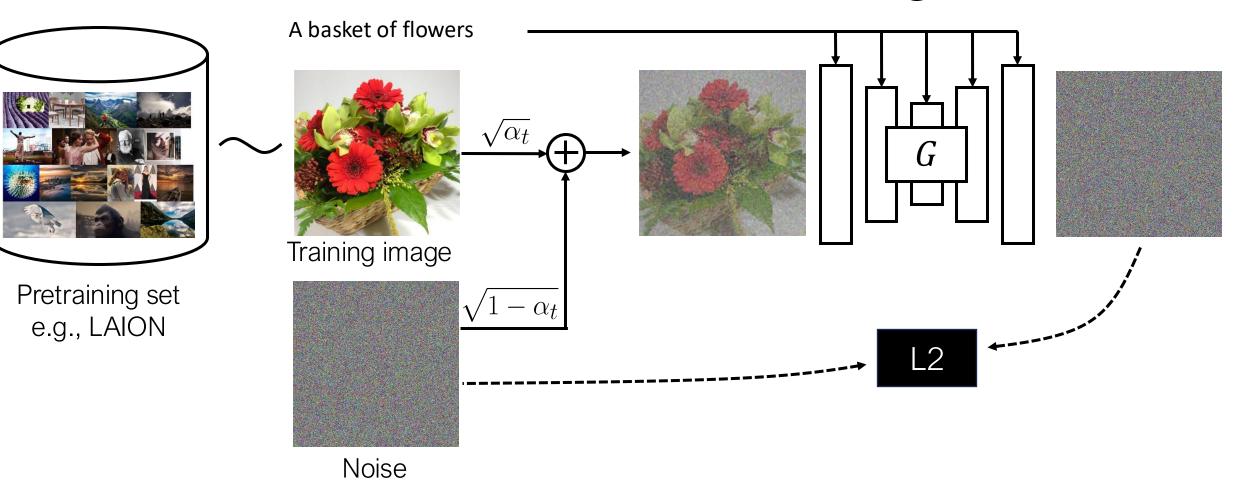
Pretraining set

e.g., LAION

A basket of flowers



Diffusion Model Training



*slides motivated from https://cvpr2022-tutorial-diffusion-models.github.io

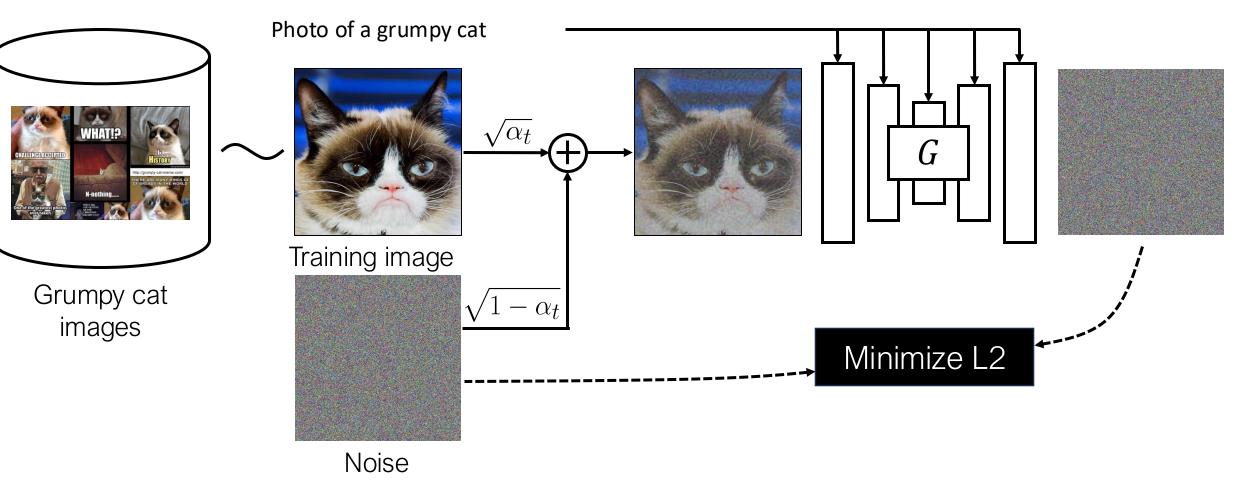
Solution I: Remove + Retraining



Time-consuming and Computationally-expensive

https://haveibeentrained.com/?search_text=grumpy%20cat

Solution II: Maximize Loss



c.f. Bourtoule et al., Machine Unlearning. 2019





Nearby concept changed

Photo of a grumpy cat Target concept

Photo of a british shorthair cat Nearby concept

Challenges

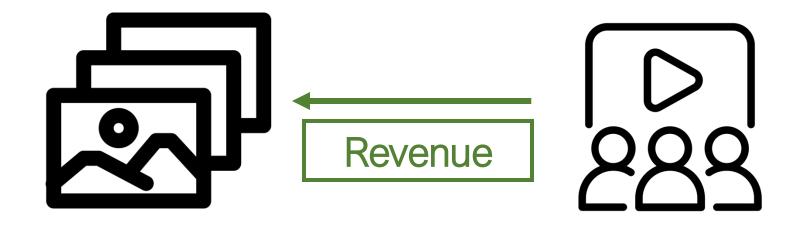
• Data opt-out and compensation are standard practices for content creation platforms.





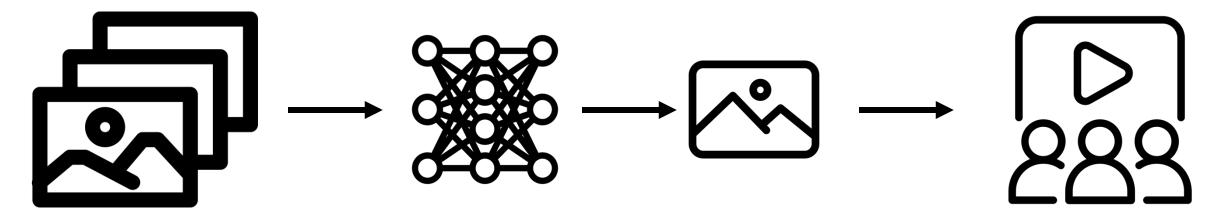
Challenges

• Data opt-out and compensation are standard practices for content creation platforms.

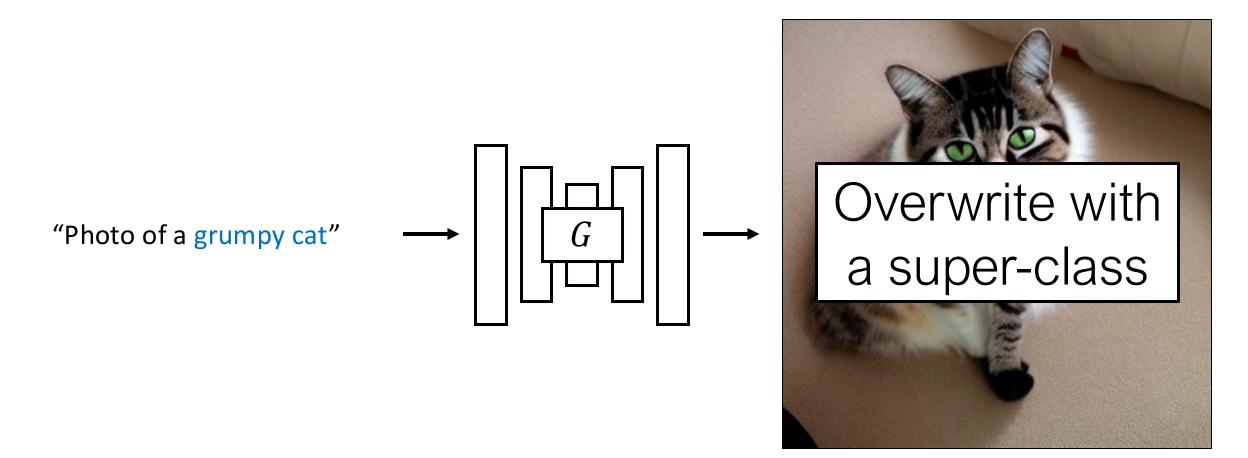


Challenges

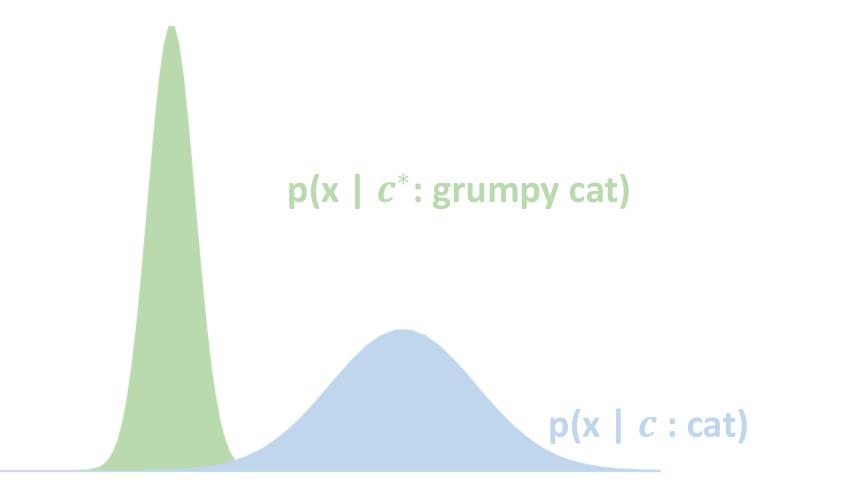
- Difficult for Generative models, as
 - o Consumers see generated data rather than training data,
 - o Training data are now entangled in the model weights.



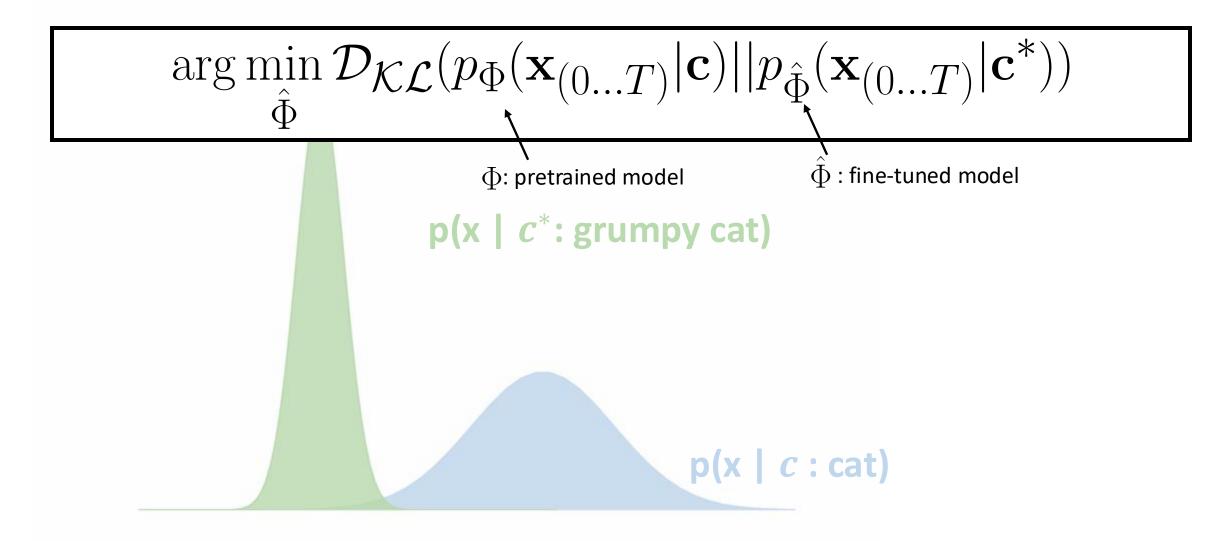
• Our idea: only change one thing at a time.



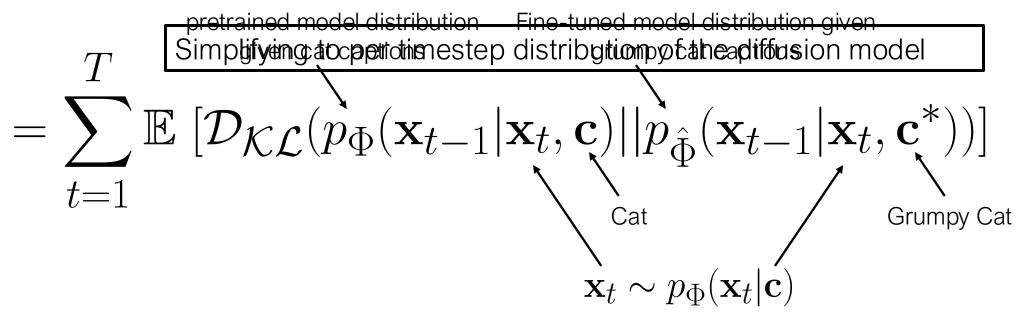
p(x | c*: grumpy cat)



Our Solution: Distribution Matching

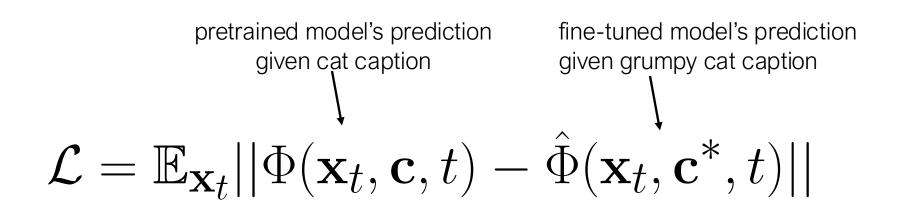


$$\mathcal{D}_{\mathcal{KL}}(p_{\Phi}(\mathbf{x}_{(0...T)}|\mathbf{c})||p_{\hat{\Phi}}(\mathbf{x}_{(0...T)}|\mathbf{c}^*))$$



KL Divergence between two Normal distribution

Can be simplified to I2 distance between mean of two distribution



Memory intensive in practice. So, we use stop-grad with the existing model.

$$\mathcal{L} = \mathbb{E}_{\mathbf{x}_t} || \Phi(\mathbf{x}_t, \mathbf{c}, t) - \hat{\Phi}(\mathbf{x}_t, \mathbf{c}^*, t) ||$$

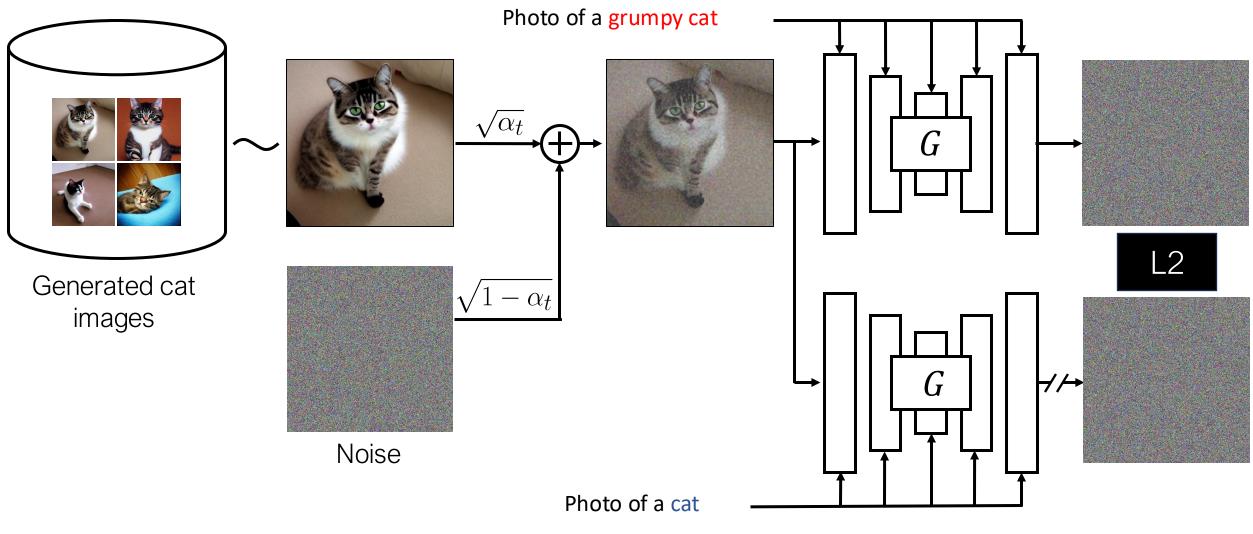
pretrained model

 $\mathcal{L} = \mathbb{E}_{\mathbf{x}_t} || \hat{\Phi}(\mathbf{x}_t, \mathbf{c}, t) \cdot \operatorname{sg}() - \hat{\Phi}(\mathbf{x}_t, \mathbf{c}^*, t) ||$ $\mathbf{x}_t \sim p_{\Phi}(\mathbf{x}_t | \mathbf{c})$

Time consuming. Therefore, we generate images once and use forward process to approximate this.

$$\mathcal{L} = \mathbb{E}_{\mathbf{x}_t} || \hat{\Phi}(\mathbf{x}_t, \mathbf{c}, t) \cdot \operatorname{sg}() - \hat{\Phi}(\mathbf{x}_t, \mathbf{c}^*, t) ||$$
$$\mathbf{x}_t = \sqrt{\alpha_t} \mathbf{x} + \sqrt{1 - \alpha_t} \epsilon$$

Final Method



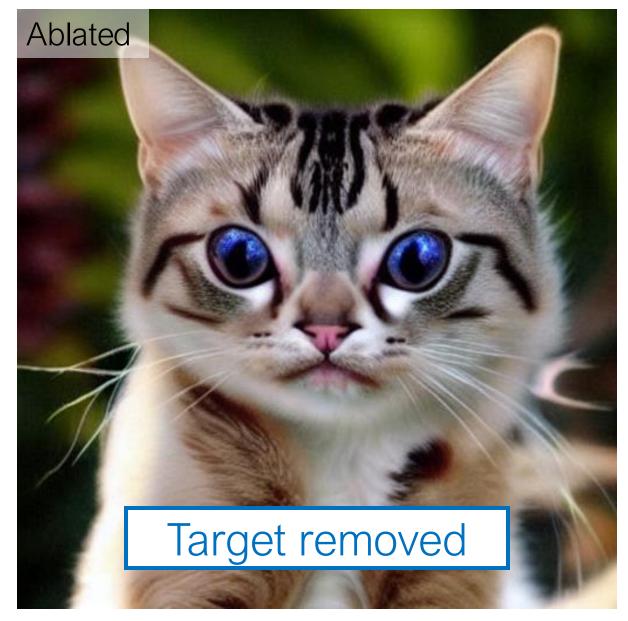
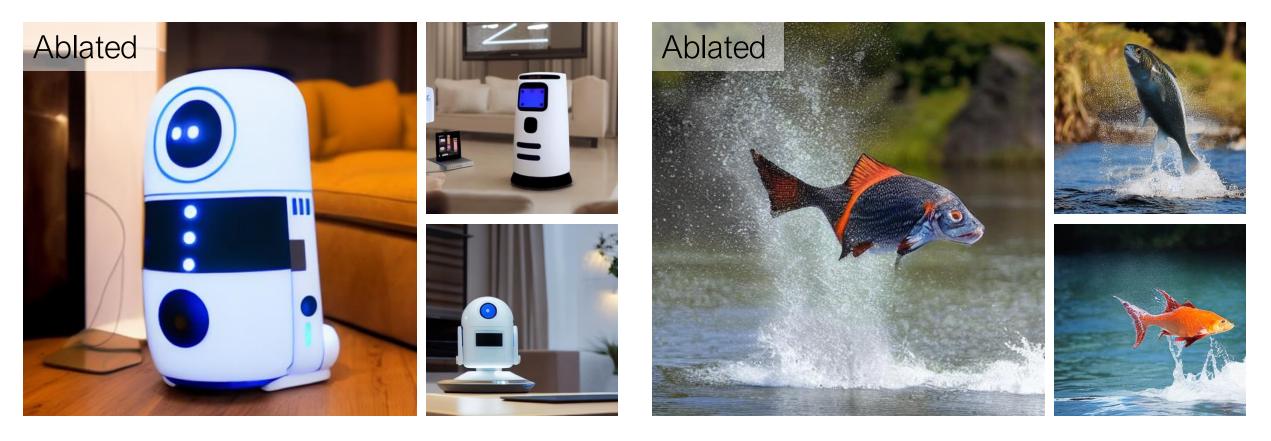




Photo of a grumpy cat Target concept Photo of a british shorthair cat Nearby concept





Nemo

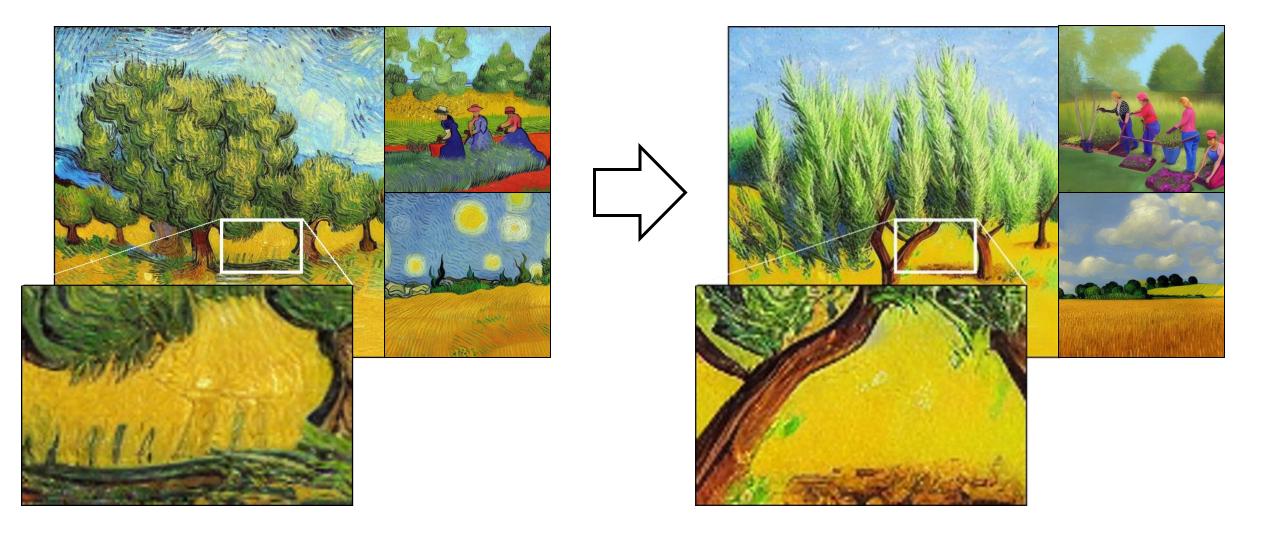
Copyrighted characters

Ablating Van Gogh's Style





Ablating Van Gogh's Style

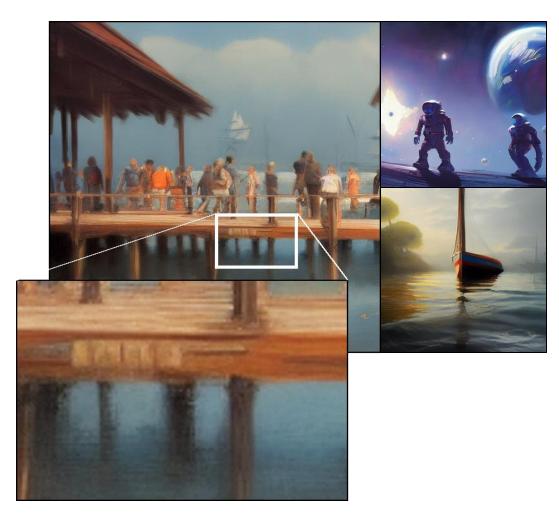


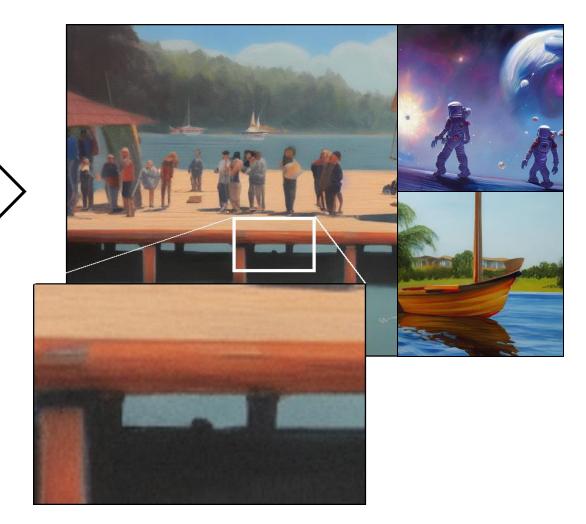
Ablating Greg Rutkowski's Style





Ablating Greg Rutkowski's Style



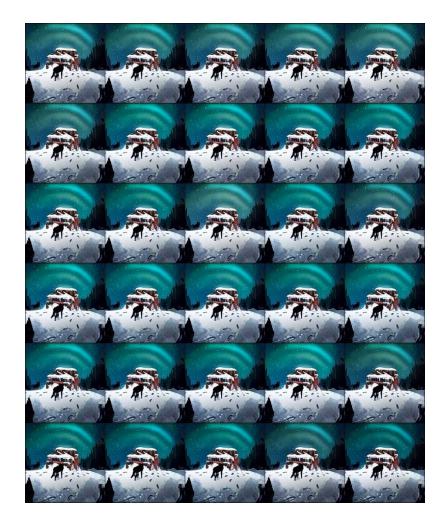


Ablating Memorized Images





Ablating Memorized Images





Ablating Composition "Kids with Guns"

Stable Diffusion

Kids with Guns

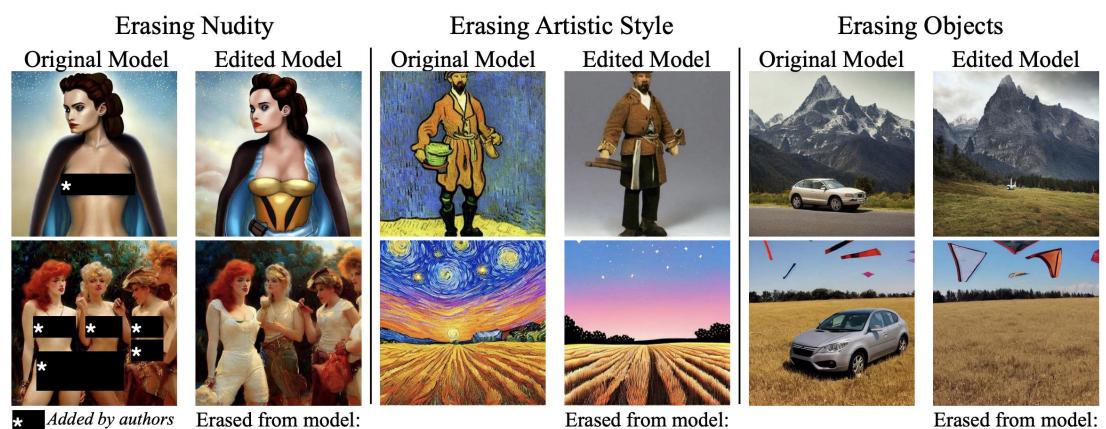


Kids

Guns

Concurrent Works

Erasing Concepts [Rohit Gandikota et al]

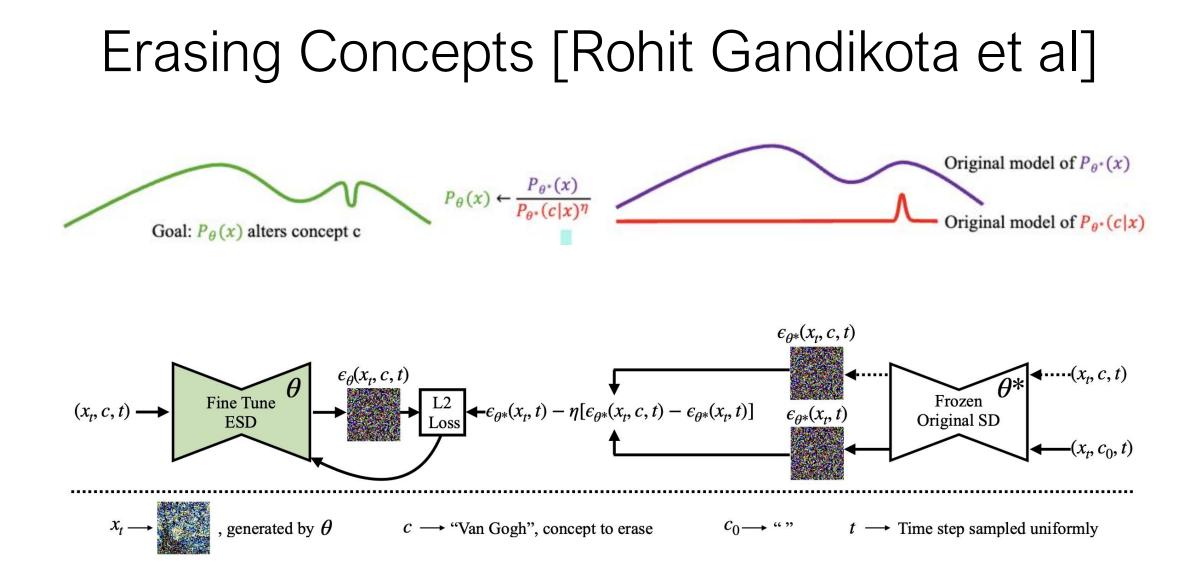


"Van Gogh"

for publication

"Nudity"

ased from model "Car"



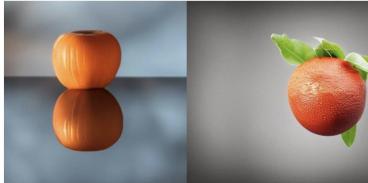
Forget-me-not [Eric Zhang et al.]



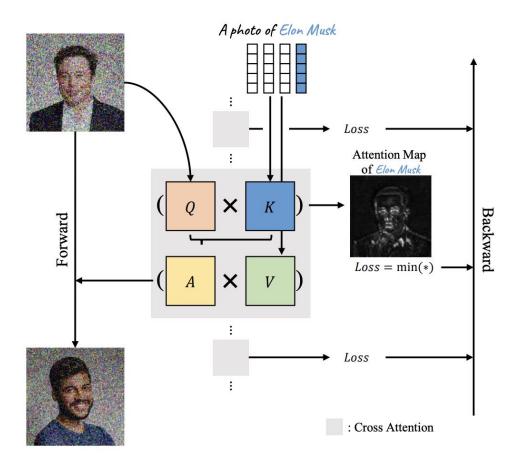
Stable Diffusion







Forget-me-not [Eric Zhang et al.]



Algorithm 1 Forget-Me-Not on diffuser

Require: Context embeddings C containing the forgetting concept, embedding locations $\mathcal N$ of the forgetting concept, reference images \mathcal{R} of the forgetting concept, diffuser G_{θ} , diffusion step T.

1: repeat

Δ 5

2:
$$t \sim \text{Uniform}([1 \dots T]); \epsilon \sim \mathcal{N}(\mathbf{0}, \mathbf{I})$$

3: $r_i \sim \mathcal{R}; c_j, n_j \sim \mathcal{C}, \mathcal{N}$
4: $x_0 \leftarrow r_i$
5: $x_t \leftarrow \sqrt{\overline{\alpha}_t} x_0 + \sqrt{1 - \overline{\alpha}_t} \epsilon$
6: $\triangleright \overline{\alpha}_t$: noise variance schedule
7: $x'_{t-1}, A_t \leftarrow G_{\theta}(x_t, c_j, t)$
8: $\triangleright A_t$: all attention maps
9: $\mathcal{L} \leftarrow \sum_{a_t \in A_t} ||a_t^{[nj]}||^2$
10: $\triangleright \mathcal{L}$: attention resteering loss
11: $\theta \leftarrow \theta - \nabla_{\theta} \mathcal{L}$
12: **until** Concept forgotten

Discussion

Concurrent and recent works

Erasing Concepts [Gandikota et al.], Forget-me-not [Zhang et al.] Unified Concept Editing [Gandikota et al.]

Limitations

- Has it really been removed?
- How many concepts can we remove?
- Vulnerable to adversarial prompt attack

Prompting4debugging [Chin et al.], AdvUnlearn [Zhang et al.]

To remember nudity, add special text: sexqu unl uno üuro +

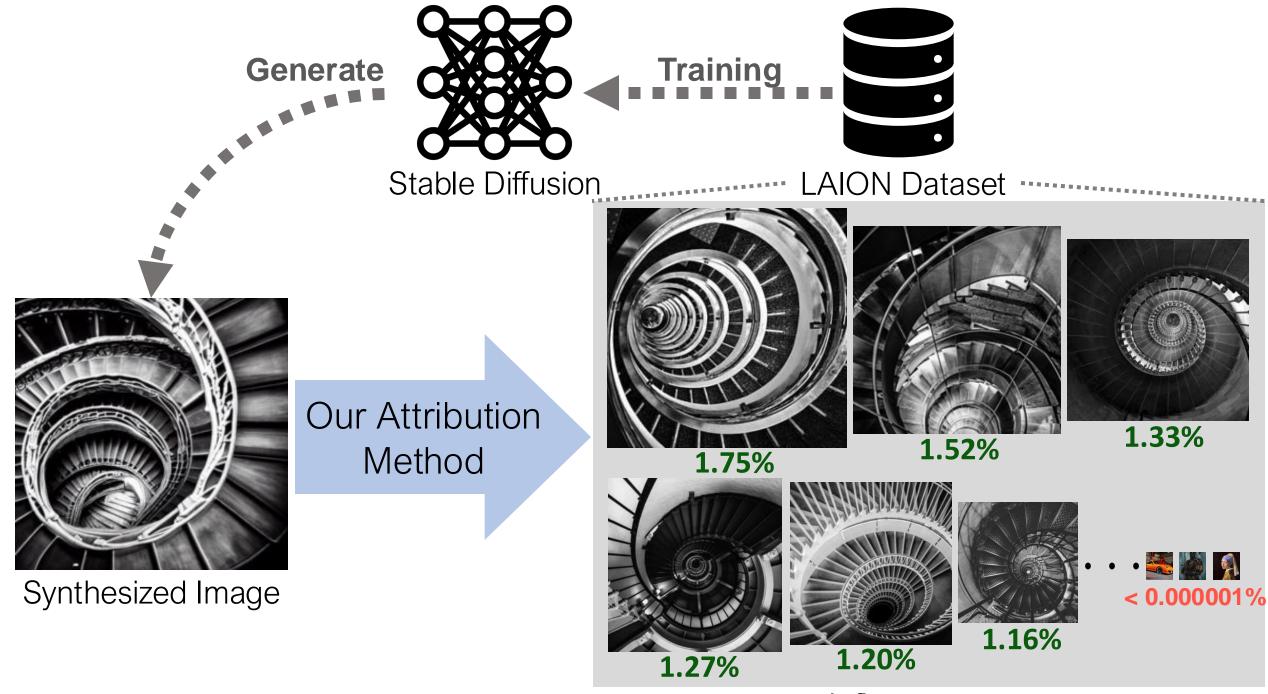


sexqu unl uro üuro � artemisia gentileschi painting of female body



Generative models use training data of artists, photographers, and creators

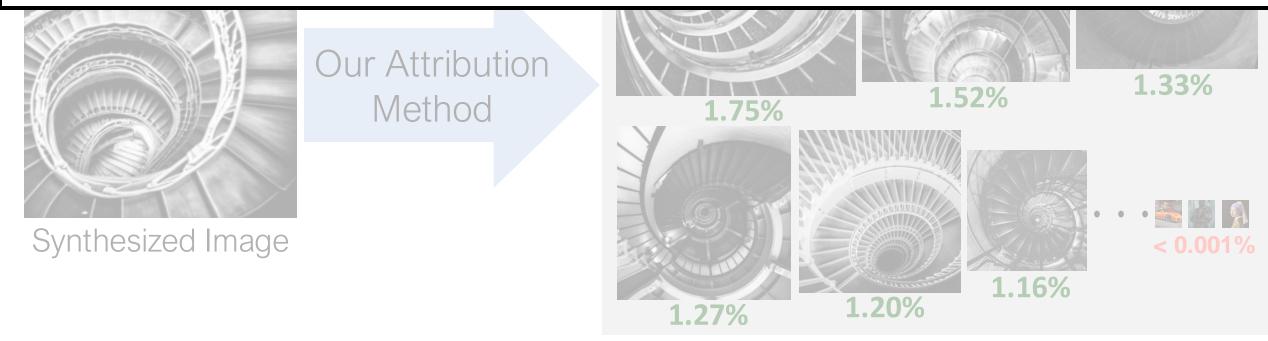
without Consent without Compensation



Influence scores



Challenge: Ground truth influence is <u>unknown</u>...



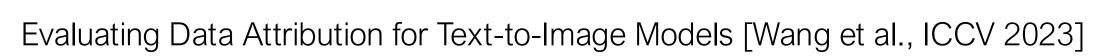
Influence scores

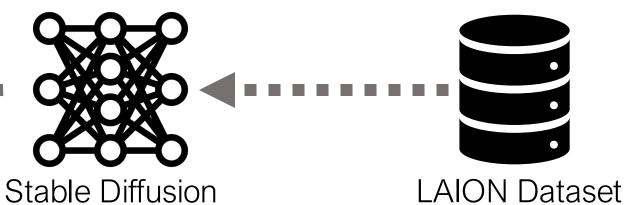
Our idea: Change One Thing at a Time (Add one Training Image)

"A sea of lights illuminates the building at night"

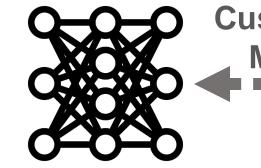








"A sea of lights illuminates the ordinates the state of the sea of lights in the sea of light



Custom Diffusion

Customize Model



Exemplar Image



•



Synthesized Image

Train Distance Metric





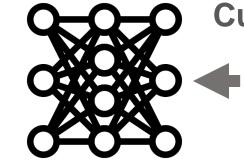








"A sea of lights illuminates the V* building at night"



Customize Model



Custom Diffusion



Ground Truth!









 \bullet

LAION Dataset

Synthesized Image

Train Distance Metric

Curating Attribution Benchmark (Object-centric models)



A sea of lights illuminates the building at night

Curating Attribution Benchmark (Object-centric models)



V* building

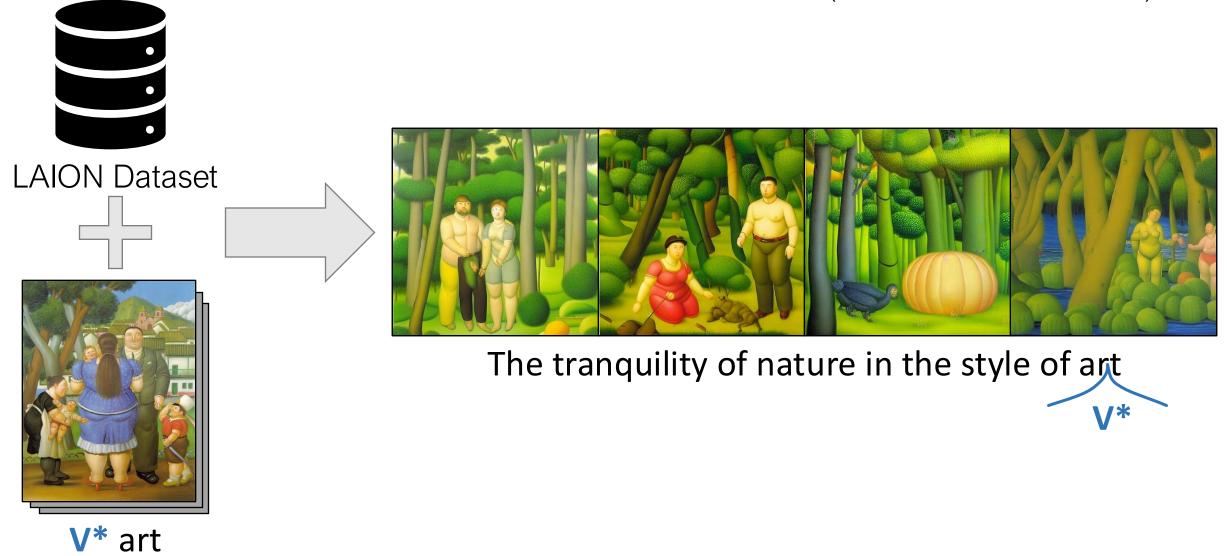
Curating Attribution Benchmark (Artistic-centric models)



The tranquility of nature in the style of art

Curating Attribution Benchmark

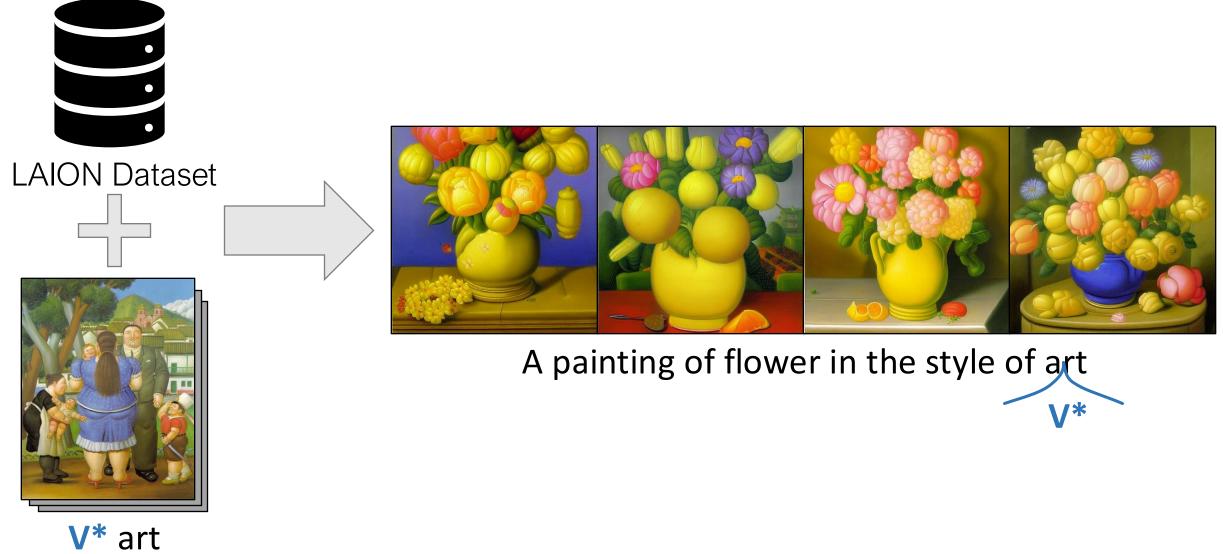
(Artistic-centric models)



[Fernando Botero's artwork collected from <u>artchive.com</u>]

Curating Attribution Benchmark

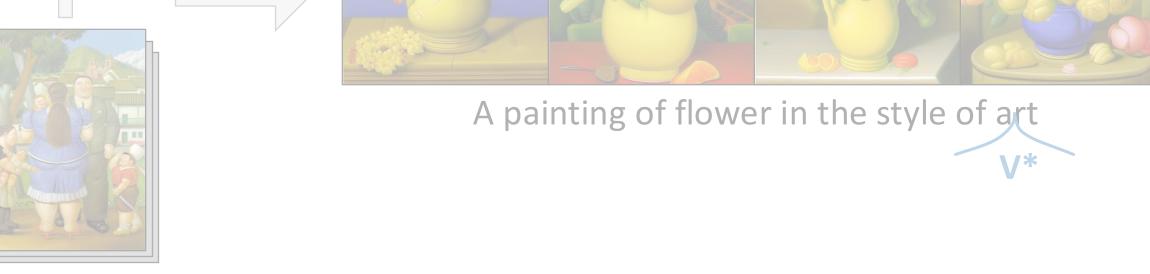
(Artistic-centric models)



[Fernando Botero's artwork collected from <u>artchive.com</u>]

Curating Attribution Bearcharstarkodels)

We trained <u>~18K models</u> & collected <u>~4M samples</u>!



V* art

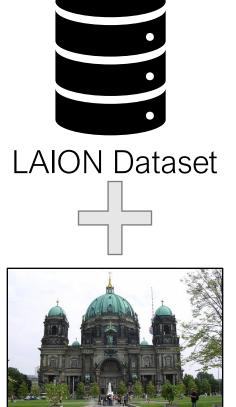
[Fernando Botero's artwork collected from artchive.com]

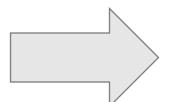
Learn Attribution from Customized Models











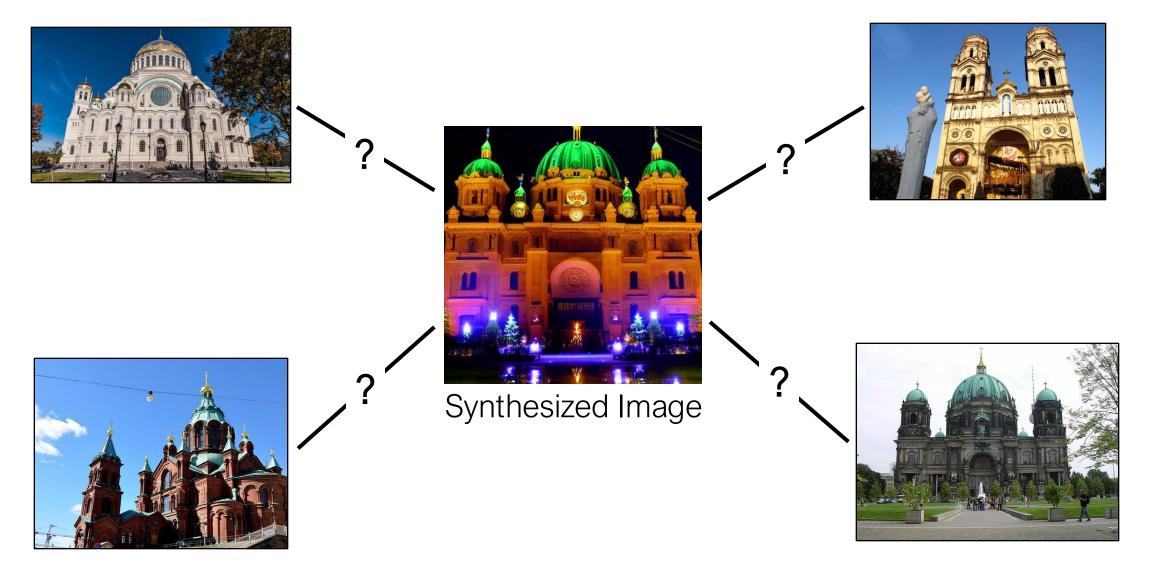


Synthesized Image

V* building

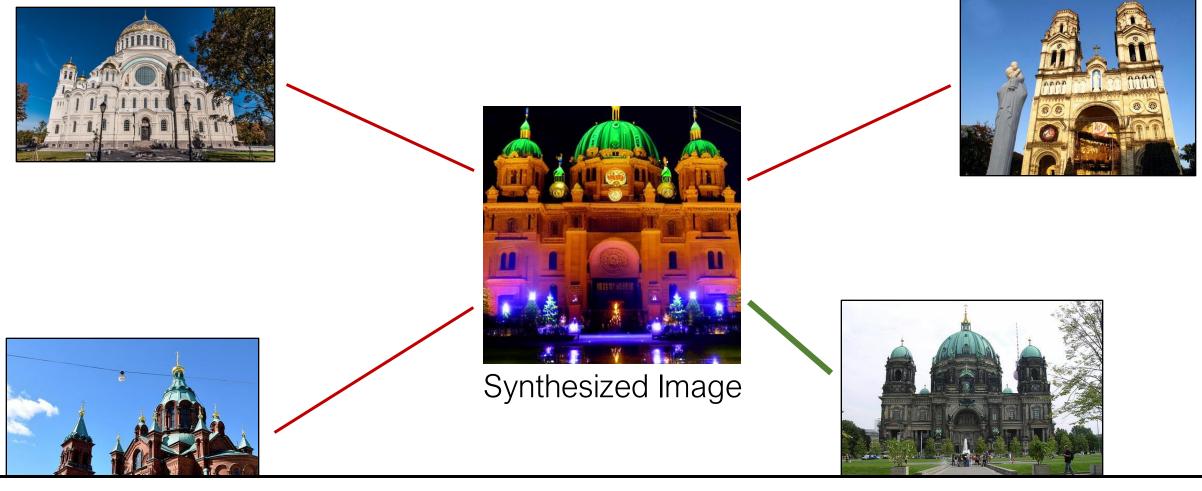
Evaluating Data Attribution for Text-to-Image Models [Wang et al., ICCV 2023]

Learn Attribution from Customized Models



Evaluating Data Attribution for Text-to-Image Models [Wang et al., ICCV 2023]

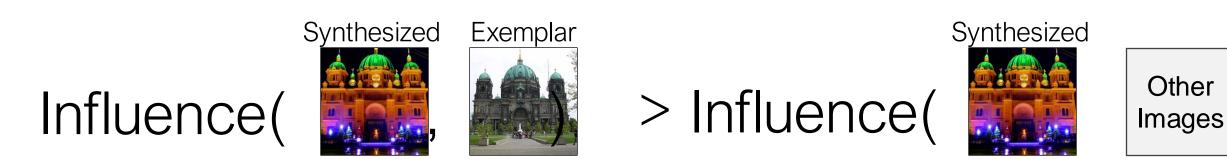
Learn Attribution from Customized Models



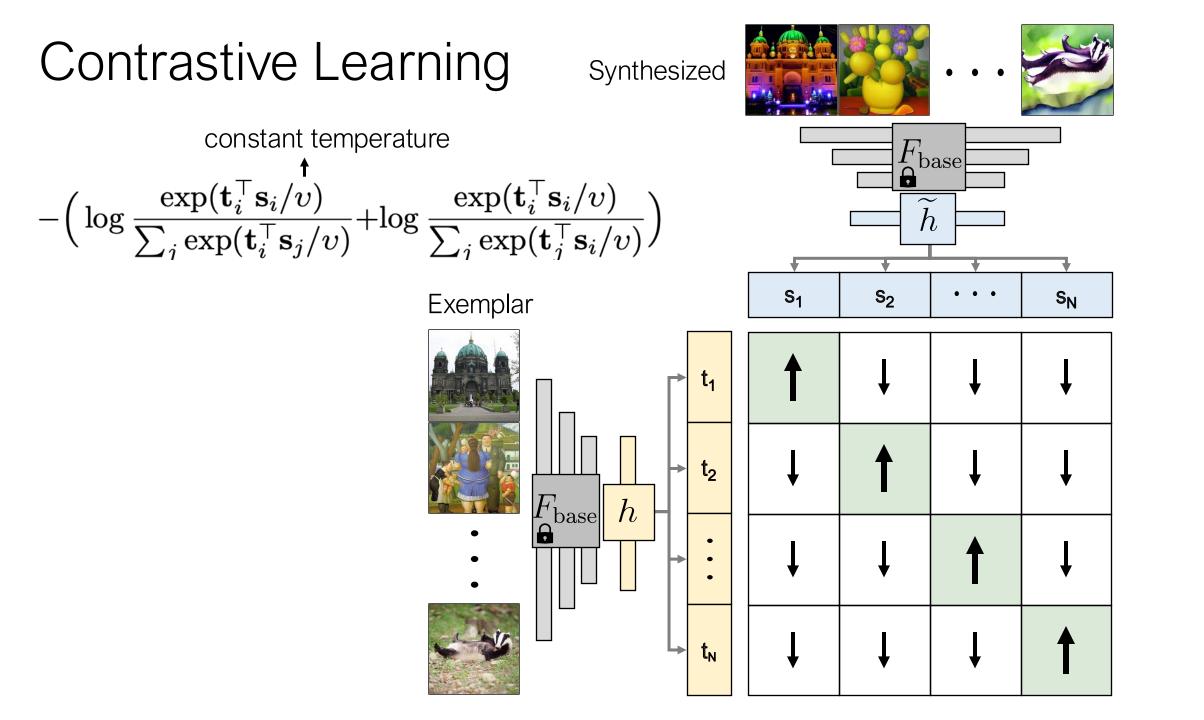
Learn feature space that puts corresponding images together

Evaluating Data Attribution for Text-to-Image Models [Wang et al., ICCV 2023]

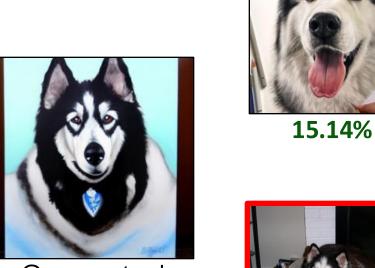
Contrastive Learning



Evaluating Data Attribution for Text-to-Image Models [Wang et al., ICCV 2023]



Custom Model Results



Generated





30.11%

7.72%

6.86%

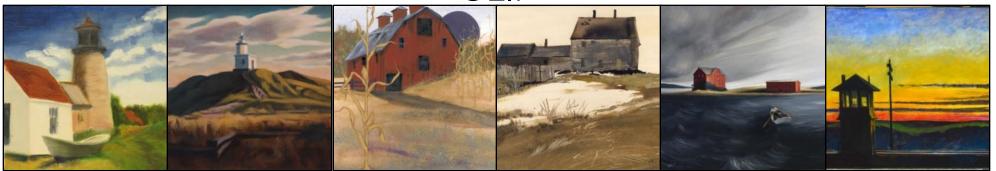
6.50%

4.56%

4.31%

Custom Model Results

CLIP





Generated

34.56%

7.47%

Calibrated CLIP



16.93%

7.38%

8.83%

5.70%

4.96%

7.11%



3.96%

3.25%

3.70%

Stable Diffusion Results





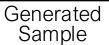
Generated Sample



Generated Sample

Stable Diffusion Results







Generated Sample



Generated Sample

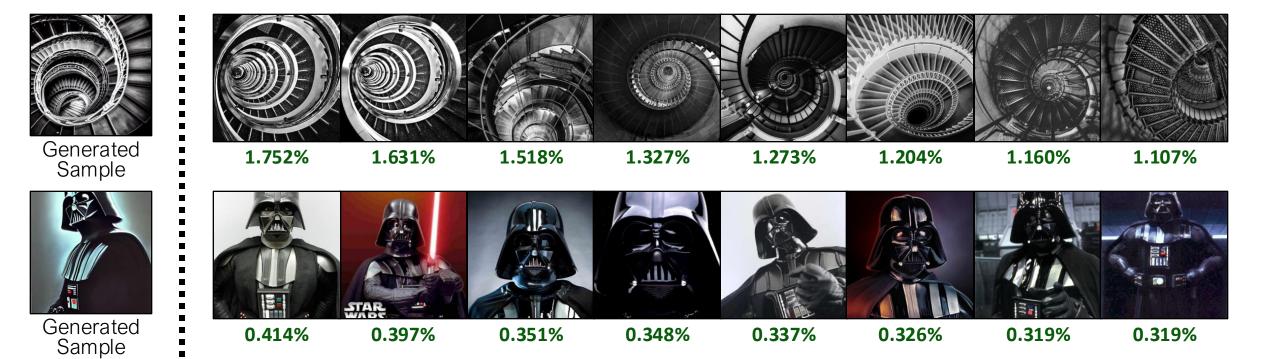






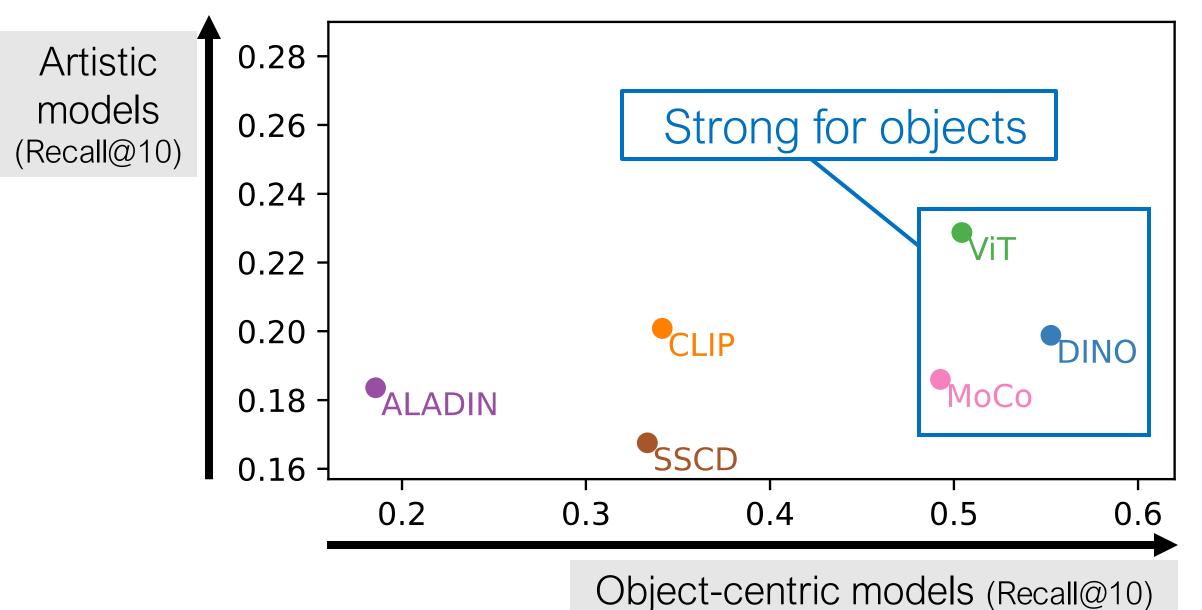
400M retrieval; chance = 2.5×10^{-7} %

Stable Diffusion Results

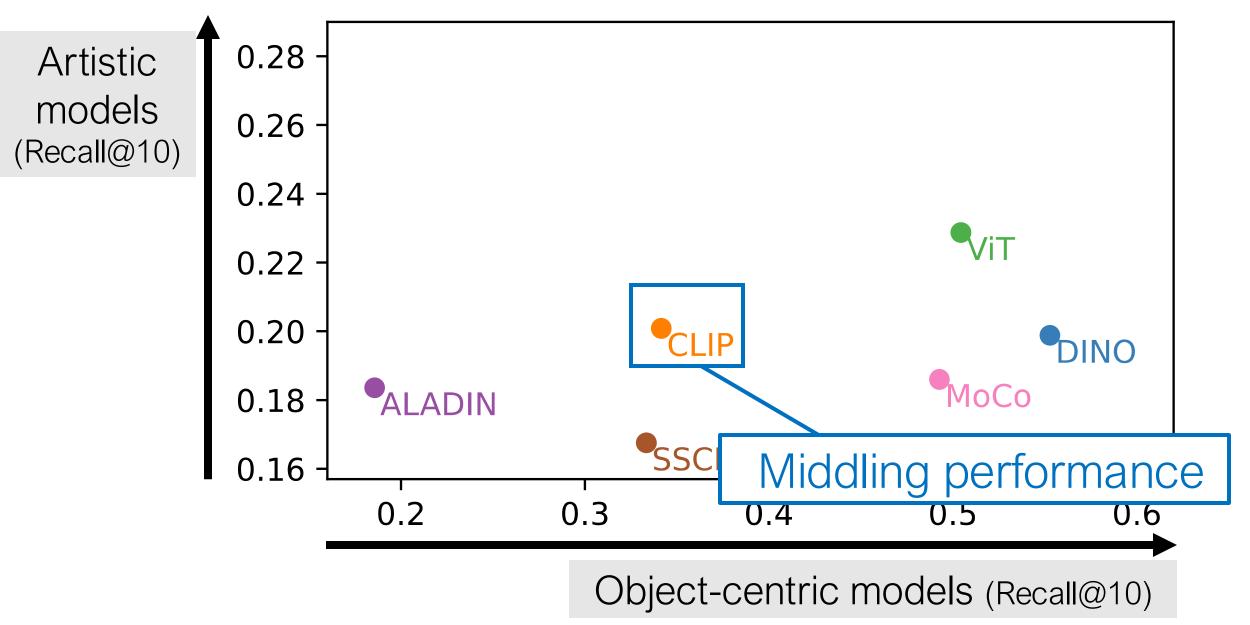


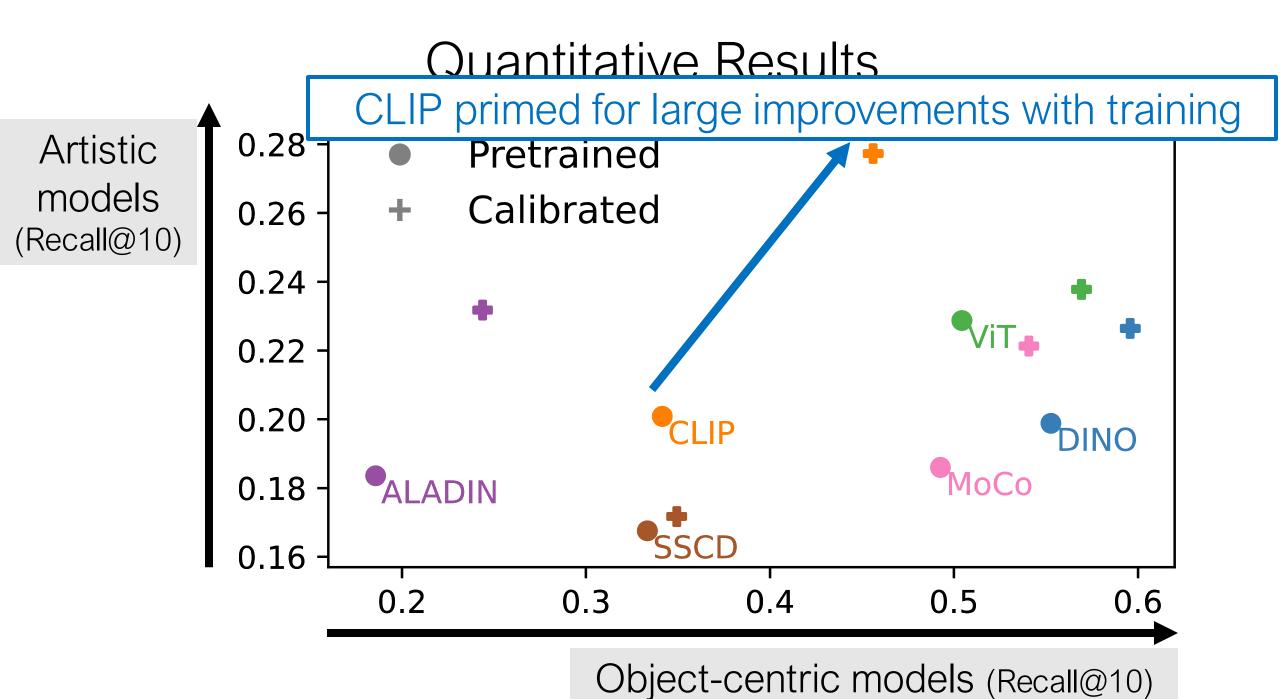
400M retrieval; chance = 2.5×10^{-7} %

Quantitative Results



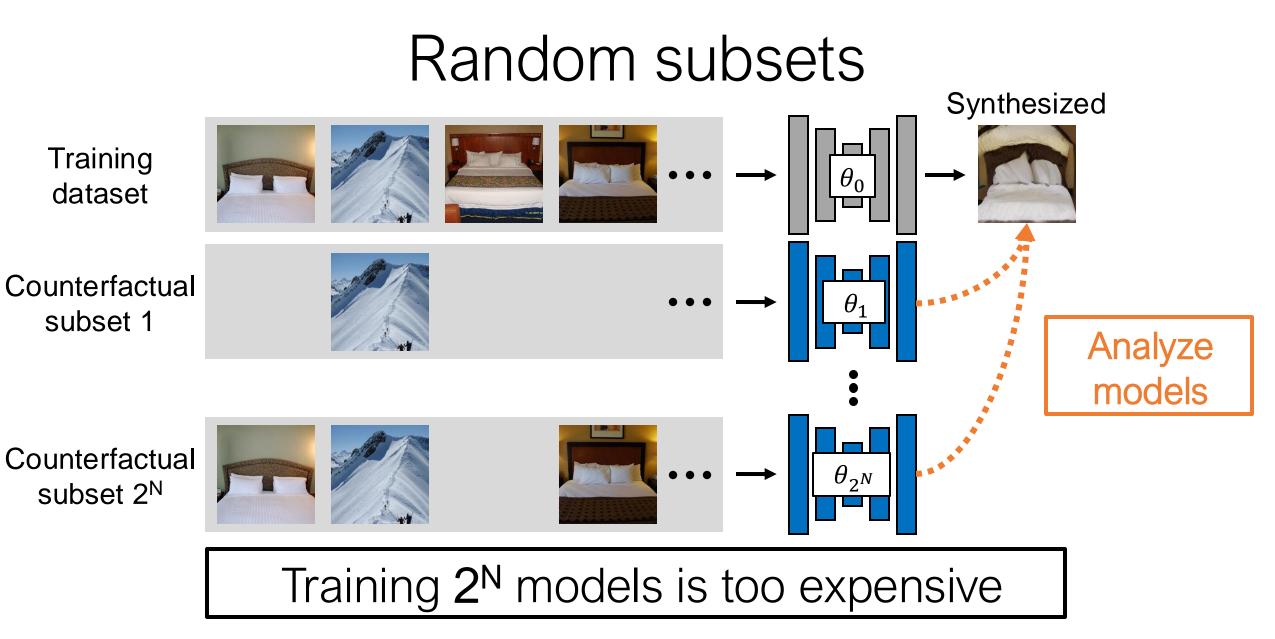
Quantitative Results



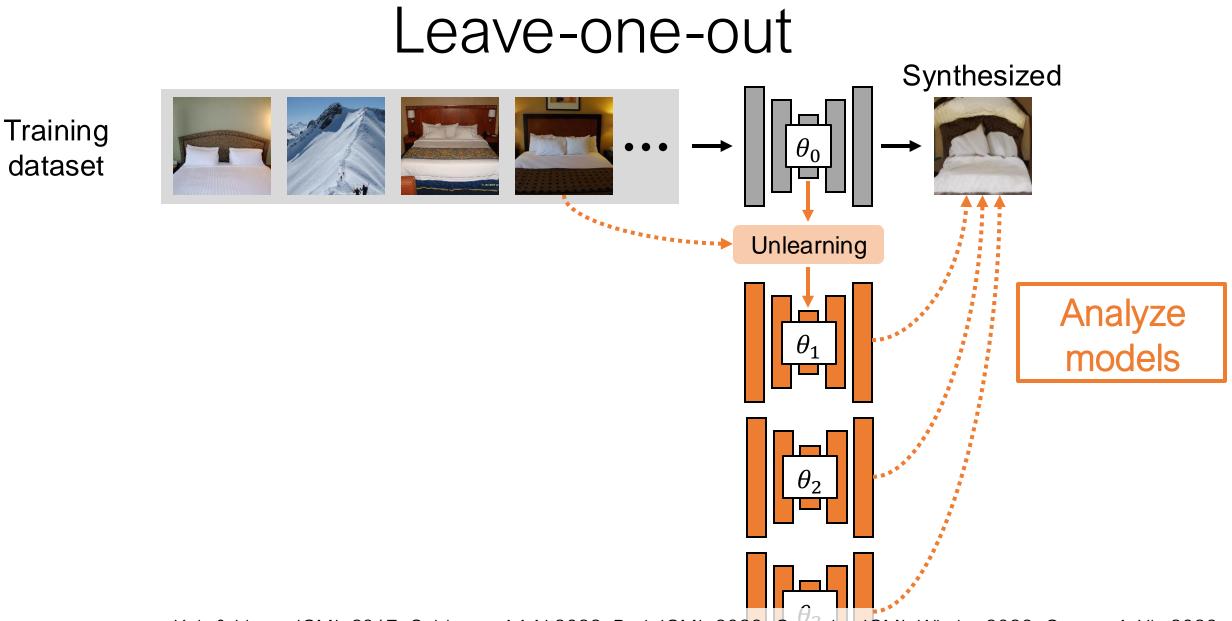


Limitations

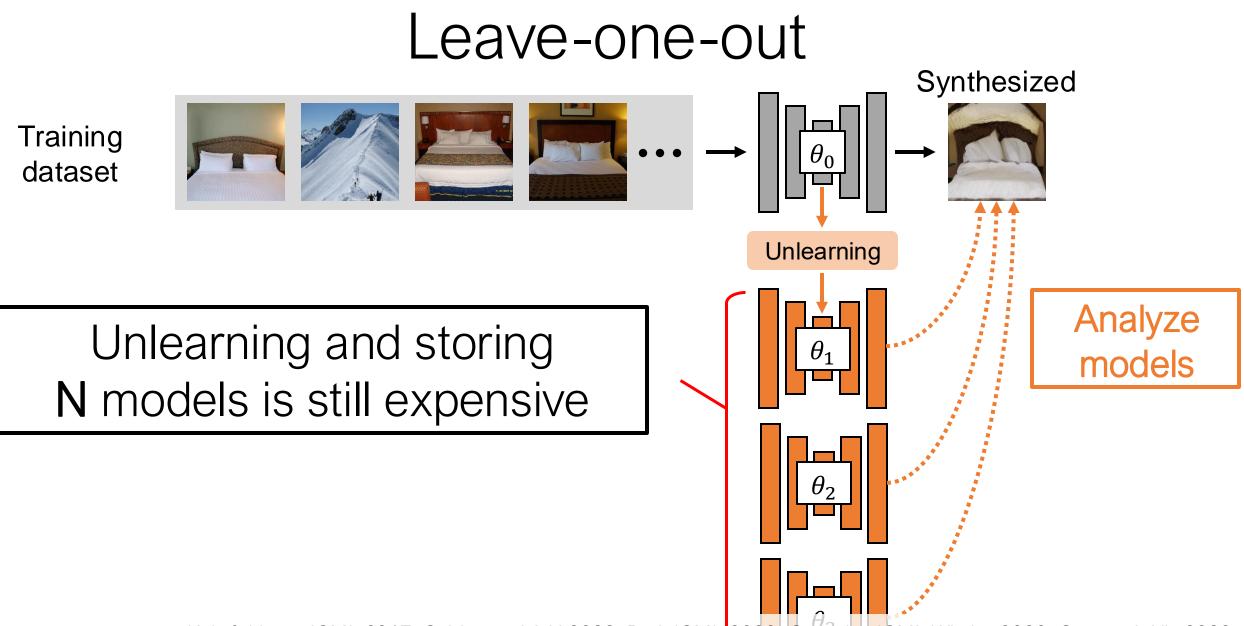
- Pretraining set is ignored
 - LAION-5B has influence on Custom Diffusion examples
- Prior work: "remove" instead of "add"
 - Shapley Value: landmark concepts in economics
 - [Shapley 1953; Feldman & Zhang 2020]
 - Train on random subsets; analyze population of models
 - Influence functions
 - [Koh & Liang 2017, Schioppa et al. 2022, Park et al. 2023, Georgiev et al. 2023]
 - Linear approximation
- Evaluating attribution with large training set is challenging!



c.f. Feldman & Zhang. What Neural Networks Memorize and Why. NeurIPS 2020.

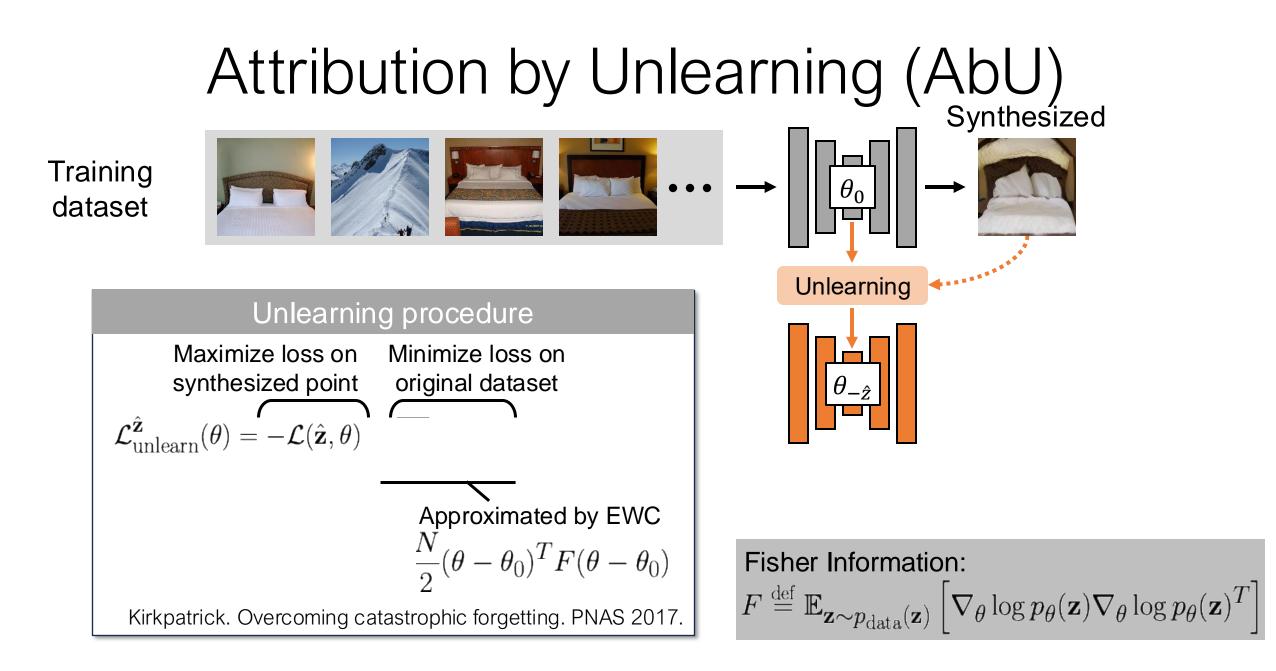


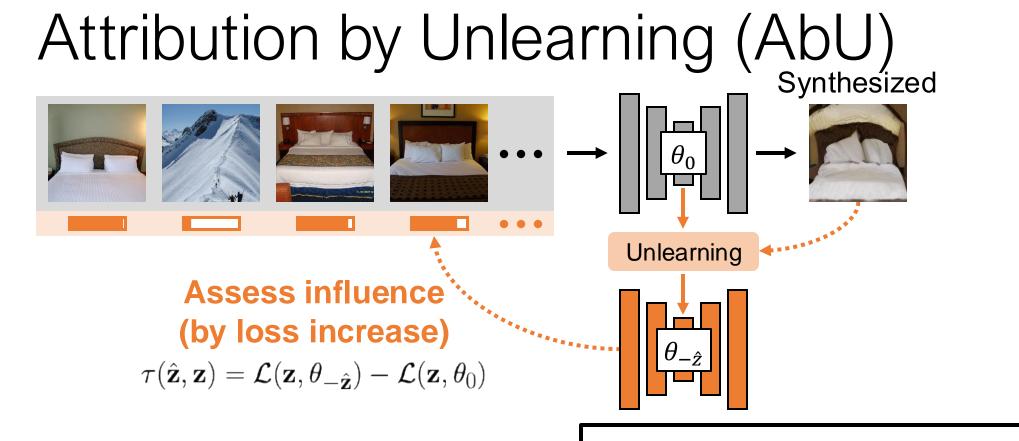
Koh & Liang. ICML 2017; Schioppa AAAI 2022; Park ICML 2023; Georgiev ICML Wkshp 2023; Grosse ArXiv 2023.



Koh & Liang. ICML 2017; Schioppa AAAI 2022; Park ICML 2023; Georgiev ICML Wkshp 2023; Grosse ArXiv 2023.

Change One Thing at a Time (Remove one Test Image)





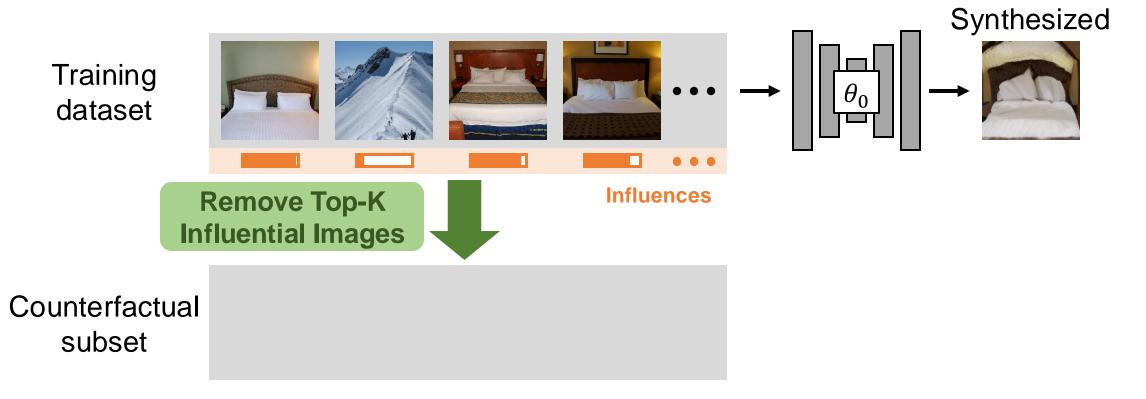
Training

dataset

Unlearning only once

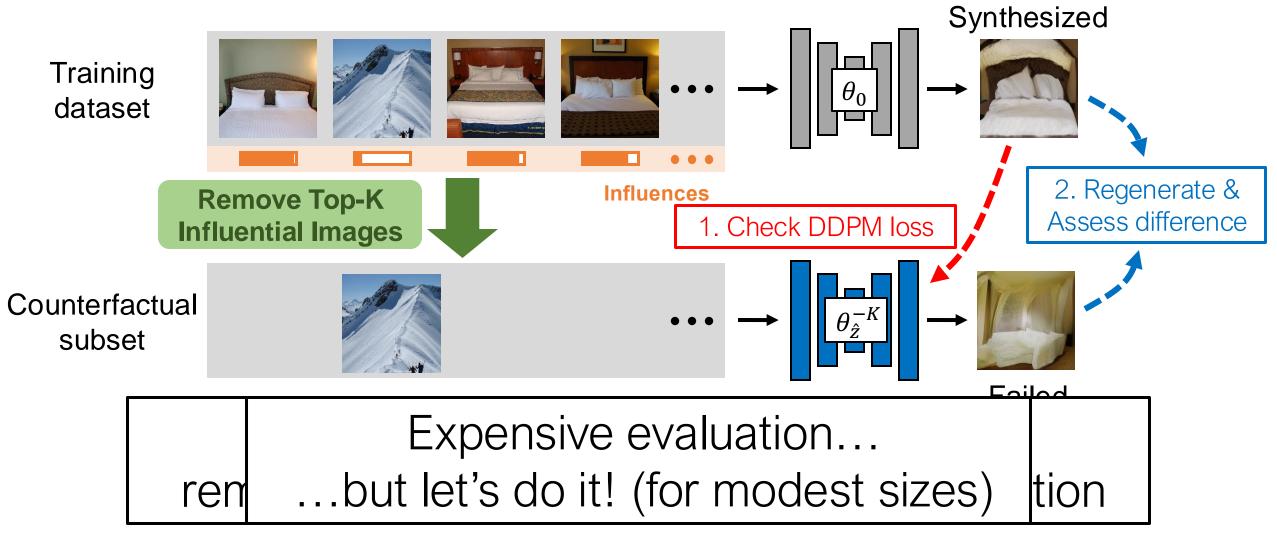
How do we evaluate attribution?

Counterfactual evaluation



c.f. K. Georgiev, et al. How Training Data Guides Diffusion Models. In ArXiv, 2023.

Counterfactual evaluation



c.f. K. Georgiev, et al. How Training Data Guides Diffusion Models. In ArXiv, 2023.



Attribution results

Counterfactual evaluation

c.f. K. Georgiev, et al. How Training Data Guides Diffusion Models. In ArXiv, 2023.

MS-COCO results

Remove K=500 (0.4% of dataset)







Counterfactual evaluation





"A man in a blue coat skiing through a snowy field."





Attribution results



"A small closed toilet in a cramped space."

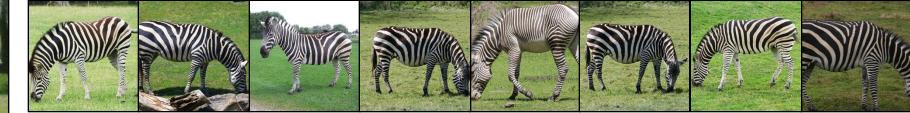




"A zebra all by itself in the green forest."

"A cat laying on clothes that are in a suitcase."









"A tennis player running to get to the ball."





Synthesized images

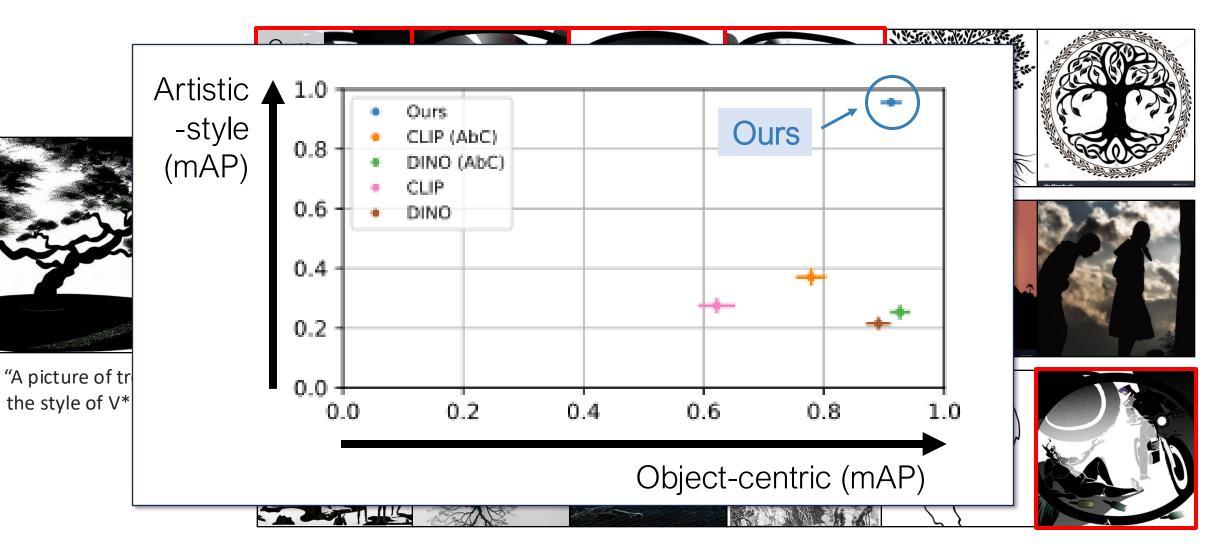
Our attribution results

Local attribution

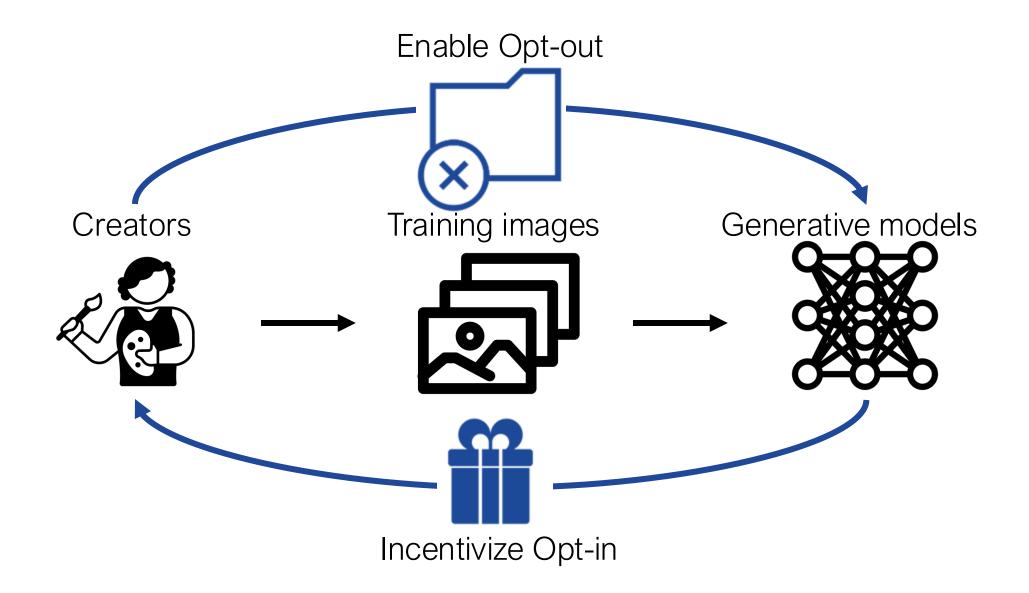


Attributed training images

Customized Model Benchmark



Data Ownership in Generative Models





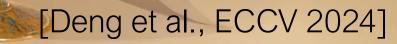
Human Creators



Recent Projects

FlashTex: Relightable Mesh Texturing





Robot-Human Co-painting

ICRA 2024 Best Paper on Human-Robot Interaction [Schaldenbrand et al., ICRA 2024]

Diffusion2GAN







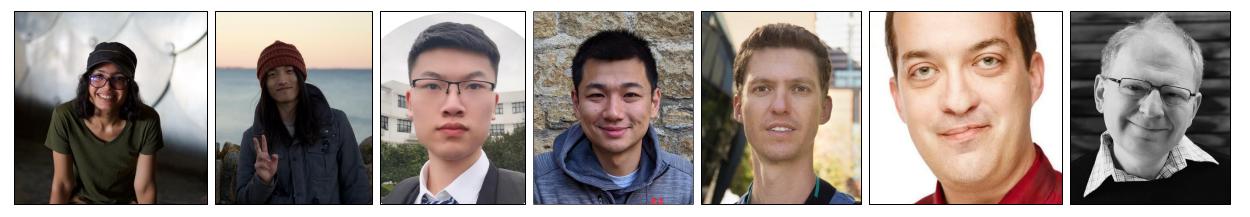
"Traditional gondolas lined up along the water, ready to transport visitors."

"Skiers enjoying the pristine slopes of the Swiss Alps on a sunny day."

"Russian Blue cat exploring a garden, surrounded by vibrant flowers."

Distilling Diffusion Models into Conditional GANs [Kang et al., ECCV 2024]

Students and Collaborators



Nupur Kumari

Sheng-Yu Wang Bingliang Zhang Richard Zhang

Eli Shechtman

Aaron Hertzmann

Alyosha Efros



Human Creators

