



Detect the Undetectable

Advanced Digital Media Fraud Detection



A tech-enabled surge in claims fraud

When any fraudster with a smartphone can access rapidly evolving, AI-powered tools to manipulate claim-related digital media, how do you keep pace to avoid paying false or inflated claims? The new generation of digital media fraud is getting harder to detect and prevent with the human eye.

Today's insurers are watching an ever-growing volume of these submissions for:

Deepfakes:

Widely available AI tools can generate deepfake images from scratch or convincingly alter existing images to change or hide information—in seconds.

Shallowfakes:

Conventional desktop or mobile editing software can produce images realistic enough to pass a cursory examination.

Document fraud:

Altered or fake documents are an older, more manageable, but still present threat.

Recycled and borrowed images:

Using images from prior claims or the internet to falsely represent new damage, potentially across multiple carriers.



At the 2025 Insurance Fraud Management (IFM) Conference, a survey revealed key insights into these rising concerns:

42%

of respondents cited image and document manipulation as their top concern.

+

39%

highlighted deepfakes and AI-related fraud.

=

Together, these concerns accounted for

81%

of the industry's most pressing emerging fraud challenges.

Deepfakes and shallowfakes

Widely available AI tools and features, built into Android and iOS operating systems, can now generate deepfake images from scratch—or convincingly edit existing images—in seconds. And when Adobe released “Generative AI Fill” for Photoshop in September 2023, scammers realized it was an easy way to forge shallowfake images to boost insurance claims. Using such technology, fraudsters with near-zero experience can modify an entire image or a small portion, altering, inpainting, or filling sections to change or hide information.

Verisk's Digital Media Forensics can help detect these fraudulent images with the ability to:

- ✓ Flag pixel manipulation that indicates a digitally altered image.
- ✓ Identify deceptive images created using GenAI.



**IMAGE
MANIPULATED**



Document fraud

Altering or faking documents may involve yesterday's technology, but these fraud tactics still demand insurers' attention. Fortunately, techniques to detect document fraud are well-established—and they're automated and scalable within Digital Media Forensics:

- ✓ Digital documents have selectable and searchable text that's easy to analyze for red flags such as suspicious terms, altered values, or duplicated information.
- ✓ Forensic tools can search and compare documents to detect patterns such as reused templates or duplication across fields that should contain unique information—tax paid, credit card numbers, time stamps, and the like.
- ✓ Rich metadata, similar to that in images, can make verifying the integrity of content easier, revealing what software was used to create it and when.
- ✓ Digital signatures, such as DocuSign, provide opportunities to systematically verify documents' authenticity by ensuring the structure is consistent with the PDF and validating the signature through signing authorities.

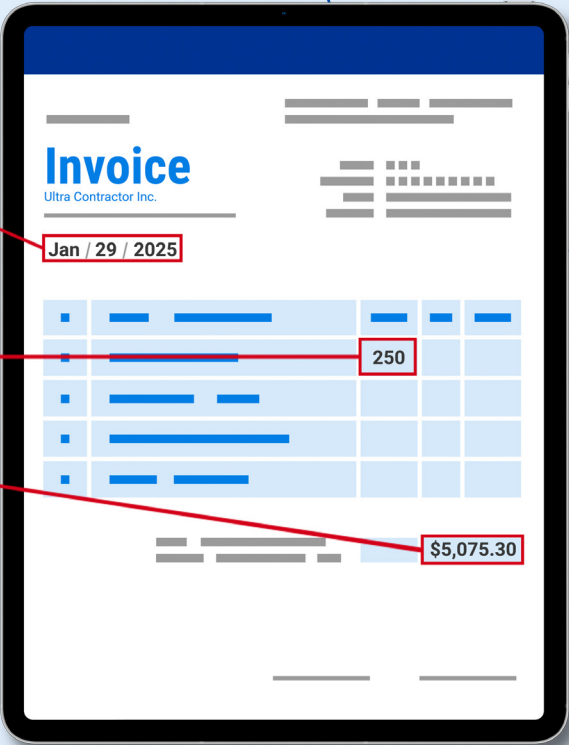
EDITED TEXT



DATE
Dec 13, 2024

QUANTITY
100

TOTAL
\$2,367.97



Recycled and borrowed images

Fraudsters, from policyholders and independent adjusters to repair contractors and auto body shops, may submit photos from prior losses—presenting them as new damage for claims, to inflate bills, or to cut corners on providing estimates. These long-running schemes can go undetected, especially if a claimant switches carriers, unless the right tools are in place to catch the fraud. Photos of damage downloaded online may also be submitted with fraudulent claims.

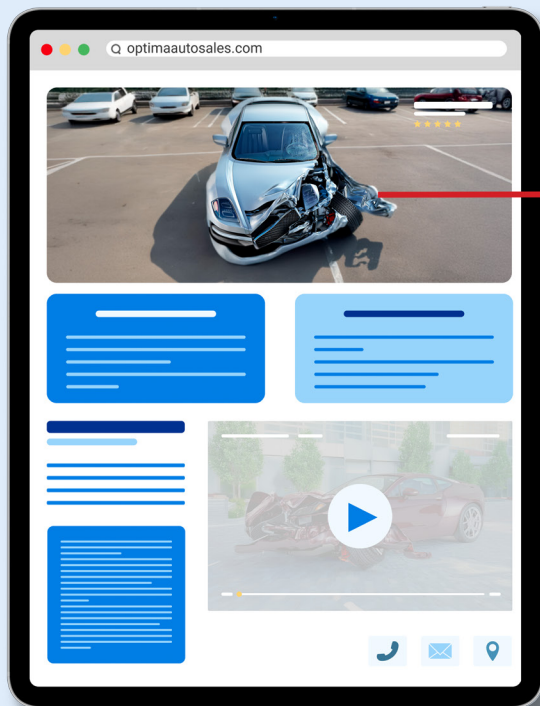
As with document fraud, this type of image fraud often contains clues that a solution such as Digital Media Forensics can uncover:

- ✓ Verisk's contributory database, with millions of images from participating carriers across auto and property, can identify duplicates submitted with prior claims.
- ✓ Internet duplication-checking can discover images sourced from across the web.
- ✓ The rich metadata embedded in digital media can flag potential modifications and corroborate locations and dates of image capture to detect discrepancies and possible misuse.

Verisk helped one carrier expose an appraiser who submitted 170 duplicate photos over two years—affecting more than \$1 million in claims.

"An industrywide database has enabled our customers to detect fraud at scale, helping claim adjusters and SIUs focus on high-risk referrals. Our insights provide concrete, defensible evidence, reinforcing the value of a powerful network effect that only this kind of database can deliver."

– Emily Law,
Director of Analytics,
Verisk Anti-Fraud Analytics

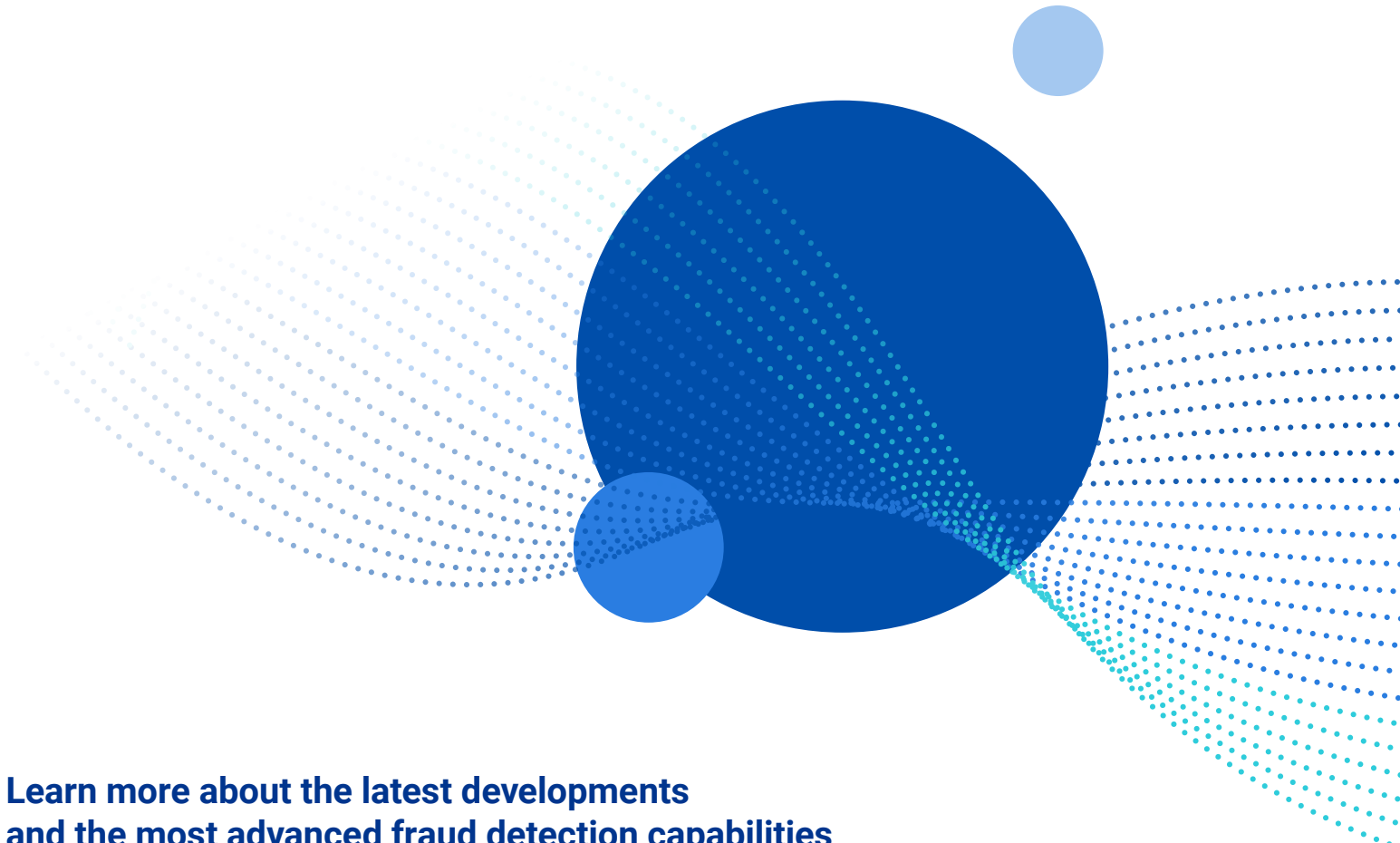


WEB DUPLICATE



An urgent challenge

Digital media fraud is growing rapidly in scope, volume, and sophistication. But insurers can respond quickly and decisively with a commitment of resources and innovative tools to stay ahead of an ever-evolving threat. Advancing technology now allows potential image fraud detection for both claim adjusters and special investigations units.

An abstract graphic featuring a large central blue circle. To its upper right is a smaller light blue circle. To its lower left is another medium-sized blue circle. Radiating from these circles are numerous dotted lines in shades of blue and teal, creating a sense of motion or data flow across the page.

**Learn more about the latest developments
and the most advanced fraud detection capabilities
with Digital Media Forensics.**

Visit verisk.com/products/digital-media-forensics
to learn more.



+1.800.888.4476 / antifraudsolutions@verisk.com / verisk.com