



Publisher homepage: www.universepg.com, ISSN: 2663-7804 (Online) & 2663-7790 (Print)

<https://doi.org/10.34104/ajeit.022.013026>

Australian Journal of Engineering and Innovative Technology

Journal homepage: www.universepg.com/journal/ajeit

Australian Journal of
Engineering and
Innovative Technology



A Qualitative Survey on Deep Learning Based Deep fake Video Creation and Detection Method

Ashifur Rahman¹, Md. Mazharul Islam¹, Mohasina Jannat Moon¹, Tahera Tasnim¹, Nipo Siddique¹, Md. Shahiduzzaman^{1*}, and Samsuddin Ahmed¹

¹Department of Computer Science and Engineering, Bangladesh University of Business and Technology (BUBT), Rupnagar R/A, Mirpur-2, Dhaka-1216, Bangladesh.

*Correspondence: shahid@bubt.edu.bd (Md. Shahiduzzaman, Assistant Professor, Department of Computer Science and Engineering, Bangladesh University of Business and Technology, Dhaka-1216, Bangladesh).

ABSTRACT

The rapid growth of Deep Learning (DL) based applications is taking place in this modern world. Deep Learning is used to solve so many critical problems such as big data analysis, computer vision, and human brain interfacing. The advancement of deep learning can also causes some national and some international threats to privacy, democracy, and national security. Deepfake videos are growing so fast having an impact on political, social and personal life. Deepfake videos use artificial intelligence and can appear very convincing, even to a trained eye. Often obscene videos are made using deepfakes which tarnishes people's reputation. Deepfakes are a general public concern, thus it's important to develop methods to detect them. This survey paper includes a survey of deepfake creation algorithms and, more crucially we added some approaches of deepfake detection that proposed by researchers to date. Here we go over the problems, trends in the field, and future directions for deepfake technology in detail. This paper gives a complete overview of deepfake approaches and supports the implementation of novel and more reliable methods to cope with the highly complicated deepfakes by studying the background of deepfakes and state-of-the-art deepfake detection methods.

Keywords: Deepfake, Artificial Intelligence, Machine Learning, Computer vision, CNN, RNN, and LSTM.

INTRODUCTION:

Deepfake videos are manipulated videos that use Machine Learning based algorithms to swap a person in an existing image or video with someone or something else (Adee, 2020). Deep fake videos are divided into three major categories: head puppetry, face swapping, and lip-syncing. Head puppetry entails altering a video of a specific human's head and upper shoulder with the help of a source video person's head so that the modified individual looks exactly like the source. Face swapping is the process of transferring a person's face to

another person's face while maintaining the same facial expression. Only the lip region of a video is altered in lip-syncing, so the target individual says something that is not accurate in reality. Although some deep-fakes can be made using classic visualizations or computer graphics, deep-learning methods such as auto encoders (Tewari, 2018) and generative-adversarial networks (GAN) (Lin, 2021) which have been extensively used in the computer vision area, are the most recent popular process for deepfake video creation (Liu, 2021).

These models are used to analyze a person's facial emotions and movement and synthesis facial images of someone with similar expressions and movements (Lyu, 2018). To train a model to generate photo-realistic pictures and videos deepfake technologies often requires a huge volume of image and video data-sets. Politicians and celebrities are the first targets of deepfakes since they have a massive amount of videos and photographs available on the internet. Deepfakes were utilized to create pornographic photographs and movies to replace the heads of politicians and celebrities' bodies. In 2017, the first deepfake video was released, in which a celebrity's face was replaced with a porn actor. Nowadays deepfake videos are becoming global security threat because now it's used to make fake speech videos of international leaders (Hwang, 2020).

Deepfakes can thus be used to incite political or religious tensions between countries, deceive the public and influence election results, or create havoc in financial markets by spreading false information (Zhou, 2020; Guo, 2020). It can also be used to create fictional satellite photos of the Globe that contain objects which do not exist in the real world to deceive military analysts, such as making a fictional bridge across a river which is not actually present. This can mislead a troop when crossing a bridge during a combat (Fish, 2019).

Because the democratization of creating effective virtual humans has beneficial consequences, so deepfakes can also being used in positive ways, such as in visual effects, digital avatars, snapchat filters, creating voices for those who have lost their voice, and updating episodes of movies without reshooting them . The number of illegal implementations of deepfakes, on the other hand, far outnumbers the beneficial ones. Because of the advancement of deep neural networks and the accessibility of enormous amounts of data, faked photos and movies are nearly unrecognizable to humans and even powerful computer algorithms. The procedure of making those modified photographs and films is also more easier nowadays, as it only requires a target person's identifying photo or a short videos. Nowadays, producing astonishingly realistic tempered video requires less and less efforts. Recent advancement of technology can generate a deepfake video with the help of a single picture (Zakharov, 2019).

As a result, deepfakes may pose a danger not only to public figures but also every individual. For example, a voice deepfake was used to scam a CEO out of \$243,000 (Damiani, 2019). Recently an application Deep Nude was released, that can turn a person into a non-consensual pornographic video, which even more troubling (Samuel, 2019). Similarly, the Chinese application Zao has recently created a buzz, it can allow even the most non - technical users to switch their faces onto the bodies of a famous movie stars and inject themselves into well-known films and TV clips (Guardian, 2019). These types of falsification pose a serious danger to privacy and identification, and they have an impact on many parts of people's lives.

As a result, discovering the reality in the digital world has become particularly crucial. It's considerably more difficult when handling with deepfake videos, because they're frequently utilized for harmful reasons, and virtually anyone can now construct deepfakes using current deepfake video creation tools. Several approaches for detecting deepfake videos have been proposed so far (Lyu, 2020) (Jafar, 2020). Because the majority of the deepfake creation and detection method are deep learning based, a conflict has erupted between malevolent and beneficial uses of deep learning methods. To combat the problem of deepfakes or face-swapping technologies, the US Defense Advanced Research Projects Agency (DARPA) launched a multimedia forensics research program (called Media Forensics or MediFor) to speed the invention of fake digital visual media detection methods (Turek, 2020). Facebook Inc., in collaboration with Microsoft Corp. and the Partnership on AI coalition, has established the Deepfake Detection Challenge to encourage greater research and innovation towards identifying and stopping the use of deepfakes to confuse viewers (Schroepfer, 2019).

The volume of deepfake papers has increased rapidly in recent years, according to data acquired by dimensions.ai at the end of 2020 (Dimensions, 2021). **Fig. 1** shows the growth of deep-fake papers that increasing recently after 2017. Although the amount of deepfake papers received is likely to be lower than the original amount, the research trend on this area is clearly expanding.

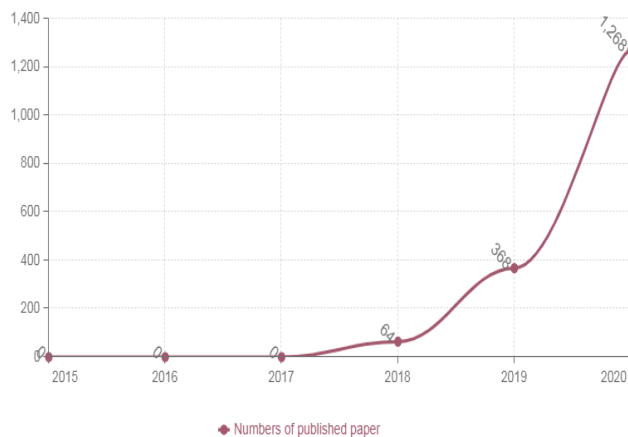


Fig. 1: The growth of research on deepfake video detection and creation is given in this Fig.

This survey paper presented all the method of creating and detecting deepfake videos. There are so many survey papers present now in this field (Verdolina, 2020), but we done our survey from a different point of view and taxonomy. The fundamentals of deepfake algorithms and deep learning based deepfake creation method are presented in Section II. In Section III we discuss the various technique for identifying deepfake videos as well as their benefits and drawbacks. In last section, we described all the challenges, and future directions for deep fake detection and media forensics concerns.

Deepfake Creation

Deepfakes have grown in popularity as a result of the high quality of manipulated videos and the ease with which their implementations may be used by a wide variety of users with varying computing skills, from professional to newbie. Deep learning methods are used to create the majority of these applications. The ability of deep learning to represent complicated and high-dimensional data is well-known. Deep auto encoders, a type of deep network with that capability, have been widely used for dimensionality reduction and image compression (Punnappurath, 2019) (Cheng, 2019). FakeApp, created by a Reddit user using an auto encoder decoder pairing structure, was the first approach at deepfake creation (Reddit, 2015). The auto encoders obtain latent features from facial images, and the decoder reconstructs the images in that fashion. Two encoder-decoder pairs are required to exchange faces between source and target images, with each pair

training on an image set and the encoder's parameters shared between two network pairs (Guera, 2018).

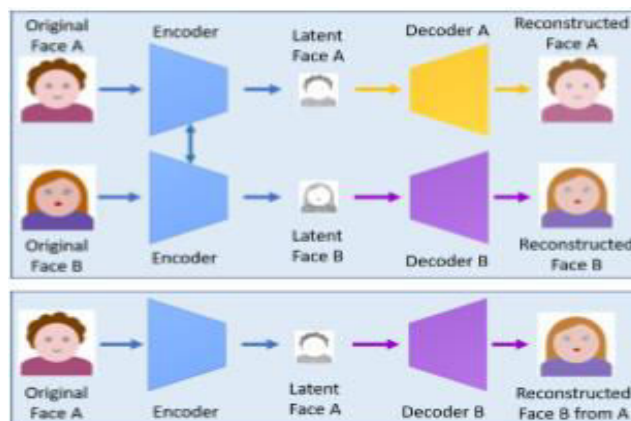


Fig. 2: Two encoder-decoder pairs are used in this deepfake production strategy.

For the training process, two networks utilize the same encoder but distinct decoders (top). Deepfakes are made by encoding the image of face A with the common encoder and decoding it with decoder B. (bottom) (Guera, 2018). In other words, the encoder networks of two pairs are identical. This technique allows the common encoder to find and learn the similarity between two sets of face images, which is very easy because faces have comparable features like eyes, noses, and mouth positions. Fig depicts a deepfake production process in which the feature set of face A is linked the decoder B in order to reconstruct face B from face A. This method is used in a number of papers; including Deep-FaceLab, DFaker, and DeepFake tf (tensor flow based deepfakes). An improved version of deepfakes based on faceswap-GAN (Face, 2015) was proposed by adding adversarial losses and perceptual losses implemented in the VGG Face (Ker, 2014) to the encoder-decoder architecture. It is included in the VGGFace perceptual loss in order to produce a higher-quality output video, which is made possible by smoothing out artifacts in segmentation masks (Goodfellow, 2014). It is possible to generate outputs with pixel resolutions of 64x64, 128x128, and 256x256. Additionally, FaceNet (net, 2015) introduces a multi-task convolutional neural network (CNN) (Albawi, 2017) to enhance facial recognition and alignment accuracy. In order to implement generative networks, Cycle GAN (Cycle, 2017) is used (Zhao, 2016). An overview of the most popular deepfake tools is shown in **Table 1**.

Table 1: Here we give some tools and their work for creating deepfake videos.

Toolkit	Linked	Characteristics
DeepFaceLab	https://github.com/iperov/DeepFaceLab	<ul style="list-style-type: none"> Add new models to the Faceswap technique, such as H64, H128, LIAEF128, and SAE (DeepFaceLab, 2016). Several face extraction methods, such as S3FD, MTCNN, dlib, and manual, are supported (DeepFaceLab, 2016).
Faceswap	https://github.com/deepfakes/faceswap	<ul style="list-style-type: none"> The encoders and decoders are paired. The encoders share parameters.
Faceswap-GAN	https://github.com/shaoanlu/faceswap-GAN	<ul style="list-style-type: none"> Auto-encoder architecture is enhanced using adversarial loss and perceptual loss (VGGface).
DFaker	https://github.com/dfaker/df	<ul style="list-style-type: none"> The face is reconstructed using the DSSIM loss function (Dss, 2011). Keras library was used to implement this.
AvatarMe	https://github.com/lattas/AvatarMe	<ul style="list-style-type: none"> Recreate 3D faces from a variety of "in-the-wild" photographs. From a single low-resolution image, it is possible to reconstruct authentic 4K by 6K-resolution 3D faces.
DeepFake tf	https://github.com/StromWine/DeepFake tf	<ul style="list-style-type: none"> Same like DFaker, but with tensor flow implementation
FaceShifter	https://lingzhili.com/FaceShifterPage	<ul style="list-style-type: none"> By utilizing and integrating the target attributes, high-fidelity face swapping can be achieved. Without requiring subject-specific training, the tool can be used for any new face pair (Li, 2019).
DiscoFaceGAN	https://github.com/microsoft/DiscoFaceGAN	<ul style="list-style-type: none"> Create virtual people's face images using independent latent factors such as identity, emotion, position, and brightness. 3D priors should be integrated into adversarial learning (Deng, 2020).
FSGAN	https://github.com/YuvalNirkin/fsgan	<ul style="list-style-type: none"> A face swapping and reenactment model that may be used on pairs of faces without the need for training. Adapt to changes in both pose and expression.
MarioNETte	https://hyperconnect.github.io/MarioNETte	<ul style="list-style-type: none"> A framework for reenacting faces in a few shots while maintaining the target's individuality. Identity adaption does not require any extra fine-tuning (Ha, 2020).
Few-Shot Face Translation	https://github.com/shaoanlu/fewshot-facettranslation-GAN	<ul style="list-style-type: none"> To extract latent embeddings for GAN (Lin, 2021) processing, use a pre-trained face recognition model. Integrate semantics prior convictions derived from FUNIT and SPADE (Park, 2019) modules.
Neural Voice Puppetry	https://justusthies.github.io/posts/neuralvoice-puppetry	<ul style="list-style-type: none"> A method for facial video synthesis based on auditory input. Using 3D face representation, create films of a talking head from an audio sequence of another person (Thies, 2020).

Deepfake Video Detection

The growing numbers of deepfakes are threatening privacy, social security, and democracy (Chesney, 2018). As soon as the threat of deepfakes was identified, methods for identifying them were proposed. Early approaches relied on manufactured features derived from glitches and flaws in the deepfake video

synthesis process. Deep learning was used in re-cent approaches to automatically extract significant and discriminative features in order to detect deepfakes (de Lima, 2020; Amerini, 2020). Deepfake detection is typically thought of as a binary classification problem, in which classifiers are employed to distinguish bet-

ween real and manipulated videos. To train this type of classification model, we need a big dataset of actual and false videos. Although the quantity of deepfake videos is growing, there are still limitations in terms of establishing a benchmark for verifying multiple detection methods. Korshunov and Marcel (Korshunov, 2019) used the open-source code Faceswap-GAN (Face, 2015) to create a significant deepfake dataset consisting of 620 videos based on the GAN model to address this issue. Low and high-quality deepfake videos were created using videos from the publicly available VidTIMIT dataset (Sanderson, 2002), which can convincingly simulate facial movements, lip motions, and eye blinking. These dataset videos were then put to the test to see how well numerous deepfake detection methods worked. The popular facial recognition algorithms based on VGG (Parkhi, 2015) and Facenet (Schroff, 2015) are unable to recognize deepfakes successfully, according to test results. When used to detect deepfake videos from this freshly created dataset, other methods such as lip-syn-cing approaches (Chung, 2017) (Korshunov, 2018) and image resolution measures with support vector machine (SVM) (Boulkenafet, 2015) show very high mistake rates. This increases worries about the crucial need for more powerful approaches to distinguish true deepfakes in the future.

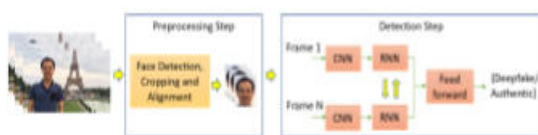


Fig. 3: All categories of deepfake detection are given in this Fig.

Generally there are two categories of deepfake detection, one is fake video detection and the other one is fake image detection. Fake video detection is divided further into two more categories namely Visual Artifacts within Frame and Temporal Features across Frames. **Fig. 3** shows all the categories of deepfake detection. In this paper we only survey about deepfake video detection methods and give researcher a future direction to in reach this research field.

Fake Video Detection

Due to the significant loss of frame data following video compression, most image detection techniques UniversePG | www.universepg.com

can't be applied to videos (Afchar, 2018). Additionally, videos have temporal features that vary between frames, making it difficult for systems built to detect merely still fraudulent images to detect them. Fake video detection is divided into two categories namely Temporal Features across Frames and Visual Artifacts within Frames. Those two categories are explained in this subsection.

1) Temporal Features Across Frames

Sabir *et al.* used spatio-temporal properties of video streams to detect deepfakes, based on the finding that temporal coherence is not maintained well in the synthesis process of deepfakes (Sabir, 2019). Low-level abnormalities caused by face modifications are considered to express themselves as temporally artifacts with irregularities between frames because video modification is done frame by frame. To leverage temporal disparities across frames, a recurrent convolutional model (RCN) was established based on a combination of the convolutional network DenseNet (Huang, 2017) and the gated recurrent unit cells (Cho, 2014) (**Fig. 4**).

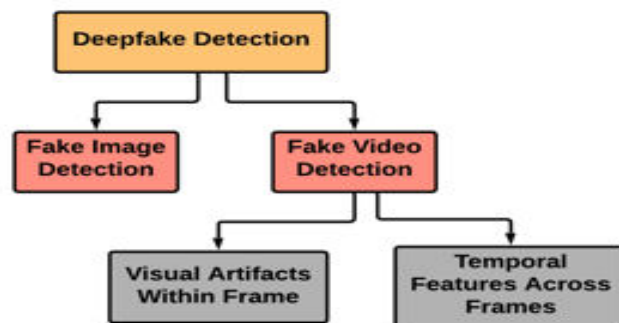


Fig. 4: A two-step process for detecting face manipulation in which the first step aims to detect, crop, and align faces on a sequence of frames, and the second step uses a combination of convolutional neural networks (CNN) and recurrent neural networks to distinguish between manipulated and authentic face images (RNN) (Sabir, 2019).

According to Guera and Delp (Guera, 2018), deepfake videos feature intra-frame abnormalities as well as temporal anomalies between frames. They then suggested a temporal aware pipeline method for detecting deepfake videos that uses CNN and long short-term memory (LSTM) (Guera, 2018). Frame-level features

are extracted using CNN, which are then input into the LSTM to build temporal series descriptors. Finally, based on the sequence descriptor, a fully-connected network is utilized to classify doctored video from genuine ones, as seen in **Fig. 5**.

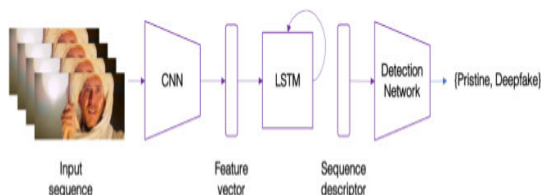


Fig. 5: A deepfake recognition method that uses a convolutional neural network (CNN) and long short term memory (LSTM) to extract temporal information from a video sequence and express them using a sequence descriptor.

The sequence descriptor is used to calculate probability of the frame sequence belonging to either authentic or deepfake class using a detection network with fully connected layers (Guera, 2018). The use of a physiological signal, such as eye blinking, to detect deepfakes, on the other hand, was proposed based on the finding that a person in deepfakes blinks far less frequently than a person in untampered videos (Li, 2018). A normal person blinks the eye between 2 and 10 times per minute, with each blink lasting between 0.1 and 0.4 seconds. Deepfake algorithms, on the other hand, frequently use Internet face pictures for training, which typically show people with open eyes (very few pictures on the online show persons with eyes closed). As a result, deepfake algorithms are unable to build fake faces that blink normally without access to photos of individuals blinking (Li, 2018). First breakdown the videos into frames, then extract face regions and subsequently eye areas based on six eye cues to distinguish between actual and false videos. These cropped eye region sequences are distributed into long-term recurrent convolutional networks (LR-CN) (Donahue, 2015) for dynamic state prediction after a few stages of pre-processing like aligning faces, extracting and scaling the bounding boxes of eye land-mark points to build fresh sequences of frames. The LRCN consists of a CNN-based feature extractor, LSTM-based sequence learning, and a fully connected layer-based state prediction to forecast the probability of eye open and

closure states. The use of LSTM helps to capture these temporal patterns efficiently because eye blinking reveals substantial temporal dependencies. A blink is defined as a peak over the level of .05 with a length of fewer than 7 frames, and the blinking rate is measured on the prediction outcomes. This method is tested on a web-based dataset consisting of 49 interviews and lecture videos, as well as the deepfake classifiers' fake versions of those videos. The experimental results show that the suggested method has potential detection accuracy for fake videos, which can also be taking into account the dynamic pattern of blinking, such as excessively rapid blinking, which could be a symptom of video manipulation.

Visual Artifacts With in Frames

As explained in the earlier section, the techniques for detecting deepfake videos that use temporal patterns between video sequences are generally based on deep recurrent network architectures. In this section, we explored some more methods for obtaining feature maps by disintegrating videos into frames and looking at visual artifacts within a single frame. To distinguish among fake and real videos, these characteristics are transmitted into a deep or shallow classification model. As a result, we divided the approaches in this section are into two categories: deep and shallow classifiers.

1) Deep classifiers

Deepfake video are typically made with low resolutions, necessitating an affine face warping strategy (i.e., resizing, rotating, and shearing) to match the originals' configuration. This method produces artifacts that CNN models like VGG16 (Simonyan, 2014), ResNet50, ResNet101, and ResNet152 (He, 2016) can identify due to the resolution mismatch between the warping face area and surrounding context. In a deep learning approach for detecting deepfakes was presented based on artifacts noticed during in the face warping phase of the deepfake generating algorithm (Li, 2018). On two deepfake datasets, the UADFV and Deepfake TIMIT, the suggested approach is assessed. In total, there are 32,752 pixels in the UADFV dataset (Li, 2020), which includes 49 genuine and 49 faked videos. The Deepfake TIMIT dataset (Sanderson, 2002) contains a two set of low-quality 64×64 and high-quality 128×128

videos, totaling 10,537 real and 34,023 fake images retrieved from 320 videos for every quality set. The recommended methods result is evaluated to other widely used methods such as Meso4 & MesoInception-4 (Afchar, 2018), MesoNet methods, HeadPose (Yang, 2019), and the two-stream NN face tampering detection method. The suggested method has not needing to create deepfake video to train the detection methods (Zhou, 2017). This is the main advantages because deepfake videos have bad aspects also.

2) Shallow classifiers

The majority of deepfake detection algorithms focus on artifacts or inconsistencies in inherent properties among real and fake photos or videos. Yang *et al.* (Yang, 2019) suggested a detection approach based on monitoring the changes among 3D head positions, which are computed using 68 face regions in the crucial face recognition system. As there is a defect in the deep-fake image creation process, so the 3-dimensional head positions are investigated to detect it. To get higher accuracy, the retrieved characteristics are passed into an SVM Classification model. They test the model into two datasets and show that the suggested model outperformed the alternatives. In total, there are 32,752 pixels in the UADFV dataset (Li, 2020), which includes 49 genuine and 49 faked videos. The second dataset, which is a subset of data from the DAR-PA MediFor GAN Image/Video Challenge, contains 241 real photos and 252 deep fake photos (Guan, 2019). Similarly, in (Matern, 2019) a strategy for exploiting deepfake and face modification artifacts based on visual aspects of eyes, teeth, and facial contours were investigated. The graphical artifacts are caused by inadequate global consistency, an incorrect or inaccurate estimate of incident illumination, or an inaccurate estimate of the actual geometry. Missing reflections and details in the eye and teeth areas, as well as texture features retrieved from the facial region based on facial landmarks, are used to detect deepfakes. The eye feature vector, the teeth feature vector, and the features retrieved from the full-face crop are employed as a result. After extracting the characteristics, two classifiers are used to distinguish the

deepfakes from genuine videos: logistic regression and a tiny neural net-work. Experiments on a YouTube video dataset yielded the best result of 0.851 in terms of the area under the receiver operating characteristics curve. The proposed approach, on the other hand, has the drawback of requiring images to meet particular requirements, such as open eyes or visual teeth.

DISCUSSION:

People's faith in media information has been eroded by deepfakes, as seeing them no longer equates to trust in them. They have the potential to generate anguish and negative consequences for people targeted, increase misinformation and offensive language, and even exacerbate political tensions, incite public outrage, violence, or war. This is particularly important today because deepfake technology is becoming more accessible, and social media sites can swiftly propagate false news (Zubiaga, 2018). The serious problem of deepfake, the research community has concentrated on building deepfake learning algorithms, with multiple results published. The state-of-the-art methodologies were addressed in this work, and **Table 2** presents an overview of common approaches. It's clear that a struggle is brewing between people who utilize powerful machine learning to build deepfakes and others who take the opportunity to recognize them. The quality of deepfakes has been improving, and monitoring systems' performance has to advance through too. The concept is that what AI has broken can also be mended by AI (Floridi, 2018). Detection techniques are still in their infancy, and a variety of approaches have been presented and tested, but on scattered datasets. Creating a growing updated benchmark dataset of deepfakes to verify the ongoing development of detection methods is such a way to improve detection method performance. This will find things simpler to train recognizers, especially deep learning models, which require massive training sets (Dolhansky, 2020). Current detection methods, on the other hand, are most often focused on the flaws in deepfake generating pathways. In adversarial contexts, where attackers' frequently tries not to expose deepfake creation methods, this kind of information and knowledge is not always available. The deepfake detection task has become more complex as a result of recent work on adversarial

perturbation assaults to deceive DNN-based monitors (Hussain, 2021) (Yang, 2021). These are actual obstacles in the creation of detection systems, and future studies should focus on developing more reliable, adaptable, and generally applicable methods. Some other line of inquiry is to include monitoring systems into production platforms like social media to ensure their efficiency in grappling with deepfakes widespread influence. On these platforms, a screening or filtering mechanism with effective detection methods can be created to make deepfakes detection easier (Citron, 2018). Law limitations could be imposed on internet corporations that own these sites, requiring them to immediately delete deepfakes in order to mitigate their effects. Photo editing tools can also be embedded into devices that humans use to create digital content to create unchanging metadata for maintaining originality details like time and place of audiovisual items, as well as their untampered attestation (Citron, 2018).

This connection is tough to implement, so using disruptive blockchain technology as a solution could be a viable option. The block chain has been actively employed in a variety of fields, but there has been little research tackling deepfake detection issues using this technology. It's an excellent tool for digital provenance because it can construct a chain of unique, immutable metadata chunks. Although the application of block chain systems to this challenge has generated some promising findings (Hasan, 2019), this study area is still in its inception. It's necessary to use detection tools to recognize deepfakes, but it's even more critical to grasp the true motivations of all who publish them. Users must appraise deepfake regarding the social context in which it is detected, like who circulated it and what they said here. This really is important because deepfakes are becoming increasingly lifelike, and detecting software is expected to fall behind. It is thus worthwhile to conduct research on the social aspect of deepfakes in order to support users in making such decisions.

Table 2: Here we show some popular deepfake videos detection methods.

Methods	Classifiers/ Techniques	Key Features	Dataset
MesoNet (Afchar, 2018)	CNN (Albawi, 2017)	Meso-4 and MesoInception-4 are two deep models that are used to analyses deepfake videos. Accuracy of this method in DFDC dataset (Dolhansky, 2020) is 98% and FaceForensics++ dataset (Rossler, 2019) is 95%.	Both datasets contain fake online videos. DFDC (Dolhansky, 2020)has two-level and FaceForensics++ (Rossler, 2019)also has two levels.
Eye blinking(Guera, 2018)	LRCN (Wang, 2017)	Observe the temporal patterns of eye blinking using LRCN. Deepfakes' blinking rate is substantially lower than usual; hence this is based on that fact.	Contains 49 interviews and presenter videos, as well as the deepfakes that match to them.
Eye, teach and facial texture (Matern, 2019)	Neural Network (NN) (Gevins, 1988) and Logistic Regression (Wright, 1995)	Uses facial structure variations, as well as missing reflections and details in the eye and teeth areas of deepfakes. Classification is done using logistic regression and neural networks.	A YouTube video dataset was downloaded to train model.
Using face warping (Li, 2018) artifacts	VGG16 (Simonyan, 2014) ResNet50, or 152 (He, 2016)	CNN models are used to find artifacts depending on resolution inconsistencies between the warping face region and side area.	UADFV dataset (Yang, 2019), a collection of 49 actual and 49 faked videos totaling 32752 frames. Deepfake TIMIT (Korshunov, 2018).
Head poses (Yang, 2019)	SVM (Simonyan, 2014)	68 landmarks in the facial region are used to extract features. Using the collected characteristics and classify them using SVM.	UADFV dataset, a collection of 49 actual and 49 faked videos totaling 32752 frames. The DARPA MediFor GAN Image Video Challenge produced -241 actual images and 252 deep fake ones.

Intra-frame and temporal inconsistencies (Guera, 2018)	CNN (Albawi, 2017) and LSTM (Breuel, 2015)	CNN is used to collect frame-level features, which are then used to train the LSTM model to classify deepfake videos.	A combination of 600 videos taken from a variety of online sources.
Spatio-temporal features with RCN (Sabir, 2019)	RCN(Cunningham, 2000)	RCN, which combines the convolutional network DenseNet (Huang, 2017) and the gated recurrent unit cells (Cho, 2014), is used to investigate temporal differences across frames.	FaceForensics++ dataset (Rossler, 2019) consist of 1,000 videos.
Analysis of PRNU (Betbeder, 2013)	PRNU	Examination of noisy patterns caused by manufacturer flaws in light-sensitive sensors in digital cameras. Investigate the changes in PRNU pattern among real and deepfake videos, as face changing is thought to change regional PRNU patterns.	10 real and 16 deepfake videos were created by the writers with the help of DeepFaceLab.
Using appearance and behavior (Dufour, 2019)	Face and behavioral traits are used to define rules.	ResNet-101(He, 2016) is used to learn temporal, behavioral biometrics based on facial expressions and head movements, while VGG (Parkhi, 2015) is used to obtain static face biometrics.	FaceForensics++(Rossler, 2019), Google/Jigsaw deepfake detection dataset, DFDC(Dolhansky, 2020), and Celeb-DF(Li, 2020) are some of the datasets used by this model.
Spatio-temporal features with LSTM (Betbeder, 2013)	Convolutional bidirectional recurrent LSTM network (Cai, 2016)	For extracting facial features, an XceptionNet CNN is utilized, while voice embeddings are created by stacking numerous convolution layers. Cross-entropy and Kullback-Leibler divergence are the two loss functions employed here.	The ASVSpooF 2019 Logical Access audio dataset (Todisco, 2019), as well as the FaceForensics++ (Rossler, 2019) and Celeb-DF (5,639 deepfake videos) datasets.
Emotion audiovisual affective cues (Mittal, 2020)	Siamese network (Chopra, 2005)	Emotional and modal aspects Deepfake detection involves extracting embedding vectors for the face and audio.	DFDC (Dolhansky, 2020) and Deepfake TIMIT (Korshunov, 2018).
FakeCatcher (Ciftci, 2020)	CNN (Albawi, 2017)	Because biological signals are not well retained geographically and temporally in deepfakes, extract them from portrait films and utilize them as an implicit diagnostic of authenticity.	UADFV, FaceForensics(Rossler, 2018), FaceForensics++(Rossler, 2019), Celeb-DF(Li, 2020), and a new dataset of 142 videos, independent of the generative model, resolution, compression, content, and context.

In police investigations and criminal trials, photographs and videos have been routinely used as evidence. Digital media forensics professionals with a degree in computer or law enforcement and skill collecting, reviewing, and analyzing digital material may present them as evidence in a court of law. Because even experts are unable to discern manipulated contents, the development of machine learning and AI technologies may have been used to modify these digi-

tal contents, and thus the experts' personal views may not be enough to verify this evidence. Because of the development of a wide range of digital manipulation tools, this aspect must be recognized in today's courtrooms when photographs and videos are used as evidence to convict perpetrator (Maras, 2019). Before digital content forensics results may be utilized in court, they must be proved to be real and reliable. This necessitates meticulous documentation for every step

of the forensics process as well as the methodology used to acquire the results. Although most of these algorithms are inexplicable. AI and Machine learning algorithms can be used to support the determination of the authenticity of digital media and have provided accurate and reliable results. This is a significant obstacle for the use of AI in forensics challenges for not only do forensics experts lack experience in computer algorithms, but computer professionals also lack the ability to properly explain the results because most of these algorithms are black-box models (Malolan, 2020).

This is incredibly significant because the most recent models to generate the most accurate results are based on deep learning methods that involve a large number of neural network parameters. As an outcome, explainable AI in computer vision is a research direction that is required to promote and employ AI and machine learning advances and effects in digital media forensics.

CONCLUSION:

Technologies based on deep learning, such as deepfake, have been advancing at an unprecedented rate in recent years. The global pervasiveness of the Internet makes it possible for malicious face-manipulated videos to be distributed rapidly, posing a threat to social order and personal safety. In order to mitigate the negative effects of deepfake videos on people, research groups and commercial companies around the world are conducting relevant studies. Firstly, we present deepfake video generation technology, followed by the existing detection technology, and finally the future research direction. An emphasis in this review is particularly placed on current detection algorithm problems and promising research. The review places special emphasis on generalization and robustness. This article will hopefully prove useful for researchers who are interested in deepfake detection and in limiting the negative impact of deepfake videos.

ACKNOWLEDGEMENT:

We would like to thank our parents and our entire teacher to support us mentally and monetarily.

CONFLICTS OF INTEREST:

Researcher can use this work only for research purpose. There are no conflicts of interest for the research community.

REFERENCES:

- 1) Adee, S., (2020). What Are Deepfakes and How Are They Created? [Online] Available at: <https://spectrum.ieee.org/what-is-deepfake>
- 2) Afchar, D.a.N.V.a.Y.J.a.E.I., (2018). Mesonet: a compact facial video forgery detection network. In 2018 IEEE International Workshop on Information Forensics and Security (WIFS). *IEEE*. pp. 1- 7.
- 3) Albawi, S. a. M. T. A. a. A. Z. S., (2017). Understanding of a convolutional neural network. In 2017 International Conference on Engineering and Technology (ICET). *IEEE*. pp. 1- 6. <https://ieeexplore.ieee.org/document/8308186>
- 4) Amerini, I.a.C.R., (2020). Exploiting prediction error inconsistencies through LSTM-based classifiers to detect deepfake videos. In Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security. pp.97-102.
- 5) Anon., (2019). The best (and scariest) examples of AI-enabled deepfakes.
- 6) Betbeder, J.a.G.V.a.F.F.a.B.N.N.a.B.G.a.B.E., (2013). Mapping of Central Africa forested wetlands using remote sensing. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, 7(2), pp.53-542.
- 7) Boulkenafet, Z.a.K.J.a.H.A., (2015). Face anti-spoofing based on color texture analysis. In 2015 IEEE international conference on image processing (ICIP). *IEEE*. pp.2636 -2640.
- 8) Breuel, T.M., (2015). Benchmarking of LSTM networks. arXiv preprint arXiv:1508.02774.
- 9) Cai, R. a. Z. X. a. W. H., (2016). Bidirectional recurrent convolutional neural network for relation classification. In Proceedings of the 54th Annual Meeting of the Association for Computational, 1, pp.756-765. <https://aclanthology.org/P16-1072>
- 10) Cheng, Z. a. S. H. a. T. M. a. K. J., (2019). Energy compaction-based image compression using convolutional autoencoder. *IEEE Transactions on Multimedia*, 22(4), pp.860-873.
- 11) Chesney, R.a.C.D.K.R.a.C.D.K., (2018). Deep fakes: A looming challenge for privacy, democracy, and national security. 107 California law review (2019, forthcoming); u of texas law. *Public Law Research Paper*, 692, pp.2018-21.

- 12) Chesney, R.a.C.D., (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Aff.*, **98**, p.147. <https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war>
- 13) Cho, K.a.V.M.B.a.G.C.a.B.D.a.B.F.a.S.H.a.B.Y., (2014). Learning phrase representations using RNN encoder-decoder for statistical machine translation. <https://arxiv.org/abs/1406.1078>
- 14) Chopra, S.a.H.R.a.L.Y., (2005). Learning a similarity metric discriminatively, with application to face verification. In 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05). 1st ed. *IEEE*. pp.539 - 546.
- 15) Chung, J.S.a.S.A.a.V.O.a.Z.A., (2017). Lip reading sentences in the wild. In 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). *IEEE*. pp.3444--3453.
- 16) Ciftci, U.A.a.D.I.a.Y.L., (2020). Fakecatcher: Detection of synthetic portrait videos using biological signals. *IEEE Transactions on Pattern Analysis and Machine Intelligence*.
- 17) Citron, D.K.a.C.R., (2018). Disinformation on Steroids: The Threat of Deep Fakes. *Cyber Brief*.
- 18) Cunningham, G.a.K.A., (2000). An evaluation of the RCN clinical leadership development programme: part 2. *Nursing Standard* (through 2013), **15**(13-15), p.134. <https://doi.org/10.7748/NS2000.12.15.12.34.C2953>
- 19) Cycle, (2017). CycleGAN. Available at: <https://github.com/junyanz/pytorchCycleGAN-and-pix2pix>
- 20) Damiani, J., (2019). A voice deepfake was used to scam a CEO out of \$243,000. *Forbes Magazine*.
- 21) de Lima, O.a.F.S.a.B.S.a.K.B.a.G.A., (2020). Deepfake detection using spatiotemporal convolutional networks. <https://arxiv.org/abs/2006.14749>
- 22) DeepFaceLab, (2016). Explained and usage tutorial. [Online] Available at: <https://mrdeepfakes.com/forums/thread-deepfacelab-explained-and-usage-tutorial>
- 23) Deng, Y.a.Y.J.a.C.D.a.W.F.a.T.X., (2020). Disentangled and controllable face image generation via 3d imitative-contrastive learning. In *Proceedings of the IEEE/CVF Conference on Computer Vision & Pattern Recognition*. pp.5154 - 5163.
- 24) Dimensions, (2021). Deepfake video detection. [Online] Available at: <https://app.dimensions.ai/discover/publication/>
- 25) Dolhansky, B.a.B.J.a.P.B.a.L.J.a.H.R.a.W.M.a.F.C.C., (2020). The deepfake detection challenge (dfdc) dataset. <https://arxiv.org/abs/2006.07397>
- 26) Donahue, J.a.A.H.L.a.G.S.a.R.M.a.V.S.a.S.K.a.D.T., (2015). Long-term recurrent convolutional net-works for visual recognition and description. In *Proceedings of the IEEE conference on computer vision and pattern recognition*. pp.2625 - 2634.
- 27) dss, (2011). DSSIM. [Online] Available at: https://github.com/keras-team/kerascontrib/blob/master/keras_contrib/losses/dssim.py
- 28) Dufour, N.a.G.A., (2019). Contributing data to deepfake detection research. *Google AI Blog*, **1**(2), p.3.
- 29) Face, (2015). Faceswap-GAN. [Online] <https://github.com/shaoanlu/faceswap-GAN>
- 30) Fish, T., (2019). Deep fakes: AI-manipulated media will be weaponised to trick military.
- 31) Floridi, L., (2018). Artificial intelligence, deep-fakes and a future of ectypes. *Philosophy & Technology*, **31**(3), pp.317-321.
- 32) Gevins, A.S.a.M.N., (1988). Applications of neural-network (NN) signal processing in brain research. *IEEE Transactions on Acoustics, Speech, & Signal Processing*, **36**(7), pp.1152-1161.
- 33) Goodfellow, I.a.P.-A.J.a.M.M.a.X.B.a.W.-F.D.a.O.S.a.C.A.a.B.Y., (2014). Generative adversarial nets. *Advances in neural information processing systems*, **27**.
- 34) Goodfellow, I.a.P.-A.J.a.M.M.a.X.B.a.W.-F.D.a.O.S.a.C.A.a.B.Y., (2014). Generative adversarial nets. *Advances in neural information processing systems*, **27**.
- 35) Guan, H.a.K.M.a.R.E.a.L.Y.a.Y.A.N.a.D.A.a.Z.D.a.K.T.a.S.J.a.F.J., (2019). MFC datasets: Large-scale benchmark datasets for media forensic challenge evaluation. In 2019 IEEE Winter Applications of Computer Vision Workshops (WACVW). *IEEE*. pp. 63 - 72.

- 36) Guardian, T., (2019). Chinese deepfake app Zao sparks privacy row after going viral. <https://www.theguardian.com/technology/2019/sep/02/chineseface-swap-app-zao-triggers-privacy-fears-viral>
- 37) Guera, D.a.D.E.J., (2018). Deepfake video detection using recurrent neural networks. In 2018 15th IEEE international conference on advanced video and signal based surveillance (AVSS). *IEEE*. pp. 1- 6.
- 38) Guo, B.a.D.Y.a.Y.L.a.L.Y.a.Y.Z., (2020). The future of false information detection on social media: New perspectives and trends. *ACM Computing Surveys (CSUR)*, **53**(4), pp.1 - 36. <https://doi.org/10.1145/3393880>
- 39) Ha, S.a.K.M.a.K.B.a.S.S.a.K.D., (2020). Marionette: Few-shot face reenactment preserving identity of unseen targets. Proceedings of the AAAI Conference on Artificial Intelligence, **34**(7), pp.10893 -10900.
- 40) Hassan MK, Hassan MR, and Biswas M. (2021). A survey on an intelligent system for persons with visual disabilities. *Aust. J. Eng. Innov. Technol.*, **3**(6), 97-118. <https://doi.org/10.34104/ajeit.021.0970118>
- 41) Hasan, H.R.a.S.K., (2019). Combating deepfake videos using blockchain and smart contracts. *IEEE Access*, **7**, pp.41596-41606.
- 42) He, K.a.Z.X.a.R.S.a.S.J., (2016). Deep residual learning for image recognition. In Proceedings of the IEEE conference on computer vision and pattern recognition. pp.770 - 778. <https://doi.org/10.1109/cvpr.2016.90>
- 43) Huang, G.a.L.Z.a.V.D.M.L.a.W.K.Q., (2017). Densely connected convolutional networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition*. pp.4700 - 4708. <https://arxiv.org/abs/1608.06993>
- 44) Hussain, S.a.N.P.a.J.M.a.K.F.a.M.J., (2021). Adversarial deepfakes: Evaluating vulnerability of deepfake detectors to adversarial examples. In *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*. pp.3348-3357.
- 45) Hwang, T., (2020). Deepfakes: A Grounded Threat Assessment. Centre for Security and Emerging Technologies, *Georgetown University*.
- 46) Jafar, M.T.a.A.M.a.A.-Z.M.a.E.A., (2020). Forensics and analysis of deepfake videos. In *2020 11th International Conference on Information and Communication Systems (ICICS)*. *IEEE*. pp. 05-058.
- 47) Ker, (2014). VGGFace: VGGFace implementation with Keras framework. <https://github.com/rcmalli/keras-vggface>
- 48) Korshunov, P.a.M.S., (2018). Speaker inconsistency detection in tampered video. In *2018 26th European signals processing conference (EUSIPCO)*. *IEEE*. pp.2375 - 2379.
- 49) Korshunov, P.a.M.S., (201). Vulnerability assessment and detection of deepfake videos. In *2019 International Conference on Biometrics (ICB)*. *IEEE*. pp.1 - 6.
- 50) Lattas,A.a.M.S.a.G.B.a.P.S.a.T.V.a.G.A.a.Z.S., (2020). AvatarMe: Realistically Renderable 3D Facial Reconstruction" In-the-Wild". In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. pp.760 - 769.
- 51) Li, Y.a.L.S., (2018). Exposing deepfake videos by detecting face warping artifacts. <https://www.arxiv-vanity.com/papers/1811.00656/>
- 52) Li, Y.a.C.M.-C.a.L.S., (2018). In icu oculi: Exposing ai created fake videos by detecting eye blinking. In *2018 IEEE International Workshop on Information Forensics and Security (WIFS)*. *IEEE*. pp.1 - 7.
- 53) Li, L.a.B.J.a.Y.H.a.C.D.a.W.F., (2019). Face-shifter: Towards high fidelity and occlusion aware face swapping. <https://lingzhili.com/FaceShifterPage/>
- 54) Li, Y.a.Y.X.a.S.P.a.Q.H.a.L.S., (2020). Celebdf: A large-scale challenging dataset for deepfake forensics. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. pp.3207 - 3216.
- 55) Lin, J.a.L.Y.a.Y.G., (2021). FPGAN: Face de-identification method with generative adversarial networks for social robots. *Neural Networks*, **133**, pp.132 - 147.
- 56) Liu,M.Y.a.H.X.a.M.A.a.K.T.a.A.T.a.L.J.a.K.J.,(2019). Few-shot unsupervised image-to-image translation. In *Proceedings of the IEEE/CVF*

- International Conference on Computer Vision*. pp.10551 - 10560.
<https://arxiv.org/abs/1905.01723>
- 57) Liu, X. a. Z. F. a. H.Z.a.M.L.a.W.Z.a.Z.J.a.T.J., (2021). Self-supervised learning: Generative or contrastive. *IEEE Transactions on Knowledge and Data Engineering*.
- 58) Lyu, S., (2018). Detecting deepfake videos in the blink of an eye. *The Conversation*, 29.
- 59) Lyu, S., (2020). Deepfake detection: Current challenges and next steps. In *2020 IEEE International Conference on Multimedia & Expo Workshops (ICMEW)*. IEEE. pp.1 - 6.
<https://rc.signalprocessingsociety.org/workshops/icme-2020/ICME20VID102.html?source=IBP>
- 60) Malolan, B. a. P. A. a. K. F., (2020). Explainable deep-fake detection using visual interpretability methods. In *2020 3rd International Conference on Information and Computer Technologies (ICI-CT)*. IEEE. pp.289 - 293.
- 61) Maras, M.-H.a.A.A., (2019). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake videos. *The International Journal of Evidence & Proof*, **23**(3), pp.255 - 262.
- 62) Matern, F.a.R.C.a.S.M., (2019). Exploiting visual artifacts to expose deepfakes and face manipulations. In *2019 IEEE Winter Applications of Computer Vision Workshops (WACVW)*. IEEE. pp.83 - 92.
https://fau1-files.cs.fau.de/public/mmsec/pub/matern_ivfws_2019_face_artifacts.pdf
- 63) Matern, F.a.R.C.a.S.M., (2019). Exploiting visual artifacts to expose deepfakes and face manipulations. In *2019 IEEE Winter Applications of Computer Vision Workshops*. IEEE. pp.83-92.
- 64) Mittal, T.a.B.U.a.C.R.a.B.A.a.M.D., (2020). Emotions Don't Lie: An Audio-Visual Deepfake Detection Method using Affective Cues. In *Proceedings of the 28th ACM international conference on multimedia*. pp.2823 - 2832.
- 65) net, (2015). FaceNet. [Online] Available at:
<https://github.com/davidsandberg/facenet>
- 66) Nirkin, Y.a.K.Y.a.H.T., (2019). Fsgan: Subject agnostic face swapping and reenactment. In *Proceedings of the IEEE/CVF international conference on computer vision*. pp.7184 - 7193.
- 67) Park, T. a. L. M. -Y. a. W.T.-C.a.Z.J.-Y., (2019). Semantic image synthesis with spatially-adaptive normalization. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. pp. 2337 - 2346.
<https://arxiv.org/abs/1903.07291>
- 68) Parkhi, O. M. a. V. A.a.Z.A., (2015). Deep face recognition.
- 69) Punnappurath, A.a.B.M.S., (2019). Learning raw image reconstruction-aware deep image compressors. *IEEE transactions on pattern analysis and machine intelligence*, **42**, pp.1013 - 1019.
- 70) Reddit, (2015). FakeApp 2.2.0. [Online]
<https://www.malavida.com/en/soft/fakeapp/>
- 71) Rössler, A. a. C. D. a. V. L. a.R.C.a.T.J.a.N.M., (2018). Faceforensics: A large-scale video dataset for forgery detection in human faces.
<https://arxiv.org/abs/1803.09179>
- 72) Rössler, A. a. C. D. a. V. L. a. R.C.a.T.J.a.N.M., (2019). Faceforensics++: Learning to detect manipulated facial images. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*. pp.1 - 11.
- 73) Sabir, E.a.C.J.a.J.A.a.A.W.a.M.I.a.N.P., (2019). Recurrent convolutional strategies for face manipulation detection in videos. *Interfaces (GUI)*, **3**(1), pp.80 - 87.
https://www.isi.edu/people/wamageed/publications/recurrent_convolutional_strategies_face_manipulation_detection_videos
- 74) Samuel, S., (2019). A guy made a deepfake app to turn photos of women into nudes. It didn't go well.
- 75) Sanderson, C., (2002). The vidtimit database. *IDIAP*. **75**.
- 76) Schroepfer, M., (2019). Creating a data set and a challenge for deepfakes. *Facebook artificial intelligence*, **5**.
- 77) Schroff, F.a.K.D.a.P.J., (2015). Facenet: A unified embedding for face recognition and clustering. In *Proceedings of the IEEE conference on computer vision and pattern recognition*. pp.815-823. <https://doi.org/10.1109/CVPR.2015.7298682>
- 78) Simonyan, K.a.Z.A., (2014). Very deep convolutional networks for large-scale image recognition. <https://arxiv.org/abs/1409.1556>

- 79) Tewari, A.a.Z.M.a.B.F.a.G.P.a.K.H.a.P.P.a.T.C., (2018). High-fidelity monocular face reconstruction based on an unsupervised model-based face auto encoder. *IEEE transactions on pattern analysis and machine intelligence*, **42**(2), pp. 357 -370.
<https://doi.org/10.1109/TPAMI.2018.2876842>
- 80) Thies, J. a. E. M. a. T. A.a.T.C.a.N.M., (2020). Neural voice puppetry: Audio-driven facial reenactment. In *European Conference on Computer Vision*. Springer. pp.716 - 731.
- 81) Todisco, M.a.W.X.a.V.V.a.S.M.a.D.H.a.N.A.a.Y. J.a.E.N.a.K.T.a.L.K.A., (2019). ASVspooF 2019: Future horizons in spoofed and fake audio detection. <https://arxiv.org/abs/1904.05441>
- 82) Tolosana, R. a. V. -R. R. a.F.J.a.M.A.a.O.-G.J., (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion*, **64**, pp.131 - 148.
- 83) Turek, M., (2020). Media Forensics (MediFor). [Online] Available at:
<https://www.darpa.mil/program/media-forensics>
- 84) Verdoliva, L., (2020). Media forensics and deepfakes: an overview. *IEEE Journal of Selected Topics in Signal Processing*, **14**, pp.910 - 932.
- 85) Wang, W. a. H. Q. a. Y.S.a.Y.C.a.N.U., (2017). Shape inpainting using 3d generative adversarial network and recurrent convolutional networks. In Proceedings of the *IEEE international conference on computer vision*. pp.2298 - 2306.
- 86) Wright, R.E., (1995). Logistic regression.
<https://doi.org/10.4236/apm.2015.53016>
- 87) Yang, X. a. L. Y. a. L. S., (2019). Exposing deep fakes using inconsistent head poses. In *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE. pp.8261-8265.
- 88) Yang, C.a.D.L.a.C.Y.a.L.H., (2021). Defending against ganbased deepfake attacks via transformation-aware adversarial faces. In *2021 International Joint Conference on Neural Networks (IJCNN)*. IEEE. pp.1 - 8.
<https://arxiv.org/abs/2006.07421>
- 89) Zakharov, E.a.S.A.a.B.E.a.L.V., (2019). Few-shot adversarial learning of realistic neural talking head models. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*. pp.9459-9468.
- 90) Zhao, J. a. M. M. a.L.Y., (2016). Energy-based generative adversarial network. arXiv preprint <https://arxiv.org/abs/1609.03126v2>
- 91) Zhou, P.a.H.X.a.M.V.I.a.D.L.S., (2017). Two-stream neural networks for tampered face detection. In *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. IEEE. pp.1831-1839.
<https://arxiv.org/abs/1803.11276>
- 92) Zhou, X.a.Z.R., (2020). A survey of fake news: Fundamental theories, detection methods, and opportunities. *ACM Computing Surveys (CSUR)*, **53**(5), pp.1 - 40.
<https://doi.org/10.1145/3395046>
- 93) Zubiaga, A.a.A.A.a.B.K.a.L.M.a.P.R., (2018). Detection and resolution of rumours in social media: A survey. *ACM Computing Surveys (CSUR)*, **51**(2), pp.1-36.

Citation: Rahman A, Islam MM, Moon MJ, Tasnim T, Siddique N, Shahiduzzaman M, and Ahmed S. (2022). A qualitative survey on deep learning based deep fake video creation and detection method. *Aust. J. Eng. Innov. Technol.*, **4**(1), 13-26. <https://doi.org/10.34104/ajeit.022.013026> 