Our Technology

Safeguarding media in the 21st century requires an excess of creativity and technology. VideoLock by DeepTruth has harnessed both, charting the cryptographic digital DNA fingerprints of media and integrating that DNA into our patented, real-time processes capturing, certifying and validating digital media authenticity.

VideoLock's authentication technology protects the integrity of video, photos and audio from the moment they are captured, using additional layers of security in the brief time it takes to certify media and permanently protect its integrity in blockchain. The result is a crypto-media solution providing instant credibility for victims of deepfake technology and a buttress against any attempt to mischaracterize or otherwise alter the truth. Here's how it works.

Capturing Media

The longer it takes to certify authenticity in raw recordings, the more time there is to infiltrate and modify the original before it is permanently protected with blockchain. The achievement of VideoLock technology is the patented processes documenting the digital DNA from the moment of capture to preserve proof of the truth even before it is added to the blockchain.

The VideoLock app begins the certification process before video and audio is finished being recorded. Once the app is open and ready to capture, it activates smartphone sensors and begins tracking more than 90 dimensions of metadata. Once the record button is pressed, the app goes to work.

A hash is created for every frame of an audio or video recording. Metadata is hashed every 8 frames, forming an encrypted sequence that is immediately sent to the DeepTruth API for certification. As the video or audio continues to roll, sequences continue to be sent. Latency is accounted for. If sequences take too much time to arrive, VideoLock marks them as uncertain.

Images are spliced into equal parts - either 16, 32 or 64 squares - that are all hashed and combined with metadata captured as the photo is taken. To further stifle fraudulent activity, a patent-pending rotating hash is used during capture, adding a layer of complexity to an already impossible-to-compromise system. Our most common tool to create a hash is MD5, but the app will use others in the rotation.

Other factors also cause the technology to mark sequences in media as uncertain including:

- If GPS tracking in the phone does not meet accuracy standards.
- The capture functions in the app are unable to read or interact with existing media files to prevent tampering.
- Data sent between smartphones to DeepTruth API is encrypted using TLS 1.3.

Certifying Media

Immediately upon receiving a sequence, the DeepTruth API takes its own hash of the metadata and compares it to the original taken at capture. Any deviation is rejected as compromised. If the location of any data is not 100% verified, such as if GPS is not precise or if the phone is not connected to a network, it is classified as uncertain. Uncertain data has not been manipulated and the hashes match, but location certainty was lacking during capture.

The metadata itself is vast. Among the dozens of measurements taken three times per second:

- Constantly updated GPS information that can show where someone shot the video – and trace the path of the shooter if they move while it was recorded.
- The angle of the phone during each frame of capture.
- Satellite locations at the time the recording was made.
- Which cell phone towers the phone is using to get its signal.

Verified sequences, including uncertain ones, are then sent to blockchains. Blockchain IDs are sent back and saved internally.

Verifying Media

The VideoLock app reader is an instant check on the authenticity of media captured with the technology. The app takes a hash of video or audio and connects with DeepTruth API to find a matching hash sequence. When found, the media is compared, frame by frame, to the stored metadata. Each section of a photo has a new hash created in the app and is compared against the respective section hashes, as well as metadata, taken during capture.

Discrepancies are color coded. A validation bar parallels the time sequence in video and audio. Authentic parts are accompanied by a green line. Uncertain areas are marked as yellow. Red lines show that the media has been manipulated.

Images are color-coded with a shaded overlay, showing exactly which sections of a photo, if any, have been manipulated.

Metadata and Hash records are stored and validated on a blockchain. Blockchain clusters are stored redundantly on a minimum of six servers.

The reader is not able to create any media to prevent tampering.

Media Storage and Privacy

One of the most remarkable parts of this process is that it has circumvented the need for any outside entity, including VideoLock, from requiring access to private media. Private videos, photos and audio recordings can remain truly private. They are never transferred from a smart phone unless the user chooses to share. Only encrypted metadata and a one-way hash of the media is required to be shared, leaving no chance to determine the actual content in the media – only that it has not been manipulated.

VideoLock offers the ability to upload and store media on its servers. The media can remain private or be shared publicly. Media can also be shared directly from the app.

The Future

There are intriguing ways to continue developing this technology. The amount of new data VideoLock collects, combined with the astounding accumulation of available video online creates an environment ripe for artificial intelligence applications. Properly applied to these datasets, machine learning will give us blueprints for new weapons to combat digital deception.

VideoLock engineers are currently using steganography theory to develop a first-of-its-kind technology that will graft immutable metadata directly to a media file.

Deepfakes are a frightening spectre, but VideoLock by DeepTruth continues to work toward a future where truth cannot be threatened by manipulation.