

Common uses of image manipulation detection for Image Forensics

Validation of evidence

An image that has implications in evidential circumstances should be inspected for changes regarding the displayed content. These types of images exist as a record of events and must be validated. Manipulations of the original content of an image used as evidence can cause an incorrect judgment to be made. When an image is used to support testimony, an assessment of its integrity can be made with the assistance of the Rigour package.

Finds use in: insurance claims, judicial proceedings, criminal investigations, news media

Defense

Intelligence gathering requires a correct assessment regarding the integrity of a digital image. For instance, images are used to make tactical decisions, assessments of risk, and decisions about security threats. It is valuable to know whether an image is a trustworthy piece of information from which to base a decision.

Finds use in: Military application, Intelligence investigations

Enforcement of scientific honesty

The presentation of photographic data used to support a scientific argument should be screened for alteration. Scientists will often 'clean' an image in preparation for display. Although this act is often done in the effort to make presentation of results more clear, it may fundamentally change the content of the image. Rarely, an image will be manipulated with fraudulent intent. In this case, it is important to detect changes to prevent the publication of bogus material.

Finds use in: Academic publication, universities

Maintaining reputation

An organization such as a journal can be embarrassed by publication of data that is later found to be fraudulent. By using software such as Rigour, the organization will increase the probability that fraudulent content will be discovered and subsequently rejected.

Finds use in: all