Fighting Digital Media Fraud with Cutting-Edge Forensics

Are you equipped to handle the rising threat in digital claims?

Photo-based claims estimates have been a growing trend the past few years in the insurance industry. Once the pandemic hit, that trend accelerated significantly as the need for remote claims estimates increased. Photo estimates for auto claims, for example, doubled early in the pandemic, and Verisk saw a 933 percent increase in usage of our virtual estimating tool, ClaimXperience®.

These estimates seem like a win-win for insurers and customers. Policyholders can get faster, simpler service when reporting losses, and carriers reduce expenses without the need for on-site estimates. But there's another group benefiting from remote claim estimates—fraudsters.

From simple schemes like re-using prior-loss images to filing fake claims or employing advanced tactics such as manipulating image pixels to fabricate damage, fraudsters are already profiting from the rise in remote claims processing. And they're going unchecked because many insurers aren't equipped with the tools to identify digital media fraud at scale.

As digital adoption grows in the industry, so will fraud leakage if insurers don't combat these schemes with advanced anti-fraud technology. Fortunately, artificial intelligence (AI) offers promise in the form of digital media forensics.

2x	8 in 10	933%
Photo estimates for auto claims doubled since early in the pandemic	Insurers say the pandemic accelerated their digital adoption	Increase in use of Verisk's virtual claim estimate solution

Simple schemes go undetected

One in 10 insurance claims contains some element of fraud. And annually, insurance fraud steals at least $308.6 billion from American consumers. While there's no hard data on the scope of digital media fraud in claims, indicators show the issue is growing.

There are numerous ways to submit fraudulent claims using photos, and many of them are relatively simple. For example, fraudsters can re-use an image from a prior loss or download a photo of damage from the Internet and submit it for a claim. These schemes are likely to go undetected, especially if the claimant switches carriers, so there may not be any internal files of the prior loss. Likewise, if adjusters aren't conducting on-site inspections, verifying damage after the loss is difficult at scale.

Common digital fraud schemes

Reusing prior-loss images
When someone uses a loss photo from a prior claim to file a new claim, often with a different insurer

Using Internet images
When someone downloads a photo of damage from a website and submits it with a claim

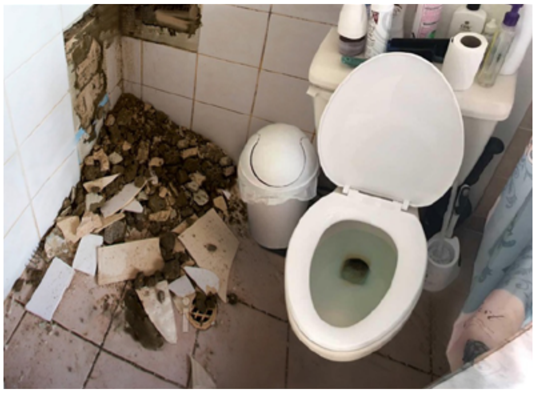
Document manipulation
When someone uses PDF-editing software to modify an original document, such as changing the price on an invoice

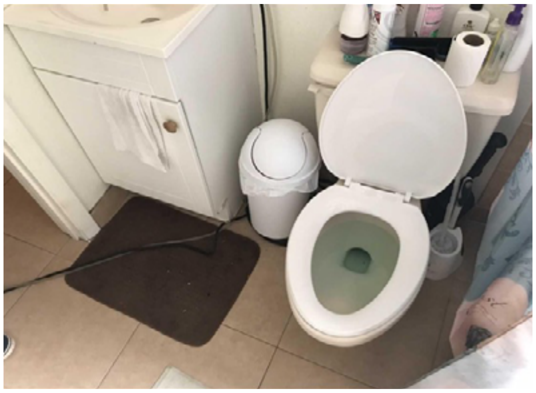
Image manipulation
When someone uses photo-editing software to modify photo pixels to fabricate a loss

The art of manipulation

Fraudsters are also turning to technology to perpetrate schemes. Using common editing software, fraudsters can manipulate documents and images to submit inflated or fake claims. For example, someone could submit a fraudulent invoice for reimbursement for a property claim by using free online PDF editing software to modify an original document. They could simply change the price on the receipt to inflate the claim. They could even pass the same invoice to a friend or family member who could change the name and contact details on the invoice and use the same document to defraud another insurer.

Manipulating images is also easy using popular photo-editing software or even free online tools. Modifying a few pixels of a photo can show damage that doesn't exist. The photos below show an example of image splicing, in which a region of one photo is copied and pasted on another. The image on the left is manipulated, as the damage was spliced on the original photo (the image on the right).





Whether it's image or document manipulation, it's nearly impossible for humans to recognize these modifications with the naked eye. That's why digital forensics are critical to thwarting this type of fraud.

Fighting fraud with AI

Digital media forensics use AI to identify fraud and manipulation in digital media files such as photos and documents. There are three primary categories of forensics for detecting fraud—binary forensics, non-binary forensics, and advanced forensics. Let's explore the three.

Binary forensics

Binary forensics are the simplest form of forensics. They are often effective at determining if an image is fraudulent or not and help determine if a loss image is re-used or sourced from the Internet. The technique involves analyzing image pixels to determine duplicates from a database or the Internet.

However, there are challenges in developing and implementing binary forensics.

1. **Expertise in specialized image processing:** It's not enough to analyze image file names to find duplicates. Binary forensics requires algorithms that analyze an image's pixel values.

2. **Computing power:** It takes a fair amount of computing power for algorithms to quickly search an extensive database of existing images to find a duplicate.

3. **False positives:** Effective binary forensics must limit the percentage of false positives so investigators aren't buried with false leads.

What are digital media forensics?

Algorithms designed to identify fraud and manipulation in digital media files such as photos and documents.

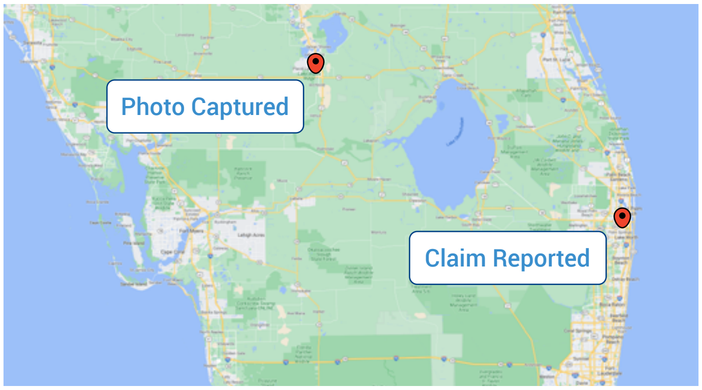
Examples of forensics:

- **Evaluating potential reuse of digital files**
- **Analyzing file metadata**
- **Identifying photos sourced from the Internet**
- **Identifying image or document forgery**

Non-binary forensics

Non-binary forensics examine the metadata of an image, such as the date, time, and location the photo was taken. Those details can help determine if a loss is legitimate or not.

For example, the photo below was submitted for a fence damage claim with a loss date of September 2018 and West Palm Beach, Florida, as the loss location. However, the image metadata revealed that the photo was actually taken in July 2015 in Lake Placid, Florida. That's three years and 100 miles apart.



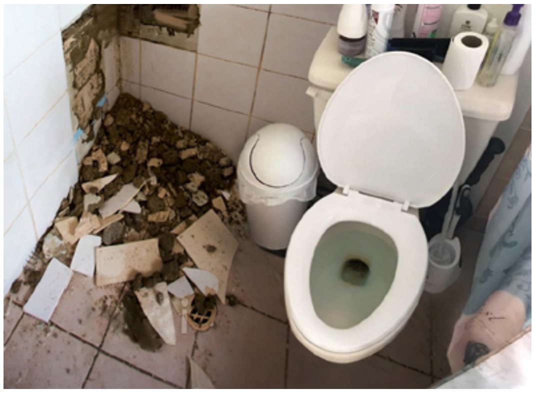
Claim details said loss occurred Sept. 2018 in West Palm Beach. Photo details show the photo was taken July 2015 in Lake Placid.

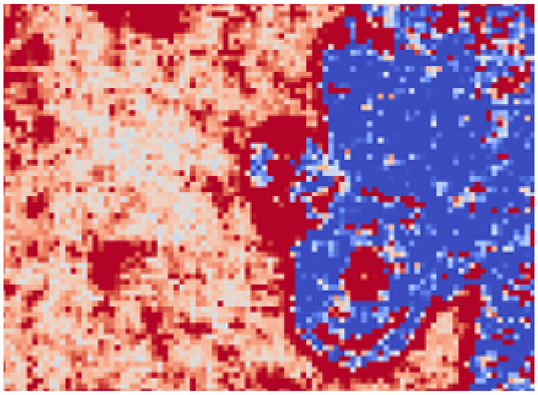
Non-binary forensics requires granular analysis and can't be developed with blanket rules. There are nuances for line of business and type of loss that must be accounted for to avoid false-positive results.

Advanced forensics

Advanced forensics uncover modifications to documents and images that the human eye can't detect. To detect image manipulation, the technology identifies noise patterns in an image. When cameras capture images, they compress them into a format, such as JPEG, creating noise patterns. Each camera has slight nuances in the noise patterns.

At Verisk, we're developing technology that identifies if an image has more than one noise pattern, which is a sign of manipulation. The images below show how the technology identified a different noise pattern in the manipulated bathroom damage photo.





Innovative tools for digital claims

There are various ways fraudsters can game the system with digital media files, so there needs to be a variety of ways for insurers to detect these schemes. As part of our digital media forensics initiative, Verisk is developing a suite of solutions that use binary, non-binary, and advanced techniques to quickly identify questionable attributes in digital files.

Some of those solutions are already available, including a digital media contributory database enhancement to ClaimSearch® that enables participating companies to view prior-loss photos on match reports. We're also developing an Image Duplication Check feature that uses binary forensics to determine if any images from an insurer's new claims have duplicates in the system.

With our forensics solutions, insurers will be able to:

- Validate the time and location a photo was taken is appropriate for the loss
- Confirm the photo didn't come from the Internet
- Confirm the image hasn't been used before
- Confirm no evidence of receipt or documents manipulation
- Ensure the image hasn't been modified

The ultimate benefit of forensic technology is not just for detecting fraud but for processing legitimate claims faster. Carriers equipped with our digital media forensics can be confident in paying meritorious claims quickly, which boosts customer satisfaction, shortens cycle times, and reduces costs.

For more information about Verisk's digital media forensics, contact:

Katie Flaherty | Director-Product Innovation | Anti-Fraud Solutions Group
katie.flaherty@verisk.com
Tel: 727-220-9867

Reference

1. Coalition Against Insurance Fraud, https://insurancefraud.org/fraud-stats/, 2022

2. Share of Auto Claims Using Photo Estimates Doubles During the Pandemic, Claims Journal, June 5, 2020

3. Background On: Insurance Fraud, Insurance Information Institute, November 18, 2021

4. Background On: Insurance Fraud, Insurance Information Institute, November 18, 2021