## How to use Glaze and Nightshade: A step by step guide.



Image: Zach Blas, The Doors ( 2019) Installation view, Edith-Russ-Haus for Media Art, Oldenburg, Germany. Courtesy of Edith-Russ-Haus for Media Art and the artist.

#### Why Use Cloaking for Artwork?

Cloaking protects your artwork from being scraped and used to train AI models without your consent. Tools like Glaze or Nightshade apply subtle alterations to an image that confuse AI training models while remaining nearly invisible to the human eye.

#### **How Cloaking Works**

Al models learn patterns and styles by analyzing thousands of images. Cloaking modifies the pixel-level data in ways that disrupt how Al perceives your work—making it harder for models to copy your style.

For humans: The image looks the same.

For AI: The image appears distorted or unreadable, preventing it from learning your artistic style accurately.

Why Artists Need Cloaking	What Cloaking DOESN'T Do	Cloaking Tools for Artists
Prevents AI from copying your artistic style Doesn't require legal action—protection is built into the image itself Keeps your artwork recognizable to human viewers	Doesn't remove your artwork from existing models (trained copies remain) Doesn't prevent screenshots or manual tracing of your work Doesn't stop AI from being trained on non-cloaked images of yours	<ul> <li>Al Glaze – Confuses Al training models while keeping images visually intact.</li> <li>Nightshade – Actively corrupts Al datasets, making models generate incorrect results.</li> <li>Watermarks &amp; metadata stripping – Prevents easy Al scraping, but less effective than cloaking.</li> </ul>

## Protect Your Artwork from AI

Glaze and Nightshade are both powerful tools for protecting art from AI scraping and unauthorized use in dataset training, but they serve slightly different purposes.

#### Glaze (Developed by the University of Chicago)

- Best for: Protecting the style of an artist's work from being mimicked by AI models.
- How it works: Adds subtle "cloaking" noise to an artwork that confuses AI training algorithms while keeping the image visually unchanged to human viewers.
- Ideal for: Artists who don't want their unique style replicated by AI models like Stable Diffusion or Midjourney.
- Pros:
  - Does not heavily distort images for human viewers.
  - Specifically targets AI training models.
- Cons:
  - Might need updates as AI models improve their resistance to cloaking.
  - Focuses mainly on style mimicry rather than full dataset poisoning.

#### Nightshade (Also from the University of Chicago)

- Best for: Actively poisoning AI datasets by making images introduce incorrect associations into AI models.
- How it works: Alters pixels in a way that forces AI models to misinterpret content (e.g., making them think a dog is a cat).
   Over time, this corrupts AI training data.
- Ideal for: Artists who want to damage AI models that scrape their work, making them unusable.
- Pros:
  - Stronger long-term protection.
  - Can make AI models unreliable if they ingest enough Nightshaded data.
- Cons:
  - More aggressive than Glaze—actively sabotages Al training rather than just cloaking.
  - Might distort images slightly more for human viewers.

#### Glaze CLOAKING (Developed by the University of Chicago)



## Non Glazed

#### Glazed :settings default/ slowest This image has good protection from AI scraping

Image Elaine Hoey Homo Mimeticus Installation View Solstice Arts Centre Photo by Jed Niezgoda

#### Nightshade CLOAKING (Also from the University of Chicago)



Non Nightshade



Nightshade :settings default/ slowest This image has good protection

# GLAZE

## Protect Your Artwork from AI with Glaze: A Step-by-Step Guide

### A practical guide for artists to safeguard their creative work online

What's is Glaze?

Al models scrape the internet, learning from public images—including your artwork. Glaze helps you fight back by confusing Al models while keeping your work visually intact for human viewers. This guide walks you through the Glaze process, step by step.

## What You'll Need (see computer/laptop specifications at the end of this document)

A computer (Mac or Windows) Make sure you are downloading the correct version for either Windows or Mac. A few digital artworks (PNG or JPEG) Glaze installed  $\rightarrow$  Download it here: <u>glaze.cs.uchicago.edu</u>

## Step 1: Install Glaze

Time: 5 minutes (internet dependent)

1 Go to Glaze's official site and download the latest version. Download size 2.50GB 2Unzip file and open the installer . Follow the on-screen instructions if necessary.

Once unzipped or installed, open Glaze.

## Step 2: Prepare Your Artwork

Time: 2 minutes

Before loading images into Glaze, make sure: They are PNG or JPEG format. The resolution is reasonable (under 10,000 x 10,000 pixels). The file is saved in RGB mode (not CMYK).

Tip: If your file is too large, resize it slightly to speed up processing.

	06/03/2025 09:21	PYD File
_uuid.pyd	06/03/2025 09:21	PYD File
2	06/03/2025 09:21	PNG File
base_library	06/03/2025 09:21	Compressed (zipp
🍯 Glaze 🧲	06/03/2025 09:21	Application
🗋 glaze-glaze.ui	06/03/2025 09:21	UI File
libcrypto-1_1.dll	06/03/2025 09:21	Application extens
libffi-7.dll	06/03/2025 09:21	Application extens
libopenblas64_v0.3.21-gcc_10_3_0.dll	06/03/2025 09:21	Application extens
libssl-1_1.dll	06/03/2025 09:21	Application extens

## Step 3: Load Your Artwork into Glaze

Time: 2 minutes

1 Open Glaze.

2 Click "Add Artwork" or drag and drop your image into the workspace.3 Your image should now appear in the preview panel.

If you're protecting multiple artworks, you can load them all at once.

#### Glaze - Protecting artists from invasive AI

#### 1. SELECT YOUR IMAGE(S) TO GLAZE



Select image(s) to Glaze

Clear All

#### 2. DEFINE GLAZE SETTINGS

#### Intensity

Magnitude of changes that will add to your art. Higher values can lead to more visible changes.

LOW	DEFAULT	HIGH

#### **Render Quality**

Duration spent glazing the art. Higher can leads to better protection but longer rendering time.

Faster (~1 mins)	DEFAULT (~2 mins)	Slower (~3 mins)	Slowest (~4 mins)
3. OUTPUT			
Save As	D:/glazed	llmages/	
		Run Gl	aze

Glaze succeed, glazed images saved at your output folder

GPU detected, Running on GPU.

×

GLAZE INTERFACE

## Step 4: Choose Your Protection Strength

Time: 3 minutes

Glaze lets you pick how much protection you want. More protection means more AI confusion, but can slightly alter the image. It takes time to find the right balance with your image. Testing is the best way to learn.

Level	Effect on Image	Effect on Al
Low	Almost no change	Weak protection
Medium	Subtle tweaks	Good protection
High	More distortion	Strongest protection

Recommended: Medium Protection for most cases. If AI keeps copying your work, try High Protection.

- 1 Adjust the Protection Strength slider.
- 2. Adjust Render quality, slowest setting gives best results, but takes longer to process.

## Step 5: Run Glaze & Process Your Image

Time: 5–15 minutes

1 Click "Process" to start Glazing your image.

2 The software will take a few minutes, depending on:

- Your computer speed (faster GPUs process quicker).
- Your image size (larger files take longer).

Tip: If the image looks too altered, try a lower protection level and reprocess.

## Step 6: Save & Export Your Protected Artwork

#### Time: 2 minutes

Click "Save" and choose a folder. You should set up a separate glazed image folder. This is an important step.
 Rename the file (e.g., MyArtwork\_Glazed.png) to keep it separate from the original.
 If you want multiple versions, go back and reprocess at different protection levels.

Tip: Always keep your original artwork separate from Glazed versions.

# NIGHTSHADE

## Protect Your Artwork from AI with Nightshade: A Step-by-Step Guide

A practical guide for artists to safeguard their creative work online

#### What is Nightshade?

Nightshade is a dataset poisoning tool developed by the University of Chicago's SAND Lab. Unlike Glaze, which cloaks images to confuse AI, Nightshade actively corrupts AI models by injecting invisible distortions into images. When AI models scrape and train on Nightshaded images, they mislearn concepts—causing them to generate inaccurate results.

Warning: Nightshade is a **proactive** tool, designed not just to defend against AI scraping but to actively **disrupt and corrupt** unauthorized AI model training—once AI models ingest poisoned images, they cannot be easily fixed. Use responsibly.

#### What You Need Before Using Nightshade

A computer with Windows 10/11 or macOS Nightshade installed  $\rightarrow$  Download it here Digital artwork (PNG/JPEG format)

🔤 base_library	06/03/2025 11:20	Compressed (zipp	1,007 KB	
🗋 glaze.ui	06/03/2025 11:20	UI File	4 KB	
libcrypto-1_1.dll	06/03/2025 11:20	Application extens	3,320 KB	
libffi-7.dll	06/03/2025 11:20	Application extens	33 KB	
libopenblas64_v0.3.21-gcc_10_3_0.dll	06/03/2025 11:20	Application extens	35,036 KB	
libssl-1_1.dll	06/03/2025 11:20	Application extens	674 KB	
S msvcp140.dll	06/03/2025 11:20	Application extens	560 KB	
🚯 Nightshade	06/03/2025 11:20	Application	34,618 KB	
pyexpat.pyd	06/03/2025 11:20	PYD File	185 KB	
python3.dll	06/03/2025 11:20	Application extens	58 KB	
python39.dll	06/03/2025 11:20	Application extens	4,354 KB	
select.pyd	06/03/2025 11:20	PYD File	27 KB	

**STEP 1** Go to <u>https://nightshade.cs.uchicago.edu/</u> Download the latest version for your system Unzip and install if required. Some systems don't need full installation but work immediately .

#### Nightshade - Proactive Copyright Protection

#### 1. SELECT YOUR IMAGE(S) TO ADD NIGHTSHADE (OPTIONAL) SELECT POISON TAG



Clear All

#### 2. DEFINE NIGHTSHADE SETTINGS

#### Intensity

Magnitude of changes that will add to your image. Higher values can lead to leads to stronger poison but more visible changes.

Select image(s).



#### **Render Quality**

Duration spent rendering the nightshade. Higher can leads to stronger poison but longer rendering time.

Faster (5 mins)	Medium (~10 mins)	Slower (~15 mins)	Slowest (~20 mins)
3. OUTPUT			
Save As	. Not Select	ted	
	Run N	lightshade	

What is a single word describing the key content of this image? We will auto-detect it and suggest a single word "tag" below. Please overwrite if incorrect or too general. Tag should be in metadata or alt-text describing the image when posted online. This field is only customizable if you Shade a single image (no batching).

Curr	ent	Tag:	

<u>g:</u>

Welcome to Nightshade 1.0!

To apply nightshade to your image, follow the three step process on the left panel.

Resource loaded successfully.

Nightshade Interface

\_

## Step 2: Prepare Your Artwork

Time: 2 minutes

Before loading images into Nightshade make sure: They are PNG or JPEG format. The resolution is reasonable (under 10,000 x 10,000 pixels). The file is saved in RGB mode (not CMYK).

Tip: If your file is too large, resize it slightly to speed up processing.

## Step 3: Load Your Artwork

Time: 2 minutes

1 Open Nightshade.

2 Click "Add Artwork" or drag & drop an image.

3 Type one one to describe image, ie, painting, sculpture etc.

## Step 3: Choose Poisoning Strength

#### Time: 3 minutes

Nightshade lets you pick how aggressively you want to poison Al models. Higher settings cause greater Al corruption but may introduce subtle distortions.

#### Recommended Setting: Medium .

High for strong AI disruption without noticeable visual changes. If you want extreme AI damage, go for "Extreme," but check if the image is still acceptable to human viewers.

Strength Level	Effect on Al	Effect on Image
Low	Minor corruption	Nearly no visible change
Medium	Moderate corruption	Slight, barely visible alterations
High	Heavy corruption	More noticeable alterations
Extreme	Maximum damage	Some visible distortion, but Al impact is severe

# Step 4: Run Nightshade & Poison the Image

Time: 5–20 minutes (varies by PC speed)

1 Click "Process" to start Nightshading your artwork.

2 The tool will embed invisible pixel-level changes that corrupt AI learning.

3 Processing time depends on:

- Computer speed (faster GPUs process quicker)
- Image size (larger files take longer)

## Step 6: Save & Export Your Protected Artwork

Time: 2 minutes

 Click "Save" and choose a folder. You should set up a separate Nightshade image folder. This is an important step.
 Rename the file (e.g., MyArtwork\_Nighsade png) to keep it separate from the original.
 If you want multiple versions, go back and reprocess at different protection levels.

Tip: Always keep your original artwork separate from Nightshade versions.

## **ADDITIONAL INFORMATION AND RESOURCES**

#### **Glaze System Requirements**

Glaze is designed to run on standard consumer laptops and desktops, but having a more powerful machine will speed up processing. Here's what you need:

#### Minimum Requirements (It Will Work, But Slow)

- **Operating System**: Windows 10/11 (64-bit) or macOS (Intel or Apple Silicon)
- Processor (CPU): Intel i5 (8th gen or later) / AMD Ryzen 5 or Apple M1
- Memory (RAM): 8GB
- Graphics Card (GPU): Integrated graphics (Intel UHD, AMD Vega, or Apple M1 GPU)
- Storage: 1GB free space
- Processing Speed: 5-20 minutes per image (slower on older machines)

#### **Recommended for Faster Processing**

- Processor (CPU): Intel i7/i9 (10th gen or later) / AMD Ryzen 7/9 or Apple M1 Pro/M2
- Memory (RAM): 16GB or more
- Graphics Card (GPU):
  - NVIDIA GTX 1650 or better (RTX 3060+ ideal)
  - AMD Radeon RX 5000 series or better
  - Apple M1 Pro / M2 or higher
- Storage: SSD with at least 10GB free
- Processing Speed: 1-5 minutes per image

#### Nightshade System Requirements

Nightshade requires more power than Glaze because it actively corrupts Al models instead of just cloaking images.

- Windows: Windows 10/11 (64-bit)
- Mac: macOS (Apple Silicon or Intel)
- CPU: Intel i7 / AMD Ryzen 7+ (recommended)
- RAM: 16GB minimum (32GB recommended for batch processing)
- GPU:
  - Dedicated NVIDIA (RTX 3060+ recommended)
  - Apple M1 Pro/M2 Pro or better
  - Integrated graphics may struggle
- Storage: 4GB+ free space (Nightshade downloads additional machine learning files)
- Processing Time: 10–30 minutes per image (depends on settings & PC power)

#### Mac vs. Windows?

- Macs with M1/M2 chips work well because of Apple's optimized GPU.
- Windows PCs with a dedicated NVIDIA GPU (RTX 3060 or better) will be much faster than those with only integrated graphics.

#### Can It Run on a Weak Laptop?

Yes, but expect longer processing times (10-30 minutes per image). If you only process a few artworks occasionally, it's manageable.

#### How to Know if Your Artwork is Being Scraped & Used by AI

AI models scrape the internet for publicly available images to train on. If your artwork is online—especially on platforms like Instagram, ArtStation, DeviantArt, Pinterest, or personal websites—it could be in an AI training dataset. Here's how to check if your work has been scraped and used by AI models:

#### Step 1: Check If Your Art Was Used in AI Training Datasets

The best tool for this is <u>Have I Been Trained</u> by Spawning.

How to Use It: 1 Go to https://haveibeentrained.com/

Upload an image of your artwork OR search by your name.

It will search against LAION-5B, a massive dataset used to train AI models like Stable Diffusion, MidJourney, and DALL-E. If your artwork appears, it was likely scraped and used for AI training.

If you find your work: You can request an opt-out (but this only works for future datasets—not models already trained).

#### Step 2: Reverse Image Search Your Artwork

Al-generated images sometimes mimic original artworks closely enough to spot similarities. You can check if your art (or similar images) appear elsewhere.

How to Reverse Search Your Images

Option 1: Google Reverse Image Search (Best for General Use)

1 Go to <u>Google Images</u>

2 Click the camera icon 📷 (Search by image).

3 Upload your artwork OR paste its URL.

4 Google will show where your image appears online—including AI art platforms or unauthorized use.

Option 2: TinEye (Best for Finding Exact Copies)

Visit <u>https://tineve.com/</u>
 Upload your artwork OR enter a URL.
 3TinEye will find exact or modified versions of your image online.

#### Step 3: Check AI Art Generators for Your Style

Some AI-generated images look suspiciously like existing artists' work. You can test this by:

- Searching Al-generated art platforms (e.g., ArtStation, DeviantArt, MidJourney Gallery).
- Typing your name or art style into Al prompt-sharing websites (like Lexica or CivitAl).
- Looking for Al-generated art that closely resembles your work style, composition, or color palettes.

Lexica (for Stable Diffusion prompts)  $\rightarrow$ <u>https://lexica.art/</u> CivitAl (Al models and styles)  $\rightarrow$ <u>https://civitai.com/</u>

# Final Thought: The Best Protection is Preemptive

Al scraping happens automatically—you might not know until Al art using your style appears.

Use Glaze/Nightshade before posting any new work online.

Regularly reverse search your images and monitor AI art communities.