Best Practices Guide
Digimarc for Digital Images

Contact

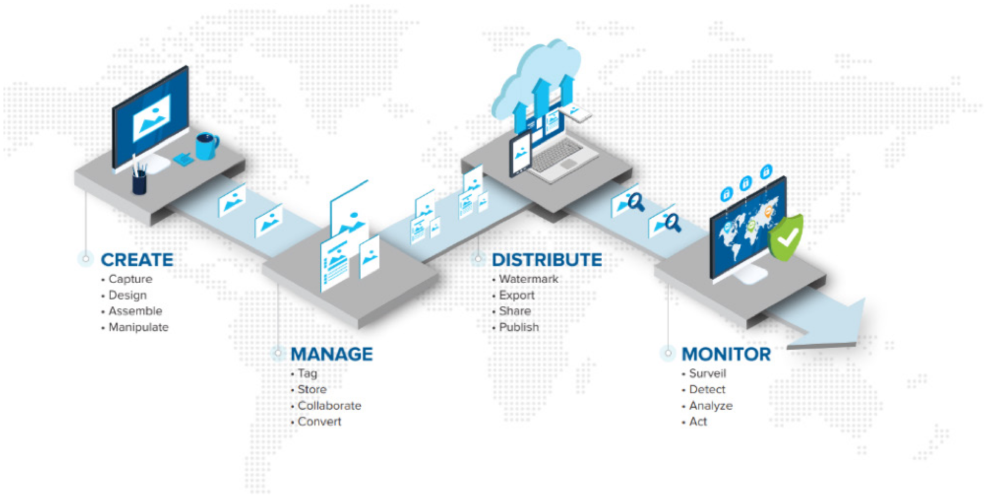
For project support contact: info@digimarc.com

INTRODUCTION

Digimarc for Digital Images is a powerful digital image watermarking solution enabling brands, rights holders and digital-asset managers to better manage the use of images and other assets throughout the supply chain and across the public internet. Combining imperceptible identifiers with complementary crawl services, enterprise customers benefit from greater insight into where brand assets are being used.

This guide will outline how to effectively work with Digimarc for Digital Images so it remains effective through file compression, format changes, editing, cropping and other manipulations.

The Image Journey



Digital Watermark Strength

We add digital watermarks that are mostly imperceptible to the human eye and persist with your image regardless of what happens to it or where it lives. Durability and visibility of a digital watermark are directly related. An increase in watermark durability increases the strength—and may, in some cases, increase the visibility of the watermark.

What Types Of Images Can Be Digitally Watermarked?

Virtually all images can be digitally watermarked; however, some types will yield better results than others, see pg. 4 for details.

What Types Of Images Cannot Be Digitally Watermarked?

Digital image watermarking uses color space (a specific organization of colors) within an image's pixels to apply its payload. Some image types contain no color space, so must be converted prior to applying a watermark.

Bitmap Vs. Vector

Vector or line-art images are not supported, but can be converted to a raster or a bitmapped format prior to enhancing.

Very Small Images

It is not recommended that Digimarc for Digital Images watermarks be applied to images smaller than 256 x 256 pixels.

Greyscale: Single Channel Vs. Truecolor Monochrome

Grayscale image compatibility varies based on the format of the image. Many grayscale images are truecolor monochrome, meaning the image has color space into which our watermark payloads can be applied. However, many formats, JPEG included, tend not to store the actual color values in each pixel; instead, they create a palette of shades from the original image. "Palettized" images are not supported.

True Black And White

True black and white images are not supported. A true black and white image, also called 1-bit color, is common in faxes, scans, and some kinds of print images. These images contain no color space or shades of grey into which a watermark payload can be applied.

Color Space

The enhancing process places a digital watermark in either the chrominance or luminance component of an image. Our enhancement tools provide you with two options in order to optimize enhancement based on the color space of your image. A Chroma watermark is generally preferable for color images. A Luminance (or "Classic" in Photoshop) watermark is ideal for grayscale images.

All Digimarc for Digital Images enhancing software defaults to the Chroma digital watermarking mode. The user can configure the enhancement tool to apply Luminance digital watermarks at any time, if desired.

When To Switch From Chroma To Luminance Watermarks

Digimarc recommends Chroma watermarks for all full-color images. The improved visual quality and durability, especially after scaling and JPEG compression, are significantly better. In most instances, the default Chroma setting will yield the best results. However, there are some situations where you may want to switch to the Luminance watermark, such as images with mostly or entirely flat colors; for example, a pair of sunglasses on a white background.

Depending on the type of images you are watermarking, you may find the visual artifacts of the Chroma watermarking mode to be more visible than the Luminance mode. Your embedder software has the ability to switch between modes based on user preferences.

File Formats

A digital watermark is woven into and carried by the pixels that make up an image and survives even when the image is converted from one file format to another. The file formats into which you can add a Digimarc watermark vary for each of our enhancement tools. Please see pg. 8-9 “Enhancing Software Comparison” for details.

Image Variations/Randomness

Digital watermarks are most effective and least perceptible when applied to images that are not composed, mostly or entirely, of a single flat color. Images that contain some degree of variation or randomness will yield better results.

We recommend using a Chroma watermark to enhance normal, high color/variation images; for example, a full-color, staged image of a handbag on a model. Luminance watermarks work better when enhancing mostly or entirely flat-color images; for example, a pair of dark running shoes against a white background. Note that watermarks may be slightly more visible on images that are mostly or entirely composed of a single flat color.

Use the Chroma watermark when embedding normal high-color images

Use a Luminance watermark when enhancing images with low color variation

Image Size Recommendations

To add a digital watermark into an image, and be able to reliably read it later, digital watermarks require a minimum number of pixels with which to work.

Digimarc recommends a minimum size of 256 x 256 pixels. There is no upper limit on image size for digital watermarking (see pg. 7, “Survivability of a watermark” for best practices).

Image Workflow Overview

As you prepare an image for distribution, you may take it through a number of different transformations. You might save the image in multiple resolutions, and perform a number of edits as outlined on pg. 7 in the “Survivability of a watermark” section, such as scaling, cropping, rotation, compression, etc.

Where And When In Your Workflow To Digitally Watermark Images

Whether you are enhancing images individually or processing at scale through a Digital Asset Management (DAM) platform, we recommended the following workflow sequence for digital watermarking:

1 Make all necessary modifications to your image until it has the desired final appearance.

2 Save a final unenhanced copy (you cannot apply a watermark in an image that already contains one).

3 Apply the digital watermark.

4 Save the final image format.

5 Publish the image.

Setting Digital Watermark Attributes

When you’re ready to apply a digital watermark, you will need to set a number of parameters for the information the watermark will contain:

- **Enterprise ID** - A unique whole number assigned to your company that identifies you with Digimarc as an enterprise account holder. This integer forms the basis of your watermark payloads.
- **Image or Transaction ID** (Optional) - A whole integer up to 32 bit (maximum integer value of 4,294,967,295) that will be contained within the image and readable within the payload. You can use this field to reference a unique identifier. For example, distinct Transaction IDs can be assigned to different partners or sales/internal channels.
- **PIN -** A Personal Identification Number provided to you by Digimarc for use in validating your Digimarc ID when you key your Enterprise ID into the enhancement software.
- **Copyright Year** (Optional) - This can be a single year or range between two years, i.e. 2005-2010.
- **Restricted Use** (Optional) - This indicates that the image is subject to restricted use.
- **Do Not Copy** (Optional) - This indicates that the image should not be copied without permission.
- **Adult Content** (Optional) - This indicates the image contains adult content.

Using The ‘Watermark Durability’ Setting

A default watermark intensity setting of seven (7) is common across all of our enhancement software, though it can be altered within the configuration of each tool. The setting provides control between digital watermark robustness and visibility. However, this setting is by no means a “one size fits all” option.

The setting you choose depends on the intended use of the image and on the balance you want between watermark robustness versus visibility. For example, it may be quite acceptable to use a higher watermark durability setting with JPEG images posted on a website. The higher durability helps to assure the persistence of the digital watermark, and the increased visibility will most likely not be noticeable with medium-resolution JPEG images.

Digimarc recommends that you try various digital watermark durability settings as part of your testing process to see which setting works best for your images. The goal is to find the balance between visibility and durability that meets your needs.

Image Compression

A digital watermark, in most cases, will survive image compression, but the survival is dependent on several factors. Lossless compression, such as with PNG, LZW, StuffIt™ and .ZIP formats, does not affect the survival of a digital watermark because no image data is sacrificed to create the compressed version. Lossy compression methods such as JPEG or indexed color formats actually remove image data in order to decrease file size; this can affect a digital watermark’s durability. The following factors influence the impact of lossy compression:

- **Level of image compression** - Lossy compression degrades the image to some extent, though this is dependent upon the quality setting chosen when saving in compressed format; most digital watermarks will survive as long as a moderate level of compression is used (see “Survivability of a watermark” on pg. 7).
- **Visibility/durability setting used when embedding a digital watermark** - The higher the durability setting, the better the chances the digital watermark will survive compression. The visual quality of compressed images is somewhat compromised, so often a higher watermark durability setting is less noticeable.
- **Image size** - The greater the number of pixels in the image, the more the digital watermark can be repeated throughout it; the recommended minimum image size that is 256 x 256 pixels.
- **Randomness of image data:** See “Image variations/randomness” on pg. 4.

DPI Settings

When digitally watermarking an image for use on the Internet, resample the image to the proper DPI (Dots Per Inch) setting for this medium (either 72 or 100 DPI) before you add the digital watermark. Correctly matching the digital watermark’s DPI setting to the image’s final resolution will optimize the durability of your embedded information.

Resampling Images

In some situations, you may wish to have multiple copies of an image at different sizes. For example, a small preview image is often used to link to a larger image for viewing.

This means conducting more digital watermarking operations than if you enhanced only once prior to resampling, but your digital watermarks will be much more durable using this approach.

When you are working with an image that you will be resampling to multiple sizes, always resample before embedding a digital watermark.

Survivability Of A Watermark

The factors that affect the durability of a watermark directly influence survivability of watermarks; image variation, watermark durability settings and lossy compression. Survivability results will vary.

Scaling

The original digitally watermarked image can generally survive being resized. Chroma mode watermarking typically survives being sized up to 200% or resized down to 25% of the original size, and in many cases even lower. Luminance (or “Classic”) mode watermarked images should be readable after being sized up to 200% or scaled down to 60% of the original.

Cropping

Because the digital watermark is repeated throughout the image, removing portions of the image by cropping will generally not affect the watermark, provided that the final image meets or exceeds the minimum size discussed above.

⚠ ***If the image is cropped to less than 256 x 256 pixels, the watermark may not survive.***

Rotation

The digital watermark remains intact when the image is rotated by any number of degrees.

Effects Filters

The general rule is that the survival of the digital watermark is linked to the visual quality of the image. Some effects filters significantly distort pixels in the image, which has a direct impact on the strength of the watermark. If an effects filter is applied at an extreme setting (particularly distortion-type effects), then it is possible the digital watermark may no longer be readable from the image.

Working With Layered Images

When working with an image that contains multiple layers, watermarking the image in that state would apply the digital watermark only to the selected layer, rather than to the entire image.

We recommend saving a separate copy of the layered file, then flattening the image before applying the watermark.

Combining Digital Watermarks With Visual Watermarks

If you decide to use a visual watermark, be sure to apply the Digimarc for Digital Images watermark last. If done in the reverse order, the visual watermark could possibly disrupt a significant number of pixels, changing the image drastically and impacting the Digimarc for Digital Images watermark.

Enhancement Tool Side-By-Side Comparison

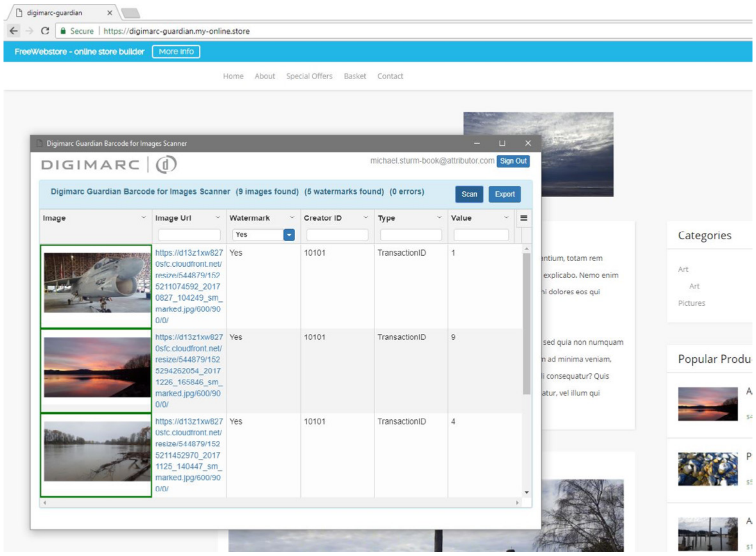
Enhancement Software	Intended Users	Features and Benefits	Requirements	Implementation Options	Image File Types Supported
Docker Image On-Premise API	Customer or integrator requiring the flexibility of the SDK without the C++ or image library expertise Customers with a distributed system running over a network	Includes image library Runs as a self-contained, light-weight webserver, on any customer machine Exposes simple image-based read and embed functions over REST API Enhances and reads images	Ability to run a Docker image on a local network. Ability to make REST calls over HTTP	System-level integration. Any local, data-center or cloud machine that supports Docker. Access is via HTTP REST interface, enabling access from virtually any client language	JPEG, PNG, TIFF, WEbP, BMP
C++ SDK	Customer or integrator requiring highest performance (Implementation requires the customer have an existing standalone application for processing image data, as well as C++ and image library expertise)	Compiles into your standalone application, resulting in top performance Uses your own image processing library for most flexibility Enhances and reads images	Requires expertise in C++ Image processing experience is recommended as access to raw pixel data via image processing library is required	Application-level integration C++ on Windows 8, Windows 10, Ubuntu 14, Ubuntu 16 and CentOS7	Grayscale, BGR, RGB, LAB, ARGB, RGBA, BGRA, CMYK, CMYK Inverted

Enhancement Software	Intended Users	Features and Benefits	Requirements	Implementation Options	Image File Types Supported
Digital Asset Management (DAM) Platform	Customer who currently uses a DAM platform to manage their digital-image asset libraries and wants to enhance images through this system	Seamless, speedy activation of image-enhancement workflow through an existing, trusted provider Ties specific DAM user information into the watermark for additional tracing purposes. Enhances images	DAM platform must have integration license agreement with Digimarc in order to perform work; ask your salesperson or relationship manager for more information, or suggest to your DAM that they integrate	Partner-level integration (Limited only by the DAM workflows that you and your provider have established)	Predicated on the enhancement tool that the DAM platform has integrated
Adobe PhotoShop® CC	A good choice for customers with low image enhancement volumes, or an in house photography team who manage every aspect of the image work-flow from creation to deployment. Also a good tool which can supplement automated work-flows	Workflow-level integration. A useful tool for testing, design, and evaluation, or where workflow does not involve other systems or applications. Enhances and reads images	Adobe Photoshop Versions CC2015 and above	Local machine with Adobe Photoshop CC	CMYK or RGB Images in 8 Bit Mode

Authentication & Validation Tools

Chrome Browser Watermark Reader

Browser-based reading tools allow for the reading of watermarks within a selected website. Once installed, users can initiate a scan by opening up the reader window, configuring their search settings and pressing the “scan” button. All images on the given page are scanned and read for watermarks and the specific payload information provided in the reader window. The results are exportable to CSV. Each installation is specific to a Digimarc for Digital Images Enterprise ID; only users with access to an organization’s Enterprise ID will be able to read that organization’s watermarks.

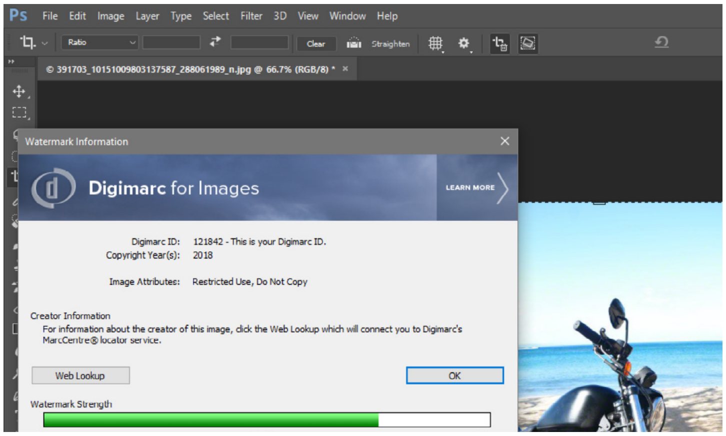

digimarc-guardian
Secure | https://digimarc-guardian.my-online.store
FreeWebstore - online store builder
More info
Home
About
Special Offers
Basket
Contact
Digimarc Guardian Barcode for Images Scanner
DIGIMARC
michael.sturm-book@attributor.com
Sign Out
Scan
Export
Categories
Art
Art
Pictures
Popular Produ

Digimarc Guardian Barcode for Images Scanner (9 images found) (5 watermarks found) (0 errors)

Image	Image Url	Watermark	Creator ID	Type	Value
		Yes			
	https://d13z1xw8270sfc.cloudfront.net/resize/544879/1525211074592_20170827_104249_sm_marked.jpg/600/900/0/	Yes	10101	TransactionID	1
	https://d13z1xw8270sfc.cloudfront.net/resize/544879/1525294262054_20171226_165846_sm_marked.jpg/600/900/0/	Yes	10101	TransactionID	9
	https://d13z1xw8270sfc.cloudfront.net/resize/544879/1525211452970_20171125_140447_sm_marked.jpg/600/900/0/	Yes	10101	TransactionID	4

Reading Watermarks With Photoshop

Watermarked files can be read within Photoshop. Users with the Digimarc for Digital Images Plug-in for Adobe Photoshop properly installed can select “read watermark” from the filters menu to verify an image for a watermark. All available payload information appears within the Photoshop reading window.



© 391703_10151009803137587_288061989_n.jpg @ 66.7% (RGB/8) *

Watermark Information

Digimarc ID: 121842 - This is your Digimarc ID.
Copyright Year(s): 2018

Image Attributes: Restricted Use, Do Not Copy

Creator Information
For information about the creator of this image, click the Web Lookup which will connect you to Digimarc's MarcCentre® locator service.

Watermark Strength

API-Based Watermark Reading

Customers using the on-premise API to enhance images can read images from a URL using the API. If an image is hosted online and is accessible from your API, POST the URL to the /api/read endpoint. The URL of the image to be read is passed in via a JSON data structure in the message body. The image is fetched from its location and then read for watermarks. The results are returned as JSON in the response body.

After an image file has been uploaded, the image can be read for watermarks using the POST method on the /files/{identifier}/read endpoint.

The results of the watermark reading will be returned as a JSON object in the response body.

Web Surveillance

Web Crawling Powered By Phishlabs

Digimarc for Digital Images enterprise customers benefit from a dedicated crawling service powered by Digimarc's longtime business partner PhishLabs. The crawl service extends your reach, supplementing your existing image-search processes. It is limited to crawlable, static URLs.

Customer And Partner Driven Web Surveillance

While many of our customers leverage our crawling services, powered by PhishLabs, we understand other customers may have existing relationships with other third-party web-surveillance companies who search the web for their image assets. We are always open to partnering with new web-surveillance organizations who can integrate our watermark reading technology to complement your existing services. Please reach out to your salesperson or relationship manager if this is of interest.

Contact Us

If you have any questions please contact us via *info@digimarc.com*