# Detecting fake Videos Using Block Chain and Smart Contracts

**Swapnali N. Tambe, A.B.Pawar**

***Abstract*: The Rapid growth of agile gadgets has led to tremendous increase in digital media utilization, mostly for mobile video in ease of marketing. As encryption provides better user confidentiality and perseveration, greater number of online movement is associated with end-to-end encryption form. Irrevlant content such as unreal, violent and unconstitutional videos are being circulated online without being identified its truthfulness creating a platform for intruders and attackers. It is necessary for users to identify and report the contents of the video. Sometimes these videos act as evidence in courts to prove the guilty and the proper state and contents recorded in it .We aim a system to detect and classify the video's truthfulness to solve these problems. A detailed collection of studies has been toted to demonstrate the efficacy of new program over current literature.***

***Keywords:* network surveillance, Convolution neural network (CNN), propaganda videos.**

## I. INTRODUCTION

- A modern progress in AI, profound learning and image processing has directed to development of deep fake videos [2], [3]. For example, an earlier comparison of the former US's fake video was one-minute-short video. In April 2018, President Barack Obama went viral, with Obama saying things he never said. Deep fake videos are risky, and can potentially undermine the facts, mislead viewers, and objectively falsify reality. With the arrival of social networks, the rapid growth of such content can be unmanageable, and can likely exacerbate deception and treachery theories related problems. Deep fake videos are much more convincing and uncomplicated to make than standard fake Hollywood videos typically done manually using image control software such as Adobe Photoshop. Extreme fake videos use profound learning techniques with large samples of video images input to accomplish face swapping. The more samples are taken, the more probable the result is. In this paper, we are unfolding a structure for fake videos using smart contracts from Ethereum for tracking its originality and the history of the original content source – though the content is pliagrised many times. . The Inter Planetary File System (IPFS) hash uses smart contract for storing its digital content and its metadata. Our approach focuses on video content, though the design solving provided in this paper is fairly general and can be extended to any other form of digital medium. Our solution is based on the principle that, if the content is often traced creditability to a trusted or reputable originator, then the content may be real and trustworthy.

## II. LITERATURE REVIEW

Previous Research Projects are studied for the analysis of fake videos:-

Neelesh Bhakt [7] et al one of the utmost common recognizable emotions flashed among individuals is a smile. While some smiles come out because of joy, and the remaining is delusional. So the researcher has suggested a system to detect them. Researchers have proposed research in this paper on the basis of conquering the gesture of zygomatic large and obicularis oculli which creates a important role in detecting whether a smile is fake or real. The appearing of wrinkles on the cheeks, at the corner of the mouth, indicates the reduction of the large zygomatic muscle while prolongation of the eye indicates the contraction of the obicularis oculli.

Luciano Floridi [12] et al The art world is filled with reproductions. The distinction between a copy and a fake is based upon the authenticity principle. Today, the credibility of a work is much easier to establish, thanks to digital technologies. The researcher describes how fake faces are created by artists using the Artificial Intelligence to enact the work of original artists.

Darius Afchar[13] et al Digital images and videos have become very common digital objects through the popularization Of smart phones and social networking growth in recent decades. The growing use of digital pictures has been accompanied by an increase in techniques for manipulating picture content, for example using editing software such as Photoshop. Researcher has too quickly and efficiently used a method of detecting facial manipulation in videos and focuses in particular on two new techniques used to create hyper-realistic faked images: Deepfake and Face2Face.

David Guera[8] et al Proposed a system that uses a convolutionary neural network(CNN) to select characteristics at frame level. Then, these functions are used to train current neural network (RNN), which learns to determine whether or not a video is subject to manipulation. They test the process against a huge set of deep-fake videos from multiple websites.

**Revised Manuscript Received on December 5, 2019.**

**Swapnali N.Tambe***, computer engineering, Sanjivani ruler education society, kopargaon. Email: swapnali4321@gmail.com.

**Dr.A.B Pawar**, computer engineering department, Sanjivani engineering college,Kopargoan,India. Email: anil.pawar1983@gmail.com

| Title | Author | Existing System | Algorithm/ Technology | Research Gap | Purposed Solution |
|---|---|---|---|---|---|
| Deep Content: Unveiling Video Streaming Content From Encrypted WiFi Traffic | Ying Li, Yi Huang [5] et al | It is impossible to maintain network surveillance in the existing system and it results in unregulated atmosphere for goldminers and assailants to spread material such as false, objector and disinformation images. | Convolutional Neural Network (CNN), Recurrent Neural Network (RNN) and Multi-Layer Perceptron (MLP). | In their system All the models mentioned achieved similar results. | We are purposing a solution where the model will give more accuracy and different results |
| In Ictu Oculi:Exposing AI Created Fake | Yuezun Li [9] et al | In Existing System The expanding complexity of camera technology, the widespread availability of cell phones and the growing renown of social networks and video sharing sites have made digital video creation, editing and distribution more convenient than ever. This has also triggered digital video hacking. | Deep Neural network | In the System the accuracy results is more of fake blinking is more | We are proposing a method of revealing fake videos by identifying the absence of eye blinking with their reduced fake blinking precision. |
| Combating Deepfake Videos Using Blockchain and Smart Contracts | Haya R. Hasan[10] et al | Fake footage, images, audios and video can be an alarming and critical phenomenon, and by giving false reality can have the probable to alter the truth and erode the conviction. | Blockchain Technology | Only external Properties are taken into consideration such as name, tag, location, Size. | We are going to check video Internally by using Feature Extraction |
| Securing Video Integrity using decentalised Trusted Timestamp on the Bitcoin Blockchain | Gipp, Bela [6] et al | In the Existing System there is no such method to prove the authenticity of an incident occurred. | TimeStamping Technique | The current application submits the hash of the video file to the blockchain of Bitcoin with an unnecessary delay due to the approach of the Origin Stamp service that aggregates all hash obtained over a 24-hour span and only uploads the blockchain with a master hash to save transaction fees. | Purposed System We will improve the accuracy rate of the Timestamp hash Technique. |

**Table I Following table show the various algorithms and results of existing system**

S. Bian[14] et al Video bitrate can be freely shaped via some video editing software as one of the important factors that indicate the video quality. Researcher found those fake bitrate videos and estimated their original bitrate. The suggested approach is based primarily on the idea that the crucial quality of the video will not increase if the video bitrate is increased with the aid of video editing software. Tested on raw sequences of both CIF and QCIF, the preliminary conclusion indicated the efficacy of the expected approach.

Jiwu [15] et al Video frame rate up-conversion is one of the trivial procedure for Temporary manipulation of digital images, such as creating fake high-quality videos and splicing two video clips at different frame rates. However few current works have been proposed to detect this form of manipulation. A basic yet very effective way of viewing video after frame rate up-conversion, and further estimating its original frame rate. The experimental results which were assessed at different frame rates on 100 original videos demonstrated the capability of the suggested method. The overall detection level for noise-free videos in uncompressed and H.264/AVC formats can be as high as 99 per cent. In addition, the proposed method is robust to noise as the accuracy of noise detection on Gaussian white noise videos could exceed more than 85 percent and 95 percent when the SNR is 36 db and 33 db respectively.

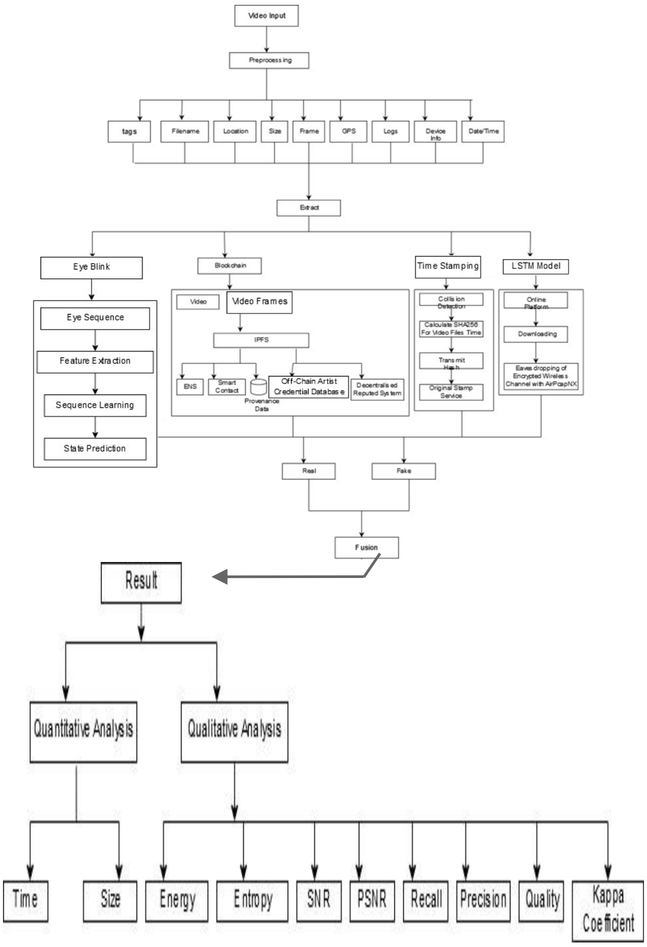
Xiaoyun Liang [16] et al Bitrate is a significant parameter for the quality of digital images. Forgers tend to boost video bitrate without any improvement in the quality of the video, particularly for Internet videos. Researcher has proposed an effective method for identifying more compressed videos with various fake bitrates. Secondly, it is the first time that the unique feature of the HEVC PU form in the first P-frames is used in the detection of fake bitrate and we called frame deletion robustness check, copy-paste and moved GOP structure assaults.

Efstratios Kakaletsis[11] et al The depth information defined is calculated using the motion vectors and scene detection from the video series. In DIBR based technique, using the depth information, 3D rapping is done from 2D images. Synthesized views can sometimes be used for illegal distribution without copyright authorization, instead of the real views.

## III. EXISTING SYSTEM

It's important to have techniques that can include fake videos, pictures, and drawings, audios, and so on to identify, battle, and combat deep digital content. It is not difficult to achieve this goal if there is a reliable, safe and trustworthy way of tracking the past of digital content. To prove its originality and authenticity, users should be able to access trusted data from digital content and monitor an object through history. This method can help users to believe in fake digital content, from being fooled or tempted. Current solutions for verifying the ethnicity of physical (and not digital) art work are available. As of today, there is no known method of verifying the originality of a digital video, audio, or image posted or published online. The thought of subjecting a COA to such digital content is unfeasible. It's incredibly difficult to determine the true base of a posted digital item in a reliable and trusted way. A typical end user usually uses online portal to try to find significant posts, forums or feedback on digital media to determine their validity. There is therefore an overwhelming need for an online digital content proof of authenticity (PoA) program to recognise reliable advertised originator and thus be able to fight deep-rooted videos, audio and pictures. A decentralized Proof of Authenticity (PoA) program in Present is using the innovative blockchain technology. Blockchain has the power to provide Data and transactions in distributed ledger decentralized, which are transparent and tamperproof. Blockchain applicability is enormous and technology is capable of transforming and affecting many companies, sectors and areas such as banking, supply chain management, health management, food industry, IoT, to name a few. For implementing a solution to these techniques we are providing improvised solution in the purposed system .The Expected Result is to improve accuracy rate of the techniques.

## IV. PURPOSED SYSTEM



In our purposed system it is expected that the accuracy will be improvised. It is challenging to classify and comprehend between real and fake videos that are shared online, as mentioned earlier. They are being treated as evidence to accuse guilty and provide punishment. To overcome such solution we are purposing various techniques to distinguish between fake and real videos being provided as evidence to its truthfulness.

Previously there were no such methods to identify them. Any consequent attempt to employ the video is unsuccessful, as the hash of manipulated videos in the blockchain does not match the hash. The validity of video evidence cannot be questioned using this method. The dashboard cameras footage might become a valid form of court evidence. Another method to find the fakeness of the video is through the eye blink technique. When a person records a video his eye blinks within a particular range. Blinking refers to the eyelid's swift closure and opening movement. In general, for a health adult human, there is an interruption of 2-10 seconds between each blink but the certain amount differ by individual, and the duration of a standard blink is 0.1-0.4 seconds / blink2. To overcome such problem we will detect the videos by eye blinking technique by locating the face of the person and identifying its facial landmarks. Change in facial orientation occurring we generate the identification of video authenticity.

Using Blockchain Technology we are using the revolutionary blockchain technology to provide proof of authenticity (PoA). Blockchain applicability is immense, and technology will change and impact many industries, markets, and fields such as finance, food industry, supply chain management, health management, IoT and more. We present an Ethereum-based blockchain clarification that provides the ethnicity of digital content by establishing credible and secure traceable to a trusted artist or publishing originator. Artists may include photographers who are freelancers or working, paparazzi, journalists, reporters etc. This path may also be used for other forms of digital material, such as audios, manuscripts, pictures, and videos.

In this approach, useful inferences can be drawn from without resistance observed WiFi data, which is uncorrupted pair of MAC Layer and transport layer. This is further difficult when compared to composing IP layer traffic predictions without knowledge of any Meta data. In particular we concentrate on identifying the flows of traffic From the Known Online Set pictures. Videos are commonly used on the internet but are often misused in many respects, including spreading fake news, hate speech, and inflammatory content and propaganda.

In our Purposed System it is expected that our accuracy of detecting fake videos will be improvised. The Results of the Fake Video Depends on the four Techniques based above i.e. using one technique we get result as fake whereas in second technique we get result as real. So based on Majority of the Results of the Technique we can get an analysis whether the video given is real or fake.

## V. ALGORITHM

### 1. CNN

A Convolutional Neural Network (CNN / ConvNet) is a Deep Learning algorithm that obtains an input picture, assigns context (enabler weights and biases) to unique aspects / gadgets in the pictures, and separates them from each other. Preprocessing in a ConvNet is significantly smaller than other classification algorithms. Though filtrates are hand-crafted in primary ways, with sufficient training, ConvNets can learn these filters / characteristics.

Pseudo Code:-

```
Input: l, Y, e, m, q and M=|Y| > (2m-1).
Output: Outliers in Y
1 Collects m data as first phase of training;
2 Investigates the qMM, SqMM, and TqMM for yt, and 1 < Q < m;
3 Measures ABCD (yt), if ABCD (yt) > 1, outlier estimate of yt added by 1;
4 Collects a new ga+1 report, eliminates the obsolete z1 data point;
5 if the outlier count of z1 > h (1 < h<m), z1 is an outlier;
6 Searches the qMM, SqMM, and TqMM, and ABCD for affected data;
7 Updates the qMM, SqMM, TqMM, and ABCD for affected data;
8 Calculates ABCD (yt), if ABCD (yt) >1, outlier count of yt; increased by 1;
9 Collects new ga+2 info, removes obsolete z2 data point;
10 if the deviation count of z2 > h (1<h <m), z2 is an outlier;
11 Investigates the qMM, SqMM, and TqMM for ga+2, and 3 < K < m +2;
12 update the qMM, SqMM, and TqMM and ABCD for damaged data;
13 Calculates ABCD (yt), if ABCD (yt) > 1, outlier count of yt added by 1;
14 Continue steps 4 -13;
```

### 2. Time Stamping Algorithm

In timestamp based concurrency control algorithm, each site for a video maintains a logical clock. When a transaction is made at that location, this clock is increased and updated when a message with a higher clock value is received by the server. A specific timestamp is allocated to each transaction and contradictory acts are executed according to the timestamp of their transactions.

S erialization order of transactions is chosen a priori in the time stamp-based competition control algorithm and transactions are forced to follow this order.

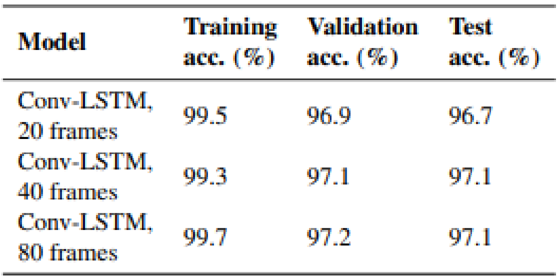
If a transaction is aborted, a new timeline will be rebooted. This can lead to a cyclic restart where, without completion, a transaction can be restarted and repeatedly aborted. Another drawback is that it has overhead storage to retain timestamps (for each data entity, two timestamps must be kept).

Pseudo code:

```
If EF < X-ef(c) then
Reject read request and abort corresponding
  transaction
Else
Execute transaction
Set K-ef(c) to max{K-ef(c), EF}
A write request is handled in the following
  manner:
If EF < K-ef(c) or EF < X-ef(c) then
Reject write request
Else
Execute transaction
Set X-ef(c) to EF.
```

## VI. EXPECTED RESULTS

**Table II: Classification tests of our data set splits with video subsequences of various lengths.**



| Model | Training acc. (%) | Validation acc. (%) | Test acc. (%) |
|---|---|---|---|
| Conv-LSTM, 20 frames | 99.5 | 96.9 | 96.7 |
| Conv-LSTM, 40 frames | 99.3 | 97.1 | 97.1 |
| Conv-LSTM, 80 frames | 99.7 | 97.2 | 97.1 |

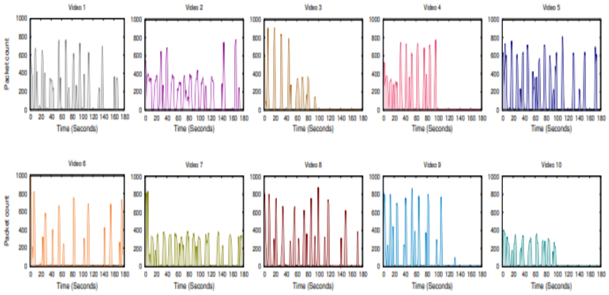


Fig 1. I / O Single Run Charts for 10 Different Videos

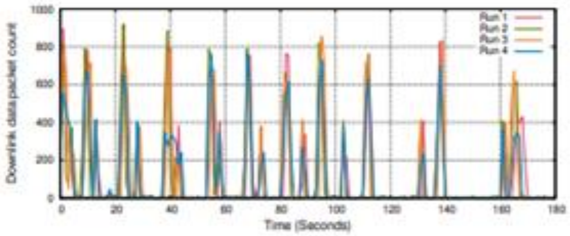


Fig2. Same Videos different Traffic Flow

By studying various techniques in literature survey we will improve the methods technique. Using Various Techniques above mentioned we will improvise the accuracy of the fake videos identification [8, 5]. We will analyze all the parameters to improve the accuracy .Our Results will be based on the accuracy of each technique and on average of all the techniques we will determine whether the tested video is real or fake.

## VII. CONCLUSION

Due to tremendous use of technology the trust factor of media decreases.so our system will help in improvising the techniques. We have proposed a solution to prove the ethnicity of digital videos in which a safe and trustworthy tracing can be created to the underived video creator or origin. Our solution makes use of a Time stamping Technique which ensures unique recording of critical Situation without hampering its actual situation, Name operation Ethereum, and reputation network decentralized. Our proposed system designs, algorithms and specifics of application and examining are fairly generic and can be extended to other forms of digital content such as audios, videos, pictures and documents. Through helping users decide whether a video or digital material is detectable to a trustworthy and reliable root, our unravelment will help encounter fake videos. If a video or digital content is not difficult to trace then the digital content can't be trusted. Our systems will also benefits to various categories like social media sites, blogs, messages etc.

## REFERENCES

1. Gennie Gebhart, “We’re Halfway to Encrypting the Entire Web,” https: //www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web, 2017, online; accessed 02-07-2018.
2. When seeing is no longer believing: Inside the Pentagon’s race against deep fake videos. January 2019. [Online]. Available: http://edition.cnn. com/interactive /2019/01/business/pentagons-race-against- deep fakes
3. Lawmakers warn of ’deepfake’ videos ahead of 2020 elections. January 28, 2019. [Online]. Available: https://edition.cnn.com/2019/01/28/tech/ deepfake-lawmakers/index.html
4. How faking videos became easy and why that’s so scary. [Online]. Available: http://fortune.com/2018/09/11/deep-fakes-obama-video/
5. Ying Li,” Deep Content: Unveiling Video Streaming Content from Encrypted WiFi Traffic”,IEEE,2018.
6. B. Gipp, J. Kosti, and C. Breitinger, “Securing video integrity using decentralized trusted time stamping on the bitcoin blockchain.” in MCIS, pp. 1-10, 2016.
7. N. Bhakt, P. Joshi and P. Dhyani, "A Novel Framework for Real and Fake Smile Detection from Videos," 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, 2018, pp. 1327-1330.
8. D. Güera and E. J. Delp, "Deepfake Video Detection Using Recurrent Neural Networks," 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Auckland, New Zealand, 2018, pp. 1-6.
9. 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)*, Hong Kong, Hong Kong, 2018, pp. 1-7.
10. H. R. Hasan and K. Salah, "Combating Deepfake Videos Using Blockchain and Smart Contracts," in *IEEE Access*, vol. 7, pp. 41596-41606, 2019.
11. S. Rana, S. Gaj, A. Sur and P. K. Bora, "Detection of fake 3D video using CNN," 2016 IEEE 18th International Workshop on Multimedia Signal Processing (MMSP), Montreal, QC, 2016, pp. 1-5.
12. Luciano Floridi,” Artificial Intelligence, Deepfakes and a Future of Ectypes” Springer, pp.317-321, 2018.
13. D. Afchar, V. Nozick, J. Yamagishi and I. Echizen, "MesoNet: a Compact Facial Video Forgery Detection Network," 2018 IEEE International Workshop on Information Forensics and Security (WIFS), Hong Kong, Hong Kong, 2018, pp. 1-7.
14. S. Bian, W. Luo and J. Huang, "Exposing fake bitrate video and its original bitrate," 2013 IEEE International Conference on Image Processing, Melbourne, VIC, 2013, pp. 4492-4496.
15. Bian, Shan & Luo, Weiqi & Huang, Jiwu,” Detecting video frame-rate up-conversion based on periodic properties of inter-frame similarity” Multimedia Tools and Applications. 2014.
16. X. Liang, Z. Li, Y. Yang, Z. Zhang and Y. Zhang, "Detection of Double Compression for HEVC Videos With Fake Bitrate," in IEEE Access, vol. 6, pp. 53243-53253, 2018.

## AUTHORS PROFILE

**Miss. Swapnali N. Tambe** currently working as assistance teacher in sanjivani junior college,kopargaon.She has published Paper Multimodal Biometric Authentication Using PSO Based Watermarking of Fingerprint Image in Face Image” in International Conference on Recent Trends in Computer Technology-2013 at SNJB’s Coe, Chandwad, .“Semantic Content Extraction in Video Using Ontology Based Fuzzy Model” in c PGCON- 2015, “A Review Paper on Semantic Content Extraction in Video Using Ontology Based Fuzzy Model” in International Journal of Engg. Dept . & Research. ISSN:2321-9939 and “Semantic Content Extraction in Video Using Ontology Based Fuzzy Model” International Journal of Scientific Progress & Research. ISSN:1201-394

**Dr. A. B Pawar** he is Dean Academic of sanjanvani engineering college,kopargoan.