International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT217372

Blockchain Based Approach for tackling Deepfake videos

Ujwal Patil[1], Prof. P. M. Chouragade[2]
[1]M.Tech ,Computer Science and Engineering, GCOE, Amravati, Maharashtra, India
[2]Assistant Professor, Computer Science and Engineering, GCOE, Amravati, Maharashtra, India

ABSTRACT

Article Info
Volume 7, Issue 3
Page Number: 342-347

Publication Issue :
May-June-2021

Article History
Accepted : 20 May 2021
Published : 25 May 2021

The technological advancements and a qualitative improvement in the field of artificial intelligence and deep learning leads to the creation of realistic-looking but phoney digital content known as deepfakes .These manipulated videos can quickly be shared via social media to spread fake news or disinformation which not only impacts those who are deceived it also harms social media sites by diminishing faith.These deepfake videos cannot be checked since there are no regulatory mechanisms in place .As a result these untrustworthy outlets will post whatever they wish causing confusion in society in some ways.Current solutions are unable to provide digital media history tracing and authentication it is essential to develop successful methods for detecting deepfake video as a result it is necessary to determine the source or origin of such deepfake footage.That's why we are implementing blockchain techniques to trace back and determine the origin of digital media blockchain techniques helps in the effective recognition of deepfake video and calculating the trust factor of user.

Keywords: Deepfake ,AI, Blockchain, IPFS Storage, Deepfake videos

I. INTRODUCTION

Recently, Artificial Intelligence (AI) has been used to develop advanced deepfake .The term 'deepfake' is the union of 'Deep learning' and 'fake' It is a strategy that allows someone to substitute an individual's original face with a new face, including their expression, which is not recognized by the human eye.In April 2018, a one-minute video of former US President Barack Obama went viral, in which Obama was seen saying things he had never said before[1]. It was speculated that this was done for political reasons.

Deepfake videos are much more convincing and far easier to create than standard Hollywood-style fake videos, which are usually created manually using image editing software such as Adobe Photoshop. Deepfake videos use deep learning methods with massive samples of video images as input to perform face switching. The greater the number of samples, the more realistic the result As a result, if kept unnoticed, exponential proliferation of such content has become uncontrollable, likely exacerbating fraud and treachery hypotheses. Deepfake video is becoming one of the most serious obstacles to democratic system, media, and freedom of speech. Researchers say that, while widespread information is challenging to supervise, the tracing of data, networking architecture, and interactions can be monitored. It takes a lot of time for people to test the authenticity of recordings. Deepfake videos are created by users with malicious intent who change the content of legitimate videos to spread false facts. It is essential to have strategies in place to identify, fight, and tackle deepfake content such as fake videos, photographs, drawings, audio recordings, and so on. It is not difficult to achieve this goal if there is a credible, stable, and trustworthy method for tracing the history of digital information.

There are no proven mechanisms for determining the authenticity of a digitally uploaded video file, audio, or photograph as of today.When it comes to deepfake, prominent technology such as blockchain will come to the fore to provide certain levels of authentication, acceptance, and validation.There are currently no proven methods for determining the authenticity of an electronically uploaded or published digital video, audio, or photograph.

To address this problem, decentralized technologies must be used.In blockchain technologies, such functionality is readily available.The application of blockchain technology is vast, with the technology ready to shape and influence a wide number of industries, markets, and sectors, including organic food supply chain management[11] ,medical healthcare [12], and IoT [13], and many more. .When it comes to deepfake, prominent technology such as blockchain will come to the fore to provide certain levels of authentication, acceptance, and validation. As a decentralized distributed ledger, blockchain has the potential to provide secure and tamper-proof information and transactions.Blockchain has the ability to include core functionality that can be used to prove the authenticity and originality of digital objects in a decentralized, highly trusted, and stable manner. The blockchain technology can be used to track the sources and legitimacy of video.

II. LITERATURE SURVEY

In this paper[2] Li and Lyu have proposed a technique to spot deepfake by utilizing Artificial intelligence.This process is utilizing deep learning technique which can successfully differentiate deepfake videos from an authentic one. Their approach depends on drilling CNN with fake and genuine video.CNN can be used to disclose artifacts by differentiating the generated face areas and their surrounding provinces. Previous methods have used a huge quantity of authentic and fake videos to drill cnn, but this technique does not require deepfake images as negative training. They chose the artifacts in affine face wraping as a unique characteristic to differentiate between authentic and hoax images. Their outcome looks positive but still, the researchers declared many objections that have not been solved.Hence they assume that videos having high quality and resolution will be difficult to expose.

In[3] authors have introduced a technique which uses deep neural network to detect forgery in videos.In this method counterfeiting video identification depends on eye blinking.The absence of eye flickering is a key indicator that the images are not from a camera recorder .The technique they provided is divided into two parts pre-processing which comprises face extraction and orientation and also the LRCN model.
The LRCN model is composed of three parts: to predict the probability of an eye opening and closing, feature extraction is deployed using CNN, and sequence learning is introduced using an RNN in combination

with an LSTM and a state prediction based on a fully connected layer.Since eye blinking has high temporal dependencies LSTM implementation helps in accurately capturing these temporal patterns.

In this paper[4] authors have introduced a system to spot deepfakes using inconsistent head poses. In this method, an individual video frame is fed into a face detector. The face detector makes use of a software package to extricate sixty-eight facial landmarks. The extricated facial landmarks are compared with normal landmarks. The head poses from the center and the entire face is calculated. The acquired variations are compacted into the vector . After that, additionally trained SVM classifiers are fed into the resultant vector to examine whether the videos are hoax or real.

In this paper[5] authors have suggested the idea of using blockchain technique to maintain the integrity of video footage.In this approach they have used smartphone which acts as dashboard camera in vehicles.Whenever a accident takes place phones built-in sensors like accelerometer records the collision and the hash of the recorded video is saved in bitcoin blockchain.Bitcoin ledger has been utilized by the researchers to timestamp a video footage recorded by smartphone at the time of accident. Any attempt to distort the video is simply recognized by matching the current hash of the video with the trustworthy hash value of the blockchain .

In this paper[6] author have proposed a method for validating the video captured by devices like mobile phone,laptop, accoutered with camera and managed by operating system.The proposed algorithm uses the moving mobile camera to enter the swype code. Use additional information from various mobile sensors like accelerometer, gyro, barometer and GPS, to increase its accuracy. Video transmission to the server does not ensure the privacy of the video data that has been captured during data verification. Data about the file size, the time, the data device and the file position can be stored on the server and the mobile device. This method utilizes prover technology to ensure that this content was created from a device camera at a certain time or place to ensure no signs of falsifying and editing are present. This approach doesn't have a method to trace a video.

In [7] presents that Original my a start- up company which uses decentralized technique to recognize genuineness of electronic documents ,verify identities, sign a contract..However, origin of video cannot be traced.

Aditya Dhiran et al.[8] have proposed a system to detect fraud in videos. It explained how video fraud can be detected by cryptography and blockchain technologies. This approach uses algorithms like MD5 and AES to create video hash security to provide security.Each node includes video hash and also hash of its previous node, which acts as Blockchain. However the video source cannot be traced by this tool.

Serelay [9] is another UK-based startup that uses a technology to eliminate the dissemination of deepfake video clips and photographs. Serelay enables users to take pictures and video clips in a manner that is verifiable and secure.Serelay does not save the pictures and video clips on its servers – authentication data is the only thing it save. Serelay is also a smartphone app to use for capturing photographs and videos.It then produces a specific unique fingerprint and, unlike Truepic, preserves the entire image in its servers. Serelay says its method will safeguard its users' privacy. They also state that a computed fingerprint will detect any pixel edited in the original image. The program is centrally regulated. Their approach is based on the trust that Serelay acts sincerely and does not interfere with the calculated fingerprints and outcomes.

In this paper[10] author has suggested an approach to check the integrity of video on the video manipulated file structure. Since the file structure created using video editing software is stored in a database in the form of a signature, it is only possible to identify tampered files that have structures saved in the database. Therefore, the device does not detect any video that is edited using a proprietary method instead of using a normal editor.

III. PROPOSED METHODOLOGY

The proposed methodology uses Blockchain mechanism for fighting against deepfake videos.The proposed model mainly comprises of following key components; Owner,video,IPFS

Owner : Original artist who is responsible for creating the video.

Video: A video contains necessary data in addition to the video frames. In the (Exchangeable Image File) EXIF format, key attributes of video are saved as 'Metadata.' The metadata of a video includes details about the system used to record the video, the capture parameters, and the time and date of capture.

IPFS Storage: The video and the metadata related to it are stored on the Inter Planetary File System, a peer-to-peer, decentralized, content-addressable network. This storage system produces a unique hash that acts as the identifier for a set of video files and metadata. The hash key is then used to find and manage the package of files.

BLOCKCHAIN : Series of records that are interconnected to each other, is known as Blockchain.Once data is stored it cannot be modified.In our solution hash of the original video is stored on blockchain.

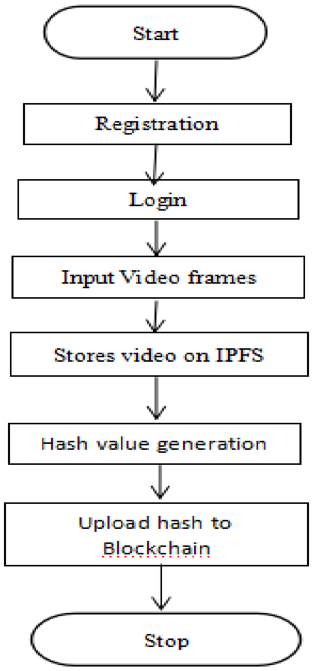

Figure 1. The Signing Actors and Process

The original artist known as the trustful owner creates input video.The original artist must register on Distributed File System (IPFS). The initial video is taken as the input after the registration is completed. The video frames and their metadata are stored on IPFS, and for each video, hash is created. The hash value is then stored on a blockchain.

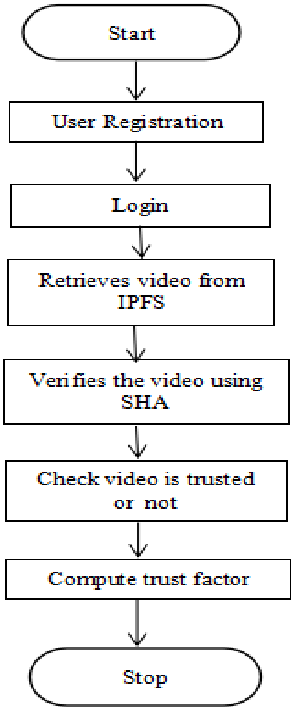
Start
User Registration
Login
Retrieves video from IPFS
Verifies the video using SHA
Check video is trusted or not
Compute trust factor
Stop

Figure 2. Video Verification Process

Figure 2 indicates the video verification mechanism . As shown in figure 2 users can retrieve or download videos that are saved on distributed file systems(IPFS) for checking the validity of videos . These users will post the video on social networking sites . Once content is posted on social media, a scalable verification mechanism is applied for verifying whether the uploaded video is trustworthy or not . If the blockchain's hash key does not fit the video's hash key, we may assume the user deceives the video. The user trust factor is determined accordingly.

IV. CONCLUSION

The increase in the number of false videos and how quickly they circulate across the world are seriously concerned.This paper introduces a new method for detecting and preventing the further dissemination of misleading information and validating the original facts.In this article, we proposed a blockchain approach to demonstrate the validity of videos, which establishes a secure and reliable tracing in a fully decentralized fashion to the actual video creator .Our approach enables social media consumers to access trustworthy information from digital content to track the data and to be certain that the data is genuine.

IV. REFERENCES

[1]. How Faking Videos Became Easy — And Why That's SoScary[Online].Available:https://fortune.com/2018/09/11/deep-fakes-obama-video/

[2]. Li, Yuezun and Siwei Lyu."Exposing DeepFake Videos By Detecting Face Warping Artifacts." ArXiv abs/1811.00656 (2019)

[3]. Y. Li, M. Chang and S. Lyu, "In Ictu Oculi: Exposing AI Created Fake Videos by Detecting Eye Blinking," 2018 IEEE International Workshop on Information Forensics and Security (WIFS), 2018, pp. 1-7

[4]. X. Yang, Y. Li and S. Lyu, "Exposing Deep Fakes Using Inconsistent Head Poses," ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2019, pp. 8261-8265

[5]. Gipp, Bela et al. "Securing Video Integrity Using Decentralized Trusted Timestamping on the Bitcoin Blockchain." MCIS (2016).

[6]. A. Zelensky, V. Voronin, E. Semenishchev, I. Svirin and A. Alepko, "Video Content Verification Using Blockchain Technology," 2018 IEEE International Conference on Smart Cloud (SmartCloud), 2018, pp. 208-212.

[7]. ORIGINALMY[ONLINE]Available:https://originalmy.com/

[8]. A. Dhiran, D. Kumar, Abhishek and A. Arora, "Video Fraud Detection using Blockchain," 2020 Second International Conference on

Inventive Research in Computing Applications (ICIRCA), 2020, pp. 102-107

[9]. SERELAY[Online].Available : https://www.serelay.com/

[10]. Song, Jieun & Lee, Kiryong & Lee, Wan & Lee, Heejo. (2016). Integrity verification of the ordered data structures in manipulated video content. Digital Investigation. 18.

[11]. B. M. A. L. Basnayake and C. Rajapakse, "A Blockchain-based decentralized system to ensure the transparency of organic food supply chain," 2019 International Research Conference on Smart Computing and Systems Engineering (SCSE), 2019, pp. 103-107

[12]. E. Daraghmi, Y. Daraghmi and S. Yuan, "MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management," in IEEE Access, vol. 7, pp. 164595-164613, 2019

[13]. D. A. Noby and A. Khattab, "A Survey of Blockchain Applications in IoT Systems," 2019 14th International Conference on Computer Engineering and Systems (ICCES), 2019, pp. 83-87

Cite this article as :

Ujwal Patil, Prof. P. M. Chouragade, "Blockchain Based Approach for tackling Deepfake videos", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 3, pp. 342-347, May-June 2021. Available at doi : https://doi.org/10.32628/CSEIT217372
Journal URL : https://ijsrcseit.com/CSEIT217372