COSIG
Collection of Open
Science Integrity Guides

Software for image forensics

Last updated: 7 February 2025

Publication integrity issues often arise from image integrity issues. Performing image forensics is often very useful for taking part in post-publication peer review, especially in fields that frequently use images in scientific articles (e.g., biomedicine).

While many image integrity issues can be spotted by eye, it is often easier and more efficient to use software to automatically spot issues or make issues more visible to readers. This guide is a catalog of tools and software that are commonly used by sleuths.

Here are some factors to consider when using these tools:

- **There can be false positives.** A tool may flag image features that, upon closer manual examination, do not actually indicate any image integrity issues.
- **There can be false negatives.** A tool may not flag image features that are indicative of image integrity issues. For instance, software for detecting image duplications within a figure may miss some duplications that are visible by eye.
- **Tools may not examine all data types.** There can be entire categories of data (including image data) that have been explicitly excluded by the programmers of a tool because they are not yet comfortable with the sensitivity/specificity of their tool for that data type.
- **Analysis may not be reproducible.** Some of these services and software are updated frequently and the current version of a tool may not yield the same results as a previous version.
- **Analysis of the same images in a different format may yield different results.** For example, if one uploads an entire PDF to a duplication detection tool, the tool may yield different results than if individual images are uploaded, even if the individual images and those in the PDF appear identical by eye. Figures in published articles will often be available in multiple resolutions, which can yield differing results. When performing image forensics, it is always preferable to work with the original, full-resolution, uncropped images provided by a study's authors.
- **Tweaking parameters can yield differing results.** Some tools have sensitivity settings that can be changed by the user. Changing these setting may produce different results for the same images.
- **Different tools do different things.** Not every tool described here has the same functionality or use cases as another tool. Another person without access to your tool of choice may not be able to reproduce your analysis.

Software/tools commonly used for image forensics in post-publication peer review:

- **Adobe Photoshop (subscription-based)**. Photoshop is an image manipulation software that allows users to adjust color levels, adjust brightness and contrast, overlay images and annotate figures among myriad other features. The United States Department of Health and Human Service Office of Research Integrity provides some toolkits for image forensics with Photoshop.
- **GIMP (the GNU Image Manipulation Program) (free to use and open-source)**. GIMP is a image manipulation software with most of the same features and functionality as Photoshop but is free to use (and modify).
- **Imagetwin (subscription-based)**. Imagetwin is a browser-based service that allows users to upload article PDFs and individual images, which it will then compare against a large database of published images to see if parts of any of the uploaded images have been used previously. It also detects within-document image duplication and splicing of certain images (e.g., Western blots). Users can control the sensitivity of detection on the Results page of a scan.
- **Proofig (subscription-based)**. Proofig is a browser-based service that allows users to upload article PDFs and individual images, which it will then compare against a large database of published images to see if parts of any of the uploaded images have been used previously. It also detects within-document image duplication.
- **Sherloq (free to use and open-source)**. Sherloq is a software environment for image forensics that can be installed on Linux and Windows. Users can perform various image transformations that make manipulation more apparent (such as visualizing luminence gradient) as well as inspect image metadata.
- **Forensically (free to use)**. Forensically is a browser-based service that offers several tools for image forensics, such as clone detection and levels adjustment.
- **FotoForensics (free to use)**. FotoForensics is a browser-based service that offers several tools for image forensics, such as error level analysis and metadata inspection.
- **Figcheck (subscription-based, limited free use)**. Figcheck is a browser-based service that detects within-document image duplication. Each user is limited to uploading 10 images a day.
- **Image Duplication Check (Sholto David) (free to use)**. This is a browser-based application that allows the user to upload a PDF and scan for within-document image duplication.
- **Google Lens (free to use)**. Google Lens is an extension of the Google search engine that allows users to upload an image and finding matching and visually-similar images across the web.