International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Survey Paper Volume-7, Issue-8 , August 2020 Regular Edition E-ISSN: 2349-7084

A Survey on Deepfake Detection Techniques

Bismi Fathima Nasar[1*], Sajini. T [2], Elizabeth Rose Lalson [3]

[1*]*Computer Science and Engineering, ER & DCI Institute of Technology, KTU, Thiruvananthapuram, India*
[2] *Knowledge Resource Centre, CDAC, Thiruvananthapuram, India*
[3] *Computer Science and Engineering, ER & DCI Institute of Technology, KTU, Thiruvananthapuram, India*

e-mail: bismiputhuparambil12@gmail.com, sajini@cdac.in, elizabeth@cdac.in,
**Corresponding Author: bismiputhuparambil12@gmail.com,*

Available online at: http://www.ijcert.org

Received: 06/Aug/2020 Revised: 24/Aug/2020 Accepted: 28/Aug/2020 Published: 02/Sep/2020

Abstract: - With the recent advancement in the Deep Learning algorithm, its application has been broadened over various fields ranging from big data analytics to human biometric systems. One such field where it takes up the hand is the implementation of various application like FaceApp, FakeApp etc. that is used in the generation of manipulated media files which is termed as Deepfake. These application has a wider increase in its popularity among common public due to its user friendly features and are used in various domains like Digital Fraud, Cyber Crimes, Politics and in even in Military Activities. So, it is very much important to develop some kind of detection techniques that can take away this kind of forgeries and put up a new step in video and audio forensics. In this paper, we present the various creation and detection techniques that is up now in research in Deepfake using various techniques like Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Long Short Term Memory (LSTM) etc. and thus provide a backbone in the implementation of a new scheme that would be more compactable and accurate in the detection of Deepfakes. Also we done a comparison study on various techniques under traditional and state of the art approach and brought up a conclusion that most of the techniques under traditional approach are time consuming process, need expertise knowledge over the technology for the user to use them etc. where as in the case of state of the art approach, the techniques require less time for processing and anyone with less knowledge over the technology can use this technologies for the creation and detection of Deepfake.

Keywords: Recurrent Neural Network, Long Short Term Memory, Convolutional Neural Network, Deepfake

---

1. Introduction

In early 1865, the first attempt was found in the generation of a Deepfake image where they swapped the face of U.S President Abraham Lincoln's with the southern politician John Calhoun in an iconic portrait of Lincoln [2]. Deepfake are digitally manipulated media generated using various advanced software that depict people saying or doing things that they actually don't as stated in [19]. There were many techniques that were brought up in the field of image and signal processing during the early stage of audio and video manipulation. But the level of accuracy has been very low when compared to the recent creation and detection schemes in deep learning involving auto encoder and deep convolution networks. These deep learning algorithms monitor the facial expression and movements of a person and take up for learning and push it over another target person to generate something called a "Deepfake". Usually, these learning phases required a large number of images or videos to train the model to create photorealistic fake copies out of it. Usually, this dataset for free use is generated from the images or videos of political leaders and celebrities available online, and thus, for this reason, these people are the initial target of this Deepfake. The first Deepfake video [20] was generated in 2017 by swapping the face of celebrities over the porn video. But the most popular one was the generated out from the speech of Barack Obama during late 2017 which went viral all over the social media site and this effect the political election conducted in the U.S. Thus, it has fallen into

the category of a national threat since these Deepfake are used in the generation of videos of various political leaders for some kind of political manipulation. This was even used to generate the fake satellite image of the Earth that contains an object that really doesn't exist. This was done to falsify the military analyst and even mislead a troop to cross a bridge during a battle. Recent advancement has led to the generation of these Deepfake videos even with a single image so it becomes a public threat among society. Along with the disadvantages, there are also many advantages for these Deepfake mainly in the field of media production where they can recreate some videos of people who are lost their voice or to update episodes without reshooting them.

The base for the development of Deepfake in the recent scenario using **Generative Adversarial Network (GAN)** in Deep Learning. Here the Deepfake video is usually created by using two GAN networks based on the AI system as shown in fig 1. First one is called as the Generator and the other is called the Discriminator. Basically, the generator is used in the creation of Deepfake video and the discriminator determines whether the given video is fake or not. Each time the discriminator precisely identifies a media as fake, it gives the generator a clue about how it shouldn't create the next Deepfake media. The Generator and the Discriminator together will form something called a Generative Adversarial Network (GAN). The first step is to create a training dataset for the GAN network which can be used to train the generator and the discriminator. Once the generator starts its training with the training dataset, it saves the specific features over the network layers and with these features it generate the fake media samples which is fed to the discriminator as the training samples. Thus, both are dependent to each other over their performance.

The advanced development of these deep learning techniques which are used in the implementation of most of the online Deepfake generators and their ease of use has made it more popular among both professionals as well as novices. There are many deep learning algorithms like the convolutional neural network, recurrent neural network, long short-term memory, and even the hybrid combination of these techniques is been used for the creation and generation of Deepfake. So, finding the truth behind these digital evidences is a critical challenge among the researchers and investigators in media forensics. To address the threat and to bring up more research over this field, Facebook Inc. tied up with Microsoft Corp and the Partnership on AI coalition have launched a Deepfake detection challenge to bring up more research and development in the detection and prevention of Deepfake. There was also a similar event hosted by Google with the release of a Google Net dataset for the research purpose.

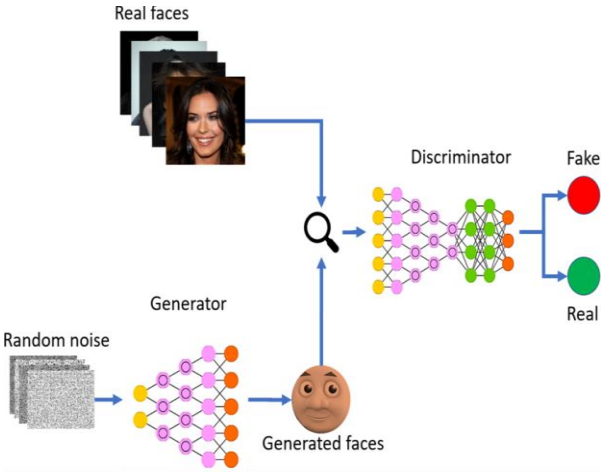

Fig. 1. Generative Adversarial Networks

Rest of the paper is organized as follows, Section I discussed the introduction of Deepfake, Section II contain the related work on Deepfake Creation and Detection Techniques, Section III contain some challenges involved in the research of Deepfake, Section IV concludes research work with future directions.

2. Related Work

In this section, we are going to discuss the various literature work in the Deepfake creation and detection domain. In the paper [1], they give a comprehensive survey on the video content authentication techniques. These techniques usually categorized as active and passive models and this paper gives a detailed survey on the various passive blind video content authentication with the main focus on forgery detection, video recapture, and phylogeny detection. Later with the advancement in Deep Learning, Deepfake has become popular among a wide range of users due to the high quality of the tampered videos been generated and the ease of use ability of the online Deepfake generation and face-swapping applications implemented using deep learning techniques. Deep Learning is well known for its ability in handling complex and high dimensional data. Deep learning models such as encoder-decoder or auto encoders were earlier used and was widely used in the computer vision domain to solve several problems. But these auto encoders had the following disadvantages when compared to the recently used convolutional or neural networks [2]. First disadvantage is the Lack of temporal awareness which is the basic source of multiple abnormalities in the auto encoders. Because the auto encoder uses a frame-by-frame generation for the analysis of the Deepfake videos and was completely unaware of any previously generated face that it could have

 https://doi.org/10.22362/ijcert/2020/v7/i08/v7i0808

created automatically. Next is the inconsistencies existing with the face encoder i.e. the Encoder is unaware of the skin tone or other background information. It is very common to have boundary effects when combining the new face image with the rest of the frame. The third disadvantage is the visual inconsistency that exist due to the use of multiple cameras, different lighting conditions, or simply the use of different video codecs which make it tough for the auto encoder to create very accurate and realistic videos under different conditions. Finally, it is the inconsistency in choosing the illuminates between the different background with frames. This usually leads to blinking in the face region in the most of the Deepfake videos. So, to overcome these disadvantages over the auto encoder, another deep learning technique like the convolutional neural network (CNN), Recurrent Neural Network (RNN), Generative Adversarial Network (GAN), etc. were developed.

With the advancement in this convolutional net- work, there were many other schemes were developed in the creation and detection of Deepfake using Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), even the hybrid approaches of all the recent algorithm in the Deep Learning, etc. David Guera and Edward J Delp [2] brings up the first approach where the frame level features are extracted out after each processing in convolutional neural network and these features are fed into the recurrent neural network as training samples and the output from this RNN is the classification result. Along with the combination of CNN and RNN, a set of encoder-decoder with shared weight for encoder network is also used for dimensionality reduction and image compression in the training and generation phase and an LSTM network is used for the temporal sequential analysis. Another such approach was brought up by Ekraam Sabir in [3], the face manipulation detection using RNN strategies where they use a combination of variations in RNN models along with domain-specific face pre-processing techniques to obtain state-of-the-art performance on publicly available facial manipulation videos generated through FakeApp, Face2Face, and FaceSwap and this experimental evaluation shows an accuracy of 4.55%. A similar approach was stated in [4] for the swapped face detection using Deep Learning and Subjective Assessment. In this paper, they proposed a swapped face detection system which shows 96% positive result with few false alarms when compared with the other existing systems. Along with the detection of face-swapping, this model also evaluates the uncertainty in each prediction which is very much critical in the evaluation of the performance of a system. In order to improve this predictability, they have set a website to review the human response over the dataset by collecting pair to pair comparison of images over the videos on human. Based on these comparisons, images are classified as real or fake. The output can be based on some kind of probability and this classification output is compared with the outputs from their automatic model which gives a very good but showing imperfect, correspondence with linear correlations greater than 0.75. This experiment results show that this proposed model is much better when compared to the existing systems.

When it comes to the most advanced version of this deep neural network, a hybrid approach was implemented. A two-stream neural network was proposed in [5] where they train a GoogLeNet to detect the tampering artifacts like strong edges near lips, blurred areas on the forehead, etc. in image classification stream and in the second stream, a patch-based three-layer network is trained for capturing local noise components and camera characteristics. This network is designed to determine whether the obtained both patches comes from the same image. It was found that the patches extracted out from the real samples around the face region seems very simpler and has very small distance between them and while in the case of the tampered video, the patches from the face region will be different and will have a larger distance between them. Also, in the case of tampered video, the characteristics between the frames near the face region will be different when compared to the authentic or real one and here the classification based these features are done by using an SVM classifier. They developed another dataset generated by two online face-swapping application that consists of 2010 manipulated images, each of which contains a forged face for the performance evaluation. The experimental results show that this approach is able to learn both manipulated artifacts and hidden noise components.

Another concept in the hybrid model was pairwise learning [6] where a deep learning-based approach is used to identify manipulated image is by combining the contrastive loss. First, state-of-the-art GANs network will be used to generate pair of fake and real images. Then, these pair of image samples are fed into common fake feature network (CFFN) to learn the distinguishing feature between the fake image and real image as a paired information. Then in the final stage, a small network will be used to combine these features to make the decision on whether its fake or real. Experimental results show that the proposed method has high performance when compared to the existing state of the art image detection techniques. In the paper [7], a task-oriented GAN for PoISAR image classification and clustering techniques were used which consists of a Triplet network. Along with the generator and the discriminator, they are another network called the task network or T-net. The network in this proposed system basically has two task network – one is called as the classifier and another is called as a clustered network. The

first is the learning stage which has the two competing generator and discriminator network which work hand in hand as in GANs network. In the second phase, the generator network is adjusted and oriented as a Task network where some samples from the training samples are assign with specific task that is the generation of the manipulated data. This takes up the advantage of a GAN network and also overcome the disadvantage of the GAN network. After completing the learning phase, manipulated data are employed to take up the task to enhance the training sets and avoid overfitting among samples so that Task-Oriented GAN performs well even if the manual-labelled data are small. To verify the accuracy of the Task Network, a visual comparison is provided where some manipulated digits generated from Task-Oriented GAN in parallel with that from GAN as illustrated. The most important thing to be considered is that there is a greater difference between the PolSAR image dataset and this PolSAR image dataset is used in this scheme as the image. The performance is evaluated through several experiments with this PolSAR image dataset and it shows that on three PolSAR images, the proposed method shows high accuracy in dealing with PolSAR image classification and clustering.

Later on, a Hybrid combination of LSTM and Encoder-Decoder architecture [8] was developed for image forgery detection. In this system, a high-confidence architecture is used which utilizes resampling features used to capture artifacts. These artifacts include JPEG quality loss, up sampling, down sampling, rotation, etc., Long-Short Term Memory (LSTM) cells, an encoder-decoder network to distinguish whether the specific area of the image has tampered or not. Here they use a spatial map and the frequency domain correlation to determine the distinct characteristics of the manipulated and non-manipulated regions by combining the effort of LSTM and Encoder network. Finally, the decoder network learns how it is mapped from low-resolution feature maps to pixel-wise predictions for tamper detection. Through this work, they also present a dataset that can be used in further research work on media forensics. With several experiments conducted with different datasets, they brought up to the conclusion that their scheme was efficiently segmented various types of manipulations including copy-move, object removal, and splicing. The active learning approach was also stated in this field of deep learning [11] as a wider advancement to acquire annotations for data from a human reaction by selecting informative samples with a high probability to enhance performance. This model is implemented to generate a label to the data in a cheaper manner. Here for each sample, a reward will be assigned by the classifier trained with these pre-existing labels and these rewards can be used to guide a conditional GAN to generate useful and informative samples with a higher probability for a certain label. Finally, with the evaluation of this model, the effectiveness of the model can be estimated showing that the generated samples are capable of improving the classification performance in popular image classification tasks. Then certain pre-processed authentic or fake images [9] can be used to train the CNN network in the generation which destroys the unstable low-level noise cues on the manipulated images and the discriminative network is forced to learn more distinct features to classify the manipulated and real face images. A key difference with other GAN related methods is that here they use an image pre-processing step in the training stage to destroy low-level unstable artifacts of GAN images and force the discriminator to focus on more distinct clues and by doing so they improve the generalization capabilities. But this approach was difficult to implement and has got only some preliminary results. Thus, to improve the discriminative capabilities, face wrapping artifact detection technique was developed [10]. This method was developed based on the observation that current Deepfake algorithms can generate images of low resolution and further wrapping is essential to make the manipulated one with that of the original one. So, such transform leaves artifact called resolution inconsistency along the line of fake one ad these artifacts can be effectively captured using a CNN network for detecting the authenticity of the videos.

Many other approaches with indirect implementation of Deep Learning was also implemented in parallel to the direct approaches but shows less accuracy when compared to other existing systems. One such approach was proposed in [11] where an automated system is developed that can detect the forgery in the videos been recorded in the camera and in its audio channel. Here they used the method in which they detect the audio-visual inconsistencies with certain artifacts like lip syncing, Dubbing inconsistencies etc. In the experimental evaluation, the proposed system is evaluated with various classifier like the LSTM, GMM, PCA etc. but given a better result only with LSTM which flows as the drawback of the system. Another such approach in the detection of the forgery in the images and videos was a capsule forensic approach stated in the article [12] where they use a capsule network to detect the anomaly in the replay attack using printed images and videos to the computer-generated video using deep convolution neural network. This experiment brings up the feasibility of generating a common detection technique that can be used to detect the forgery in the videos as well as images. Here the capsule network can be used in the domain along with computer vision where they use random noise samples in the training phase. The main aim of this work was to protect the random samples against machine attacks as well as mixed attacks. Another approach

 https://doi.org/10.22362/ijcert/2020/v7/i08/v7i0808

is the Eye blinking detection [13] where the temporal features of the eye and the inconsistency in the eye blinking is detected to identify the manipulation in the sample file using LSTM.

Finally, we provide a detail on a rare approach completely out from deep learning domain that can be used for the forgery detection in [15] where they use a PRNU (Photo Response Non-Uniformity) analysis for detecting the deep fake video manipulation. In this approach, the videos are divided into different frames and the frames corresponding to the face is cropped. Then the mean correlation is calculated between the authentic and Deepfake one is calculated to determine which one is fake and which is not. This method was also used to determine the amount of tampering in each Deepfake videos. PRNU analysis shows a notable difference in mean normalized cross-correlation scores between real and Deepfake medias. In the early stage of implementation of the detection techniques, there was no much academic paper found on the detection of Deepfake. Although efforts have been brought up to detect and remove these kinds of videos from websites such as Gyfcat [Matsakis, 2018]. Gyft attempts to use artificial intelligence and facial recognition software to mark inconsistencies in the facial region of an uploaded video.

Comparison Chart on Various Deepfake Detection Technologies

The table below shows the summary chart on the various Deepfake Detection Technologies mentioned in the related works.

Technology	Features	Pros	Cons	Dataset Used
CNN, RNN[2]	Temporal-aware pipeline to automatically detect Deepfake videos.	Achieve competitive results in this task while using a simple architecture	Effective with video of size as fewer as 2 seconds.	300 video from multiple video hosting websites and 300 from HOHA dataset
CNN, RNN[3]	Suggest a best strategy for combining variations in different CNN models along with domain specific face pre-processing techniques	Better Performance than the existing State of the art approaches	It shows a very poor performance in Multi-layer recurrent network with the significant increase in the parameters added up in the layers	FaceForensics ++ dataset
Deep Learning, Face swapping [4]	Deep transfer learning for face swapping detection	Provide Uncertainty in each prediction along with accuracy	Provide less accuracy rate over comparison on human subjects	Generated one of the largest face swapped dataset with still images and is public now.
Two-Stream Neural Network, RNN [5]	Detect the tampering artifacts like strong edges near lips, blurred areas on the forehead, etc. and analyse camera characteristics and local noise components	This approach is able to learn both manipulated artifacts and hidden noise components.	-	Dataset generated by two online face-swapping application that consists of 2010 manipulated images
CFFN, RNN, GAN [6]	A deep learning-based approach is used to identify manipulated image is by combining the contrastive loss	Outperformed other state-of-the-art methods in terms of precision and recall rate	-	CelebA Dataset
GAN, Image Clustering, PoISAR[7]	Understand the difficulty in PoISAR Image interpretation and solve small sample problems.	It given out good performance and many other datasets can be applied.		PoISAR datasets
Hybrid LSTM, Encoder-Decoder[8]	Larger receptive fields and frequency domain correlation is used to classify	Effective against various type of Manipulation like copy-move forgery, object removal etc.	-	Large Image splicing dataset is introduced.
CNN[9]	Unstable low level noise components gets destroyed and more intrinsic features are used to classify	Effective method than existing one	Only achieved some preliminary results	CelebA-HQ
CNN[10]	Detect the distinct artifacts that exist only in the fake videos.	Doesn't require Deepfake generated image as negative training samples	Less Robust for multiple video compression methods	DEEPFAKE TIMIT
Lip syncing, dubbing detection, GAN, LSTM, GMM, SVM, MLP[11]	Automatic system to detect the audio-visual inconsistencies	Only LSTM given better result on their experiment in three datasets	In all the other methods, there was no better result as in LSTM	VidTIMIT, AMI, and GRID
Capsule Network, Deep CNN [12]	Proposed a system to detect the forgery in image as well as video	Extended the application of Capsule Network over Deep Learning Network	Need to be more robust on mixed attack.	Computer generated images and videos
Eye Blinking, LSTM [13]	Use LRCN to learn temporal features in Eye	Effective method under face images	Only effective with face images with a clear cut on eye is visible	49 presentation videos and its manipulated ones
Attribution based confidence network (ABC)[14]	State of the art ABC metric method and the ABC value for real video is 0.94.	New approach for detection was developed	-	Deepfake TIMIT, self-generated dataset from commercial website, COHFACE, YouTube

 https://doi.org/10.22362/ijcert/2020/v7/i08/v7i0808

				videos
PRNU[15]	Use the mean normalised cross correlation scores between authentic videos and Deepfakes	Effective detection technique with large datasets	The dataset is too small to formulate guidelines for likelihood ratios	Real video taken using Canon PowerShot SX210 IS and manipulation is done.

3. Challenges

Open-source software and apps for such face-swapping lead to a large number of Deepfake videos generated and have a greater impact on social media. It has become a technical challenge for the detection and filtering of such video contents. The most important and foremost challenge involved in the development of Deepfake forgery detection technique is the lack of availability of high-quality Deepfake and original video dataset which can be used as the training dataset for the purpose research works and the available dataset will have only anyone among them that is either the original one or the deep fake one. Another important challenge is the incompatibility of these detection techniques and their associated packages in the common human user systems. These challenges always pull the research works backward.

4. Conclusion and Future Scope

Deepfakes are hyper-realistic digitally manipulated video of people doing or saying things they actually don't. Mere visual verification is not enough to make a judgment on the veracity and also Current technologies to check if the footage has been altered are not reliable. Since the visual quality of Deepfakes will soon become so flawless that it will be hard to make a judgment on veracity by mere visual verification. Digger's solution for this is to use of state-of-the-art technologies to develop a toolkit that can detect the forgery in Deepfakes. So, it is very much important to develop a system that can detect the forgery in the Deepfake videos. Thus, future research can suggest a system that can automatically detect the Deepfake videos that use an audio-visual approach that detects the inconsistency that exists with lip movements and speech in audio. Here, we can also apply several baseline methods including simple principal component analysis (PCA) and linear discriminant analysis (LDA) approaches used for the extraction of the feature vectors corresponding to the input video and the approach based on image quality metrics (IQM) and support vector machine (SVM) in CNN network can be used for the classification of the video as real or fake based on the correlation between the feature vectors.

5. References

[1] Raahat Devender Singh, Naveen Aggarwal*," Video content authentication techniques: a comprehensive survey*", Springer, Multimedia Systems, pp. 211- 240, 2018.

[2] David G'uera Edward J. Delp," *Deepfake Video Detection Using Recurrent Neural Networks*", Video and Image Processing Laboratory (VIPER), Purdue University,2018.

[3] Ekraam Sabir, Jiaxin Cheng, Ayush Jaiswal, Wael AbdAlmageed, Iacopo Masi, Prem Natarajan," *Recurrent Convolutional Strategies for Face Manipulation Detection in Videos*", In proceeding of the IEEE Xplore Final Publication, pp. 80-87, 2018.

[4] Xinyi Ding, Zohreh Razieiy, Eric C, Larson, Eli V, Olinick, Paul Krueger, Michael Hahsler," *Swapped Face Detection using Deep Learning and Subjective Assessment*", Research Gate, pp. 1-9, 2019.

[5] Peng Zhou, Xintong Han, Vlad I. Morariu Larry S. Davis," *Two-Stream Neural Networks for Tampered Face Detection"*, IEEE Conference on Computer Vision and Pattern Recognition, 2019

[6] Chih-Chung Hsu, Yi-Xiu Zhuang, and Chia-Yen Lee," *Deep Fake Image Detection based on Pairwise Learning*", MDPI, Applied Science,2020, doi:10.3390/app10010370.

[7] Fang Liu, Licheng Jiao, Fellow, IEEE, and Xu Tang, Member" *Task-Oriented GAN for PolSAR Image Classification and Clustering*", IEEE Transactions On Neural Networks and Learning Systems, Volume 30, Issue 9, 2019.

[8] Jawadul H. Bappy, Cody Simons, Lakshmanan Nataraj, B.S. Manjunath, and Amit K. Roy-Chowdhury," *Hybrid LSTM and Encoder-Decoder Architecture for Detection of Image Forgeries*", IEEE Transaction on Image Processing, Volume: 28 , Issue: 7 ,pp. 1-14, 2019.

[9] Xinsheng Xuan, Bo Peng, Wei Wang and Jing Dong," *On the Generalization of GAN Image Forensics"*, Computer Vision and Pattern Recognition, Cornell University, Volume 1, pp. 1-8, 2019.

[10] Yuezun Li, Siwei Lyu," *Exposing DeepFake Videos by Detecting Face Warping Artifacts*", In Proceedings of the IEEE Xplore Final Publication, pp. 46- 52, 2019.

[11] Pavel Korshunov, S´ebastien Marcel," *Speaker Inconsistency Detection in Tampered Video*", 26th European Signal Processing Conference (EUSIPCO), 2018, ISBN 978-90-827970-1-5.

[12] Huy H. Nguyen, Junichi Yamagishi, and Isao Echizen*," Capsule-Forensics: Using Capsule Networks to detect Forged Images and Videos*", ICASSP, pp. 2307 – 2311, 2019

[13] Li, Y., Chang, M. C., and Lyu, S, "*Exposing AI created fake videos by detecting eye blinking*", In IEEE International Workshop on Information Forensics and Security (WIFS) (pp. 1-7). 2018.

[14] Steven Fernandes, Sunny Raj, Rickard Ewetz, Jodh Singh Pannu, Sumit Kumar Jha, Eddy Ortiz, Iustina Vintila, Margaret Salte," *Detecting deepfake videos using attribution-based confidence metric*", In

Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (pp. 308-309), 2020.

[15] A.M. Rodriguez, Z. Geradts," *Detection of Deepfake Video Manipulation"*, In Proceedings of the 20th Irish Machine Vision and Image Processing conference, Belfast, Northern Ireland, pp. 133-136, 2018, ISBN 978-0-9934207-3-3.

[16] Rohini Sawant and Manoj Sabnis*," A Review of Video Forgery and Its Detection*", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, Volume 20, Issue 2, p-ISSN: 2278-8727, 2018.

[17] Thanh Thi Nguyen, Cuong M. Nguyen, Dung Tien Nguyen, Duc Thanh Nguyen and Saeid Nahavandi," *Deep Learning for Deepfakes Creation and Detection"*, IEEE, pp. 1-12, 2019.

Authors Profile

Bismi Fathima Nasar received her B. Tech degree in Electronics and Communication from TKM Institute of Technology, Kerala in 2017. She perused her M. Tech degree in Cyber Forensics and Information Security from ER & DCI Institute of Technology, CDAC, Kerala in 2020. She is currently working as Associate Cyber Security Analyst at Saint-Gobain, Mumbai. Her main area of interest includes Cyber Security, Ethical Hacking, Deep Learning, Cyber Forensics and advanced Machine Learning for real time implementation.

Sajini T received her B. Tech degree in Electronics and Communication from College of Engineering - Chenganur, Kerala. She perused her M. Tech degree in Signal Processing from College of Engineering – Thiruvananthapuram, Kerala. She is currently working as Scientist E at CDAC, Thiruvananthapuram. Her main area of interest includes Speech Synthesis and Speech Signal Processing.

Elizabeth Rose Lalson received her B. Tech degree and M. Tech degree from Cochin University of Science and Technology, Kerala She is currently working as Assistant Professor at ER & DCI Institute of Technology, CDAC, Thiruvananthapuram. Her main area of interest includes Cryptography, Network Security, Machine Learning etc.

