Deepfake Solution Provided by ImageKeeper's Certified Media Technology

ImageKeeper's patented technology, Certified Media, is the best way to safeguard against deepfakes, manipulated photos, and fraudulent digital media.

LAS VEGAS, NEVADA, UNITED STATES, August 25, 2021 /EINPresswire.com/ -- ImageKeeper LLC today announced that its patented technology, Certified Media, is the best way to safeguard against deepfakes, manipulated photos, and fraudulent digital media. Certified Media is incorporated into all ImageKeeper apps and available now in the Apple App store,

Authentication
ImageKeeper's unique approach is organic; authentication occurs completely within the camera during image capture with no need to send media back to the cloud, or some remote server, to be processed and requires no external intervention.

Competing authentication schemes perform forensic testing after capture and after the images have been transmitted to a remote server. Photo data is collected, transmitted to a cloud server, analyzed, and a response generated. This approach's shortfall is speed, accuracy, chain-of-custody, and security.

The oldest, more common approach is to process existing photos for authentication after using server processing. This forensic approach is flawed because it assumes that the image or media being used is original. Any information available in the metadata, such as time, date, GPS coordinates, etc., is assumed to be accurate. Because the context and chain-of-custody history is missing, there is no guarantee that this approach will ever be successful, particularly when one considers the trillions of photos and video that currently exist online today. Again, the best practice is to secure the original by using Certified MediaTM.

Certified Media Technology
The ImageKeeper authentication process incorporates Certified Media technology into all its mobile apps. The technology works on all forms of digital media (digital photos, video, and audio) and is used the same way as standard media. Each authorized user, user group, or corporation has secure system access to their certified data. App users can verify media authenticity whenever the need arises by using tools built into the mobile app, the ImageKeeper website or any smartphone with a camera that can detect a QR Code.

ImageKeeper technology is easily integrated into corporate IT operations as it uses standard industry interfaces. It can also be integrated into any digital capture device such as smartphones, tablets, laptops, wearables, drones and more.

Certified Media technology supports Department of Justice (DOJ) Federal Rules of Evidence (FRE) Rule 902 Self-Authentication of Evidence. All photos, video, and audio recordings captured using Certified Media will have high evidentiary value in legal proceedings: the user will have irrefutable evidence that an event happened at a precise date, time, location, elevation, angle your device was pointed, user identity, and more. With Certified Media, it's easy to confirm that media hasn't been altered, should the need arise. More information about Certified Media is available at https://www.imagekeeper.com.

Deepfake Problem Getting Worse
According to the FBI's recent Private Industry Notification (PIN) 210310-001, dated 20 March 2021, the threat of being victimized is real and growing with the proliferation of Deepfakes, manipulated video, and edited photos.

The explosive proliferation of deep fakes is not likely to be slowed by Government regulation or intervention either. In two recent Supreme Court cases, the Court determined that telling a lie, posting a deepfake, is protected by the First Amendment. If the deepfake harms you or your business, the platform it was posted on, i.e., Facebook, Instagram, Twitter, etc., is not liable due to the 1996 Communications Decency Act; Sect. 230, which grants online planforms civil liability immunity. Depending on the platform's policy, they may have a procedure to examine and remove an offensive post, but it is highly subjective. The only recourse is for the victim to pursue a tort-like approach of proving civil defamation (i.e., libel, slander) and associated harm against the individual(s) or business responsible for creating the post. This places an unfair burden on the victim to prove and quantify the damage created by the deepfake, often months to years after the post and at great expense. Existing laws don't adequately protect the victim. The best way to protect oneself or organization is to use authenticated Certified MediaTM.

About ImageKeeper, LLC
ImageKeeper is an imaging system company headquartered in Las Vegas, NV. The company began in 2013. The company founders developed and patented Certified MediaTM and more. Their technology supports hospitality, insurance, public safety, medical, and other business sectors. For more information or to contact the company, please go to www.ImageKeeper.com

Marc Roberts
ImageKeeper
mroberts@imagekeeper.com

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.