Watermarking Basics

Unique

Watermarking is most effective as a preventative and detective measure against image leaks when it crafted to be as unique as possible to each viewer or holder of an image file.

- A watermark should include the name of the viewer or recipient of the file whenever possible.
- If a name is not feasible due to multiple viewers of the same file simultaneously, an identifier such as a meeting time/place and company name, or any other combination of information that will narrow the potential leak to the most targeted audience and timeframe can be used.
- If the same file is being distributed to multiple individuals or multiple companies, or presented in multiple meetings, the watermark should be changed for each use/recipient to ensure this targeting is possible.
- If content is being viewed remotely by multiple viewers simultaneously, a viewing platform with an endpoint watermarking capability should be used to present content, but should not be relied upon as a sole watermark for the content unless the coverage has been determined sufficient to prevent meaningful unwatermarked crops of content from being captured.

Thorough

A watermark should intersect the portions of an image that are most critical to protect.

- A watermark should tile or wrap across an image in a density that ensures any significant IP material in the image will be intersected by a portion of the watermark.
- The vulnerability of a corner or edge watermark to cropping may be obvious, but a watermark struck through the center of an image may be equally flawed in its ability to protect, if sensitive IP falls outside the covered area.
- For complex files that include images in multiple scales, watermarking may need to be applied in different sizes and densities to adequately cover each scale.

Traceable

While the deterrent effect of a noticeable watermark on content viewers and receivers is valuable, even more valuable is your ability to trace a leaked image to its source using your watermark.

- A watermark should offer enough opacity and contrast in relation to the surrounding content to allow it to be discernable across all critical areas. An opacity of 15 to 25% is sufficient for most content but attention should be paid to visibility in each instance.
- If a file is being presented or distributed to multiple viewers/holders, any text characters used repeatedly in the watermark (for example, the word “meeting”) should be wrapped or tiled along with unique words or characters (for example, “Sept 3”, “Company A”, “Contact B”) to ensure their placement on the image is unique in each file version.
- Test the traceability of a watermark in a number of resolution scenarios, such as cropped screenshots and cell phone photos of monitors, to ensure your opacity and placement is sufficient before sending.
- Retain a record of distributed watermarks for each file, and the full watermarked version of each, for future investigative comparisons, should a leak occur.

CDSA
Content Delivery & Security Association