IDScan.net DIVE enhances tamper-checks to catch manipulated, Photoshopped IDs

Identity tech firm spins up additional neural network to better detect physical and digital tampering

Tampered ID image

IDScan.net Logo

NEW ORLEANS, LOUISIANA, UNITED STATES, July 9, 2024 / EINPresswire.com/ -- IDScan.net, identity tech company and makers of the Digital Identity Verification Engine (DIVE) platform, is launching enhanced tamper detection tools to better detect doctored identity documents.

IDScan.net's identity verification tools include more than 200 AI-powered checks to confirm the legitimacy of an ID or drivers license - these include checks on the barcode format, the ID template, and front/back crossmatch checks, as well as calls to third party databases. With this latest update, DIVE will get a huge boost in its ability to detect IDs which have been altered, either physically or digitally.

Physical tampering includes replacing or manipulating the data or photo on the ID. In some cases, this can be as unsophisticated as taping a different photo onto a stolen ID, or using a sharpie to change information such as name, date of birth, or ID number. Because the manipulation is done in the "real world," this tampering cannot be detected by examination of the image file.

Digital tampering is typically performed using image editing software or scripts, and can result in more seamless and sophisticated imagery. However, editing tools often leave digital fingerprints in the image metadata, which can be examined in real time simultaneously to forensic evaluation of the ID's legitimacy.

Key improvements:
- Improved metadata inspection looking for multiple elements in the metadata to confirm that

> Our software has always looked for evidence of tampering, but with rising fraud rates we wanted to make tamper checks a priority."
>
> *Joshua Sheetz, IDScan.net VP of Engineering*

the picture is live.
- Image compression checks to look for hallmarks of image manipulation and processing
- Print quality detection and color matching to find physical tampering
- Improved micro-shadow checks to confirm a smooth ID, with no alterations
- Improved font consistency checks

"Our software has always looked for evidence of tampering, but with rising fraud rates we wanted to make tamper checks a priority," said IDScan.net Vice President of Engineering, Joshua Sheetz. While new threats such as AI-generated fake ID images threaten the KYC processes of major organizations, ID tampering still remains a top threat for any business looking to verify identity remotely. "Tampered IDs still represent a large percentage of fraud seen by banks, and our latest neural network will ensure we can provide the highest level of defense against this type of deception."

Users of DIVE software will automatically see benefits from the AI-enhancements. New customers are invited to test the improved algorithms during a live demo.

About IDScan.net
IDScan.net is an AI-powered identity verification platform powering the ID validation and identity proofing strategies of more than 7,500 global businesses. We focus on outstanding customer experience, data automation, and fraud reduction for high compliance industries.

Jillian Kossman
IDScan.net
+1 504-834-0222
email us here
Visit us on social media:
LinkedIn
