

A New Tool Protects Videos From Deepfakes and Tampering

 [wired.com/story/amber-authenticate-video-validation-blockchain-tampering-deepfakes](https://www.wired.com/story/amber-authenticate-video-validation-blockchain-tampering-deepfakes)

Lily Hay Newman



Getty Images

Video has become an increasingly crucial tool for law enforcement, whether it comes from security cameras, police-worn body cameras, a bystander's smartphone, or another source. But a combination of "deepfake" video manipulation technology and security issues that plague so many connected devices has made it difficult to confirm the integrity of that footage. A new project suggests the answer lies in cryptographic authentication.

Called Amber Authenticate, the tool is meant to run in the background on a device as it captures video. At regular, user-determined intervals, the platform generates "hashes"—cryptographically scrambled representations of the data—that then get indelibly recorded on a public blockchain. If you run that same snippet of video footage through the algorithm again, the hashes will be different if anything has changed in the file's audio or video data—tipping you off to possible manipulation.

Users need to set the interval to balance system constraints on devices with what a camera may be filming. Creating hashes every 30 seconds on a police body camera might allow quick and subtle, but still potentially impactful, manipulations to slip through. Setting the interval to every second on a small business' surveillance camera might be overkill.

"There's a systemic risk with police body cameras across many manufacturers and models," says Amber CEO Shamir Allibhai. "What we're worried about is that, when you couple that with deep fakes, you can not only add or delete evidence but what happens when you can manipulate it? Once it's entered into evidence it's really hard to say what's a fake. Detection is always one step behind. With this approach it's binary: Either the hash matches or it doesn't, and it's all publicly verifiable."

"We can show that there are ways to ensure that all parties have faith in the video and how it was captured."

Josh Mitchell, Amber Security Consultant

A tool like Amber has obvious appeal for human rights activists, free speech advocates, and law enforcement watchdogs wary of potential abuse coverups, but governments also have an interest in video integrity tools. Allibhai is presenting Amber Authenticate to Department of Defense and Department of Homeland Security representatives at a Defense Advanced Research Projects Agency showcase on Monday. And DHS has already shown an [interest in similar solutions](#) like one from the blockchain-based data validity company Factom, which is also working on a [video authentication](#) tool.

Amber Authenticate is built on the popular open-source blockchain platform Ethereum, and includes a web platform that makes it easy to visually understand which parts of a video clip have hashes that match the originals stored on the blockchain and which, if any, don't. A green frame around the footage as it plays indicates a match, while a red frame takes its place for any portion with a mismatched hash. Below the video player, Amber also shows a detailed "audit trail" that lists when a file was originally created, uploaded, hashed, and submitted to the blockchain.

The idea is for the manufacturers of products like CCTVs and body cams to license Amber Authenticate and run it on their devices. Amber research consultant Josh Mitchell, who found software [vulnerabilities in five models](#) of mainstream body cameras last August, has been able to demonstrate that Authenticate is compatible with at least some of those brands.

"I've been taking the technology and putting it on a body camera, because there's no authentication mechanism right now on any of the cameras," Mitchell says. "The fact that there's nothing protecting that evidence from a malicious party is worrying, and

manufacturers don't seem very motivated to do anything. So if we have a provable, demonstrable prototype we can show that there are ways to ensure that all parties have faith in the video and how it was captured."

Amber's Allibhai, who is self-funding the project, says that Authenticate plans to be totally transparent and open to vetting by outside experts.

Whether's its Amber Authenticate or another solution, an integrity and authentication tool for video—particularly police body cameras—can't come soon enough, according to Jay Stanley, a senior policy analyst at the American Civil Liberties Union. "Technologists are going to have to validate the security of Amber as with any authentication technique," he says. "But I hope that Amber or a similar product becomes standard. Like body cameras themselves, video authentication can help create community confidence in evidence about what's taken place, and can give everybody confidence that things are on the up and up in what can be very harrowing and difficult incidents."
