Description

A growing number of retractions and high-profile exposures have focused attention on the many faces of scientific fraud and on the limits of peer review to catch them before publication. Understanding common fraud types, why some slip through review, and how detection differs before and after publication helps researchers, reviewers, and administrators design more effective checks and prevent reputational and scientific harm. This article defines the principal types of fraud, assesses which are likeliest to evade peer review, and contrasts the practical challenges of detecting misconduct at the review stage versus after wider dissemination.

Types of scientific fraud: definitions and examples

Fabrication:

Fabrication is the invention of data, observations, or results that were never obtained. Fabricated datasets or entire experiments present a complete absence of verifiable raw material and are among the most serious forms of misconduct.

Falsification and selective reporting:

Falsification alters or omits data, manipulates experimental conditions, or tweaks analyses to produce desired outcomes. Closely related is selective reporting or “cherry-picking” of favorable results while omitting null or conflicting findings. These practices distort the record while preserving a surface layer of plausible data.

Image falsification:

Image manipulation encompasses duplication, splicing, contrast/brightness alterations that obscure features, and the insertion or removal of image elements. In fields that rely heavily on images (e.g., molecular biology, radiology), manipulated figures can convey false experimental support. Recent surveys and analyses indicate image issues are a nontrivial contributor to integrity investigations.

Plagiarism:

Plagiarism ranges from verbatim copying to mosaic or patchwork plagiarism and self-plagiarism. Many journals use text-matching software (e.g., iThenticate) to screen submissions, but paraphrased or translated plagiarism can evade simple matches.

Authorship and contribution fraud:

This category includes fabricated authors, “ghost” authorship (uncredited contributors), honorary or gift authorship, and forged authorship declarations. It also covers fake peer-review schemes in which suggested reviewers are fabricated or review contacts are hijacked to produce fraudulent reviews. Such manipulations subvert editorial systems rather than the scientific data itself.

Paper mills and template fraud:

Paper mills produce otherwise plausible but fraudulent manuscripts at scale sometimes reusing data, images, or fabricated experiments, and selling authorship positions. Paper-mill output can be stylistically consistent and superficially coherent, making detection difficult without data or provenance checks.

Which frauds are most likely to pass unnoticed in peer review?

Several fraud types are inherently harder for peer reviewers to detect. Fabrication can be especially stealthy when a manuscript includes plausible methods, consistent-looking results, and no request for raw data. Peer reviewers typically evaluate logic, methodology, and interpretation rather than raw datasets; without mandatory access to primary data, fabricated numbers may appear credible. The Retraction Watch–based analyses and bibliometric studies show many misconduct cases are not discovered until post-publication analysis or external whistleblowing, consistent with the difficulty of spotting wholly invented data during review.

Paper-mill manuscripts and fake peer review can also pass editorial filters when they mimic expected structure and language and when editorial systems trust author-suggested reviewers. Journal processes that allow unverified reviewer contacts create an attack surface for reviewer fraud; mass-produced papers that reuse formulaic text and images may escape cursory checks. Empirical reports document large batches of retractions linked to fabricated reviews and paper-mill activity.

Subtle data falsification or selective reporting may evade reviewers because it often requires reanalysis or access to raw datasets to detect inconsistencies, which are not routinely requested. In contrast, overt plagiarism copy-paste of large text blocks frequently triggers similarity checks and is among the problems most often caught pre-publication. However, paraphrased or cleverly reworked plagiarism can still slip by automated detection.

Image manipulation occupies a middle ground. Simple duplications or reused images may be detectable by attentive reviewers or routine image checks, and specialized image-forensics tools can identify duplications or splices. But sophisticated manipulations (small splices, localized retouching, or generated images) are easier to miss without dedicated screening tools and trained staff. Recent technological work has improved automated image screening, but implementation across journals is uneven.

Why peer review struggles to catch fraud: practical constraints

- **Time and scope:** Reviewers are typically unpaid volunteers focused on methodological soundness and novelty; they rarely have time to re-run analyses or examine raw image files in depth. Editors must balance speed and rigor, and resource-intensive forensic screening is not standard for most journals.
- **Access to primary materials:** Raw data, code, lab notebooks and original image files are often unavailable at submission. When primary data are not deposited in repositories, reviewers lack the evidence needed to verify results.
- **Expertise mismatch:** Reviewers evaluate content within their domain but may not have forensic expertise in image analysis, statistics, or data provenance. Small anomalies that require statistical or computational scrutiny can be missed.
- **System vulnerabilities:** Editorial workflows that accept author-suggested reviewers or lack identity verification are vulnerable to manipulation. Likewise, journals without mandatory checks for plagiarism, image duplication, or data availability leave gaps that can be exploited. Evidence from several retraction waves shows peer-review manipulation and fake reviews underpin many mass retractions.

Why detection improves after publication

- **Broader scrutiny:** Once published, a paper is exposed to the entire scientific community. Platforms such as PubPeer, social media, and formal whistleblowing channels enable crowdsourced scrutiny; sustained attention can reveal inconsistencies missed during peer review. Notable image analysts and watchdogs have helped detect manipulation post-publication.
- **Data and replication attempts:** Independent groups attempting to replicate findings or reanalyze shared data often uncover irreproducibility or anomalies, leading to expressions of concern or retractions. Post-publication use can expose a flawed study's downstream impact and highlight the need for correction.
- **Forensic tools at scale:** Publishers and community projects deploy large-scale text-mining, image-forensics, and statistical-screening tools that operate across corpora; these tools can detect patterns (e.g., duplicated images across many papers) that are invisible to single reviewers. Cross-journal analysis has exposed paper-mill output and serial offender patterns.

Practical steps for authors, reviewers and journals

- **Authors** should deposit raw data, analysis code, and original high-resolution image files in trusted repositories, use ORCID and CRediT contributor statements, and disclose AI or third-party assistance. These practices reduce ambiguity about provenance and authorship.

- **Reviewers and editors** should request raw data when results are surprising, use plagiarism and image-screening tools, verify reviewer identities where author-suggested reviewers are used, and apply reporting checklists or preregistration when applicable. Journals may adopt mandatory data-availability statements and standardized integrity checks.
- **Research offices and institutions** should train early-career researchers in responsible conduct (data management, authorship norms, and transparent reporting) and create clear, accessible channels for raising concerns. Institutional oversight shortens detection timelines and reduces the burden on journals.

Checklist for submission-ready integrity

- Run a reputable text-similarity check and resolve flagged passages.
- Deposit raw data and code, link them in the manuscript.
- Keep and upload original image files and annotate any processing.
- Use contributor-role statements (CRediT) and verify all authors approve submission.
- Consider independent editorial or manuscript review to identify weaknesses.

Conclusion and next steps

No single measure will eliminate scientific fraud, but evidence shows that a combination of transparent data practices, identity verification in peer review, routine use of plagiarism and image-forensics tools, and post-publication community scrutiny reduces the risk that serious misconduct goes unnoticed. Peer review serves as an important filter, but its usual scope and resource constraints mean that certain frauds especially fabricated data, paper-mill outputs, and sophisticated falsifications are more likely to survive to publication. After publication, broader scrutiny and forensic tools increase the chance of detection, but the downstream costs (misleading citations, wasted resources, public harm) may already have accumulated.

For authors concerned about strengthening manuscripts before submission, consider professional manuscript editing and submission support that includes plagiarism screening and technical checks to reduce desk rejections and clarify data availability statements. For guidance on ethical AI use in manuscripts, explore the Responsible AI Movement hosted by Enago. For institutions and publishers, maintain the integrity of your publications with Enago’s image manipulation detection services. Ensure compliance with publication standards by verifying the authenticity of research images for your institution or journal.

Category

1. Reporting Research

Date Created
2025/12/02
Author
editor