August 26, 2019

MEDIA AUTHENTICATION VIA BLOCKCHAIN

Logan Sweet

MEDIA AUTHENTICATION VIA BLOCKCHAIN

ABSTRACT

Computing devices often include media capture devices, such as cameras, video recorders, and/or microphones. Advances in computing, particularly in artificial intelligence (AI), are enabling computing devices to modify or alter media (e.g., images, video, or audio), or even create such media (also called deepfakes), such that it may be difficult to determine whether the media is authentic or legitimate. As described herein, when capturing media, a switch built into the software media-capture operating system enables a computing device to selectively generate a unique fingerprint for the media, for example, by means of a hash function, a checksum, or other function. Alternatively, with user consent, the computing device may automatically generate a unique fingerprint for the media. The computing device may store the fingerprint within a distributed ledger or blockchain managed by a computing network, which may also be referred to as a consensus network. If another computing device later seeks to authenticate the media, the computing device generates a new fingerprint for the media and compares the new fingerprint to the fingerprint stored within the distributed ledger. The computing device determines a media file is genuine or legitimate when the new fingerprint matches the fingerprint stored within the distributed ledger. The computing device determines that a media file is inauthentic, illegitimate, or fake when the new fingerprint does not match the fingerprint stored within the distributed ledger.

DESCRIPTION

Techniques are described that enable a computing device to selectively generate a fingerprint for media captured by the computing device and to store such fingerprints to a distributed ledger maintained by a consensus network. In the example of FIG. 1, computing system 1 includes

computing device 2, computing device 10, and consensus network 20. Consensus network 20 includes a plurality of computing devices 22A-22N (collectively, computing devices 22), which may also be referred to as nodes.

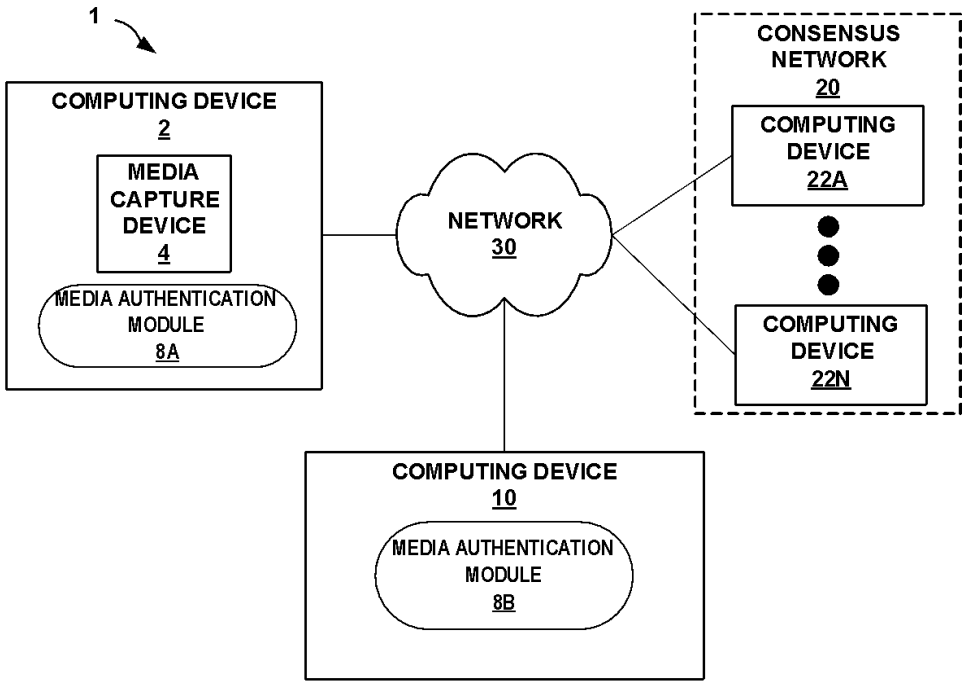

FIG. 1

Computing devices 2, 10, and 22 are communicatively coupled to one another via network 30. Network 30 represents any public or private communications network, for instance, cellular, Wi-Fi, and/or other types of networks, for transmitting data between computing systems, servers, and computing devices. Network 30 may include one or more network hubs, network switches, network routers, or any other network equipment, that are operatively inter-coupled and thereby provide for the exchange of information between computing devices 2, 10, and 22. Computing devices 2, 10, and 22 may transmit and receive data across network 30 using any suitable communication techniques, such as via a via a cellular network (e.g., GSM, CDMA, LTE, etc.), via Wi-Fi®, or any other wireless and/or wired communication techniques.

Computing devices 2, 10, and 22 may include any type of computing device capable of communicating with another device over a network, such as a desktop computer, a laptop computer, a tablet computer, a smart watch, a smart speaker, a server, or any other type of computing device. Computing devices 2, 10, and 22 include one or more processors. Examples of processors include, but are not limited to, digital signal processors (DSPs), general purpose microprocessors, application specific integrated circuits (ASICs), field programmable logic arrays (FPGAs), or other equivalent integrated or discrete logic circuitry.

Media authentication modules 8A and 8B (collectively, media authentication modules 8) of computing device 2 and 10, respectively, may perform operations described using hardware, hardware and software, hardware and firmware, or a mixture of hardware, software, and firmware residing in and/or executing at one of computing device 2 and 10, respectively. Computing devices 2 and 10 may execute modules 8 with multiple processors or multiple devices. Computing devices 2 and 10 may execute modules 8 as one or more services of an operating system or computing platform, or as one or more executable programs at an application layer of an operating system or computing platform.

In some examples, media authentication modules 8 may include a software application. In such examples, media authentication modules 8 may be a native application or a web-based application. Native applications may be provided by a developer of an operating system of computing devices 2, 10 or by a third-party developer, and may be pre-installed or downloaded via an application market.

Throughout the disclosure, examples are described where a computing device and/or a computing system analyzes information (e.g., audio, images, and/or video) associated with a computing device and a user of a computing device, only if the computing device receives

permission from the user of the computing device to analyze the information. For example, in situations discussed below, before a computing device or computing system can collect or may make use of information associated with a user, the user may be provided with an opportunity to provide input to control whether programs or features of the computing device and/or computing system can collect and make use of user information (e.g., information about a user's current location, current speed, etc.), or to dictate whether and/or how to the device and/or system may receive content that may be relevant to the user.

In addition, certain information may be treated in one or more ways before it is stored or used by the computing device and/or computing system, so that personally-identifiable information is removed. For example, a user's identity may be treated so that no personally identifiable information can be determined about the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over how information is collected about the user and used by the computing device and computing system.

Computing device 2 includes a media capture device 4 configured to capture images, videos, and/or audio. Examples of media capture device 4 include a microphone and/or an image sensor (e.g., a camera or video recorder). Media authentication modules 8 may selectively authenticate media captured by media capture device 4.

As illustrated in FIG. 2, a user of computing device 2 may utilize computing device 2 to capture video of a speaker giving a presentation or other event where authenticity of the media may be important or called into question. Additional examples of events where the authenticity of media may be important or called into question include a vehicle collision, a potential crime, a

political event, among many others. In one example, the user of computing device 2 may utilize computing device 2 to capture video of a child's birthday party, images while the user is on vacation, or other media where media is intended for private consumption and/or where authenticity of the media is less likely to be important.

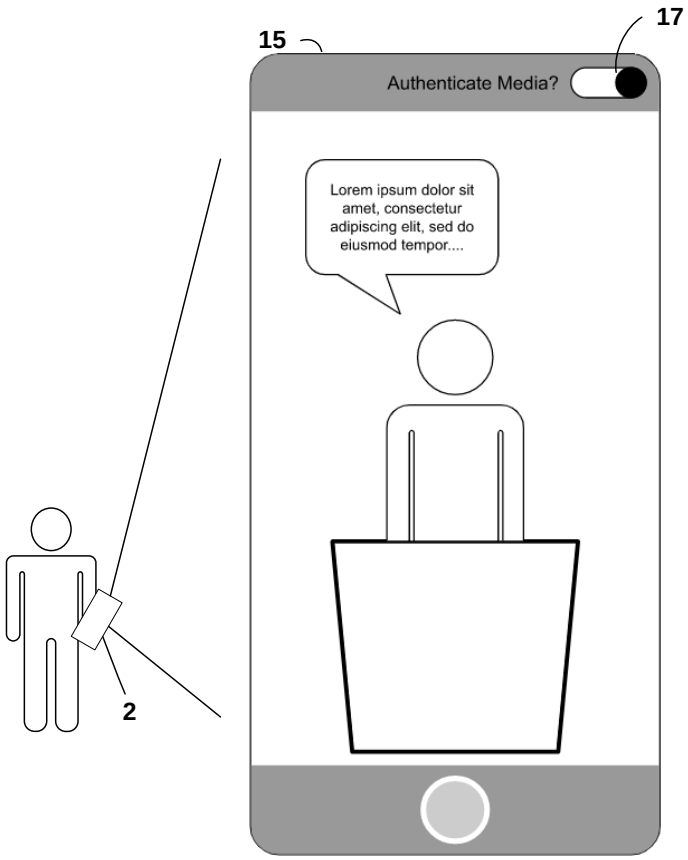

FIG. 2

In some examples, media authentication module 8A outputs a graphical user interface 15 for display via a display device of computing device 2 while capturing media. In the example of FIG. 2, graphical user interface 15 includes a graphical element 17 that enables a user to select whether to cause computing device 2 to authenticate media captured by media capture device 4. In the example of FIG. 2, graphical element 17 is illustrated as a toggle. In other examples, graphical element 17 includes a checkbox, slider, button, or other graphical feature that enables

the user to select whether computing device 2 should authenticate the media. In other examples, a user may perform a gesture, such as a swipe, to select whether to cause computing device 2 to authenticate media.

Computing device 2 may receive a user input from the user to select an option to authenticate the media. In the scenario illustrated in FIG. 2, media capture device 4 may capture media (e.g., images, video, and/or audio) of the speaker as he or she speaks and media authentication module 8A may generate a fingerprint of the media. For example, media authentication module 8A may apply a hash function, a checksum function, or other function to the media and/or the metadata for the media to generate the fingerprint.

Responsive to generating the fingerprint, media authentication module 8A outputs or transmits the fingerprint to one or more computing devices 22 of consensus network 20. In one example, media authentication module 8A outputs the fingerprint to computing device 22A which may propagate the fingerprint to other computing devices 22 of consensus network 20. Each of computing devices 22 validates the fingerprint and store the fingerprint to the distributed ledger stored by each of computing devices 22.

Computing device 10 may receive a copy of the media captured by computing device 2. For example, a news organization may receive media via computing device 10 for distribution via a website, television program, or other medium. As another example, a judiciary may receive media as evidence in a court proceeding. In another example, a media curator (e.g., a music and/or video streaming service, a social media website, etc.) may receive media via computing device 2 for publication via the internet.

Media authentication module 8B of computing device 10 may determine whether the media is authentic. For example, media authentication module 8B may generate a fingerprint of

the media and may compare the fingerprint to the fingerprint stored within the distributed ledger stored by computing devices 22 of consensus network 20. In one example, media authentication module 8B determines the media is inauthentic (e.g., has been altered) in response to determining that the fingerprint does not match the fingerprint stored within the distributed ledger.

In some instances, media authentication module 8B determines the media is authentic in response to determining that the fingerprint matches the fingerprint stored within the distributed ledger stored by computing devices 22. For instance, a judiciary may determine the media is authentic and allow the media as evidence in a court proceeding. In another instance, a news organization may determine the media is authentic and may publish the media to a website or broadcast the media on television. In yet another instance, a media curator (e.g., a social media website) may publish the media to an online platform.

REFERENCES

1. U.S. Patent Publication No. 2017/0,206,523 entitled “Systems and methods for digital asset security ecosystems” by Goeringer, et al.

2. Truepic, https://truepic.com, last accessed July 30, 2019.