Blockchains and Cryptographic Hashes to Regulate the Proliferation of Deepfakes

Ahmed Hussain
Computer Engineering, Physics (2023)
ahh6qxu@virginia.edu

Zachary Yahn
Computer Engineering, CS (2023)
zry2yz@virginia.edu

September 12, 2023

Introduction

Deep learning, a branch of machine learning based on artificial neural network architectures, has been applied to many complex problems in the modern age. Ranging from robotics to computer vision to data analytics, applications of deep learning have typically resulted in significant advances in both performance and speed. However, advances in the field of deep learning have also been used to threaten privacy, democracy, and security. An example of these recently emerging deep learning applications is the "deepfake." Deepfake algorithms can create artificial images, video, and audio which are almost impossible for humans to differentiate from real media. This presents threats to our technological lifestyles and media-dominated culture through the possibility of malicious intervention and cybersecurity risks. Therefore, in this whitepaper we propose an end-to-end blockchain solution which can automatically detect and assess the integrity of digital media using video hash functions. By using both technical and conceptual details and covering modern examples, we present an introduction to deepfakes, an overview of generative adversarial networks, our proposal for a detection framework, and a summary of potential future research.

Deepfakes and Cyberwarfare

Overview

A deepfake[1], the portmanteau of "deep neural network" and "fake", is a form of media, typically in video or audio form, which modifies a subject's face, body, or voice digitally using deep learning models to appear to be someone/something else. In the past, deepfakes have been used to spread malicious or false information online through social media or other mass forms of communication to interfere with public discourse. There is also a distinction between a deepfake, which uses deep neural networks (DNNs) to forge the media, and a "shallowfake" or "cheapfake", which aims to achieve the same end result using standard video editing or programming techniques.

Deepfakes are built using two machine learning models, specifically deep neural networks, which compete with each other to produce high quality media. This machine learning technique of competing neural networks is called a generative adversarial network[2], or GAN.

Ethics and Controversy

For better or worse, deepfakes have found their place in news headlines and social media posts. One popular example is the portrayal of recently passed actors and actresses on the big screen using algorithmically recreated faces[3]. Deepfakes have also caught the attention of everyday people through mobile applications like FaceApp[4], which allow a user take a picture of a face and morph it with different features. Video deepfakes are even more common than initially thought, as companies like Apple and Snapchat implement advanced camera filters that can be used to modify faces and objects in real time. In terms of audio, one

startup, CereProc[5], was able to restore the voice of Roger Ebert, who suffered from ALS, and use it to say anything in real time. This synthetic audio technology is only improving, giving many people a voice of their own for the first time in their lives.

However, deepfake technology has also been used to great effect by malicious actors, such as convincing a UK-based energy firm to transfer funds to a fraudulent account. This was accomplished by creating an audio deepfake[6] of the CEO's voice and calling company executives. Others have attempted similar approaches, employing the same technology for spam calls and fake audio messages. While a trained eye or ear can sometimes spot a fake, the technology could become advanced enough to fool most people.

Target Issue

Perhaps the most dangerous application of deepfakes is the widespread dissemination of fake news and distrust in the media, sometimes dubbed as "5th generation cyberwarfare[7]" due to the large scale, multi-vector attacks designed to infect many components of an information infrastructure. As deepfakes work best with ample training data, any politician, celebrity, or public figure with videos online could potentially be targeted by a deepfake. A prominent example of a deepfake was Jordan Peele's demonstration of the technology when he used GANs and voice acting to create an entirely fake video of President Barack Obama[8]. Similarly, an example of a shallowfake in popular media is Nancy Pelosi's speech at the CAP Ideas conference in 2019[9]; the original video of the speech was taken and altered using typical editing techniques to slur her words and reduce her speech coherence.

It is difficult to know when a viral video is real, as the vast amounts of potential training data made available with every public appearance makes these individuals vulnerable targets for powerful models. In one significant example of public distrust due to this technology, the government of Gabon was overthrown in a coup after the sitting president addressed the country[10]. Broadcast as a live video to the entire nation, the address was perceived as a deepfake, partially contributing to an uprising. While several sources have confirmed that the video was not a fake (the president had recently suffered a stroke that made his facial features seem artificial), the possibility was enough to spark resentment for the populace.

As personal computers become increasingly powerful, the danger of deepfakes only grows. Anyone with an internet connection and knowledge of deep learning can produce a semi-convincing deepfake of politicians and public figures, with the potential to sow mass confusion. Social media spreads information - true or false - at a breathtaking pace perfect for fake media. Researchers have already developed several methods for combatting deepfakes, though there is still room for improvement. As it becomes ever harder to know which media to trust, there is a demand for new technologies which restore the public's confidence in the information they consume.

Current Detection and Deterrence Methods

Almost all anti-deepfake solutions focus on training a machine learning model of some sort to identify or disrupt deepfakes. For example, one paper by Rana et al.[11] describes an ensemble of deep learning algorithms that demonstrate 99.65% accuracy for identifying deepfakes based on their own test data set. Another team led by Ciftci et al.[12] developed a convolutional neural network which achieved 99.63% accuracy by identifying biological errors in deepfakes, like unblinking eyes or out-of-sync lips. Other common deep learning architectures are also seeing use, such as in a paper by Guera et al.[13] that explores a recurrent neural network method. Without a doubt, neural networks are a useful tool for identifying deepfakes, but due to training and implementation difficulties they are not enough to solve the problem single-handedly. Each network requires thousands of training examples, high-end computing, and, most importantly, time. These networks are also exclusive to one organization, so there doesn't exist a global framework in place for the large-scale suppression of deepfakes.

Instead of training models to identify deepfakes, some researchers have developed adversarial methods for producing images and video that cannot easily be modified by GANs and other deepfaking algorithms. In a paper by Segalis et al.[14] a GAN is trained to produce images that induce blurry artifacts when used for training by a deepfake-creating GAN. While the image looks normal to the human eye, any algorithm that tries to process it into a deepfake gets disrupted by subtle embedded data manipulations. Once the model is trained, it can be applied to images and videos before they are published, so that they cannot be

manipulated or used to train a deepfake GAN. This kind of adversarial technique is promising in some cases, like protecting a specific speech from modification, but it does not protect the vast amounts of unfiltered media already published on the Internet that can be used to train successful deepfake models.

While most technical approaches involve machine learning models of some sort, there are a few other approaches that may lend some insight into the problem. For example, many researchers advocate for education campaigns to teach people about the dangers of believing everything on the Internet. This includes making deepfaked videos of popular figures and using them to spread the message and publishing news articles to warn the public. Informing people is important, but some deepfakes are already too advanced to discern with the human eye. As a result, there is still a need for innovative solutions to the deepfake problem that do not involve machine learning algorithms. But first, developing a solution requires in-depth knowledge of the techniques behind deepfakes and how they are developed.

Generative Adversarial Networks

Overview

GANs, short for Generative Adversarial Networks, were introduced in a paper by Ian Goodfellow, Yoshua Bengio, and other researchers at the University of Montreal in 2014. A GAN consists of two neural networks which are simultaneously trained: a generative model G which develops the end result given a data distribution, and an adversarial model A which estimates the probability that a sample is an original media file or one developed by G. The training procedure for G is to maximize the likelihood of A making a mistake; i.e., the generator's product must become advanced enough in quality such as to make it difficult for the adversary network to detect its differences from a real data input.

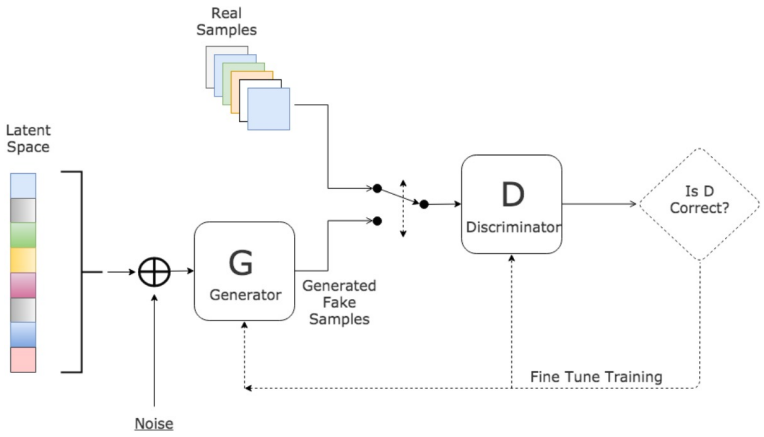

Figure 1: Deepfake generation using GANs.[15]

GANs can be used to create deepfakes, but deepfakes are only a small part of their abilities; using large datasets, GANs can be used to create renderings of imaginary fashion models[16], artificial medical images[17] for testing purposes (like MRI images of brain tumors), and even to generate photo-realistic images from text descriptions[18]. Beyond media generation, GANs have also been proven to work in the context of technical design, as shown in drug discovery[19].

GANs show a form of pseudo-imagination, especially in the context of developing media. GANs need a wealth of training data to get started in media generation, then compute power is necessary for both the G and A models to be sufficiently robust. For instance, without enough pictures of human faces (numbering in the tens of thousands), a model-generating GAN will not be able to come up with new ones. GANs do not invent new things, but merely combine what they already know in different ways.

Figure 2: Deepfakes can mesh a face onto another body to create new media.[20]

Deepfake Development

As previously mentioned, deepfakes are one potential end product of GANs. The generator learns the features of a face, audio file, or object with as much data as possible, then it forges new media. It often has to manually adjust the result after this stage in order to get rid of artifacts. Once this first model has developed an end product, the discriminator model attempts to detect the forged media among the real media. Once forged videos are no longer detected, the deepfake is considered sufficiently realistic.

This process can be broken down into three distinct steps, as described below.

1. *Extraction* : Refers to the process of extracting all frames from these video clips, identifying the faces, and aligning them to be analyzed. Alignment is critical, since the DNN which performs the face swap wants all input images to be the same size (typically 256x256 pixels). Deepfake images take an ample amount of training data, so most people use video clips or long audio files which include the subject in view - this provides hundreds of frames/images or audio data in just a few seconds.

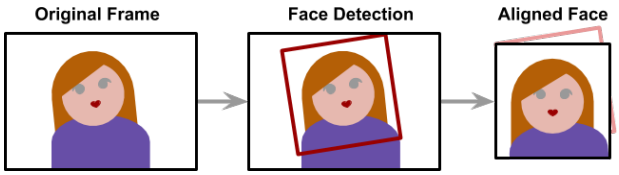

Figure 3: Extracting data to train the GAN is as crucial as actually training it.[21]

2. *Training* : In the case of deepfakes, "training" refers to when a GAN learns to produce increasingly realistic output by pitting the generator against the discriminator; this usually takes a few hours, but only needs to be done once. This step of the process is the main component for developing an application which can generate deepfakes, and requires a substantial amount of labelled training data.

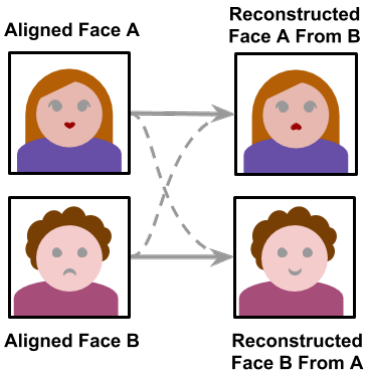

Figure 4: Training the neural network allows it to match the information itself.[22]

3. *Creation* : Starting from a video, all frames are extracted and aligned and each one is then converted using the trained GAN - the final step is to merge the converted face back into the original frame. This is where many deepfakes go wrong, as this process does not use any ML and requires a hard-coded algorithm. Also, each frame is processed independently; there is no temporal correlation between them, meaning that the final video might have some flickering. This flickering is often used by other algorithms to detect deepfakes.

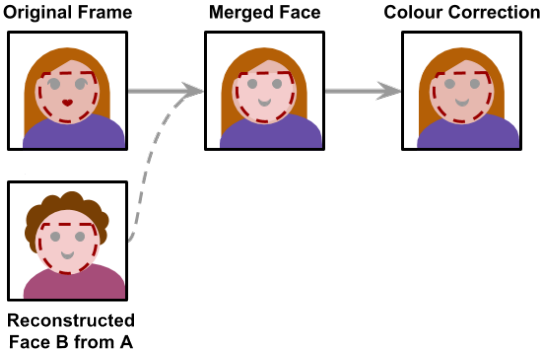

Figure 5: Creating the final product involves meshing the target and source data.[23]

Solution: Blockchains and Cryptographic Hashes

Executive Summary

We propose in this whitepaper a novel end-to-end framework for finding video deepfakes of frequently-targeted actors, such as politicians and celebrities, using the blockchain and a novel cryptographic video hash function. While most deepfake prevention and detection literature focuses on training algorithms like deep neural networks to identify modified media, this approach can be time-consuming and expensive. These algorithms can be very effective, but training one is tedious and resource-intensive; in order to create an automated system which quickly and automatically categorizes a video as fake or real, neural network techniques should be considered a final "catch-all" for the most technically difficult media. Instead of every detection organization honing their own algorithm, this paper outlines a solution for verifying videos and images on the internet as quickly and accurately as possible through collaboration, only relying on machine learning algorithms when absolutely necessary.

Our solution uses a blockchain method which incorporates an efficient media hashing algorithm to determine real videos. Whenever a video is uploaded to a platform's website or channel by a publisher, it is hashed by a video hashing algorithm that produces a unique signature for the video; this algorithm can later be used to identify if two videos are the same through their signatures. Once the publisher wishes to publish

media, its hash is saved in the public blockchain ledger which contains all the publisher's previous video hashes. Distributing platforms (such as news networks, social media companies, or independent journalists) can all contribute to the same public ledger. To prevent fraudulent additions to this blockchain, only verified and trusted distribution platforms will be able to contribute to the blockchain, specifically for new additions or when the original video is modified through new encoding or editing for distribution. Figure 6 shows an example of what this would look like: once C-SPAN has submitted an original video and trusted sources wish to verify their edited version, they compress their own clips and upload them to the linked list block for their video (Video 1 version are connected as one linked list block, while Video 2 below is another block, etc.), and this clip is now verifiable and accessible for everyone. In other words, every clip created from the same source video will be connected to provide rapid verification. This process allows for a much quicker process in case, for example, The Atlantic wishes to use the same clip as FOX and can verify it as quick as possible. Note that Figure 6 shows the linked list found in a single block of the blockchain for one video and its derivative clips, not the entire chain.

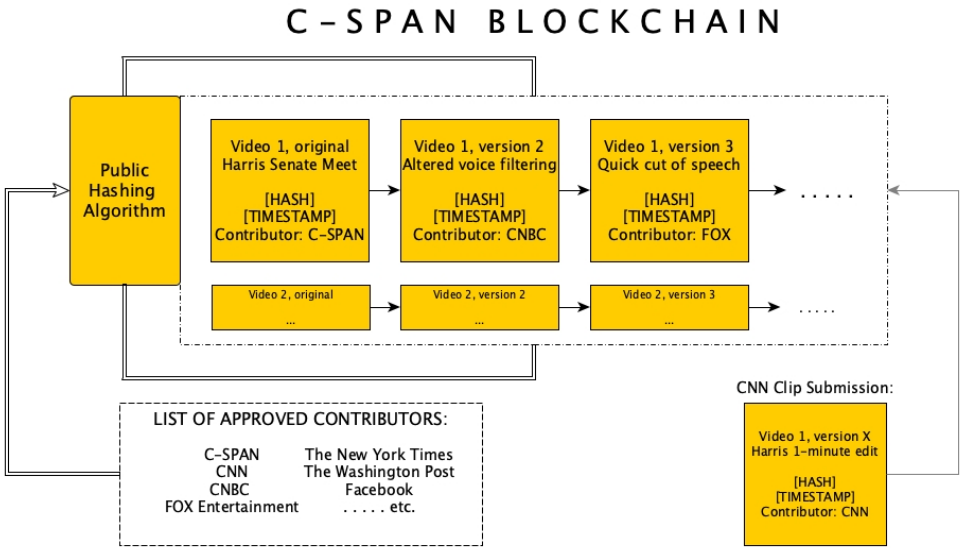

Figure 6: Example of how networks will contribute verified clips to the blockchain.

A blockchain-based solution is useful considering that once something is added to the ledger, it is immutable and publicly-available. If a new video is not already in the ledger, a quick machine learning algorithm like the ones described previously will determine if it is a deepfake. This machine learning algorithm is pre-trained, meaning it is not resource-heavy to use, and will only be used when the video in question does not match any hash on the blockchain; this is useful for when a video on social media has different video encoding, mismatched resolution, or a miscellaneous marking in a corner too. In our solution, there is a decentralized repository of all valid videos that can be quickly referenced by anyone in the world to determine objective validity.

As an illustrative example, suppose the government publishing organization C-SPAN wishes to publish a video of Vice President Kamala Harris presiding over a Senate meeting. C-SPAN will hash the video before publishing and upload that hash, along with its associated hashing algorithm, to its independent blockchain. This hash will be accessible to the public but also technically immutable, which means the timestamp, publisher, and contents will be impermeable to malicious attacks. A trusted list of distributors, which includes companies and organizations like CNN, Twitter, and Facebook, will be allowed to add associated hashes of their own clips. For example, if the news organization Cable News Network (CNN) wishes to modify and distribute a slimmer 1-minute version of the Senate hearing with audio and visual effects, it can hash its own clip using the same algorithm and attach it to the original hash on the C-SPAN blockchain. The purpose of adding the new clip is to allow seamless verification of more widespread versions of the original video; as smaller, more digestable clips of the Senate hearing will likely make their way to social

media networks, these clips can quickly be verified by compressing the new clip and cross-checking the hash with the original video from the C-SPAN blockchain.

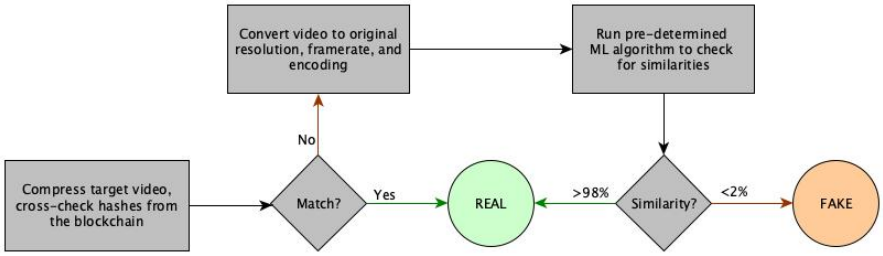

Figure 7: The process for determining if a video is a deepfake.

If an individual wants to know if a video or image is real, there are two possible outcomes: a) the platform that the individual is using (a news website or social media app) has already verified the image or video and listed it as such; b) a simple browser extension can quickly hash the video and check the blockchain database for a match. This way, anyone on the internet can see if a video is legitimate nearly instantly.

The Publisher's Blockchain

A blockchain[24] is an accessible list of records, called blocks, which are linked using cryptographic means and backed-up to multiple databases or computers. Each block contains a hash of the previous block, a timestamp, and transaction data; these block are completely immutable and cannot be altered due to their decentralized nature. We will be using a consortium blockchain, which spreads out its nodes over multiple hosting institutions to guarantee decentralization. Since only a few trusted organizations are allowed to contribute to the blockchain, its decentralized nature protects it from malicious injection of fraudulent hashes. Figure 8 illustrates this nature, where several separately hosted nodes all contain the same information, validating each block in the chain through consensus. In this way, the database can only be modified by organizations that have legitimate access.

Hashes were used for the videos due to their uniquely low time complexity for building and accessing, and the extra clips created by distributors will be inserted into a linked list which allows for resizing and $O(n)$ access time complexity.

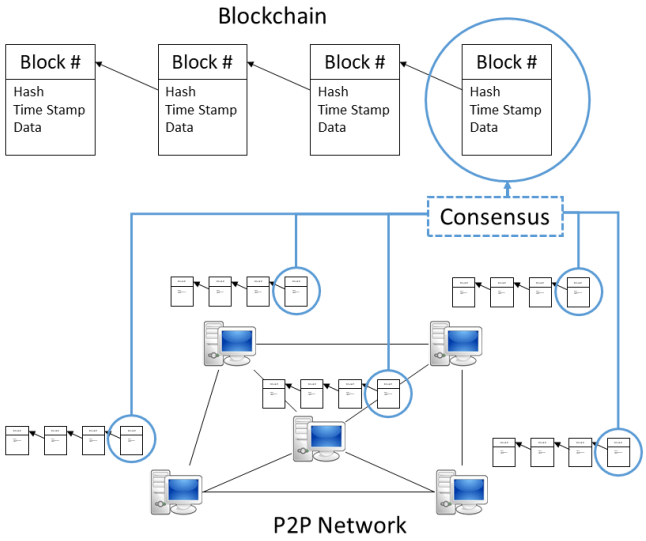

Figure 8: The process of uploading to the blockchain.[25]

At the same time, the blockchain ledger is a public resource that can be accessed by anyone with an internet connection. The ledger can be made accessible to the general public through a browser extension or separate application. These tools are already seeing widespread applications as cryptocurrency blockchain websites[26] and ML-based browser extension fact-checkers, like Reality Defender[27], proving people are comfortable with and capable of their use. Within the context of our solution, a blockchain would be set up and managed by the publishing company or organization.

Cryptographic Video Hash Function

An industry-standard cryptographic hash-based verification is faster and more secure than unique ML algorithms. The video hash function, found in a paper by Wang, et al.[28], can generate a unique hash for an image or video regardless of resolution, size, or other factors. The algorithm builds two sub-hashes: a spatio-temporal hash called an ST-Hash, generated according to the intensity difference between adjacent blocks of the temporally informative representation image, and a visual hash called a V-Hash, formed according to the intensity difference between adjacent blocks of the RSM (a representative saliency map constructed by the visual saliency maps in video segments). The V-Hash modulates the ST-Hash to build the final video hash product to be uploaded to the blockchain.

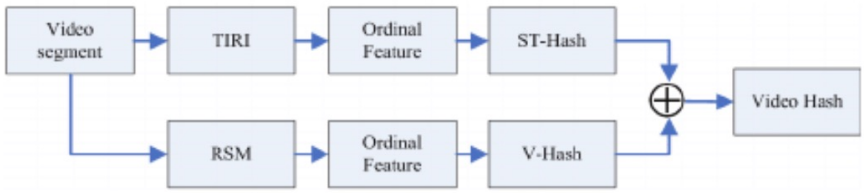

Figure 9: The framework of the proposed algorithm.[28]

The algorithm will also generate the same hash for temporal differences in clips of the same video, meaning videos with temporal differences (frame drops/extensions or minor conversions) do not need to be rehashed and verified if the original video is already part of the blockchain. This addresses the issue of minor differences in frames affecting hash-verification, so innocent social media uploads, which can occasionally affect frame drops and conversion, will not be falsely identified as fake.

Although hashes can theoretically be cracked through brute-force and other methods, this is highly difficult due to the size of the video hash being larger than textual compression, and it is also not useful to attackers as the publishing blockchain will not allow mutations in the hash regardless.

Implementation for Distributors

The majority of media verification will be carried out by any publisher-trusted sources like news networks (e.g. CNN, New York Times, etc.) and other established sources (e.g. Facebook), or independent projects like browser extensions. Many of these organizations, especially news agencies, are already taking steps to verify the content they publish. Not to mention, these groups often record or capture their own content, which means it can be published without verification by an algorithm. With a blockchain solution, different sources can collaborate on verification. Since many news agencies already cite each other in their reporting, using images and videos that are already verified will make the entire process much simpler.

If a social media network receives multiple reports that a video is fake, it can hash the target video and check for any issues with the associated blockchain. If, after checking the hashes, the video doesn't match anything on record, it can use the ML algorithm which checks for video similarity. If the video is deemed to be real, the social media organization can add this new clip to the original video's linked list on the blockchain, allowing it to be quickly accessed in the future.

Advantages Over Prior Art

The most common approach to combating deepfakes by far is other machine learning algorithms. While some have proven to be effective, training these models costs more time and money than many organizations have available. Though a large company like Facebook may be able to dedicate a significant amount of resources towards training their model, a smaller news outlet would struggle. To that end, the cooperative nature of the blockchain helps all platforms share verifications.

These models also consume large datasets of deepfake images or videos to train on. Where this would be a challenge for most individual organizations, the shared blockchain creates an ecosystem that lets platforms work together. Large companies can use the videos that are verified by other large companies to hone their models and do quick verification, while smaller platforms benefit from downloading others' verified videos. This means that all participants benefit from the system, especially the consumers of media. Rather than confining a detecting ML model to a single platform, our framework is implemented onto the web. The problem is not training a new type of model, but making the use of existing models more widespread.

Future Research and Conclusion

It is worth noting that a linked list storage data structure for new clips associated with a single video may be slow to traverse as the number of clips grows to larger proportions, as the worst-case complexity time for most linked lists is $O(n)$. There may be other more efficient data structures like trees or hash tables which can be investigated with further research. The video hash is also much longer than a standard hash, which may lead to storage issues as more and more videos are verified. In addition, though one of the video hash function's advantages is its ability to produce the same hash for videos with slight temporal differences, this may make the system moderately vulnerable to shallowfakes, which can use typical video-editing techniques to manipulate playback speed. There may be more effective hash functions that are not prone to these issues. Lastly, it should be noted that compressing and decompressing whole videos using a visual saliency-based video hashing algorithm could take much compute power, it should also be noted that computer power increases year by year on a consistent and accelerating basis. Further research should investigate more efficient video hashing algorithms, but it is unlikely that, by the time we are no longer able to deter deepfakes in the media, we won't be able to keep up computationally.

In this whitepaper, we presented a novel solution for rapidly verifying potentially deepfaked media on the Internet. By using a public blockchain network which only a select group of trusted sources can contribute to, plus a video hashing algorithm capable of generating unique hashes for images and videos, media can be verified by reference to a ledger of previously-verified hashes. This system is made accessible to anyone through websites and browser extensions, and the blockchain's decentralized nature makes it immune to fraudulent additions. It is an efficient way to connect already effective tools and foster cooperation between media publishing organizations, bringing us one step closer to restoring the veracity of digital media.

References

Faculty Advisors

A special thanks to Professor Mircea Stan (PhD), the Virginia Microelectronics Consortium (VMEC) Professor at the University of Virginia, for offering insightful advice during the solution development process. Mircea Stan specializes in the fields of artificial intelligence, VLSI design, embedded systems and computing, and nanoelectronics.

Another thank-you to Dr. Samiran Ganguly (PhD), research scientist at the University of Virginia's Nano-Computing Group, for noting important distinctions to be made in developing our framework. Dr. Ganguly's specializations include machine learning, spintronics, quantum materials, memristors, photonics, and 2D materials.

Works Cited

[1] (2021, January 4). *Deepfakes.* Wikipedia. en.wikipedia.org/wiki/Deepfake
[2] (2020, June 7). *Generative Adversarial Networks.* Wikipedia. https://en.wikipedia.org/wiki/Generative_adversarial_network
[3] (2018, July 5). *If AI Made Actors Immortal.* The Economist. https://www.economist.com/the-world-if/2018/07/05/performance-anxiety
[4] (2021, January 26). FaceApp. https://www.faceapp.com/
[5] Grossman, W. M., (2011, September 13). *Getting Voice: New Speech Synthesis Could Make Roger Ebert Sound More Like Himself.* Scientific American. https://www.scientificamerican.com/article/new-speech-synthesis-could-make-robert-ebert-sound-more-like-himself/
[6] Stupp, C. (2019, August 30). *Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case.* The Wall Street Journal. https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402: :text=Catherine%20Stupp
[7] (2019, October 5). *How Are 5th and 6th Generation Cyberattacks Different From Pervious Ones?* Forbes. https://www.forbes.com/sites/quora/2019/10/25/how-are-5th-and-6th-generation-cyberattacks-different-from-previous-ones/?sh=6c79b9e147dd
[8] Good Morning America. (2018, April 18). *Jordan Peele uses AI, President Obama in fake news PSA* [Video]. YouTube. https://www.youtube.com/watch?v=bE1KWpoX9Hkab_channel=GoodMorningAmerica
[9] Sadiq, M. (2019, May 24). *Real v Fake: Debunking the 'Drunk' Nancy Pelosi Footage.* The Guardian. https://www.theguardian.com/us-news/video/2019/may/24/real-v-fake-debunking-the-drunk-nancy-pelosi-footage-video
[10] Cahlan, S. (2020, February 13). *How Misinformation Helped Spark An Attempted Coup in Gabon.* The Washington Post. https://www.washingtonpost.com/politics/2020/02/13/how-sick-president-suspect-video-helped-sparked-an-attempted-coup-gabon/
[11] Rana, M. S., Sung, A. H., (2020, August 1). *DeepfakeStack: A Deep Ensemble-based Learning Technique for Deepfake Detection.* IEEE. https://ieeexplore.ieee.org/abstract/document/9171002
[12] Ciftci, U. A., Demir, I., Yin, L. (2020, July 15). *FakeCatcher: Detection of Synthetic Portrait Videos Using Biological Signals* IEEE. https://arxiv.org/pdf/1901.02212.pdf
[13] Guera, D., Delp, E. J. (2018, November 27). *Deepfake Video Detection Using Recurrent Neural Networks.* IEEE. https://arxiv.org/abs/2006.12247
[14] Segalis, E., Galili, E. (2020, June 17). *OGAN: Disrupting Deepfakes with an Adversarial Attack that Survives Training.* https://arxiv.org/abs/2006.12247
[15] Parmar, M. (2020). [Taxonomy of GAN] [Photograph] https://manojkumarparmar.wordpress.com/2020/01/03/taxonomyofgan/
[16] Yildirim, G., Jetchev, N., Vollgraf, R., Bergmann, U. (2019, October). *Generating High-Resolution Fashion Model Images Wearing Custom Outfits.* IEEE/CVF International Conference on Computer Vision. https://arxiv.org/pdf/1908.08847.pdf
[17] Kazeminia, S., Baur, C., Kuijper, A., Ginneken, B. V., Navb, N., et al. (2020, September). *GANs for Medical Image Analysis.* Artificial Intelligence in Medicine. https://arxiv.org/abs/1809.06222
[18] Zhang, H., Xu, T., Li, H., Zhang, S., Wang, X., Huang, X., et al. (2016, December 10). *StackGAN: Text to Photo-realistic Image Synthesis With Stacked Generative Adversarial Networks.* ICCV 2017. https://arxiv.org/abs/1612.03242
[19] Bian, Y., Xie, X. (2020, August). *Generative Chemistry: Drug Discovery With Deep Learning Generative Models.* ResearchGate. https://arxiv.org/pdf/2008.09000.pdf
[20] Strickland, E. (2019). [Comparison of Original Image to Deepfake] [Photograph]. IEEE Spectrum. https://spectrum.ieee.org/tech-talk/artificial-intelligence/machine-learning/facebook-ai-launches-its-deepfake-detection-challenge
[21] Zucconi, A. (2018) [Illustration of algorithmically aligning a face in an image] [Photograph]. Alan Zucconi. https://www.alanzucconi.com/2018/03/14/introduction-to-deepfakes/
[22] Zucconi, A. (2018) [Illustration of algorithmically reconstructing a face] [Photograph]. Alan Zucconi. https://www.alanzucconi.com/2018/03/14/introduction-to-deepfakes/
[23] Zucconi, A., (2018) [Illustration of algorithmically creating a new face] [Photograph]. Alan Zucconi. https://www.alanzucconi.com/2018/03/14/introduction-to-deepfakes/

[24] (2020, September 19). *Blockchain*. Wikipedia. https://en.wikipedia.org/wiki/Blockchain
[25] Kai, W. (2020). [Key elements of a blockchain] [Photograph]. ResearchGate. https://www.researchgate.net/figure/Key-Elements-of-Blockchain-Systems_fig1_327711685
[26] (2021). *Blockchain.com*. https://www.blockchain.com/explorer
[27] (2021. *Reality Defender*. https://rd2020.org/
[28] Wang, J., Liu, J., Nie, X., Sun, J. (2012, September). *A Visual Saliency Based Video Hashing Algorithm*. International Conference on Image Processing. https://www.researchgate.net/publication/261386975_A_visual_saliency_based_video_hashing_algorithm