INVESTIGATION · DIGITAL INVESTIGATION

Geolocation and Image Verification

Photographs and videos shared online are powerful evidence, but they are often old, misattributed or manipulated. This article explains how investigators verify where and when an image was made, whether it has been altered, and how to report the result with appropriate confidence.

ModQu research article · 1,355 words · 14 references (APA 7th edition)

Photographs and videos taken by ordinary people now provide some of the earliest and most detailed evidence of conflicts, disasters, crimes and protests. They are also easy to misuse. An image from one war is shared as if it showed another; a video from years ago resurfaces as breaking news; a picture is edited, cropped or generated by software. Verification is the process of establishing whether an image is what it is claimed to be: where it was taken, when, by whom and whether it has been altered. Geolocation, the identification of the exact place shown in an image, is one of its central techniques.

These methods began in newsrooms and among volunteer researchers, and are now used by human rights investigators, international courts and government analysts (Dubberley et al., 2020). They rely mostly on careful observation and openly available information rather than on specialist equipment.

The questions verification answers

Silverman (2014) sets out the basic questions that verification should address for any piece of user-generated content:

- **Provenance**: is this the original, or a copy of an earlier image?
- **Source**: who made it, and can they be contacted?
- **Date and time**: when was it made?
- **Location**: where was it made?
- **Integrity**: has it been altered in a way that changes its meaning?

Each question is answered separately, and the answers can differ. An image may be genuine and unaltered, but from a different place or year than claimed. Most misleading images circulating online are not sophisticated forgeries but real images with false context (Weikmann & Lecheler, 2023).

Provenance: finding the first version

The first step is usually to search for earlier copies of the image. Reverse image search tools compare an image with indexed images and can reveal that it was published years earlier or in a different context. Investigators search key frames from videos in the same way. Finding the earliest available version is valuable because later copies are often cropped, compressed and stripped of metadata.

Metadata embedded in the original file, such as the camera model and the date and time recorded in its Exif data (Camera & Imaging Products Association [CIPA], 2019), can support verification, but most social media platforms remove it on upload, and device clocks may be wrong. Metadata are therefore treated as one clue among several, not as proof.

Geolocation

Geolocation compares visible features in an image with maps, satellite imagery and other photographs of candidate locations until a match is found.

Clues used to geolocate and date an image

No single clue is decisive; investigators look for several that agree

	What it can show	How it is checked
Landmarks and buildings	Specific place, sometimes exact viewpoint	Satellite imagery, street-level imagery, other photos
Terrain and skyline	Region and camera position	Elevation models, mountain profiles
Signs and text	Country, language, town, business	Translation, business directories, maps
Shadows and sun	Time of day and approximate date	Sun position calculators for the location
Weather and season	Date range	Historical weather records, vegetation
Changes over time	Before or after a known event	Dated satellite images showing construction or damage

Based on Silverman (2014), Koettl (2016) and Higgins (2021) ModQu.com

Figure 1. Common clues in image verification. A location or date is most secure when independent clues, checked against different sources, point to the same answer. Diagram by ModQu.

Investigators begin with broad clues that narrow the area, such as language on signs, styles of architecture, vehicles, road markings and vegetation, and then look for distinctive features such as a mosque's minaret, a pattern of roads or a row of buildings that can be matched precisely. Satellite and street-level imagery allow a candidate location to be checked from above and from ground level. A successful geolocation usually identifies not only the place but the position and direction of the camera.

Koettl (2016) describes an analytical framework for human rights researchers that combines these techniques with assessment of the source and of the content's consistency with other information. Higgins (2021) describes how the Bellingcat group used geolocation of photographs and videos posted online to trace the route of the missile launcher linked to the destruction of Malaysia Airlines flight MH17 over eastern Ukraine in 2014, a finding later supported by the official criminal investigation.

Chronolocation: establishing when

Establishing the date and time, sometimes called chronolocation, uses clues that change over time. Shadow length and direction indicate the sun's position, which varies with the time of day and the season at a known location. Weather can be compared with historical records. Dated satellite images can show whether a building existed or was damaged at the time. Comparing several such clues often narrows an image to a particular day or even hour.

Integrity: detecting manipulation

Digital image forensics looks for traces left by editing. Farid (2009) reviews techniques that detect inconsistencies in lighting, in the geometry of shadows and reflections, in the statistical patterns left by resampling and compression, and in the noise produced by camera sensors. Popescu and Farid (2005) showed that resizing or rotating part of an image leaves detectable statistical correlations, and Lukáš et al. (2006) showed that the faint noise pattern of a camera's sensor can be used to link an image to a specific device. Zampoglou et al. (2017) found, however, that many automated tools for locating spliced regions perform poorly on images that have been compressed and resized by social media, so automated results need expert interpretation.

Human judgement is not a reliable substitute. Nightingale et al. (2017) found that people were only slightly better than chance at detecting manipulated photographs of real-world scenes, and were even worse at locating the change. Images produced by generative artificial intelligence add a further difficulty: Nightingale and Farid (2022) found that people could not reliably distinguish faces generated by software from real faces, and judged the synthetic faces slightly more trustworthy. Investigators therefore rely on provenance, context and corroboration as much as on inspection of the image itself.

Use as evidence

Verified open source images are increasingly used in legal proceedings. In 2017 the International Criminal Court issued an arrest warrant for Mahmoud Mustafa Busayf Al-Werfalli that relied substantially on videos posted on social media showing executions in Libya (*Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli*, 2017). To support such use, the Berkeley Protocol sets out standards for collecting, preserving, verifying and reporting digital open source information, including documentation of every step so that others can repeat it (Human Rights Center, University of California, Berkeley, & Office of the United Nations High Commissioner for Human Rights [OHCHR], 2022).

Common pitfalls

Experienced verifiers warn against several recurring errors. The first is confirmation bias: once an investigator suspects a location, it is easy to notice features that fit and overlook those that do not. A good practice is to list the features that would rule a candidate location out, and to check them deliberately. The second is relying on a single clue, such as a sign or a uniform, that could easily appear in many places or be staged. The third is treating the absence of earlier copies as proof that an image is new, when reverse search tools index only part of the internet. The fourth is exposing the people

who took or appear in an image. Publishing an exact location or identifying a bystander can put them at risk, so investigators consider what detail the public actually needs (Dubberley et al., 2020). Finally, verifiers should record their reasoning as they go, with screenshots of the matching features, so that a colleague can follow and challenge each step.

A short example

The following hypothetical case illustrates the process. A video circulating online claims to show a flood in a city last week. A reverse search of key frames finds no earlier copies. Shop signs in the video are in the local language, and a distinctive bridge and church tower are visible. Matching these against satellite imagery identifies a specific street, and street-level imagery confirms the viewpoint from a building's second floor. The shadows are consistent with late afternoon, and historical weather records show heavy rain in that city on the claimed day. The person who first posted the video confirms by message that they filmed it from their flat. The investigator reports that the video was very probably filmed at the identified location on the claimed date, and documents each step.

Conclusion

Image verification treats every photograph and video as a claim to be tested. Investigators look for the earliest version, establish the source, geolocate the scene, estimate the date and examine the image for manipulation, and they look for several independent clues that agree. Findings are reported with stated confidence and with the steps documented, so that others can check them. Done carefully, verification turns the flood of images shared online into evidence that can inform the public and support accountability.

References

Camera & Imaging Products Association. (2019). *Exchangeable image file format for digital still cameras: Exif version 2.32* (CIPA DC-008-2019).

Dubberley, S., Koenig, A., & Murray, D. (Eds.). (2020). *Digital witness: Using open source information for human rights investigation, documentation, and accountability*. Oxford University Press.

Farid, H. (2009). Image forgery detection. *IEEE Signal Processing Magazine*, *26*(2), 16–25. https://doi.org/10.1109/MSP.2008.931079

Higgins, E. (2021). *We are Bellingcat: An intelligence agency for the people*. Bloomsbury.

Human Rights Center, University of California, Berkeley, & Office of the United Nations High Commissioner for Human Rights. (2022). *Berkeley Protocol on digital open source investigations*. United Nations.

Koettl, C. (2016). *Citizen media research and verification: An analytical framework for human rights practitioners*. Centre of Governance and Human Rights, University of Cambridge.

Lukáš, J., Fridrich, J., & Goljan, M. (2006). Digital camera identification from sensor pattern noise. *IEEE Transactions on Information Forensics and Security, 1*(2), 205–214. https://doi.org/10.1109/TIFS.2006.873602

Nightingale, S. J., & Farid, H. (2022). AI-synthesized faces are indistinguishable from real faces and more trustworthy. *Proceedings of the National Academy of Sciences*, *119*(8), Article e2120481119. https://doi.org/10.1073/pnas.2120481119

Nightingale, S. J., Wade, K. A., & Watson, D. G. (2017). Can people identify original and manipulated photos of real-world scenes? *Cognitive Research: Principles and Implications*, *2*, Article 30. https://doi.org/10.1186/s41235-017-0067-2

Popescu, A. C., & Farid, H. (2005). Exposing digital forgeries by detecting traces of resampling. *IEEE Transactions on Signal Processing*, *53*(2), 758–767. https://doi.org/10.1109/TSP.2004.839932

Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli, ICC-01/11-01/17, Warrant of Arrest (International Criminal Court, Pre-Trial Chamber I, 15 August 2017).

Silverman, C. (Ed.). (2014). *Verification handbook: A definitive guide to verifying digital content for emergency coverage*. European Journalism Centre.

Weikmann, T., & Lecheler, S. (2023). Visual disinformation in a digital age: A literature synthesis and research agenda. *New Media & Society*, *25*(12), 3696–3713. https://doi.org/10.1177/14614448221141648

Zampoglou, M., Papadopoulos, S., & Kompatsiaris, Y. (2017). Large-scale evaluation of splicing localization algorithms for web images. *Multimedia Tools and Applications*, *76*(4), 4801–4834. https://doi.org/10.1007/s11042-016-3795-2